TECHNICAL SPECIFICATION

ISO/TS 11633-1

First edition
2019-08

Health informatics — Information security management for remote maintenance of medical devices and medical information systems —

Part 1: Requirements and risk analysis

Informatique de santé — Management de la sécurité de l'information pour la maintenance à distance des dispositifs médicaux et des systèmes d'information médicale —

Partie 1: Exigences et analyse du risque

Reference number
ISO/TS 11633-1:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

This first edition cancels and replaces ISO/TR 11633-1:2009, which has been technically revised. The main changes compared to the previous edition are as follows:

— complete revision to correspond to the latest editions of the reference standards, ISO/IEC 27001 and ISO/IEC 27002;

— addition of use case 'remote monitoring'.

A list of all parts in the ISO 11633 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The advancement and spread of technology in the information and communication technology field, and the infrastructure based on them, have brought many changes in how technology and networks are used in modern society. Similarly, in healthcare, information systems which were once closed in each healthcare facility (HCF) are now connected to the outside by networks and are progressing to the point of being able to facilitate mutual use of health information accumulated in these information systems. Such information and communication networks are spreading not only in between HCFs but also between HCFs and vendors of medical devices and healthcare information systems. Maintenance of such systems is paramount to keeping them up-to-date. By practicing so-called 'remote maintenance services', it becomes possible to reduce down-time and lower costs for this maintenance activity.

Whilst there are benefits to remote maintenance, such remote connections with external organizations also expose HCFs and vendors to risks regarding confidentiality, integrity and availability of information and systems; risks which previously received scant consideration.

Although normal remote maintenance is generally done on a contract basis, in the case of medical devices, risk assessment is commonly a legal prerequisite. Therefore, it is necessary to implement appropriate risk assessment where remote maintenance is provided in any healthcare context. The risk assessment examples provided in ISO/TR 11633-2 provide support for HCFs and RMS providers to implement risk assessment effectively.

By implementing the risk assessment process and employing controls referencing ISO/TR 11633-2, HCFs owners and RMS providers will be able to obtain the following benefits:

— Risk assessment can result in improved efficiency. If the risk assessment document created through the use of ISO/TR 11633-2 does not fully conform to ISO/IEC 27001, it can be used in part in a risk assessment of an incompatible area, thus reducing the risk assessment effort required.

— Documented validity of the RMS security countermeasures in place will be available to third parties.

If providing RMS to two or more sites, the provider can apply countermeasures consistently and effectively.

Health informatics — Information security management for remote maintenance of medical devices and medical information systems —

Part 1: Requirements and risk analysis

1 Scope

This document focuses on remote maintenance services (RMS) for information systems in healthcare facilities (HCFs) as provided by vendors of medical devices and health information systems.

This document specifies the risk assessment necessary to protect remote maintenance activities, taking into consideration the special characteristics of the healthcare field such as patient safety, regulations and privacy protections.

This document provides practical examples of risk analysis to protect both the HCF and RMS provider information assets in a safe and efficient (i.e. economical) manner. These assets are primarily the information system itself and personal health data held in the information system.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
asset
anything that has value to the organization

[SOURCE: ISO/IEC 21827:2008, 3.4]

Note 1 to entry: In the context of health information security, information assets include

a) health information,

b) technical information (credentials, passwords, calibration data, etc.),

c) non-health information (e.g. financials, administrative, legal, human resources, etc.),

d) IT services,

e) hardware,

f) software,

g) communications facilities,

h) media,

i) IT facilities, and

j) medical devices that record or report data.

3.2
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 21547:2010, 3.2.7]

3.3
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 21827:2008, 3.13]

3.4
information security
preservation of *confidentiality* (3.3), integrity and *availability* (3.2) of information

Note 1 to entry: Other properties, particularly accountability of users, but also authenticity, non-repudiation, and reliability are often mentioned as aspects of information security but could be considered as derived from the three core properties in the definition.

3.5
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

[SOURCE: ISO/IEC 31000:2018, 3.1]

3.6
risk assessment
overall process of risk identification, risk analysis, and risk evaluation

[SOURCE: ISO/TS 13131:2014, 3.5.4]

3.7
threat
potential cause of an unwanted incident, which may result in harm to a system or organization

4 An outline of RMS security of medical devices and medical information systems

4.1 Contents of RMS security of medical devices and medical information systems

4.1.1 General

The following architectural configuration is assumed in this document (Figure 1):

— target device;

— internal network within a HCF;

— external network connecting a HCF and remote service centre (RSC);

— internal network within a RSC;

— equipment and services in the RSC.

