Power Systems Monitoring and Control using Telecom Network Management Standards

S. Díaz, J. Luque, M.C. Romero and J. I. Escudero

Abstract-- **Historically, different solutions have been developed for power systems control and telecommunications network management environments. The former was characterized by proprietary solutions, while the latter has been involved for years in a strong standardization process guided by criteria of openness. Today, power systems control standardization is in progress, but it is at an early stage compared to the telecommunications management area, especially in terms of information modeling. Today, control equipment tends to exhibit more computational power, and communication lines have increased their performance. These trends hint at some conceptual convergence between power systems and telecommunications networks from a management perspective. This convergence leads us to suggest the application of well-established telecommunications management standards for power systems control. This paper shows that this is a real medium-to-long term possibility.**

Index Terms—**Power system monitoring, Power system control, Data communication, Computer network management, ITU, ISO, Internet.**

I. Introduction

Our main objective in this paper is to suggest a brand new approach for carrying out power control, consisting in the adoption of well-established telecommunications network management standards. Although originally developed for this specific environment, we find they are also suitable for the power systems area, taking into account current trends in this field. Telecommunications management standards provide an open approach for the management of diverse equipment, by defining a common set of rules to follow for modeling, structuring and accessing management information.

In Section II and III we discuss the singularities of both telecommunications and power systems environments, while Section IV focuses on the reasons that gave rise to this proposal. Section V shows the similarities between both environments and proposes a mapping from the current telecontrol approach onto a standard telecommunications management architecture. Comments on gradual migration from legacy SCADA/EMS to telecommunications management architectures are provided in Section VI. Conclusions by the authors are collected in Section VII.

II. Telecommunications Network Management Overview

In the telecommunications area, the equipment to be managed is very diverse, with many different technologies and suppliers in the market. Communication lines in telecommunications networks are usually fast, typically in the Mbps range. These characteristics lead to open solutions for network management, which allow interconnectivity and interoperability between those different elements – no matter if the protocols used for this purpose are not especially lightweight. Within this framework, we find two widely applied standards: SNMP (Simple Network Management Protocol) [1] and TMN (Telecommunications Management Network) [2]. These solutions are basically characterized by defining the following:

- physical and functional architectures,
- a management information model, and
- a protocol for information interchange.

We address the fundamentals of both management technologies in the following paragraphs.

A. Simple Network Management Protocol

SNMP is an Internet standard frequently used in computer network management applications, and, though at first it was considered a simple, short-term solution in telecom management, the reality is that its acceptance in the industry is still increasing.

SNMP functional architecture distinguishes between two software components: the *agent* and the *manager*. An agent is related to a managed resource (which can be physical or logical) and contains the managed objects which represent its properties. These objects can be read or written by the manager at any time. Reading a managed object can result in some kind of access to the managed resource, as writing to a managed object can result in the modification of some characteristic or in the firing of some action on the managed resource. This architecture also contains the notion of *proxy agent*. A proxy agent is needed when some kind of translation between a SNMP environment and a non-SNMP environment should be done.

Agents and managers could be deployed on physical components in different ways, leading to distinct physical

S. Díaz is with the Departamento de Tecnología Electrónica, Universidad de Sevilla, Sevilla, 41012 SPAIN (e-mail: sdiaz@dte.us.es).

J. Luque is with the Departamento de Tecnología Electrónica, Universidad de Sevilla, Sevilla, 41012 SPAIN (e-mail: jluque@us.es).

M. C. Romero is with the Departamento de Tecnología Electrónica, Universidad de Sevilla, Sevilla, 41012 SPAIN (email: mcromero@dte.us.es).

J. I. Escudero is with the Departamento de Tecnología Electrónica, Universidad de Sevilla, Sevilla, 41012 SPAIN (e-mail: ignacio@us.es).

architectures. An agent is a process which runs inside the managed device (or in a module attached to it) and hosts the managed resource(s). Proxy agents run outside the device, in a separate box, but physically connected to it. The manager is also a process but it is run in the management station. Managed resources and management station are connected to a network which enables the communication among them. In large environments, it may be necessary to split the management system in logical *subdomains*, leading to a hierarchical architecture known as *manager of managers*. There is a *top-level* manager which manages the entire network, and several *mid-level* managers which are responsible for each subdomain. These mid-managers exhibit manager behavior from the managed devices perspective, and agent behavior from the top-level manager perspective. See Fig. 1. Virtually, this structure can exhibit any number of levels.

