INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Z.331

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

MAN-MACHINE LANGUAGE

INTRODUCTION TO THE SPECIFICATION OF THE MAN-MACHINE INTERFACE

ITU-T Recommendation Z.331

(Extract from the *Blue Book*)

NOTES

1 ITU-T Recommendation Z.331 was published in Fascicle X.7 of the *Blue Book*. This file is an extract from the *Blue Book*. While the presentation and layout of the text might be slightly different from the *Blue Book* version, the contents of the file are identical to the *Blue Book* version and copyright conditions remain unchanged (see below).

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

Recommendation Z.331

INTRODUCTION TO THE SPECIFICATION OF THE MAN-MACHINE INTERFACE

1 Scope of the Section

The man-machine interface comprises the set of inputs, outputs and special actions, together with the man-machine interaction mechanisms, including dialogue procedures. Those elements are combined to manipulate the varied telecommunications functions which cover the management of SPC telecommunications systems. Consideration of these functions has been an essential prerequisite for the development of the CCITT MML Recommendations.

As stated in Recommendation Z.301, the CCITT MML can be used to facilitate operation, maintenance, installation, and acceptance testing of SPC systems. With the tendency of Administrations to centralize operations and maintenance jobs, many of the SPC systems functions may be controlled at terminals associated with operation and maintenance systems as well as at terminals associated with SPC systems. These terminals can be either local or remote relative to the system.

In order to help Administrations aiming to achieve uniformity among various systems, the MML Recommendations include not only the syntax of the language and dialogue procedures, but also the semantics relevant to the man-machine interface. Section 4 provides the means for deriving such semantics.

2 Organization of Section 4

Section 4 consists of the following Recommendations:

Z.331	Introduction to the specification of the man-machine interface
Z.332	Methodology for the specification of the man-machine interface – General working procedure
Z.333	Methodology for the specification of the man-machine interface – Tools and methods.
Z.334	Subscriber administration
Z.335	Routing administration
Z.336	Traffic measurement administration
Z.337	Network management administration

Recommendation Z.331 lists the operation, maintenance, installation and acceptance testing functions to be controlled by means of the MML.

Recommendation Z.332 presents the first part, the general working procedure of a methodology by which the man-machine interface can be generated for a particular functional area or subarea.

Recommendation Z.333 presents the second part, the tools and methods, of a methodology by which the man-machine interface can be generated for a particular functional area or subarea.

Recommendations Z.334 to Z.337 are based on the applications of phases 1, 2 and 3 of the methodology defined in Z.332 and Z.333 for the subscriber administration, routing administration, traffic measurement administration and the network management administration.

The main part of each Recommendation contains the model of the functional area or sub-area. Annex A of each Recommendation contains the list of functions to be controlled by means of the MML and the list of jobs considered in the development of the model. Annex B of each Recommendation contains a list of MML functions and associated information structure diagrams to be used as guidelines.

3 Functions to be controlled by means of the MML

The functions to be controlled by means of the MML are subdivided into four main areas: operation, maintenance, installation and acceptance testing. They are listed below. Based on the relationships existing among them, in each main area functions are grouped into functional areas and sometimes functional sub-areas. Due to the potentially different organization needs and system design philosophies, it is recognized that not all functions apply to every system.

The list of functions is not complete and it is expected to continue to evolve.

In particular, the issuing of Recommendations on specific areas or sub-areas will lead to the refinement of the preliminary list identified in this Recommendation for those functional areas or sub-areas. So far, this refinement has been achieved for subscriber administrations, traffic measurement administration, routing administration, network management administration (partially) specified in Recommendations from Z.334 to Z.337.

3.1 *Operation functions*

3.1.1 *Subscriber administration*[1)] (see Recommendation Z.334)

- administering subscriber lines related data;
- tracing malicious calls;
- retrieving subscriber charging information;
- observing subscriber charging.

3.1.2 *Routing and digit analysis administration*

3.1.2.1 *Routing administration* (see Recommendation Z.335*)*

- managing the routing data base;
- querying the routing data base.

3.1.2.2 *Digit analysis administration*

- managing the digit analysis data;
- querying the digit analysis data base.

3.1.3 *Traffic administration*

3.1.3.1 *Traffic measurements administration* (see Recommendations E.502 and Z.336)

- performing traffic measurements;
- scheduling the execution of traffic measurements and the output of results;
- managing measurements data;
- retrieving measurements data.

