International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

L.80

(05/2008)

SERIES L: CONSTRUCTION, INSTALLATION AND PROTECTION OF CABLES AND OTHER ELEMENTS OF OUTSIDE PLANT

Operations support system requirements for infrastructure and network elements management using ID technology

Recommendation ITU-T L.80

Recommendation ITU-T L.80

Operations support system requirements for infrastructure and network elements management using ID technology

Summary

Telecommunication networks require proper allocation of network elements and planned periodic maintenance to deliver services quickly and efficiently, to minimize out-of-service risk and to guarantee service level agreement satisfaction. It is particularly important to focus on the issue of optical fibre-based infrastructures and the related huge amount of transmitted information. Network elements that undergo allocation and maintenance operations can be of several types and can differ in terms of position, dimensions, services, field work and scheduled times for periodic planned maintenance.

Identification data (ID) technology can be applied to solutions that focus on the proper management of infrastructure and network elements. The ID uniquely identifies an element of interest in terms of its allocation and maintenance.

Source

Recommendation ITU-T L.80 was approved on 29 May 2008 by ITU-T Study Group 6 (2005-2008) under Recommendation ITU-T A.8 procedure.

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/.

CONTENTS

		Page
1	Scope	1
2	References	1
3	Definitions	1
4	Abbreviations and acronyms	1
5	Operations support system	2
	5.1 Data communication network	2
	5.2 Database	3
	5.3 User interface	3
Appendix I – Italian experience regarding RFID tag solution for telephony poles		5

Recommendation ITU-T L.80

Operations support system requirements for infrastructure and network elements management using ID technology

1 Scope

This Recommendation deals with support systems for infrastructure and network elements management using ID technology for telecommunication networks. In particular, it describe system architecture and points out functional requirements for data transmission, database access and interoperability for an operations support system (OSS) that enables operations, administration and maintenance of network elements.

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 L.64] Recommendation ITU-T L.64 (2007), *ID tag requirements for infrastructure and network elements management*.

[ITU-T L.69] Recommendation ITU-T L.69 (2007), *Personal digital assistant requirements and relevant data structure for infrastructure and network elements management*.

3 Definitions

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APN Access Point Node

DCN Data Communication Network

GPRS Global Packet Radio Service

GSM Global System for Mobile communication

HTTP HyperText Transfer Protocol

ID Identification Data

NE Network Element

OSS Operations Support System

PDA Personal Digital Assistant

RFID Radio Frequency Identification

TMN Telecommunications

VPN Virtual Private Network

XML eXtensible Markup Language

5 Operations support system

An OSS generally refers to the system or systems that perform management, inventory, planning, engineering and maintenance functions for communications service providers and their networks.

An OSS for ID of network elements (ID OSS) can be defined as the system for management of NEs identification supporting other OSSs functions such as maintenance and inventory.

It is recommended to use an ID OSS to support operations, administration and maintenance of NEs that feature ID technology. A general system architecture that defines logical relations between an ID OSS and other components of the network management system of the service provider is illustrated in Figure 1. Terminals and devices other than PDAs can be used.