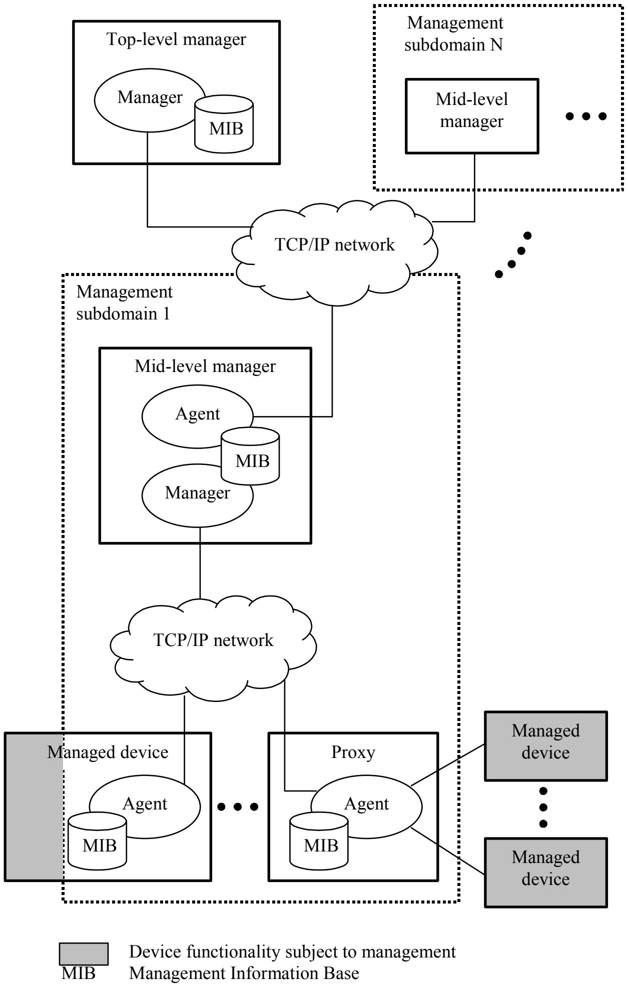


Fig.1. SNMP physical and logical architecture.

Managed objects and their structure conform the *management information model*. These are described using a relatively small subset of ASN.1 type constructors, as specified in the standard SMI (Structure of Management Information) document [3]. The models are organized in modules known as *MIBs* (Management Information Base), provided as text files. There are a large number of generic and specific MIBs defined for SNMP management. Managed objects are restricted to atomic and tabular types and are placed into a tree-shaped structure, which represents containment. There is no notion of object *class* and thus there is no inheritance possible. The model is not object-oriented despite the term "managed *object*".

Management information, in form of managed objects, can be interchanged by SNMP protocol messages. These messages are issued under service requests made by the agent or the manager processes. SNMP managers use services to get and set managed object values in agents, and agents use services to send confirmed or unconfirmed asynchronous notifications to managers.

More information about SNMP can be found in the References Section.

B. Telecommunications Management Network

TMN presents a more elaborated, object-oriented framework, developed by ITU-T (International Telecommunications Union – Telecommunications standardization sector) over existing ISO OSI (International Organization for Standardization Open Systems Interconnection) management standards. TMN is a recommendation focused on the management of large telecommunications networks. The term *TMN* refers itself to a data network, conceptually (but may not physically) separated from the telecommunications network, where management information flows.

In TMN, the functional architecture is built upon different types of functional blocks:

- *Network Element* Functions (NEFs) represent the functionality of network devices from a management perspective;
- *Operations Systems* Functions (OSFs) process management data in order to monitor, coordinate and/or control both telecommunications and management functions;
- *Workstations* Functions (WSFs) provide a means for the human user to access management information;
- *Q Adaptor* Functions (QAFs) allow the integration of non-TMN entities in the TMN environment; and
- *Mediation* Functions (MFs) translate data between OSFs and NEFs/QAFs when their respective information models differ in their abstraction level. This translation may imply the storage, adaptation, filtering, thresholding and/or condensation of the information.

To represent the communication between two functional blocks, TMN introduces the concept of *reference point*. In a reference point, the blocks involved communicate using the manager-agent paradigm, as in SNMP. In TMN, all the management environment is functionally split into four layers depending on its scope: *element* management, *network* management, *service* management and *business* management. Then, each functional block can be placed in one of these layers.

The functional blocks are placed in physical boxes or *building blocks* in TMN terminology. The building blocks taxonomy resembles the functional blocks one: there are *Network Elements* (NEs), *Operations Systems* (OSs), *Workstations* (WSs), *Q Adaptors* (QAs) and *Mediation Devices* (MDs). Each one of these blocks can perform one or more TMN functions, e.g. an OS building block contains an OSF functional block, but it also may contain MF, QAF or WSF functional blocks. Building blocks can communicate via a *Data Communications Network* (DCN), which they are connected to by means of physical *interfaces*. A TMN interface is, therefore, the physical realization of a reference point that is between functional blocks placed on different building blocks. Fig. 2 summarizes these points. Note the similarity between this architecture and that of SNMP despite differences in terminology.

