International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2222

(04/2013)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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

Sensor control networks and related applications in a next generation network environment

Recommendation ITU-T Y.2222

ITU-T

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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

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

Recommendation ITU-T Y.2222

Sensor control networks and related applications in a next generation network environment

Summary

Recommendation ITU-T Y.2222 provides an introduction to sensor control networks (SCNs) and related applications in a next generation network (NGN) environment. More specifically, it provides an overview of SCNs, configurations for SCN applications and service requirements of SCN applications for support in a NGN environment.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2222	2013-04-13	13

Keywords

Actuator, configurations for SCN applications, decision-making process, emergency management, gate, mote, NGN, SCN, SCN applications, SCN controller, sensor control networks, sensor networks, verification application.

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

Page

Recommendation ITU-T Y.2222

Sensor control networks and related applications in a next generation network environment

1 Scope

This Recommendation provides an introduction to sensor control networks (SCNs) and related applications in a next generation network (NGN) environment. More specifically, this Recommendation provides:

– definitions of SCN and SCN related terms;

– overview of SCNs;

– description of possible configurations for SCN applications and the decision-making process for these configurations;

– service requirements of SCN applications for support in NGN environment.

Moreover, two important use cases of SCNs are described in the appendices: SCNs for verification and SCNs for emergency management.

Business models and charging issues are outside of the scope of this Recommendation.

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 Y.2020] Recommendation ITU-T Y.2020 (2011), *Open service environment functional architecture for next generation networks*.

[ITU-T Y.2061] Recommendation ITU-T Y.2061 (2012), *Requirements for the support of machine-oriented communication applications in the next generation network environment*.

[ITU-T Y.2234] Recommendation ITU-T Y.2234 (2008), *Open service environment capabilities for NGN*.

[ITU-T Y.2240] Recommendation ITU-T Y.2240 (2011), *Requirements and capabilities for next generation network service integration and delivery environment*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 actuator [ITU-T Y.2061]: A device performing physical actions caused by an input signal.

NOTE 1 – As examples, an actuator might act on the flow of a gas or liquid, on electricity distribution, or through a mechanical operation. Dimmers and relays are examples of actuators. The decision to activate the actuator may come from an MOC application, a human or MOC devices and gateways.

NOTE 2 (added by ITU-T Y.2222) – There are three types of actuators: information actuators, which are intended to provide visual, audio, sensory interaction with the human user; gateway actuators, which are intended to forward control commands given by SCN to other networks; machine actuators, which are electromechanical devices intended for physical interaction with the external environment.

3.1.2 application [b-ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.3 context awareness [b-ITU-T Y.2201]: A capability to determine or influence a next action in telecommunication or process by referring to the status of relevant entities, which form a coherent environment as a context.

3.1.4 machine oriented communication (MOC) [ITU-T Y.2061]: A form of data communication between two or more entities in which at least one entity does not necessarily require human interaction or intervention in the communication process.

3.1.5 next generation network (NGN) [b-ITU-T Y.2001]: A packet-based network able to provide telecommunication1 services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.1.6 NGN service integration and delivery environment (NGN-SIDE) [ITU-T Y.2240]: An open environment in NGN integrating resources from different domains and delivering integrated services to applications over NGN.

NOTE – These domains include, but are not limited to, telecommunication domain (e.g., fixed and mobile networks), Internet domain, broadcasting domain and content provider domain.

3.1.7 nomadism [b-ITU-T Q.1706]: The ability of the user to change their network access point on moving. When changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no service continuity or hand-over used. It is assumed that normal usage pattern is that users shut down their service session before attaching to a different access point.

3.1.8 open service environment capabilities [ITU-T Y.2234]: Capabilities provided by open service environment to enable enhanced and flexible service creation and provisioning based on the use of standards interfaces.

3.1.9 seamless handover [b-ITU-T Q.1706]: It is a special case of mobility with service continuity since it preserves the ability to provide services without any impact on their service level agreements to a moving object during and after movement.

3.1.10 sensed data [b-ITU-T F.744]: Data sensed by a sensor that is attached to a specific sensor node.

3.1.11 sensor [b-ITU-T Y.2221]: An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

3.1.12 service [b-ITU-T Y.101]: A structure set of capabilities intended to support applications.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 aggregate value: A value calculated by combining the sensed data of several spatially distributed motes, reference values and other data and intended to represent the environmental conditions of a given geographical area.

3.2.2 central communication channel: A communication channel or a set of communication channels for transmitting data between SCN controllers and actuators without utilizing motes.

3.2.3 gate: Intermediate device that is used to provide a communication channel between an actuator and one or several nearby motes.

3.2.4 mote: A miniature computing device equipped with sensors and signal transceivers operating in a given radio band, and used for transmitting sensed data.

NOTE 1 – It is a kind of sensor node and it is characterized by a mandatory minimal level of computing resources.

NOTE 2 – Depending on application, a mote has one or more of the following capabilities: data manipulation, intelligent commutation and connectivity with actuators, retrieving data on the read-outs of near-site sensors.

3.2.5 mote group: A set of motes connected to each other without making usage of external networks.

3.2.6 non-SCN-enabled actuator: An actuator that is not able to communicate with motes directly, and uses networks to communicate with motes.

NOTE – In this Recommendation, a non-SCN-enabled actuator uses NGN to communicate with motes.

3.2.7 reference value: A value calculated by combining the sensed data of one or several closely situated motes and intended to represent the environmental conditions of some specific location.

3.2.8 sensor control network (SCN): A sensor network consisting of motes which is intended for controlling one or more actuators.

3.2.9 SCN application: An application that uses SCNs for controlling actuators.

3.2.10 SCN controller: A hardware/software system designed to collect and process data from motes and to transmit to actuators the necessary information for their control.

3.2.11 SCN-enabled actuator: An actuator that is able to communicate with motes directly.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	Third Generation
GPRS	General Packet Radio Service
MOC	Machine Oriented Communication
NGN	Next Generation Network
NGN-SIDE	NGN Service Integration and Delivery Environment
OSE	Open Service Environment
PDA	Personal Digital Assistant
QoS	Quality of Service
SCN	Sensor Control Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of SCNs

Sensor networks are becoming more and more utilized and are under active development for different applications. These networks are frequently deployed with some control: sensor control networks (SCNs) are used to allow control by applications of the "actuators" which can be found in many sensor network deployments. The control is realized on a real-time basis and depending on environmental parameters.

