GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

GB/T 20271-2006

Information Security Technology – Common Security Techniques Requirement for Information System

Issued on: May 31, 2006 **Implemented on: December 1, 2006**

Issued by: **General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China;**

Standardization Administration of the People's Republic of China.

Table of Contents

Foreword

Appendixes A, B and C of this Standard are informative.

This Standard was proposed by and shall be under the jurisdiction of the National Technical Committee on Information Security of Standardization Administration of China.

Drafting organizations of this Standard: Beijing Siyuan Xinchuang Information Security Information Co. Ltd. AND Technical Service Center of Jiangnan Institute of Computing Technology.

Main drafters of this Standard: Ji Zengrui, Wang Zhiqiang, Chen Guanzhi, Jing Qianyuan and Song Jianping.

Introduction

This Standard mainly, from the classification of information system security protection level, specifies the security technical measures which shall be taken to realize the security function requirements of each security protection level as specified in GB 17859-1999 and the differences of security protection levels in specifically realizing the security function.

A complex large/enormous type of information system may be composed of several subsystems. Generally, from the angle of total system, subsystem or subsystem, the information system is composed of hardware system (including computer hardware system and network hardware system) supporting the software operation, system software (including computer operating system software, database management system software, network protocol software and management software) managing the system resource and providing basic support for the user, application system software realizing the application function of information system, and etc. These hardware and software operate in coordination, realizing the integral function of information system. From the security perspective, the hardware and software constituting each part of the information system shall be provided with appropriate security functions to ensure the information security within their jurisdiction and provide definite service. These security functions are: physical security ensuring the hardware system security, network security ensuring the data security during on-line transport and exchange, and system security (including protection for system security operation and data security) ensuring the security of operating system and database management system. Such four security layers, together with management measures which must be taken to ensure its security function to reach proper security, constitute five security layers to realize the information system security. Actually, many security functions and realization mechanisms are the same among such layers. For example, identity authentication, audit, access control, confidentiality protection, integrity protection and etc. are embodied in each layer and provided with corresponding security requirements. Security functions are described from the angle of security techniques in this Standard. The requirements of each security technique (including function requirements and assurance requirements) are generally applicable. For example, the description of identity authentication is not only applicable to operating system, but also to network system, database management system and application system. Such method describing security techniques requirement according to security element is simple and clear.

Technical contents of security function requirements and security assurance requirements in GB/T 18336-2001 (idt ISO/IEC 15408:1999) are massively adopted in this Standard; corresponding level classification is carried out according to the five levels specified in GB 17859-1999.

Firstly, this Standard comprehensively describes the technical requirements of security

function and security assurance involved in graded protection for information security, and then details the technical requirements of security function and security assurance of each security protection level according to the five security protection levels specified in GB 17859-1999.

It should be specially explained that the information security technology level and information system security level are two different but mutually-related concepts. This Standard is the description for technical requirements of information security technology of different security levels. Information technology security level is determined according to the realization differences of security function technology and security assurance technology by reference to domestic and foreign existing standards, and combining with the actual situation of current information system security in China. Whereas the security level of information system is determined according to the security requirements of information system by reference to the adopted security technology level (see "About Information Security Technology Level and Information System Security Level" (A.6) for detailed description of relevant concepts). Appendix B provides design reference for graded information system security to help the user design and realize information system of different security levels by utilizing these security techniques.

Appendix C provides the corresponding relationship between the elements and graded requirements of security technology of information system. Table C.1 is the corresponding relationship between the elements and graded requirements of security function technology, while Table C.2 is the corresponding relationship between the elements and graded requirements of security assurance function.

Chapter 6 specifies the description for technical requirements of security function and security assurance of every security protection level. In order to clearly express the addition and strengthening of security techniques requirement for each security level compared with those of the lower level, the newly added part of each level is indicated in **"bold"**.

Information Security Technology - Common Security Techniques Requirement for Information System

1 Scope

This Standard specifies the requirements of every security level for the security technology required for information system security according to the classification of five security protection levels in GB 17859-1999.

This Standard is applicable to the design and realization of security information system according to the graded requirements, and serves for reference for the test and management of the information system security implemented according to graded requirements.

2 Normative References

The following normative documents contain the provisions which, through reference in this text, constitute the provisions of this Standard. For dated references, the subsequent amendments (excluding corrigendum) or revisions of these publications do not apply. However, all parties who enter into an agreement according to this Standard are encouraged to study whether the latest edition of the normative document is applicable. For undated references, the latest edition of the normative document applies.

GB 17859-1999 Graded Criteria for Security Protection of Computer Information System

GBJ 45-1982 Specifications for the Design of Highrise Civil Buildings (Trial) - Fire Prevention

TJ 16-1974 Code for Design of Building Fire Protection

3 Terms, Definitions and Abbreviations

3.1 Terms and Definitions

For the purposes of this Standard, the terms and definitions specified in GB 17859-1999 AND those listed below apply.

3.1.1

Security of information system

The representation of confidentiality, integrity and availability of information system and the information that are stored, transported and processed by information system.

3.1.2

Common security technology of information system

The security technology that is generally applicable for realizing various types of security of information system.

3.1.3

Security subsystem of information system

A generic term for security protection devices in information system, including hardware, firmware, software and combined entity responsible for implementing security policy. It establishes a basic security protection environment for information system, and provides additional user service required for security information system.

Note: According to the definition of TCB (trusted computing base) in GB 17859-1999, SSOIS (security subsystem of information system) is TCB of information system.

3.1.4

Security element

The composition of security contents that is contained in technical requirements of security function and security assurance in this Standard.

3.1.5

Security function policy

The security policy that is adopted to realize the function required for SSOIS security element.

3.1.6

Security function

The function that is provided to realize security element requirements and correctly implement corresponding security function policy.

3.1.7

Security assurance

The method and measure that are taken to ensure that the security function of security element meets the required security target.

3.1.8

SSOIS security policy

A group of rules for managing, protecting and allocating resources in SSOIS. A SSOIS may contain one or more security policies.

3.1.9

SSOIS security function

The function that is provided by all hardware, firmware and software correctly implementing SSOIS security policy. The realization of each security policy constitutes a SSOIS security function module. All security function modules of a SSOIS constitute the security function of this SSOIS.

3.1.10

SSF scope of control

The scope of subject and object that is involved in SSOIS operation.

3.1.11

User identification

It is used to indicate the user identity and ensure the uniqueness and identifiability of the user in system. Generally, the user name and user identifier (UID) are used to indicate the user in system. Both user name and user identifier are published plain code information.

3.1.12

User authentication

The confirmation for the authenticity of user identity with specific information. Generally, information used for authentication is not published and is difficult to be imitated.

3.1.13

User-subject binding

It refers to that the designated user is associated with the subject (e.g. process) serving it with certain method.

3.1.14

Label of subject and object

The sensitivity label that is designated for subject and object. These sensitivity labels are the combination of level classification and non-level category as well as the reference for performing mandatory access control.

3.1.15

Security attribute

The information that relates to subject and object used for implementing security policy. For discretionary access control, security attribute includes relevant information determining the access relationship of subject and object; for mandatory access control adopting multi-level security policy model, security attribute includes information of identification and security label of subject and object.

3.1.16

Discretionary access control

The method that initiatively specifies the object access right by the owner subject of this object. The subject having access right can access the designated object in authorization mode, and can transfer access right according to authorization.

3.1.17

Mandatory access control

The method that determines the access right of subject to object by the system according to the sensitivity label contained in subject and object. The subject having access right can access the designated object in authorization mode. The sensitivity label is arranged and maintained by system security officer or automatically by the system according to specified rules.

3.1.18

Rollback

The process that revokes last / a series of operation and returns to the known state before this operation due to certain cause.

3.1.19

Trusted channel

The communication path that is established and maintained between SSF and other

a) Water pipe installation requirements: the installation of water pipe shall not penetrate the roof and below the movable floor; for water pipe penetrating the wall and slab, sleeve shall be adopted and reliable sealing measures shall be taken;

b) Water hazards prevention: certain measures are taken to avoid rainwater from passing through the roof, indoor vapor from condensation and underground accumulated water from transfer and penetration;

c) Waterproofing inspection: water sensitive instrument or component is installed to carry out waterproofing inspection for machine room and timely alarm when finding water hazard;

d) Drainage requirements: the machine room shall be equipped with drainage outlet and installed with water pump so as to rapidly exhaust the accumulated water.

4.1.1.1.7 Static protection for machine room

Static protection for machine room is graded as follows according to different requirements for security protection of machine room:

a) Earthing and shielding: necessary measures are taken to provide a set of reasonable static protection earthing and shielding system;

b) Static protection for garment: apparel fabric not liable to generate static is adopted for personnel garment while low-resistance material is selected for footwear;

c) Temperature and humidity static protection: the temperature and humidity of machine room is controlled to make them within the range not liable to generate static;

d) Static protection for floor: the resistance value of machine room floor from the surface to earthing system shall be within the range not liable to generate static;

e) Static protection for material: materials generating small static shall be selected for various furniture, workbenches and cabinets used in machine room;

f) Maintenance MOS circuit protection: during hardware maintenance, special maintenance platform shall be adopted for the metal plate tabletop to protect the MOS circuit;

g) Static elimination requirements: static inhibitor, electrostatic eliminator and etc.

are used in machine room to further reduce the static generation.

4.1.1.1.8 Earthing and lightning protection for machine room

Earthing and lightening protection for machine room is graded as follows according to different requirements for security protection of machine room:

a) Earthing requirements: ground pile, horizontal grid mesh, metal plate and building foundation reinforcement are adopted to construct the earthing system to ensure favorable earthing of the earthing electrode;

b) Decoupling and filtering requirements: arrange signal ground and DC power supply ground and pay attention to not cause additional coupling to ensure favorable effect of decoupling, filtering and etc.;

c) Lightning protection requirements: arrange lightning protection ground and regard the deeply buried and favorably earthed metal plate as the earthing point; thick red copper strip shall be adopted for the lead to lightning rod, or the reinforcement of the whole building whole building is welded into a reinforcement mesh below the foundation and is connected with the lightning rod as the "ground";

d) Requirements for shelter ground and shield ground: security shelter ground and shield ground are arranged and thick wire of good conductor with impedance as small as possible is adopted to reduce the potential difference among various grounds; welding method shall be adopted, earthing condition shall be regularly inspected and earthing resistance is tested to ensure the security of human body, equipment and operation;

e) Earth wire requirements for AC power supply: earth wire of AC power supply is arranged; AC power supply line shall be provided with three-core wire (namely phase wire, neutral wire and earth wire) regulating the connecting position, and the "earth wire" shall be connected to the ground net to ensure its security protection function.

4.1.1.1.9 Electromagnetic protection for machine room

Electromagnetic protection for machine room is graded as follows according to different requirements for security protection of machine room:

a) Earthing anti-interference: earthing method is adopted to avoid the interference on computer system by intercoupling between external electromagnetism and equipment;

b) Shield anti-interference: shield method is adopted to avoid instant interference on computer system by external electrical equipment;

c) Distance anti-interference: distance protection method is adopted to locate the computer room in position with low external electromagnetic interference and far away from potential radiated signal;

d) Electromagnetic compromising emanation protection: necessary measures shall be taken to avoid information leakage caused by electromagnetic compromising emanation generated by computer equipment;

e) Medium protection: during the storage of magnetic media like tape and disk, attention shall be paid to the effect of electromagnetic induction, such as storage in iron cabinet;

f) Machine room shield: shield method is adopted to carry out electromagnetic shielding for computer room and further to avoid the interference on computer equipment by exterior electromagnetic field and the information leakage caused by electromagnetic signal leakage.

4.1.1.2 Security protection for communication line

Security protection for communication line is graded as follows according to different requirements for security protection of communication line:

a) Ensuring line smoothness: take necessary measures to ensure the smoothness of communication line;

b) Finding line intercept: take necessary measures to find line intercept event and then alarm;

c) Timely finding line intercept: take necessary measures to timely find line intercept event and then alarm;

d) Avoiding line intercept: take necessary measures to avoid line intercept event.

4.1.2 Equipment Security

4.1.2.1 Burglary prevention and crash protection for equipment

Burglary prevention and crash protection for equipment are graded as follows according to different requirements for equipment security:

a) Labeling requirements for equipment: equipment and component of computer system shall be provided with visible and irremovable label to avoid replacement and be convenient for searching booty;

b) Burglary prevention for computing center ① : burglary prevention and alarm device shall be installed for computing center to avoid burglary by breaking into from window or door;

c) Burglary prevention for computing center ② : the computing center shall be arranged with machine room alarm system by utilizing light, electricity and passive infrared techniques and shall be attended by specific personnel to avoid burglary by breaking into from window or door;

d) Burglary prevention for computing center ③ : all important positions of the computing center are monitored by utilizing closed circuit television system, and the computing center is attended by specific personnel to avoid burglary by breaking into from window or door;

e) Burglary prevention for external equipment of machine room: reinforcement protection and other measures shall be taken for external equipment of machine room; where necessary, it shall be attended by specific personnel to avoid burglary and damage.

4.1.2.2 Security and availability of equipment

The security and availability of equipment may be graded as follows according to different requirements for equipment security:

a) Basic operation support: all equipment of information system shall be provided with basic operation support and shall possess necessary tolerance and fault recovery capability;

b) Security and availability of equipment: all equipment supporting the information system operation, including computer main, external equipment, network equipment and other auxiliary equipment, etc. shall be secure and available;

c) Uninterruptible operation of equipment: provide reliable operation support and support the information system to realize uninterruptible operation by taking tolerance and fault recovery measures.

4.1.3 Record Medium Security

Record medium security is graded as follows according to different requirements for equipment security:

a) Public data medium protection: certain measures shall be taken for various record media storing useful data, like paper medium, magnetic medium, semi-conductor medium, optical medium and etc., to avoid crash and damage;

b) Internal data medium protection: certain measures shall be taken for various record media storing internal data, like paper medium, magnetic medium, semi-conductor medium, optical medium and etc., to avoid burglary, crash and damage; certain measures shall be taken for internal data which is

required to be deleted and destroyed to avoid illegal replication;

c) Important data medium protection: relatively strict protection measures shall be taken for various record media storing important data, like paper medium, magnetic medium, semi-conductor medium, optical medium and etc., to avoid burglary, crash and damage; important data which shall be deleted and destroyed shall be provided with valid management and approval procedures to avoid illegal replication;

d) Key data medium protection: strict protection measures shall be taken for various record media storing key data, like paper medium, magnetic medium, semi-conductor medium, optical medium and etc., to avoid burglary, crash and damage; key data required to be deleted and destroyed shall be provided with strict management and approval procedures and effective measures to avoid illegal replication;

e) Nuclear data medium protection: the strictest protection measures shall be taken for various record media storing nuclear data, like paper medium, magnetic medium, semi-conductor medium, optical medium and etc., to avoid burglary, crash and damage; key data shall be stored for long term and provided with effective measures to avoid illegal replication.

4.2 Operation Security

4.2.1 Risk Analysis

The risk analysis of information system shall be carried out according to the following requirements:

a) Comprehensively analyze the security risk caused by physical, systemic, management, man-made and natural reasons by starting from system security operation and data security protection;

b) Define the risks existing in the system and find out overcoming methods by knowing and analyzing many factors affecting security operation of information system;

c) Analyze common risks (e.g. back door/trap door, use rejection, radiation, embezzlement, counterfeit, impersonation, logic bomb, destructive activity, stealing, wiretap on-line, computer virus, etc.) to determine the degree of each risk;

d) Static risk analysis shall be carried out before design and operation of system so as to found potential security risks in system;

e) Dynamic risk analysis shall be carried out during the system operation

process to test, trace and record its activity so as to find security leak during the system operation period and provide corresponding system vulnerability analysis report;

f) Adopt risk analysis tools to carry out risk analysis and determine security countermeasure through methods like collecting, analyzing and outputting data, determining the severity level, analyzing dangerous probability, etc.

4.2.2 Test and Analysis of Information System Security

According to different requirements on security operation of information system, test and analysis of information system security are divided into:

a) Test and analysis of operating system security: assess the file approval, file host, network service setting, account setting, program factuality, general security points and invasion phenomenon correlated with the user, etc. from the aspect of operating system in the capacity of administrator to test and analyze operation system security and find the existing potential security risks;

b) Test and analysis of database management system security: for the test and analysis of security for database management system supporting information system operation, it is required to analyze its existing disadvantage and leak by scanning specified security vulnerability of database management system in database system correlated with authentication, authorization, access control and system integrity setting, and propose remedial measures;

c) Test and analysis of network system security: adopt intrusion simulator to automatically scan, test and report the defect and leak existing in network system (including each constituent part of security network system like fire wall) through the method of simulating intrusion at key parts of network equipment and propose remedial measures to enhance the network security;

d) Test and analysis of application system security: for the test and analysis of security for the developed application system, it is required to analyze its existing defect and leak by scanning specified security vulnerability in application system concerned with authentication, authorization, access control and system integrity, and propose remedial measures;

e) Test and analysis of hardware system security: for the security test of hardware system supporting system operation, analyze its existing defect and leak by scanning specified security vulnerability (including electromagnetic compromising emanations, electromagnetic interference, etc.) in hardware system concerned with system operation and data protection, and propose remedial measures;

f) Test and analysis of attack: carry out the attack test for important information

4.3 Data Security

4.3.1 Identity Authentication

4.3.1.1 User identification and authentication

4.3.1.1.1 User identification

According to different requirements on user identification and authentication, user identification is divided into:

a) Basic identification: the user who proposes the operation shall be identified before SSF executes the required operation;

b) Unique identification: the uniqueness of the identified user shall be ensured within the life cycle of information system and the user identification shall be associated with security audit;

c) Identification information management: the user identification information shall be managed and maintained so as to ensure that it is not unauthorizedly accessed, modified or deleted.