3.1.3.2 *Traffic analysis administration* (see Recommendation E.502)

- inputting measured data;
- inputting the identification and capacity information of the measurement object;
- managing traffic data records;
- managing the output of reports;
- managing analysis description data;
- supervising the control of the time-delay of the various analysis operations.

3.1.4 *Tariff and charging administration*

- changing the tariff for a certain traffic destination;
- changing parameters for a charging rate;
- changing time for switching between day and night rate;
- reading accounting statistics (accounting between operating companies);
- changing the parameters involved in the accounting methods for traffic between different operating companies;
- retrieving of charging information.

---

1) Subscriber administration deals with both single-line and multi-line subscribers.

3.1.5 *System control operation*

- setting and reading of a calendar;
- administering output routing;
- administering files;
- administering man-machine terminal capabilities;
- administering the system (hardware/software) configuration.

3.1.6 *User-system access control administration* (see Appendix I to Z.331)

- administering authority;
- retrieving authority information.

3.1.7 *Network management administration* (see Recommendation Z.337)

- performing measurements of network status and performance;
- performing network management actions;
- performing network management information distribution.

3.2 *Maintenance functions*

3.2.1 *Maintenance of subscribers' lines*

- testing one subscriber's line and associated equipment;
- testing a group of subscribers' lines and associated equipment;
- measuring one subscriber's line and associated equipment;
- measuring a group of subscribers' lines and associated equipment;
- blocking or unblocking a subscriber's line for maintenance purposes;
- observing or supervising of subscribers' lines and equipment.

3.2.2 *Maintenance of circuits between exchanges and associated equipment* (see Recommendation M.250)

- testing/measuring one circuit or a group of circuits and associated equipment;
- observing and supervising circuits and associated equipment;
- control the status of a circuit or a group of circuits and associated equipment;
- analysing maintenance data;
- administering and controlling maintenance reports.

3.2.3 *Switching network maintenance*

- making test calls;
- initiating a call trace;
- holding faulty connections;
- testing and measuring peripheral equipment (relay sets, signalling receivers and senders, etc.);
- testing and measuring switch units;
- reducing service for low priority subscribers;
- setting up a connection via a specific path through the network;
- supervising and measuring the quality of service of the switching network;
- localizing faults in the speech path network;
- providing access for traffic observation for maintenance purposes;
- reporting alarms;
- recording switch unit status.

3.2.4 *Control system maintenance*

- reporting system status;
- reporting alarms;
- localizing faults;
- testing on a functional basis after repair;
- initiating periodic testing operations;
- changing system configuration for maintenance purposes;
- checking consistency of data;
- initiating restart;
- setting traps for programme fault tracing;
- changing memory contents;
- memory dumping for maintenance purposes;
- controlling overload parameters;
- changing the criteria for the recognition of degradation of service;
- reducing service for low-priority subscribers.

3.3 *Installation functions*[2)]

3.3.1 *SPC system installation*

3.3.1.1 *SPC system hardware installation*

Installing:

- network blocks;
- trunks;
- signalling equipment;
- test equipment;
- blocks of subscriber-circuits;
- interface equipment;
- control equipment;
- memory equipment;
- input/output devices.

3.3.1.2 *SPC system software installation*

Installing:

- operational packages;
- test programmes;
- statistics programmes;
- programmes patches;
- signalling systems programmes;
- services, facilities programmes;
- system data.

3.4 *Acceptance testing functions*

Acceptance testing functions include any additional functions beyond those presented above to aid the administrations when testing a system to check its compliance with the Administrations' specifications.

---

2) Installation also covers the extensions or reductions of the system after it is placed into service.

APPENDIX I

(to Recommendation Z.331)

User-system access control administration

I.1 *General*

This appendix has been developed in accordance to the methodology defined in Recommendations Z.332 and Z.333.

The main part of this appendix deals with the model of User-System Access Control Administration. A glossary of the terms used is also included.

The list of functions to be controlled and the list of jobs are contained in Annex A.

For each function to be controlled by means of MML, one or more functions can be derived and each of them can be described using the metalanguage defined in Recommendation Z.333 in order to detail the relevant information structure.

Annex B contains a list of MML functions and information structure diagrams associated to each of them to be used as guidelines.

I.2 *Introduction*

User-system access control (here and after access control) is provided within a system to restrict the input allowed to be entered in order to prevent unauthorized system modification and or viewing of information.

Access control is the system function which performs the control of the access to systems and their functions by the users.

Access control administration is defined as the administration of the access rights of the users.

This Recommendation mainly covers human beings as users.

Machine to machine access control administration is not covered by this appendix.