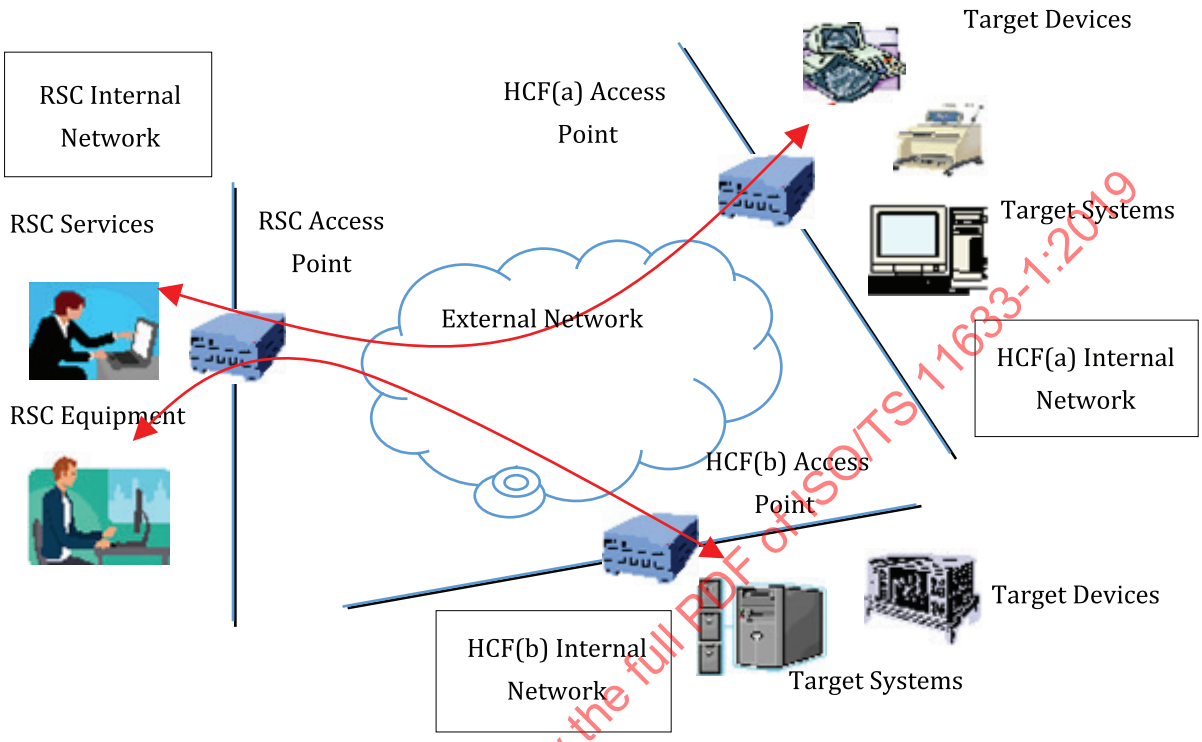

Figure 1 — Assumed RMS architecture

This document introduces the potential types of RMSs and provides options for appropriate security controls to be considered in the risk analysis phase.

Use cases of RMSs are provided in Annex A.

The types of RMS and technical security measures related to each type are explained in 4.1.2 and 4.1.3.

4.1.2 RMS using a public switched telephone network

Where a HCF sets up a machine for dial-up server function, the machine connects with a public switched telephone network via modem and waits for access from a RSC remote connection. Telecommunications equipment that offer these functions such as dial-up routers are in widespread use.

In the use of the public switched telephone network, telecommunication lines have the following features:

— a one-to-one communication pathway between a HCF and the RSC can be secured;

— tapping is difficult because a public switched telephone network is fully-digitalized.

Using these features, security can be maintained by the following technical measures:

— determination of caller number — use of call back certification function or caller ID specification certification function;

— user certification — use of one-time password and encryption of password; and

— review of communication audit logs to detect illegal access attempts to a HCF.

4.1.3 RMS using the Internet

A device using an Internet connection with an externally accessible IP address is placed at the HCF. The RSC prepares the Internet connection environment and connects itself to the HCF through the Internet.

This subclause specifies the technologies for communication and user authentication between a HCF and a RSC using the Internet for connection. This is the same as a typical Internet connection and not a one-to-one communication like the public switched telephone network.

