341

INTEGRATED MANAGEMENT INFORMATION IN UTILITIES

Working Group
D2.17

February 2008

WG D2.17

Integrated Management Information in Utilities

Members		Corresponding members	
Mr Jorge Fonseca	Portugal	Mr Peter Cristaudo	Australia
Mr Günter Endlich	Germany	Mr Bernhard Gutmann	Germany
Mr Anders Runesson	Sweden	Mr Jan Piotrowski	Poland
Mr. Mehrdad Mesbah	France	Mr. Rodolfo Pellizzoni	Argentina
Mr. Daniel Gonzalez	Spain	Ms. Milena Matic	Yugoslavia
Mr. Enrique Garcia	Spain	Mr. Claudio Trigo	Brasil
Mr Hermann Spiess	Switzerland	Mr Hironaga Yamazaki	Japan
Mr Carlos Samitier (Convener)	Spain	Mr Stuart Mann	UK
		Dr Fernando Gonzalo	Spain
Mr William Caffrey (Secretary)	Ireland	Mr. Maurizio Monti	France
		Ms. Mirjana Stojanovic	Serbia
		Mr. Wan Azlan	Malaysia
		Mr. Allan Riesz	Australia

Copyright © 2008

"Ownership of a CIGRE publication, whether in paper form or on electronic support only infers right of use for personal purposes. Are prohibited, except if explicitly agreed by CIGRE, total or partial reproduction of the publication for use other than personal and transfer to a third party; hence circulation on any intranet or other company network is forbidden".

Disclaimer notice

"CIGRE gives no warranty or assurance about the contents of this publication, nor does it accept any responsibility, as to the accuracy or exhaustiveness of the information. All implied warranties and conditions are excluded to the maximum extent permitted by law".

ISBN 978-2-85873-029-2

TABLE OF CONTENTS

1. Introduction

The objective of the present brochure is to assist utilities to define, specify and evaluate the high-level management systems that form the information infrastructure and to describe the integration of the different components. The considered scope includes not only the telecommunication networks, but also information processing platforms and system components, as well as intelligent devices incorporated into the automation architecture of the power substations (programmable controllers, Intelligent Electronic Devices (IEDs), etc.).

The document covers the technical and business reasons leading to the adoption of such an Integrated Management Information (IMI) approach. It does it by identifying the services that are required, bearing in mind different utility organisations, different utility business models and different management information user demands.

A general survey of managed equipment and systems is given together with their potential management interfaces in section 3, followed by the different ways for gathering management information in section 4.

Section 5 describes a number of typical utility management applications that must be implemented through or in association with an IMI approach.

Section 6 describes the different data communication networks and protocols that may be employed jointly or separately in order to bring management information from the field to the network management centre and to the different management facilities dispersed across the network.

The last section highlights the business and technical issues related to the implementation of an integrated management system.

A case study has been included in appendix B in order to show a practical approach to the use of the some of the concepts and technologies depicted in this brochure.

1.1. The role of a modern Network Management Centre

The Network Management Centre (NMC) constitutes the core entity for day-to-day operation, administration, maintenance and security monitoring of the network, medium term extension and enhancement planning as well as an advisory entity for long term and strategic decision making through a synthetic and statistical view of the information network, systems and services.

The technological evolution has widened the scope of the network beyond the limits of telecommunication equipment. The information exchange system includes all communicating entities from the substation IED to the different management platforms of the power utility (power network management, energy management, enterprise applications, etc.). A more general concept of integrated management information can therefore become attractive. In this case, the NMC need not be a single geographical entity but a distributed platform serving the different functional layers of the infrastructure and the different functions in the utility organization (cable monitoring, system administration, telecommunication network management, security monitoring, etc.).

The following tasks are to be performed through the NMC:

- Control, operate and manage in a unified manner all elements constituting the telecommunication network (cable, equipment, system)
- Control, operate and manage auxiliary systems required for the proper operation of the telecommunication network (Power supplies, Air-conditioning, Site intrusion detection, etc.)
- Supervise, locate and isolate faults in the system through monitoring of the different constituents in a permanent manner (24H/7Day).
- Supervise IT platforms (servers, workstations, LAN components, etc) associated to the operation of the system (Network Management components, IP network servers, EMS platforms, etc.).
- Track all fault management tasks through to conclusion including restoration of services, replacement of faulty units, return of faulty units to the manufacturer and restoration of spares to the required level.
- Assign maintenance and problem solving to the appropriate staff which may be geographically remote and dispersed. Escalate faults to higher level maintenance organization (maintenance contractor, supplier, expert, etc.) if necessary.
- Supervise network, system and data security against attacks, intrusions and viruses.
- Monitor the performance of the different constituents through the measurement of traffic, loss rates, service times and overall delays in the system. In particular, switching networks and IP infrastructure must be monitored.
- Determine service impact of infrastructure faults and take appropriate action (notify, restore, etc.).
- Produce business-oriented dashboards and management reports with dedicated synthetic information for maintenance management, overall system management, network engineering and planning, cyber-security management, power system communication management, and dedicated service-provider business management.
- Perform Asset Management and inventory activities for the whole system and produce up-to-date network documentation available online to all concerned parties. The documentation shall include details of all components constituting the telecom network (identification, type, location, status, configuration and parameter settings, hardware and software release, maintenance history, etc.). The centralized network documentation must furthermore track configuration changes in the past and in future and hence provide change management functionality.
- Perform network and system documentation including physical and logical resource management e.g.
  - Which channels are multiplexed over a certain higher level container, through a certain equipment or over a certain communication medium
  - Which processes are using a particular processing resource.
  - Which services are carried over a certain network resource.
  - Which users are affected by the failure of a particular resource.

  This aspect applies also to VLAN management and in general, the organization of distinct virtual networks across the physical system.
- Perform Directory services, IP Address management, priority management, and user inventory functions in general.
  - Perform service-oriented and business-oriented management tasks for both internal (the utility) and external customers. In particular provide Customer

Relationship Management (CRM) including service usage monitoring, billing and service notification for each customer and each category of service, as well as Service Level Agreement (SLA) monitoring for each customer contract.

1.2. Network and System Management - Present Status

At present, the different components of the communication network are connected and managed through dedicated vendor-specific Network Management Systems (NMS) generally located at a Control Centre. Many utilities desire to “integrate” their different NMS components, without a clear definition of the significance and extent of the integration and the functionalities to be obtained.

The network generally includes many generations of equipment with variable management accessibility. The access possibilities of the different systems range from specific craft terminals with no standard access point, to ITU-T Q-interfaces, SNMP platforms, MML, CORBA, or system level logs for IT components. Many elaborated management systems incorporate some form of standard database in their architecture (Oracle, etc.).

A great number of communication equipment and associated facilities, particularly those in the peripheral part of the communication network (not on the digital infrastructure) are only accessible through the power system SCADA collecting their alarm contacts and storing them in the SCADA historical information database. This management information arrives at present to the control centre and is made available at the operator desk congesting the control centre with non-process information. In this case, it is the control centre operator that transfers manually, often by telephone, equipment alarm indications to the appropriate staff.

The different NMS may be made accessible through the same PC workstation acting as a client or as an emulated terminal, or even incorporated on the same server as different applications (separate windows). However, this type of integration, already implemented by many utilities, does not allow any interaction between the different systems.

At the other extremity, a full interconnection as per ITU-T TMN model, designed to carry out all management functions remains costly and time-consuming, despite several standards for the network management model, protocol stacks, functions, object presentations and information base formats. Moreover, the implementation of a unifying ITU-T TMN layer, defined for large telecom operators, is rarely adequate for a utility telecommunication network due to scale issues. A telecom operator has generally an extensive “installed base” for each type of equipment and the problem of multi-vendor integration can be solved at the Network Operation Centre, through large investments and with extensive collaboration from the individual vendors. In the case of a utility, the large variety of equipment types and the relatively small quantity per type of equipment do not incite any major collaboration from the manufacturers, or any important investments from the utility. Moreover, the effort must be repeated every time a new type or a new release of equipment is added into the system.

Expert intervention on the equipment for detailed diagnostics and reconfiguration is fulfilled by the dedicated vendor applications purchased with the equipment itself. Many new communication system designs are embedding management intelligence directly in the equipment reducing the central management system’s complexity.

The information processing system composed of multiple platforms such as Energy Control Centre, Substation Control, Energy Metering and Billing, Network Planning, Maintenance Management, etc. are managed separately and to varying extent. The task of management is limited to computer monitoring and does not generally take into account the interactions between these platforms and the associated communication infrastructure.

The different condition monitoring systems in the power utility like transmission lines, power transformers, breakers, etc. are stand-alone systems which may interact with the power system SCADA to transfer information to the control centre. The information processing, storage and exchange platforms used in these systems are generally not managed in a formal manner.

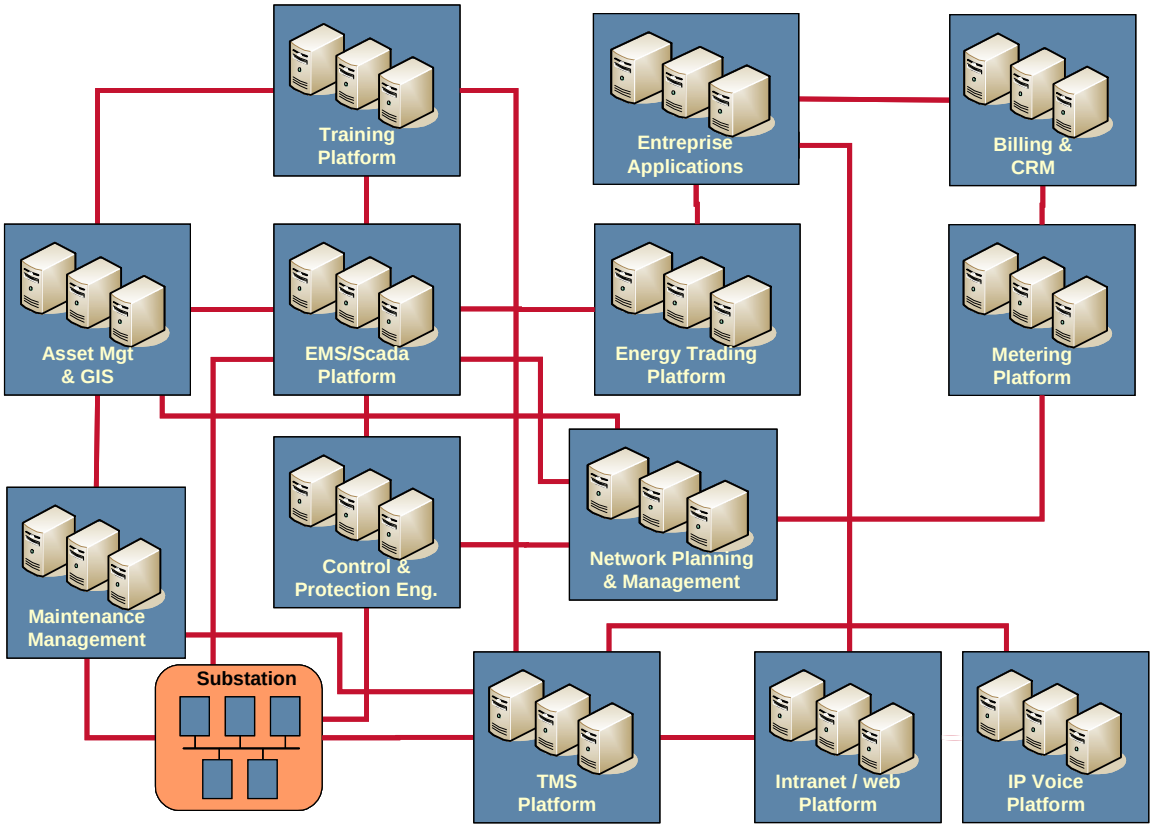

Figure 1.1 Information Processing Platforms

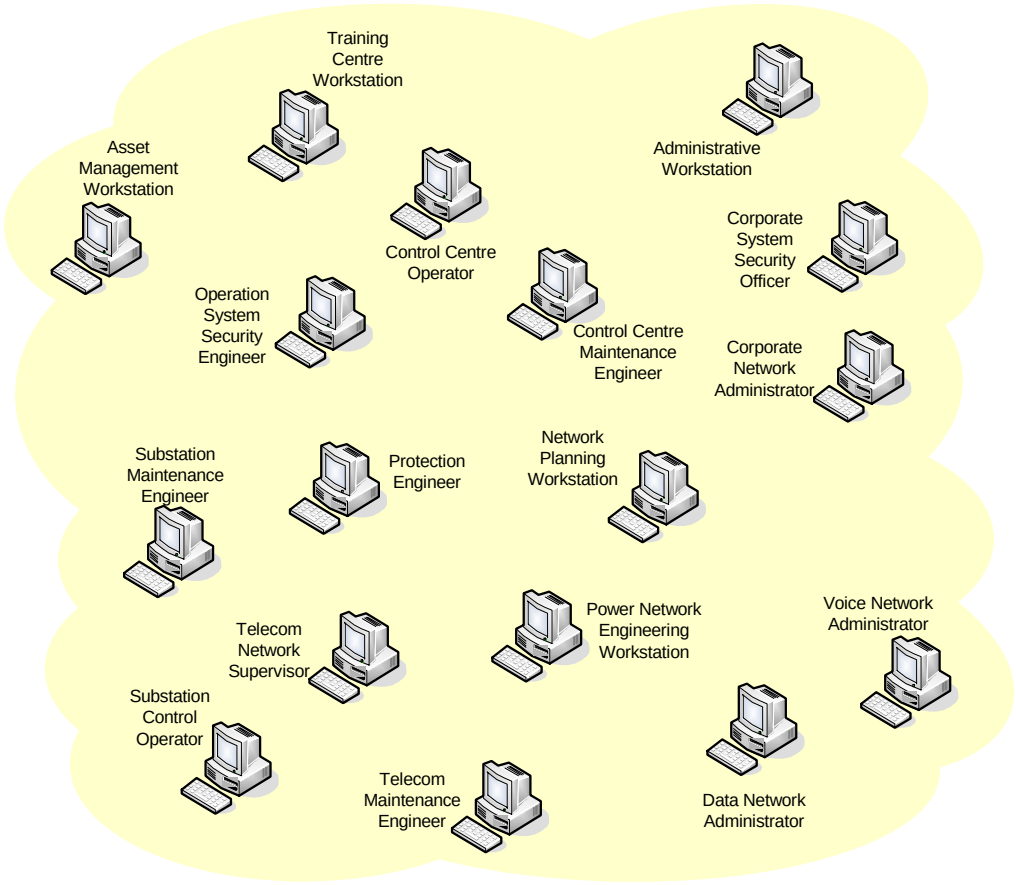

Figure 1.2 Management Information Users

1.3. Integrated Management Information Concept

An Integrated Management Information system is a common platform that permits the different information processing, storage and exchange systems and other associated infrastructure components in the Power Utility to interact, in order to perform different tasks such as asset management, maintenance, condition and performance monitoring, administration, planning and supervision. It overcomes the problem of multiplicity of management systems in a multi-vendor, multi-technology environment as existing in most telecommunication networks, IT infrastructures and different automation and system monitoring components. It also allows a global vision of the utility information infrastructure, relating the different layers and components, which are otherwise divided into separate worlds, and hence provides a better and faster understanding of the cause and consequence of different system events through sharing of management information on the utility scale. Web-technology permits easy access to relevant information for the different users.

Concerned systems and devices include all components in the utility information chain:

- information source and capture device (Intelligent Electronic Devices - IEDs, meters and transducers),
- information processing, storage and MMI (servers, process controllers, system software, IT platforms, workstations)
- information exchange and related security components (communication network, LAN switches, routers, firewalls, etc)

- auxiliary systems (batteries and chargers, UPS, air conditioning facilities, site surveillance facilities)

The managed entity can be any device or system or any service provided to a group of utility staff.

The integrated management is able to produce comprehensive view of the information based on different and distinct management systems in order to feed different actors with appropriate information concerning their managed, administered or used systems.

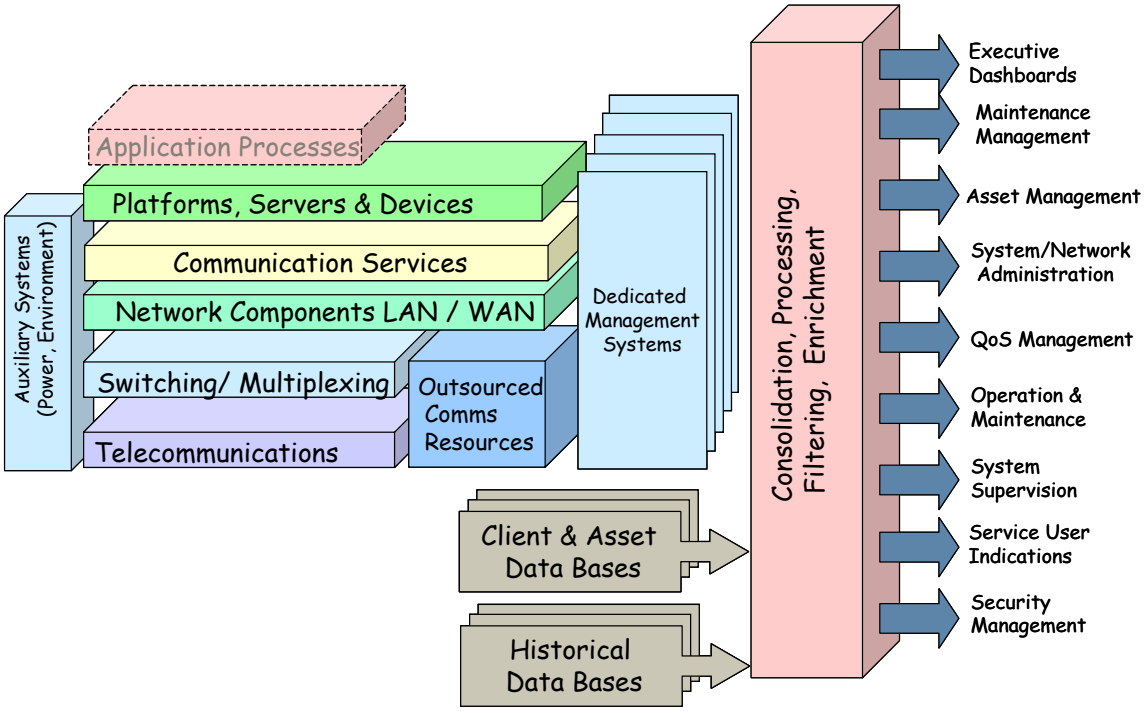

Figure 1.3 Functional Management Information Model

Two basic classes of management actors can be distinguished:

Service providers need information about the systems that they manage, maintain or administer as well as the service that they provide over these systems.

Service users need to be informed of the state of the resources that they use and the impact that they may have on the quality or continuity of the service.

Different management actors may be at the same time provider and user of different services.

Integrated Management concept is based upon the principle of collecting information through whatever system that allows access to the information and in whichever form that the information is available. Different dedicated management systems and the power system SCADA are examples of data collection mechanisms.

This allows any authorized actor requiring access to certain information to do so without having a direct link to the collection system for this information. Moreover, the information is to be presented in the most useful manner to each user. e.g. an electronic board failure is to be presented with manufacturer specific details to the

concerned maintenance engineer, as a generic failure information to the general system supervisor and as a statistic on a type of equipment or as a statistic in a given region to the concerned management actors, and finally as a service unavailability to the users requiring the operation of the faulty equipment.

The interaction with the managed entity can be bi-directional or uni-directional. In the former case, the integrated system permits parameters to be set or the managed entity to be reconfigured. In the uni-directional case, it is only necessary to read the entity's status or to receive event information from the entity. Most integrated management tasks require only uni-directional interaction. Setting and configuration tasks are by nature reserved to a very restricted class of operators which have this possibility through the dedicated management tools. Moreover, the integrated management system can allow the particular operator to connect remotely to the dedicated management system through terminal emulation for more close interaction with the managed entity.