In SCNs, for the measurement of environmental parameters, motes are deployed and they can be seen as an evolutive version of sensors. In comparison with a sensor in a sensor network, a mote, besides physical conditions monitoring, can also have capabilities of data manipulation, intelligent commutation and connectivity to actuators. Motes are connected to NGN, by the use of a gateway or directly, and may also act as an access network to the SCN applications for actuators.

NOTE 1 – The details of sensors and actuators are outside of the scope of this Recommendation.

The goal of any application using SCNs ("SCN application") is to run a decision-making process and finally provide all involved actuators with relevant control commands. This process includes various activities of data acquisition, data transmission and data manipulation. A range of configurations (see details in clause 7) may be employed for SCN application's decision-making process depending on the capabilities of actuators and motes. For example, an actuator may only use commands provided by the SCN application to itself, or may customize them in order to meet its own capabilities and user requirements or may perform decision making completely by itself based on the data provided by the SCN application.

Application field examples of SCNs include:

– everyday life: navigation, excursions, sports;
– medicine: body control, e-health;
– enterprise: logistics, stock management;
– industrial field: fabrication automation, production process control;
– military field: combat assistance, remote piloting;
– emergency and disaster management: early warning, evacuation, emergency orchestration of civilians and rescuers, automatic danger elimination.

The decisions of SCN applications may be targeted for both human users and control of machines (e.g., gears, vehicles, robots). The latter case also includes machine oriented communication (MOC) devices [ITU-T Y.2061] implying communications between two or more entities in which at least one entity does not necessarily require human interaction or intervention in the process of communication.

Since decisions of SCN applications directly involve the operations of actuators, tight integration between SCN infrastructure and actuators' capabilities must be achieved. Although the following matter is outside of the scope of this Recommendation, it is expected that standardization of the interfaces between SCNs and actuators will be critical.

In addition, although the following matter is also outside of the scope of this Recommendation and for further study, it is anticipated that some enhancements to the NGN capabilities

[b-ITU-T Y.2201] will be required in order to support the service requirements of SCN applications identified in this Recommendation.

Figure 6-1 shows an overview of SCNs, including SCN applications and the supporting role of NGN.

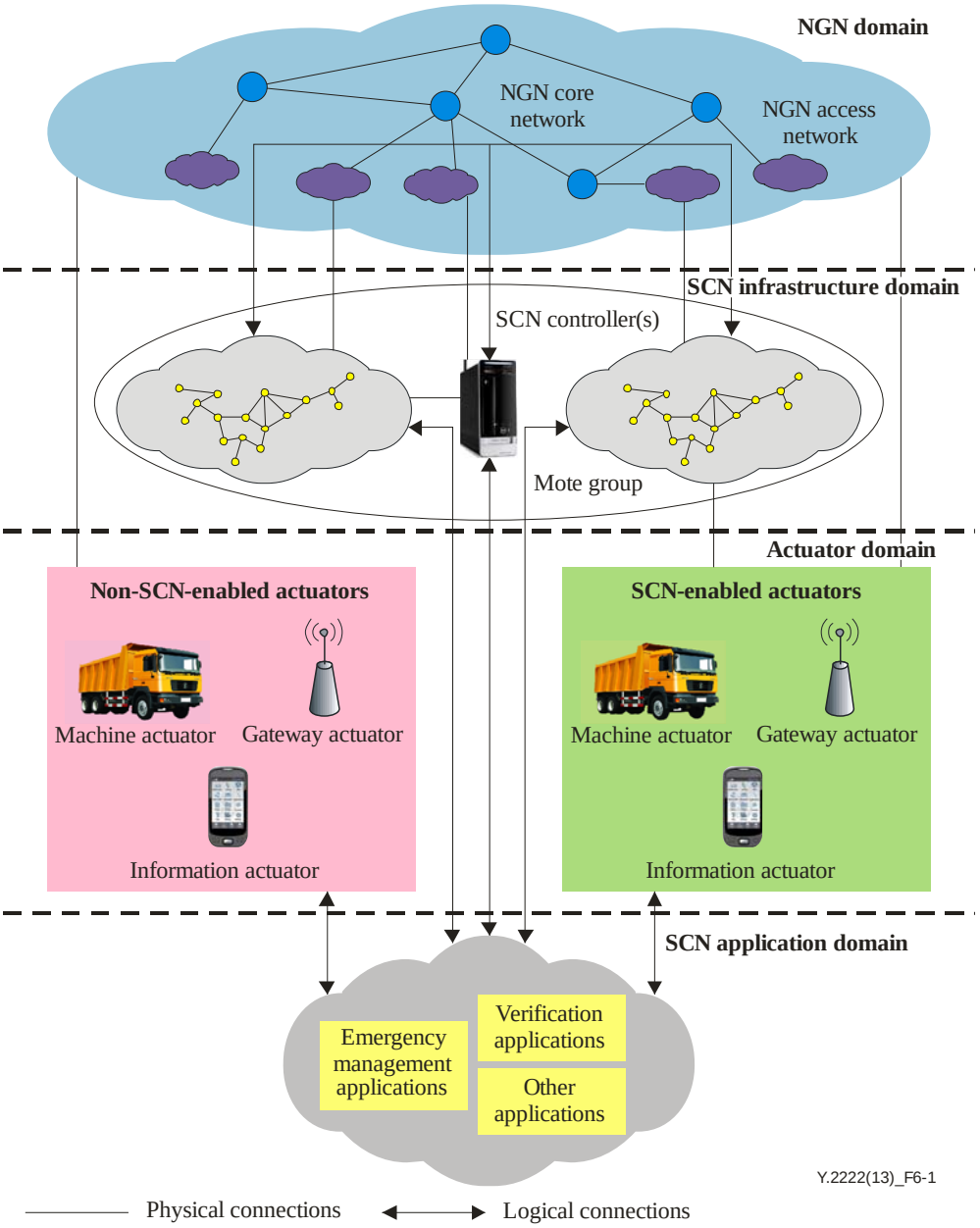

Figure 6-1 – Overview of SCNs

Figure 6-1 depicts four domains:

1) NGN domain: the connectivity via NGN fulfils two objectives. First, NGN provides access to SCN applications for both non-SCN-enabled and SCN-enabled actuators when direct communication of actuators with motes is not possible or desirable (e.g., when an actuator is a mobile phone and its owner does not want his/her location to be exposed due to privacy reasons). Second, NGN is used to unite spatially distributed mote groups and the SCN controllers into a single network.