Examples of security control are shown below:

— using firewall(s);

— using tools such as anti-virus software;

— communication using VPN for encryption of the communication path; and

— use of a variety of user authentication methods such as one-time passwords, multi-factor authentication and digital certificates

4.2 Security requirement of RMS of medical devices and medical information systems

4.2.1 General

The RMS security requirements can be classified into three categories: measures, contracts and protection measures.

4.2.2 Security measures in RMS operation

Regulations and legislation commonly drive specific requirements on how to operate a system securely and protect the privacy of personal information. Examples are shown below:

— those concerning the RSC operator;

— measures for excluding unauthorized operations;

— requirements for when RSC remote terminals are increased or relocated; and

— requirements for access from mobile terminals.

4.2.3 Contracts between HCF and RSC including 3rd parties

The following can be used to prepare for security incidents:

— requirements for responsibility demarcation between a HCF and a RSC;

— establishment of contracts between a HCF and a RSC, including requirements for confidentiality, integrity and availability of information.

4.2.4 Protection of personal information

There might be provisions that impose obligations on a HCF for the protection of personal health information. As remote services provide an interface with a health information system which potentially contains personal health information, the RMS provider shall incorporate security measures to protect personal information.

There are various means for providing security measures in a RMS. Each RMS provider maintains security by using these mean, taking into account the relevant provisions.

4.3 Roles of RSC and HCF

Where the HCF has entrusted the RMS provider with providing security for the RMS by establishing a maintenance contract with the RMS providers, the security of RMS is implemented under the requirements and responsibility of each RMS provider.

In this case, the following issues can arise:

— there is no statement through which the third party can verify that the RMS provider is providing sufficient and appropriate security measures.

— the HCF has not considered the management measures as much as technological measures related to the security measures.

— the HCF has insufficiently examined the sequence of events after an accident occurs.

— the HCF has not examined the broad threat landscape and associated risks such as computer viruses.

In some cases, it might be required that HCFs take responsibility for personal information protection. The HCF also has to take responsibility for the security of the RMS. Therefore, this document explains the role of HCF and RMS providers. Implementing security in RMS is the role of RMS providers, with oversight by the HCF, because the RMS provider is responsible for implementation of the RMS function. RMS providers need to consider implementing them properly in combination with various security technologies and operations so that dissemination of RMS is not impeded due to security deficiencies. RMS providers need to consider implementing them properly in combination with various security technologies and operations so that dissemination of RMS is not impeded due to security deficiencies.

RMS providers are encouraged to use standard and widely used security technologies when designing and implementing their RMS solutions. Proprietary and overly complex solutions can lead to unintended security weaknesses and therefore should be avoided.

In preparing access points for each RMS, RMS providers might make security management complicated. Such complicated management allows security breaches to take place. Therefore, each RMS provider shall to adopt and implement standard and widely used security technologies.

Management measures are important as well as technological measures. These are necessary for both the HCF and the RSC. They should document a current information security management system based on International Standards such as ISO/IEC 27001, which support the implementation of appropriate security policy. Subsequently, the HCF and RSC should compare and understand their associate security policies to ensure consistency in protection. It is important to clarify the minimum standard of security required by the RMS. The HCF decides and takes measures based on its own security policy and examines and evaluates the security policy and security measures provided by the RMS provider. Consequently, the HCF should contract the RMS provider with specific requirements for operational compliance and confidentiality. The contract agreement should be implemented before commencing operations. As a result, RMS security is achieved to an agreed and predefined level.

5 Risk analysis

When the RMS is implemented, the RMS provider and HCF should jointly perform and reach agreement on the risk analysis process and outcomes for the RMS implementation.

Example of risk analysis result of RMSs are provided in Annex B and example of risk analysis criteria in Annex C.

Examples of risk analysis are shown in ISO/TR 11633-2.

Annex A
(informative)

Use case of RMSs

A.1 General

This annex describes four typical use cases of RMSs, considered as a model of basic operations.

a) Trouble shooting for outages

In case of outage of equipment within the HCF site, and in response to a request from the HCF site, maintenance operations are performed by accessing the targeted devices from the RSC site.

b) Scheduled maintenance

Scheduled maintenance operations are performed from the RSC site by obtaining consent of the HCF site. This might cause periodic access to target devices in the HCF.

c) Software updating

Updating software of targeted devices within the HCF site by direct access from the RSC site.

d) Performance monitoring

Performance monitoring checks the maintenance activities (preventive maintenance, normal state check, life-and-death monitoring, and so on) on a target device in the HCF.

