International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2243

(08/2019)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Next Generation Networks – Service aspects: Service capabilities and service architecture

A service model for risk mitigation service based on networks

Recommendation ITU-T Y.2243

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2243

A service model for risk mitigation service based on networks

Summary

A risk mitigation service based on networks monitors risk events, stores the data in real time and analyses the associated data. Furthermore, it may perform the analysis of plant disease risks, marine aquaculture risks, or livestock disease risks, and provide corresponding mitigation services. Recommendation ITU-T Y.2243 describes the service model for risk mitigation based on networks that covers real time data acquisition, monitoring of risk events, and provision of mitigation services for the identified risks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2243	2019-08-13	13	11.1002/1000/13982

Keywords

Risk mitigation function, risk mitigation service, risk monitoring function.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2243

A service model for risk mitigation service based on networks

1 Scope

This Recommendation concerns the following:

- Risk mitigation service concepts and service model;
- Risk mitigation service requirements;
- Risk mitigation service network capability requirements;
- Risk mitigation service scenarios.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T T.135] Recommendation ITU-T T.135 (2007), *User-to-reservation system transactions within T.120 conferences.*

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 service user [ITU-T T.135]: A person, an organization or any intermediate entity using the services provided by a service provider.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 risks: Events or possibilities of events that may cause harmful impact on plants, (e.g., plant diseases), livestock (e.g., livestock diseases) or marine aquaculture (e.g., harmful algal bloom).

3.2.2 risk mitigation: Action to prevent a risk and reduce the impact of a risk incident.

3.2.3 risk mitigation control servers: Servers that react to the external risk occurrences via the reception of external risk information and internal decisions.

3.2.4 risk mitigation process: Processes running inside the risk mitigation control servers to measure the seriousness and possibilities of the risks from the collected risk information.

3.2.5 risk mitigator: A person, an organization or any entity that is responsible for preventing possible risks or reducing the possibilities of risks.

3.2.6 risk sufferer: A person, an organization or any entity affected by any risks.

3.2.7 service provider: An organization owning or controlling one or more systems and using them to provide services.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization, Accounting
AI	Avian Influenza
API	Application Programming Interface
CEO	Chief Executive Officer
DRM	Digital Rights Management
ELISA	Enzyme-Linked Immunosorbent Assay
FMD	Foot and Mouth Disease
HPAI	Highly-Pathogenic Avian Influenza
ISDN	Integrated Service Digital Network
NGN	Next Generation Network
PCR	Polymerase Chain Reaction
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFID	Radio Frequency Identification
RMAF	Risk Mitigation Action Function
RMDF	Risk Monitoring and Detection Function
VS	Vesicular Stomatitis

5 Conventions

The words "is required to" indicate a requirement which must be met and from which no deviation is permitted if conformance with this Recommendation is to be claimed.

The words "is recommended" indicate a requirement which is recommended but which is not absolutely required to be met to claim conformance with this Recommendation.

The words "can optionally" indicate an optional feature which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation is required to provide the option and that the feature can be optionally enabled by a network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

In this Recommendation, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted respectively as, is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Concept of risk mitigation service

Risk mitigation service refers to all aspects of the risk mitigation processes which are intended to reduce the impact of risks and develops mitigation processes, as part of the service, based on data. In the conceptual diagram shown in Figure 1, risk events are detected by analysing risk data obtained from service areas owned by farm owners or enterprises, i.e., risk sufferers via communication networks. Risk mitigation service providers then classify the risk types and assess the impacts due to the detected risks. The risk status will be delivered based on the risk types and impact levels to the relevant parties, i.e., risk mitigators that are responsible for coping with risks such as disaster prevention headquarters or local officers to prevent risk dispersion . The results after these risk mitigation actions have been performed will ultimately be delivered to the service users (risk mitigators and risk sufferers). A reference architecture based on this concept will be described in clause 7.