   NOTE 2 – NGN is expected to provide the same capabilities (e.g., load balancing, fault tolerance) as a single mote group directly connected to the SCN controllers.

2) SCN infrastructure domain: the SCN infrastructure includes one or several SCN controllers and mote groups. They may be spatially distributed: in that case, NGN is used to unite them into a single network. Authorized personnel may use the SCN controllers for SCN monitoring and administration. Motes can allow direct access to SCN applications of SCN-enabled actuators, while direct access via motes to SCN applications of non-SCN enabled actuators is not possible. The SCN controllers are connected to NGN directly.

3) Actuator domain: the actuators can be of three different types: machine actuators (e.g., car, water sprinkler, door lock), information actuators (e.g., screen, loudspeaker, mobile phone, PDA, notebook) and gateway actuators (e.g., computer with telephone private branch exchange software).

NOTE 3 – The term "SCN objects" is used in the following clauses to cover motes and SCN controllers (which constitute the SCN infrastructure), as well as actuators.

4) SCN application domain: consists of SCN applications, e.g., verification applications (see Appendix I), emergency management applications (see Appendix II) and others.

NOTE 4 – Different parts of SCN applications can reside in different SCN objects according to the specific application requirements.

7 Configurations for SCN applications

7.1 Basic operations for SCN applications

Four types of operations are identified for SCN applications:

1) Fetching of sensed data (shown as Sensed data in Figures 7-1 to 7-5 and I.1).

2) Calculation of reference values by combining (e.g., averaging) the sensed data of one or several closely situated motes (shown as Reference values in Figures 7-1 to 7-5 and I.1). The aim of this process can be for example:
   - comparison of sensed data readings with thresholds for the purpose of filtering sensed data and taking them into account during calculations of aggregate values and/or decision making,
   - auxiliary pre-calculations for the purpose of quicker calculation of aggregate values and/or decision making,
   - synchronous analysis of multiple sensed data readings.

3) Calculation of aggregate values by combining (e.g., averaging) the sensed data of several spatially distributed motes, reference values and other data (shown as Aggregate values in Figures 7-1 to 7-5 and I.1).

4) Decision making (shown as Decision making in Figures 7-1 to 7-5 and Figure I.1). During this process a specific control command for the actuator is formed. It can use fetched aggregate values.

In SCNs, data can be transmitted via the SCN infrastructure (i.e., using motes and SCN controllers as intermediate nodes) and via the central communication channel (e.g., using GPRS/3G, Wi-Fi and WiMAX technologies).

The above-described operations and the associated data transmissions can be represented in a flow chart. The rows of such a chart represent the above listed operations and the columns represent elements participating in the decision-making process. Data transmission flows are depicted as horizontal arrows whose endings correspond to the sending and receiving elements of the actual transmission stage, while data computational flows are depicted as vertical arrows corresponding to the above described operations. Figure 7-1 shows an example of such a flow chart.

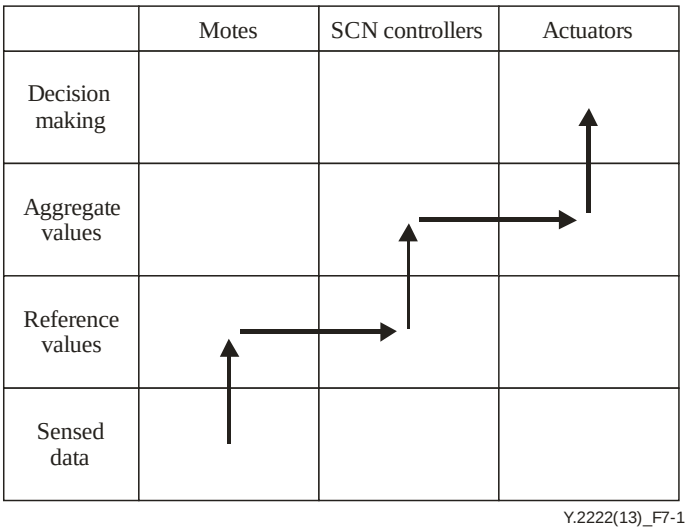

Figure 7-1 – Flow chart example of basic operations for a SCN application

7.2 Decentralized configuration for SCN applications

7.2.1 Introduction to decentralized configuration for SCN applications

The decentralized configuration is the most universal configuration for SCN applications in terms of flexibility, expansibility and reliability. It is so called because it makes minimal demand to the central communication channel and the SCN controllers. This provides the possibility of ubiquitous usage of such configurations in a wide range of applications, including emergency management applications (due to the high risk of failure related to centralized entities in case of disaster or emergency).

7.2.2 Role distribution in decentralized configuration for SCN applications

- **SCN controller:**

– It receives from the actuators via the central communication channel requests about aggregate values, which are necessary for making decision but cannot be calculated by the actuators themselves.

– It requests transmission of sensed data and reference values from the appropriate motes via the SCN infrastructure and regularly calculates the necessary aggregate values.

– It transmits to each actuator via the central communication channel the aggregate values requested by that actuator.

– It interoperates with external systems (e.g., a different application server) and the authorized personnel administrating the SCN.

- **Actuator:**

– It requests the necessary sensed data and reference values from the motes via the SCN infrastructure.

– It requests from the SCN controllers via the central communication channel the aggregate values which are necessary for decision making but cannot be calculated by the actuator itself.

– It receives from the motes via the SCN infrastructure the requested sensed data and reference values and calculates the other necessary reference values and aggregate values.

– It receives from the SCN controllers via the central communication channel the requested aggregate values.

– It forms the appropriate control commands.

– It transmits to the SCN controllers information about its own status via the central communication channel.

• **Mote:**

– It receives requests from the SCN controllers and the actuators via the SCN infrastructure about sensed data or reference values.

– It transmits the requested data to the SCN controllers and the actuators via the SCN infrastructure.

7.2.3 Decision-making process

The decision-making process follows the following procedure:

1) The necessary sensed data, reference values and aggregate values are kept in the SCN controllers' memory and regularly updated.

2) Each actuator sends requests for sensed data and reference values to the motes, and then stores the received ones in memory. The data requests can be of different types, such as broadcast requests (all motes send data on demand to actuators via the SCN infrastructure), or threshold-exceeding requests (only motes whose sensed data exceed some thresholds send data), etc.

3) Some other reference values can be computed as needed by the actuators based on received sensed data and reference values.