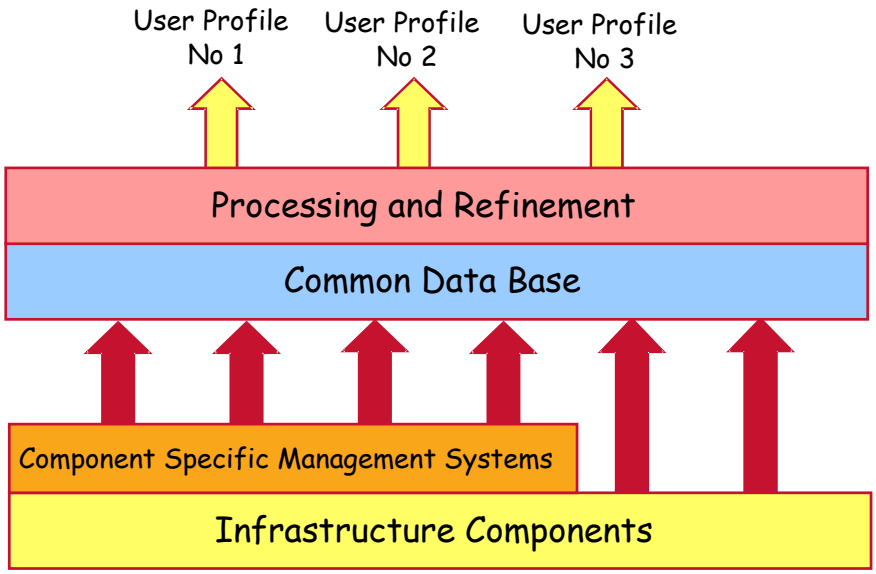

Figure 1.4 Management Information Process

1.4. Benefits

By developing an integrated management information approach, the IMI can deliver many new benefits to an increased audience. Network managers can take advantage of centralized administration, using consistent tools to manage applications and resources. The different network management users can be more productive with seamless access to information via Web-based applications, all with a single network-access. Network implementers benefit from an integrated application development framework, which allows them to focus on delivering business solutions instead of designing an application infrastructure.

To deliver effective IMI, a unified platform with a single security model is preferred, with a single network infrastructure, a single data access model and a single application development framework. The end result is a network management platform that is easier to use, to manage and to implement new applications. All of which can decrease the total cost of ownership.

By adopting an integrated management approach the following benefits can be expected:

- Increased flexibility:
  - to access different types of information in a co-ordinated fashion, such as operational and business oriented information,
  - to access information from different situations such as remote or outside the traditional business locations.
- Improved operation and maintenance performance:
  - Increasingly, as networked devices become more sophisticated, the level of self-diagnosis and the amount of information available from networks in the event of a fault is increasing. Effective fault management needs to present this information in a manner that reduces the MTTR through more accurate and faster diagnosis of problems, influencing the service availability as well as maintenance cost.
  - Performance monitoring has not, in the past, been widely used. However, as devices become more sophisticated with inbuilt intelligence, a greater reliance on condition monitoring can significantly reduce routine maintenance requirements. That is, the preventative maintenance capability of an organisation can be better targeted to reduce the overall maintenance cost.
- Information format standardisation.
- Improved use of resources.
- Greater efficiency in information collection.
  - The same source of information may be made available to different users or systems.
- Greater efficiency of information use
  - Easier to extract or synthesise useful information from collected data.
- New functionality or improved visibility arising through integration of diverse information.
- Improved security co-ordination.
  - A single security model can be implemented such that all applications and services provide users with a common entry point (a single logon) for their specific network management access. Thus, for example, users do not have to maintain multiple accounts, passwords and profiles for different networked systems. This also makes it easier for network management administrators to protect information environment against malicious attacks.
- Reduced design/expansion costs. Electricity networks and their associated telecommunications networks are characterised by an ongoing requirement for gradual expansion and replacement of assets. A large part of the effort for each project to expand the network involves the interface to legacy systems and the collection of data defining existing equipment and configurations. Integrated network management provides readily available and accurate data in a usable format to the designer as it is required. Costly redesign at the commissioning stage is avoided.

This should happen in a comprehensive and consistent manner across all network environments through a unified network management infrastructure, with common directory services, numerous communications options, and intranet and Internet services.

In addition, broader support for networking standards and protocols allows network administrators to integrate new management applications into their existing network architecture, reducing deployment costs and protecting their current investments. It has the following advantages:

- Reduces operations cost and complexity by standardizing on one platform type that share common spares and software management processes.
- Enables greater organisation flexibility.
  - Ability to outsource specialised functions.
  - Ability to monitor performance of outsourced services.
- By consolidated fault alarm and performance management, with single screen network topology views, and a common network management application platform, the IMI provides a common look and feel across multiple systems while centralizing key management functions that simplify and streamline operations.
- Reduces the time and cost required for system integration by providing a common set of standardized interfaces to northbound network management/Open Source Softwares/(OSSs). In addition, seamless integration of new network elements at the element management layer enables rapid deployment with minimal impact to the customer's operations.
- Filtering and alarm correlation capabilities reduce multiple fault information handling and keeps the larger scale of operations manageable.
- Graphical network topology visibility and real-time fault isolation tools provide broader views to network issues for maintainability and immediate problem resolution.

1.5. Market and Technology Drivers

1.5.1. Integration of Services

The borderline between the operational and corporate worlds is blurred in the integrated information flow of the power utility. Information captured or generated in the electrical grid may well be required for asset management, statistics, planning or other non-operational tasks in the utility offices. The diversity and the quantity of the resulting traffic leads to a complex multi-layer, multi-technology architecture with varying degrees of service integration at different levels (wavelength, transmission, multiplex, VLAN or IP), implicating a multitude of distinct management platforms. Consequently, operational and corporate communication facilities cannot be managed or monitored independently and the Load Dispatch Centre is no longer the natural place for the management of the communication infrastructure.

1.5.2. Integration of Technologies

The communication system is no longer composed of a transmission network providing transparent point-to-point channels dedicated to distinct applications. It is migrating into one or several multi-service networks integrating different applications with or without virtual service separation. The borderline between the IT and telecom resources is no longer clearly defined. The SDH transmission and multiplexing network incorporates Ethernet transport, VLAN and switching functions. On the other hand, Giga-Ethernet switches and IP routers incorporate optical transmission, voice interfaces and low speed data multiplexing. The optimized network becomes an assembly of different implementation possibilities which are difficult to monitor separately. This is because the different constituents of the information exchange infrastructure only have access

to the management components of the dedicated equipment (e.g. manage IP network without access to SDH equipment management).

1.5.3. Management Dashboards

The management of the integrated information infrastructure is not limited to fault supervision, diagnostics and maintenance (short-term management) but also “medium- and long-term” actions related to telecom and IT asset management, and network and resource planning. These tasks require access to a completely different view of the infrastructure events composed of statistics and performance indicators (e.g. fault statistics for a type of component or for a geographical region, network and service availability values for different applications or users, time to restore for a given maintenance section, rate of use for a given facility, etc.). Management information must be filtered, processed and presented in different forms according to the requirements of different users.

1.5.4. Multiplicity of Service Users and Providers

Considering the change of scale in the size of the system, several actors are engaged in the provision of communication and IT services. As an example, the proper operation of the telecommunication network depends also upon the availability of power supplies, air-conditioning and site surveillance facilities at the different sites as well as the IT platform constituting its dedicated network management. The “facilities manager” in charge of the proper operation of the power supplies, air-conditioning and site surveillance requires communications to the different sites for remote monitoring access to the facilities, but also the IT platform constituting its dedicated management system. Finally, the IT manager requires communications and power in order to fulfil his duty. In the case of a telecom service provider, the three mentioned actors are all dedicated to a same final product which is “communication services” and are placed in a “Network Operation Centre”. In the case of a power utility, communication service not being the final product, this approach is too constraining and not necessarily feasible. An intermediate platform would be required to present useful indications from the multiple providers to the multiple users. As mentioned previously, an actor can simultaneously be provider of one service and user of multiple services.

1.5.5. Reduction of System Operation Expenditure

Considering the multi-technology nature of the information infrastructure, a single operator cannot have a detailed grasp of all the involved technologies and dedicated management systems. On the other hand, system monitoring and maintenance cannot mobilize permanently a whole team of different equipment and systems experts. It is therefore important to translate network events into generic, easy-to-understand indications allowing a non-specialist network supervisor to distinguish the nature of anomalies in order to assign the resolution of the problem to the appropriate staff (sub-system level) which can in turn forward the problem to an internal or external expert level or return it to the general supervisor if the intervention of another sub-system team is required. This escalation mechanism allows the operator to keep track of the problem solving process at all times and at all levels (e.g. maintenance management) and to clear the event when it has been resolved with the necessary time stamping for the maintenance history and for statistics purposes. This type of mechanism is particularly necessary in the case of outsourcing of system maintenance or during the system’s warranty period.

1.5.6. Event Refinement and Reduction

One of the most cumbersome problems in the supervision of communication and IT infrastructures is the multiple indications of events that arrive at the supervisor desk on

the same management platform and even worse, on different management platforms. In communication networks, a single event can generate tens or hundreds of different fault messages from the same network element, from other network elements in the same site but at different layers (vertical event propagation), and from network elements in the same layer but in different sites (horizontal event propagation). A cable failure can generate indications on the cable monitoring system, but also on the transmission, multiplex and switch management systems. In the case of IT management an event can be indicated tens of thousands of times during a short time interval. The avalanche of event indications in the management system can also hide a completely independent critical event indication. An important function to be performed by an integrated event management system is to refine indications through de-duplication and site correlation. A more elaborate event reduction can be obtained through Root Cause Analysis functions which can help to determine the cause and consequence relationship between received events using a pre-established network model i.e. how do the different components interact, and a network inventory database that shows how the different components in the network are interconnected.

1.5.7. Consumer / Provider Service Management

The integration of multiple user applications into a multi-service network generates the need for the monitoring of the Quality of Service. The “Best Effort” approach to service availability and performance currently used in the fully dedicated communication networks is not acceptable in a shared (and contracted) environment. The organizational changes in the power utility due to the deregulation and the separation of multiple power generation and power distribution entities lead to federating intercommunication platforms generally operated by the national power transmission entity or by an affiliated communication company. This implies that utility communications are no longer purely “internal” and a provider/consumer model is more appropriate. In such a context, communication services delivered to each consumer must be quantified (for service billing) and the quality parameters of the delivered services must be measured to prove the respect of the contractual obligations.

2. Utility Organisation Issues

The power utility information environment is increasingly integrated: information flows from the electrical process level up to the power network and service control level and further up to the utility business management level. Information is used, processed, stored and transmitted at different levels and for different operational and non-operational tasks implicating numerous stages of information processing and exchange infrastructure. Many of the required components can no longer be considered as dedicated to an operational process, but shared between different operational and administrative tasks.

Two types of information flow can be distinguished in the power utility:

Power System Applications information flows are those directly linked to the generation, transmission or distribution of the electrical power. These information flows include electrical parameters and measurements collected in the power system, subsequent substation information generated in the automation components, power network and energy management related information in the control centre, as well as power quality service and metering information in the overlaying power service management layer. Also the business management applications information flow including energy billing and energy trading are included. The management of the process-related information that is performed by specific "Power Network Management" systems is outside the scope of this report.

Auxiliary Infrastructure information flows are those related to the management and administration of associated systems, platforms and devices constituting the infrastructure used for the utility's operational and corporate processes. *This information flows are the subject of the present document.*

The organization of the integrated management information infrastructure depends greatly on the proper organization and mission of the power utility to which it is applied. From the point of view of information infrastructure, at present different situations exist in power utilities as described below. It is important to note that a power utility can meet multiple criteria. Moreover, the situation is not static but rather permanently evolving depending upon economical and strategic imperatives in the company and national regulatory constraints.

2.1. Utilities with Separate IT and Operation Infrastructures

These utilities have completely disjointed infrastructures (communications and processing platforms) for mission-critical operations and for corporate administrative applications. The operational communication infrastructure, dedicated to SCADA, protection and substation telephone applications is therefore mostly composed of low capacity PLC, radio and some optical fibre used as backbone. The management of the operational infrastructure can be centralized at the power system control centre with the mission of providing optimal information exchange and processing facilities towards a single user. The corporate IT facilities are managed separately. However, with the increasing interaction between the two worlds, some level of coordination shall be necessary for certain management functions such as security.

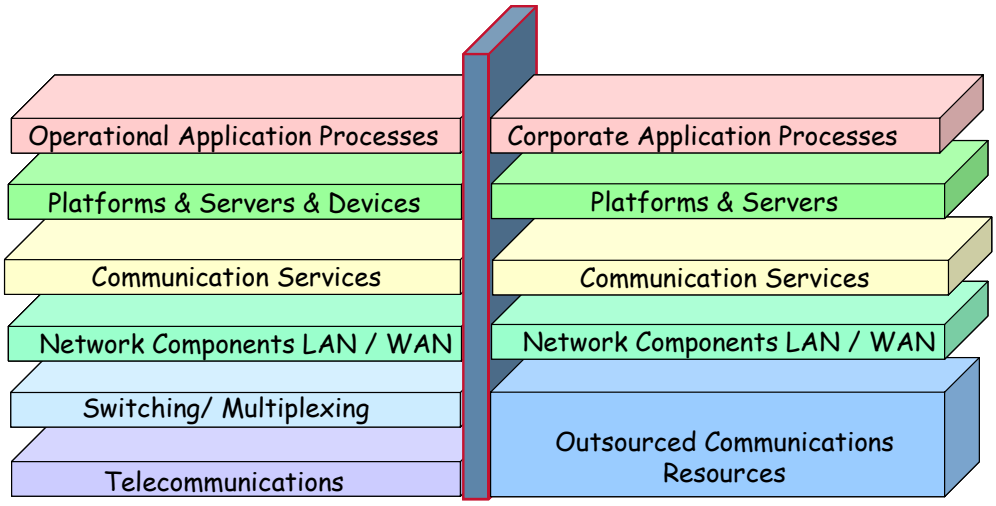

Figure 2.1 Separated IT and Operations Infrastructure

2.2. Utilities with a Common Communication Backbone

Power utilities which have implemented large-scale optical fibre telecommunication backbones serve in general both operational and corporate applications through a complex multi-layer multi-vendor communication network with different availability and fault tolerance requirements for different types of traffic.

The management of the communication backbone infrastructure management tends to be in this case, separate from the power system operation organization which itself may require another layer of infrastructure management for its dedicated assets.

The power system operation and the utility corporate applications have each their own “enterprise network” consisting of dedicated access and interfacing equipment as well as the information processing platforms, servers and devices covering all operational or corporate sites of the utility.

The power system operation is the “priority consumer” and often the owner of the backbone, receiving generally a “carrier-type” communication service.
The network to be managed by the Network Management Centre covers in this case, at the same time:

- a service provider network (backbone) with internal operational and corporate customers.
- an enterprise network using communication services of the backbone entity together with its own dedicated resources in order to fulfil all communication requirements of the utility, as well as the management of the information infrastructure in general.

The management of the corporate IT system beyond the backbone is outside the scope of this document.

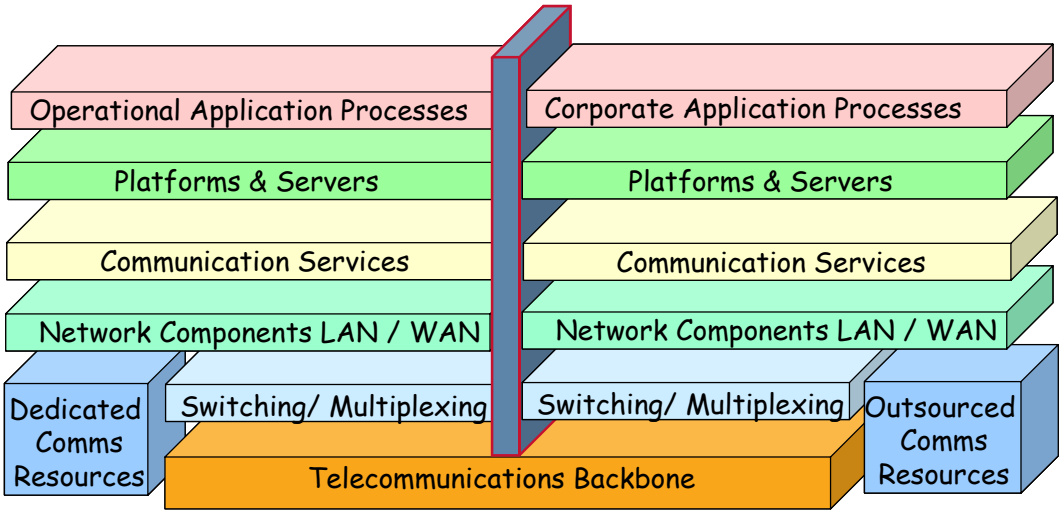

Figure 2.2 Common Communication Backbone

2.3. Utilities providing Communication Services to External Customers

Many utilities take advantage of the potential of their backbone network and the opportunities created by a deregulated environment for proposing some level of communication service to external customers. The extent of this operation depends upon the market opportunities and the level of investment, engagement and risk that the utility company is prepared to accept. This diversification influences greatly the organization and therefore the management of the communication infrastructure.

The backbone service provider becomes a separate commercial entity serving a great number of customers and requires competitive pricing, contractual engagements (Service Level Agreements), Customer Care services and Billing facilities.

The responsibility of the Utility limits to the provision of the contracted services with some means of measuring the service which is provided (metering), permanently monitoring the quality of service for each customer (QoS monitoring), and proving that the contractual requirements are met (SLA monitoring). Moreover, customer relations would require the identification of customers and services which are impacted by an infrastructure anomaly and some means of customer notification. Consequently, a service management layer becomes highly desirable, or mandatory, in this case. This task, which can be relatively primitive when the provided services are limited to dark fibre or E1 circuits, becomes more elaborate for higher layer service provision such as Ethernet transport or IP connectivity.

2.4. Utilities with a Separate Service Provider or Outsourced services

In the previously described case of a communication backbone service provider with external customers, the proper applications of the power utility lead to constitution of separate “enterprise-type” infrastructures for corporate (utility office users) and operational (power system) users. The backbone provider is a Telco entity and is unlikely to cover the management of Utility operational resources with a blurred border between communication and application e.g. protection signalling, SCADA, etc. Even if the management of the two entities is collocated with some synergy between the two, it is likely that different organisations are to be differentiated functionally and their needs

must be considered separately: a service provider organisation and a corporate enterprise network organisation.

This situation closely resembles the case of utilities which outsource their communication services to one or multiple external communication service providers.
The management requirements in both internal and external outsourcing are not only the supervision of the owned infrastructure, but also the monitoring of the Quality of service which is being delivered by the service provider.

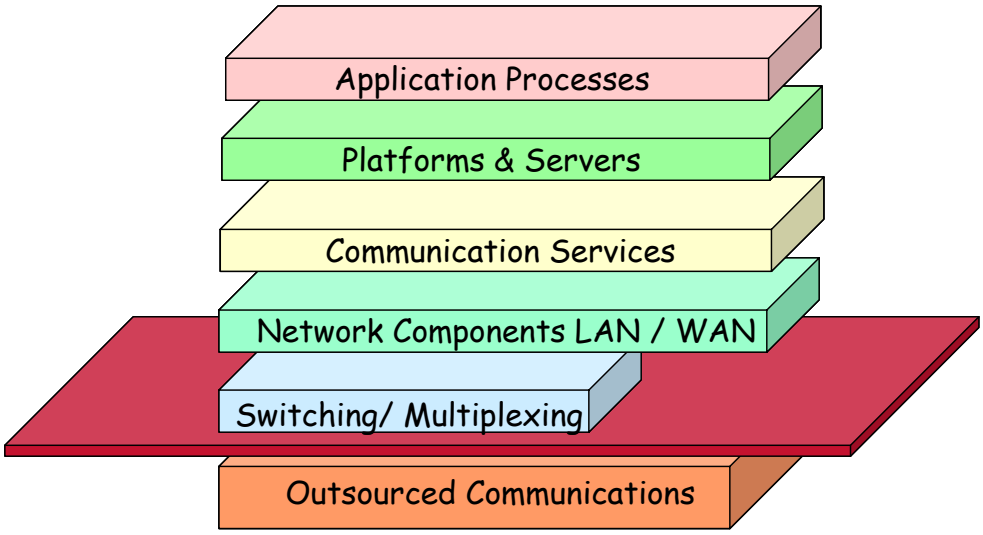

Figure 2.3 Outsourced Commmunications

Moreover, the present trend of external providers to replace dedicated channel leasing by packet-oriented services such as IP network or Ethernet transport renders critical the monitoring of the Quality of Service as described in the following paragraph.

2.5. Utilities with a multi-service operational and corporate IP network

IP convergence simplifies utility communications, provides flexibility and allows a more economical approach to system design through service integration. However, it also generates a number of problems that must be addressed by the management centre.