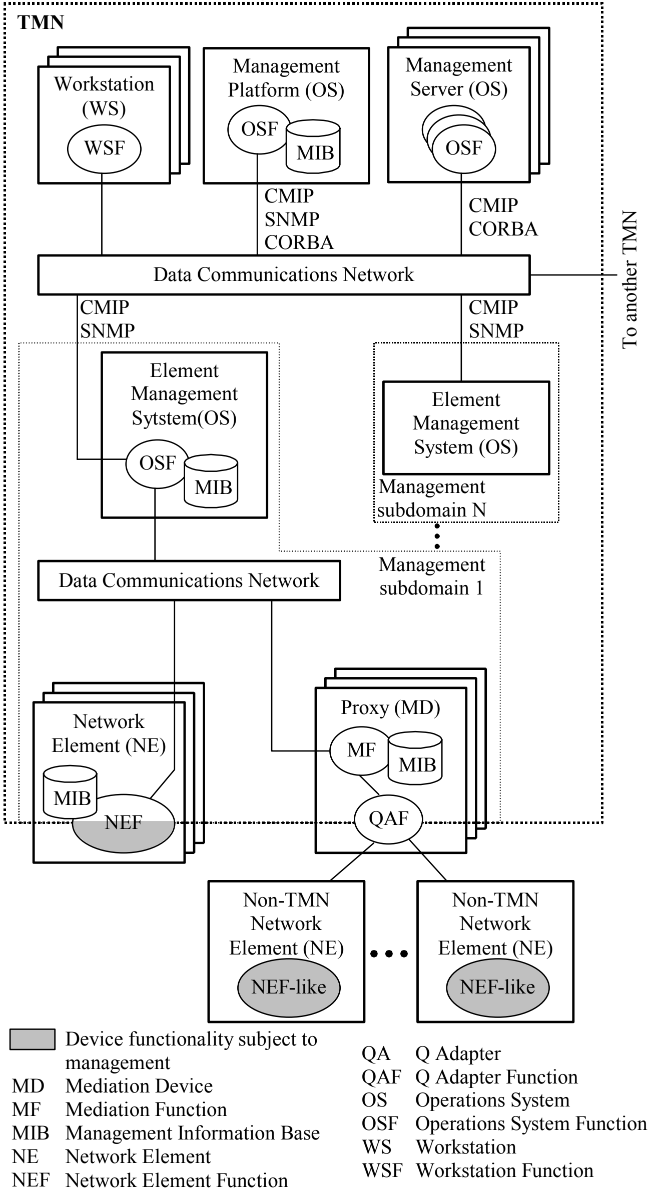


Fig. 2. TMN physical and logical architecture.

TMN information architecture is fully imported from OSI management. A management information model is specified in terms of *object classes* built upon *packages* which can contain *attribute*, *action* and *notification* definitions. This is a true object-oriented model with support for (multiple) inheritance and containment (i.e., aggregation). In particular, containment relationship leads to a tree-shaped arrangement of the object instances, known as the *containment tree*, which is also used for instance naming. A management information model in OSI (and hence TMN) is specified by using the Guidelines for the Definition of Managed Objects (GDMO) [4], which introduces a concrete syntax for that purpose. GDMO provide text-based templates to define each element of the model (class, package, behavior, attribute, attribute group, action, notification, relationship, etc.), relying on ASN.1 only for specifying the basic data types. A management information model is provided, therefore, as a set of GDMO and ASN.1 text files. OSI management standards define a set of classes (using GDMO) which are the basis of the TMN generic network information model. This model is then specialized for specific network types.

CMIP (Common Management Information Protocol) is the main protocol in TMN/OSI management standards, though it is not the only choice. CMIP messages are issued under CMIS (Common Management Information Service) service requests, which enable the manipulation of the objects: get/set attribute values, start actions, create/delete object instances and report events. CMIS uses a selection mechanism known as *scoping and filtering* in order to define the set of objects which the protocol operation will be applied to. In essence, scoping uses the containment tree as basis to select the subtree of instances where the filter will be applied to. Only those instances which were selected by scoping and passed the filter test will be used as destination for the protocol operation.

TMN and OSI management standards define a rich set of management functions. These functions can be seen as extensions to the services provided by CMIS, facilitating the performance of management tasks such as: event reporting, log control, state management, etc.

TMN is more powerful than SNMP, but also more complex and expensive. Nevertheless, TMN can interact with SNMP by means of a gateway. Merging adequately both approaches, a cost-effective and financially less risky solution can be reached. It also enables a way to a gradual migration from SNMP to TMN, if needed. TMN can also interact with CORBA (Common Object Request Broker Architecture), an solution mainly adopted in service management area.

More information about TMN and OSI management can be found in the References Section.