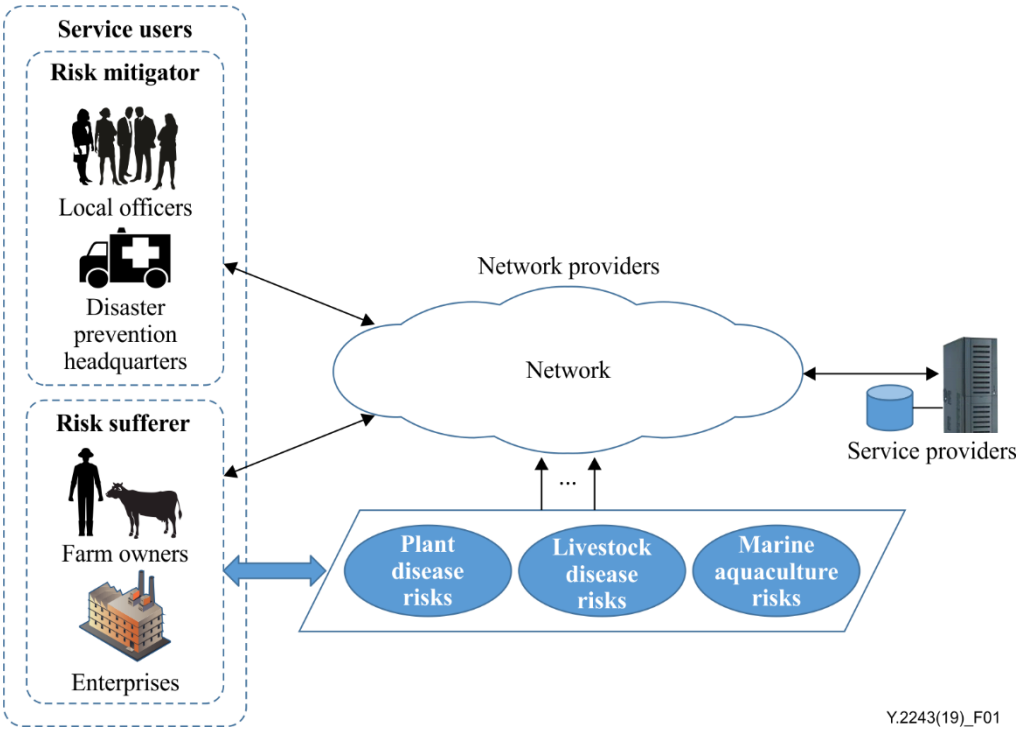

Figure 1 – Conceptual diagram of risk mitigation service

7 Risk mitigation service model

According to the concepts outlined in clause 6, there are two types of service users for the risk mitigation service, risk mitigators and risk sufferers. Risk mitigators such as disaster prevention headquarters or local officers require a reliable communication capability with risk sufferers and their peers. Risk sufferers such as farm owners or the chief executive officers (CEOs) of enterprises also demand ongoing feedback regarding the current status of the risks.

Considering these aspects, a reference architecture for a risk mitigation service model is shown in Figure 2. There are two service roles, specifically, service provider and service user. The service users' role includes both the roles of the risk mitigator and risk sufferer. The risk service provider's role includes both the risk monitoring and detection function (RMDF) and the risk mitigation action function (RMAF). The RMDF comprises a data acquisition functional entity and a risk detection functional entity. The data acquisition functional entity collects raw data from field sensors and other sources. The risk detection functional entity filters the collected raw data to determine if risk-related data have been received and if so, delivers it to the RMAF. The RMAF consists of the risk classification functional entity, the risk urgency and impact assessment functional entity,

the mitigation action decision functional entity, and the risk action indication functional entity. The risk classification functional entity classifies the type and level of risks from the received risk-related data. The risk urgency and impact assessment functional entity analyses the impact of the risks from the received risk type and urgency. The mitigation action decision functional entity decides the appropriate actions on how to mitigate the risk from the assessed result and the recommended mitigation action is delivered to service users by the risk action indication functional entity. The network infrastructure includes multiple communication network interfaces for risk mitigation service so as to achieve interconnection and interworking among different network providers. The network infrastructure mainly consists of the Internet network and the mobile communication network. In this architecture, plant disease risks (e.g., downy mildew, phytophthora and insect infestations), livestock risks (e.g., foot and mouth disease (FMD), highly-pathogenic avian influenza (HPAI), rinderpest disease, bovine diseases, anthrax disease, and fowl typhoid), and marine aquaculture risks (e.g., red tide and shellfish toxin) could be detected and mitigated.