4.3.1.1.2 User authentication

According to different requirements on user identification and authentication, user authentication is divided into:

a) Basic authentication: the user who proposes operation shall be authenticated before SSF executes the required operation.

b) Unforgeable authentication: the use of forged or replicated authentication information shall be tested and avoided. On one hand, SSF is required to test or avoid authentication data forged or replicated by any other users; on the other hand, it is required to test or avoid the application of authentication data replicated by the current user from any other users.

c) Disposability authentication: authentication mechanism for disposable authentication data shall be provided, namely SSF shall avoid the reuse of identified authentication data relevant with the authentication mechanism.

d) Multi-mechanism authentication: different authentication mechanisms shall be provided for authenticating the user identity of special event, and the identity alleged by any user shall be authenticated according to the authentication rules described by different authentication mechanisms.

e) Re-authentication: it shall have the capability to specify the user's event requiring re-authentication, namely re-authentication is carried out to the user

where the re-authentication condition is applicable. For example, re-authentication is required for reconnection where it is disconnected due to operation timeout of end user.

f) Authentication information management: the user authentication information shall be managed and maintained so as to ensure that it's not unauthorizedly accessed, modified or deleted.

4.3.1.1.3 Authentication failure handling

A value shall be defined for unsuccessful authentication attempt (including attempt frequency and time threshold) and the operation which shall be taken where this value is reached shall be explicitly specified by SSF. Authentication failure handling shall include the test of the condition where the frequency of relevant unsuccessful authentication attempt is the same with the specified one and the predefined handling.

4.3.1.2 User-subject binding

An identified and authenticated user shall be associated with its service subject (e.g. process) through user-subject binding within the control scope of SSOIS security function to associate the user identity with all its auditable behaviors for realizing the check-ability of user behavior.

4.3.1.3 Concealing

SSOIS shall provide the user with protection avoiding discovery or misuse by other users under the premise of ensuring identity authenticity. According to different requirements on identity authentication, concealing is divided into:

a) Cryptonym: the user identity is not exposed while using resource or service, namely, it shall be ensured that the actual user associated with current subject and/or operation can't be determined by any user and/or subject, and the actual user name is not asked while providing services for the subject;

b) Alias: the authentic name of the user is not exposed while using the resource or equipment, but it can still be responsible for such use; namely, it shall be ensured that the actual user name associated with current subject or operation can't be determined by the user and/or subject set, multiple aliases can be are provided for one user, and whether the alias used meets the alias measurement can be verified;

c) Unlink-ability: the resource and service may be used by one user for several times, while these uses can’t be associated by any person; namely: it shall be ensured that whether certain operations in the system are caused by the same user can't be determined by any user and/or subject;

d) Unobservability: where the resource and service are being used by the user, they can't be observed by other person, especially the third party; namely, it shall be ensured that the operation carried out by the protected user and/or subject on the object can't be observed by any user and/or subject.

4.3.1.4 Equipment identification and authentication

4.3.1.4.1 Equipment identification

According to different requirements on equipment identification and authentication, equipment identification is divided into:

a) Identification before connection: equipment being connected to information system shall be identified before being connected to the system;

b) Identification information management: equipment identification information shall be managed and maintained so as to ensure that it's not unauthorizedly accessed, modified or deleted.

4.3.1.4.2 Equipment authentication

According to different requirements on equipment identification and authentication, equipment authentication is divided into:

a) Authentication before connection: equipment being connected to information system shall be authenticated before being connected to the system to avoid illegal connection of equipment;

b) Unforgeable authentication: authentication information shall be invisible and uneasy to forge, and the forged or replicated authentication information shall be tested and avoided;

c) Authentication information management: the equipment authentication information shall be managed and maintained so as to ensure that it is not unauthorizedly accessed, modified or deleted.

4.3.1.4.3 Authentication failure handling

Authentication failure handling shall be realized by carrying out preliminary definition on value of unsuccessful authentication attempt (including attempt frequency and time threshold) and explicitly specifying the measure which shall be taken where this value is reached.

4.3.2 Non-repudiation

4.3.2.1 Non-repudiation of origin

The data sender shall be ensured failing to successfully deny the sending of this data before. SSF is required to provide a method to ensure that the data receiving subject is capable of obtaining the evidence proving data origin during data exchanging period, moreover, this evidence may be verified by this subject or the subject of the third party. According to different requirements on non-repudiation, the non-repudiation of origin is divided into:

a) Selective origin certification: SSF shall be provided with the capability of generating origin evidence of the transported data according to the subject's request, namely, the SSF is capable of generating the origin evidence of the transported data upon receiving the recipient to prove that this data is sent by this originator;

b) Mandatory origin certification: origin evidence of the transported data shall always be generated by SSF, namely, SSF is capable of generating origin evidence of the transported data at any time to prove that this data is sent by this originator.

4.3.2.2 Non-repudiation of receipt

The data recipient shall be ensured failing to deny the receiving of this data before. SSF is required to provide a method to ensure that the data sending subject is capable of obtaining the evidence of receiving such data during data exchanging period, moreover, this evidence may be verified by this subject or the subject of the third party. According to different requirements on non-repudiation, the non-repudiation of receipt is divided into:

a) Selective receiving certification: SSF shall be provided with the capability of generating receiving evidence of the transported data according to the subject's request, namely, the SSF is capable of generating the receiving evidence of the transported data upon receiving the recipient to prove that the data is received by this recipient;

b) Mandatory receiving certification: receiving evidence of the transported data shall always be generated by SSF, namely, SSF is capable of generating receiving evidence of the transported data at any time to prove that this data is received by this recipient.

4.3.3 Discretionary Access Control

4.3.3.1 Access control policy

SSF shall be designed according to the established discretionary access control security policy to realize the operation control of the subject to object under the policy control. Multiple discretionary access control security policies are allowable, but they must be designated independently without mutual conflict. Common discretionary

access control policies include: access control of access control list, directory list and capability list, etc.

4.3.3.2 Access control function

SSF shall realize the specific function of adopting a designated access control policy, and describe the application, characteristic and the control scope of the policy.

Regardless of which discretionary access control policy is used, SSF shall be able to provide:

— Execute access control SFP on object of security attribute or designated security attribute team;

— Allow the subject to access the object on the basis of the rules of security attribute of allowing access from the subject to the object;

— Deny access from the subject to the object on the basis of the rules of security attribute of denying access from the subject to the object.

4.3.3.3 Scope of access control

According to the different requirements of discretionary access control, coverage of discretionary access control is graded into:

a) Subset access control: for each established discretionary access control, SSF shall cover the defined subject, object and operation between them in security system;

b) Full access control: for each established discretionary access control, SSF shall cover all the defined subjects, objects and operations between them in information system, namely SSF shall ensure that all the operations between any subject and any object within SSC are covered at least by one established access control SFP.

4.3.3.4 Granularity of access control

According to the different requirements of access control, granularity of discretionary access control is graded into:

a) Coarse granularity: the subject is user group/user level, and the object is document and database table level;

b) Medium granularity: the subject is user level, and the object is document and database table level and/or record and field level;

c) Fine granularity: the subject is user level, and the object is document and

database table level and/or records, field and/or element level.

4.3.4 Label

4.3.4.1 Subject label

Sensitivity labels shall be designated for the subject implementing mandatory access control, and such sensitivity labels are the basis for implementing mandatory access control. For example, sensitivity labels of level classification and non-level classification are the basis for implementing multi-level security model.

4.3.4.2 Object label

Sensitivity labels shall be designated for the object implementing mandatory access control, and such sensitivity labels are the basis for implementing mandatory access control. For example, sensitivity labels of level classification and non-level classification are the basis for implementing multi-level security model..

4.3.4.3 Output of label

Where data is outputted from the inside of SSC to the outside of its scope of control, sensitivity label of data may be reserved or not as required. According to the different requirements of label, the output of label is graded into:

a) The output of user data without sensitivity label: user data is not provided with data-dependent sensitivity label where it output from the SFP control to the outside of SSC;

b) The output of user data with sensitivity label: user data shall be provided with data-dependent sensitivity label where it is output from the SFP control to the outside of SSC, and the association between sensitivity label and output data is ensured.

4.3.4.4 Input of label

The corresponding sensitivity label shall be provided where data is inputted from the outside of SSF scope of control to the inside of its scope of control, so as to protect the input data. According to the different requirements of label, the input of label is graded into:

a) The input of user data without sensitivity label: SSF shall:

— Execute the access control SFP where user data is input beyond SSC under the control of SFP;

— Omit any data-dependent sensitivity label which is input beyond SSC;

— Execute additional input control rules, and set sensitivity label for input data.

b) The input of user data with sensitivity label: SSF shall:

— Execute the access control SFP where user data is input beyond SSC under the control of SFP;

— Use the sensitivity label related to the data input;

— Provide definite relationship between sensitivity label and the received user data;

— Ensure that the explanation for sensitivity label of the input user data is consistent with that of original sensitivity label.

4.3.5 Mandatory Access Control

4.3.5.1 Access control policy

The mandatory access policy shall include subject(s) and object(s) under the policy control and operation(s) between the controlled subject(s) and object(s) and covered by the policy. Multiple discretionary access control security policies are allowable, but they must be designated independently without mutual conflict. Common mandatory access control policies currently include:

a) Multi-level security model: the basic idea is that, all direct or indirect accesses from all subjects to the object within SSOIS scope of control on the basis of labeling the subject and object, shall meet the following requirements:

— Downward reading principle: the subject can read the object only when the level classification of subject label is higher than or equal to that of object and the non-level classification of subject label includes all that of object label;

— Upward reading principle: the subject can read the object only when the level classification of subject label is lower than or equal to that of object label and the non-level classification of subject label is included in that of object label.

b) Role-based access control (BRAC): the basic idea is that, the permission is distributed and managed based on the roles; the subject gains the authority of corresponding role by granting the subject roles; the corresponding role authority gained by the subject is canceled by revoking the granted role of the subject. In the role-based access control, label information is the authorized information of the subject.

c) Privileged user management: the basic idea is that, the permission of privileged user is managed according to the least privilege principle in allusion to the security risk caused by excessive concentration of its authority. The permission separation of privileged user is realized; the privileged user is only granted with the least privilege required for completing his tasks.

4.3.5.2 Access control function

SSF shall explicitly point out the specific function realized by adopting one designated mandatory access control policy. SSF shall be able to provide:

— Execute access control SFP on the object of label or designated label group;

— Decide to allow the controlled subject to execute the controlled operation to the controlled object according to the rules of allowing the access between the controlled subject and the controlled object;

— Decide to deny the controlled subject to execute the controlled operation to the controlled object according to the denied access rules between the controlled subject and the controlled object.

4.3.5.3 Scope of access control

According to the different requirements of mandatory access control, coverage of mandatory access control is graded into:

a) Subset access control: for each established mandatory access control, SSF shall cover the subject and the object which are defined by security function and operation between them in information system;

b) Full access control: for each established mandatory access control, SSF shall cover the defined subject, object and operation between them in information system, namely SSF shall ensure that all operations between any subject and any object within SSC are covered at least by one established access control SFP.

4.3.5.4 Granularity of access control

According to the different requirements of mandatory access control, granularity of mandatory access control is graded into:

a) Medium granularity: the subject is user level, and the object is document, database table level and/or record and field level;

b) Fine granularity: the subject is user level, and the object is document, database table level and/or record, field and/or element level.

4.3.5.5 Access control environment

For mandatory access control, different system operation environment below shall be considered:

a) Single security domain environment: the mandatory access control implemented in the single security domain environment shall maintain uniform label information and access rule in this environment. Where the controlled object is output beyond security domain, its label information shall be output simultaneously;

b) Multi-security domain environment: where the mandatory access control of the uniform security policy is implemented in multi-security domain environment, uniform label information and access rule shall be maintained in this environment. Where the controlled object moves among these security domains, the label information shall be moved accordingly.

4.3.6 Integrity Protection for User Data

4.3.6.1 Integrity of stored data

Integrity protection for user data stored in SSC shall be carried out. According to the different integrity protection requirements of user data, integrity of stored data is graded into:

a) Integrity test: integrity test shall be carried out by SSF where reading user data stored in SSC in order to find the damage condition of data integrity;

b) Integrity test and recovery: integrity test shall be carried out by SSF where reading user data stored in SSC, and necessary recovery measures should be taken where the integrity error is tested.

4.3.6.2 Integrity of transported data

Integrity protection for user data shall be provided where transported between SSFs. According to the different integrity protection requirements of user data, integrity of transported data is graded into:

a) Integrity test: during the transport, integrity test for user data of network transport shall be carried out to timely find the conditions of tampering, deletion and insertion of the user data transported or received in certain manner;

b) Integrity test and recovery: during the transport, integrity test for user data of network transport shall be carried out to timely find the conditions of tempering, deletion and insertion of user data transported or received in certain manner;

and necessary measures are taken where integrity error is tested.

4.3.6.3 Integrity of processed data

The data processed in information system shall be subject to integrity protection through "rollback", namely SSF shall execute the processed data integrity SFP in order to allow the rollback the defined operation sequence.

4.3.7 Confidentiality Protection for User Data

4.3.7.1 Confidentiality protection for stored data

User data stored in SSC shall be subject to the confidentiality protection with varying degrees according to different confidentiality requirements of different data types, thus ensuring that other users (except for the legal users with access permission) cannot obtain the data.

4.3.7.2 Confidentiality protection for transported data

User data transported among different SSFs or different SSF users shall be subject to confidentiality protection with varying degrees according to different confidentiality requirements of different data types, thus ensuring that data is free of divulging and stealing during the transport.

4.3.7.3 Secure reusing of object

In the dynamic management system of resources, the residual information of object resources (recording media such as register, internal memory, magnetic disk, etc.) shall not cause information leakage. According to different requirements for confidentiality protection of user data, secure reusing of object is graded into:

a) Subset information protection: the original information in the object shall not be divulged where the object resources of a certain subset within the scope of SSOIS security control are released and redistributed to a certain user or on behalf of the process operated by this user;

b) Complete information protection: the original information in the object shall not be divulged where all object resources within the scope of SSOIS security control are released and redistributed to a certain user or on behalf of the process operated by this user;

c) Special information protection: on the basis of complete information protection, special methods shall be adopted to completely eliminate the residual information in the object resources (such as remanence elimination, etc.) for some information in need of special protection.

4.3.8 Data Flow Control

In information system realizing data flow by means of data flow, the data flow control mechanism shall be adopted to realize the data flow control, and to prevent data information with high security level from flowing to the area with low-level.

4.3.9 Trusted Path

Trusted path between the user and SSF shall:

a) Provide real endpoint identification and protect communication data from modification and leakage;

b) Initiate communication of trusted path through SSF itself, local user or remote user;

c) Use trusted path(s) for the authentication of originator or other service(s) in need of trusted path(s).

4.3.10 Password Support

Graded configuration of password support with corresponding password management level shall be provided according to the matching principle of cryptographic strength with security protection level of information system and the requirements of the national competent password authority.

5 Technical Requirements of Security Assurance

5.1 SSOIS Self-security Protection

5.1.1 SSF Physical Security Protection

5.1.1.1 Physical attack test

Specific test method is provided to deal with the potential physical tampering jeopardizing the security of SSF, and the authorized user shall check security by activating the automatic security test function or using manual mode, so as to identify whether the tampering occurs or not.

5.1.1.2 Automatic report of physical attack

On the basis of the above physical attack test, the physical tampering shall be automatically reported to the designated user where it is found.

5.1.1.3 Physical attack resistance

On the basis of the automatic report of above physical attack, physical tampering shall

be resisted for SSF equipment or SSF element so as to protect SSP from damage. For example, according to the requirements of integrity policy, information stored in certain storage medium is kept to be writable so as to protect it from tampering.

5.1.2 SSF Operation Security Protection

5.1.2.1 Security operation test

SSF shall provide security operation test for SSF software periodically under normal operation, as required by the authorized user or under other conditions, through operating test suit during the system initialization, so as to verify that the security assumption provided by SSF can be executed correctly.