- Communications become more critical due to the risk of simultaneous loss of all services at one site.
- Quality of Service depends upon system's load and is therefore variable. The permanent monitoring of Quality of Service is essential.
- Undetected network anomalies like faults, traffic or routing problems lead to degraded network performance rather than service unavailability. It is therefore essential to detect and remove anomalies which may otherwise persist for long periods.
- Communication network and IT platforms and servers are closely linked together and no longer distinct layers. They must be managed in a consolidated manner.
- Security management is no longer limited to the IT platforms but extended to the whole communication infrastructure.

- Communication services are no longer provided through a unique layer of infrastructure. They can overlay multiple infrastructure layers e.g. voice service through classical PABX and VoIP in the same network, TCP/IP SCADA through Ethernet switches and EoSDH. Consolidated service management is not just “nice-to-have” but mandatory.

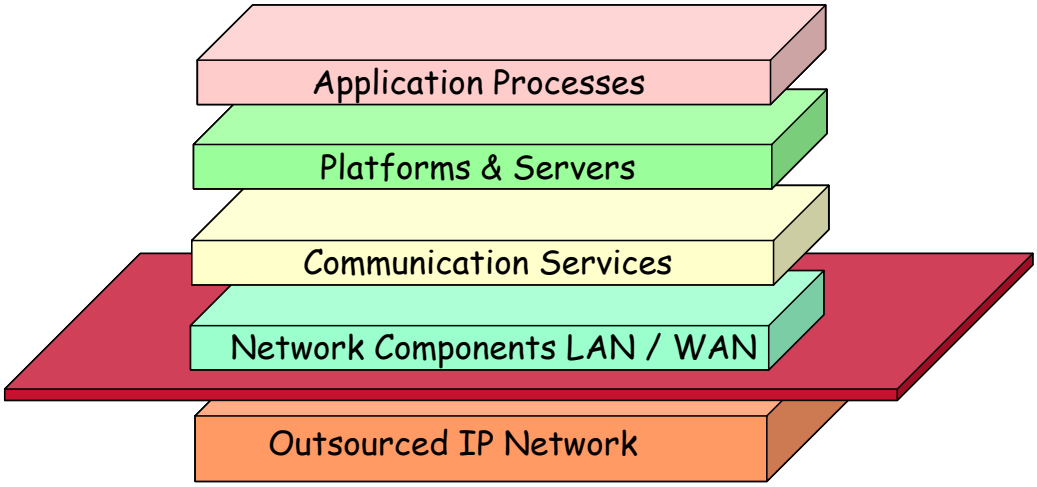

Figure 2.4 Multi-service IP Network

2.6. Utilities moving towards the fusion of IT and Operational information infrastructure management organization

A number of power utilities are adopting an even more integrated approach in which not only the communications, but also the overall management of IT and operation infrastructures are being integrated. This approach takes account of the fact that the borders between the operational and utility office applications are increasingly disappearing. In this case, the common infrastructure includes an important part of the processing platform which may even be managed externally. Security management, service management dashboards, quality of service monitoring and system monitoring become important components of the management organization. SLAs must be monitored for the different users of such a multi-service system.

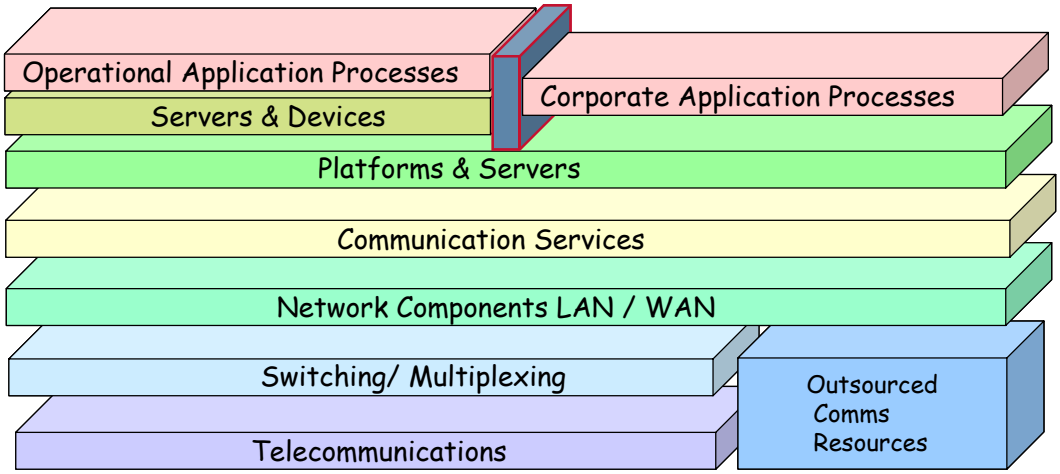

Figure 2.5 Merged IT and Operational Infrastructure

3. Management Service Model

3.1. Modelling Processes and Services

The power utility management can be modelled as a number of management processes as described previously which interact in order to fulfil the overall mission of the organisation. Each management process may be further expanded into multiple interacting processes.

A process is materialized over an IT platform which covers a certain geographical zone through distributed processing or simply because its actors or end service users are dispersed across the geographical zone. The different components of the platform and its service users interact through the communication network.

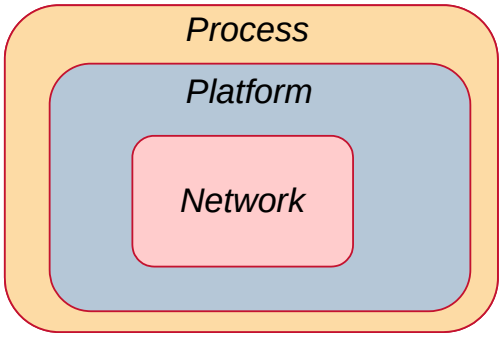

Figure 3.1 – Process, Platform and Network concepts

Even if the following description can also be applied to the business processes of the power utility, defining in this way “service management functions” for each of the activities of the power utility (substation management, power network management, energy management, etc.), the present report is not concerned with these core activities but rather with the network infrastructure and the IT services associated with the core business activities.

The different processes interact through services. A process can be characterized through its actors, its assets and its information flow. It receives at its input a number of services and it provides at its output one or many services. A service, seen by its consumer, is characterized by its attributes which may be quality, continuity, availability, security and cost. The service seen by its provider may be characterized by the service level engagement and price.

It is indeed necessary that the service expectation at the consumer end meets the service delivery at the provider end. Moreover, it is part of the process management to assure that the services obtained at its input allow the provision of the required service at its output. The cost of the consumed services, in addition to the implicit costs of the process (actors and assets used) shall determine the pricing policy for the service at the process output.

The process owner shall further provide an access point to its service consumers for query and shall provide indications on the provided service. This access point is generally referred to as a “Service Desk”. The service consumer, in its turn shall require a way to measure the received service both in quantity and in quality in order to check whether the service level engagement is met by its provider and that the pricing is appropriate.

The management of the process consists of the management of the implicit attributes of the process, actors, assets and information flow, the proper management of the services which are provided by the process, and monitoring of the services used by the process and their influence on the provided services. This general model is presented in the following figure.

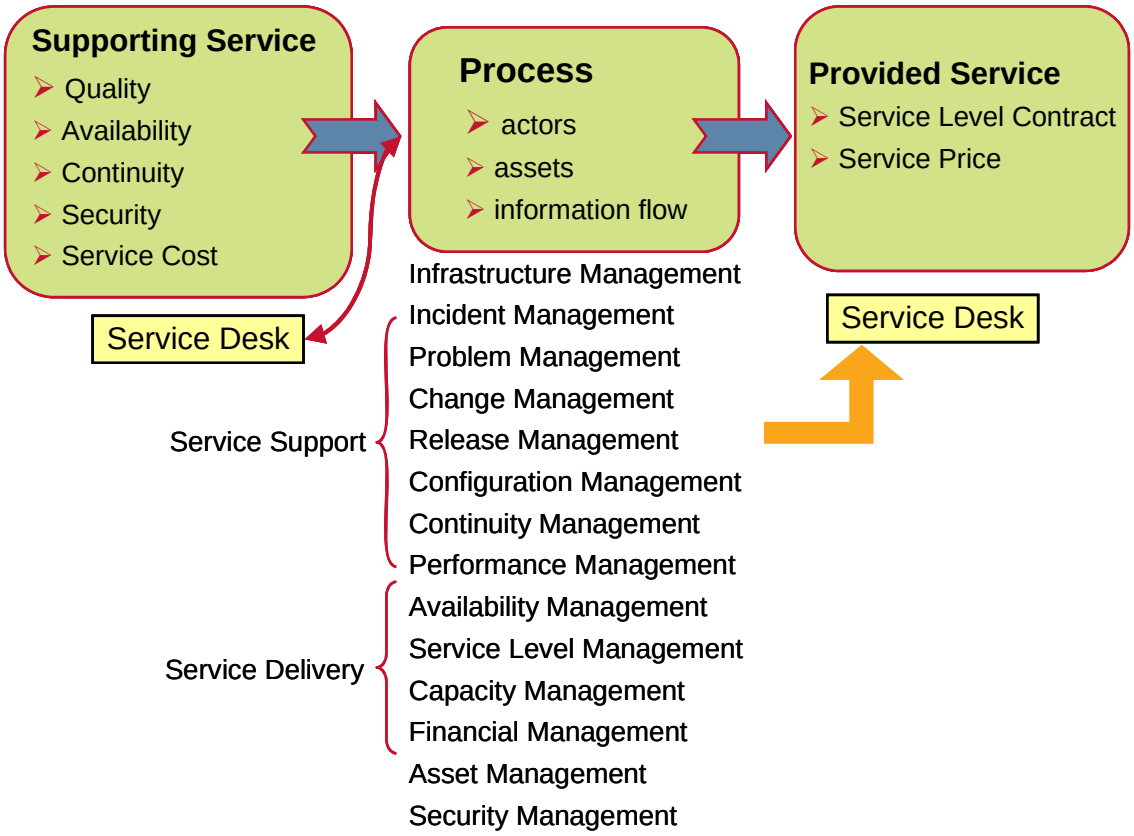

Figure 3.2 – IT Service and Infrastructure Management Process Model

3.2. IT Service Management Guidelines and Standards

One major initiative in the field of IT management has come in the late 80's from the UK Central Computer and Telecommunication Agency (CCTA) incorporated at present in the Office of Government Commerce (OGC). A set of best practices published under the name of IT infrastructure library (ITIL) gives a very exhaustive account covering different aspects of Service Support, Service Delivery, Infrastructure Management, Security management, etc.

ITIL has been the starting point for the IT Service Management Forum (itSMF), an independent, non-profit forum of IT service management professionals worldwide since 1991, with over 2500 member companies at present. It provides an accessible network of industry experts, information sources and events to help addressing service management issues.

The British Standard BS15000 is the first standard specifically aimed at IT Service Management. This standard was used to define the international standard ISO/IEC20000 completed in 2005. As with BS15000, the ISO/IEC 20000 describes an integrated set of management processes for the effective delivery of IT services aligned with and complementary to ITIL. It is composed of a Formal specification (Part

1) and a Code of Practice (Part 2). ISO/IEC 20000 (and BS15000) allows organisations to be audited and certified. It does not specify or certify tools and technology.
ITIL is not a standard, but rather a set of guidelines for a structured, common-sense, process-driven approach to ensure close alignment between IT and business processes. It recognizes that there is no universal solution to the process design and implementation for the management and delivery of IT services. As such, tools cannot be “ITIL compliant”, but management processes and organisations can be assessed through ITIL. Through its scalable and flexible “adopt and adapt” approach, ITIL is applicable to all IT organizations irrespective of their size or the technology in use.

3.3. Service Management Components

The following diagram, adapted from the ITIL model, represents the main components of the power utility’s ICT management. It includes both the activities related to the management of the infrastructure and the management of the services. The different management processes are more oriented towards the service users, customers and the ICT service provision business e.g. the provision of service indications, a service desk for incident management, service billing, or oriented towards the technology e.g. the asset management of the infrastructure, planning of infrastructure extensions and changes. Certain processes such as the planning of new services or security management can be considered as both technology-oriented and user-oriented.

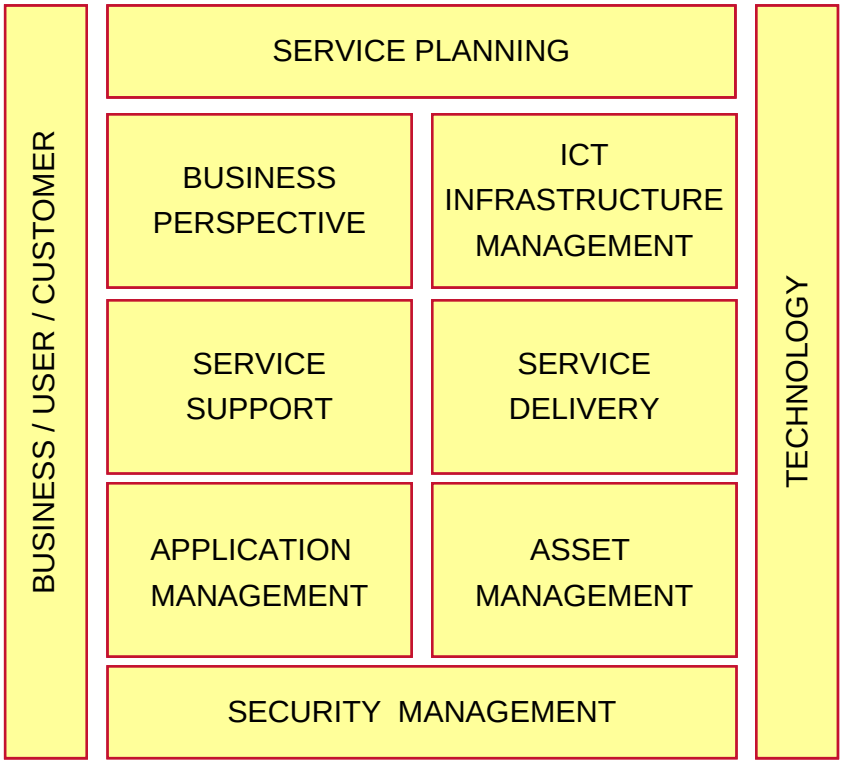

Figure 3.3 – Power Utility ICT infrastructure and service management processes

The most basic process of IT management is the technical supervision, maintenance, monitoring and operation of the communication network and the IT platforms constituting the information infrastructure of the utility. It includes the different activities of Telecommunication Network Management and the management of platforms,

servers, intelligent devices, and auxiliary components of the Utility system. A schematic figure of the managed components is given in figure 3.3. The different components generally provide different levels of management information through interfaces ranging from simple alarm loops, flat ASCII files and system logs to SNMP traps, ITU-T TMN interfaces and CORBA. Many different dedicated management systems are generally employed allowing to perform fault and performance management on the constituents, to configure different equipment or to monitor usage of resources providing in this way the first elements of accounting management e.g. resource usage and security management such as passwords and access rights. The present trend is to federate the different dedicated management systems through a common management layer for the ICT infrastructure. The configuration management described here under provides a centralized documentation system allowing storage and visualization of a layered view of the different elements of the infrastructure. This is a particularly useful means to assure the coherence of the different management actions taken at different levels of the ICT infrastructure. The different management functions of the Network and platform management at this level contribute into the more general functions of the IT management as described here after.

3.3.1. Service Support Process

Service Desk Function – The service desk function is the “user-visible” part of the whole process of service support. It provides a point of contact to the IT service provider for the different users of IT services. It is often a web-based facility allowing the IT service user to have on-demand or pop-up access to dedicated information on the state of the service that the network service providers are delivering, and the possibility to notify an incident to the service provider. Different user dashboards are made available depending upon the profile of the management service user.

Incident management – Incident management is the process of clearing network and system events typically by identifying the concerned staff, directing the events to adequate persons and launching the escalation process for the clearing of the incident and restoration of normal operation.

Problem management – Problem management is the complementary process to incident management. This process allows analysis of incidents in order to determine the Root Cause, analyze infrastructure events before they result in user-visible incidents, examine recurrent events and incidents and propose appropriate modifications and configuration changes to avoid them.

Change management – The power utility ICT is a very dynamic environment. It changes frequently to cover power network extensions and modifications, new users, new applications, service upgrades and capacity enhancements. Wherever be the origin of change (power network, application processes, communications or IT platforms), it implicates changes in the other constituents. Change management is the process of standard handling of changes through adequate procedures and tools in order to conserve the coherence of the system. Moreover, the process of change management allows the user to program and coordinate multiple modifications into the network or the infrastructure when several projects are concurrently implemented. It is in permanent interaction with other processes such as configuration management, service planning and problem management. A centralized client-server documentation system, which can be the basis of a configuration management database (CMDB) or asset management system, can be made accessible to all IMI actors and is a useful

tool for effective change management and its coordination with other management processes.

Configuration management – This process is closely linked with the asset management process described in the following sections. It allows the user to keep track of all components of the IT infrastructure, their respective configurations and details. It permits the user to see how the different constituents are interconnected (network and system inventory). The configuration management through its documentation system allows the user to visualize the system on physical and logical perspectives.

Performance management – This process allows the user to monitor the obtained performance of each part of the ICT infrastructure and to detect resource saturations, anomalies and dimensioning problems of the different resources of the ICT infrastructure.

Service Continuity management – The task of the Service continuity management process is to implement Fault Tolerance into the system and to devise a Disaster Recovery plan for the critical parts of the utility's IT infrastructure. In this way an adequate level of minimal service can be maintained and/or restored rapidly in the event of major catastrophe.

Release management – This process ensures that the different constituents of the system are coherent and uniform. It allows the user to drive the decision of release changes in a concerted manner and after necessary validations. It also allows the system to be kept updated, extendable and compatible within its constituents during its lifetime.

3.3.2. Service Delivery Process

Service Level management - The IT service provider's focus for the different service users of the power utility is to provide them with a certain level of service depending upon the requirements of each application. This engagement is increasingly formalised through a Service Level Agreement, whether the IT provider be internal or external. The process of Service Level Management allows the user to check continuously whether the agreed provision of quality, throughput, delay and availability are met. It allows the provider to determine the criticality of an incident depending on the users which are concerned and considering the past incidents on the service delivered to the user.

Availability management – This process allows monitoring of the availability of the constituents of the infrastructure through the different fault management systems and the determination of the availability of each service through the association of different component faults.

Capacity management – In relation with the asset management and the configuration management, the capacity management process allows the performance of physical and logical resource management of the communication network and the IT infrastructure in general. It examines the load of different IT resources determining which applications are using a particular processing resource, or which communication services are carried over a certain network resource. The capacity management is in charge of VLAN and VPN management on the multi-service communication network.

Financial management – The need for control of service costs within Power utilities is increasingly important. Investment in system and network extensions and the maintenance of an extensive ICT infrastructure is a costly process that necessitates a precise control over the costs and their transfer to the different groups of IT service users in the utility. The translation of supporting service costs and implicit costs of the infrastructure into a service pricing policy is the task of the financial management process.

3.3.3. Service Planning Process

New communication and processing services are permanently being considered and implemented into the power utility. The process of Service Planning allows the definition, specification and implementation of new services and assurance that the necessary infrastructure components are purchased and installed in order to support these new services. In this manner it interacts with other IT management processes. As an example, the implementation of Voice over IP telephony (VoIP) in a power utility requires prior implementation of its platform for infrastructure management, the capacity planning and management of the IP network and service cost determination and management, as well as a business plan to justify the return on investment.

3.3.4. Asset Management

Asset management and inventory activities produce up-to-date and coherent documentation of the whole ICT system (network, platforms and users), available on-line to all concerned parties and in particular to all other management processes described here. The documentation shall include details of all components constituting the infrastructure (identification, type, location, status, maintenance history, etc.). It can furthermore track all configuration changes in the past and programmed in future in collaboration with the change management process.

3.3.5. Business Perspective

Business perspective is the process that analyses the changing requirements of IT users and allows in this way to define IT changes, extensions and new services to be implemented. It allows the alignment of service delivery and support with the customer expectations. This process determines the economic feasibility and return on investment of new services considering the required infrastructure and application expenses.

3.3.6. Application Management

Application management is the process of defining, specifying, implementing and following different IT applications through their entire lifetime up to their withdrawal. It is a process that must interact with the different processes defined here and constitutes the frontier with software development engineering.

3.3.7. Security Management

The Security Management process produces the Utility’s security policy and assures that the security policy of the power utility is respected. It allows the operator to supervise network, system and data security against attacks, intrusions and viruses, to take appropriate blocking and isolating measures and to inform the different IT users through the service desk and user dashboards.