It is therefore recognized that this appendix will require further study within a wider scenario including the various aspects of access control (man-machine, machine-machine, etc.).

I.3 *Access control model*

I.3.1 *Introduction*

Access criteria are defined to be the attributes that characterize the access to the system.

Permissions are defined to be the rights granted to the user.

Authority is defined to be the relationship between the access criteria and the permissions.

The inputs submitted are accepted by the system, provided that the system has verified the authority to enter them.

I.3.2 *Model*

The main attributes (see Figure I-1/Z.331) which have been adopted to identify access criteria and permissions are the following (other attributes of the two categories can be adopted depending on the administration's needs):

a) for access criteria
   - user identity
   - terminal identity
   - time interval

b) for permissions
   - command class
   - command parameters
   - system identity
   - time interval

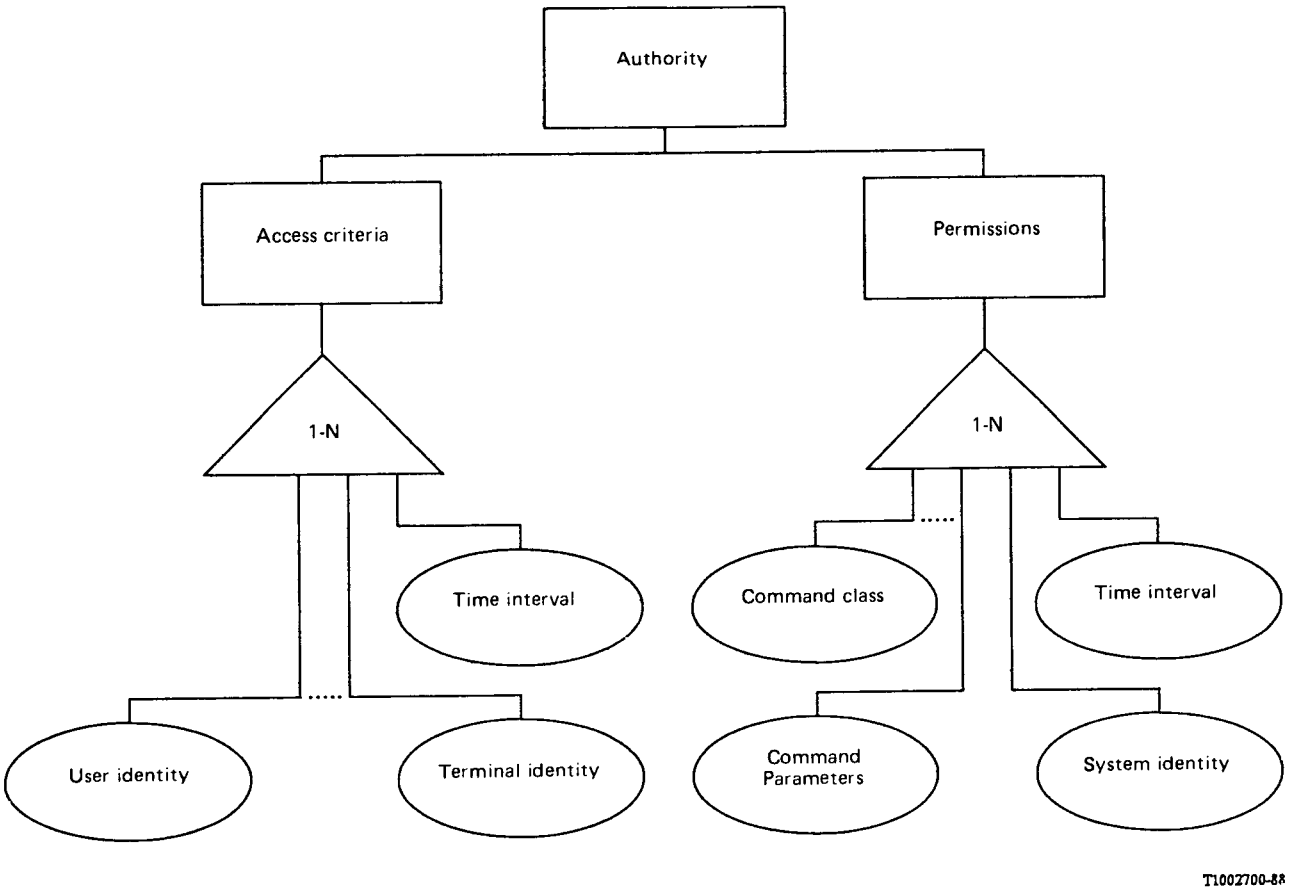

FIGURE I-1/Z.331

User-system access control administration

Some of the attributes listed above may not be implemented according to administration requirements.