4) Each actuator needs to have the up-to-date aggregate values necessary to make a decision. These aggregate values can be computed by the actuator itself or fetched from the SCN controllers.

5) Each actuator forms a control command depending on the aggregate values.

Two examples of flow charts for decentralized configuration are shown in Figures 7-2 and 7-3.

In the first example, actuators use aggregate values received from the SCN controllers (data flow 2) and aggregate values calculated using reference values received from motes (data flow 1).

In the second example, actuators use only aggregate values calculated using reference values received from motes (data flow 1). There is no influence of the SCN controllers on the decision-making process. The SCN controllers only calculate (data flow 2) and store in memory aggregate values for the purpose of interoperation with external systems and the authorized personnel administrating the SCN.

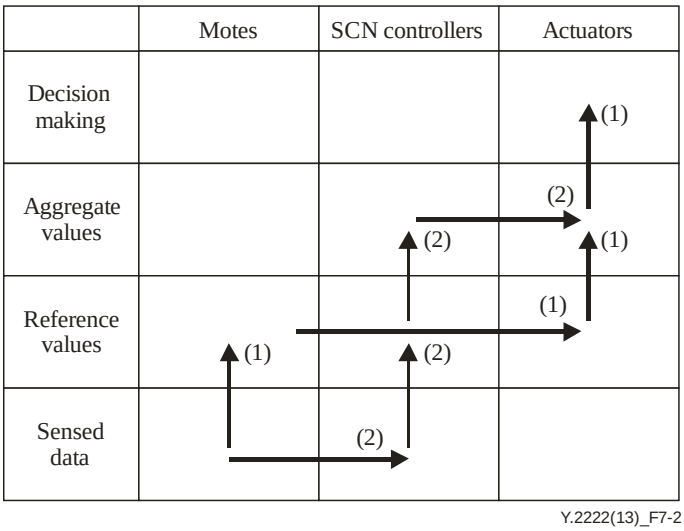

Figure 7-2 – A first example of a flow chart for decentralized configuration for SCN applications

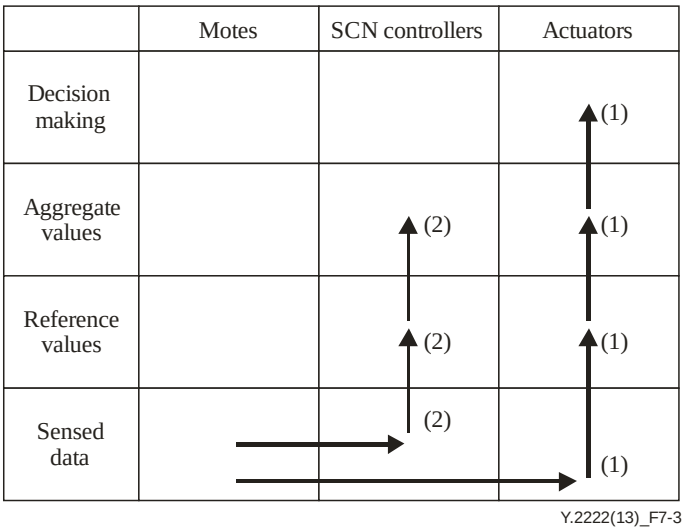

Figure 7-3 – A second example of a flow chart for decentralized configuration for SCN applications

7.3 Transitional configurations for SCN applications

Nowadays most mass mobile user terminals, such as mobile phones, PDAs and netbooks, have no technical possibility of direct data exchange with existing infrastructures of motes because of differences in transceiver types and transmission standards. Therefore, transitional configurations are needed to provide a possibility of using SCNs with mass mobile user terminals.

7.3.1 Centralized configuration for SCN applications

7.3.1.1 Introduction to centralized configuration for SCN applications

This configuration is so called because the data for every decision made by SCN are transferred through the SCN controllers and are delivered to the actuators via a central communication channel. It should be employed when actuators can only communicate via the central communication channel and/or it is not desirable to change the existing infrastructure of motes and actuators to enable SCN applications.

7.3.1.2 Role distribution in a centralized configuration for SCN applications

- **SCN controller:**

– It receives from the actuators requests via the central communication channel about aggregate values.

– It requests transmission of sensed data and reference values from the appropriate motes via the SCN infrastructure and regularly calculates the necessary aggregate values.

– It transmits to each actuator via the central communication channel the aggregate values requested by that actuator.

– It interoperates with external systems (e.g., a different application server) and the authorized personnel administrating the SCN.

- **Actuator:**

– It requests from the SCN controllers via the central communication channel aggregate values, which are necessary for making a decision.

– It receives from the SCN controllers via the central communication channel the requested aggregate values.

– It forms the appropriate control commands.

– It transmits information about its own status to the SCN controllers via the central communication channel.

• **Mote:**

– It receives requests from the SCN controllers via the SCN infrastructure about sensed data or reference values.

– It transmits to the SCN controllers the requested data via the SCN infrastructure.

7.3.1.3 Decision-making process

The decision-making process follows the following procedure:

1) The necessary sensed data, reference values and aggregate values are kept in the SCN controllers' memory and regularly updated.

2) Each actuator needs to have the up-to-date aggregate values necessary to make a decision. These aggregate values are fetched from the SCN controllers.

3) Each actuator forms a control command depending on the aggregate values.

An example of a flow chart for centralized configuration is shown in Figure 7-4.

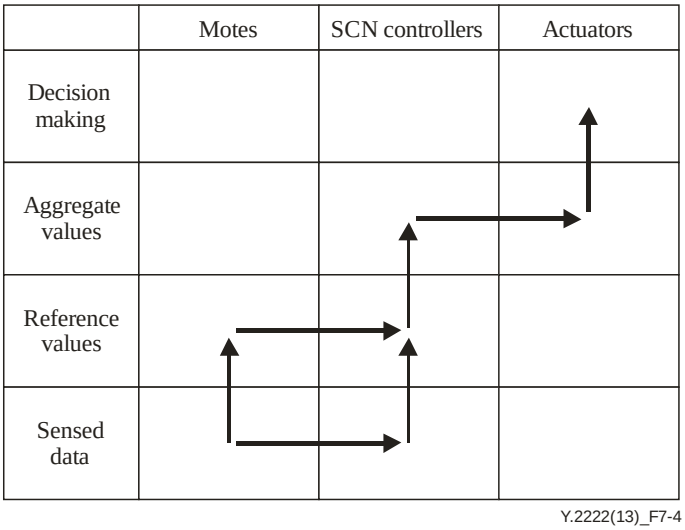

Figure 7-4 – Example of flow chart for centralized configuration for SCN applications

7.3.2 Ad-hoc configuration for SCN applications

7.3.2.1 Introduction to ad-hoc configuration for SCN applications

This configuration is so called because it utilizes ad-hoc networks (e.g., based on Bluetooth or Wi-Fi technologies) to deliver data to actuators. It should be employed when there is the possibility to expand the existing SCN infrastructure and the actuators have some ad-hoc wireless network capabilities. Some intermediate devices called gates are used to provide a communication channel between actuators and one or several nearby motes.