5.1.2.2 Failure protection

Where the established failure tape emerges in SSF, a protection state shall be preserved. This protection state ensures the correctness of security policy where recovering from the failure.

5.1.2.3 Replay test

The replay of established entity (message, service request, service response, session, etc.) shall be tested so as to avoid the replay attack effectively, and execute the operation shown in the operation list in case of any replay request. These operations include: ignoring the replayed entity, confirming entity from the source of identification, and terminating the activity of the original subject of replayed entity.

5.1.2.4 Reference arbitration

For a specified SFP, the access monitor and/or front-end filter realized shall be "always activated", executed correctly and successfully; thus all actions in the mandatory execution shall be confirmed by SSF, namely SSF shall be featured with non-bypassing and tamper-proofing towards SSP.

5.1.2.5 Domain separation

SFP shall ensure at least a security domain to protect SSF implementation from external interference and tampering (e.g. modify the SSF code or data structure) by the untrusted subject. According to the different requirements of SSF operation security protection, domain separation is graded into:

a) SSF domain separation: SSF shall be provided with different protection domains and separation among objects in SSC. The specific requirements of SSF domain separation are as follows:

— SSF shall maintain a security domain for its execution to avoid the interference and tampering of the untrusted subject;

only, correct generation of SSOIS configuration item is assisted by introducing automatic CM, and changes between SSOIS and its previous version and future version are defined. According to different requirements of configuration management, CM automation is graded into:

a) Partial automation of CM: realization expression of SSOIS shall be ensured that it is controlled in automatic mode so that problems, which are hard to solve, of complicated realization or cooperative development by numerous partners, and various changes in the development process are solved, and these changes are ensured to be generated by authorized behavior. Requirements of partial automation of CM:

   — CM system used by SSOIS developer shall ensure that realization expression of SSOIS only makes authorized changes in the provided automatic mode, and be able to support the generation of SSOIS by providing automatic mode;

   — CM plan, provided by developer shall describe automated tools used in CM system and how to use them.

b) Full automation of CM: except for the same content of above-mentioned partial automation of CM, it shall also be able to automatically determine the changes among SSOIS versions, and identify configuration item affected by the modification of the remaining configuration items.

5.2.1.3 Configuration management scope

The integrity of these configuration items is ensured by ensuring that CM system traces all necessary SSOIS configuration items. According to different requirements of configuration management, CM scope is graded into:

a) SSOIS configuration management scope: realization expression, design document, test document, user document, security administrator document, CM document, etc. of SSOIS are placed under the CM, so as to ensure that modification is carried out in a correct, authorized and controllable mode, therefore, requirements of CM document provided by developer shall:

   — Show that CM system is able to trace the content under the CM;

   — Describe the way used by CM system to trace these configuration items;

   — Provide adequate information to prove that all requirements are met.

b) Problem-tracking configuration management scope: except for the content described by configuration management scope of SSOIS, tracing for security defect is specially emphasized.

c) Development tool configuration management scope: except for the content described by problem-tracking configuration management scope, tracing for development tools and the relevant information is specially emphasized.

5.2.2 Distribution and Operation

5.2.2.1 Distribution

SSOIS product received by the receiving party shall be ensured to be transported by the very sender without any modification, the primary objective is to test SSOIS and avoid any modification to it in the process of distribution. According to different requirements of distribution and operation, distribution is graded into:

a) Distribution process: distribution of SSOIS or its part shall be provided to users in form of documents, the distributed document shall describe all processes necessary for maintaining security maintenance upon distributing each version of SSOIS to users, and distribution shall be carried out according to this process;

b) Modification test: except for the distribution of SSOIS according to the requirements of distribution process, the distributed document shall also:

— Describe methods and techniques of modification test and the difference between main copy of developer and version received by user;

— Describe the method used to test the attempt of sending product to user by disguising as a developer.

c) Modification prevention: on the basis of modification test, the distributed document shall describe the methods and techniques of how to prevent modification.

5.2.2.2 Operation (installation, generation and start)

It shall be ensured that installation, generation and start is carried out in the security mode which is expected by developer, and realization expression of SSOIS under the control of configuration is securely converted to initial operation in the user environment. The installation, generation and start process may be described in an independent document. According to different requirements of distribution and operation, operation is graded into:

a) The process of installation, generation and start: developer is required to describe that the secure installation, generation and start of SSOIS, and ensure that secure configuration is generated finally;

b) Log generation: document is required to describe the process of establishing

the log, and this log includes generation options generating SSOIS, so that it is able to explicitly determine when and how SSOIS is generated.

5.2.3 Development

5.2.3.1 Function design

According to the requirements of formalization degree and detail degree of the provided SSF external interface, and different requirements of development, function design is graded into:

a) Non-formalized function design: the non-formalized style is used to completely describe SSF and its external interface; function design shall be internally consistent, and the intended use and methods of all the external joints of SSF shall be described; and exceptional case of result and details of wrong information shall be provided in due time;

b) Fully defined external interface: except for the requirements of the above-mentioned non-formalized function design, the function design shall also completely express the basic principle of SSF;

c) Semi-formalized function design: semi-formalized function style is used to describe SSF and its external interface completely, and supported by non-formalized and explanatory text where necessary. The rest requirements are the same as the above;

d) Formalized function design: semi-formalized function style is used to describe SSF and its external interface completely, and supported by non-formalized and explanatory test where necessary. The rest requirements are the same as the above.

5.2.3.2 Security policy modeling

It is ensured that security function in function design can implement the policy of SSF by developing security policy model based on SSP and establishing the correspondence between function design, security policy model and SSP policy. According to different requirements of development, security policy model is graded into:

a) Non-formalized SSOIS security policy model: SSP model shall clarify the correspondence of function design and SSP model, and meet the requirements:

— SSP model shall be non-formalized and describe rules and characteristics of SSP policy which may be modeled;

— SSP model shall include a basic principle and clarify that this model is complete and consistent with all SSP policies which may be modeled;

— The correspondence clarification between SSP model and function design shall describe that security function of function design shall be consistent and complete with SSP model.

b) Semi-formalized SSOIS security policy model: except for the requirements of the above-mentioned non-formalized SSOIS security policy model, the provided SSP model as required shall be semi-formalized;

c) Formalized SSOIS security policy model: except for the requirements of the above-mentioned non-formalized SSOIS security policy model, the provided SSP model as required shall be formalized.

5.2.3.3 High-level design

Requirements of SSOIS security function shall be realized by describing functions of every SSF subsystems and their interrelationship. According to different requirements of development, high-level design is graded into:

a) Descriptive requirements of high-level design:

— System structure of SSOIS is consistently described in the viewpoint of subsystem and in the non-formalized method;

— The security function provided by each subsystem and their interrelationship shall be described;

— Any fundamental hardware, firmware and/or software as required by SSF are identified, and SSF function is provided by the protection mechanism which is realized by them;

— All interfaces of SSF subsystem are identified, and they are marked on SSF subsystem of which interfaces are visible from the outside.

b) Security-intensified high-level design: except for the descriptive requirements of high-level design, the intended use and methods of all the interfaces of SSF subsystem shall be described, and the details of exceptional case and wrong information are provided, and how to separate SSOIS into the intensified unit of SSP and other subsystem is described.

c) Semi-formalized high-level design: except for the security-intensified high-level design, the expression of this high-level design shall be semi-formalized, and provide the complete details of all results to SSF subsystem.

d) Formalized high-level design: except for the requirements of semi-formalized

high-level design, the expression of this high-level design is formalized.

5.2.3.4 Low-level design

For every module of SSF, the realization of its purpose, function, interface, dependence and all SSP intensified functions shall be described. According to different requirements of development, low-level design is graded into:

a) Descriptive requirements of low-level design:

— The expression of low-level design shall be non-formalized with internal consistency, and described in the way of modular terms;

— The purpose of every module is described;

— Interrelationship among modules is defined by the provided security function and dependence terms to other modules;

— How to provide the implementation of every SSP function is described;

— All interfaces of SSF module are identified, interfaces of SSF module which are visible from the outside are identified, and the purposes and methods of all SSF modules are described, and the details of effect, exceptional case and wrong information shall be provided where necessary;

— How to separate SSOIS into SSP implementation module and other modules is described.

b) Semi-formalized low-level design: except for the requirements of low-level design, the low-level design shall be semi-formalized, and the complete details, exceptional case and wrong information of all results to SSF subsystem shall be provided where necessary.

c) Formalized high-level design: except for the requirements of semi-formalized high-level design, the expression of this high-level design is formalized.

5.2.3.5 SSF internal structure

SSF internal structure is designed by adopting modularization, layering, minimized complexity so as to simplify the design of SSF, and reach the analyzable degree. According to different requirements of development, SSF internal structure is graded into:

a) Modularization: SSF shall be designed and constructed in modular method, and the advent of unnecessary interaction among design modules shall be avoided, therefore:

— SSF module shall be identified, and purpose, interfaces, parameter and effect of every SSF module shall be described;

— How does SSF design avoid the unnecessary interaction among independent modules is described.

b) Layering: except for the requirements of modularization, SSF shall also be designed and constructed by means of layering so as to minimize the interaction among design layers, therefore:

— Where SSF is designed and constructed, SSF local complexity shall be minimized by means of strengthening access control policy;

— SSF module shall be identified, and SSF parts strengthening the security policy shall be described;

— The layered structure and the way to minimize the interaction are described;

— The construction method of SSF parts of strengthening the security policy is described so as to reduce the complexity of it.

c) Minimized complexity: except for the requirements of layering, the design and construction of SSF shall also minimize the complexity of whole SSF, therefore:

— Where SSF is designed and constructed, the SSF part implementing any security policy shall be made to be "simple enough to be analyzed";

— Functions which are irrelevant with SSF shall be confirmed to be rejected from SSF.

5.2.3.6 Realization expression

Specific symbolic representation of SSF shall be expressed by means of source code, firmware or hardware, etc. so as to obtain the internal performance of SSF in detail. According to different requirements of development, and realization expression is graded into:

a) SSF subset implementation: SSF realization expression in the level of detail shall be defined for the selected SSF subset unambiguously, and realization expression shall be internally consistent;

b) Full realization of SSF: realization expression shall be provided for the whole SSF, and shall describe the relationship among every part. The rest of requirements are the same as those for implementation of SSF subset;

c) Structured realization of SSF: realization expression shall be the smaller structure, and easy for comprehension. The rest requirements are the same as those for full realization of SSF.

5.2.3.7 Expression correspondence

Various SSF expressions, e.g. adjacent expressions of function design, high-level design, low-level design, realization expression, etc. shall be provided with strict correspondence among them. According to different requirements of development, expression correspondence is graded into:

a) Non-formalized correspondence description: correspondence analysis shall be provided among adjacency pairs which are expressed by the provided SSF, and for every adjacency pairs, it shall be clarified that all correlated security functions represented by abstract SSF are detailed correctly and completely in the less abstract SSF;

b) Semi-formalized correspondence description: except for the non-formalized correspondence requirements, where every part of two adjacency pairs expressed by SSF at least are described in the semi-formalized form, its correspondence description shall be semi-formalized;

c) Formalized correspondence description: except for the semi-formalized correspondence requirements, the requirements shall be met:

— The correspondence of the corresponding part expressed by formalization requirement shall be proved;

— For every adjacency pairs which are expressed by the provided SSF, where one of SSF expression is the semi-formalized while the other expression is at least semi-formalized, the correspondence description among parts is also semi-formalized;

— For every adjacency pairs which are expressed by the provided SSF, if the every part of SSF and adjacency pairs are specified in formalization, the correspondence description among neighboring parts shall also be semi-formalized.

5.2.4 Document Requirements

5.2.4.1 Security administrator guide

The correct mode and method for arranging, maintaining and managing SSOIS shall be described to ensure the secure operation of SSOIS to the maximum. Security administrator guide shall help security administrator comprehend the security function provided by SSOIS, including the requirements that urgent security measures shall be

taken by security administrator. Security administrator guide shall cover the following contents:

a) Describe the management function and interface which is accessible to security administrator;

b) Describe how to manage SSOIS in secure mode;

c) Describe the warnings of function and permission available to security administrator in the security processing environment;

d) Describe all assumptions of users' behavior concerned with security operation;

e) Describe all security parameters controlled by security administrator;

f) Describe every security-related event concerned with management function, including that security characteristics of entity controlled by security function change;

g) Describe all security requirements of system environment concerned with security administrator.

5.2.4.2 User guide

The security function and command and guideline for security function shall be described, including the description of warning information, etc. User guide provides the assumption basis about the application of SSOIS and the measurement of confidence, SSOIS security operation is understood and executed consciously by non-malicious users, application provider and other personnel who use the external interface of SSOIS. User guide may provide independent documents to different users of two categories: one is the user of general operator, the other is the application programmer and/or hardware designer who use the interface between software and hardware. User guide shall include the following contents:

a) Describe the function and interface which are accessible to the user of non-security administrator;

b) Describe the usage of security function and interface which are available to user;

c) Describe that the warnings of function and permission are available to users in the security processing environment;

d) Clarify that the responsibility shall be taken by users in the security operation, including the assumption of user behavior in the security environment;

e) Describe all security requirements of system environment concerned with

users.

5.2.5 Life Cycle Support

5.2.5.1 Development security

Security measures of physical, procedural, personnel and other aspects shall be adopted to protect the security of SSOIS, including the selection of the physical security of development site and developer; appropriate protective measures shall be taken to eliminate or decrease security threats confronted by SSOIS development. According to different requirements of life cycle support, development security is graded into:

a) Security measures description: the provided security document of development shall include the following content:

— Describe necessary security measures of physical, procedural, personnel and other aspects to protect the security of the design and realization of SSOIS in the development environment of SSOIS;

— Provide the evidence of executing security measures in the process of developing and maintaining the SSOIS.

b) Sufficiency of security measures: except for the requirements of security measures description, the evidence of security measures, provided by the development security documents, shall prove that security measures provide necessary protection for maintaining the security of SSOIS.

5.2.5.2 Defect correction

The defects of SSOIS shall be traced and corrected, and the policy and process adopted by defect information and defect correction are provided. According to different requirements of life cycle support, defect correction is graded into:

a) Basic defect correction: requirements in program document of defect correction shall:

— Describe that the process of security defect which has already been reported in all SSOIS versions is used to be traced;

— Describe the property and effect of every provided security defect, and its condition of defect correction;

— Identify the correction measures adopted by every security defect;

— Describe the methods of information, correction and direction for the correction behavior of SSOIS user.

b) Defect report: except for the basic defect correction, the defect report shall also be provided. Defect report shall:

— Record the process of defect correction, and enact measures of user accepting security defect report and the requirements of correcting these defects;

— Describe that the process of security defect which has already been reported in all SSOIS versions is used to be traced;

— It shall be ensured that all known defects during processing the reported security defect are corrected, and the user is informed with correction measures;

— Ensure that correction methods, which are introduced to correct the security defect by the prevention mechanism provided by the reported security defect processing procedure, cannot bring new defects.

c) Organized defect correction: except for the defect report, one or more special connection point(s) for the report and inquiry of SSOIS security issues related to user shall also be designated to take charge of timely issuing the report of security defects and the corresponding methods of them to the registered users who may be affected by such security defects.

5.2.5.3 Life cycle definition

The model of developing and maintaining SSOIS shall be established in the life cycle of SSOIS. Model of life cycle shall include the process, tool and technique used for developing and maintaining SSOIS. The content involved with this model includes design method, reexamination process, project management control, switching control process, test method and receiving process. According to different requirements of life cycle support, the definition of life cycle is graded into:

a) Life cycle model defined by developer: developer shall establish the life cycle model for developing and maintaining SSOIS, which is provided with the necessary control, and the model used for developing and maintaining SSOIS is described in document;

b) Standard life cycle model: developer shall establish the standardized life cycle model which is used for developing and maintaining SSOIS. Standardized life cycle model shall be the model approved by certain expert panel (e.g. subject specialist, standardized entity, etc.). This model shall provide the necessary control for the development and maintenance of SSOIS. Definition document of life cycle provided by developer shall describe the model used for developing and maintaining SSOIS, explain the reason for selecting this model, explain how to use this model to develop and maintain SSOIS, and

clarify the correlation with the model of standardized life cycle;

c) Measurable life cycle model: developer shall establish the life cycle model which is standardized, measurable and used for developing and maintaining SSOIS. Measurable life cycle model shall be provided with arithmetic parameters and/or metrics measuring the developing characteristic of SSOIS (e.g. complexity metric of source code). This model shall provide the necessary control for developing and maintaining SSOIS. Definition document of life cycle provided by developer shall describe the model used for developing and maintaining SSOIS, explain the reason for selecting this model, explain how to use this model to develop and maintain SSOIS, clarify the correlation with the standardized and measurable life cycle model, and provide the measurement result by using the standardized and measurable life cycle model to develop SSOIS.