A.2 Trouble shooting for outages

The workflow, in the case of trouble shooting for outages, is shown in Figure A.1.

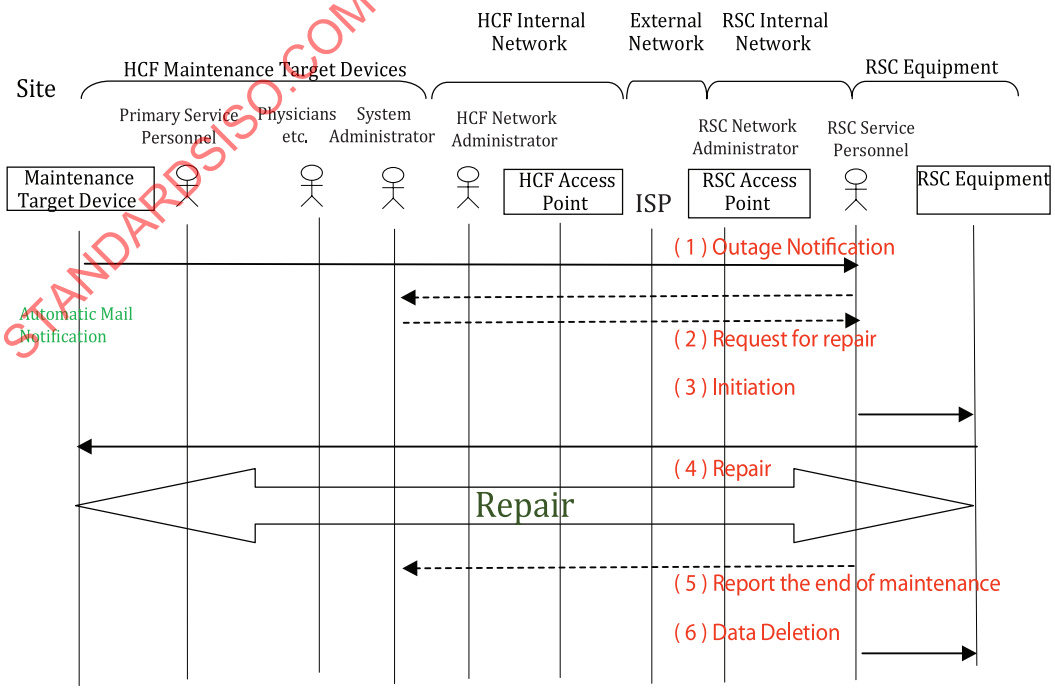

Figure A.1 — Workflow in the case of trouble shooting outages

(1) An alert is issued from the maintenance target device to the RSC equipment via the always-connected line, and the RSC service person informs the HCF system administrator by telephone or the like.

(2) HCF system administrator requests RSC service person for repair.

(3) Execute network connection from RSC to HCF in the following procedure.

a) RSC service personnel operates RSC equipment.

b) Establish network connection between RSC equipment and maintenance target equipment.

(4) RSC service staff, individuals or team, perform inspection, treatment, and acknowledgement via the network connection. This might include the following:

a) implementation of an automatic inspection program

b) collection of related information from targeted equipment, including (but not limited to)

i) operation logs,

ii) image data,

iii) configuration files / system configurations, and

iv) contents of database

c) investigation of the problem

d) if the problem has its origin in software, modification or update of the targeted equipment the following actions may be taken:

i) modification of configuration files;

ii) update software:

iii) data restoration.

e) if the problem has its origin in hardware, contact with the device primary service contact to resolve issue and potentially exchange non-functioning hardware elements.

f) carrying out inspection after repair.

(5) RSC service personnel notifies the HCF system administrator of the completion of remote maintenance work.

(6) If RSC resolution required the transfer of protected health information (PHI), RSC deletes all copies of the PHI transferred locally to their site.

A.3 Scheduled maintenance

The workflow in the case of scheduled maintenance is shown in Figure A.2.