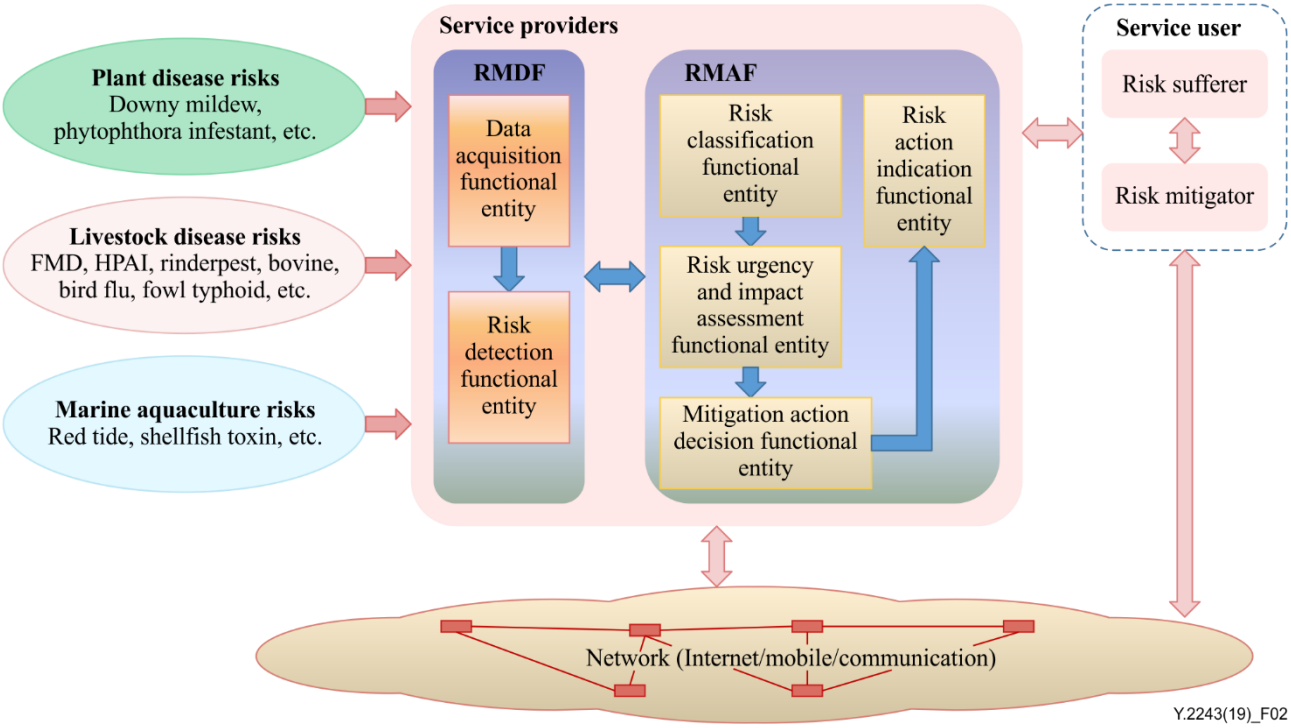

Figure 2 – Reference architecture for a risk mitigation service model

7.1 Risk monitoring and detection function

The risk monitoring and detection function (RMDF) consists of the data acquisition functional entity, which collects the raw data, and the risk detection functional entity which processes the raw data.

7.1.1 Data acquisition functional entity

Raw data from sensors (e.g., temperature, humidity, pH, image) is collected and is either immediately passed on to the risk detection functional entity for processing or temporarily stored in the data acquisition functional entity. If the data is temporarily stored, the stored data will not be processed within the data acquisition functional entity but will be passed on to the risk detection functional entity at a subsequent point in time.

7.1.2 Risk detection functional entity

The risk detection functional entity receives the raw data from the data acquisition functional entity and processes it. The processing function will exclude normal status data and identify data that is

abnormal (i.e., data that is beyond predetermined normal ranges). The resultant abnormal data will be delivered to the risk itigation action function (RMAF) entity.

7.2 Risk mitigation action function

The RMAF includes the risk classification functional entity, the risk urgency and the impact assessment functional entity, the mitigation action decision functional entity, and the risk action indication functional entity.

7.2.1 Risk classification functional entity

The risk classification functional entity classifies the input risk event into one of the risk types such as AI-suspected, FMD-suspected, etc.

7.2.2 Risk urgency and impact assessment functional entity

The risk urgency and impact assessment functional entity assesses the urgency according to the analysed result of the received risk type and the tendency of received data value. It also assesses the impact level using results from big data analysis.

7.2.3 Mitigation action decision functional entity

The mitigation action decision functional entity recommends mitigation actions after assessing the results from the risk urgency and impact assessment functional entity. It may recommend implementation of one or more mitigation actions such as isolation, vaccination, evacuation, etc.

7.2.4 Risk action indication functional entity

The risk action indication functional entity indicates and recommends to the service users the mitigation action that should be taken.

8 Service requirements for risk mitigation

Risk mitigation service should be effective to reduce risks in relation to rescue, evacuation, safety confirmation and life sustainability. The risk types and associated levels of risk possibilities could be considered. Therefore, risk types need to be identified, and for each risk type it may be required to distinguish several levels of risk possibilities. Service providers should provide risk message boards, risk notices, risk mitigation guidance, and safety confirmation and message broadcast capabilities for risk indication to users.

In order to support these aforementioned capabilities, requirements for the functions identified in clause 7 are provided in clauses 8.1 to 8.2.

8.1 Requirements for RMDF

RMDF includes functional entities for data acquisition and risk detection. Requirements for these functional entities are provided below.

8.1.1 Requirements for data acquisition functional entity

– Raw data from various sensors (e.g., temperature, humidity, pH, image) located at farms or aquafarms are required to be delivered to the service provider via any means on the network side;

– The recommended capabilities required to deliver sensor data to the service provider are presented in clause 9;

– A local storage capability is recommended for the storage of attained raw data to ensure that raw data is not lost before it is sent to the risk detection functional entity for processing.

8.1.2 Requirements for risk detection functional entity

– Data obtained from the data acquisition functional entity are recommended to be arranged to facilitate the extraction of abnormal status data (i.e., data beyond the predetermined normal range thresholds);

– For the data arrangements, normal range threshold values for each sensor are required and should be consistent with the characteristics of each sensor;

– It must be possible to set normal range threshold values in a flexible manner and these threshold values must also be sufficiently flexible so as to accommodate various types of sensors, locations of sensors, or outer situations;

– Data beyond the normal threshold values are required to be captured and delivered to the RMAF. Data within the normal threshold values are not to be delivered to the RMAF and may be stored for an unspecified period of time or purged.