7.3.2.2 Role distribution in ad-hoc configuration for SCN applications

• **SCN controller:**

– It receives from the actuators via the central communication channel requests about aggregate values, which are necessary for making a decision but cannot be calculated by the actuators themselves.

– It requests transmission of sensed data and reference values from the appropriate motes and regularly calculates the necessary aggregate values.

– It transmits to each actuator via the central communication channel the aggregate values requested by that actuator.

– It interoperates with external systems (for example, a different application server) and the authorized personnel administrating the SCN.

• **Gate:**

– It receives requests from the actuators via the ad-hoc network about sensed data and reference values and forwards them to the motes via the SCN infrastructure.

– It transmits the requested data to the actuators via the ad-hoc network.

• **Actuator:**

– It requests the necessary sensed data and reference values from the gates via the ad-hoc network.

– It requests from the SCN controllers via the central communication channel aggregate values, which are necessary for a decision but cannot be calculated by the actuator itself.

– It receives from the gates via the ad-hoc network the requested sensed data and reference values and calculates the other necessary reference values and aggregate values.

– It receives from the SCN controllers via the central communication channel the requested aggregate values.

– It forms the appropriate control commands.

– It transmits to the SCN controllers information about its own status via the central communication channel.

• **Mote:**

– It receives requests from the SCN controllers and the gates via the SCN infrastructure about sensed data or reference values.

– It transmits the requested data to the SCN controllers and the gates via the SCN infrastructure.

7.3.2.3 Decision-making process

The decision-making process follows the following procedure:

1) The necessary sensed data, reference values and aggregated values are kept in the SCN controllers' memory and regularly updated.

2) Each gate forwards sensed data and reference values from the motes to the actuators.

3) Each actuator sends requests for sensed data and reference values to the gates, and then stores the received ones in memory. The data requests can be of different types, such as broadcast request (the gates send data of all motes on demand to the actuator), threshold-exceeding request (gates send data only of the motes whose sensed data exceed some thresholds), etc.

4) Some other reference values can be regularly computed as needed by the actuators based on received sensed data and reference values.

5) Each actuator needs to have the up-to-date aggregate values necessary to make a decision. These aggregate values can be computed by the actuator itself or fetched from the SCN controllers.

6) Each actuator forms a control command depending on the aggregate values.

An example of flow chart for ad-hoc configuration is shown in Figure 7-5.

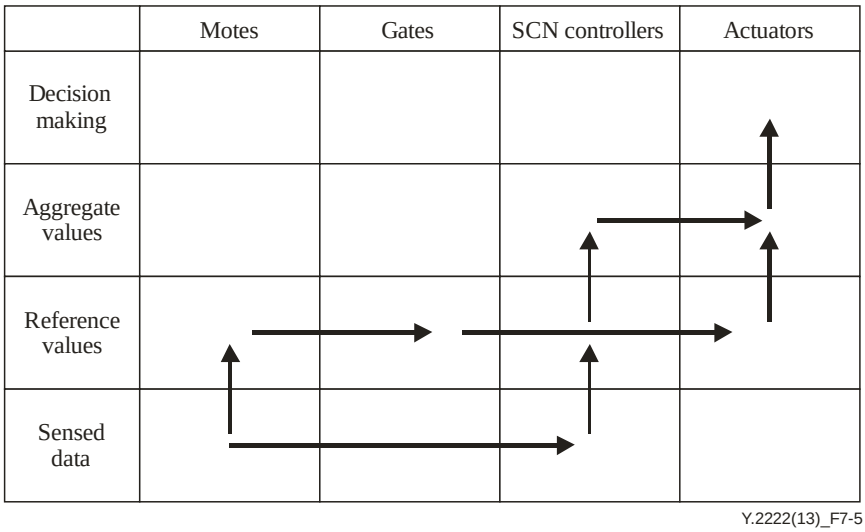

Figure 7-5 – Example of flow chart for ad-hoc configuration for SCN applications

8 Service requirements of SCN applications

The followings are high-level service requirements of SCN applications.

8.1 Connectivity

1) SCN applications are required to support three types of communications:
   - SCN controller-actuator communication: actuators communicate with the SCN controllers;
   - Infrastructure communication (including one-to-one, one-to-many, many-to-one and many-to-many): motes from different mote groups communicate with each other and with the SCN controllers;
   - SCN controller-NGN communication: NGN elements communicate with the SCN controllers.
2) SCN applications are recommended to support the following type of communications:
   - Mote-actuator communication (including one-to-one, one-to-many and optionally many-to-one and many-to-many): actuators communicate with motes.
3) SCN applications can optionally provide these types of communications:
   - Inter-actuator communication: actuators communicate with each other;
   - Actuator-NGN communication: NGN elements communicate with actuators;
   - Mote-NGN communication: NGN elements communicate with motes.

8.2 Mobility support

Actuators as well as motes can be classified as follows:

- Network-specific actuators and motes, designed to operate in specific SCN application fields (e.g., complex industrial mechanisms);
- Mission-specific actuators and motes, designed to be deployed after preliminary setup (e.g., mass-produced switches);
- Generic actuators and motes, designed to be instantly deployed and used in a wide range of SCN applications (e.g., PDAs).

SCN applications have the following general requirements concerning mobility:

1) SCN applications are required to support nomadism for mission-specific and generic actuators and motes.

2) SCN applications are recommended to support seamless handover for generic actuators and motes.

8.3 Context awareness

Context information can have a great effect on the decision-making process. Examples of context information elements include the following:

– Capabilities of SCN objects;

– Location of actuators and motes;

– Presence and operational status of actuators and motes;

– Traffic load and computational load of SCN objects;

– Information about faults of SCN objects.

SCN applications have the following general requirements concerning context-awareness:

1) Context information is required to be collected and distributed to any interested SCN object.

2) Delays in context information updates are required to be minimized so that the reliability of the decision making is not decreased significantly.