3.4. Management Architecture

The management services are organized into a four layer hierarchical architecture by the ITU-T as described hereafter. Even if the four-layer BSNE-ML model (Business-, Service-, Network-, Element- Management Layer) has been devised for telecommunication network management services, the conceptual model can be adopted for other information related infrastructure management in the power utility environment.

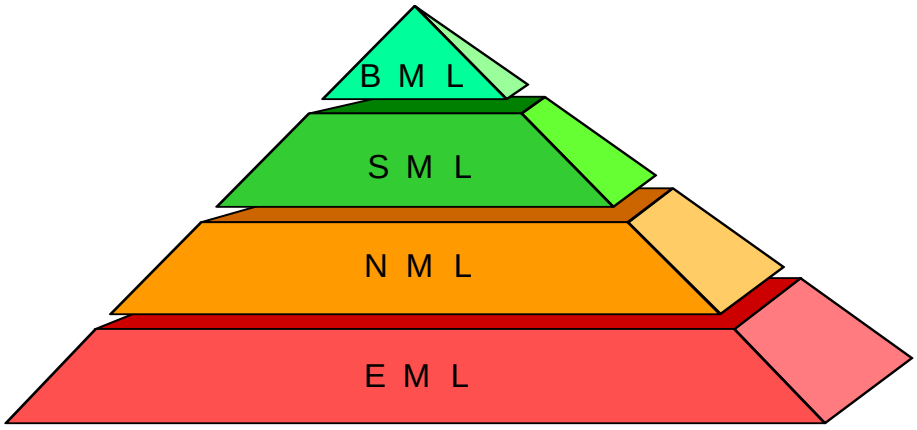

Figure 3.4 ITU-T Management Model

3.4.1. EML (Element Management Layer)

This layer consists of the management of individual equipment. It covers the different tasks related to the maintenance, administration, logging of usage and statistics on the events recorded from this equipment.

3.4.2. NML (Network Management Layer)

This layer consists of the management of a group of interconnected equipment performing a particular task. It can be assimilated to system management with end-to-end overall functional and performance requirements. The task of this management layer is therefore to interact with each component of the system whether aggregated together or geographically dispersed in order to control and coordinate their operation for the proper functioning of the system, to assess the utilisation of the system by authorized users and to reconfigure it if necessary in order to fulfil the system's requirements.

3.4.3. SML (Service Management Layer)

This layer consists in the management of a whole service delivered to a group of users e.g. switched voice service or SCADA service, through the monitoring of one or many different systems or networks. It manages the interfacing between the service users and service providers through personalised service availability indications, the measurement of the Quality of Service, the monitoring of Service Level Agreements taking necessary measures in order to meet the pre-established SLA, and the billing of the services.

3.4.4. BML (Business Management Layer)

This layer consists in the management of a whole business which may comprise multiple services e.g. operational communications, third party communications, corporate IT infrastructure or control centre facilities, with overall management and/or enterprise responsibility. Business oriented statistics for system & human resource

planning and budgeting and for the elaboration of executive master plans are typically at this layer.

3.5. Management Functions

In a similar manner to the four layer BSNE management service architecture, the model for management functions to be performed has been derived from the world of telecommunications and adapted to the requirements of the power utility's information infrastructure management. The FCAPS model (Fault, Configuration, Accounting, Performance, Security) covers the different functions that may have to be implemented for the information infrastructure management.

- ***Fault Management (FM)***
  - Alarm collection and processing
  - Fault event indication to users
  - Trouble Ticketing
  - Maintenance organization and fault escalation
- ***Configuration Management (CM)***
  - Addition, suppression and modification of equipment, systems, channels,
  - Provisioning and configuration of new services,
- ***Accounting Management (AM)***
  - ticketing and billing for the utilization of equipment, systems, network or services by different categories of internal and external users
- ***Performance Management (PM)***
  - monitoring of performance parameters for each service, system or equipment
  - statistics and trends for planning purposes and proactive measures
- ***Security Management (SM)***
  - access control to facilities, services, devices, etc

A non-exhaustive list of management functions organised according to the described service architecture is present below:

	Fault	Configuration	Accounting	Performance	Security
Element	Maintenance, Supervision, Spare Management	Parameter setting and recording of equipment, Change management	Monitoring of equipment usage	Equipment perf. monitoring, Condition monitoring, Preventive maintenance	Equipment access monitoring, Password management
Network (System)	Network Management, End-to-end system analysis,	Group configuration of multiple elements constituting a system / network	Billing of the usage of a system or a network	Network or system performance monitoring, QoS monitoring	System and site access monitoring,
Service	Service availability, QoS monitoring, Service Impact analysis	Service Provisioning, Configuration of new services into the network	Billing of voice & data processing, storage and exchange services	Service Monitoring,	Operational and corporate IT platform security management,
Business	Fault statistics, OPEX estimation SLA monitoring	----------	Utility-wide internal IT service billing	Service Contract Management, SLA Monitoring,	Utility-level security engineering

3.6. Management System User profiles

The specification of a Management system requires prior definition of the different categories of users that may require output from the system and the nature and form of information that each category of user shall expect to receive. An exhaustive definition of the so-called “User Profiles” is part of the system requirements analysis to be performed in close collaboration with the relevant utility staff, and in relation with the organizational aspects.

As described in the previous sections, a management system user may be a service provider or a service user depending on the different service layers and may therefore need different types of management information depending on the services for which a person who may be a provider or a user.

The following table gives a non-exhaustive list of different user profiles for management information together with the type of information and functions that they may require. It may be extended, constrained or modified according to the utility’s management organization and the perimeter of the system to be implemented. It is important to note that the following profiles are purely functional and in practice the same person may correspond to multiple profiles or inversely a defined profile may be further split into multiple roles in a utility’s organization.

Utility Function	Management System User	Required management information & capabilities
System Supervision	Telecom Backbone Supervisor	Alarm information from different telecom network elements Standard generic information without distinction of the manufacturer (e.g PABX major alarm) Secondary information concerning the fault-generating element (network position, manufacturer, etc.) Capability to move across the network layers in order to locate the fault (cable, transmission, switching, multiplexing, etc) Capability to transfer the event ownership to maintenance staff (maintenance specialist).
	Power System Communication Supervisor	Same as above, but for the telecom components owned and used only for the process control communications of the power system.
	Control Centre System Engineer	Information from the EMS servers, workstations, and networking components concerning status, events and load Event information concerning communication service interruptions and quality of service Event information from IT security management system. Make system event information available to Control Centre Operator.
System Maintenance	Telecom Maintenance Engineer	Remote access to Dedicated Management System for the faulty element for more detailed information (board level, etc) and perhaps remote configuration setting. Communication access to the O&M operator Event Acknowledge or transfer.
	Control Centre Maintenance Engineer	Access to management function of different system components for more detailed information and parameter setting. Communication service information (status, quality, etc.) Event Acknowledge or transfer.
	IT platform maintenance engineer	Remote access to Dedicated Management System for the faulty element for more detailed information (board level, etc) and perhaps remote configuration setting.
	Maintenance Manager, Maintenance Contract Manager	Fault statistics and service downtime for each system, region, contractor, etc.
System Administration	Corporate Network Administrator	Communication Service Availability and Quality of Service information Service interruption indications indicating concerned sites IP Network availability and loading Status and event information on the components of the corporate communication system (LAN/WAN, Switch, Videoconferencing and multimedia facilities, etc.)
	Voice Network Administrator	Voice service availability, grade of service, limitations and facilities available for each user.
	IT Network Administrator	Event and Monitoring Information from the different servers, workstations and LAN/WAN components of the network Shared system load information, and network configuration Access to Dedicated Management Systems and direct access to the managed components Event information concerning communication service interruptions Send service information to all or privileged users

Utility Function	Management System User	Required information & capabilities
System Security	Corporate System Security Engineer	Intrusion attempts and attack information from Firewalls and different security devices Information on the current configuration of the computer network and the status of different security barriers and networking components Information on different access requests in the intranet, communications to and from outside world, Access to the Dedicated Management Systems, Event information from related computer monitoring systems, Transmit security event information to System engineers at different sites.
	Operation System Security Engineer	Same as above but for the Operation system (control centre and substation platforms).
	Site Security Officer and Facilities Manager	Access to information from different site surveillance systems and intrusion alarms, Access to Housekeeping alarms collected by the telecommunication devices at all sites (e.g. Repeater sites) and available in the dedicated telecom management systems, Event information from related monitoring systems.
Asset & SLA Management	IT & Communications Asset Manager	Statistics and synthetic information on the availability and fault rate of the different system components Service Restoration Time and Service Level Agreement Monitoring information for outsourced services Loading and rate of use information for shared resources
	Telecom Contract Manager	Quality of Service, throughput, Service Restoration Time and Service Level Agreement Monitoring information for contracted communication services
System Users	Control Centre Operator	Communication Service Availability and Quality of Service information Service interruption indications indicating concerned sites EMS Server and network availability and loading
	Protection Engineer	Service indications for communication services (PLC, fibre, E1, etc.), status information for protection resources (protection relay, protection signalling equipment, etc.)
	Power System Asset Manager and support	Statistics and synthetic information from Device Condition Monitoring Systems (Transformers, Breakers, Transmission Lines, etc) Statistics and synthetic information from Protection and Control Monitoring Systems (Protection Relays, IEDs, Transducers, etc.)
	Administrative User	Service indications (voice, data, etc.)
	Substation Control Operator	IED and communication information concerning the substation.

4. Management System Architecture

4.1. Management components

The management system can be considered in term of three key elements, agents, mediation devices, and the management centre.

4.2. Agents

An agent is an application entity that is capable of acting with a certain degree of autonomy in order to accomplish tasks on behalf of its user. An agent is defined in terms of its behaviour. For example, an SNMP agent gathers internal alarms of the system where it is embedded generating traps to the management centre to report them.

The agents can be distinguished from other programs because of its main characteristics:

- Reaction to the environment. Agents are normally programmed to control or react to changes in their environment, making decisions based on logical equations or with artificial intelligence.
- Autonomy. Agents do not need any other application to perform their tasks.
- Goal-Orientation. Agents perform their tasks to achieve a goal.
- Persistence. Agents do not need to be activated or called by any other procedure to perform their tasks.

Network management systems may be based on the agent paradigm. Management tasks are controlled from the network management centre. Management tasks are broken down into simpler tasks that are delegated to agents installed in managed objects. These agents perform these tasks autonomously so they continue to carry out these tasks even in the event of loss of communication with the management centre. This approach increases the robustness and survivability of the system assuring that basic management functions will keep its operation in spite of major outages in the management system.

4.2.1. Mobile agents

Mobile agents are programs that can migrate from host to host in a network, at times and to places of their own choosing. The state of the running program is saved, transported to the new host, and restored, allowing the program to continue in the same point and status that has when it left the previous host. Mobile agents differ from ``applets'', which are programs downloaded as the result of a user action, then executed from beginning to end on one host.

Mobile agents are an effective choice for many applications since they improve latency and bandwidth of client-server applications and reduce vulnerability to network disconnection. Although not all applications will need mobile agents, many other applications will find mobile agents the most effective implementation technique for all or part of their tasks.

Network management systems have to deal with the collection of a big amount of data stored in heterogeneous environments. The problem with information flooding a network in the case of malfunction is particularly severe if we take into account that the fault has to be diagnosed and found quickly. This is especially relevant in medium and

large networks. There are several research works that propose the use of mobile agent to carry out some management task. Nevertheless, practical results are scare. Research outcome suggest that mobile agent technology will become very useful, and perhaps even critical, in many areas of system and network management.

The main advantages of the mobile agent approach are:

- Reduction in network traffic
- Better real-time performance. Being closer to the real-time system prevents delay that may be introduced by a congested network
- Support for heterogeneous environments. Agents are implemented in Java code.
- Easy software upgrade.

On the other hand, that are many concerns due to the lack of control of the user, and security concerns related with viruses as well as the difficulty of combining mobile agents with a standard security architecture based on firewalls.

4.3. Mediation devices

The concept of Mediation Device (MD) was formerly introduced in the ITU-T TMN architecture in the recommendation series M.3000. The same concept can also be applied in other heterogeneous management scenarios.

A mediation device provides management information interfacing between TMN physical blocks that incorporate incompatible communication mechanisms. A Q-mediation device (QMD) is a physical block that supports connections within one TMN. An X-mediation device (XMD) is a physical block that supports connections of Network Elements (NEs) with different management architectures. A QMD is a box with different Q interfaces whereas a XMD is a box with Q and other management protocols able to implement gateway functionality for the management information and services.

The Mediation Devices (MD) can be used to provide mid-level management services that represent aggregate behaviours of groupings of the network elements supported by the NE and Q Interface Adapters. A Mediation Device may block, store, adapt, filter, threshold and condense management information. For heterogeneous networks it will also provide protocol and data format translation. A MD includes a management agent able to support all the management function of the network.

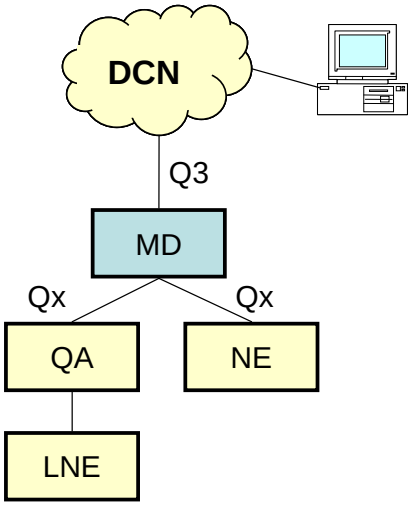

Figure 4.1 TMN Physical blocks

The figure shows the main building blocks of the TMN architecture. The role of the MD as well as the interfaces between the managed elements or Network Elements (NE) and the Data Communication Network (DCN) that provides the connectivity between the NE and the management centre are also shown.

The Q3 interface defines the interconnection point between the managed network and the DCN. The Q3 interface protocol suite is defined in the ITU-T recommendations Q.811 and Q.812. It represents the Common Management Interfaces Service Element (CMISE) interface between the participating elements of the network.

The Qx interface is a lightweight version, intended to facilitate the development of agents in situations where the complexity of providing a complete CMIS based MIB isn't feasible. This interface is typically found between the MD and supporting NE and Q interface Adapter (QA) whose main function is to connect non-TMN network elements.

4.4. Management Centre

The management of a Multiservice network is a complex task which requires a network-wide view and specific applications to carry out maintenance and management works.

From the perspective of a service provider, whether internal, external or both, the challenge of maintaining serviceability can only be achieved with the aid of complex tools that provide a set of maintenance and management services.

The management centre is formed by the equipment and applications that gather management information in a consolidated database and the applications that provide management and maintenance services.

The complexity of a management centre depends on the size of the network, the number and the type of services integrated. In consequence, the size can range from a single PC to a farm of servers, running few applications or hosting a management database and vertical applications that provides very specific services.

The key issues to consider in the design and operation of a management centre are:

- **Serviceability**. It is a function of the operational requirements of the services. It will determine the availability requirement of the control centre.
- **Architecture**. It is a function of the availability requirements, security specification and the type of applications that will run on the control centre.
- **Service access**. It is a function of how the management and maintenance personnel use the management centre services and applications, how customers access service information and how service reports are transmitted to customers and managers.

4.4.1. Serviceability

The management centre is a necessary component for service provision. Its criticality depends on the network design criteria. When the network has spare capacity to cope with outages and auto-recovery procedures, the availability of the management centre is less critical but when service recovery has to be carried out manually, the availability of the management centre becomes more critical.

When the network is integrating critical operational services, or it is providing services to third parties with very high availability requirements, the management centre availability must be able to scale up to 99.99%. This implies that the management centre has to be implemented with a fault-tolerant architecture. In general, the availability of the management centre has to be of the same order of magnitude of that required by the most demanding service managed by the centre.

4.4.2. Hardware Architecture

The hardware architecture depends on the complexity and the availability requirements of the management centre.

- The architecture of an "*emerging*" management centre use to be formed by a collection of PCs equipped with proprietary applications and connected with the managed elements by means of dial-up modems that uses public or private telephone network to access managed elements. This is a cost-effective solution when there are few elements to manage. Nevertheless, it does not scale and would become expensive and non-serviceable when the number of elements to manage grows.

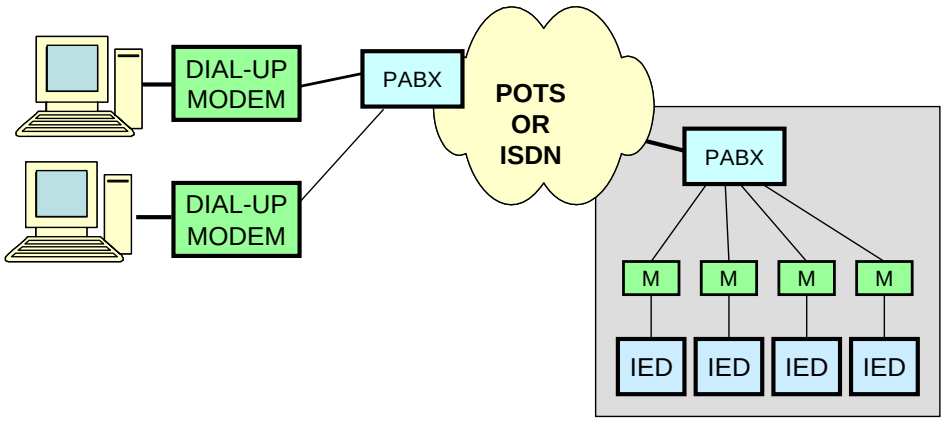

Figure 4.2 Emerging Management Centre

- A mid-size management centre may be formed by a server with redundant power supply and mirroring hard disks working in RAID configuration. The size and

configuration of the server depends on the availability requirements. The server is normally connected to a LAN and uses a router to access managed elements. Further operator terminals can be implemented using X-terminals. The scalability of this architecture is also limited to a mid-size network and few operators.

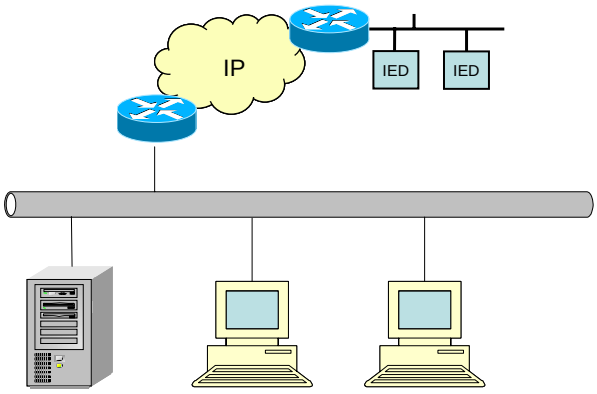

Figure 4.3 Mid-size Management Centre

- Critical management centre. This architecture is normally required when the management centre controls a large system which provides services to third parties. Due to the high availability requirements, fault-tolerant architectures are required. This implies that the system is formed by redundant servers configured in hot standby mode equipped with redundant communication interfaces and connected through two independent LANs to the rest of the system and the routers which allows access to the managed elements. In function of the size of the system there may be several independent servers, one for the management database and the rest for the applications.

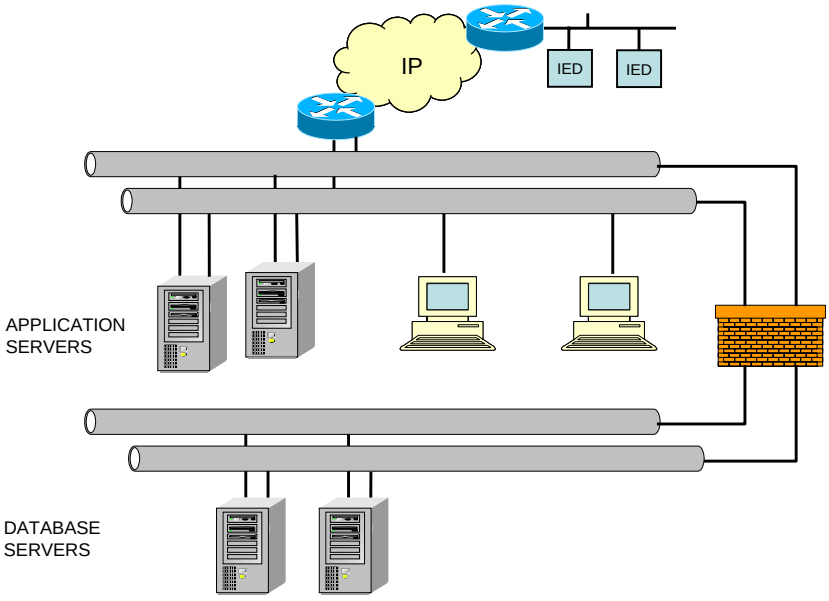

Figure 4.4 Critical Management Centre

4.4.3. Application architecture

Multiservice networks require “Service Delivery Mechanisms” which are applications that exert control over access to network services, service performance, compliance of SLA, billing and other functions that have to be performed in real-time.