8.2 Requirements for RMAF

RMAF includes functional entities for risk classification, risk urgency and impact assessment, mitigation action decision, and risk action indication. Requirements for these functional entities are described in clauses 8.2.1 to 8.2.4.

8.2.1 Requirements for risk classification functional entity

– The risk classification functional entity must be able to analyse the arranged data from the RMDF and classify it into one of three levels of risk possibilities:

  • level 1: symptoms;

  • level 2: suspicious;

  • level 3: confirmed.

– For the proper classification, the risk classification functional entity must be able to analyse the arranged data from the RMDF and classify it as one of the various risk types (e.g., avian influenza (AI)], foot and mouth disease (FMD));

– The risk classification functional entity could, in addition to classifying data as one of the various risk types, classify the level of risk (e.g., AI-level 1, FMD-level 2).

8.2.2 Requirements for risk urgency and impact assessment functional entity

– The risk urgency and impact assessment entity will analyse the data received from the risk classification entity and check it for risk urgency and impact assessment;

– Risk urgency is recommended to be decided by combining the latest trend of the corresponding risk situations (e.g., broadcasting news, expertise information) and the level of risk possibilities;

– Impact assessment for each risk type is recommended to be based on up-to-date data analysis methods such as big data analysis.

8.2.3 Requirements for mitigation action decision functional entity

– Risk mitigation actions need to be predefined to cope with unexpected risk events. One or a combination of predefined mitigation actions such as isolation, vaccination, evacuation, etc. may be recommended in response to risk urgency and impact assessments;

– An example of risk mitigation action is given in Appendix II.

8.2.4 Requirements for risk action indication functional entity

– The recommended mitigation action shall be indicated to service users via any means on the network side;

– The recommended capabilities required to indicate the recommended mitigation action to the service provider are presented.

9 Network capabilities

The high-level network capabilities for the support of risk mitigation service are as follows:

– Connecting to anything capabilities: Theses capabilities refer to the support of the different ubiquitous networking communication types (person-to-person communication, person-to-object communication and object-to-object communication) and include the support of tag-based devices (e.g., radio frequency identification(RFID)) and sensor devices. Identification, naming and addressing capabilities are essential for supporting "connecting to anything".

– Open web-based service environment capabilities: Emerging ubiquitous services and applications will be provided based upon an open web-based service environment, as well as on legacy telecommunication and broadcasting services. In particular, application programming interfaces (APIs) and web with dynamics and interactivities will be supported. Such a web-based service environment will allow not only the creation of retail community-type services, but also the building of an open service platform environment which third-party application developers can access to launch their own applications. Using interactive, collaborative and customizable features, the web can provide rich user experiences and new business opportunities for the provision of ubiquitous networking services and applications.

– Context-awareness and seamlessness capabilities: Context-aware means the ability to detect changes in the status of objects. Intelligence systems associated with this capability can help to provide the best service, which meets the situation using user and environmental status recognition. Seamlessness is a key capability for "5 Any" (anytime, anywhere, any-service, any-network and any-object).

– Multi-networking capabilities: A transport stratum needs multi-networking capabilities in order to simultaneously support unicast/multicast, multi-homing and multi-path. Because of high traffic volume and the number of receivers, ubiquitous networking requires multicast transport capability for resource efficiency. Multi-homing enables the device to be always best connected using multiple network interfaces including different fixed/mobile access technologies. These capabilities can improve network reliability and guarantee continuous connectivity with desirable quality of service (QoS) through redundancy and fault tolerance.

– End-to-end connectivity over interconnected networks: For risk mitigation, it is critical to develop a solution to provide end-to-end connectivity between relevant users or terminals over interconnected heterogeneous networks such as next generation networks (NGNs), other IP-based networks, broadcasting networks, mobile/wireless networks and public switched telephone network/integrated services digital networks (PSTN/ISDNs).

– Networking capabilities: Provide relevant control functions of network connectivity and transport resource control functions, mobility management or authentication, authorization and accounting (AAA) [b-ITU-T Y-Sup. 3].

– The device capabilities include, but are not limited to: Direct interaction with the communication network: Devices are able to gather and upload information directly (i.e., without using gateway capabilities) to the communication network and can directly receive information (e.g., commands) from the communication network [ITU-T Y.4000].

– IoT service providers offer products and services to end users, with wide area embedded connectivity. To ensure quality and reliability of services, they also need to ensure quality and reliability of embedded network connectivity of each IoT device. With tens or hundreds of thousands of deployed devices, it is difficult to monitor and manage network connectivity

manually by enterprise customers and IoT service providers through traditional customer care services provided by network operators.