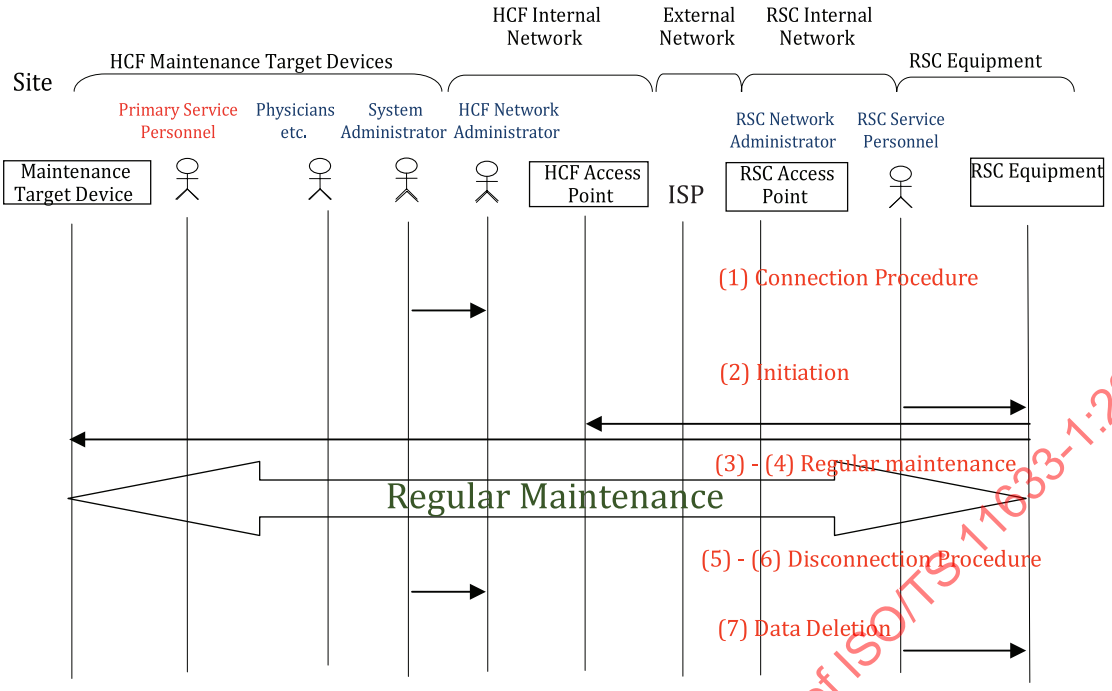

Figure A.2 — Workflow in the case of scheduled maintenance

The process steps are as follows:

(1) RSC requests the HCF to connect the network for the RMS.

(2) RSC initiates the network connection.

(3) RSC service staff, individuals or team perform scheduled inspection via the network connection. This might include the following:

a) implementation of an automatic inspection program;

b) log checking;

c) image quality and accuracy checking;

d) collection of operational information.

(4) RSC reports the inspection result to the HCF.

(5) RSC disconnects the network connection for the RMS.

(6) RSC requests HCF to disconnect the network connection for the RMS.

(7) If RSC transferred PHI, RSC deletes all copies of the PHI transferred locally to their site.

A.4 Software updating

The workflow in the case of software updates is shown in Figure A.3.

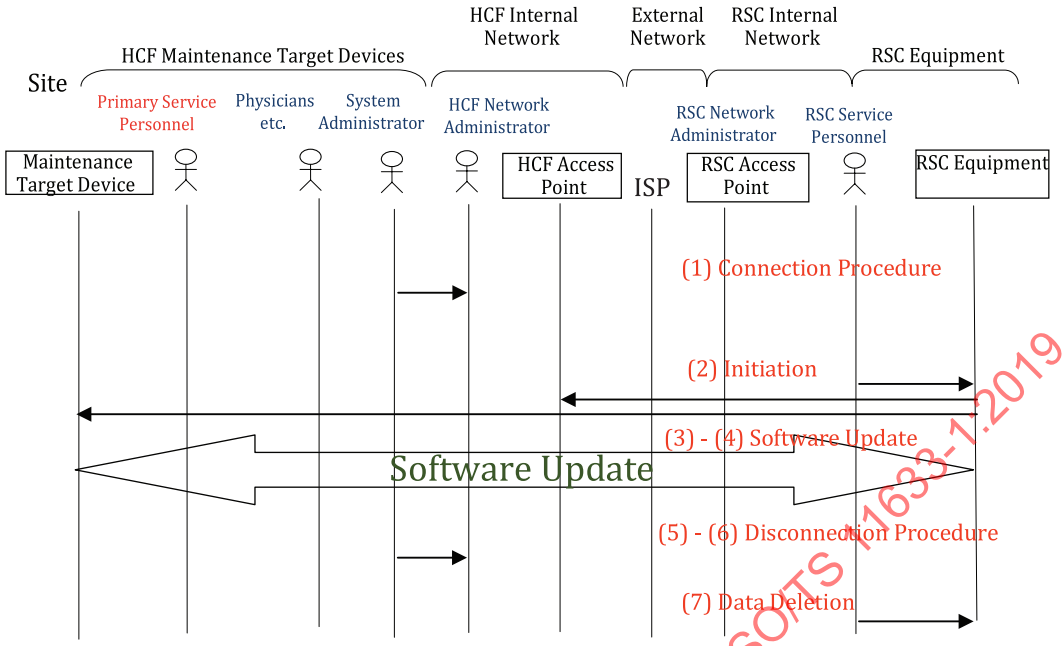

Figure A.3 — Workflow in the case of software updates

Steps are as follows:

(1) RSC requests the HCF for a network connection for the RMS.

(2) RSC initiates network connection.

(3) RSC service staff, individuals or team update the software via the network connection. This might include

a) replace necessary software,

b) update necessary configurations, and

c) confirmation of functional operation.

(4) RSC reports the update outcomes to the HCF.

(5) RSC disconnects network connection for the RMS.

(6) RSC requests HCF to disconnect network connection for the RMS.

(7) If RSC transferred PHI, RSC deletes all transferred data locally to their site.

A.5 Performance monitoring

The workflow in the case of performance monitoring is shown in Figure A.4.

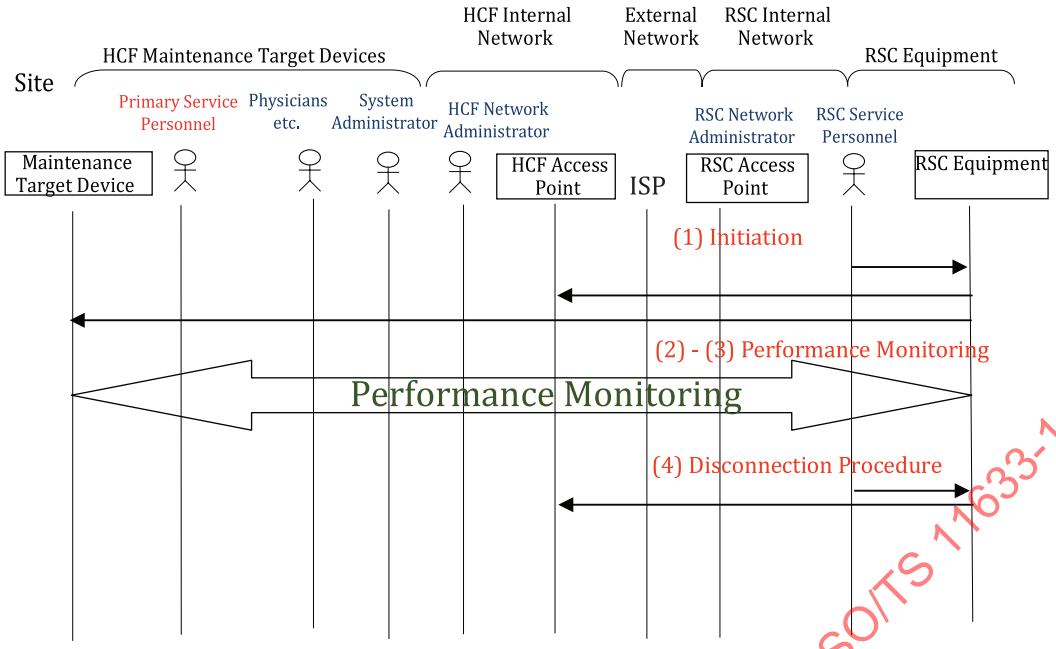

Figure A.4 — Workflow in the case of performance monitoring

Steps are as follows:

(1) RSC initiates the network connection.

(2) RSC service staff, individuals or team perform monitoring via the network connection. This might include the following:

a) implementation of an automatic inspection program;

b) log checking;

c) collection of operational information.

(3) RSC reports the performance monitoring result to the HCF.

(4) RSC disconnects the network connection for the RMS.