III. Power Systems Control Overwiew

Telecontrol is basically structured in SCADA (Supervisory Control And Data Acquisition) and RTUs (Remote Terminal Units). The SCADA system is placed on the CC (Control Center), monitoring and controlling the RTUs. Each RTU belongs to a substation, managing its power devices. Usually, a group of study applications run over the information managed by the SCADA, in order to estimate the network state and its parameters, determine the optimal power flow, etc. These application are usually referred as EMSs (Energy

Management Systems).

Traditionally, power systems equipment was not very diverse, so openness was not so important. RTUs were simple and lacked intelligence. Moreover, power systems have been using slow communication lines for telecontrol, such as legacy power line communications and radio-relays. Delays are critical in alarm notification, so protocols were designed lightweight and efficient to deal with low transmission rates, but they also became unlayered and, very frequently, proprietary.

Currently there is a deployment of new communication facilities in progress throughout the power systems, such as OPGW (Optic Fiber Composite Overhead Ground Wire) and fast power line communications. Therefore, data bandwidth has increased over traditional telecontrol communication lines, supporting the distribution of intelligence. Current substation automation systems and IEDs (Intelligent Electronic Devices), can support a broader functionality than legacy RTUs. Diversity among telecontrol systems has increased as well as market choices. Therefore, openness now becomes a necessity against proprietary implementations.

Efforts are being made, mainly by some IEC (International Electrotechnical Commission) workgroups, to standardize telecontrol systems. Fig. 3 shows the telecontrol architecture proposed by IEC. According to IEC, control centers are composed by a set of servers running energy and distribution management applications (EMS and DMS) over SCADA services. The SCADA monitors and control the substations belonging to the control center domain. The telecontrol of the substation devices (switchgears, transformers, etc.) is carried out through its associated remote terminal unit or substation automation system.

IEC standards span the whole telecontrol architecture. Specifically, we want to highlight the following:

- IEC 60870-5 specifies a set of protocols aimed to the exchange of telecontrol information between RTU-CC, and inter-RTU. They follow the approach of traditional telecontrol protocols, but with the benefit that they are standardized.
- IEC 60870-6 or TASE.2 (Telecontrol Application Service Element 2) defines a set of server objects and a protocol to support the inter-CC communications, though the specification does not preclude the possibility of its use for RTU-CC communications [5].
- IEC 61850 deals with substation communications and systems. Specifically, 61850-7, proposes an object-oriented information model for the representation of substation devices [6] [7] [8].
- IEC 61968 and 61970 define standard interfaces for DMS and EMS systems, enabling an easier integration of these applications in the system.

IV. Motivation

The increment in the capacity of the communication lines means that electric utilities can use their data networks not only for telecontrol, but also for their own telecommunications needs. Furthermore, even with these distributed applications running, there is an excess of bandwidth which can be marketed. Thus, electric utilities, in a medium-to-long term, can enter the telecommunications market, offering data and voice services, e.g,, Internet access to residential users [9]. In this context, it will be necessary to deploy a telecommunications management system throughout the network. Power systems control standards are not flexible enough to be adapted to telecommunications management, so the obvious solution would be the use of separate architectures for power control and telecommunications management. Nevertheless, we find that a unified solution is possible, based on already existing telecommunications management standards, such as SNMP or TMN. This is the issue we address, from a technical point of view, in the next chapters.