– The device is required to have enough precision to sense IoT data from monitored things in order to measure and record the characteristics of the monitored things.
– The device is recommended to mark the sensed IoT data with labels to indicate the types (related to the monitored things' characteristics) of the sensed IoT data, so that other IoT components can understand the types of the sensed IoT data.
– Big data, where a large amount of data will be transferred from those sensors and cameras to the IoT platform. All data will experience the data collection, data transfer, data pre-processing, data storage and data analysis procedures.
– During the data collection procedure, the data collection schedulers in the IoT platform will arrange the collection period and collection sequence to balance the network and the IoT platform load. The collected data from the city environment sensors will be partially annotated with time stamp and semantic information according to the capability of sensors.

10 Service scenarios

Risk mitigation services could be provided in various ways. Appendix I provides example detailed information flows associated with the following service scenarios:

– Prior notification of risks;
– Risk mitigation action notification;
– Risk event report.

11 Security consideration

This Recommendation is recognized as an enhancement of IP-based networks. Thus, it is assumed that security considerations in general are based on the security of IP-based networks and thus it is required to follow the security considerations identified by clauses 7 and 8 of [ITU-T Y.2701]. Additional information can be found in [b-ITU-T Y-Sup.19].

While implementing requirements related to risk mitigation service networking, security best practices should be adopted such as authentication, authorization and access control.

In addition, to achieve the necessary interconnection the network infrastructure includes multiple communication network interfaces necessary for risk mitigation service. The network infrastructure should be protected in order to avoid information leaking or destruction.

Operations related to network resources should have multiple levels of reliability in order to avoid incorrect operation of network resources and the degradation of network performance.

Appendix I

Example of detailed information flows for service scenarios

(This appendix does not form an integral part of this Recommendation.)

This appendix provides example information flows for the following service scenarios:

– Prior notification of risks;

– Risk mitigation action notification;

– Risk event report.

I.1 Service scenario for prior notification of risks

Prior notification of risks might be the most appropriate service to use to prevent the spread of risk effects.

The information flow for this service is shown in the Figure I.1.

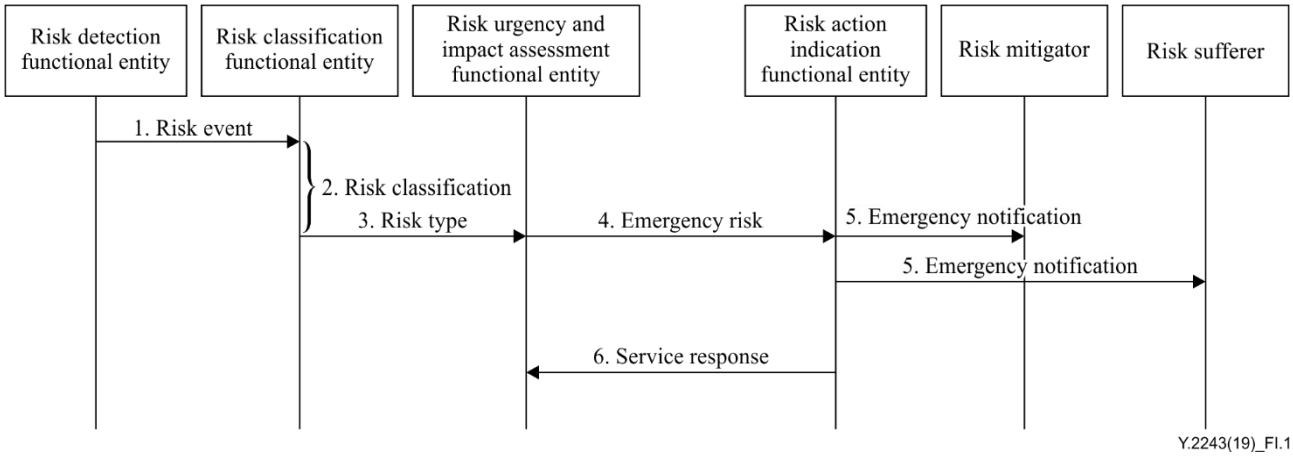

Figure I.1 – Information flow for the Prior Notification of Risks Service

Assumptions:

1. The risk sufferer and risk mitigator are subscribed to a risk mitigation service provider and will be charged on a usage basis by each service provider.
2. Digital rights management (DRM) processing for license transaction in service providers is hidden.
3. The flows shown here are at high level and not meant to show the actual protocol procedures.

Flow descriptions:

1. Risk detection functional entity detects a risk event and sends the detected risk event to the risk classification functional entity.
2. Risk classification functional entity classifies the risk type of the received risk event.
3. Risk classification functional entity sends risk type which includes the classified result to the risk urgency and impact assessment functional entity.
4. Risk urgency and impact assessment functional entity sends emergency risk to the risk action indication functional entity if the received risk type is urgent.
5. If emergency risk was received, risk action indication functional entity sends emergency notification to risk mitigator and risk sufferer.

6. If emergency notification was sent from risk action indication functional entity, risk action indication functional entity sends service response to risk impact assessment functional entity.

I.2 Service scenario for risk mitigation action notification

The risk mitigator requires risk mitigation recommendations provided by the risk mitigation action notification service to mitigate the impact of risks. The information flow for this service is shown in the Figure I.2.