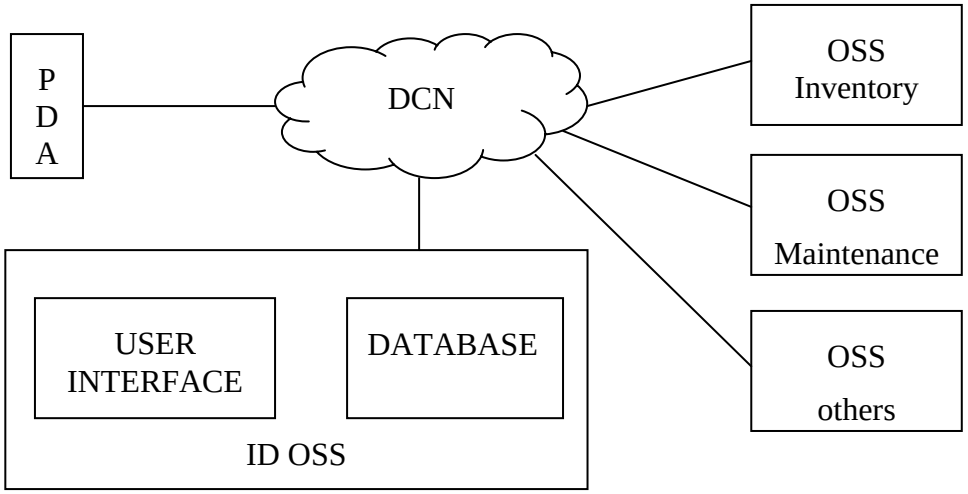

Figure 1 – Example of system architecture for ID OSS

Each NE administered by an ID OSS should have a unique ID.

An ID OSS should have a database to store NE information.

An ID OSS should have a user interface to support database access and data processing.

An ID OSS typically is supported by a DCN that enables communication between different parts of the system and with other OSSs.

An ID OSS should provide secure communication (e.g., authentication and/or data encryption) when confidential data are transferred through public networks: between a database and a PDA, between a database and other OSSs, between a database and a user interface.

5.1 Data communication network

A DCN is the set of technological instruments that enables connection and communication between different components inside an ID OSS and between an ID OSS and other components in the network management system. A DCN could be based on both private and public networks.

A DCN should support communication between a PDA and an ID OSS to enable database content updating and information retrieving on the PDA. An ID OSS and a PDA must be in communication at least when data transfer is needed. It means that in the work area, a PDA can be used in online or off-line mode. In the first scenario, data transfer can be performed in real time, typically using a wireless connection. In the second one, data transfer is performed before and/or after activity in the work area using a wired or wireless connection. Such a scenario is typical in work areas where wireless communication is not allowed.

A DCN should provide a connection between a user interface and a database to enable data access and processing.

A DCN should provide a connection to external OSSs when information exchange is required.

An ID OSS should provide secure communication (e.g., authentication and/or data encryption) when confidential data are transferred through public networks: between a database and a PDA, between a database and other OSSs, between a database and a user interface.

5.2 Database

A database is the OSS's component used to store data records of each NE that features ID technology.

Each network element administered by the OSS and stored in the database should have a unique distinguishing ID.

The First step is the creation of a network element data record in the database. From this moment on, as a result of an action executed on a network element, information in the database is updated. It is suggested to add and not substitute old data values with new ones in case it is needed to trace activity and keep history on each NE (network evolution).

It is suggested to make a clear distinction between physical and logical NEs in the database when it is needed. A physical NE is the specific material, while a logical NE is typically defined by a function in the network.

A database should support administration of both individual NEs and an aggregation of NEs that share one or more specific data values in their records (e.g., all the fibres terminated on a rack).

A database could be controlled by monitoring algorithms in real-time or off-line mode. Real-time monitoring is designed to check data before database content updates. Off-line monitoring is designed to check database content. Alarms should be triggered when incongruent information is detected.

A database should be accessible by operators to perform queries.

A database should be accessible from other OSSs if their procedures require retrieval of such information for other purposes (e.g., work force management).

5.3 User interface

A user interface is the OSS's component that enables users to access and process database content inside a computer system.

A user interface could be available wherever users need to interact with the database. It is suggested to use a technology that enables database access even from public networks if it is needed.

User interface access should be protected using a log-on procedure. Such a procedure enables user activity tracking and user profile-based access. A user profile definition is suggested because it limits user access to data content and processing functions. Typically, the administrator profile has complete access to data and functions.

It is recommended that information on a network element can be retrieved from the database using just its unique ID.

A user interface should support query functions. For each query function, the user should be enabled to set as many filters as data fields are defined for each network element in the database. It should be possible to use multiple filters at the same time.

A user interface could support exporting functions in case it is needed to extract information from the database. In this way, a user can manipulate such data with third-party software.

A user interface could display an alert if information retrieved from the database has still not been checked by monitoring algorithms.

As a valid means of support, a user interface could be linked to cartographical maps where the NE position can be displayed (if geographical coordinates are available in the database).