5.2.5.4 Tools and techniques

Tools used for developing, analyzing and realizing SSOIS shall be well-defined, e.g. programming language, document, realization standard and other libraries supporting the operation of SSOIS, etc. Such tools may be used without further inspection. According to different requirements of life cycle support, tools and techniques are graded into:

a) Well-defined development tools: developer shall identify the tools used for developing SSOIS, and all development tools used for realization shall be well-defined. Documentation of development tool options which are already selected for realization is done by the developer, development tool document shall define the meaning of every sentence of realization and meaning of all options based on the realization explicitly.

b) Comply with the realization of standard - application part: except for the requirements of well-defined development tool, developer shall describe the realization standard of application part.

c) Comply with the realization of standard - all parts: except for the requirements of well-defined development tool, developer shall describe the realization standard of all parts of SSOIS.

5.2.6 Test

5.2.6.1 Test scope

It shall be indicated how the identified test scope can be consistent with SSF like those described in function design. Here it is unnecessary for the developer to cover every aspect of SSF while it is necessary to consider its defects. According to different requirements of test, the test scope is graded into:

a) Evidence of scope: developer shall provide the corresponding evidence to indicate that SSF has already been tested according to function requirements. Evidence of test scope provided by developer shall indicate the correspondence between the identified test in test document and SSF described by function design.

b) Scope analysis: developer shall provide the correspondence analysis to indicate that SSF have tested the function design with system method. Therefore:

— The identified test clarified by developer shall include tests of all security functions described by function design;

— Scope analysis provided by developer shall indicate that the correspondence between the test identified by test document and function design described by SSF;

— Test scope analysis shall clarify that the correspondence between SSF described by function design and test identified by test document is complete.

c) Strict scope analysis: except for the scope analysis, the test scope analysis is required to strictly clarify that all external interfaces identified by function design have been tested completely.

5.2.6.2 Test depth

Test depth determined according to the required security protection level shall be reached. According to different requirements of test, test depth is graded into:

a) High-level design test: high-level design test shall be described in "unit". SSF unit provides a high-level description of SSF internal work. Test of unit level for clarifying defects ensures that the unit has been realized correctly. Test depth analysis provided by developer shall clarify that the identified test in test document is enough to indicate the consistency between the behavior of SSF and high-level design.

b) Low-level design test: test of SSF low-level design shall be described in "module". SSF module provides the low-level description of SSF internal work. Test of module level for clarifying defects ensures that SSF module have been realized correctly. Test depth analysis provided by developer shall clarify that the identified test in test document is enough to indicate the consistency between the high-level design and low-level design.

c) Realization expression test: it shall be ensured that design requirements of SSF have been realized correctly. Test depth analysis provided by developer

cannot have the roles of auditor and the administrator simultaneously, and user having the role of assistant must also have the role of owner, etc.".

c) Acting as the security role: the request of acting as a certain role is proposed explicitly to SSF. PP shall specify the request of requiring to becoming a specific role (e.g. auditor or administrator, etc.).

5.3.5 Centralized Management of SSOIS Security Mechanism

The centralized management function shall be provided for security mechanism of SSOIS. These functions shall include:

a) Configuration and management of security mechanism: for security mechanism and product (including security products of different manufacturer) of every layer, every security domain, and every procedure which distributed in information system, according to the established security policy and operation requirement, the uniform configuration and management is carried out to make security function and performance of information system reach the security target as required;

b) Collection and analysis of security information: collect the security-related information generated in the operation of information system, including various audit information, inspection and monitoring message, and other security-related information, and use the method of risk analysis to analyze such information, and find the attack and threat of information system, and propose the remedial methods and measures.

6 Graded Requirements for Security Technology of Information System

6.1 Level-1: the User's Discretionary Protection Level

6.1.1 Physical Security

6.1.1.1 Environmental security

6.1.1.1.1 Central machine room security

The central machine room security function is designed and realized according to the requirements of 4.1.1.1. It is required by this security protection level to:

a) Select the machine room site according to the description of basic requirements in 4.1.1.1.1;

b) Design and realize internal security protection of machine room according to

the requirements of access and article management of machine room in 4.1.1.1.2;

c) Design and realize the machine room fire protection according to the requirements of fire prevention for building material ① and alarm and fire extinguishing system ① in 4.1.1.1.3;

d) Design and realize power supply and distribution of machine room according to the requirements of separate power supply and emergency power supply ① in 4.1.1.1.4;

e) Design and realize waterproofing and moisture proofing for machine room according to basic temperature requirements in 4.1.1.1.5;

f) Design and realize the waterproofing and moisture proofing of machine room according to the requirements of water pipe installation and water hazards prevention in 4.1.1.1.6;

g) Design and realize static protection according to the requirements of earthing and shielding, and garment static protection and temperature and humidity in 4.1.1.1.7;

h) Design and realize earthing and lightning protection of machine room according to the requirements of earthing, decoupling and filtering as well as lightning protection in 4.1.1.1.8;

i) Design and realize electromagnetic protection according to the requirements of earthing, shielding and distance anti-interference in 4.1.1.1.9.

6.1.1.1.2 Communication line security

The communication line security protection is designed and realized according to the requirements of ensuring line smoothness in 4.1.1.2.

6.1.1.2 Equipment security

The equipment security function is designed and realized according to the requirements of 4.1.2. The security protection level requires to:

a) Design and realize equipment security protection according to the requirements of equipment labeling and burglary prevention for computing center ① in 4.1.2.1;

b) Design and realize equipment security function according to the requirements of basic operation support in 4.1.2.2.

6.1.1.3 Record medium security

Record medium security protection function is designed and realized according to the requirements of published data medium protection in 4.1.3.

6.1.2 Operation Security

6.1.2.1 Risk analysis

The risk analysis is carried out according to the requirements of 4.2.1 for the determination of overall security requirements of information system; security technology and security management measures shall be taken for the confidentiality, integrity and availability determined to be required for the realization of the user's discretionary protection level based on the requirements of the user's discretionary protection level on physical security, operation security and data security.

6.1.2.2 Test and analysis of information system security

The security of the selected or developed operating system and database system are tested with relevant tools according to the requirements for the test and analysis of security of operating system and database management system in 4.2.2, and the existing problems are improved through the analysis of the test result according to the security requirements of the user's discretionary protection level.

6.1.2.3 Security protection of information system boundary

The security protection function of the external boundary of information system and the boundary of each security domain in it is designed and realized according to basic security protection requirements in 4.2.5.

6.1.2.4 Backup and fault recovery

The backup and recovery function is designed and realized according to the requirements of user information and incremental information backup and recovery in 4.2.6.

6.1.2.5 Malicious code protection

The malicious code protection function is designed and realized according to the requirements of strict management in 4.2.7.

6.1.2.6 Emergency handling of information system

The emergency plans and measures are designed and developed in combination with specific requirements of the user's discretionary protection level on information system according to the requirements of taking various security measures in 4.2.8 to define measures which shall be taken where various conditions occur to the information system.

6.1.3 Data Security

6.1.3.1 Identity authentication

6.1.3.1.1 User identification

The user identification function is designed and realized according to the requirements of basic identification and identification information management in 4.3.1.1.1, and the user-subject binding is realized according to the requirements of 4.3.1.2. Generally, user name and user identifier (UID) are used to identify a user.

6.1.3.1.2 User authentication

The user authentication function is designed and realized according to the requirements of 4.3.1.1. It is required by this security protection level to:

a) Carry out authentication each time when the user logs in the system according to the requirements of basic authentication and authentication information management in 4.3.1.1.2, the authentication information shall be invisible and provided with security protection during storage;

b) Security protection shall be provided for cross-network remote user during on-line transport;

c) Design and realize authentication failure handling function according to the requirements of 4.3.1.1.3.

6.1.3.2 Discretionary access control

The discretionary access control function is designed and realized according to the requirements of 4.3.3. It is required by this security protection level to:

a) Determine the discretionary access control policy according to the requirements of 4.3.3.1;

b) Design and realize discretionary access control function according to the requirements of 4.3.3.2;

c) Determine the discretionary access control scope according to the requirements of subset access control in 4.3.3.3;

d) Determine the granularity of discretionary access control according to the requirements of coarse granularity in 4.3.3.4;

e) Be capable of allowing the named user to specify and control the access to the object as user or user group identity and prevent the access of unauthorized user to the object whatever the discretionary access control

function realized by the access control policy is adopted.

6.1.3.3 User data integrity

The user data integrity protection function is designed and realized according to the requirements of 4.3.6. The corresponding SSOIS security function module is designed and realized by this security protection level according to the requirements of integrity test in 4.3.6.2 to carry out integrity protection for the user data transported between two SSOISs through the network. SSOIS is required by this security protection level to provide the user data integrity monitoring function, namely being capable of testing the occurrence of such conditions as tampering, deletion and insertion of the transported user data.

6.1.3.4 Password support

According to the need, the data requiring transport encryption protection may be encrypted during the transport according to the configured password support in 4.3.10.

6.1.4 SSOIS Self-security Protection

6.1.4.1 SSF physical security protection

The physical security protection of SSF is realized according to the requirements of 5.1.1. Passive test of physical attack is realized by this security protection level according to the requirements of 5.1.1.1.

6.1.4.2 SSF operation security protection

The operation security protection of SSF is realized according to the requirements of 5.1.2. It is required by this security protection level to:

a) Realize the test for SSF security operation according to the requirements of 5.1.2.1;

b) Realize the SSF failure protection according to the requirements of 5.1.2.2;

c) Provide reliable time stamp support for SSOIS operation according to the requirements of 5.1.2.7;

d) Realize SSF self-test while starting according to the requirements of 5.1.2.9.

6.1.4.3 SSF data security protection

The security protection of SSF data is realized according to the requirements of 5.1.3. The protection of SSF data transport in SSOIS is realized by this security protection level according to the requirements of basic transport protection in 5.1.3.4.

6.1.4.4 SSOIS resource utilization

SSOIS resource utilization is realized according to the requirements of 5.1.4. It is required by this security protection level to:

a) Realize SSOIS tolerance handling according to the requirements of degraded tolerance in 5.1.4.1;

b) Realize SSOIS priority of service handling according to the requirements of priority of limited service in 5.1.4.2;

c) Realize SSOIS resource allocation according to the requirements of at maximum quota in 5.1.4.3.

6.1.4.5 SSOIS access control

SSOIS access control is realized according to the requirements of 5.1.5. It is required by this security protection level to:

a) Realize the management of session establishment according to the requirements of SSOIS session establishment in 5.1.5;

b) Realize the restriction of security attribute scope of session according to the requirements of scope restriction of optional attribute in 5.1.5;

c) Realize concurrent session restriction according to the requirements of restriction of multiple concurrent sessions in 5.1.5.

6.1.5 SSOIS Design and Realization

6.1.5.1 Configuration management

SSOIS configuration management is realized according to the requirements of 5.2.1. The version No. management is realized by this security protection level according to the requirements of version No. in 5.2.1.1.

6.1.5.2 Distribution and operation

SSOIS distribution and operation is realized according to the requirements of 5.2.2. It is required by this security protection level to:

a) Compile distribution and operation instructions according to the requirements of distribution process in 5.2.2.1;

b) Compile installation, generation and start description according to the requirements of installation, generation and start process in 5.2.2.2.

6.1.5.3 Development

SSOIS development is carried out according to the requirements of 5.2.3. It is required by this security protection level to:

a) Realize SSOIS function design according to the requirements of non-formalized function design in 5.2.3.1;

b) Realize SSOIS high-level design according to the requirements of descriptive high-level design in 5.2.3.3;

c) Realize SSOIS low-level design according to the requirements of descriptive low-level design in 5.2.3.4;

d) Realize SSOIS internal structure design according to the modularization requirements in 5.2.3.5;

e) Complete SSOIS realization expression design according to the requirements of subset realization of SSF in 5.2.3.6;

f) Realize SSOIS correspondence design according to the requirements of non-formalized correspondence in 5.2.3.7.

6.1.5.4 Document requirements

The security administrator and user guidance is compiled according to the requirements of security administrator and user guidance in 5.2.4 based on the requirements of the user's discretionary protection level on configuration management, distribution and operation, development, life cycle support and test.

6.1.5.5 Life cycle support

SSOIS life cycle support is realized according to the requirements of 5.2.5. The design of SSOIS life cycle model is realized by this security protection level according to the requirements of life cycle model defined by the developer in 5.2.5.3.

6.1.5.6 Test

Test for SSOIS is carried out according to the requirements of 5.2.6. It is required by this security protection level to:

a) Realize function test according to the requirements of general function test in 5.2.6.3;

b) Realize independence test according to the requirements of corresponding independence test in 5.2.6.4.

6.1.6 SSOIS Security Management

SSOIS security management is designed based on relevant contents like technical requirements of physical security, operation security and data security in relation to the technical requirements for security function as well as SSOIS self-security and SSOIS design and realization in relation to the technical requirements for security assurance in this security protection level according to the requirements described in 5.3. Corresponding operation, operating rules and behavior rules and regulations are developed by this security protection level according to SSF function management requirements realized according to 5.3.1

6.2 Level-2: System Audit Protection Level

6.2.1 Physical Security

6.2.1.1 Environmental security

6.2.1.1.1 Central machine room security

The central machine room security function is designed and realized according to the requirements of 4.1.1.1. It is required by this security protection level to:

a) Select the machine room site according to the description of basic requirements in 4.1.1.1.1;

b) Design and realize internal security protection of machine room according to the requirements of access and article management of machine room in 4.1.1.1.2;

c) Design and realize the machine room fire protection according to the requirements of fire prevention for building material ①, alarm and fire extinguishing system ① and **area separation and fire protection** in 4.1.1.1.3;

d) Design and realize power supply and distribution of machine room according to the requirements of separate power supply, emergency power supply ①, **stable voltage power supply and power protection** in 4.1.1.1.4;

e) Design and realize waterproofing and moisture proofing for machine room according to basic temperature requirements in 4.1.1.1.5;

f) Design and realize the waterproofing and moisture proofing of machine room according to the requirements of water pipe installation and water hazards prevention in 4.1.1.1.6;

g) Design and realize static protection according to the requirements of earthing and shielding, garment static protection as well as temperature and humidity in 4.1.1.1.7;

h) Design and realize earthing and lightning protection of machine room according to the requirements of earthing, decoupling and filtering as well as lightning protection in 4.1.1.1.8;

i) Design and realize electromagnetic protection according to the requirements of earthing, shielding and distance anti-interference in 4.1.1.1.9.

6.2.1.1.2 Communication line security

The communication line security protection is designed and realized according to the requirements of ensuring line smoothness in 4.1.1.2.

6.2.1.2 Equipment security

The equipment security function is designed and realized according to the requirements of 4.1.2. The security protection level requires to:

a) Design and realize equipment security protection function according to the requirements of equipment labeling requirements and burglary prevention for computing center ① in 4.1.2.1;

b) Design and realize equipment security function according to the requirements of basic operation support in 4.1.2.2.

6.2.1.3 Record medium security

Record medium security protection function is designed and realized according to the requirements of **internal data medium protection** in 4.1.3.

6.2.2 Operation Security

6.2.2.1 Risk analysis

The risk analysis is carried out according to the requirements of 4.2.1 for the determination of overall security requirements of information system; security technology and security management measures shall be taken for the confidentiality, integrity and availability determined to be required for the realization of **system audit protection level** based on the requirements of **system audit protection level** on physical security, operation security and data security.

6.2.2.2 Test and analysis of information system security

The security of the selected or developed operating system, database management system, **network system, application system and hardware system** is tested with relevant tools according to the requirements for the test and **analysis of security of** operating system, database management system, **network system, application system and hardware system** in 4.2.2, and the existing problems are improved

through the analysis of the test result according to the requirements of system audit protection level.

6.2.2.3 Security audit

The security audit function is designed and realized according to the requirements of security audit in 4.2.4. The security audit function of system audit protection level shall be checkable and its design shall be tightly combined with that of all security functions of information system like user identification and authentication, discretionary access control, data integrity, etc., the security audit function is designed and realized according to general requirements for security audit function design and specific security audit requirements in technical requirements of each security function. It is required by this security protection level to:

a) Design and realize audit response function according to the requirements of keeping audit log in 4.2.4.1;

b) Design and realize audit data generating function according to the requirements of 4.2.4.2;

c) Design and realize audit analyzing function according to the requirements of potential harm analysis in 4.2.4.3;

d) Design and realize audit review function according to the requirements of basic and limited audit review in 4.2.4.4;

e) Design and realize audit event selection function according to the requirements of 4.2.4.5;

f) Design and realize audit event preservation function according to the requirements of the protected audit trail storage in 4.2.4.6.

6.2.2.4 Security protection of information system boundary

The security protection function of the external boundary of information system and the boundary of each security domain in it is designed and realized according to stricter security protection requirements in 4.2.5.

6.2.2.5 Backup and fault recovery

The backup and recovery function is designed and realized according to the requirements of backup and recovery of user information, incremental information and local system as well as **backup and tolerance of equipment** in 4.2.6.