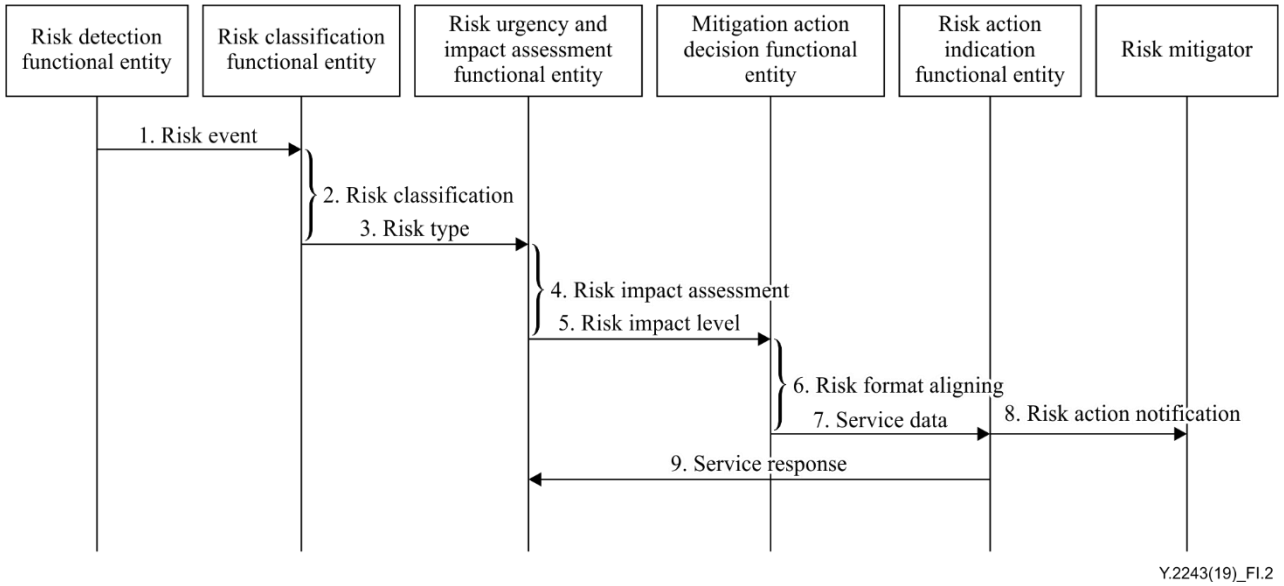

Figure I.2 – Information flow for the risk mitigation action notification

Assumptions:

1. The risk sufferer and risk mitigator are subscribed to a risk mitigation service provider and will be charged on a usage basis by each service provider.
2. DRM processing for license transaction by service providers is hidden.
3. The flows shown here are at a high level and not meant to show the actual protocol procedures.

Flow descriptions:

1. Risk detection functional entity detect a risk events and sends the detected risk event to risk classification functional entity.
2. Risk classification functional entity classifies the risk type of the received risk event.
3. Risk classification functional entity sends risk type which includes the classified result to risk urgency and impact assessment functional entity.
4. Risk urgency and impact assessment functional entity analyses the impact of risk from the received risk type.
5. Risk urgency and impact assessment functional entity sends risk impact level which includes the analysed result to risk action decision functional entity.
6. Risk action decision functional entity decides mitigation action for the current risk.
7. Risk action decision functional entity sends service data which includes the recommended mitigation action to the risk action indication functional entity.
8. Risk action indication functional entity sends risk action notification to risk mitigator.

9. Risk action indication functional entity sends service response to risk impact assessment functional entity.

I.3 Service scenario for risk event report

A risk suffer may issue a risk event report to the risk classification functional entity to initiate a process that will facilitate an early detection of a risk event. The information flow for this service is shown in the Figure I.3.