In order to facilitate access control administration, groups may be formed in terms of single access control attributes (e.g. group of user identities can form a maintenance group).

An example of implementation is represented in Figure I-2/Z.331.

Authority					
Access criteria			Permissions		
User identity	Terminal identity	Time interval	System identity	Command class	Command parameters
User 1	Terminal 1	Any	Any	Any	Any
User 1	Terminal 2	8-17 h Monday through Friday	System 1	Subscrib. Administr.	Direct numb. : 81 000-82 000
User 2	Terminal 3	20-8 h	System 1	Junction maintenance	Junction identity 1A23 1800
User 3	Any	8-17 h	System 2	Subscrib. maintenance	Direct numb. : 73 000-87 000
Any	Terminal 4	8-17 h	Any	Subscrib. administr.	–
–	–	–	–	–	–

FIGURE I-2/Z331

Example of application

I.3.3 *Attributes of access control*

In the following the meaning of the main attributes which are likely to be used in the access control administration, is described.

a) User identity

The user identity results from the identification procedure (see Recommendation Z.317) and uniquely identifies the user to the system.

In the identification procedure usually the identity of the individual user is used.

b) Terminal identity

The terminal identity is the identity of the I/O device as known to the system, via its hardware or logical connection.

c) Time interval

The access control may depend on the time when the input is entered and/or executed.

d) Command class

A command class can be either a single command code (see Recommendation Z.315) or an identifiable set of command codes.

e) System identity

System identity is the identity of the system or an application in which the command is allowed to be performed. In a centralized support system, individual systems connected to it may have their own access control. Alternatively, centralized control may be used based on the identity of the system addressed.

f) Command parameters

Access control may depend on a parameter (see Recommendation Z.315) or a combination of parameters. The control may be based on either the parameter name or the parameter name and its values.

If a parameter is considered, it may be desirable to limit such use to major objects in the system relevant to specific O&M Administration needs.

I.4 *Glossary of terms*

access criteria

The set of attributes that characterize the access to the system. Example attributes are user identity and terminal identity.

permissions

The rights granted to the user.

authority

The relationship between access criteria and permissions.

terminal identity

Identifies a physical terminal, a channel or a port to an SPC system.

I.5 *List of functions and jobs*

I.5.1 *List of system independent Class B functions*

I.5.1.1 Administering authority

I.5.1.2 Retrieving authority information

I.5.2 *List of jobs*

I.5.2.1 *To create/change authority*

- the purpose of the job is to create/change a specific authority by means of managing the relevant attributes;
- the system is supposed to record the data and check their correctness;
- the operator is supposed to input all needed data;
- the complexity of the job may be high depending on the amount of the data to be input;
- the frequency of the job is low.

I.5.2.2 *To delete a specific authority*

- the purpose of the job is to delete all the data related to the specific authority;
- the system is supposed to delete the data related to the authority,
- the operator is supposed to input the identity of the authority to be deleted;
- the complexity of the job is low;
- the frequency of the job is low.

I.5.2.3 *To interrogate the authority information*

- the purpose of the job is to retrieve authority information;
- the system is supposed to output the requested information on the selected device;

- the operator is supposed to input the identity of the access control attributes;
- the complexity of the job is low;
- the frequency of the job is low.

I.5.2.4 *To activate/deactivate an authority*

- the purpose of the job is to activate/deactive a specific authority previously created/changed; this job may be implied in the creation/changing job;
- the system is supposed to activate/deactivate the authority;
- the operator is supposed to input the date and the time for the activation/deactivation and the identity of the authority;
- the complexity of the job may be medium;
- the frequency of the job is low.

I.6 *Guidelines for the list of MML Functions and associated information structure diagrams*

I.6.1 *Introduction*

This section contains guidelines for the list of MML functions and associated structure diagrams related to the access control administration model defined in § 3 of this Recommendation.

I.6.2 *List of MML functions*

This list contains possible MML functions for the Access Control Administration.

This list is not mandatory nor complete; it may vary according to administration needs, telecommunication network levels, regulatory needs, etc.

I.6.2.1 *Creation*

- create authority

I.6.2.2 *Changing*

- change authority

I.6.2.3 *Deletion*

- delete authority

I.6.2.4 *Interrogation*

- interrogate authority

I.6.2.5 *Activation/deactivate*

- activate/deactivate authority

I.6.3 *Information structure diagrams*

(To be developed.)