Annex B
(informative)

Example of risk analysis result of remote maintenance services

B.1 Assets and Threats (Site: RSC Equipment)

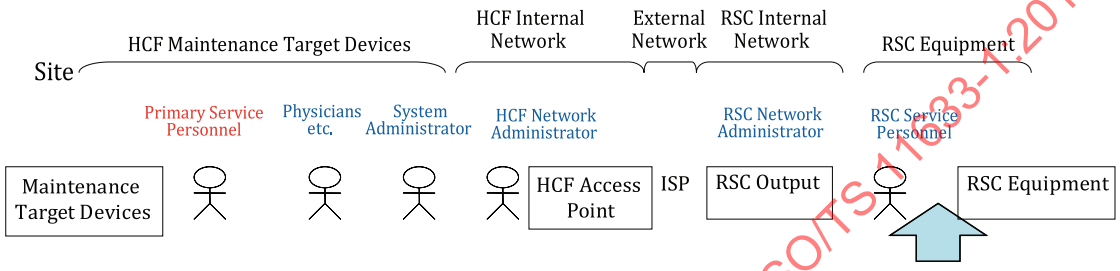

Figure B.1

Assets	No.	Threat (C: Confidentiality, I: Integrity, A: Availability)
PHI on memory, disk, and screen	1-1	Exposure [C] by Deletion failure on site [C], Peeping [C]/Theft [C], Unauthorized login to RSC equipment [C]/ Spoofing [C]
	1-2	Exposure [C] by Theft from path [C], Unauthorized login to RSTC equipment [C]/Spoofing [C]
Physical outputs (e.g. memos and printed reports) of PHI	1-3	Exposure [C] by Peeping of paper records for repair [C], Carrying out [C]
Backup media of PHI	1-4	Exposure [C] by Carrying out of recorded media for repair [C]
Software dealing with PHI	1-5	Exposure [C] by Back door/Installation of information-stealing program [I]
Equipment dealing with PHI	1-6	Exposure [C] by Carrying out [C], Tampering [C], Leakage electromagnetic radiation [C]
	1-7	Service impossible [A] due to Failure [A], Disaster [A], Damage [A]
Equipment dealing with PHI [a]	1-8	Service impossible [A] due to Failure [A], Disaster [A], Damage [A]
Operators dealing with PHI	1-9	Exposure by bribery [C], Service Failure [A] by Incorrect input [I]/ Deletion failure [A]
Encryption algorithm, keys, and key distribution method	1-a	Exposure [C] by Decoding of encrypted data [C]

[a] Indicate the power/disaster facilities. Note, however, that the network equipment is not included.

B.2 Assets and Threats (Site: RSC Internal Network)

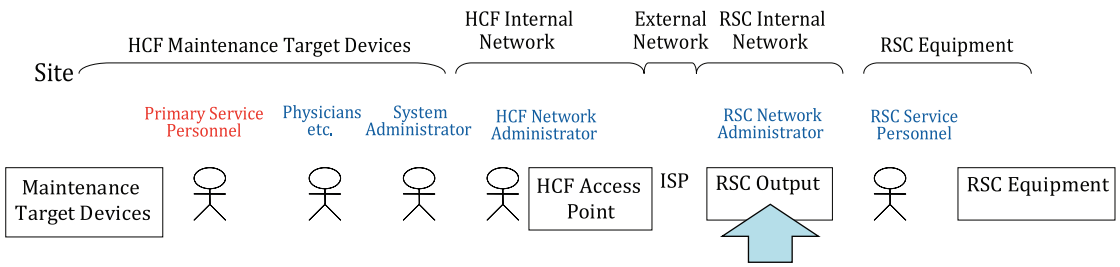

Figure B.2

Assets	No.	Threat (C: Confidentiality, I: Integrity, A: Availability)	
		Without countermeasures on VPN	With countermeasures on VPN
PHI on RSC internal network	2-1	Exposure [C] by Peeping of path [C], Unauthorized login to RSC network equipment [C]/Spoofing [C], Tapping [C]	Threat other than [A] Availability is negligible
Physical outputs (e.g. memos and printed reports) of communication traces	2-2	Exposure [C] by Peeping of monitor recording sheet [C], Carrying out [C]	
Backup media of communication trace	2-3	Exposure [C] by Carrying out of monitor recording media [C]	
Network equipment software	2-4	Exposure [C] by Back door/Installation of information-stealing program [I]	
Network equipment	2-5	Exposure [C] by Carrying out [C], Tampering [C], Leakage electromagnetic radiation [C]	
	2-6	Service impossible [A] due to Failure [A], Disaster [A], Damage [A]	
Environmental facilities of network equipment [a]	2-7	Service impossible [A] due to Failure [A], Disaster [A], Damage [A], Cable discontinuity [A]	
Network equipment operators	2-8	Exposure by bribery [C], Exposure [C] by Incorrect setting [C]	
Encryption algorithms, keys, and key distribution method	2-9	Exposure [C] by Decoding of encrypted data [C]	

[a] Indicate the power/disaster facilities.