The management architecture dictated by the market products comprises the following managing applications which includes an specific node management view that is not specifically described in the ITU-T model but required by the practical management of network infrastructure and included in the ITU-T element layer:

- **Element Management Applications -** The term element refers to every single component within the network. This is the simplest management action like, for instance, the management of an interface port. Element management is the basic function of management for both service provider and large-scale enterprise networks. Day-to-day operations are carried out using element management tools to assist in a variety of functions such as commissioning, database backup and restoration as well as network administration. By means of element managers with graphical User Interfaces the Network operator is able to save training and personnel costs. This allows streamlining of operational procedures and enables efficient operation of large network environments.
- **Node Management Applications -** It includes all the management actions that operate at node level to provide the support for the provision of services. The complex management operation involved in the management of a multiservice network requires powerful node management functions to allow profitable, cost-effective and timely network service to be deployed. Billing, accounting and provisioning are the most critical functions to achieve service commitments. These applications can only achieve a real time performance when advanced node configuration, monitoring and fault management functions are provided.
- **Network-Wide-Management Applications -** It provides a network-wide view of the network performance which allows overall operations to be carried out. The challenge of these applications is the provision of a consistent view of the services over the whole network since the network is normally formed by a multi-vendor platform with an internetworking architecture formed by a number of different technologies.
- **Service Management Applications -** It provides the means for service activation, for maintaining the level of performance of the services. One the most important function of a network management centre is the ability to rapidly and cost-effectively create and deploy new services to very large numbers of customers. The main functionality of a service management application is to maintain customer’s related information, and assists in implementing service specific configurations over the underlying network infrastructure. Modern Service Deployment and Management Systems offer the following functionality:
  - Service creation
  - Service activation
  - Customer management and
  - Accounting capabilities.

  Customers may be provided with mechanisms for:
  - requesting new services
  - indicating specific needs that will support applications and services including:
    - Multicast audio and video applications

- Video streaming applications
- Voice services
- Interactive gaming
- Variable bandwidth (“Turbo button”)

Application architecture will be a function of the network size, its complexity, the number of services provided and the business model to be implemented.

The most relevant application architecture requirements are:

- **Scalability**. The degree of scalability of the management centre has to be similar to the scalability of the network managed. The scalability is basically a function of the architecture of the different software modules and their interfaces. Although hardware architecture may also influence the scalability of the management centre, modern equipment offers a wide range of capabilities and so, they do not introduce any relevant limitation whether in the choice of application architecture or in the system capacity dimensioning.
- **Modularity.** The standardisation of Application Programming Interface (API) and data interchange methods is an important requirement to allow software module interchange. The implementation of the management services based on modules with standard interfaces introduces the flexibility and capability of system configuration and upgrading.
- **Security capabilities.** The architecture has to be designed in such a way that security can be included and configured according to the global management security requirements.
- **Mobility support**. Mobility is a key requirement nowadays. It has two aspects:
  - ***Remote access***. It implies that the capacity of accessing management centre services from remote locations using private communication facilities, public network infrastructures or a combination of both.
  - ***Application/Server ubiquity***. This is another aspect of mobility. It refers to the ability of finding servers and/or applications located in the management centre domain in order to complete the modules required to support a management service. This facility introduces a great flexibility in the implementation and maintenance of the management centre and opens the possibility of upgrading management services on the fly.

Although there are many application architectures that may provide scalability and modularity, the most common approach is the layered architecture. This architecture allows scalability and mobility to be easily achieved providing at the same time mechanisms to implement security. The modularity of the applications is basically a function of the implementation approach; the layered architecture helps in the development of modular applications.

The figure 4.5 shows the typical layered architecture with the three layers, the client layer, the application layer and the data layer. When this architecture is implemented using web technology, the client layer consist of personal computers equipped with an Internet browser connected to the application layer whether directly through IP facilities or remotely using VPNs. The application layer consists of a number of Java applications and a collection of standard and proprietary Java beans. The application layer is connected to the data layer using J2EE interface or JDBC.

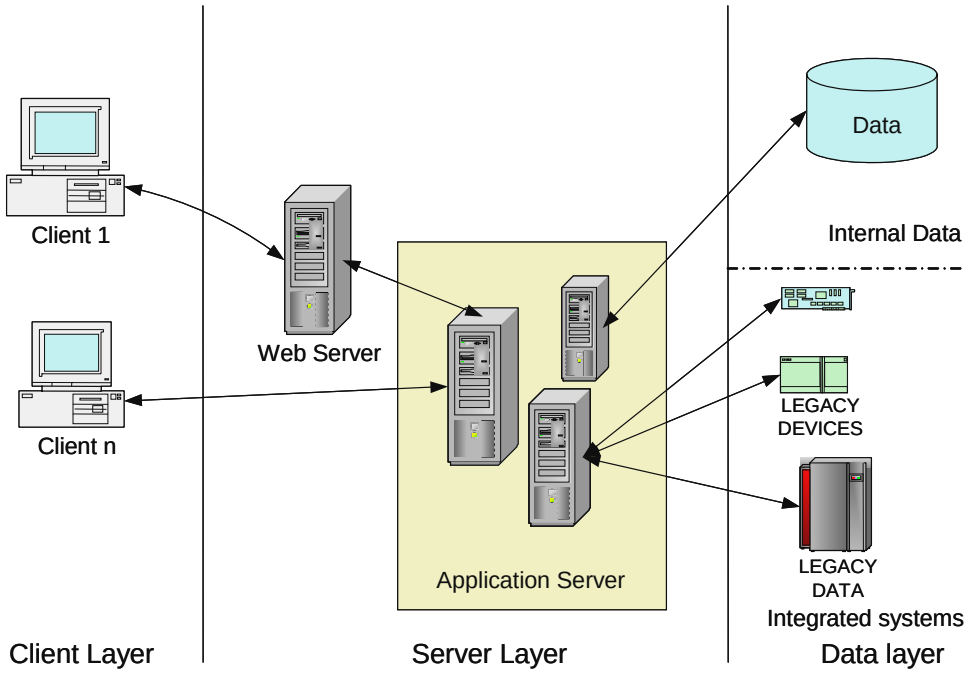

Figure 4.5 Layered architecture

4.4.4. *Service provision*

The main task of the network management centre is to implement a set of functions in order to provide management and maintenance services. The way TMN and the management centre applications are implemented determines the flexibility and capabilities of providing this service in different ways. This is very relevant to provide different access mode, service modularity and flexibility and user interface independence in order to leverage the functionality of the whole management system.
The issues of mobility and modularity are very relevant in the service provision. There are two aspects to be considered:

- The requirements for remote access to management centre services and applications.
- The capability of distributing applications or management data in different servers.

Application architecture has a capital influence in the way the service is provided and the capabilities that can be obtained. Object distribution technologies like CORBA or Web services are the most common approaches to implement management and maintenance service centres. Although CORBA is one of the components of the TMN ITU-T architecture, modern developments are based on the web approach using XML for object representation and Java technology.

Several architectures of the management centre applications can be distinguished. They strongly influence the capabilities for implementing mobility and remote access as well as the requirements of bandwidth and performance of the communication facilities.

- Proprietary MMI provided with proprietary application architecture and interfaces. These applications are normally based on public or almost standard graphic libraries. The use of these libraries does not imply that the application is open and may interoperate with other applications even in the case where they use standard

protocols. This approach is limited to local access in the management centre. Remote access may require a lot of bandwidth.

- Web based interface. In this case, the MMI application is based on the Internet standards so all the protocol stack as well as the presentation follows Internet specifications. If the web server is public and remotely accessible remote access can be implemented using Internet access techniques.
- Web based application (Web services) In this case; the standardisation is extended from the MMI to every small applications, or agents, that support elementary services. This architecture intrinsically provides open remote access capabilities.

In any case, remote access can be implemented using Web interfaces. In this case, the architecture of the management centre is hired from the user. A web server provides the service access point. Consequently, the service interface is made available to any user having connectivity and access rights.

4.4.5. Service access

This chapter describes the way and the tools required to access the services provided by a management centre.

In general, applications are structured in a client-server approach. Both client and server use to be located in different hosts, the user is equipped with the client application that, among other functions, provides user interface and all the representation functions required to support the service whereas the server provides the core functionality of the service thereby including information access and process. The way both applications are implemented together with the type of protocol used to support this communication determine the capabilities for mobility and remote access as well as the communication requirements.

Modern implementations are based on Internet technologies, the IP protocol stack, web based applications and Web services.

- The use of IP provides straightforward connectivity allowing remote access and mobility to be easily implemented.
- Web based interface provides isolation from hardware and operating systems
- Web services provide isolation from atomic service implementation and capacity to automatically adapt to new developments and system reconfiguration.

Using the Internet approach, the service is provided by a web browser. Because of this, client application is a standard piece of software normally provided in the basic configuration of any computer. This is a great advantage since any computer can use the service without the need for a specific configuration or proprietary application. Due to this, remote access and mobility is simplified if IP connectivity is available. The main issues to consider in this case are:

- Bandwidth required for information transfer. The bandwidth required by the IP approach is normally higher than the required by proprietary or specific protocols.
- Security risk and the necessary countermeasures. The fact any computer with IP connectivity can become a user of the system has to be taken into account to prevent cyber-attacks.

Different communication media and access networks may be used for remote access:

- Dial-up channels
- Wireless access

- VPN through an IP network

4.4.6. Service Oriented Architecture

The Classical client-server application architecture is evolving towards a more flexible approach based on the concept of small and flexible applications called software agents. In this approach, a service is a unit of work done by a service provider to achieve desired end results for a service consumer. The goal of this approach is to improve system scalability, reliability and performance. This is achieved by using two key architectural characteristics:

- A small set of simple and ubiquitous interfaces universally available to all service providers and consumers.
- A set of descriptive messages written in a format, structure and vocabulary that may be understood by all parties.
- A mechanism that enables a consumer to discover a service provider.

Web services are a particular implementation of the service oriented application architecture. Web services are self-contained, self-describing, modular applications that can be published, located, and invoked across an IP network. The specific characteristics of Web services are:

- Interfaces are based on Internet protocols.
- Messages are written in XML.
- The Universal Description, Discovery and Integration service (UDDI) provides a mechanism for clients to dynamically find other web services.

The web services platform is based on XML document carried by the HTTP protocol. XML provides a metalanguage used to write specialized languages that express complex interactions between clients and services.

The elements that web services platform are:

- SOAP (Simple Object Access Protocol). SOAP provides a uniform way of passing objects, that is to say, XML-encoded data between applications (Clients and servers).
- UDDI (Universal Description, Discovery and Integration service). UDDI provides a mechanism for clients to dynamically find other web services. UDDI works like DNS service for application searching for services. A UDDI registry has two kind of clients: Applications that want to publish a service and clients that want to obtain services of a certain kind used them.
- WSDL (Web Service description Language) WSDL describes how to use and interact with a Web service. XML is used to describe the service.

4.5. Security

Security is very important for any critical utility infrastructure. Strong authentication of users, objects, and data integrity are required. A robust and flexible access control system that provides both role-based and location-based access control methods is required.

In an IMI approach, a coordinated security model should be implemented such that all applications and services provide users with a common entry point (a single logon) for

their specific network management access. This also makes it easier for network management administrators to protect the information environment against malicious attacks by using the following:

- Manage user rights and access policies
- Assign appropriate and consistent security to network elements
- Facilitate more complete auditing and tracking
- Protect information investments through digital certificates, signatures and encryption
- Provide secure Internet access via Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Virtual LAN, and virtual private networks (VPNs) using Proxy Server.

Confidentiality should be considered particularly where there is commercial information involved. Functional requirements related to confidentiality are dealt primarily with communication outside of physical security boundary.

Management control centres security can be treated in a similar way to SCADA control centres and large IT infrastructure. Currently, there is no complete solution to protect information, control and diagnostic systems and intranets in electric power systems from attack and to protect data from improper use.

It is essential for electric system providers to recognize that while cyber security is an important component of protecting their systems, it is only one tool from a much larger set of information control techniques.

The issue of proper handling of information security has been raised within Cigré on a broad basis. The JWG D2/B3/C2-01 "Security for Information Systems and Intranets in Electric Power Systems" has been formed, with members from these three Study Committees.

4.5.1. Control Centres Security

The Control Centre boundaries are both physical, such as a control centre room, and logical. A logical boundary could include a primary control centre, backup control centre, and remote HMI stations. The protection profile must define the confidentiality, integrity, and availability requirements for information and communication while inside a physical and logically defined control centre boundary. The protection profile also must define requirements for the import of data from IEDs, and the field devices that are outside the TOE (Target of Evaluation).

A possible solution is to place the control centres in a firewall-protected area or in a DMZ (De-Militarized Zones). The DMZ is a computer host or small network inserted as a “neutral zone” between a utility enterprise network and the outside public network. The objective is always to protect and secure the critical system by means of a “barrier” from the non-trusted enterprise area or network to the trusted area. The most common approach is to use the protected area for the control centre.

There are products designed to encrypt and authenticate communication from substations to the control centre, providing “security” over the WAN, but this issue is still the biggest security problem without a good solution.

Detailed control centre security description is outside the scope of this document.

5. Interaction with Utility Management Applications

5.1. Introduction

A power utility is a complex multi-facet enterprise with its core mission being generation, transmission or distribution of electrical power, and its delivery to power customers. It is at the same time a service provider, an industrial process and an enterprise. The term “power utility” covers many organizations providing these services to varying degrees in one city, in one region, across the country, or between several countries.

In a very general manner the utility management can be described as presented in Figure 5.1.

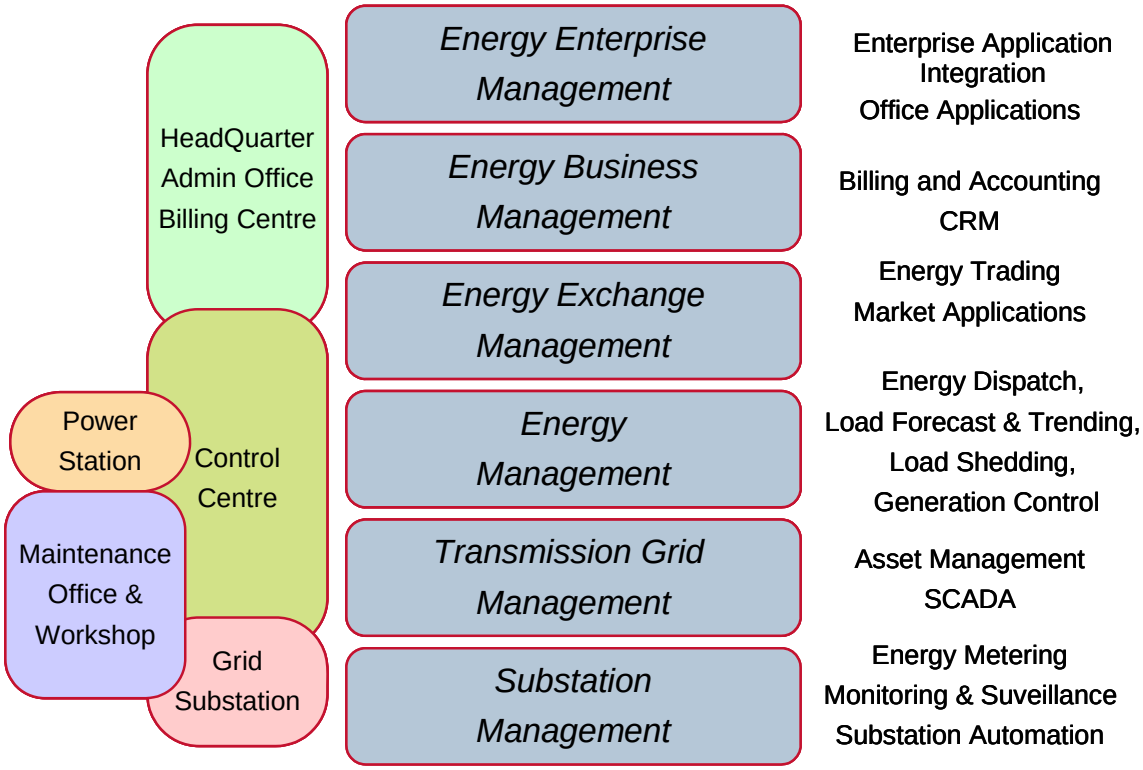

Figure 5.1 – Power Utility Management Processes and Applications

Each utility management process consists of a number of different applications, concerns different actors located at several geographical locations and owns an information platform requiring internal communications and interactions with other utility management processes.

The diagram shows that the simple distinction between administrative (or corporate) and operational applications is no longer sufficient. A whole spectrum of different utility applications have been developed ranging from the purely administrative tasks of the power utility enterprise to the real-time interactions between the intelligent components of the power system automation.

5.2. Interactions with Integrated Management Information

The interaction between the Integrated Management Information infrastructure and the relevant users can be performed in many different manners, such as the Power Utility Management (PUM) platform through read/write of a database, or the PUM user's workstation by pop-up windows or directly to the user by e-mail, SMS, pager, phone call, etc. It can also be performed through a consultable web-based service desk.

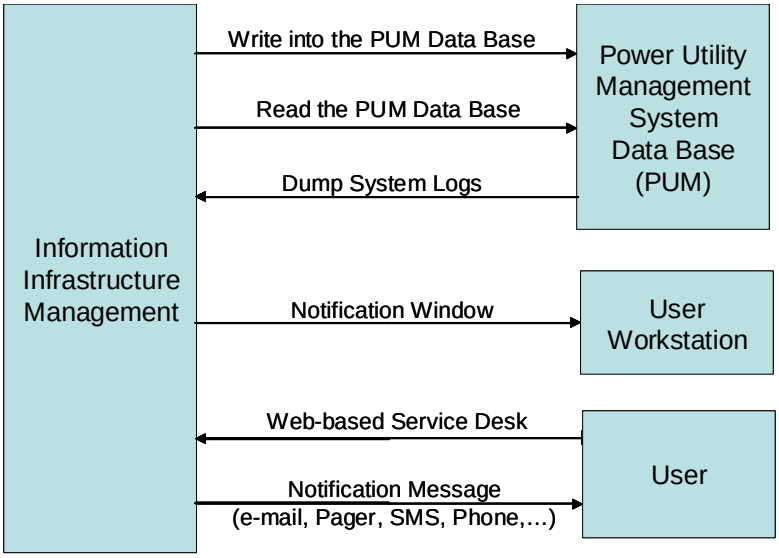

Figure 5.2 – Interaction interfaces between Information Infrastructure Management and Power Utility Management

The different Utility management applications interact with the information infrastructure management in the following ways:

A. **Platform Information :** Any Power Utility Management (PUM) system generates management and service information related to the events taking place in its platform such as fault, performance, security, etc. This information is collected, stored, processed and displayed by the IMI system to be used by concerned parties such as maintenance, asset management, administration, etc.

B. **Information Collected from other devices :** A PUM system may be the only way to access management information generated by some other infrastructure components e.g. status and alarms of substation IED and telecommunication equipment available through the power system SCADA.

C. **Service Status and Incident Information** : The PUM system or user can receive appropriate service information from the infrastructure management system (IMI) either as notification messages or as a consultable dashboard e.g. service desk and queries, incident notification, capacity and change management, quality monitoring, etc.