6.2.2.6 Malicious code protection

The malicious code protection function is designed and realized according to the

requirements of strict management and **gateway protection** in 4.2.7.

6.2.2.7 Emergency handling of information system

The emergency plans and measures are designed and developed in combination with specific requirements of the system audit protection level on information system according to the requirements of taking various security measures and **setting normal backup mechanism** in 4.2.8 to define measures which shall be taken where various conditions occur to the information system.

6.2.3 Data Security

6.2.3.1 Identity authentication

6.2.3.1.1 User identification

The user identification function is designed and realized according to the requirements of basic identification, unique identification and identification information management in 4.3.1.1.1, and the user-subject binding is realized according to the requirements of 4.3.1.2. Generally, user name and user identifier (UID) are used to identify a user so as to ensure the uniqueness of user name and user identifier in an information system. **Such uniqueness shall be effective in the whole life cycle of information system, namely, where a user's account number is deleted, his user identification cannot be used again**, ensuring the user's uniqueness and distinguishability. The user identification shall be associated with audit to provide check-ability.

6.2.3.1.2 User authentication

The user authentication function is designed and realized according to the requirements of 4.1.1.1. It is required by this security protection level to:

a) Carry out authentication each time when the user logs in the system according to the requirements of basic authentication, **unforgeable authentication** and authentication information management in 4.3.1.1.2; the authentication information shall be invisible and provided with security protection during storage;

b) Security protection shall be provided for cross-network remote user during on-line transport;

c) Design and realize authentication failure handling function according to the requirements of 4.3.1.1.3.

6.2.3.2 Discretionary access control

The discretionary access control function is designed and realized according to the requirements of 4.3.3. It is required by this security protection level to:

a) Determine the discretionary access control policy according to the requirements of 4.3.3.1;

b) Design and realize discretionary access control function according to the requirements of 4.3.3.2;

c) Determine the discretionary access control scope according to the requirements of subset access control in 4.3.3.3;

d) Determine the granularity of discretionary access control according to the requirements of **medium granularity access control** in 4.3.3.3;

e) Be capable of allowing the named user to specify and control the access to the object as user identity and prevent the access of unauthorized user to the object whatever the discretionary access control function realized by the access control policy is adopted.

6.2.3.3 User data integrity

The user data integrity protection function is designed and realized according to the requirements of 4.3.6. It is required by this security protection level to:

a) **Carry out integrity protection for the user data stored within the SSOIS security control scope by adopting discretionary integrity policy, and designing and realizing corresponding SSOIS security function module according to the requirements of integrity test. It is required by this security protection level to test whether integrity error occurs to the user data stored within the SSOIS control scope while reading.**

b) Design and realize corresponding SSOIS security function module according to the requirements of integrity test in 4.3.6.2 to carry out integrity protection for integrity protection for the user data transported between two SSOISs through the network. SSOIS is required by this security protection level to be capable of testing the occurrence of such conditions as tampering, deletion and insertion of the transported user data.

c) **Design and realize corresponding SSOIS security function module according to the rollback requirements in 4.3.6.3 to ensure the integrity of processed data through the rollback of operation sequence under various abnormal conditions.**

6.2.3.4 User data confidentiality

The user data confidentiality protection function is designed and realized according to the requirements of 4.3.7. It is required by this security protection level to:

4.2.4.3;

d) Design and realize audit review function according to the requirements of basic, limited and **optional audit review** in 4.2.4.4;

e) Design and realize audit event selection function according to the requirements of 4.2.4.5;

f) Design and realize audit event preservation function according to the requirements of the protected audit trail storage and **audit data availability assurance** in 4.2.4.6.

g) Design and realize network environmental security audit and assessment function according to the requirements of 4.2.4.7.

6.3.2.5 Security protection of information system boundary

The security protection function of the external boundary of information system and the boundary of each security domain in it shall be designed and realized according to **strict security protection** requirements in 4.2.5.

6.3.2.6 Backup and fault recovery

The backup and recovery function shall be designed and realized according to the requirements of user information, incremental information and local system backup and recovery, equipment and **network backup and tolerance as well as backup and recovery of the whole system** in 4.2.6.

6.3.2.7 Malicious code protection

The malicious code protection function shall be designed and realized according to the requirements of strict management, gateway protection and **integral protection** in 4.2.7.

6.3.2.8 Emergency handling of information system

The emergency plans and measures shall be designed and developed in combination with specific requirements of security label protection level on information system according to the requirements of taking various security measures, setting normal backup mechanism and **improving security management organization** in 4.2.8 to define measures which shall be taken where various conditions occur to the information system.

6.3.3 Data Security

6.3.3.1 Identity authentication

6.3.3.1.1 User identification

The user identification function shall be designed and realized according to the requirements of basic identification, unique identification and identification information management in 4.3.1.1.1, and the user-subject binding is realized according to the requirements of 4.3.1.2. Generally, user name and user identifier (UID) are used to identify a user so as to ensure the uniqueness of user name and user identifier in an information system. Such uniqueness shall be effective in the whole life cycle of information system, namely where a user's account number is deleted, his user identification cannot be used again, ensuring the user's uniqueness and distinguishability. The user identification shall be associated with audit to provide check-ability.

6.3.3.1.2 User authentication

The user authentication function shall be designed and realized according to the requirements of 4.1.1.1. It is required by this security protection level to:

a) Carry out authentication each time when the user logs in the system according to the requirements of basic authentication, unforgeable authentication, **disposable authentication** and authentication information management in 4.3.1.1.2; the authentication information shall be invisible and **protected according to the password support requirement in 4.3.10** during storage and transport;

b) For cross-network remote user, it shall be protected according to **the password support requirement in 4.3.10** during on-line transport of identity authentication information;

c) Design and realize authentication failure handling function according to the requirements of 4.3.1.1.3.

6.3.3.2 Non-repudiation

Non-repudiation function shall be designed and realized according to the requirements of 4.3.2. It is required by this security protection level to:

a) Design and realize non-repudiation of origin function according to the requirements of selective origin certification for data receiving party;

b) Design and realize non-repudiation of receipt function according to the requirements of selective receiving certification for data receiving party.

6.3.3.3 Discretionary access control

The discretionary access control function shall be designed and realized according to

the requirements of 4.3.3. It is required by this security protection level to:

a) Determine the discretionary access control policy according to the requirements of 4.3.3.1;

b) Design and realize discretionary access control function according to the requirements of 4.3.3.2;

c) Determine the discretionary access control scope according to the requirements of subset access control in 4.3.3.3;

d) Determine the granularity of discretionary access control according to the requirements of medium granularity access control in 4.3.3.3.

e) Be capable of allowing the named user to specify and control the access to the object as user identity and prevent the access of unauthorized user to the object whatever the discretionary access control function realized by the access control policy is adopted.

6.3.3.4 Label

Label function shall be designed and realized according to the requirements of 4.3.4. It is required by this security protection level to:

a) Design and realize subject label function according to the requirements of 4.3.4.1;

b) Design and realize object label function according to the requirements of 4.3.4.2;

c) Design and realize label output function according to the requirements of output of user data without label in 4.3.4.3;

d) Design and realize label input function according to the requirements of unlabeled user data input in 4.3.4.4.

6.3.3.5 Mandatory access control

Mandatory access control function shall be designed and realized according to the requirements of 4.3.5. It is required by this security protection level to:

a) Determine security policy model for mandatory access control according to the requirements of 4.3.5.1;

b) Design and realize mandatory access control function according to the requirements of 4.3.5.2;

c) Determine the scope of mandatory access control according to the requirements of subset access control in 4.3.5.3;

d) Determine the granularity of mandatory access control according to medium granularity requirement in 4.3.5.4;

e) Design and realize mandatory access control suitable to corresponding environment according to the requirements of 4.3.5.5.

6.3.3.6 Data flow control

Data flow control function shall be designed and realized for information system exchanging data through data flow mode according to the requirements of 4.3.8.

6.3.3.7 User data integrity

The data integrity protection function is designed and realized according to the requirements of 4.3.6. It is required by this security protection level to:

a) Carry out integrity protection for the user data stored within the SSOIS security control scope by adopting discretionary integrity policy, and designing and realizing corresponding SSOIS security function module according to the requirements of **integrity test and recovery** in 4.3.6.1. It is required by this security protection level to test whether integrity error occurs to the user data stored within the SSOIS control scope while reading, **take necessary recovery measures where integrity error is tested and carry out the integrity test for data stored in encryption through password support provided in 4.3.10**.

b) Design and realize corresponding SSOIS security function module according to the requirements of integrity test and **data exchange recovery** in 4.3.6.2 to carry out integrity protection for integrity protection for the user data transported between two SSOISs through the network. SSOIS is required by this security protection level to be capable of testing the occurrence of such conditions as tampering, deletion and insertion of the transported user data, **taking necessary measures where integrity error is tested and carrying out the integrity test for data for transported in encryption through password support provided in 4.3.10**.

c) Design and realize corresponding SSOIS security function module according to the rollback requirements in 4.3.6.3 to ensure the integrity of processed data through the rollback of operation sequence under various abnormal conditions.

6.3.3.8 User data confidentiality

Data confidentiality protection function shall be designed and realized according to the requirements of 4.3.7. It is required by this security protection level to:

a) Adopt storage encryption or other effective measures for user data requiring storage confidentiality protection based on the password support or other corresponding security mechanism configured in 4.3.10 according to the requirements of 4.3.7.1 to design and realize user data storage confidentiality protection function;

b) Adopt transport encryption or other effective measures for user data requiring transport confidentiality protection based on the password support or other corresponding security mechanism configured in 4.3.10 according to the requirements of 4.3.7.2 to design and realize user data transport confidentiality protection function;

c) Design and realize object security reusing function according to the requirements of subset information in 4.3.7.3.

6.3.3.9 Password support

The security function provided by password mechanism shall be designed and realized according to the password support arranged in 4.3.10.

6.3.4 SSOIS Self-security Protection

6.3.4.1 SSF physical security protection

SSF physical security protection shall be realized according to the requirements of 5.1.1. It is required by this security protection level to:

a) Realize passive test of physical attack according to the requirements of 5.1.1.1;

b) Realize automatic report of physical attack according to the requirements of 5.1.1.2.

6.3.4.2 SSF operation security protection

The operation security protection of SSF shall be realized according to the requirements of 5.1.2. It is required by this security protection level to:

a) Realize the test for SSF security operation according to the requirements of 5.1.2.1;

b) Realize the design of SSF failure protection according to the requirements of 5.1.2.2;

c) Realize the design of SSF replay test according to the requirements of 5.1.2.3;

d) Realize the design of SSF reference arbitration according to the requirements of 5.1.2.4;

e) Realize SSF domain separation design according to the requirements of SSF domain separation in 5.1.2.5;

f) Realize the design of SSF state synchronization agreement according to the requirements of simple trusted receipt in 5.1.2.6;

g) Provide reliable time stamp support for SSOIS operation according to the requirements of 5.1.2.7;

h) Realize SSF self-test while starting according to the requirements of 5.1.2.9.

6.3.4.3 SSF data security protection

The security protection of SSF data shall be realized according to the requirements of 5.1.3. It is required by this security protection level to:

a) Realize the availability design of the output SSF data according to the requirements of 5.1.3.1;

b) Realize the confidentiality design of the output SSF data according to the requirements of 5.1.3.2;

c) Realize the integrity design of the output SSF data according to the requirements of inter-SSF modification test;

d) Realize the protection of SSF data transport within SSOIS according to the requirements of basic transport protection, **data separated transport and data integrity protection** in 5.1.3.4;

e) Realize the consistency protection of SSF data between SSF according to the requirements of 5.1.3.5;

f) Realize the consistency protection of SSF data replication within SSOIS according to the requirements of 5.1.3.6.

6.3.4.4 SSOIS resource utilization

SSOIS resource utilization shall be realized according to the requirements of 5.1.4. It is required by this security protection level to:

a) Realize SSOIS tolerance handling according to the requirements of degraded

tolerance and **limited tolerance** in 5.1.4.1;

b) Realize SSOIS priority of service handling according to the requirements of **the priority of entire service** in 5.1.4.2;

c) Realize SSOIS resource allocation according to the requirements of **minimum and maximum quota** in 5.1.4.3.

6.3.4.5 SSOIS access control

SSOIS access control shall be realized according to the requirements of 5.1.5. It is required by this security protection level to:

a) Realize the management of session establishment according to the requirements of SSOIS session establishment in 5.1.5;

b) Realize the restriction of security attribute scope of session according to the requirements of scope restriction of optional attribute in 5.1.5;

c) Realize concurrent session restriction according to the requirements of restriction of multiple concurrent sessions in 5.1.5;

d) Realize session history management according to the requirements of SSOIS access history in 5.1.5;

e) Realize session lock-in handling according to the requirements of session lock-in in 5.1.5.

6.3.5 SSOIS Design and Realization

6.3.5.1 Configuration management

SSOIS configuration management is realized according to the requirements of 5.2.1. It is required by this security protection level to:

a) Realize configuration management capability design according to the requirements of version No., **configuration item and authorized control** in 5.2.1.1;

b) Realize configuration management automation design according to the requirements of partial automation of CM in 5.2.1.2;

c) Realize configuration management scope design according to the requirements of **problem-tracking configuration management scope** in 5.2.1.3;

d) Place the realization expression, design document, test document, user

document, security administrator document, configuration management document, etc. of SSOIS under configuration management.

6.3.5.2 Distribution and operation

SSOIS distribution and operation shall be realized according to the requirements of 5.2.2. It is required by this security protection level to:

a) Prepare SSOIS distribution and operation instructions according to the requirements of **modification test** in 5.2.2.1;

b) Prepare SSOIS installation, generation and start process description according to the requirements of installation, generation, start process and log generation in 5.2.2.2.

6.3.5.3 Development

SSOIS development shall be carried out according to the requirements of 5.2.3. It is required by this security protection level to:

a) Realize SSOIS function design according to the requirements of fully defined external interface in 5.2.3.1;

b) Realize SSOIS security policy model design according to the requirements of non-formalized SSOIS security policy model in 5.2.3.2;

c) Realize SSOIS high-level design according to the requirements of **high-level design for security reinforcement** in 5.2.3.3;

d) Realize SSOIS low-level design according to the requirements of descriptive low-level design in 5.2.3.4;

e) Realize SSOIS internal structure design according to the layering requirement in 5.2.3.5;

f) Complete SSOIS realization expression design according to the requirements of **SSF realization** in 5.2.3.6;

g) Realize correspondence design of SSOIS expression according to the requirements of non-formalized correspondence.

6.3.5.4 Document requirements

The security administrator and user guidance is compiled according to the requirements of security administrator and user guidance in 5.2.4 based on the requirements of the **security label protection level** on configuration management, distribution and operation, development, life cycle support, vulnerability assessment

and test.

6.3.5.5 Life cycle support

SSOIS life cycle support shall be realized according to the requirements of 5.2.5. It is required by this security protection level to:

a) Realize development security according to the requirements of security measures in 5.2.5.1;

b) Realize defect correction according to the requirements of basic defect correction in 5.2.5.2;

c) Realize the design of life cycle model according to the requirements of standard life cycle model in 5.2.5.3;

d) Determine the adopted tool and technology according to the requirements of well-defined development tools in 5.2.5.4.

6.3.5.6 Test

Test for SSOIS shall be carried out according to the requirements of 5.2.6. It is required by this security protection level to:

a) Determine the test scope according to the requirements of scope evidence and analysis in 5.2.6.1;

b) Realize design test according to the requirements of high-level and **low-level design tests** in 5.2.6.2;

c) Realize function test according to the requirements of **sequential function test** in 5.2.6.3;

d) Realize independence test according to the requirements of corresponding independence test and **sampling independence test** in 5.2.6.4.

6.3.5.7 Vulnerability assessment

SSOIS vulnerability assessment shall be realized according to the requirements of 5.2.7. It is required by this security protection level to:

a) Realize the misuse prevention design according to the document inspection and **analysis confirmation requirements** in 5.2.7.2;

b) Realize SSOIS security function strength assessment design according to the requirements of 5.2.7.3;

c) Realize vulnerability analysis design according to the **requirements of**

independent vulnerability analysis in 5.2.7.4.

6.3.6 SSOIS Security Management

SSOIS security management shall be designed based on relevant contents like technical requirements of physical security, operation security and data security in relation to the technical requirements for security function as well as SSOIS self-security and SSOIS design and realization in relation to the technical requirements for security assurance in this security protection level according to the requirements described in 5.3. **It is required by this security protection level to respectively arrange specific personnel to assume importance security roles like system administrator, security officer and auditor, and respectively grant them with the minimum privilege required to complete their own tasks according to the "least authorization principle". At the same time, mutual restriction relationship shall be formed between them.** Corresponding operation, operating rules as well as behavior rules and regulations shall be developed by this security protection level according to the following requirements:

a) Realize SSF function management according to the requirements of 5.3.1;

b) Realize security attribute management according to the requirements of 5.3.2;

c) Realize management of SSF data according to the requirements of SSF data management, SSF data bound and **secure SSF data** in 5.3.3;

d) Realize the definition and management of security role according to the requirements of 5.3.4;

e) Realize centralized management of SSOIS security mechanism according to the requirements of 5.3.5.