B.3 Assets and Threats (Site: External Network)

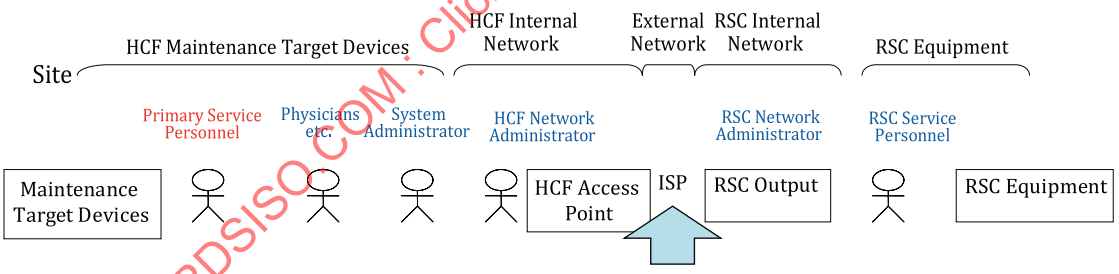

Figure B.3

Assets	No.	Threat (C: Confidentiality, I: Integrity, A: Availability) The presence of countermeasures on the VPN is assumed. Threats except for Availability (A) are negligible.
PHI on external networks	3-1	Negligible
Physical outputs (e.g. memos and printed reports) of information communication traces	3-2	Negligible
Backup media of information communication traces	3-3	Negligible
Network equipment software	3-4	Negligible

[a] Indicate the power/disaster facilities.

Assets	No.	Threat (C: Confidentiality, I: Integrity, A: Availability) The presence of countermeasures on the VPN is assumed. Threats except for Availability (A) are negligible.
Network equipment	3-5	Negligible
	3-6	Service impossible [A] due to Failure [A], Disaster [A], Damage [A]
Environmental facilities of network equipment [a]	3-7	Service impossible [A] due to Failure [A], Disaster [A], Damage [A], Cable Discontinuity [A]
Network equipment operators	3-8	Negligible
Encryption algorithm, keys, and key distribution method	3-9	Exposure [C] by Decoding of encrypted data [C]
[a] Indicate the power/disaster facilities.		

B.4 Assets and Threats (Site: HCF Internal Network)

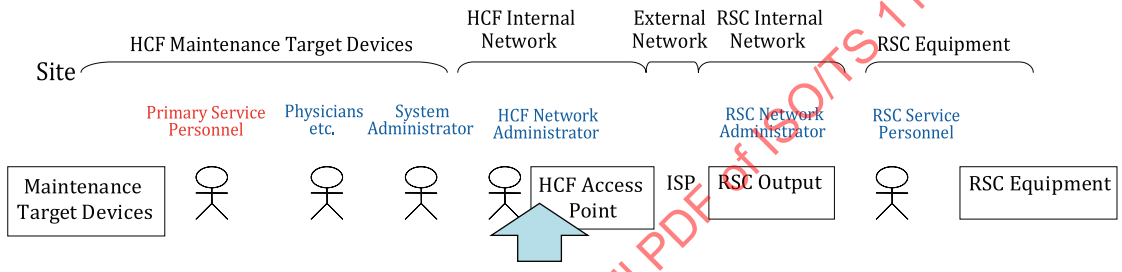

Figure B.4

Assets	No.	Threat (C: Confidentiality, I: Integrity, A: Availability)
PHI on HCF internal network	4-1	Exposure [C] by Peeping of path [C], Unauthorized login to HCF network equipment [C]/Spoofing [C], Tapping [C]
Physical outputs (e.g. memos and printed reports) of information communication traces	4-2	Exposure [C] by Peeping of monitor recording sheet [C], Carrying out [C]
Backup media of information communication traces	4-3	Exposure [C] by Carrying out of monitor recording media [C]
Network equipment software	4-4	Exposure [C] by Back door/Installation of information-stealing program [I]
Network equipment	4-5	Exposure [C] by Carrying out [C], Tampering [C], Leakage electromagnetic radiation [C]
	4-6	Service impossible [A] due to Failure [A], Disaster [A], Damage [A]
Environmental facilities of network equipment [a]	4-7	Service impossible [A] due to Failure [A], Disaster [A], Damage [A], Cable Discontinuity [A]
Network equipment operators	4-8	Exposure by bribery [C], Exposure [C] by Incorrect setting [C]
[a] Indicate the power/disaster facilities.		