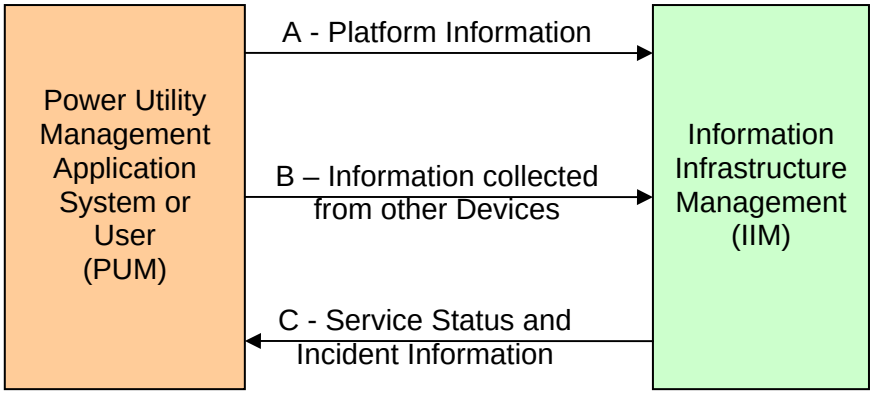

Figure 5.3 – Interactions with Information Infrastructure Management

5.3. Utility Management Processes

5.3.1. Substation Management

Substation management consists in all processes involving a particular electrical substation including the local automations such as protection functions, feeder and substation control, condition monitoring of devices, measurements, metering and site surveillance. The concerned platforms for information collection, processing, storage and exchange are the different protection relays and transducers, event recorders, protection signalling devices, bay controllers, digital substation controllers and SCADA remote terminal units, energy meters, and also Power Line Carrier communication terminals, substation LAN components, surveillance cameras and other dedicated equipment found in the substation.

The frontier between the substation management and information infrastructure management is somehow difficult to localize. Intelligent components of the power system are generally part of the utility management process and part of the information infrastructure process e.g. protection relay and signalling equipment, bay and substation controller, etc. It is reasonable to assume that in most cases where a system component is both part of the substation management process and the information infrastructure management process, the latter shall obtain its information through the former or independently e.g. an informative interface based on IEC61850 connected to a management LAN, in addition to the process interface connected to a process LAN.

5.3.2. Transmission Grid Management

The transmission grid management is composed of those utility application processes that consider the power network rather than the individual substations. It mainly articulates around the Power system SCADA. It is localized at the Control Centre (SCADA platform) connected through the communication network to SCADA RTUs at the different nodes and/or substations of the power network.

The interaction of the Transmission Grid Management applications with the Information infrastructure management is through sending of management information collected

through the SCADA system on different data collection, communication, and processing device status to the Information Infrastructure Management, sending of SCADA processing platform information and receiving of service indications. Different applications such as power network maintenance, planning, asset management are all users of the IT and communication infrastructure and must receive as such, quality, incident and other service indications.

5.3.3. Energy Management and Exchange Management

Energy Management Process includes all applications allowing optimal dispatch and delivery of power through the network. It uses information obtained through the Power System SCADA. The Energy Management platform is mainly located at the National Dispatch Centre and may interact with other Dispatch Centres, with power generation plants and possibly with a Market platform dealing with energy exchange management processes.

The interaction with the information infrastructure management is through the receipt of service indications from communications, server, security, etc. and sending of platform management data for consolidation.

5.3.4. Energy Business and Enterprise Management

Business Management includes all processes interacting with the utilities' customers. It includes utility service billing and customer relation management (CRM or Customer Care). Business management processes involve IT processing platforms and may include the use of communication services such as web-based CRM and billing, connection of billing system to metering devices in substations or customer premises, connection of service desk to Control Centre, Call Centres. The interaction with the integrated management information is through the receipt of service indications from communications, server, security, etc. and transmitting platform management data for consolidation.
Enterprise Management includes all processes involving the corporate staff of the utility and their internal interactions. It includes Work Management and ERP platforms of the utility as well as Corporate Multi-media communications. The interaction with the Integrated Management Information infrastructure is also through the receipt of service indications from communications, server, security, etc. and the transmitting of platform management data for consolidation.

Utility Management Process	Utility Application	Interacting Utility Management System	Interaction with IMI		
			A- Platform Info. **PUM → IIM**	**B- Collected Info.** **PUM → IIM**	**C- Service Status & Incidents Info.** **IIM → PUM**
Substation Management	Protection & Control	Substation Control System	Management Information for the Processing Platform	Management Information for Devices accessed through Substation Controller	Protection Signalling and Communication Quality Status and Service Incidents
	IED Management	IED Management System	Management Information for the Processing Platform	Management Information for IED	
	Substation LAN Management	Substation Management System	Management Information for the Processing Platform	Management Information for Substation LAN components	Communication service information
	Primary Device Monitoring	Condition Monitoring Platforms (Transformers, Switches, etc.)	Management Information for the Processing Platform		
	Substation Surveillance	Camera and Video Surveillance System	Management Information for the Processing Platform	Site Security Alarm Information	

Note : The following process interactions are non-exhaustive, utility policy dependant and evolving. They are presented here for illustrating the approach and should be produced in each specific case.

Utility Management Process	Utility Application	Interacting Utility User / System	Interaction with IMI		
			A- Platform Info. **PUM → IIM**	**B- Collected Info.** **PUM → IIM**	**C- Service Status & Incidents Info.** **IIM → PUM**
Grid Management	Power System Asset Management & GIS	Asset Management and GIS platforms	Management Information for the Processing Platform		Communications and processing service status and incidents
	Power System SCADA	SCADA System	Management Information for the Processing Platform	Management Information for RTU and devices accessed through SCADA	RTU communication channels status and incidents information
	Power Network Planning	Network Planning Workstations	Management Information for the Workstations		Communications and processing service status and incidents
	Power Network Maintenance	Maintenance Management System	Management Information for the Processing Platform		Communications and processing service status and incidents
Energy Management	EMS	Energy Dispatch Operator	Management Information for the Processing Platform		Communications and processing service status and incidents
	Control Centre Maintenance and Platform Administration	Maintenance Management System	Management Information for the Processing Platform		
	Control Centre Cyber-Security	Operation System Security Engineer	Management Information from different security components		Filtered and refined security data from relevant devices across the network

Note : The following process interactions are non-exhaustive, utility policy dependant and evolving. They are presented here for illustrating the approach and should be produced in each specific case.

Utility Management Process	Utility Application	Interacting Utility User / System	Interaction with IMI		
			A- Platform Info. **PUM → IIM**	**B- Collected Info.** **PUM → IIM**	**C- Service Status & Incidents Info.** **IIM → PUM**
Energy Exchange Management	Inter-Dispatch Communications	Other Dispatch Operators			Service Status and Incident messages from different control centres
	Energy Trading	Market Partners			Service Status and Incident messages
	Billing and Customer Relation Management	Power System Billing & Service Desk	Management Information for the Platform		Service Status and Incident messages
	Business IT Platform Management and Administration	Business IT System Engineer and Administrator	Management Information for the IT Platform		Service Status and Incident messages
	Business Data & Network Security	Business IT Security Engineer	Management Information from different security components		Filtered and refined security data from relevant devices across the network
Energy Enterprise Management	Enterprise IT Platform Management	Enterprise IT System Engineer	Management Information for the IT Platform		Service Status and Incident messages
	Corporate Multi-media Communications	Multi-media Service Administrator	Management Information for the Platform		Service Status and Incident messages
	Enterprise Data & Network Security	Corporate IT Security Engineer	Management Information from different security components		Filtered and refined security data from relevant devices

Note : The following process interactions are non-exhaustive, utility policy dependant and evolving. They are presented here for illustrating the approach and should be produced in each specific case.

6. ACCESS TO MANAGED OBJECTS

6.1. Introduction

The gathering of management information has in the past been accomplished by means of facilities and technologies that were available at the particular time. The process of information gathering and distribution comprises the local provision of the information on the one hand, and the transport and presentation of the same to the – normally remotely located - user on the other. The actual available technologies were at any time decisive on how this could be achieved. The introduction of electronics and telecommunication facilities finally paved the way to perform the task of information collection and distribution more effectively.

Different solutions evolved over time, driven by the economic and technology considerations. Starting from simple and proprietary signalling systems they evolved to more elaborate solutions based on SCADA- or telecom technologies and adhering to local practice or global standards as far as available and applicable.

The following table gives an overview of managed objects and standards in use, where available and applicable.

Communication equipment	
WAN	**Standards for management (typical)**
Multiplexers (SDH, PDH)	ITU-T (Q-series) IETF (SNMP)
Line terminals	ITU-T (Q-series) IETF (SNMP)
Modems (Voice band, xDSL)	ITU-T (Q-series) IETF (SNMP)
Radio equipment	ITU-T (Q-series) IETF (SNMP)
Optical amplifiers	Proprietary/SNMP/(Q-Series)
Repeater station	Proprietary/SNMP/(Q-Series)
Power line carrier terminals	Proprietary/SNMP
Routers	IETF (SNMP)
Switches (ATM IP)	IETF (SNMP)
Gateways	IETF (SNMP)
PABX	Proprietary
Voice applications servers	Proprietary and IETF (SNMP)
Satellite Terminals	Proprietary
Time clock synchronisation receiver	Proprietary/SNMP/(Q-Series)
Teleprotection devices	Proprietary
Leased lines and external services	Proprietary/SNMP/(Q-Series)
LAN	
Hubs, Bridges, Routers	IETF (SNMP)
Firewalls	IETF (SNMP)
PCs and Workstations	IETF (SNMP)
WLAN and Bluetooth devices	IETF (SNMP)

Substation equipment (secondary equipment)	
IEC61850 IEDs	
Virtually any device of primary or secondary equipment compliant with IEC61850, like:	
Protection relays	IEC61850
Substation and Bay controllers	IEC61850
PLC (Programmable Log. Contrl.)	IEC61850
Meters	IEC61850
Tap changer controller	IEC61850
Load control	IEC61850
Disturbance recorders	IEC61850
Legacy devices	
Same as above, however non-manageable or manageable by means of proprietary protocols via local COM port (serial) or Ethernet	Proprietary, IEC (101, 104, 103), DNP, Modbus.
RTUs	Proprietary, IEC (101, 104, 103), DNP, Modbus.
Control centres	
Workstations	IETF (SNMP) and/or proprietary
Servers	IETF (SNMP) and/or proprietary
SCADA communication front-ends	IETF (SNMP) and/or proprietary
(See also LAN section)	
Condition monitoring devices	
Circuit breakers monitoring	Proprietary
Transformer monitoring	Proprietary
Battery chargers monitoring	Proprietary, IETF (SNMP)
Battery condition monitoring	Proprietary
Environmental monitoring	Proprietary
Power line monitoring	Proprietary
OPGW line monitoring	Proprietary or IETF (SNMP)

6.2. Different ways of gathering information

6.2.1. SCADA

A major step towards a more comprehensive gathering of information was the introduction of Telecontrol and SCADA systems: Facilities like RTUs and telecommunication networks permit the collection of information locally in substations and the transfer of it to regional or national Control Centres. SCADA systems are primarily intended for the control and the operation of the power grid, however they are likewise used to gather and distribute management information for a variety of assets as far as these can be interfaced and integrated into the SCADA system. The applicable standards are mainly from IEC and ANSI/IEEE.

6.2.2. Dedicated network management systems

In order to manage the increasingly complex telecommunication networks in the WAN, the telecom industry developed appropriate standards. These are detailed in the ITU-T recommendations (Q-Series). In some instances, assets external to the telecom infrastructure were also integrated to some degree into the telecom network management system (TNM). In many practical cases however, one would still find isolated, dedicated management systems for the various types of infrastructures (telecom, primary equipment, ancillary alarm systems and equipment) rather than truly integrated solutions. The reasons are mainly found in historic developments and in the lacking of suitable and generally agreed methods and standards.

6.2.3. Internet, Intranets, IP Networks

Internet technology brought about new protocols and standards, developed primarily by the IETF. The SNMP (Simple Network Management Protocol) has – thanks to its simplicity compared to telecom TNM and driven by the rapid deployment of Ethernet/IP in the LAN and the availability of open management platforms – been widely adopted by the process industry.

Seen from a technical point of view, the public Internet could basically be used to gather information from geographically remote areas, in addition to or as a substitute for legacy telecommunication facilities. However, one has to bear in mind the imminent high risks regarding security and privacy when planning to use the global Internet or an IP network from an external provider for management purposes. Malicious attacks, intrusions, viruses etc. present a high risk for catastrophic incidents when for example the flow of management information is impeded, corrupted or faked. Although management information may be less critical than immediate operational control information, the unwanted change of the settings of a protection relay for example may have severe impact on the power grid stability in case of a line fault. Hence, a sound security policy has to be in place in addition to an adequate infrastructure, sound Service Level Agreement, etc. Intranets based on VPNs and the implementation of information security classes for different types of management information is a possible approache.

6.2.4. Ancillary alarm systems

SNMP as a standardized means for device monitoring and/or controlling is today available with an increasing number of ancillary devices found in substations, like UPS systems, battery chargers etc.

6.3. Legacy protocols

Apart from proprietary protocols, the gathering of management information from devices in remote locations across a WAN (Wide-Area-Network) has traditionally made of standard communication protocols like IEC60870-5-101, IEC60870-5-104, or DNP 3.0 to name the most common ones.

These protocols were originally designed for general telecontrol applications like the exchange of data between a Control Centre and RTUs (Remote Terminal Units), providing the required degree of data integrity.

Managed objects either provided a dedicated management interface compliant with one of the standard protocols, or they connect via binary status- and/or control signals to RTUs that multiplex the management information of several managed objects, using

one of the standard protocols for communicating across the WAN. The response time for collection and distribution of management information is subject to the properties of the protocol whether polling, spontaneous, unbalanced, or balanced and the speed of the WAN.

Telecommunication equipment frequently used proprietary protocols for their management. With the introduction of SDH in the transport layer and modern network technologies (ATM, IP) in the upper layers, the management of telecom devices and networks became more open by adhering to standards as defined by the ITU-T (TNM) or IETF (SNMP).

6.4. IEC-61850 Communication networks and systems in substations

International Standard IEC 61850 has been prepared by IEC Technical Committee 57: "Power systems management and associated information exchange", and consists of ten parts, under the general title "Communication networks and systems in substations" [3].

The goal of IEC 61850 series is to provide interoperability between the IEDs from different suppliers or, more precisely, between functions to be performed in a substation but residing in physical devices from different suppliers.

One of the most important features of IEC 61850 is that it is the first global standard, and furthermore introduces a new architecture for the automation of substations based on Intelligent Electronic Devices (IEDs), mainstream communication technologies like Ethernet, and TCP/IP, and defines a standard service provision and device modelling, and also a normalized substation configuration language.

Some of the most important aspects of the standard are the definition of the information models and the information exchange methods. The main abstraction of this model is the Logical Node (LN), which is the basic building block for substation automation. The logical nodes, data, and data attributes model substation devices and specify their interaction rules. The information exchange is defined in terms of services.

For configuration purposes IEC 61850 defines the Substation Configuration Language (SCL), which is an XML schema. In addition to the on-line retrieval of the self-description, the capability of IEDs can be made available in a second way that is to say, through an XML SCL instance file. SCL allows configuring the communication-related attributes of an IED, as well as the equipment and communication topology within the substation. The physical hierarchical structure of the substation is defined in SCL only, whereas the rest of the standard focuses on LN and their data objects.

SCL allows the description of an IED configuration to be passed to a communication and application system engineering tool, and to pass back the whole system configuration description to the IED configuration tool in a compatible way. Its main purpose is to allow the interoperable exchange of communication system configuration data between an IED configuration tool and a system configuration tool from different manufacturers.

The standard specifies a file format for describing communication related IED configuration and IED parameters, communication system configurations, switchyard structures, and the relations between them. The main purpose of this format is to exchange IED capability descriptions and SA (Substation Automation) system

descriptions between IED engineering tools and the system engineering tool of different manufacturers in a compatible way.

Some important features of the standard are that it does not specify individual implementations or products using the language, nor does it constrain the implementation of entities and interfaces within a computer system, nor does it specify the download format of configuration data to an IED, although it could be used for part of the configuration data.

The great development of the technology related with the web will make easier to combine the web services with the IEC 61850 standard to implement engineering, management, maintenance and control services of substations designed in accordance with the new standard.

6.4.1. IEC 61850 management services

As mentioned the services provided by a 61850 IED are based on the concept of virtualization of the physical devices.

The virtualization of a device provides a description of data and behaviour as well as the methods for exchanging information.

IEC 61850 ACSI (Abstract Communication Service Interface) [4] specifies the mechanism to access and control the devices. Abstract in this context means that the service interface is defined in terms of "what" the service provides. The concrete coding of messages interchanged between devices is specified when the service is mapped to actual application protocol. The Specific Communication Service Mapping (SCSM) [5] defines how object models and the services supported are implemented using a specific communication stack, the application protocol MMS (ISO-9506) and TCP/IP in this case. SCSM specific extensions or usage rules may be required in the appropriate parts.

IEC 61850 does not provide specific management services; the management functionality of every IED is built into the object definition. By using the standard services, maintenance and management functions can be performed. The following list shows the services that can be provided by 61850 IEDs:

- Directory services
- Get data value
- Set data value
- Setting Group-Control-Block
- Report Control-Block
- Real time data transmission
- Sampled value transmission
- Control services
- Time Synchronization
- File transfer

The type of device and specific vendor implementation would determine which services are available for a specific device. Most of the services, out of real-time data transmission, sample values or control services are used in maintenance and management operations.

The IEC 61850 standard provides a common environment for the management of every aspect of every IED installed in a substation. The service covers the functionality required to implement an advanced protection and control system. Since this new architecture required an advanced communication system, both inside the substation and from the substation to the management centre, specific functions to maintain this communication infrastructure have also to be provided. In this case, the IP management architecture is used, and therefore, every communicating device would have to include an SNMP agent to support the IP management functions.

The standardization of the management applications is out of the scope of the IEC 61850 standard; this implies that the management of every IED requires the use of vendor-specific tools.

In order to provide a unified service provision platform, the standardization of the applications that provide the management services is strongly recommended. This can only be achieved by using emerging Internet standards.

6.5. Gathering information of distributed objects

The Common Object Request Broker Architecture (CORBA) is an architecture that allows the deployment and management of large-scale distributed object systems.

CORBA is the middleware technology specified in the ITU-T TMN architecture. Although CORBA can be used for management information gathering which includes every type of managed object integration, its main application is related with the implementation of distributed umbrella management centres.

CORBA is based on two main components, the Interface Description Language (IDL) and the Object request Broker (ORB)

The ORB delivers requests to objects and returns any responses to the clients making the requests. The object that a client wishes the ORB to direct a request to is called the target object. The key feature of the ORB is the transparency of how it facilitates client/object communication.
ORB performs the following functions:

- Object location: The client does not need to know where the target object resides. It could reside in a different process on in another machine across the network. ORB provides the functionality to locate the object.
- Object implementation: The client does not need to know how the target object is implemented. ORB unifies heterogeneous systems.
- Object execution state: When it makes a request on a target object, the client does not need to know whether that object is currently activated (i.e., in an executing process) and ready to accept requests. The ORB transparently starts the object if necessary before delivering the request to it.
- Object communication mechanisms: The client does not need to know what communication mechanisms are used by the ORB to deliver the request to the object and return the response to the client.

The general ORB interoperability architecture is based on the General Inter-ORB Protocol (GIOP), which specifies transfer syntax and a standard set of message formats for ORB interoperation over any connection-oriented transport. GIOP is designed to be simple and easy to implement while still allowing for reasonable scalability and performance. The Internet Inter-ORB Protocol (IIOP) specifies how to implement GIOP over TCP/IP.

The connection between the client and the ORB, and the object and the ORB is carried out by means of a standard interface implemented using the Interface Definition Language (IDL).

The IDL provides a language neutral and location-neutral messaging interface for component integration.

The CORBA IDL specification is not an implementation model, but rather an interface and services model. It is language-neutral and leaves maximum flexibility for underlying implementation details.

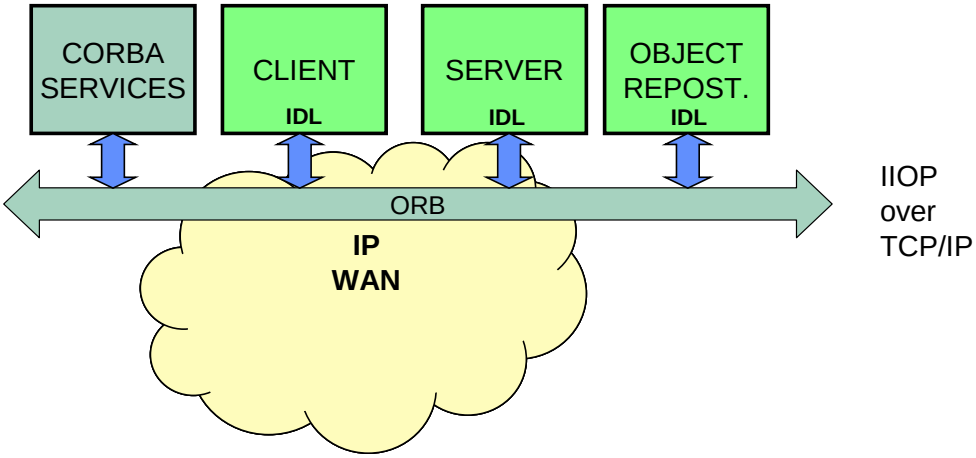

Figure 6.1 CORBA Architecture

6.6. Web User's Interface

Web technology was developed to offer a unified method to access information of different formats using a consistent, easy-to-use user's interface. This system is based on three main components, the application protocol, HyperText Transfer Protocol (HTTP), the URL addressing scheme that identifies the location of the retrieved data and the data coding language the HyperText Markup Language (HTML). The great advantage of this system is its total portability, both the application used to access the information and the information itself are operating system and platform independent.
The HTML language permits the creation of Hypertext documents that can be linked by means of Hyperlinks. This structure, together with the new addressing scheme, hides the actual location and the format of the data.