6.4 Level 4: Structured Protection Level

6.4.1 Physical Security

6.4.1.1 Environmental security

6.4.1.1.1 Central machine room security

The central machine room security function shall be designed and realized according to the requirements of 4.1.1.1. It is required by this security protection level to:

a) Select machine room site according to the fire protection, anti-pollution, moisture-proof, lightning protection, shock-proof and noise-proof requirements, strong electrical field and magnetic field protection requirements, earthquake and flood protection requirements, position requirements and **public interference protection requirements** in 4.1.1.1.1;

b) Design and realize internal security protection of machine room according to the requirements of access, articles, personnel, subarea and access control of machine room in 4.1.1.1.2;

c) Design and realize the machine room fire protection according to the requirements of **fire prevention for building material ③, alarm and fire extinguishing system ③** and area separation and fire protection in 4.1.1.1.3;

d) Design and realize power supply and distribution of machine room according to the requirements of separate power supply, **emergency power supply ③,** standby power supply, stable voltage power supply, power protection, uninterrupted power supply, **electric apparatus noise protection and emergency protection** in 4.1.1.1.4;

e) Design and realize waterproofing and moisture proofing for machine room according to the requirements of **complete air conditioning system** in 4.1.1.1.5;

f) Design and realize the water and moisture-proof of machine room according to the requirements of water pipe installation, water hazards prevention, waterproofing test and **drainage** in 4.1.1.1.6;

g) Design and realize static protection according to the requirements of earthing and shielding, garment static protection, temperature and humidity, floor and material, **maintenance MOS circuit protection and static elimination** in 4.1.1.1.7;

h) Design and realize earthing and lightning protection of machine room according to the requirements of earthing, decoupling and filtering, lightning protection, shelter ground and shield ground as well as **earth wire for AC power supply** in 4.1.1.1.8;

i) Design and realize electromagnetic protection according to the requirements of earthing, shielding and distance anti-interference, electromagnetic compromising emanation protection as well as **machine room shield** in 4.1.1.1.9.

6.4.1.1.2 Communication line security

The communication line security protection is designed and realized according to the requirements of ensuring line smoothness, **timely finding line intercept and avoiding line intercept** in 4.1.1.2.

6.4.1.2 Equipment security

The equipment security function shall be designed and realized according to the

requirements of 4.1.2. It is required by this security protection level to:

a) Design and realize equipment security protection function according to the requirements of equipment labeling, **burglary prevention for computing center** ③ and burglary prevention of external equipment in machine room in 4.1.2.1;

b) Design and realize equipment security function according to the requirements of basic operation support, availability of equipment and **uninterrupted equipment operation** in 4.1.2.2.

6.4.1.3 Record medium security

Record medium security protection function shall be designed and realized according to the requirements of **key data medium protection** in 4.1.3.

6.4.2 Operation Security

6.4.2.1 Risk analysis

The risk analysis shall be carried out according to the requirements of 4.2.1 for the determination of overall security requirements of information system; security technology and security management measures shall be taken for the confidentiality, integrity and availability determined to be required for the realization of the **structured protection level** based on the requirements of **structured protection level** on physical security, operation security and data security.

6.4.2.2 Test and analysis of information system security

The security of the selected or developed operating system, database management system, network system, application system and hardware system is tested with relevant tools according to the requirements for the test and analysis of security of operating system, database management system, network system, application system, hardware system and **attack** in 4.2.2, and the existing problems are improved through the analysis of the test result according to the security requirements of the **structured protection level**.

6.4.2.3 Information system security monitoring

The security monitoring function of information system shall be designed and realized according to the requirements of security detecting mechanism and security monitoring center in 4.2.3.

6.4.2.4 Security audit

The security audit function shall be designed and realized according to the requirements of security audit in 4.2.4. Security audit shall be checkable and its design

the requirements of 5.1.3.7.

6.4.4.4 SSOIS resource utilization

SSOIS resource utilization shall be realized according to the requirements of 5.1.4. It is required by this security protection level to:

a) Realize SSOIS tolerance handling according to the requirements of degraded tolerance and limited tolerance in 5.1.4.1;

b) Realize SSOIS priority of service handling according to the requirements of the entire priority of service in 5.1.4.2;

c) Realize SSOIS resource allocation according to the requirements of minimum and maximum quota in 5.1.4.3.

6.4.4.5 SSOIS access control

SSOIS access control shall be realized according to the requirements of 5.1.5. It is required by this security protection level to:

a) Realize the management of session establishment according to the requirements of SSOIS session establishment in 5.1.5;

b) Realize the restriction of security attribute scope of session according to the requirements of scope restriction of optional attribute in 5.1.5;

c) Realize concurrent session restriction according to the requirements of restriction of multiple concurrent sessions in 5.1.5;

d) Realize session history management according to the requirements of SSOIS access history in 5.1.5;

e) Realize session lock-in handling according to the requirements of session lock-in in 5.1.5.

6.4.5 SSOIS Design and Realization

6.4.5.1 Configuration management

SSOIS configuration management shall be realized according to the requirements of 5.2.1. It is required by this security protection level to:

a) Realize configuration management capability design according to the requirements of **generation support and acceptance process** in 5.2.1.1;

b) Realize configuration management automation design according to the requirements of partial automation of CM in 5.2.1.2

c) Realize configuration management scope design according to the requirements of **configuration management scope of development tool** in 5.2.1.3;

d) Place the realization expression, design document, test document, user document, security administrator document, configuration management document, etc. of SSOIS under configuration management.

6.4.5.2 Distribution and operation

SSOIS distribution and operation shall be realized according to the requirements of 5.2.2. It is required by this security protection level to:

a) Prepare SSOIS distribution description according to the requirements of **modification prevention** in 5.2.2.1;

b) Prepare SSOIS installation, generation and start process description according to the requirements described in installation, generation, start process and log generation in 5.2.2.2.

6.4.5.3 Development

SSOIS development shall be carried out according to the requirements of 5.2.3. It is required by this security protection level to:

a) Realize SSOIS function design according to the requirements of **semi-formalized function design** in 5.2.3.1;

b) Realize SSOIS security policy model design according to the requirements of **semi-formalized SSOIS security policy model** in 5.2.3.7;

c) Realize SSOIS high-level design according to the requirements of **semi-formalized high-level design** in 5.2.3.2;

d) Realize SSOIS low-level design according to the requirements of **semi-formalized low-level design** in 5.2.3.5;

e) Realize SSOIS internal structure design according to the requirements of **minimized complexity** in 5.2.3.4;

f) Complete SSOIS realization expression design according to the requirements of **structured realization of SSF** in 5.2.3.3;

g) Realize correspondence design of SSOIS expression according to the requirements of **semi-formalized correspondence description** in 5.2.3.6.

6.4.5.4 Document requirements

The security administrator and user guidance is compiled according to the requirements of security administrator and user guidance in 5.2.4 based on the requirements of the **structured protection level** on configuration management, distribution and operation, development, life cycle support, vulnerability assessment and test.

6.4.5.5 Life cycle support

The design of life cycle support shall be realized according to the requirements of 5.2.5. It is required by this security protection level to:

a) Realize security development according to the requirements of **sufficiency of security measures** in 5.2.5.1;

b) Realize defect correction according to the requirements of basic defect correction in 5.2.5.2;

c) Realize the design of life cycle model according to the requirements of standard life cycle model in 5.2.5.3;

d) Determine the adopted tool and technology according to the requirements of **complying with the realization of standard - application part** in 5.2.5.4.

6.4.5.6 Test

Test for SSOIS shall be carried out according to the requirements of 5.2.6. It is required by this security protection level to:

a) Determine the test scope according to the requirements of scope evidence and **strict scope analysis** in 5.2.6.1;

b) Realize the design test the requirements of high-level design test, low-level design test and **realization expression test** in 5.2.6.2;

c) Realize the function test according to the requirements of **sequential function test** in 5.2.6.3;

d) Realize independence test according to the requirements of corresponding independence test and sampling independence test in 5.2.6.4.

6.4.5.7 Vulnerability assessment

SSOIS vulnerability assessment shall be realized according to the requirements of 5.2.7. It is required by this security protection level to:

a) Realize convert channel analysis design according to the requirements of general convert channel analysis in 5.2.7.1;

b) Realize misuse prevention design according to the requirements of 5.2.7.2;

c) Realize SSOIS security function strength assessment design according to the requirements of 5.2.7.3;

d) Realize developer vulnerability analysis design according to the requirements of **intermediate resistance** in 5.2.7.4.

6.4.6 SSOIS Security Management

SSOIS security management shall be designed based on relevant contents like technical requirements of physical security, operation security and data security in relation to the technical requirements for security function as well as SSOIS self-security and SSOIS design and realization in relation to the technical requirements for security assurance in this security protection level according to the requirements described in 5.3. It is required by this security protection level to respectively arrange specific personnel to assume importance security roles like system manager, security officer and auditor, and respectively grant them with the minimum privilege required to complete their own tasks according to the "least authorization principle". At the same time, mutual restriction relationship shall be formed between them. Corresponding operation, operating rules as well as behavior rules and regulations shall be developed by this security protection level according to the following requirements:

a) Realize SSF function management according to the requirements of 5.3.1;

b) Realize security attribute management according to the requirements of 5.3.2;

c) Realize management of SSF data according to the requirements of 5.3.3;

d) Realize the definition and management of security role according to the requirements of 5.3.4;

e) Realize centralized management of SSOIS security mechanism according to the requirements of 5.3.5.

6.5 Level-5: Access Verification Protection Level

6.5.1 Physical Security

6.5.1.1 Environmental security

6.5.1.1.1 Central machine room security

The central machine room security function shall be designed and realized according to the requirements of 4.1.1.1. It is required by this security protection level to:

a) Select machine room site according to the fire protection, anti-pollution,

moisture-proof, lightning protection, shock-proof and noise-proof requirements, strong electrical field and magnetic field protection requirements, earthquake and flood protection requirements, position requirements and public interference protection requirements in 4.1.1.1.1;

b) Design and realize internal security protection of machine room according to the requirements of access, articles, personnel, subarea and access control of machine room in 4.1.1.1.2;

c) Design and realize the machine room fire protection according to the requirements of fire prevention for building material ③, alarm and fire extinguishing system ③ and area separation and fire protection in 4.1.1.1.3;

d) Realize power supply and distribution of machine room according to the requirements of separate power supply, emergency power supply ③, standby power supply, stable voltage power supply, power protection, uninterrupted power supply, electric apparatus noise protection and emergency protection in 4.1.1.1.4;

e) Design and realize waterproofing and moisture proofing for machine room according to the requirements of complete air conditioning system in 4.1.1.1.5;

f) Realize the water and moisture-proof of machine room according to the requirements of water pipe installation, water hazards prevention, waterproofing test and drainage in 4.1.1.1.6;

g) Design and realize static protection according to the requirements of earthing and shielding, garment static protection, temperature and humidity, floor and material, maintenance MOS circuit protection and static elimination in 4.1.1.1.7;

h) Realize earthing and lightning protection of machine room according to the requirements of earthing, decoupling and filtering, lightning protection, shelter ground, shield ground as well as earth wire for AC power supply in 4.1.1.1.8;

i) Carry out electromagnetic protection according to the requirements of earthing, shielding and distance anti-interference, electromagnetic compromising emanation protection as well as machine room shield in 4.1.1.1.9.

6.5.1.1.2 Communication line security

Security protection shall be carried out for communication line according to the requirements of ensuring line smoothness, timely finding line intercept and avoiding line intercept in 4.1.1.2.

6.5.1.2 Equipment security

The equipment security function shall be designed and realized according to the requirements of 4.1.2. The security protection level requires to:

a) Design and realize equipment security protection according to the requirements of equipment labeling, burglary prevention for computing center ③ and burglary prevention of external equipment in machine room in 4.1.2.1;

b) Design and realize equipment security function according to the requirements of basic operation support, availability of equipment and uninterrupted equipment operation in 4.1.2.2.

6.5.1.3 Record medium security

Record medium security protection function shall be designed and realized according to the requirements of **nuclear data medium protection** in 4.1.3.

6.5.2 Operation Security

6.5.2.1 Risk analysis

The risk analysis shall be carried out according to the requirements of 4.2.1 for the determination of overall security requirements of information system; security technology and security management measures shall be taken for the confidentiality, integrity and availability determined to be required for the realization of **access verification protection level** based on the requirements of **access verification protection level** on physical security, operation security and data security.

6.5.2.2 Test and analysis of information system security

The security of the selected or developed operating system, database management system, network system, application system and hardware system is tested with relevant tools according to the requirements for the test and analysis of security of operating system, database management system, network system, application system, hardware system and attack in 4.2.2, and the existing problems are improved through the analysis of the test result according to the security requirements of **access verification protection level**.

6.5.2.3 Information system security monitoring

The security monitoring function of information system shall be designed and realized according to the requirements of security detecting mechanism and security monitoring center in 4.2.3.

6.5.2.4 Security audit

The security audit function shall be designed and realized according to the requirements of security audit in 4.2.4. Check-ability is provided by security audit

mainly, requiring that the design of security audit function shall be tightly combined with that of all security functions of information system like user identification and authentication, discretionary access control, label, mandatory access control, data flow control, data integrity, convert channel analysis, trusted path, **fault recovery**, etc., it is carried out according to general requirements for security audit function design and specific security audit requirements in technical requirements of each security function. It is required by this security protection level to:

a) Design and realize audit response function according to the requirements of keeping audit log, violation progress termination, **service cancellation and user account disconnection and failure** in 4.2.4.1;

b) Design and realize audit data generating function according to the requirements of 4.2.4.2;

c) Design and realize audit analyzing function according to the requirements of potential harm analysis, abnormal test, simple attack detection and **complex attack detection** in 4.2.4.3;

d) Design and realize audit review function according to the requirements of basic, limited and optional audit review in 4.2.4.4;

e) Design and realize audit event selection function according to the requirements of 4.2.4.5;

f) Design and realize audit event preservation function according to the requirements of the protected audit trail storage, audit data availability assurance, measures for potential audit data loss and **audit data loss prevention** in 4.2.4.6;

g) Design and realize network environmental security audit and assessment function according to the requirements of 4.2.4.7.

6.5.2.5 Security protection of information system boundary

The security protection function of the external boundary of information system and the boundary of each security domain in it shall be designed and realized according to the highest security protection requirements in 4.2.5.

6.5.2.6 Backup and fault recovery

The backup and recovery function shall be designed and realized according to the requirements of user information, incremental information and local system backup and recovery, equipment and network backup and tolerance, as well as whole system and disaster backup and recovery in 4.2.6.

6.5.2.7 Malicious code protection

The malicious code protection function shall be designed and realized according to the requirements of strict management, gateway protection, integral protection, combination of protection and management as well as multilayer defense in 4.2.7.

6.5.2.8 Emergency handling of information system

The emergency plans and measures shall be designed and developed in combination with specific requirements of access verification protection level on information system according to the requirements of taking various security measures, setting normal backup mechanism, improving security management organization and developing processing flow chart in 4.2.8 to define measures which shall be taken where various conditions occur to the information system.

6.5.2.9 Trusted computing and trusted connecting technology

a) Support of trusted computing technology: set trusted computing mechanism in computer system according to the requirements of 4.2.9 a) to provide support for the factuality verification of software and hardware of computer system in information system, the user's identity authentication and data confidentiality and integrity protection.

b) Support of trusted connecting technology: set trusted connecting mechanism in network system according to the requirements of 4.2.9 b) to provide support for trusted connection of network equipment in information system.

6.5.3 Data Security

6.5.3.1 Identity authentication

6.5.3.1.1 User identification

The user identification function shall be designed and realized according to the requirements of basic identification, unique identification and identification information management in 4.3.1.1.1, and the user-subject binding is realized according to the requirements of 4.3.1.2. Generally, user name and user identifier (UID) are used to identify a user so as to ensure the uniqueness of user name and user identifier in an information system. Such uniqueness shall be effective in the whole life cycle of information system, namely where a user's account number is deleted, his user identification cannot be used again, ensuring the user's uniqueness and distinguishability. The user identification shall be associated with audit to provide check-ability.

6.5.3.1.2 User authentication

The user authentication function shall be designed and realized according to the requirements of 4.1.1.1. It is required by this security protection level to:

a) Carry out authentication each time when the user logs in the system and during each reconnection according to the requirements of basic authentication, unforgeable authentication, disposable authentication, multi-mechanism authentication, **re-authentication** and authentication information management in 4.3.1.1.2; the authentication information shall be invisible and protected according to the password support requirement in 4.3.10 during storage and transport; smart IC card identity authentication shall be designed based on encryption technology;

b) For cross-network remote user, it shall be protected according to the password support requirement in 4.3.10 during on-line transport of identity authentication information;

c) Design and realize authentication failure handling function according to the requirements of 4.3.1.1.3.