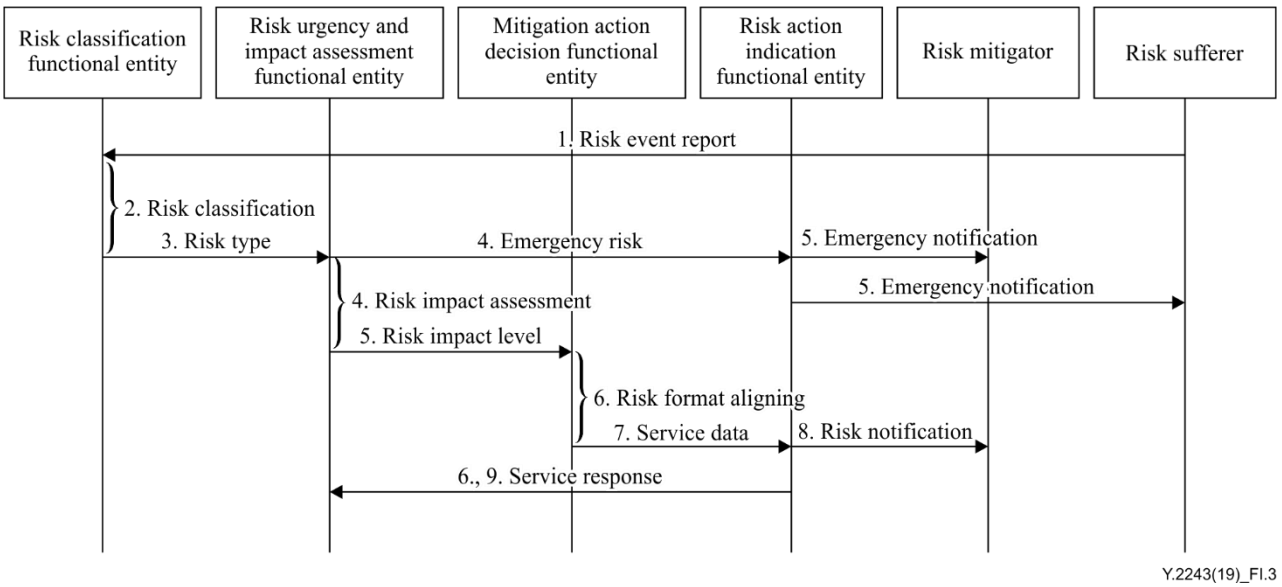

Figure I.3 – Information flow for the risk event report

Assumptions:

1. The risk sufferer and risk Mitigator are subscribed to a risk mitigation service provider and will be charged on a usage basis by each service provider.
2. DRM processing for license transaction by service providers is hidden.
3. The flows shown here are at high level and not meant to show the actual protocol procedures.

Flow descriptions:

1. Risk sufferer detects risk events and sends risk event report to risk classification functional entity.
2. Risk classification functional entity classifies the risk type of the received risk event.
3. Risk classification functional entity sends risk type which includes the classified result to risk urgency and impact assessment functional entity.
4. Risk urgency and impact assessment functional entity sends emergency risk to risk action indication functional entity if the received risk type is urgent. Otherwise, it analyses the impact of risk from the received risk type.
5. If emergency risk was received, risk action indication functional entity sends emergency notification to risk sufferer and risk mitigator. Otherwise, risk urgency and impact assessment functional entity sends risk impact level which includes the analysed result to risk action decision functional entity.
6. If emergency notification was sent from risk action indication functional entity, risk action indication functional entity sends service response to risk urgency and impact assessment functional entity. Otherwise, risk action decision functional entity aligns service format for the risk notification to risk mitigator.

7. Risk action decision functional entity sends service data which were aligned according to the risk impact level to risk action indication functional entity.
8. Risk action indication functional entity sends risk notification to risk mitigator.
9. Risk action indication functional entity sends service response to risk urgency and impact assessment functional entity.

Appendix II

An example of risk mitigation action

(This appendix does not form an integral part of this Recommendation.)

Livestock diseases can severely harm animal health as well as human health, and may also have adverse economic impacts through their effects on producer incomes, markets, trade, and consumers.

Foot and mouth disease is considered to be the most economically devastating livestock disease in the world, and represents a worst-case scenario for livestock diseases because of the variety of spaces involved, rapid spread, and difficulty in controlling outbreaks.

Immediate notification is necessary because of its rapid and substantial impact on the international trade of animals and animal products.

Figure II.1 shows the risk mitigation function and Figure II.2 shows the risk classification function flow.

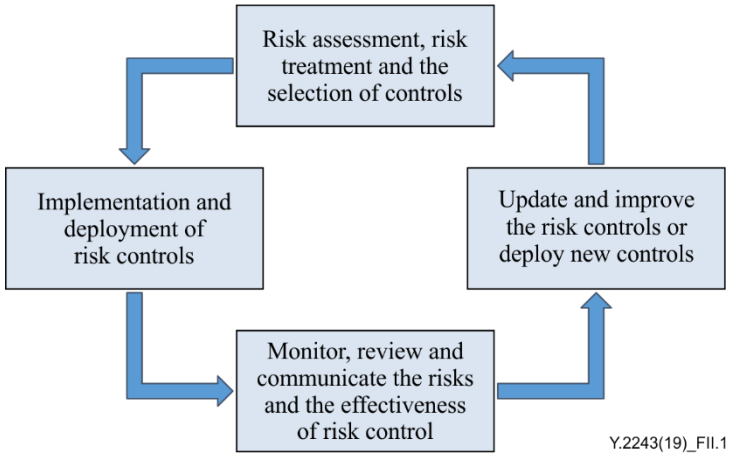

Figure II.1 – Risk mitigation action function

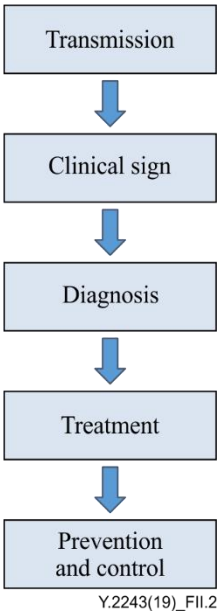

Figure II.2 – Risk classification function flow

– Transmission

Foot and mouth disease virus is spread via contact and fomites (including contaminated inanimate objects and people moving between infected and uninfected animals). Inhalation and ingestion are routes of infection. Outbreaks may originate in swine herds fed raw garbage containing infected meat and are usually propagated by the transport of infected animals to markets or new locations. Introduction of an infected animal to a susceptible herd or insemination of a susceptible cow with infected semen may also initiate outbreaks. Airborne transmission has been reported, and cattle may be more susceptible to this route of infection. Dispersion of airborne viruses is influenced by weather conditions. The incubation period is usually two to five days but may be longer in sheep and goats. The disease is highly contagious and infectious. Cattle may shed the virus for four or more days before clinical signs appear.