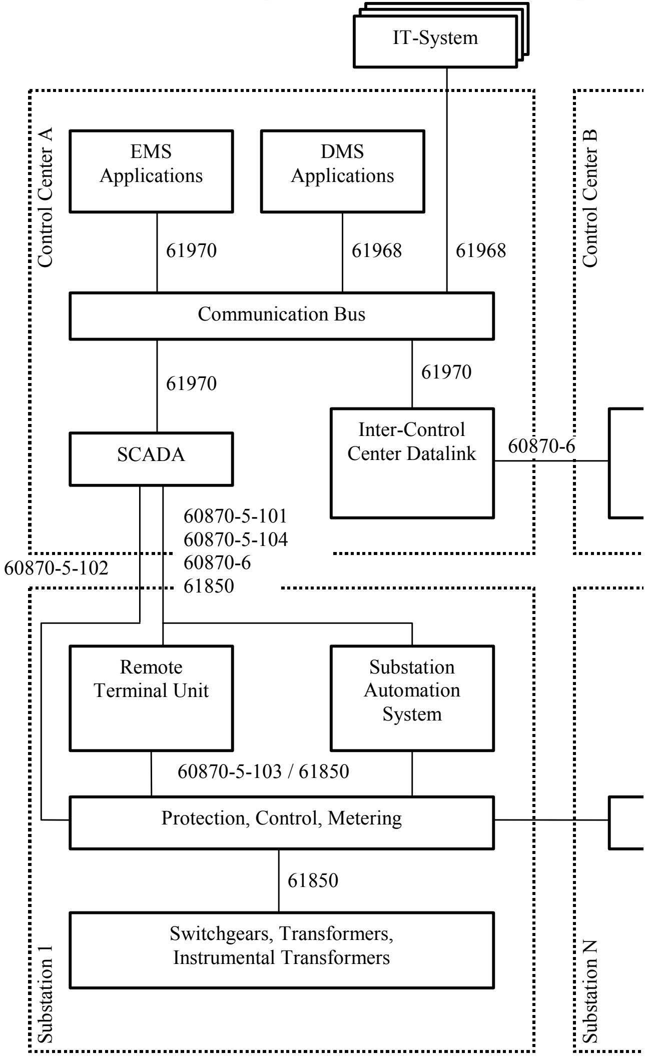


Fig. 3. IEC telecontrol architecture.

Provided that electric utilities face, or will do in the near future, telecommunications management requirements, the adoption of TMN and/or SNMP for both power system control and telecommunications network management environments imply the adoption of the same software tools and platforms for them. This will reduce the costs related to the purchase, implantation, operator training and maintenance of the telecontrol and management software systems.

Moreover, experience on TMN and SNMP span several years, with great success; many tools, platforms and management applications are available in the market today at affordable prices due to the competition of a large number of vendors. Some power systems IEC key standards, such as the 61850 set, are still under development or in an early stage of production compared to TMN/SNMP.

V. Mapping Telecontrol Systems onto a Telecommunications Management Architecture

We propose the application of TMN/SNMP management architectures to RTU-CC, intra-CC and inter-CC scopes. Communication of management information inside a substation can be done by legacy protocols, DNP3 or IEC 60870/61850 standard protocols; the integration with the rest of the telecontrol system is responsibility of the RTU or substation automation system.

To show how TMN/SNMP can be applied to power systems telecontrol, we address the following key issues:

A. The mapping of IEC telecontrol architecture onto TMN/SNMP physical and functional architectures;
B. The description of power devices using GDMO or SNMP SMI syntax, including a simple example;
C. The mapping of usual telecontrol services to CMIP/SNMP protocol operations.
D. Security against external network attacks.

A. Architectural mapping

The architectural mapping can be deduced by comparing the architectures shown on Figs. 1-2 and Fig. 3. In a control center, the SCADA system can be implemented as a network management platform, having a view of every power network device in the management domain, and providing basic management services to the EMS/DMS applications. These are manager processes carrying out network and service management functions. This management platform could be deployed following a hierarchical structure in order to optimize polling. At substation level, proxy agent processes run in the RTUs or substation automation systems, performing Q-adaptor functions and mediation functions. Devices such as switchgears, transformers, protections, etc. are out of the scope of the management network, being under the jurisdiction of the RTU or substation automation system. Fig. 4 summarizes these points showing both physical and functional blocks, using, as reference, TMN notation.

Normally, this management architecture will be integrated with the existing telecontrol architecture. Integration and migration issues are covered in Section VI.

The architecture depicted in Fig. 4 would eventually evolve to a model whose network elements would become TMN/SNMP-compliant so the RTUs could simply be replaced by network routers. This is the approach that telecommunications management takes.

B. Telecontrol information mapping

Managed devices are represented by managed objects which reside in the MIB-caches associated to the TMN/SNMP-compliant RTUs or substation automation systems. These objects are instances of the managed classes which are specified in MIB modules, using a standard notation such as GDMO or SNMP SMI syntax. These classes can be based on IEC 61850-7 standards. The management platform, performing SCADA functions, uses the MIB modules to learn the capabilities of the objects to manage.

As a example, a *circuit breaker* can be described using GDMO and ASN.1 syntax, see Fig. 5. This example is based on IEC 61850-7-4 `XCBR` class [7] [8]. `circuitBreaker` class is defined with a `MANAGED OBJECT CLASS` template as a specialization of `logicalNode` class. Then, `circuitBreaker` is characterized by the following packages: `basicLogicalNodeInfoPackage` (inherited from `logicalNode`), `controllableDataPackage` and `statusInformationPackage` (which are specialized `circuitBreaker` packages). Each package must be further defined in a `PACKAGE` template, in terms of attributes, notifications and actions. In this example, for the sake of simplicity, some parts of the complete definition are omitted. Notifications and actions (defined using `NOTIFICATION` and `ACTION` templates) are commented in Subsection C, regarding protocol operations.