6.5.3.1.3 Concealing

Concealing function shall be designed and realized according to the requirements of cryptonym, alias, unlink-ability and unobservability in 4.3.1.3.

6.5.3.1.4 Equipment identification

Equipment identification function shall be designed and realized according to the requirements of identification before connection and identification information management. Generally, an equipment is identified with equipment name and identify.

6.5.3.1.5 Equipment authentication

The equipment authentication function shall be designed and realized according to the requirements of 4.3.1.4. It is required by this security protection level to:

a) Design and realize the authentication function of identification equipment according to the requirements of authentication before connection, unforgeable authentication and authentication information management in 4.3.1.4.2;

b) Handle authentication failure according to the requirements of 4.3.1.4.3;

c) Adopt authentication information supported by password system to carry out the authentication of factuality of access equipment identity before equipment access;

d) Authentication information shall be invisible and be protected according to the

requirements of cryptographic support in 4.3.10 during storage and transport.

6.5.3.2 Non-repudiation

Non-repudiation function shall be designed and realized according to the requirements of 4.3.2. It is required by this security protection level to:

a) Design and realize non-repudiation of origin function according to the requirements of mandatory origin certification for data sending party;

b) Design and realize non-repudiation of receipt function according to the requirements of mandatory receiving certification for data receiving party.

6.5.3.3 Discretionary access control

The discretionary access control function shall be designed and realized according to the requirements of 4.3.3. It is required by this security protection level to:

a) Determine the discretionary access control policy according to the requirements of 4.3.3.1;

b) Design and realize discretionary access control function according to the requirements of 4.3.3.2;

c) Determine discretionary access control scope according to the requirements of full access control in 4.3.3.3;

d) Determine the granularity of discretionary access control according to the requirements of **fine granularity access control** in 4.3.3.3;

e) Be capable of allowing the named user to specify and control the access to the object as user identity and prevent the access of unauthorized user to the object whatever the discretionary access control function realized by the access control policy is adopted.

6.5.3.4 Label

Label function shall be designed and realized according to the requirements of 4.3.4. It is required by this security protection level to:

a) Design and realize subject label function according to the requirements of 4.3.4.1; b) Design and realize object label function according to the requirements of 4.3.4.2;

c) Design and realize label output function according to the requirements of output of user data without label in 4.3.4.3;

d) Design and realize label input function according to the requirements of input of user data with sensitivity label in 4.3.4.4.

6.5.3.5 Mandatory access control

Mandatory access control function shall be designed and realized according to the requirements of 4.3.5. It is required by this security protection level to:

a) Determine security policy model for mandatory access control according to the requirements of 4.3.5.1;

b) Design and realize mandatory access control function according to the requirements of 4.3.5.2;

c) Determine the scope of mandatory access control according to the full access control requirements;

d) Determine the granularity of mandatory access control according to the **fine granularity access control** requirements;

e) Design and realize mandatory access control suitable to corresponding environment according to the requirements of 4.3.5.5.

6.5.3.6 Data flow control

Data flow control function shall be designed and realized for information system exchanging data through data flow mode according to the requirements of 4.3.8.

6.5.3.7 User data integrity

The user data integrity protection function is designed and realized according to the requirements of 4.3.6. It is required by this security protection level to:

a) Carry out integrity protection for the user data stored within the SSOIS security control scope by adopting discretionary integrity policy, and designing and realizing corresponding SSOIS security function module according to the requirements of integrity test and recovery in 4.3.6.1. It is required by this security protection level to test whether integrity error occurs to the user data stored within the SSOIS control scope while reading, take necessary recovery measures where integrity error is tested and carry out the integrity test for data stored in encryption through password support provided in 4.3.10;

b) Design and realize corresponding SSOIS security function module according to the requirements of integrity test and data exchange recovery in 4.3.6.2 to carry out integrity protection for integrity protection for the user data transported between two SSOISs through the network. SSOIS is required by this security protection level to be capable of testing the occurrence of such

conditions as tampering, deletion and insertion of the transported user data, taking necessary measures where integrity error is tested and carrying out the integrity test for data transported in encryption through password support provided in 4.3.10;

c) Design and realize corresponding SSOIS security function module according to the rollback requirements in 4.3.6.3 to ensure the integrity of processed data through the rollback of operation sequence under various abnormal conditions.

6.5.3.8 User data confidentiality

The user data confidentiality protection function shall be designed and realized according to the requirements of 4.3.7. It is required by this security protection level to:

a) Adopt storage encryption or other effective measures for user data requiring storage confidentiality protection based on the password support or other corresponding security mechanism arranged in 4.3.10 according to the requirements of 4.3.7.1 to design and realize user data storage confidentiality protection function;

b) Adopt transport encryption or other effective measures for user data requiring transport confidentiality protection based on the password support or other corresponding security mechanism arranged in 4.3.10 according to the requirements of 4.3.7.2 to design and realize user data transport confidentiality protection function;

c) Design and realize object security reusing function according to **special information protection** requirements in 4.3.7.3.

6.5.3.9 Trusted path

Trusted path function shall be designed and realized according to the requirements of 4.3.9. A secure data transport path shall be developed by SSOIS between user and it where the initial login and/or authentication are carried out by the user.

6.5.3.10 Password support

The security function provided by password mechanism shall be designed and realized according to the password support arranged in 4.3.10.

6.5.4 SSOIS Self-security Protection

6.5.4.1 SSF physical security protection

SSF physical security protection shall be realized according to the requirements of 5.1.1. It is required by this security protection level to:

a) Realize passive test of physical attack according to the requirements of 5.1.1.1;

b) Realize automatic report of physical attack according to the requirements of 5.1.1.2;

c) Realize physical attack resistance according to the requirements of 5.1.1.3.

6.5.4.2 SSF operation security protection

The operation security protection of SSF shall be realized according to the requirements of 5.1.2. It is required by this security protection level to:

a) Realize the test for SSF security operation according to the requirements of 5.1.2.1;

b) Realize the design of SSF failure protection according to the requirements of 5.1.2.2;

c) Realize the design of SSF replay test according to the requirements of 5.1.2.3;

d) Realize the design of SSF reference arbitration according to the requirements of 5.1.2.4;

e) Realize SSF domain separation design according to the requirements of SSF and SFP domain separation in 5.1.2.5;

f) Realize the design of SSF state synchronization agreement according to the requirements of mutual trusted receipt in 5.1.2.6;

g) Provide reliable time stamp support for SSOIS operation according to the requirements of 5.1.2.7;

h) Realize trusted recovery design according to the requirements of 5.1.2.8;

i) Realize SSF self-test while starting according to the requirements of 5.1.2.9.

6.5.4.3 SSF data security protection

The security protection of SSF data shall be realized according to the requirements of 5.1.3. It is required by this security protection level to:

a) Realize the availability design of the output SSF data according to the requirements of 5.1.3.1;

b) Realize the confidentiality design of the output SSF data according to the requirements of 5.1.3.2;

c) Realize the integrity design of the output SSF data according to the requirements of inter-SSF modification test and the correction to the modification between SSF in 5.1.3.3;

d) Realize the protection of SSF data transport within SSOIS according to the requirements of basic transport protection, data separation transport and data integrity protection in 5.1.3.4;

e) Realize the consistency protection of SSF data between SSF according to the requirements of 5.1.3.5;

f) Realize the consistency protection of SSF data replication within SSOIS according to the requirements of 5.1.3.6;

g) Realize the design of trusted path between user and SSF according to the requirements of 5.1.3.7;

h) Realize the design of trusted channel between SSF according to the requirements of 5.1.3.8.

6.5.4.4 SSOIS resource utilization

SSOIS resource utilization shall be realized according to the requirements of 5.1.4. It is required by this security protection level to:

a) Realize SSOIS tolerance handling according to the requirements of degraded tolerance and limited tolerance in 5.1.4.1;

b) Realize SSOIS priority of service handling according to the requirements of the priority of entire service in 5.1.4.2;

c) Realize SSOIS resource allocation according to the requirements of minimum and maximum quota in 5.1.4.3.

6.5.4.5 SSOIS access control

SSOIS access control shall be realized according to the requirements of 5.1.5. It is required by this security protection level to:

a) Realize the management of session establishment according to the requirements of SSOIS session establishment in 5.1.5;

b) Realize the restriction of security attribute scope of session according to the requirements of scope restriction of optional attribute in 5.1.5;

c) Realize concurrent session restriction according to the requirements of restriction of multiple concurrent sessions in 5.1.5;

d) Realize session history management according to the requirements of SSOIS access history in 5.1.5;

e) Realize session lock-in handling according to the requirements of session lock-in in 5.1.5.

6.5.5 SSOIS Design and Realization

6.5.5.1 Configuration management

SSOIS configuration management shall be realized according to the requirements of 5.2.1. It is required by this security protection level to:

a) Realize configuration management capability design according to the requirements of further support in 5.2.1.1;

b) Realize configuration management automation design according to the requirements of full automation of CM in 5.2.1.2;

c) Realize configuration management scope design according to the requirements of configuration management scope of development tool in 5.2.1.3;

d) Place the realization expression, design document, test document, user document, security administrator document, configuration management document, etc. of SSOIS under configuration management.

6.5.5.2 Distribution and operation

SSOIS distribution and operation shall be realized according to the requirements of 5.2.2. It is required by this security protection level to:

a) Prepare SSOIS distribution and operation description according to the requirements of modification prevention in 5.2.2.1;

b) Prepare SSOIS installation, generation and start process description according to the requirements described in installation, generation, start process and log generation in 5.2.2.2.

6.5.5.3 Development

SSOIS development shall be carried out according to the requirements of 5.2.3. It is required by this security protection level to:

a) Realize SSOIS security function design according to the requirements of **formalized function design** 5.2.3.1;

b) Realize SSOIS security policy model design according to the requirements of **formalized SSOIS security policy model** in 5.2.3.2;

c) Realize SSOIS high-level design according to the requirements of **formalized high-level design** in 5.2.3.3;

d) Realize SSOIS low-level design according to the requirements of **formalized low-level design** in 5.2.3.4;

e) Realize SSOIS internal structure design according to the requirements of minimized complexity in 5.2.3.5;

f) Realize SSOIS realization expression design according to the requirements of structured realization of SSF in 5.2.3.6;

g) Realize correspondence design of SSOIS expression according to the requirements of **formalized correspondence description** in 5.2.3.7.

6.5.5.4 Document requirements

The security administrator and user guidance is compiled according to the requirements of security administrator and user guidance in 5.2.4 based on the requirements of **access verification protection level** on configuration management, distribution and operation, development, life cycle support, vulnerability assessment and test.

6.5.5.5 Life cycle support

SSOIS life cycle support shall be realized according to the requirements of 5.2.5. It is required by this security protection level to:

a) Realize security development according to the requirements of sufficiency of security measures in 5.2.5.1;

b) Realize defect correction according to the requirements of **system defect correction** in 5.2.5.2;

c) Realize life cycle model design according to the requirements of **measurable life cycle model** in 5.2.4.3;

d) Determine the adopted tool and technology according to the requirements of **complying with the realization of standard - all parts** in 5.2.5.4.

6.5.5.6 Test

Test for SSOIS shall be carried out according to the requirements of 5.2.6. It is required by this security protection level to:

a) Determine the test scope according to the requirements of scope evidence and strict scope analysis in 5.2.6.1;

b) Realize the design test the requirements of high-level design test, low-level design test and realization expression test in 5.2.6.2;

c) Realize the function test according to the requirements of sequential function test in 5.2.6.3;

d) Realize independence test according to the requirements of corresponding independence test and **complete independence tes**t in 5.2.6.4.

6.5.5.7 Vulnerability assessment

SSOIS vulnerability assessment shall be realized according to the requirements of 5.2.7. It is required by this security protection level to:

a) Realize convert channel analysis design according to the requirements of **strict convert channel analysis** in 5.2.7.1;

b) Realize misuse prevention design according to the requirements of 5.2.7.2;

c) Realize the design of SSOIS security function strength assessment according to the requirements of 5.2.7.3;

d) Realize vulnerability analysis design according to the requirements of **resistance of high-level** in 5.2.7.4.

6.5.6 SSOIS Security Management

SSOIS security management shall be designed based on relevant contents like technical requirements of physical security, operation security and data security in relation to the technical requirements for security function as well as SSOIS self-security and SSOIS design and realization in relation to the technical requirements for security assurance in this security protection level according to the requirements described in 5.3. It is required by this security protection level to respectively arrange specific personnel to assume importance security roles like system administrator, security officer and auditor, and respectively grant them with the minimum privilege required to complete their own tasks according to the "least authorization principle". At the same time, mutual restriction relationship shall be formed between them. Corresponding operation, operating rules as well as behavior rules and regulations shall be developed by this security protection level according to the following requirements:

a) Realize SSF function management according to the requirements of 5.3.1;

b) Realize security attribute management according to the requirements of 5.3.2;

c) Realize management of SSF data according to the requirements of 5.3.3;

d) Realize the definition and management of security role according to the requirements of 5.3.4;

e) Realize centralized management of SSOIS security mechanism according to the requirements of 5.3.5.

consideration of national security. Where determining the classification of own data information, each department and unit shall not only consider the national security according to the requirements of No. 66 document, but also consider its own security problems.

1) Category I data information: the data information for which Level-1 security protection is required to be carried out. This category of data information would have certain effect on the rights of citizen, legal person and other organizations after being destroyed, but will not endanger the national security, social order, economic construction and public interest.

2) Category II data information: the data information for which Level-2 security protection is required to be carried out. This category of data information would cause some damage to the national security, social order, economic construction and public interest after being destroyed.

3) Category III data information: the data information for which Level-3 security protection is required to be carried out. This category of data information would cause large damage to the national security, social order, economic construction and public interest after being destroyed.

4) Category IV data information: the data information for which Level-4 security protection is required to be carried out. This category of data information would cause serious damage to the national security, social order, economic construction and public interest after being destroyed.

5) Category V data information: the data information for which Level-5 security protection is required to be carried out. This category of data information would cause extremely serious damage to the national security, social order, economic construction and public interest after being destroyed.

It should be specially explained that the above classification of data information shall be consciously considered during risk analysis. The risk analysis is required to be implemented into data information; the risk of different data information shall be distinguished rather than carrying out risk analysis on the whole information system. In order to simplify the description, the category of data information is completely corresponding to the security protection level in the later description. For example, Category III data information is corresponding to Level-3 security protection and so on.

B.1.4 Principle and Method for Classification and Determination of Security Protection Level

B.1.4.1 Classification principle of security domain and security protection level

B.1.4.1.1 Partitioned protection principle

For a large-scale complex information system, partitioned protection according to the category of data information is the basic principle and method for the classification of security protection level. Area division shall be determined based on the classification of data information according to the business process needs of application system and the flow range of similar data information. Optimal area division shall be realizing the storage, transport and processing of data information for which the same security protection is required to be carried out in the same domain. The actual situation is often much more complex.

From the perspective of level classification, the security domain of typical information system may be graded into security computation domain, security user domain and security network domain. The security computation domain, security user domain and security network domain for which the same security protection is required to be carried out jointly compose a security domain with the security level of this information system.

a) Security computation domain

The security computation domain is the area storing and processing data information which is composed of a host/server or multiple hosts/servers connected through local area network in information system. Security computation domain shall have clear boundary. Where a security computation domain is composed of multiple hosts/servers, they shall be connected through local area network mutually. The classification of security computation domain shall be determined according to the range involved with the storage and processing of data information. Similar data information shall be stored and processed on the single host/server or that with close physical position as possible for constituting the security computation domain which is easy to carry out security protection.

b) Security user domain

Security user domain is the area storing, processing and using data information which is composed of one or more user terminal computers. Security user domain shall have clear boundary for protection. The classification of security user domain shall be determined according to the category of data information in computation domain which can be accessed by the user and the physical position of user computer. The users who can access to similar data information and have close physical position may constitute a security user domain for carrying out the security protection for the same level.

c) Security network domain

The security network domain is the area composed of network systems connecting the security computation domain and security computation

domain as well as the security computation domain and security user domain in information system. The security network domain is graded into local area network environment and wan environment. The security network domain constituted in local area network environment may be used to the connection between security computation domains constituted by single computer and the connection between security computation domains constituted by multicomputer. For the latter, this security network domain is actually the constituent part of security computation domain. The security network domain constituted in wan environment is used to the connection between remote security computation domains and the connection between security computation domain and security user domain. Security network domain is logical domain. Multiple different security network domains may be constituted in a physical network environment.