– Clinical Signs

Affected animals develop vesicular lesions of the tongue, dental pad, gums, cheek, hard and soft palates, lips, nostrils, muzzle, interdigital space (between the hooves), and on the coronary band. In affected ruminants, vesicular lesions may be observed on the udder and teats. Lesions may be observed on the snout of affected swine. Excessive salivation is often the first observed clinical sign. The saliva is sticky, foamy, and stringy in consistency. A transient, high fever may be observed. Over a period of seven to 14 days, the vesicles break, erode, ulcerate, then heal. Abortions may also occur. Marked loss of condition is often observed because of reduced feed consumption secondary to oral pain. Milk production may be markedly decreased. The malignant form may produce myocardial degeneration and death in calves. Lameness and reluctance to move may be observed. A carrier state is possible in recovered ruminants but plays an unknown role in transmission of the virus. Clinical signs may be subtler in sheep and goats, resulting in delayed recognition that may increase the risk of spread of the outbreak. Lameness is often the first observed clinical sign of FMD, and the vesicles may be more difficult to recognize. Up to 25% of affected sheep may not develop clinically apparent vesicles and others may only develop a single lesion or develop vesicles that are visible for less than three days.

– Diagnosis

A tentative diagnosis of FMD is made based on clinical signs, but distinguishing FMD from vesicular stomatitis (VS) is not possible based on clinical signs. Diagnosis can be confirmed by detection of the virus in samples from affected tissues or esophageal-pharyngeal fluid. Laboratory methods to confirm FMD include enzyme-linked immunosorbent assay (ELISA), complement fixation, virus isolation, virus neutralization, mouse inoculation, cell culture, and polymerase chain reaction (PCR).

– Treatment

Foot and mouth disease is a reportable disease. State or federal animal health officials should be immediately notified when vesicular disease is observed. There is no treatment for FMD. Strict quarantine and slaughter methods are employed to control outbreaks. Vaccination may also be used to control outbreaks. Infected, recovered, and FMD-susceptible contact animals are slaughtered, and carcasses, bedding, and all animal products in the affected area are destroyed. Vaccinated animals may be killed and destroyed, or slaughtered with salvage of the meat under supervised procedures. Recovery from uncomplicated FMD is relatively rapid, but the virus can persist in the pharyngeal tissues. Permanent reduction in productivity has been observed following recovery from acute FMD infection.

– Prevention and control

A cell culture-origin vaccine is available but must be matched to both the type and subtype of virus involved in the infected region. Vaccinated animals develop protection against clinical signs of FMD within seven to eight days. In the face of an outbreak, the use of interferon is being researched to bridge the gap in protection before vaccination is effective. Vaccination can be instituted to create a barrier of protected animals between infected and susceptible animals. Vaccination complicates

diagnosis of FMD (although tests are being developed that differentiate vaccinated from infected animals) and may increase the risk of subclinical infection and subsequent outbreak, but the level of risk is unknown. Rarely, vaccination may result in an outbreak if the vaccines are not properly manufactured. Prohibition of importation of live ruminants and swine and their products from FMD-affected countries is paramount to preventing outbreaks. Travelers returning from FMD-affected countries are advised to avoid contact with livestock, zoo animals, and wildlife for a minimum of five days.

Bibliography

[b-ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities.*

[b-ITU-T Y.4450] Recommendation ITU-T Y.4450/Y.2238(2015), *Overview of Smart Farming based on networks.*

[b-ITU-T Y-Sup.3] ITU-T Y-series Recommendations Sup.3 (2008), *ITU-T Y.2000-series – Supplement on service scenarios for convergence services in a multiple network and application service provider environment.*

[b-ITU-T Y-Sup.19] ITU-T Y-series Recommendations Sup.19 (2012), *ITU-T Y.2200-series – Supplement on the risk analysis service in next generation network*s.

[b-ITU-T FG-DR&NRR] ITU-T FG-DR&NRR (2014), ITU-T Focus Group on Disaster Relief Systems, *Network Resilience and Recovery, Requirements for Disaster Relief System.* <https://www.itu.int/en/ITU-T/focusgroups/drnrr/>

[b-OECD] OECD Publishing, Food, Agriculture and Fisheries Paper No. 91 (2015), *Risk Management of Outbreaks of Livestock Diseases*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019