Appendix I

Italian experience regarding RFID tag solution for telephony poles

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

In Italy, RFID technology for maintenance support has been tested on the poles used in the wireline access network throughout the country where wooden poles represent almost the totality.

The first step was to trace the in-field maintenance actions and to collect more information on these items, in order to better understand causes of poles turnover. On one side, better knowledge of the pole network means avoiding random and massive monitoring actions, better spare parts management and network planning. On the other side, information maintenance can be certified because the tag is on the pole and stores information of the latest actions (date, operator code, etc.).

Typical periodic maintenance requires checking all poles inside a network area. More than 40 000 poles have been checked in several network areas spread across the national territory.

In this scenario, the following solution has been adopted for the OSS, as illustrated in Figure I.1.

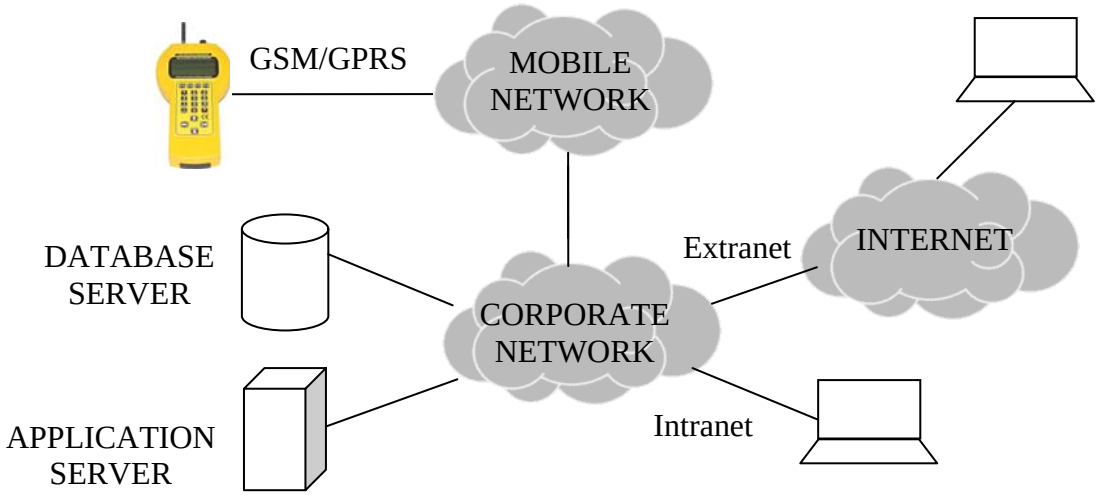

Figure I.1 – Simplified system architecture for ID OSS

A PDA communicates using a GSM/GPRS network. A GPRS connection is the first choice, if available, and is performed through a private APN directly connected to the ID OSS private network. When a GPRS connection is not available, a data GSM connection is used. If communication is delivered through a public network (e.g., Internet), confidential information is protected.

Communications between a PDA and an ID OSS is based on HTTP and XML in a client/server architecture. Every access from a PDA is traced in a log file.

Data transmitted from a PDA and regarding NEs are stored on a SQL server database. NE in a database can be active or passive: active NE is currently used in the network, while passive NE has been dismissed, but information regarding it is still available in the database.

A user interface application has been developed using a technology based on standards. This application is accessible both inside an intranet and through an extranet. An Internet browser is the only software required for the user terminal to access this application. HTTPS must be supported to provide secure connection.

Log-on is based on different user profiles (username and password) that enable different functions inside the application. The user interface is divided into two sections, operations and administration.