NOTE – Requirements specific to some context-related aspects are given in other specific clauses.

8.4 Location awareness

Location information needs to be maintained and managed in order to support context awareness with location information for SCN applications. Management can be in static or dynamic conditions of the located entities. In addition, SCN application service and device discovery can be facilitated by the usage of the location information. Thus, SCN applications have the following requirements:

1) Location information of mote groups is recommended to be managed for SCN applications.

2) Location information of actuators is recommended to be managed for SCN applications.

3) Location information of individual mote can be optionally managed for SCN applications when the location information of a single mote is useful.

8.5 Presence awareness

Presence information includes the network-related part of presence information (e.g., concerning connectivity and willingness to communicate) and the operation-related part of presence information (e.g., concerning workability and currently performing operation). SCN applications have the following requirements:

1) The network-related part of presence information is required to be managed for SCN applications.

2) The operation-related part of presence information is recommended to be managed for SCN applications.

8.6 Traffic and load awareness

To realize traffic and load optimization, SCN applications have the following requirements:

1) Information related to traffic and computational capabilities of SCN objects is recommended to be registered for SCN applications.

2) Information about current traffic and computational load is recommended to be managed for SCN applications.

8.7 Fault awareness

A SCN needs to react to the failure of any SCN objects in order to provide reliability and availability.

1) Information about SCN object faults is required to be managed for SCN applications.

8.8 Routing

1) SCN applications are required to support routing using distributed mechanisms, such as those based upon peer-to-peer (P2P) techniques.

2) SCN applications are recommended to identify the preferred path between any pair of SCN objects. The path selection can be based on historical data or on real-time data to reflect the traffic congestion situation between those SCN objects.

8.9 Load balancing

1) SCN applications are required to dynamically balance the traffic load of SCN objects, based on the status and/or capabilities of SCN objects, traffic balancing policy, etc.

8.10 Scalability

1) SCN applications are required to offer scalability by using P2P and/or other distributed mechanisms, so that the capacity of the SCN infrastructure to provide services to users is proportional, or nearly proportional, to the number of the motes and actuators.

8.11 Fault tolerance

1) SCN applications are required to ensure reliability and availability of the SCN infrastructure in order to handle a single mote failure and a mote group failure.

2) SCN applications are recommended to ensure reliability and availability of the SCN infrastructure in the case of failure of the SCN controllers.

NOTE – In the case of these failures, the capabilities of the failed SCN object(s) can be dynamically replaced by those of other SCN objects to provide consistent service to end users.

8.12 Quality of service (QoS)

Different SCN applications may have different QoS requirements. For example, data transmission in verification applications may require much lower delays than in other SCN applications.

1) SCN applications are recommended to support QoS differentiation according to the required service level quality.

2) It is required that the traffic volume generated by SCN applications be managed.

3) It is recommended that SCN applications avoid access concentration in a single SCN controller or a single mote.

4) It is recommended that specific QoS support for emergency applications be provided.

NOTE 1 – Clause 8.18 provides further information and requirements about emergency applications in SCNs.

5) It is recommended that specific QoS applications intended for pledging of security of decisions be provided.

NOTE 2 – Clause 8.14 provides further information and requirements about pledging of security of decisions.

8.13 Management

1) SCN applications are required to allow the user to enable and disable the provided services.
2) SCN applications are required to allow the user to apply different policies concerning allowing and denying specific commands to actuators.
3) SCN applications are recommended to provide the user with the ability to personalize the services.

8.14 Pledging of security of decisions

The decision-making process in SCN applications includes different activities on different SCN objects and can be very complicated. As a result, there are a number of sources of errors in decisions including erroneous, outdated, incomplete data and object synchronization errors. Some erroneous decisions of SCN applications can entail considerable negative consequences.

1) SCN applications are required to provide measures to avoid considerable negative consequences of their decisions on condition that all the actuators carry out commands given by the SCN applications exactly.
2) SCN applications are required to provide all the necessary measures to identify the party responsible for erroneous decision operations entailing considerable negative consequences.
3) SCN applications are required to provide operational logging sufficient to determine the source of errors entailing considerable negative consequences.

8.15 Open service environment (OSE) support

SCN applications can optionally support open service environment (OSE) capabilities as described in [ITU-T Y.2020] and [ITU-T Y.2234].

In case of SCN applications' support of OSE capabilities, SCN applications, services, actuators, motes and mote groups are recommended to be registered beforehand in order to enable the ability to be discovered (by specifying one or more related attributes).

It may be desirable for the user to use the same application in different SCN infrastructures. As the user changes his location and moves to another SCN infrastructure, service discovery is automatically started to check if that SCN infrastructure provides the required services. If these services are not registered, the SCN application may try to use a service composition procedure to create the required services from other existing services based on the capabilities of the SCN infrastructure. A service description language and its associated execution framework are recommended to be provided to support service registration, discovery and composition.

The following requirements are identified in the case of SCN applications' support of OSE capabilities:

1) It is recommended to support registration and discovery of SCN applications, services, actuators, motes and mote groups.
2) It is recommended to support at least one service description language and its associated execution framework.
3) Automatic service discovery and service composition can be optionally supported.

8.16 NGN service integration and delivery environment (NGN-SIDE) support

SCN applications can optionally support next generation network service integration and delivery environment (NGN-SIDE) capabilities [ITU-T Y.2240].

The SCN objects can be integrated with resources from different domains (e.g., telecommunication domain (fixed and mobile networks), broadcasting domain, Internet domain or content provider domain) over NGN with the use of NGN-SIDE.

From this point of view, the SCN objects can be considered as resources, and NGN-SIDE acts as a mediator between these resources and SCN applications. More specifically, the NGN-SIDE adaptation layer adapts the resources offered by the SCN objects in order to provide uniformly adapted resources (e.g., control and media format) for interaction with the NGN-SIDE integration layer as described in [ITU-T Y.2240]. The NGN-SIDE adaptation layer provides adaptation capabilities, called adaptors, hiding the details of the resources offered by the SCN objects.

The following requirement is identified in the case of SCN applications' support of NGN-SIDE capabilities:

1) SCN applications are required to access SCN objects through adaptors.

8.17 Mass mobile user terminal support

Most of the mass mobile user terminals have no technical possibility of direct data exchange with an existing infrastructure of motes. However, it is generally desirable to offer SCN applications to the users of these terminals because of their prevalence and considerable communication and computing capabilities. SCN applications may provide connectivity with such terminals using available communication technologies (e.g., Bluetooth, GPRS/3G, Wi-Fi, WiMAX).