Since management requires the access to heterogeneous information that must be presented in a user friendly format, Web technology is a suitable technology to implement whether local or remote access to management information.

Web architecture is based on a Client-Server approach. The users request information from a Web server by means of an HTTP query. The server processes the request and sends back an HTTP response containing the requested information in HTML format. Queries to Web server are carried out from a Web browser that includes a Web client application and a standard Graphical User Interface (GUI) to present HTML information. The figure below shows the components that an embedded system requires implementing Web management.

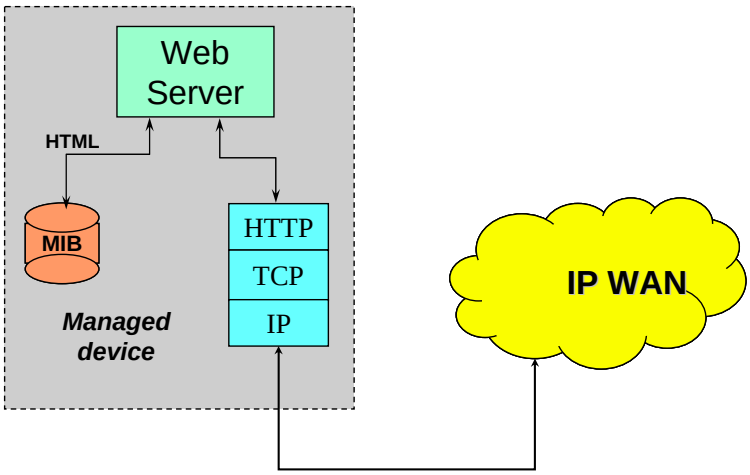

Figure 6.2 Web management components

Web technology offers a way of accessing and performing operations over distributed objects that completely match Network Management requirements. At the same time, it also offers a simple and easy to use user interface for any type of task and application.

Web technology offers a standard well-known and easy-to-use GUI. Any management object stored in a MIB can be accessed from a Web browser and displayed in an HTML page.

Web pages can contain text, images, audio and video, link to other pages, Java code or forms to introduce data and set values in related objects. Java code is executed in the station that is browsing the Web and can perform any type of operation or management task with the management information retrieved from the equipment under supervision. Java applications permit the visualisation of dynamic management objects such as alarms, traffic measurement, performance figures, etc. Furthermore, complex automatic management action can be performed locally without the need to install any specific management application, as it comes embedded in the HTML page.

Web management can be mixed with SNMP. Typically, a SNMP agent provides management services to the management centre whereas the web server provides Web pages with management information and with interaction capability that allows IED configuration and management to be carried out locally or remotely if IP connectivity is provided.

6.6.1. HTTP

According to the OSI (Open System Interconnection) model, HTTP (HyperText Transfer Protocol) is an application level protocol described earlier in RFC1945 (HTTP 1.0) and described in RFC 2616. This protocol is based on request – response actions, typical client – server activity.

A client, running a browser application, establishes a connection with a server and sends a request to the server in the form of a request method.

The server responds with a status line, including the message's protocol version and a success or error code, followed by a message containing server information, entity information and possible body content.

- The HTTP transaction is divided into four actions
- Connection opened by browser
- Request to the server is sent by the browser
- Response to the browser is sent by the server
- Connection is closed

There is also one adaptation of the HTTP, the Secure HTTP (HTTPS), according RFC 2660, in order to provide secure communication between an HTTP client-server pair and normally used for commercial transactions in the Internet. Secure HTTP provides a flexible protocol that supports multiple orthogonal operation modes, key management mechanisms, trust models, cryptographic algorithms and encapsulation formats through option negotiation between parties for each transaction.

6.6.2. XML

In this section, XML (eXtensible Markup Language) is explained, but first of all is necessary to introduce HTML the origin of XML. HTML stands for the HyperText Markup Language, is a well known language commonly used in the web pages.
A markup language is a mechanism to identify structures that is present in almost all documents. Structured information contains text, images, streaming video and others, additionally includes some indication of what role that content plays. Content in a heading section has a different meaning from content in a footnote and also different to figures, streaming video or database content.

The HTML is supported by a wide range of applications including browsers, editors, email, and others. HTML was designed to display data with the focus on how data is presented and it looks.

With the popularity of the web, the HTML had to change in order to satisfy the new needs of the incumbent technologies and to bring variations in presentation of web pages, according to this it was extended (e.g. HTML version 4.0 has around 100 tags nor counting browser-specific tags), was introduced new streaming content, JavaScripts, Flash content and others. Nevertheless HTML is presented with a set of semantics and does not provide arbitrary structure, is rigidly confined by what the manufacturers implement. In HTML, both the tag semantics and the tag set are fixed. An “<h1>” tag is always a first level heading and the tag “<IED state>” is meaningless.

XML is a generic language (meta-language) that defines a standard way to add mark-up structured information. It was developed by the World Wide Web Consortium in order to overcome the limitations in HTML and lack of freedom in the semantic definitions. In summary, XML was designed to describe data with the focus on what the data is.

XML specifies neither semantics nor a tag set. It provides a facility to define tags and the structural relationships between them, is not based in any preconceived semantics.

All of the semantics of an XML document will be defined either by the applications that process them or by the users.
There are two different types of XML uses:

- Document
  - In document publishing the advantage of XML is the focus on the structure of the document, in this way is possible to obtain a document independent from the delivery medium. With XML is possible to make documentation which is a media independent format, automatically convert into other formats such as HTML, PDF, RTF and others.
- Data
  - XML can be used to define the database's structure and the data itself. This application has major importance in web based content which use dynamic database values (e.g. web page presenting energy consumption values from national TSO) and for data interchange between IEDs.

These two types use the same XML standard and are implemented using the same editors, but are different because they serve distinct purposes.

Using XML mark-up language since the information is structured, software can automatically update the information in the database and consequently in the web page.

6.7. Mapping of legacy devices

Legacy managed devices working with proprietary interfaces and/or legacy protocols require and adaptation process to become integrated in a standardised TMN system.

Mapping of Legacy devices is a rather complex task. Its complexity depends on how far the managed device technology is from the current standard technology.

Mapping may range from a simple profile adaptation to a complex adaptation of a wired device.

Three main aspects may be distinguished in the mapping process: Protocol translation, data modelling and service mapping. These three aspects are not independent since all of them are usually present in a mapping process

Finally, the validation of a mapping requires conformance testing. Therefore, the final step of mapping consists of defining performance requirements and the corresponding conformance testing procedures.

6.7.1. Protocol translation

Mapping via protocol translation is a solution for legacy device integration when data modelling and service of the legacy device has the same structure as the TMN.

Protocol translation has to be applied at the first common protocol layer. By doing this, the PDU of the common layer can be directly delivered to the other protocol stack and vice versa. Depending on the layer in which is operation is carried out, protocol translation may become a mere interface conversion, a bridging, routing or transport interconnection.

When data modelling and services of legacy and TMN are different, the mapping process has to be carried out.

6.7.2. Mapping Process

Figure 6.3 shows the overall mapping process. Protocol translation is not explicitly shown in the process since it is assumed that the mediation device or the interfacing equipment implementing the mapping has this facility. In fact, protocol translation is carried out using the gateway approach, that is to say, the device supporting this functionality is equipped with the two protocol stacks, legacy and TMN. Protocol translation in fact is reduced to service translation or mapping.

Service mapping is the process that look for matching between the services provided by the legacy protocol stack and the new services provided by the TMN protocol stack. In function of how old the legacy protocol is, the matching will be more difficult. In a general case, there will be some services that can be directly mapped whilst, some others will require a translation process because of the fact that they work in a different way or even are not defined at all in the legacy protocol.

The service translation process will produce the specification of the algorithms required to implement this task.

When there is a big difference between services, it may happen that some new services will have to be simulated using fixed default values.

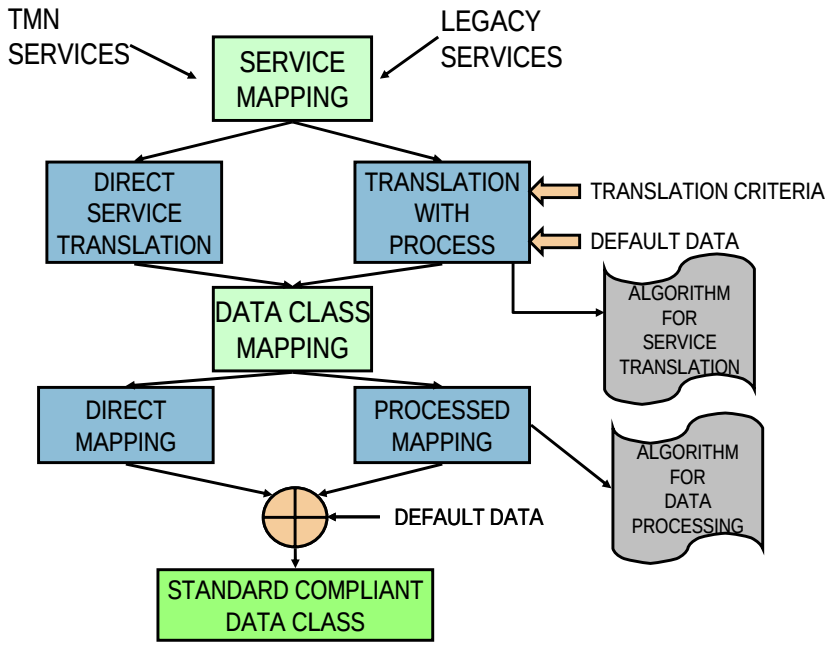

Figure 6.3 Mapping process

The next step is the data class mapping. In some cases a direct mapping from some legacy classes may be possible but in others it will be necessary to process legacy data to conform new data classes. The specification of this data process will be the input for the design of the algorithms to implement this mapping.

The library of standard data classes will be formed using the direct mapped classes together with the new processed data classes. For some legacy systems, fix default data would have to be added in order to complete standard data class profiles.

6.7.3. Implementation

Mapping implementation takes the information produced during the mapping process as the input for the implementation. The integration of legacy devices requires a middle box able to implement the mapping.

Figure 6.4 shows a conceptual block diagram of this equipment. The figure shows the two interfaces sides, the standard TMN with a standard agent and MIB and the legacy interface side with the legacy protocol and the state-machine that implement service and data class mapping.

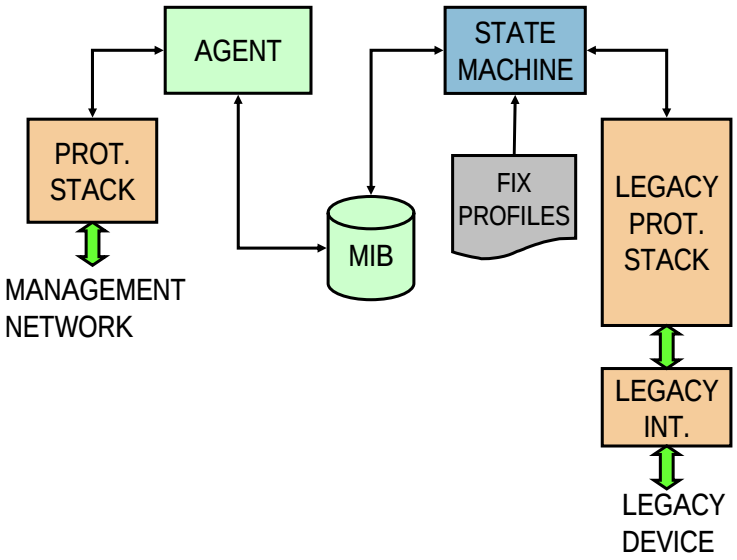

Figure 6.4 Mapping mediation device

Figure 6.5 shows the adaptation approach for a legacy wire system adaptation.

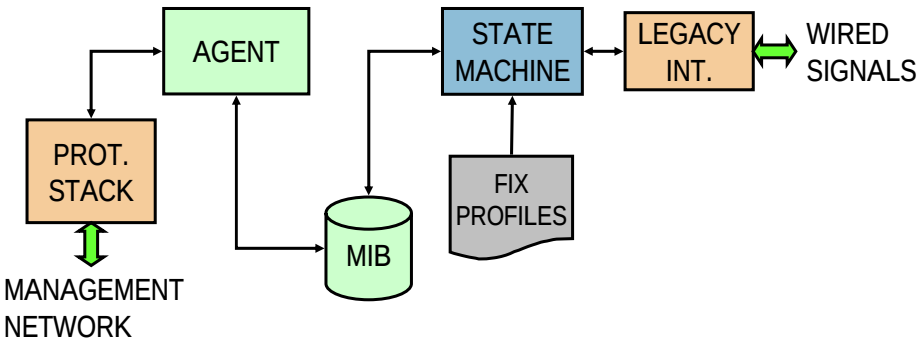

Figure 6.5 Legacy wired

6.7.4. Conformance Testing

Conformance testing requires performance requirements specification, including static and dynamic aspects, and the definition of the corresponding testing process.

In order to carry out a complete conformance test the following documents are required:

- Static requirements
- Dynamic requirements
- Test suit description
- PICS (Protocol Implementation Conformance Statement) for every protocol implemented
- MICS (Model Implementation Conformance Statement)
- PIXIT (Protocol Implementation eXtra Information for Testing) for every protocol implemented

7. Implementation of an Integrated Management System

7.1. Business issues

There is a number of business issues associated with implementing an Integrated Management Information strategy that should be taken into consideration. The degree of importance or scale of these issues will obviously vary from one company to the next and will be subjective to the company depending on the extent of change involved, the organisation of the company and the development stage the company is at with respect to their network management infrastructure and policies. At a general level the potential impact on the following areas should be considered:

- Organisational:
  - Integrating information may impact on the responsibilities and ownership of the information within an organisation, e.g. security needs to apply across the IMI platform.
  - The IMI should be adaptable to changes in the organisation.

- Market impact:
  - Requirements of different market operation in terms of sharing information between market players e.g. suppliers, distribution and generation companies, etc.
  - Regulatory constraints on information exchange.

- Processes and Procedures:
  - Processes and procedures associated with change management, configuration management, fault and repair services, management accounting and customer billing account and performance management may need to be re-engineered.

- Administration:
  - Authority levels associated with network access and security.
  - Release management e.g. application version and patch management.

- Asset refresh strategy:
  - A co-ordinated approach is required for replacement and investment of the information assets involved.

- Skills and Resources:
  - It is important to have a full understanding of the business benefits through adopting this integrated approach across the organisation in order to minimise the politics that may arise from parts of the organisation that were traditionally separate and independent and may end up having a dependency or risk that conflicts with their business strategies.
  - New skills or a new combination of existing skills (e.g. LAN operation systems and stations power system services) may be required to be developed.

- Products and standards life cycle:
  - Products life cycle. The point at which different products are available and supported by suppliers.
  - Standards. Life cycle of published standards and consistency of application.

- Information formats:
  - Development and implementation of an acceptable information format across the IMI.
  - Functional compatibility with legacy formats.

- Costs arising from Implementation:
  - There may need to be a co-ordinated approach to how the implementation is justified and paid for within the company.
  - Consideration will also be required for the sharing of operational costs depending on the benefits to the different users.

7.2. Architecture

The implementation of an Integrated Management Information System must start with a feasibility study and the analysis of the systems that must be managed. This task is performed through investigations at the various concerned utility organizations, and through the suppliers of the systems. Any existing dedicated management systems, their possibility of being northbound interfaced, their software release and their market availability (obsolete or not) shall be assessed.

The analysis shall also determine the type and extent of management functions that can be performed for any given system and those that may be required to be performed remotely from the Management System.

The architecture has to be selected on the basis to fulfil the functional requirements in a cost effective manner. In addition to performing the basic functionality of managing the objects at a level and comfort as supported by the facilities of managed objects themselves, the system architecture will have to meet additional requirements, such as:

- Providing the requested system availability for gathering and distributing the information
- Preventing loss of information due to system failures
- Preventing unauthorized access to the information (security)
- Ensuring timely recovery of relevant data in case of major system disturbances or after catastrophic failures

In order to keep complexity and cost at an affordable level, the design and architecture of the Integrated Management Information System may take into account that the criticality of the data is not the same for all managed objects, i.e. the requirements on reliability, data integrity and security depend on the managed object.

Resiliency by an appropriate communication network design, redundancy for critical components to prevent single points of failures, and the implementation of an IT security policy are key issues that have to be considered for the architectural design.

The IT- and communication architecture is also governed by factors like existing infrastructure, need for integration of legacy systems, anticipated migration strategy, geographical extension of the managed area, as well as information distribution- and workflow policy of the enterprise.

Preference may be given to designs supporting open management platforms with standardized interfaces, for example by integration of multi-vendor devices (managed objects) through compilation of their MIBs into the northbound NMS. Such more or less straightforward integration may lack all the Bells and Whistles of a dedicated proprietary system, but would provide access to most of the variables of the managed object, making at least the basic functions like status- and alarm monitoring available to the northbound umbrella management system. In order to access the full management functionality of the managed object, it may then still be necessary to invoke its proprietary (element) manager. How this can be achieved depends on the particular systems used. Although a homogeneous system would be most desirable, it may not always be feasible for technical, historical and practical reasons.

7.2.1. System Specification

The implementation of an Integrated Management Information System must start with a feasibility study and an analysis of the systems that must be managed. This task is performed through investigations at the various concerned utility organizations, and through the suppliers of the systems. Any existing dedicated management systems, their possibility of being northbound interfaced, their software release and their market availability (obsolete or not) shall be assessed.
The analysis shall also determine the type and extent of management functions that can be performed for any given system and those that may be required to be performed remotely from the Management System.

The following areas need to be evaluated in detail as part of the specification process:

- Managed Systems
- Management information users (Profiles)
- Management Services
- Management Organization & Architecture
- Available communications for management information

The evaluation report shall also assess the different services that are being provided through the above-mentioned systems and their management requirements to be covered by the Integrated Management Information system.

7.3. Data Communication Network

A communication infrastructure between managed devices and management centres is required to provide gathering of management information. This infrastructure is known as the Data Communication Network (DCN). A DCN consists of a data network connecting every device involved in the management infrastructure.

There are several implementation alternatives:

7.3.1. In-band

In this alternative the network management system uses resources from the same communication network that has to be managed as in the case of SDH or IP.

The use of in-band DCN requires a number of issues to be considered, namely:

- Transport capacity. The bandwidth provided by the managed network to transport management information is limited so it has to be crosschecked against communication management requirements.
- Overload protection. Management information is not a constant data flow. On the contrary, management information tends to be transmitted in bursts so in the event of an outage, the amount of management information to be transferred can overload the network unless some protection mechanism would be deployed.
- Common-mode failure. A failure in the managed network may jeopardize management services. It is important to analyze the impact of outages in the management services and plan how the management system will cope with these outages.
- Intrinsic limitations. The design of the managed network may introduce several limitations in the management capabilities. When In-band DCN is implemented, management requirements have to be considered in the network design process.

In-band DCN tends to be the most economical approach to deployment of management services when the managed network technology is capable of providing this functionality.

7.3.2. Out-of-band

In this alternative the network management system uses resources that are independent from that of the communication networks to manage. This can be provided by creating a different data network for the management system or by overlaying on the network being managed. In the second case, the management traffic must have privileges over the data traffic.

When using out-of-band management the following issues have to be checked:

- Capacity of the management network. When the management service requires more capacity than the one provided by the managed network, out-of-band is the only approach.
- Compatibility between managed network technology and DCN technology.
- Management and availability of DCN. The deployment of a DCN will require specific management to assure DCN service availability.
- Cost. The deployment of a new data network for DCN purposes will introduce an extra cost. Nevertheless, the use of existing infrastructure or public networks may reduce the overall cost.