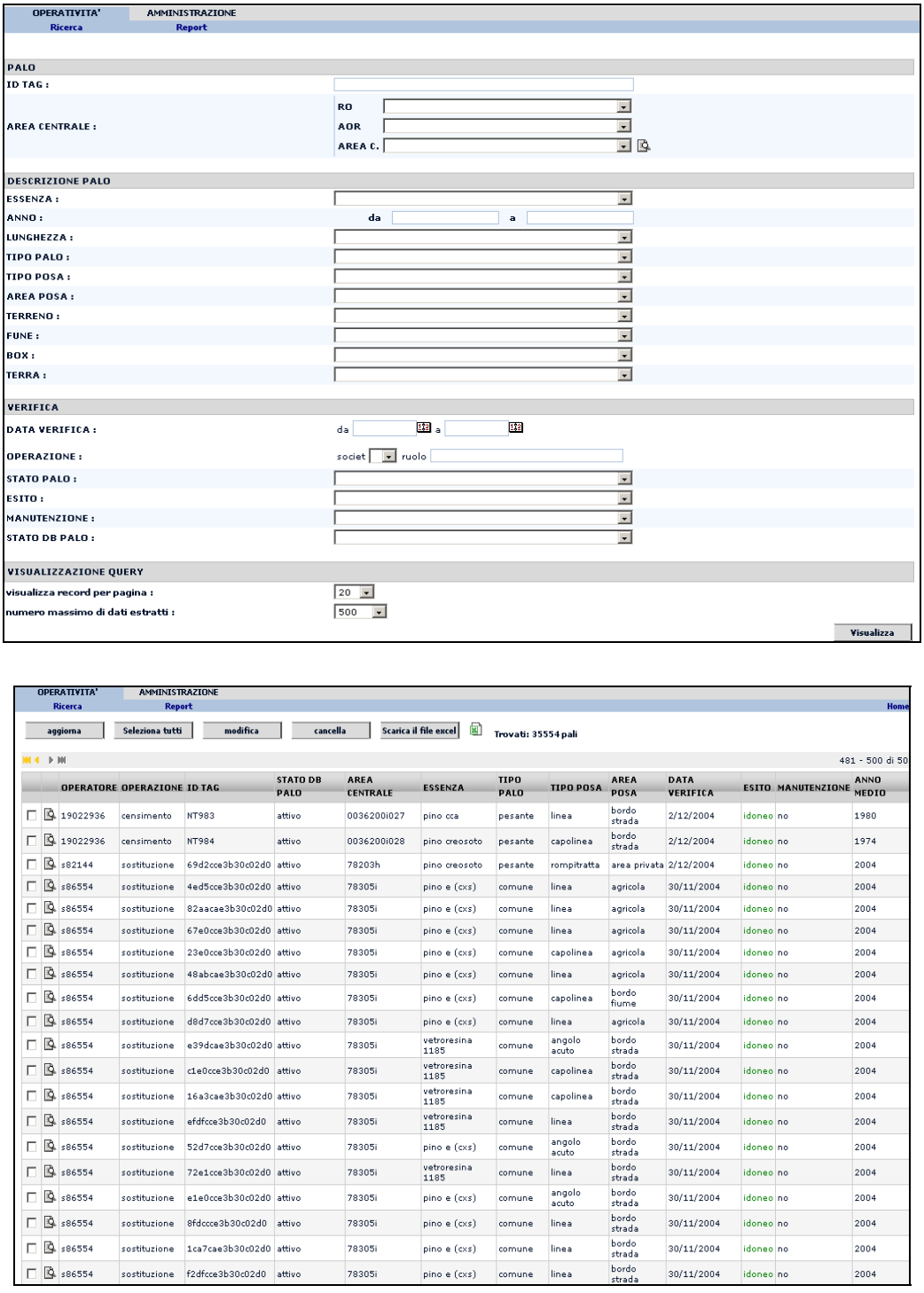

Figure I.2 – Screenshots of user interface application

The main features in the operations section of the user interface are:

- Database query: it is possible to search information using as many filters as there are NE data fields.
- Report creation: it is possible to create automatically reports using a database query based on customized criteria.

- Export: after database query or manual NE selection, it is possible to export data to a spreadsheet software.

The main features in the administration section of the user interface are:

- Access monitoring: it is possible to monitor access from a PDA using filters such as "time period", "PDA serial number" and so on.
- Web users: it is possible to manage the user profile associated with the user interface application.
- PDA: it is possible to enable/disable user terminal devices that are supplied for the activities on NEs.

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	Telephone transmission quality, telephone installations, local line networks
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, 2009