B.1.4.1.2 Specific principles of the classification of security domain and security protection level

The following specific principles of the classification of security domain and security protection level have certain universal applicability;

a) A large-scale complex system is divided into multiple security domains implementing the same security protection level according to the system network architecture and the classification and distribution of data information.

b) The classification of security domain may be physical or logical, both shall fully consider the security protection factor, such as certain boundary shall be provided.

c) The security computation domain, security user domain and security network domain which may implement the same level protection are determined according to the physical or logical structure. The scope of security domain shall be completely consistent with the flow range of data category.

d) A security computation domain may be composed of a set of host or server, or a local area network environment.

e) The security protection level which shall be provided for the security domain is determined according to the category of data in this security domain.

f) The security computation domain and security user domain may be viewed as the node of security network domain.

g) High-level (Level-4 and Level-5) security domain shall be divided according to the physical structure as possible, and there is only one category of data information in the same security domain.

h) The security domain below Level-3 may be of nested structure. For example, Level-3 security domain may be composed of one host or server in Level-2 security computation domain composed of one local area network.

i) The scope of data information for which lower-level security protection is required to be carried out is generally greater than that of data information for which high-level security protection is required.

j) The data information for which high-level (such as Level-4 and Level-5) security protection is required to be carried out shall be generally restricted within a smaller range, just like the traditional office confidential document is required to be archived in confidentiality room.

B.1.4.2 Classification method for security domain and security protection level

a) Define the category of data information which is required to be protected in information system.

In a complicated information system, the data information which is required to be protected may involve various data information categories. Generally, the category of data information for which low-level protection is required to be carried out is distributed widely, and that of data information for which high-level protection is required to be carried out is distributed intensively. Some system environment may have every category of data information and some only have a few or a certain category of data information. Before the classification of security domain and security protection level, the category of data information which is required to be protected in information system shall be defined firstly.

b) Carry out data distribution according to the principle of relative centralization for similar data information.

Data distribution is carried out according to the category of data information which is required to be protected in information system and the principle of relative centralization for similar data information so as to organize the security domains of different security levels. Such principle of relative centralization for data information is relatively easy to be implemented for the condition of carrying out security design synchronously with the newly-designed information system. For the design of existed information system security scheme, due to various reasons, the storage and processing of multi-category data may appear on one host or server (such condition shall be avoided for high level, such as Level-4 or Level-5). But where possible, the relative centralization of storage and processing of similar data information shall be considered as possible.

c) Set and determine the security protection level of security computation domain according to the distribution of data information category.

For Category V data information, special host or server shall be set in principle to constitute security computation domain according to the physical structure. Only Category V data information is stored and processed in this security domain for implementing the strictest security protection.

For Category IV data information, special host or server shall be set as possible to avoid sharing the host or server with data information of low security protection levels (Level-1, Level-2 and Level-3) and to constitute security computation domain according to the physical structure for implementing strict security protection.

For Category III data information, the host or server may be separately set according to the actual situation to constitute the security computation domain of single security protection level (Level-3), or the host or server is shared with Category I and Category II data information to constitute the security computation domain provided with multiple security protection levels (Level-3 and below).

For Category II data information, the host or server may be separately set according to the actual situation to constitute the security computation domain of single security protection level (Level-2), or the host or server is shared with Category I data information to constitute the security computation domain provided with multiple security protection levels (Level-2 and Level-1).

For the information system only having Category I data information, one or more security computation domains provided with Level-1 security protection are constituted according to the principle of close area.

d) Determine the security protection level of user domain according to the category of user-accessible data information.

The security protection level of security user domain entirely depends on the category of user-accessible data information. Furthermore, the security protection level of security user domain shall be determined according to the category of user-accessible highest-level data information. Where dividing the security user domain, the user terminal computers which can access to the same category of data and are geographically close shall be considered to be divided into one security user domain.

e) The security protection level of security network domain is determined according to that of security computation domain and security user domain connected through network.

The security network domain composed of network environment used for connecting the security computation domains and/or security user domain of the same security protection level shall be provided with the same security protection level as that of security computation domain. The security network domain composed of local area network which is regarded as the constituent part of security computation domain shall be provided with the same security protection level as that of security computation domain.

B.2 Overview of the Security Design of Information System

B.2.1 Overall Explanation for the Security Design of Information System

B.2.1.1 Schematic diagram for the security design of information system

The security design of a typical information system is as shown in Figure B.1. The security design of each specific information system is only some parts therein.

Figure B.1 is the schematic diagram for the security design of limited user information system in a controllable scope. In which, the circle diagrams of different thicknesses are used to represent the security computation domains with different security protection levels, the boxes of different thicknesses are used to represent the security user domains with different security protection levels and the lines with different thicknesses are used to represent the security network domains with different security protection levels. Independent circle diagrams represent the security computation domains of single level; nested circle diagrams represent the security computation domains with multiple security levels.

environment and condition aspect will also make some change in the threat). On this basis, risk analysis is carried out again to determine the security risk of target information system or security domain after adopting security measures, and to make the target information system or security domain reach the required security design target through adjusting security measures according to the principle of residual risk acceptance.

d) Security level determination

So far, the security design work of information system is far from being completed. Determining the security level of target information system or security domain according to the requirements of information security graded protection system and the security management needs of information system becomes an important part of the security design of graded information system. The corresponding security technologies (including security function technology and security assurance technology) and security management are selected based on the above determined security measures according to the graded requirements of information security technology and information security management in this Standard and other relevant standard to realize the determined security measures and determine the security level of target information system or security domain on this basis. This security level is the basis for the design, realization, test and assessment of target information system or security domain, and the basis for the operation control, supervision and inspection management of target information system or security domain.

B.2.3.3 Security design methods and steps of graded information system

The security design of information system shall be carried out in accordance with the following methods and steps according to the relevant factors of security design of information system and their interrelationship as shown in Figure B.3 as well as the requirements of graded protection:

Step I: Data classification. Classify the stored, transported and processed data information in information system by value with risk analysis method according to the idea that the data information asset is the prime asset of information system, and determine the security risk of various data information.

Step II: Data distribution. Determine the respective security demand according to the security risk of various data information, and reasonably distribute the stored, transported and processed data in information system according to the relative centralization principle of similar data information.

Step III: Security domain classification. Divide and determine the security computation domain and its security level according to the distribution

condition of various data information in information system; determine the security user domain and its security level according to the access condition of security computation domain; determine the network security domain and its security level according to the principle that the network connecting the security computation domain and/or security user domain with the same security level shall be provided with the same security level.

Step IV: System security level determination. Determine the security level of information system according to the security level of security domain in the system. If all security domains in information system are provided with the same security level, this information system is provided with this security level; if the security domain in information system is provided with multiple security levels, the security level of this information system shall be determined in accordance with the highest security level of security domain.

Step V: Security design of information system. Carry out system security design by security domain and layer, as shown in Figure B.2. The physical security with different security protection levels shall be designed according to the requirements of different security levels; for mixed security domain with multiple different security levels, the physical security shall be designed according to the requirements of the supported highest security level; the system security shall provide the support for operating system and database management system support with corresponding security level according to different requirements of different security levels; for network security, the corresponding security level design shall be carried out respectively for the relevant local area network and wide area network according to the determined security level; for application security, the development tool with corresponding security level shall be selected according to the determined security level, and the development of application system with corresponding security level shall be carried out according to the required security level. The security of application system is the starting point and destination of the security design of information system. The security functions required for application system shall be realized under the support of all lower-layer security mechanisms or the self-design of application layer. These security functions in different layers cannot be mutually replaced.

B.2.3.4 Security design example of graded information system

B.2.3.4.1 Schematic diagram for the security design of graded information system

Figure B.4 is the schematic diagram for the security design example of information system.

security for connecting each host or server, etc. Mixed security network domain shall be designed according to high-level requirements.

d) Level-1 security domain design

Logically, Level-1 security domain may be that in mixed security domain with multiple security levels, or a security domain with single security level which is composed of the security computation domain, security user domain and security network domain with Level-1 security only. Level-1 security domain as shown in Figure B.4 mainly includes: Level-1 security computation domain in a mixed security computation domain with Level-1, -2 and -3 security, Level-1 security computation domain in a mixed security computation domain with Level-1 and -2 security, one single security computation domain with Level-1 security as well as the user domain and network domain with Level-1 security. The design of mixed security computation domain shall be realized in unit of host or server. If the mixed security computation domain is composed of multiple independent hosts or servers with single security level, independent security design shall be carried out for each host or server; if one host or server is provided with multiple security levels, the security design is carried out according to high-level requirements. The security design of Level-1 security computation domain is mainly the physical security design of computer system and the security design of operating system, database management system and application system, including the configuration of security operating system and database management system with at least Level-1 security, the development of application system with at least Level-1 security, and the security design of local area network with at least Level-1 security for connecting each host or server, etc. Mixed security network domain shall be designed according to high-level requirements.

Appendix C

(Informative)

The Corresponding Relationship between the Elements and Graded Requirements of Security Technology

The corresponding relationship between the elements and graded requirements of security technology are given in Table C.1 and Table C.2.

Table C.1 The Corresponding Relationship between the Elements and Graded Requirements of Security Function Technology

Element of security function technology	Graded requirements of security function technology				
	The user's discretionary protection level	System audit protection level	Security label protection level	Structured protection level	Access verification protection level
4.1 Physical security	*	*	*	*	*
4.1.1 Environmental security	*	*	*	*	*
4.1.1.1 Security protection for central machine room	*	*	*	*	*
4.1.1.1.1 Site selection for machine room	*	*	*	*	*
a) Basic requirements	*	*			
b) Fire protection requirements			*	*	*
c) Anti-pollution requirements			*	*	*
d) Moisture-proof and lightning protection requirements			*	*	*
e) Shock-proof and noise-proof requirements			*	*	*
f) Strong electrical field and magnetic field prevention requirements			*	*	*
g) Earthquake and flood prevention requirements			*	*	*
h) Position requirements			*	*	*
i) Public interference prevention requirements				*	*
4.1.1.1.2 Protection for internal security of machine room	*	*	*	*	*
a) Machine room access	*	*	*	*	*
b) Machine room articles	*	*	*	*	*
c) Machine room personnel			*	*	*

Element of security function technology	Graded requirements of security function technology				
	The user's discretionary protection level	System audit protection level	Security label protection level	Structured protection level	Access verification protection level
d) Machine room subarea			*	*	*
e) Machine room access control			*	*	*
4.1.1.1.3 Fire protection for machine room	*	*	*	*	*
a) Fire prevention for building material ①	*	*			
b) Fire prevention for building material ②			*		
c) Fire prevention for building material ③				*	*
d) Alarm and fire extinguishing system ①	*	*			
e) Alarm and fire extinguishing system ②			*		
f) Alarm and fire extinguishing system ③		*		*	*
g) Area separation and fire protection	*	*	*	*	*
4.1.1.1.4 Power supply and distribution of machine room	*	*	*	*	*
a) Separate power supply	*	*			
b) Emergency power supply ①			*		
c) Emergency power supply ②				*	*
d) Emergency power supply ③			*	*	*
e) Standby power supply		*	*	*	*
f) Stable voltage power supply		*	*	*	*
g) Power protection			*	*	*
h) Uninterrupted power supply				*	*
i) Electrical appliance noise protection				*	*
j) Emergency protection				*	*
4.1.1.1.5 Air conditioning and cooling of machine room	*	*	*	*	*
a) Basic temperature requirements	*	*			
b) Relatively complete air conditioning system			*		
c) Complete air conditioning system				*	*
4.1.1.1.6 Waterproofing and	*	*	*	*	*

Element of security assurance technology	Graded requirements of security assurance technology				
	The user's discretionary protection level	System audit protection level	Security label protection level	Structured protection level	Access verification protection level
5.2.1 Configuration management	*	*	*	*	*
5.2.1.1 Configuration management capacity	*	*	*	*	*
a) Version No.	*	*	*	*	*
b) Configuration item			*	*	*
c) Authorized control			*	*	*
d) Generation support and acceptance process				*	*
e) Further support					*
5.2.1.2 Configuration management automation			*	*	*
a) Partial automation of CM			*	*	
b) Full automation of CM					*
5.2.1.3 Configuration management scope		*	*	*	*
a) SSOIS configuration management scope		*			
b) Problem-tracking configuration management scope			*		
c) Development tool configuration management scope				*	*
5.2.2 Distribution and operation	*	*	*	*	*
5.2.2.1 Distribution	*	*	*	*	*
a) Distribution process	*	*			
b) Modification test			*		
c) Modification prevention				*	*
5.2.2.2 Operation (installation, generation and start)	*	*	*	*	*
a) The process of installation, generation and start	*	*	*	*	*
b) Log generation		*	*	*	*
5.2.3 Development	*	*	*	*	*
5.2.3.1 Function design	*	*	*	*	*
a) Non-formalized function design	*				
b) Fully defined external interface		*	*		
c) Semi-formalized function design				*	
d) Formalized function design					*
5.2.3.2 Security policy modeling		*	*	*	*

Element of security assurance technology	Graded requirements of security assurance technology				
	The user's discretionary protection level	System audit protection level	Security label protection level	Structured protection level	Access verification protection level
a) Non-formalized SSOIS security policy model		*	*		
b) Semi-formalized SSOIS security policy model				*	
c) Formalized SSOIS security policy model					*
5.2.3.3 High-level design	*	*	*	*	*
a) Descriptive requirements of high-level design	*	*			
b) Security-intensified high-level design			*		
c) Semi-formalized high-level design				*	
					*
d) Formalized high-level design	*	*	*	*	*
5.2.3.4 Low-level design	*	*	*		
a) Descriptive requirements of low-level design				*	
b) Semi-formalized low-level design					*
c) Formalized low-level design	*	*	*	*	*
5.2.3.5 SSF internal structure	*				
a) Modularization		*	*		
b) Layering				*	*
c) Minimized complexity	*	*	*	*	*
5.2.3.6 Realization expression	*	*			
a) Subset realization of SSF			*		
b) Full realization of SSF				*	*
c) Structured realization of SSF	*	*	*	*	*
5.2.3.7 Expression correspondence	*	*	*		
a) Non-formalized correspondence description				*	
b) Semi-formalized correspondence description					*
c) Formalized correspondence description					
5.2.4 Document requirements	*	*	*	*	*
5.2.4.1 Security administrator guide	*	*	*	*	*
5.2.4.2 User guide	*	*	*	*	*
5.2.5 Life cycle support	*	*	*	*	*

Element of security assurance technology	Graded requirements of security assurance technology				
	The user's discretionary protection level	System audit protection level	Security label protection level	Structured protection level	Access verification protection level
5.2.7.2 Misuse prevention		*	*	*	*
a) Document inspection		*	*	*	*
b) Analysis validation			*	*	*
c) Test and analysis of security state				*	*
5.2.7.3 Strength assessment of SSOIS security function		*	*	*	*
5.2.7.4 Vulnerability analysis		*	*	*	*
a) Developer vulnerability analysis		*			
b) Independent vulnerability analysis			*		
c) Resistance of medium level				*	
d) Resistance of high-level					*
5.3 SSOIS security management	*	*	*	*	*
5.3.1 SSF function management	*	*	*	*	*
5.3.2 Security attribute management		*	*	*	*
a) Management security attribute		*	*	*	*
b) Secure security attribute		*	*	*	*
c) Static attribute initialization		*	*	*	*
d) Security attribute termination		*	*	*	*
e) Security attribute revocation		*	*	*	*
5.3.3 SSF data management		*	*	*	*
a) Management of SSF data		*	*	*	*
b) Management of SSF data bound		*	*	*	*
c) Security SSF data			*	*	*
5.3.4 Definition and management of security role			*	*	*
a) Definition of security role			*	*	*
b) Restriction of security role			*	*	*
c) Acting as the security role			*	*	*
5.3.5 Centralized management of SSOIS security mechanism			*	*	*
Note: "*" represents that this requirement is provided. Specific requirements for each security protection level may be different, as detailed in Chapter 6.					

References

[1] GB 50174-1993 Designing Code for Electronic Machine room

[2] GB/T 18336.I-2001 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 1: Introduction and General Model (idt ISO/IEC 15408-1:1999)

[3] GB/T 18336.2-2001 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 2: Security Function requirements (idt ISO/IEC 15408-2:1999)

[4] GB/T 18336.3-2001 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3: Security Assurance Requirements (idt ISO/IEC 15408-3:1999)

_____ END _____

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

Full-copy PDF can be purchased from 1 of 3 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

3. https://www.google.com/search?tbm=bks&q=ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Google Books -- Select your currency.
- Processed by Google (delivery, tax invoice etc.). Delivered in 9 seconds by Google.
- Tips: Download an unprotected True-PDF (text-editable) from Google-Books:
  1. https://play.google.com/books → 2. Sign in → Google account
  3. Find the BOOK you bought → 4. Click "3-dots" → Export
  5. Save as "*.pdf" (Save True-PDF to your local computer for offline reading/printing)

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

Accountable person and shareholder: Wayne Zheng

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------