Out-of-band DCN based on public networks or an existing private ISDN is a cost-effective solution when the managed network is not capable of supporting in-band management.

7.3.3. Hybrid Solutions

Any combination of the above-mentioned alternatives can be used to implement DCN. In fact, the more common approach is a hybrid solutions made of a combination of the two above-mention alternatives. Typically the choice between in or out-of- band depends on several aspects:

- Managements requirements. When management requirements cannot be fulfilled by the management network in some areas of the network, out-of-band is the only choice.
- Lack of capacity. When the capacity provided by the managed network for management service in some areas is not enough for the management requirements, extra out-of-band capacity has to be provided. The areas covered by a proper in-band capacity will not need out-of-band provision.
- Economy. The proper combination of in-band management services and out-of-band based on already existing infrastructure or public networks reduces the investment and therefore, may reduce the overall cost.
- Technology mismatch. When the in-band communication service provided by the managed network does not match the technology of the management service, it may be cheaper to use the out-of-band approach instead of deploying protocol and interface adapters.

7.3.4. Polling versus traps

Another aspect to consider is how the request of alarms to the equipment is going to be made.

It is not an issue to be decided in the datacom, but rather in the designing of the management software and the managed equipment. It also refers to the user equipment management too. However, the way of collecting the information, affects the network.

When equipment has a problem, or one of its defined variables has passed a threshold, it can notify to management software in that moment. That notification is called a trap.

The other way, is a passive way. The equipment does not communicate anything except if the management software asks for it.

If the equipment is well configured, a management system with traps produces much less traffic than polling.

The main disadvantage of polling is the fact that as equipments do not communicate their problems, the management software has to do a lot of enquires to all equipment at regular intervals. It is necessary to consider this feature in order to design the management network with enough capacity.

The main disadvantage of trapping is the fact that if equipment dies, it cannot communicate anything.

Because of that fact, a mixture solution is mainly used. Equipment use traps, and the management software do a polling to verify that equipment are alive.
Of course, the polling is used to collect different variables that the manager wants to analyze. Traps are only used for alarms.

7.3.5. DCN Topologies

This section contains information regarding solutions that have influence on the network quality and availability.

Networks are normally built with core network as the backbone and access network to provide access to services on the core network. Core networks are bearer of traffic from many access nodes and therefore normally have ring or meshed structure. Access nodes can be dependent on availability requirement to be configured in several configurations.

The following are some factors to be considered when selecting topology:

- Availability
- Capacity need
- Equipment limitations
- Error performance and availability objectives
- Leased line availability
- Cost
- Existing infrastructure
- Time schedule
- Location of Core nodes

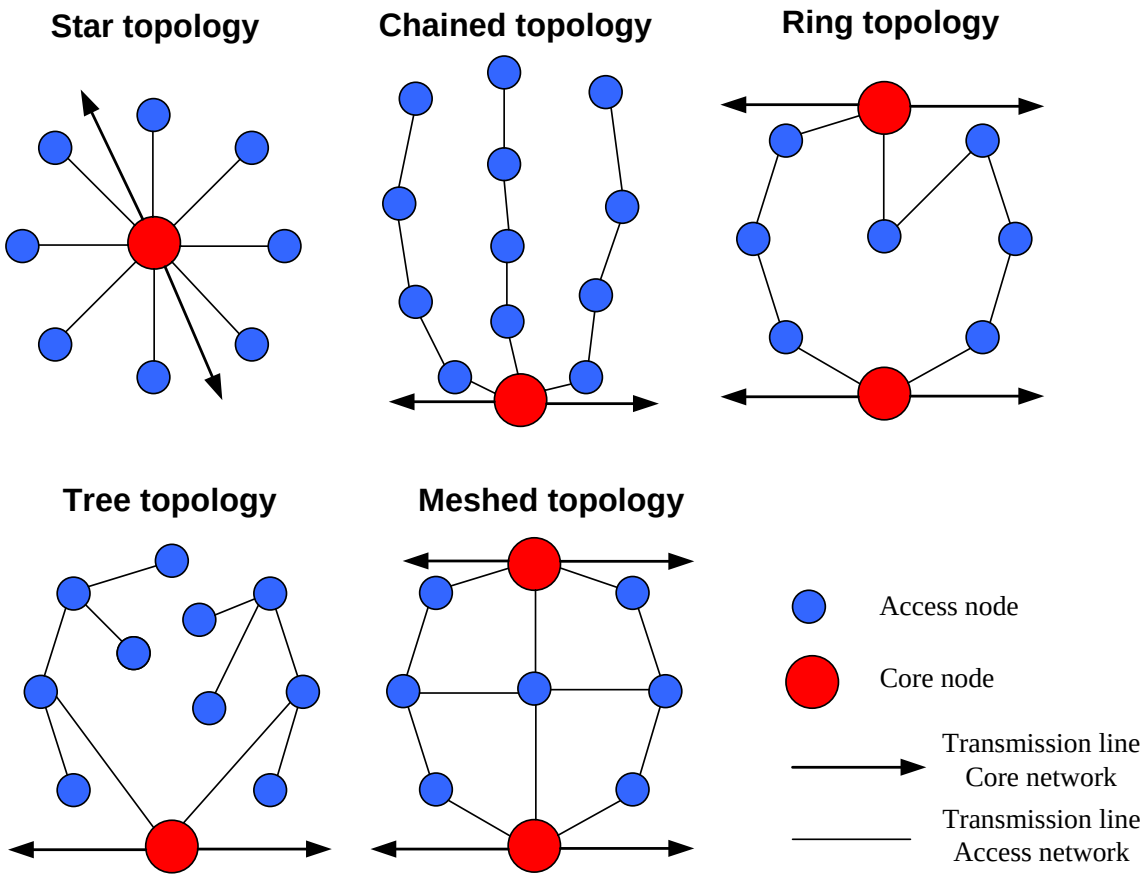

Figure 7.1 Examples of network topologies

- Star topology offers a cost effective and high capacity network. Access nodes have only ”one way” connection to core networks and for operating power network this sometimes does not fulfil requirements for availability.
- Chained topology gives also a cost effective solution for the network. Chain networks can if access network speed is low result in low capacity. Building long chains also leads to longer delay which can cause problems if real-time traffic such as IP-telephony is used. Access nodes have only ”one way” connection to core networks and for operating power networks this sometimes does not fulfil requirements for availability.
- Tree topology is a mix of star and chain topology and gives the same advantages and disadvantages.
- Ring topology is probably the most used topology to build a robust network with reasonable costs. All access nodes have two-way connection to Core network and this means that even if one fails, there is still the other one left. The capacity will be limited but it is always possible to connect this node with high priority traffic.
- Meshed topology is similar to ring but even more robust and costs more. If some nodes are important and a third connection is needed this can be a solution.

Appendix A: REN Case Study

Integrated Telecommunications Management Network

REN - Rede Eléctrica Nacional, S.A., is responsible for the electricity transmission in Portugal.
REN was set up as a company in August 1994, during the split-up of EDP - Electricidade de Portugal, S.A., to which it already belonged as its Operational Department. Its history actually goes back to 1947, however, which was when the pioneer of electricity transmission in Portugal and its oldest ancestor, CNE - Companhia Nacional de Electricidade, S.A.R.L., was founded.
REN left the EDP in November 2000 when the European energy market was liberalized, requiring the legal separation of electricity transmission and of electricity distribution and production companies.
In particular, the Information System Division is responsible to assure reliable communication for all activities of the group based on own telecommunication infrastructure and telecommunication equipment divided into the following technologies:

- Power Line Communication (PLC);
- Plesiochronous Digital Hierarchy (PDH);
- Micro Wave (MW);
- Synchronous Digital Hierarchy (SDH);
- Dense Wavelength Division Multiplexing (DWDM).

The principal services provided are:

- SCADA network;
- Fixed and Mobile Private Voice Service;
- Data/IP – Local Area Network (LAN) / Wide Area Network (WAN);
- Video surveillance.

REN is also responsible for the operation of each of these technological platforms, for this propose individual management systems were implemented according to Telecommunication Management Network (TMN) standards.

Each of the management system interacts with the physical network equipments through dedicated communication channel running specific protocols. In order to have geographical redundancy it was also considered the implementation of a backup stand-by management system for each of those main systems, all of them have a replica for all critical data in order to restore the operation and supervision for the telecommunication network if something critical happens with the main servers.
The data synchronization between main and backup sites is provided through dedicated telecommunication channels (out band) or through the own network (in band).

Besides these all value data (database, log files, performance files and alarm history) is sent to the corporate servers responsible for the corporation data backup and also sent to a Disaster Recovery Site (DRS), which is also owned by REN.

The implementation presented before in shown in the Figure A1.1.

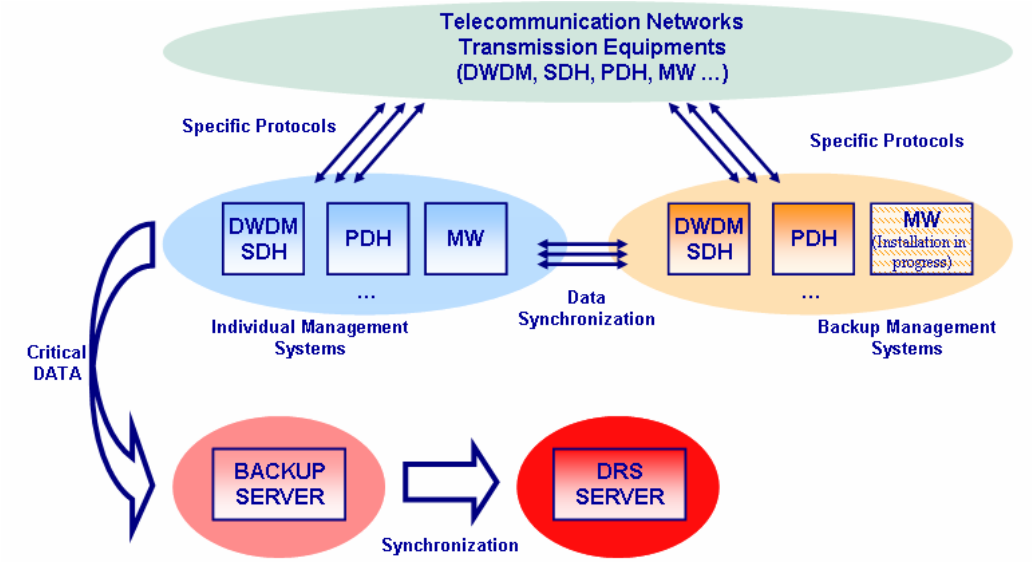

Figure A1.1 – REN's Telecommunication Management Network

REN has also one umbrella system used to integrate all alarms from all telecom platforms, in this way it's possible to have one unique view of all network and equipments in the network. This integrated system is also used to analyze the performance and statistics for the different services provides independently from the telecommunication technology used, as can be seen in Figure A1.2.

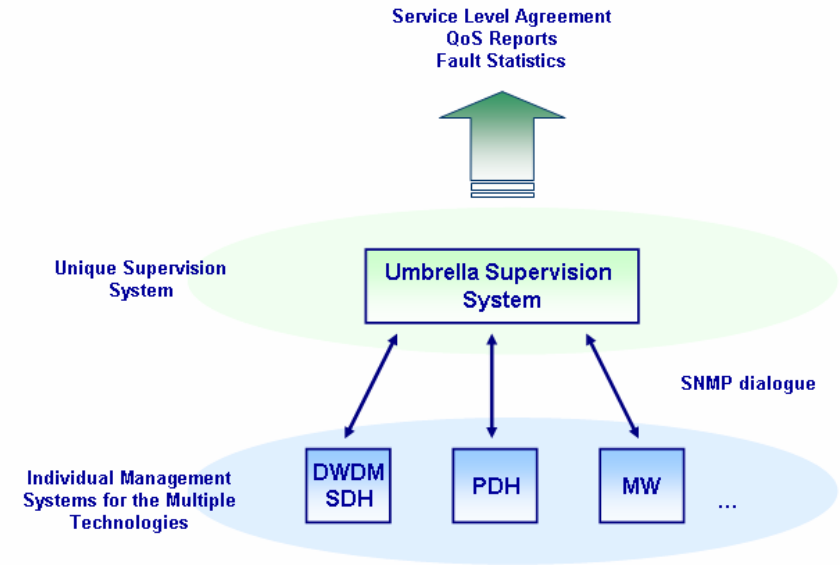

Figure A1.2 – REN's Umbrella System

This Integrated Telecommunication Management Network composed of several systems and applications reduce the maintenance task time and also facilitates the day-by-day services supervision. Other main characteristic is that all layers have open interface to the above or below layer in this way it's simple to integrate new systems.

Appendix B – Standards

- IEC/TR 62210 – Ed. 1.0 – 2003 - “Power system control and associated communications – Data and communication security”. Applies to computerised supervision, control, metering, and protection systems in electrical utilities. Deals with security aspects related to communication protocols used within and between such systems, the access to, and use of the systems. Discusses realistic threats to the system and its operation, the vulnerability and the consequences of intrusion, actions and countermeasures to improve the current situation.
- BS7799: Information technology: Code of practice for information security management. BS7799 is the UK national standard for best practice in information security derived from the International Standard ISO/IEC 17799:2000. This standard comes in two parts and replaces BS 7799-1:1999 which has now been withdrawn. It is a management standard, and explains how to build, maintain and improve an Information Security Management System (ISMS). It provides an excellent basis on which to build the management controls necessary to achieve an organisation´s mission, to manage risk, to assure effective control and to seek improvements where appropriate
- ISO/IEC 17799 - (2000) – “Code of Practice for Information Security Management”. As well as giving detailed security controls for computers and networks, also provides guidance on security policy, staff security awareness, and legal requirements.
- ISO/IEC 15408 (1999) – “Information technology - Security techniques – Evaluation criteria for IT security” - Part 1: Introduction and general model.
- ISO/IEC 15408 (1999) – “Information technology - Security techniques – Evaluation criteria for IT security” - Part 2: Security functional requirements. International Standard ISO/IEC 15408-2, was prepared by Joint Technical Committee ISO/IEC JTC 1, Information Technology, in collaboration with Common Criteria Project Sponsoring Organizations (CCPSO). The identical text of ISO/IEC 15408-2 is published by CCPSO as “Common Criteria for Information Technology Security Evaluation”
- Security functional components, as defined in this part of ISO/IEC 15408, are the basis for the TOE (Target of Evaluation) IT security functional requirements expressed in a protection profile (PP) or a Security Target (ST). These requirements describe the desire security behaviour expected of a TOE and are intended to meet the security objectives as stated in a PP or an ST.
- ISO/IEC 15408- (1999) – “Information technology - Security techniques – Evaluation criteria for IT security” - Part 3: Security assurance requirements. IEC Technical Committee N° 57 (Power Systems Management and Associated Information Exchange) has created a Working Group (WG 15) which studies “Data and communication security”.
- NIST (National Institute of Standards and Technology) Special publication 800-series. This series may be particularly useful for organizational information security management.

There are many other organizations outside the electrical field, like the American Gas Association (AGA), American Petroleum Institute (API), Chemical Industry Data Exchange/American Chemistry Council, Instrumentation, Systems, and Automation

Society (ISA), to mention only a few, that have been working in IT security and specifically in SCADA and Control Center security.

- AGA 12 (American Gas Association) has taken a unique approach to focus on securing the communications link between devices and the control servers or Control Center.
- API 1164 (American Petroleum Institute) is aimed at the small to medium size pipeline operator that needs basic and understandable information on securing their SCADA systems.
- CIDX/ACC (Chemical Industry Data Exchange/American Chemistry Council).This document provides broad, general guidance and ties in with the American Chemistry Council's (ACC) Responsible Care Program. The Responsible Care Program includes Management Practices such as "prioritization and periodic analysis of potential security threats, vulnerabilities, and consequences using accepted methodologies". The CIDX Guidance document then explains how each Management Practice is applicable to cybersecurity activities and how to apply the practice. CIDX has also analyzed a set of vulnerability assessment methodologies.
- Process Control Security Requirements Forum (PCSRF) was established by the U.S Government's National Institute of Standards and Technology (NIST). PCSRF is a group of vendors, end-users, industry groups, and government officials working together to secure the process control networks that make up the critical infrastructure in the US.
- PCSRF has selected the very rigorous and internationally recognized Common Criteria approach.
- SP99 is the Manufacturing and Control Systems Security Committee in the ISA (Instrumentation, Systems, and Automation Society). SP99 has focused on documenting guidelines and considerations for control system security in a set of Technical Reports (TR). TR1 is a guideline or resource document that identifies those activities that are important to provide electronically secure systems. A large part of the document provides information on a broad range of security technologies, such as authentication, encryption, and firewalls.

Appendix C - Definitions and Abbreviations

ACSI	Abstract Communications Service Interface
API	Applications Program Interface
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
BSNE	Business, Service Network and Element – layers of Management
CCTA	Central Computer and Telecommunications Agency (UK)
CMIS	Common Management Interface Service
CORBA	Common Object Request Broker Architecture
CRM	Customer Relationship Management
DCN	Data Communications Network
DMZ	De-Militarized Zone
EMS	Energy Management System
EoSDH	Ethernet over SDH
ERP	Enterprise Resource Planning
FCAPS	Fault, Configuration, Accounting, Performance, Security – Management functions
GIOP	General Inter-ORB Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
HTML	HyperText Markup Language
IEC	International Electrotechnical Commission
ICT	Information and Communications Technology
IDL	Interface Description Language
IED	Intelligent Electronic Device
IIM	Information Infrastructure Management
IIOP	Internet Inter-ORB Protocol
IP	Internet Protocol
IT	Information Technology
ITIL	IT Infrastructure Library
itSMF	IT Service Management Forum
ITU-T	International Telecommunications Union – Telecommunications Standardisation
J2CA	J2EE Connector Architecture
J2EE	Java 2 Platform, Enterprise Edition
JDBC	Java Database Connectivity
LAN	Local Area Network
MD	Mediation device
MIB	Management Information Base

MICS	Model Implementation Conformance Statement
MMI	Man Machine Interface
MML	Maker Markup Language
MTTR	Mean Time to Repair
NE	Network Element
NMS	Network Management System
NMC	Network Management Centre
OGC	Office of Government Comerse (UK)
ORB	Object request Broker
OSI	Open System Interconnection
OSS	Open Sourced Software
PDH	Plesiochronous Digital Hierarchy
PICS	Protocol Implementation Conformance Statement
PIXIT	Protocol Implementation eXtra Information for Testing
PLC	Power Line Carrier
PUM	Power Utility Management
Q3	Interface protocol suite defined in the ITU-T recommendations Q.811 and Q.812
QMD	Q interface mediation device
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RTU	Remote Terminal Unit
SA	Substation Automation
SCADA	Supervisory Control and Data Acquisition
SCL	Substation Configuration Language
SCSM	Specific Communication Service Mapping
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
TCP	Transport Control Protocol
TNM	Telecommunications Network Management
UDDI	Universal Description, Discovery and Integration service
UML	Unified Modelling Language
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network (LAN)
VoIP	Voice over IP
VPN	Virtual Private Network
WSDL	Web Service Description Language
WAN	Wide Area Network
XML	Extensible Markup Language

REFERENCES

[1] M. Mesbah. “Event Management in Power Utility Communication and Information Exchange Systems”, CIGRE Colloquium paper D2-E07, Cuernavaca, México, June 2005.

[2] M. Mesbah. “Management of Information Technology Infrastructure in the Power Utility, A Consolidated Approach” CIGRE paper D2-301, Paris, France, August 2006.

[3] IEC 61850 Series. Communication networks and systems in substations.

[4] IEC 61850-7-2, Communication networks and systems in substations - Part 7-2: Basic communication structure for substation and feeder equipment - Abstract communication service interface (ACSI).

[5] IEC 61850-7-2, Communication networks and systems in substations - Part 8-1: Specific Communication Service mapping (SCSM) - Mapping to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3.

[6] Web Services, a new Approach to Substation Management.
J. Bembibre (Red Eléctrica de España); C. Samitier (GNE, S.L.)

[7] ITU-T Q series

[8] TCP/IP Tutorial and Technical Overview, IBM REDBOOKS

[9] http://www.protocols.com

[10] http://www.w3schools.com/xml/default.asp

[11] http://www.xml.com/pub/a/98/10/guide0.html

[12] www.niscc.gov.uk

[13] http://www.itsmf.org

[14] http://www.tmforum.org