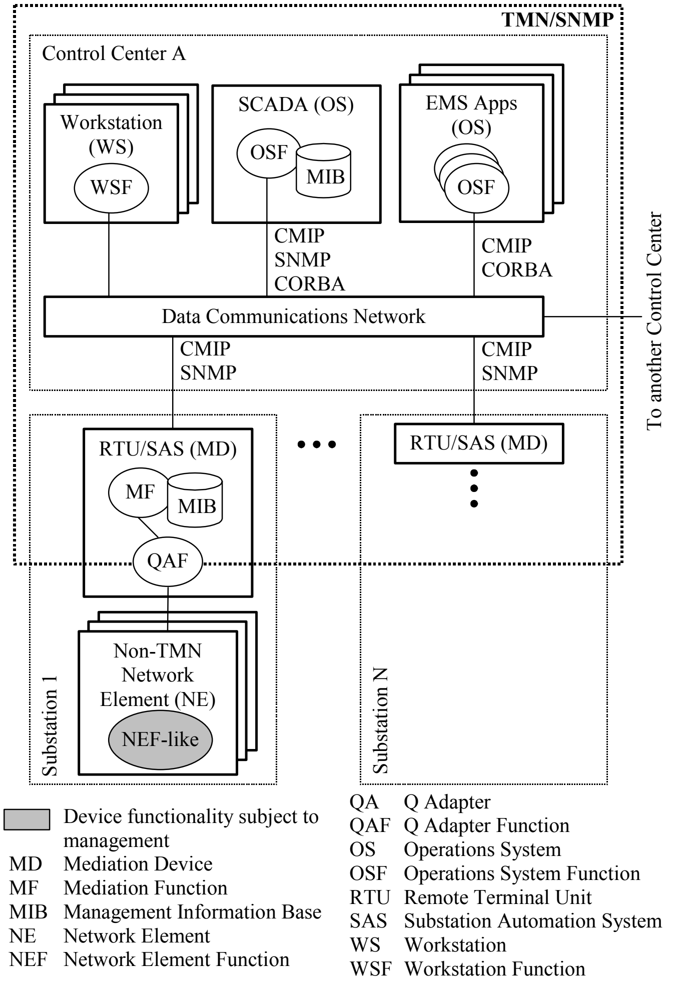
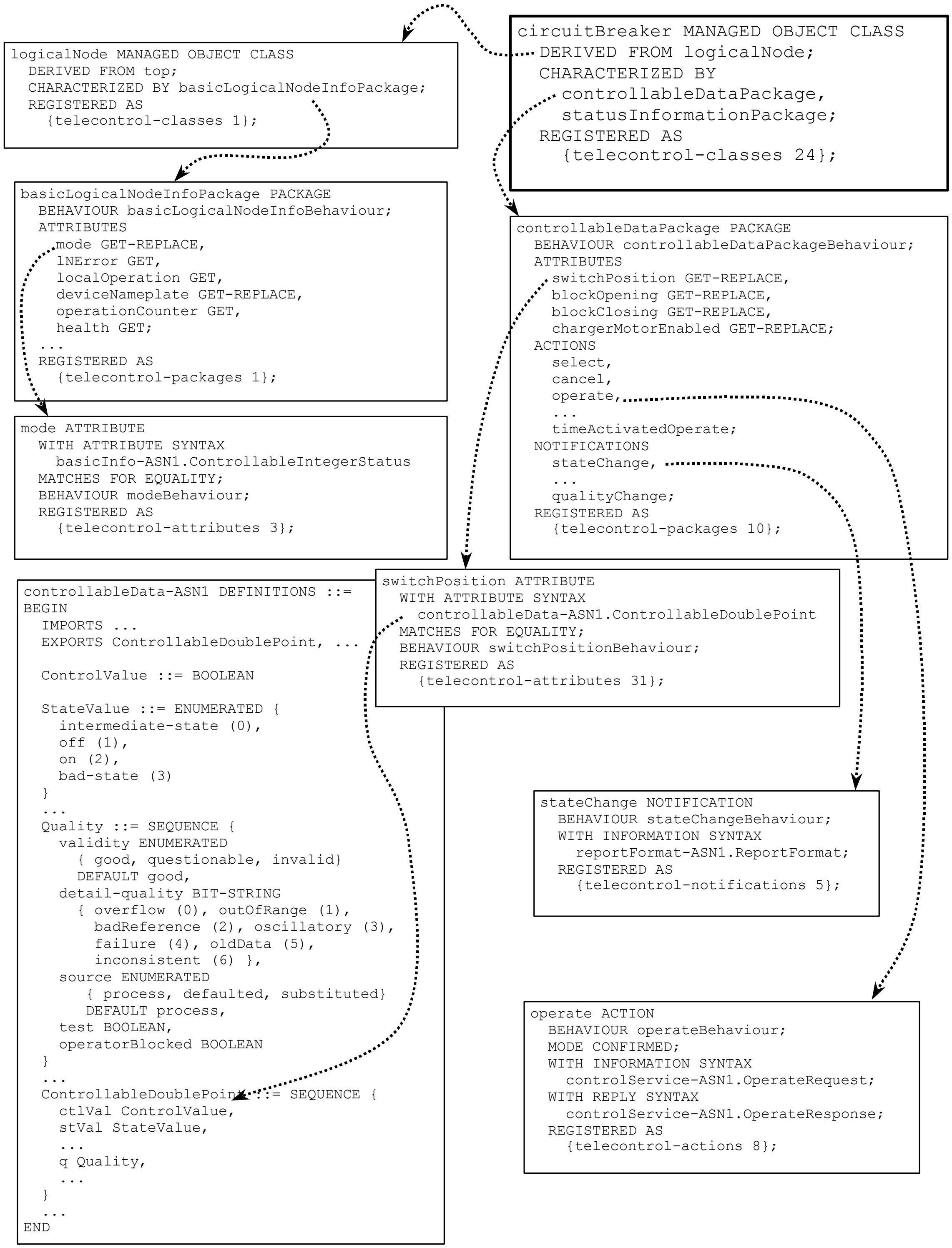