1) SCN applications can optionally support the mass mobile user terminals including the terminals that are not specifically intended for SCN applications.

8.18 Emergency management applications

Some SCN applications provide support for early-warning emergency enhanced by recommendations about the escape from emergency situations based on the features of user location awareness and service personalization according to users' medical peculiarities or duties.

1) SCN applications for emergency management are recommended to be supported by the SCN objects.

9 Security considerations

SCN applications are required to support the integrity and confidentiality of the data exchanged during the application operations.

SCN applications are required to provide security for exchanged data against malicious attacks.

SCN applications are required to authenticate motes and mote groups to prevent compromising of sensed data.

It is recommended to provide a secure channel to protect the sensed data among SCN objects.

NOTE – Detailed security requirements for SCN applications are outside of the scope of this Recommendation.

Appendix I

Use case of SCN for verification

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

I.1 Errors in decisions

The decision-making process in SCN applications includes different activities and can be very complicated. As a result, there is a whole series of sources of errors in decisions:

– Unreliability of communication channels. Normally, SCN applications intend to make wide usage of wireless communications which are more error-prone in comparison with wired communications.

– Distributed calculation model. This model makes it difficult to synchronize all the activities and to provide all the SCN objects with actual data.

– Not very predictable duration of the decision-making process, due to different delays in calculations and data transmissions.

– Mobility of actuators and possibility of their usage for different SCN applications. When this is accompanied by the presence of several software and hardware vendors of actuators, this feature deprives the system designer of the possibility to test the system thoroughly in various conditions. Furthermore, when the interaction of the actuator with the SCN infrastructure is not on a systematic basis, making critical decisions cannot be entrusted entirely.

– Hardware and software errors.

As a result, control commands given by SCN applications should be analysed in order to ensure that possible errors do not result in considerable negative consequences. When a control command is intended for an information actuator, it can be analysed by the human who receives the control command. When a control command is forwarded to another network by a gateway actuator, the duty of analysis shifts onto the other network. But when a control command should be carried out without any direct human intervention to a machine actuator, special measures should be taken to counteract errors in decisions made by SCN applications.

I.2 Verification

For a machine actuator, there is a set of critical operations which can lead to considerable negative consequences when carried out in an improper system state. To avoid this, for each critical operation, a set of rules should be defined, which must be checked before this operation and/or while the operation is in progress. These rules are called "verification rules". To check the verification rules, a number of values of different types must be determined:

– Aggregate values, reference values, sensed data obtained in SCN application as part of normal flow of decision making.

– Aggregate values, reference values, sensed data obtained in SCN application which are only intended to support verification.

– Sensed data obtained from sensors associated with machine actuators.

– Values obtained upon request from SCN controllers or NGN entities.

In order to provide verification applications, verification networks are used. A verification network consists of devices and communication channels which are used to fetch and process the above described values. A verification network can have some elements which are also SCN objects or that constitute a part of the SCN infrastructure. A verification network may have much more strict requirements concerning reliability, security and performance compared to other SCN applications.

Data processing and transmission for the purpose of verification may have higher priority in QoS in comparison with other operations of SCN applications.

Examples of operations which require verification, verification rules and verification network elements are given below.

The operations in a verification network can be executed once before critical operations of SCN applications, or at the time of these operations or periodically. For each possible machine actuator state and detected verification rule failure, some operations should be defined to be performed instead of those given by the SCN application when one of the verification rules is mismatched. Such operations can be, for example:

– Immediate machine actuator stop.
– State transition of the machine actuator to some safe state.
– Alarm notification to authorized personnel administrating the SCN.
– Generation of a log entry.
– No action.

An example of flow chart for the decision-making process in verification networks can be depicted as in Figure I.1.

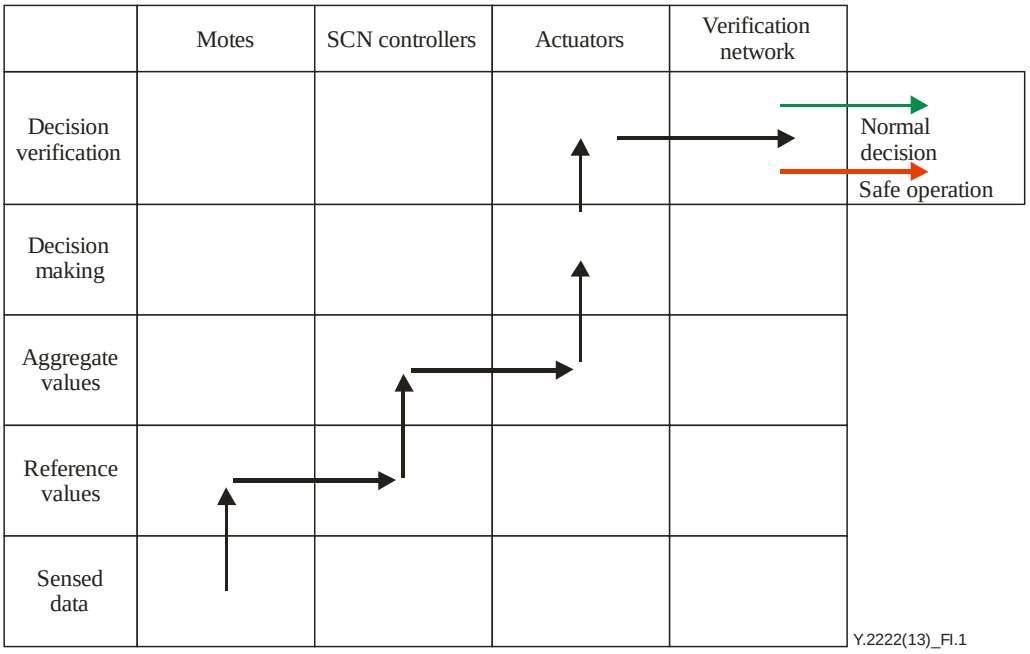

Figure I.1 – Decision-making process in verification networks

The figure depicts a normal decision-making flow, but because the decision involves a machine actuator, the verification process is initiated by the verification network.

If some of the checks of the verification process fail, some safe operation (or no action) is performed instead of normal decision.

I.3 Examples of verification applications

I.3.1 Fire safety system

A fire safety system is deployed in a building. If one of its sensors detects ignition or smoke, it activates machine actuators that lock doors and windows to prevent air circulation. The considerable negative consequences include people being locked inside the rooms and people being crushed by automatic doors.