Fig. 4. Physical architecture of a TMN/SNMP-compliant power system management environment.



```
circuitBreaker MANAGED OBJECT CLASS
  DERIVED FROM logicalNode;
  CHARACTERIZED BY
    controllableDataPackage,
    statusInformationPackage;
  REGISTERED AS
    {telecontrol-classes 24};
```

```
logicalNode MANAGED OBJECT CLASS
  DERIVED FROM top;
  CHARACTERIZED BY basicLogicalNodeInfoPackage;
  REGISTERED AS
    {telecontrol-classes 1};
```

```
basicLogicalNodeInfoPackage PACKAGE
  BEHAVIOUR basicLogicalNodeInfoBehaviour;
  ATTRIBUTES
    mode GET-REPLACE,
    lNError GET,
    localOperation GET,
    deviceNameplate GET-REPLACE,
    operationCounter GET,
    health GET;
  ...
  REGISTERED AS
    {telecontrol-packages 1};
```

```
mode ATTRIBUTE
  WITH ATTRIBUTE SYNTAX
    basicInfo-ASN1.ControllableIntegerStatus
  MATCHES FOR EQUALITY;
  BEHAVIOUR modeBehaviour;
  REGISTERED AS
    {telecontrol-attributes 3};
```

```
controllableDataPackage PACKAGE
  BEHAVIOUR controllableDataPackageBehaviour;
  ATTRIBUTES
    switchPosition GET-REPLACE,
    blockOpening GET-REPLACE,
    blockClosing GET-REPLACE,
    chargerMotorEnabled GET-REPLACE;
  ACTIONS
    select,
    cancel,
    operate,
    ...
    timeActivatedOperate;
  NOTIFICATIONS
    stateChange,
    ...
    qualityChange;
  REGISTERED AS
    {telecontrol-packages 10};
```

```
switchPosition ATTRIBUTE
  WITH ATTRIBUTE SYNTAX
    controllableData-ASN1.ControllableDoublePoint
  MATCHES FOR EQUALITY;
  BEHAVIOUR switchPositionBehaviour;
  REGISTERED AS
    {telecontrol-attributes 31};
```

```
controllableData-ASN1 DEFINITIONS ::=
BEGIN
  IMPORTS ...
  EXPORTS ControllableDoublePoint, ...

  ControlValue ::= BOOLEAN

  StateValue ::= ENUMERATED {
    intermediate-state (0),
    off (1),
    on (2),
    bad-state (3)
  }
  ...
  Quality ::= SEQUENCE {
    validity ENUMERATED
      { good, questionable, invalid}
      DEFAULT good,
    detail-quality BIT-STRING
      { overflow (0), outOfRange (1),
        badReference (2), oscillatory (3),
        failure (4), oldData (5),
        inconsistent (6) },
    source ENUMERATED
       { process, defaulted, substituted}
       DEFAULT process,
    test BOOLEAN,
    operatorBlocked BOOLEAN
  }
  ...
  ControllableDoublePoint ::= SEQUENCE {
    ctlVal ControlValue,
    stVal StateValue,
    ...
    q Quality,
    ...
  }
  ...
END
```

```
stateChange NOTIFICATION
  BEHAVIOUR stateChangeBehaviour;
  WITH INFORMATION SYNTAX
    reportFormat-ASN1.ReportFormat;
  REGISTERED AS
    {telecontrol-notifications 5};
```

```
operate ACTION
  BEHAVIOUR operateBehaviour;
  MODE CONFIRMED;
  WITH INFORMATION SYNTAX
    controlService-ASN1.OperateRequest;
  WITH REPLY SYNTAX
    controlService-ASN1.OperateResponse;
  REGISTERED AS
    {telecontrol-actions 8};
```

Fig. 5. Partial example of management information definition using GDMO: circuitBreaker class.

`ATTRIBUTE` templates specify the data type of the attribute along with their allowable matching tests. Attribute data types are defined using ASN.1 basic and structured constructs in separate ASN.1 modules, such as `controllableData-ASN1` in the example. Attributes can be grouped to create data sets.