Therefore, the verification network should consist of:

– sensors of movement in rooms;

– light sensors between door wings, and strain sensors on the motors of door wings to halt the motors if there is a person between the door wings.

I.3.2 On-road speed control

Sensors are used to monitor road conditions. Vehicles are equipped with actuators able to communicate with sensors which can automatically decrease the vehicle speed if the road conditions are dangerous.

A possible relevant negative consequence is that if the speed decrease is too fast, chances of collision with vehicles behind can happen. To prevent this result, the verification network should use a rear parking sensor that can monitor the free space behind the vehicle and slow the rate of speed decrease if there is another vehicle nearby.

I.3.2 Rescue robots

After a plane crash, rescuers use autonomous robots to retrieve survivors from under the wreckage. These robots pick up wreckage fragments and move them to a safe place.

If a robot runs out of energy after it has picked up a heavy fragment, it could drop it on the injured human or rescuers, causing therefore relevant negative consequences. The verification network should be based on energy sensors and on robot's CPU. The latter should be able to estimate the weight of the fragment to be picked up and the amount of energy required. If the robot's energy level is not sufficient, the operation must be blocked.

Appendix II

Use case of SCN for emergency management

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

An emergency management system [b-ITU News] uses motes to observe the physical conditions of a building (temperature, smoke, etc.). At the entrance to the building, a mobile user terminal (e.g., phone, PDAs or tablet PC) automatically connects to the SCN infrastructure and obtains data from the motes.

An emergency management system automatically detects emergency situations. In this case, the user equipment launches software for guidance in emergency cases. It gives instructions on how to leave the building in the safest way, for example:

– evacuation plans or maps;
– step-by-step sound commands and visual hints (e.g., interior photos with overlaid arrows towards the exit);
– videos showing how to use safety equipment.

The content of these instructions depends on various factors, for example:

– state of building detected by motes like accessibility and hazard level of rooms and escape routes;
– position of the user determined by the nearest network node or using GPS;
– user's state of health determined by e-health equipment.

In addition, special information containing both needs and duties is taken into account by the system. It may be limitations of motion and senses for disabled people that influence the route choice. At the same time, special personnel of the building may need specific instructions concerning their service duties (for example, emergency case specialists at the time of an accident at a nuclear power plant).

In-building actuators (e.g., door openers, emergency lightning and sprinklers) also get commands from the system and start working.

The emergency operation centre and/or emergency services also get information about the emergency including its type and place of origin.

If the motes detect no emergency situations, energy consumption of the system should be minimized. The system should be optimized for low traffic. Motes and mobile user terminals may be sleeping most of the time or be used for other applications. However, as an emergency situation is detected, the system must switch to special mode in order to rescue people as soon as possible (15 minutes or less), e.g.,:

– all the motes and mobile user terminals should be awakened from sleep;
– traffic not related to rescue should be discarded to provide low latency and high transmission rate;
– software applications running on mobile user terminals and not required for rescue (e.g., games, media players) should be suspended to decrease hardware resources consumption (CPU, memory, etc.) and switch user's attention entirely to the rescue tasks.

Figure II.1 shows an emergency management use case.

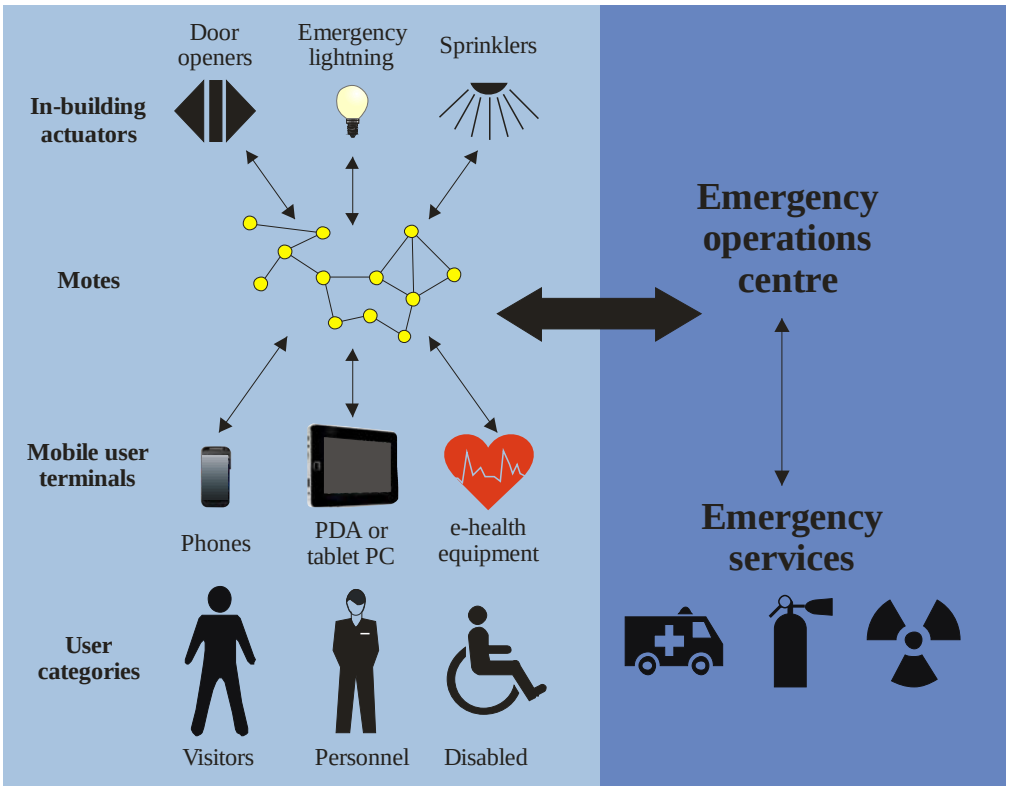

Figure II.1 – Emergency management use case

Bibliography

[b-ITU-T F.744] Recommendation ITU-T F.744 (2009), *Service description and requirements for ubiquitous sensor network middleware*.

[b-ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN.*

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN.*

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN.*

[b-ITU-T Y.2221] Recommendation ITU-T Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.*

[b-ITU News] ITU News No. 3 (April 2012), *Personal safety in emergencies – Innovative application for mobile phones.*
<https://itunews.itu.int/En/2475-Personal-safety-in-emergencies.note.aspx>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014