Every GDMO element definition should be registered to assure its uniqueness. In the example, we arbitrarily assigned unique values to the classes, packages and attributes using the `REGISTERED AS` clause. In a real-world case, registration should be conducted by a recognized authority.

GDMO definitions are machine-readable and can be compiled to automatically obtain instrumentable code for agent development. Package, attribute, notification, etc. behaviour should be implemented manually because `BEHAVIOUR` templates (referenced but omitted in the example) are specified in natural language.

C. Protocol operations and services mapping

Data attributes can be read or modified, provided that their access requirements are met, using *get* and *set* CMIP or SNMP operations.

Event reporting in TMN can be carried out by means of *event-report* CMIP operation and ITU-T X.734 management function, which introduces an event forwarding discriminator class that filters notifications emerging from managed objects, and redirects them to the specified destinations. The notifications that an object can issue are defined, along with their parameters, in `NOTIFICATION` templates referenced from the packages included in the GDMO class definition of that object, as it is done in the example with `stateChange` notification. Event format should be defined in an ASN1 module. Event logging, ITU-T X.735, is similar to event reporting except that the destination is a log file. Both TMN event reporting and logging mechanism are very similar to that of IEC 61850-7-2 [6]. In SNMP, event reporting mechanism is based on *trap* and *inform* protocol messages. Filtering and logging design is up to the SNMP MIB developer.

Telecontrol specific services such as value substitution or *select-before-operate* control [6] can be implemented in TMN as *action* CMIP operations and specified in GDMO using `ACTION` templates. Actions are referenced in the packages imported by the classes which actually perform them. In the example, the `operate` action is defined as a confirmed service; its request and response format should be specified using ASN.1 types. In SNMP, such services can be mapped onto *set* operations, performed over a group of variables representing the action arguments, and a special variable whose behavior consists in firing the action when it is written. Again, specific design is up to the SNMP MIB developer.

Finally, CMIP has support for the dynamic creation or deletion of object instances. In SNMP case, this behavior should be implemented by means of *set* operations.

D. Security issues

The security of the telecontrol systems against external attacks is an important issue if the utility telecommunications network routes user data traffic (e.g. by offering Internet services) along with telecontrol information. Security mechanisms must be deployed to assure reliability of the power system.

Fortunately, CMIP and SNMP can be used in secure distributed applications by using cryptographic keys for authentication and encryption. In particular:

- CMIP protocol can work over Internet IPsec (IP security protocol) or ISO NLSP (Network Layer Secure Protocol);
- SNMPv3 embeds a cryptographic security mechanism, though it is also possible to employ the more widely available SNMPv2 over IPsec.

Telecommunications network management and power system telecontrol, even built upon the same kind of systems, are separate distributed applications and this can be taken into account when designing the data network and configuring access control rules into the routers, in order to reduce potential security risks.

VI. Migration and Coexistence Between Legacy and TMN/SNMP-based Telecontrol Systems

For TMN/SNMP management to be successful as option for power systems telecontrol, it must be easy to:

- migrate from legacy telecontrol subsystems to TMN/SNMP-compliant subsystems; and
- integrate new TMN/SNMP-compliant subsystems with existent telecontrol subsystems.

These requisites enable a cost-effective planning of telecontrol systems as an integrated mixture of upgradeable technologies.

At control center level, existing telecontrol systems and TMN/SNMP systems can be integrated by means of gateways, responsible of the translation between protocols and information models. For example, a CMIP/SNMP-IEC 61850 gateway could be developed to reach interoperability between those systems, especially if the TMN/SNMP MIBs are based on the 61850 standard classes definition. Moreover, existing IEC 61970-based EMS applications could interact with the TMN/SNMP platform via a CORBA gateway.

At substation level, legacy RTUs can be integrated into a TMN/SNMP environment by developing a custom proxy agent. This agent will be similar to the one embedded in a TMN/SNMP-compliant RTU, because it will implement the same functions, but it will be deployed in a separate hardware module. Another option would be the simultaneous integration of several legacy RTUs by a proxy agent module located in the control center. Both approaches are shown in Fig. 6.

Tools for agent development already exists in the market. These tools aid in the definition of the MIB module, its compilation and the generation of a code skeleton which can be completed to implement managed object behaviors and protocols for the communications with the legacy RTU.

VII. Conclusions

Telecommunications management architectures utilize standard protocol and information models, thus assuring interoperability among the physical and logical management entities. These protocols and models, designed for the management of telecommunication networks and services, are flexible enough to be adapted to energy management following the guidelines described in Section V.

Today utilities are experiencing an increment in their data bandwidth due to recent developments such as fast power line communications and the installation of optic fiber in high voltage power networks. Consequently, energy utilities are now interested in providing telecommunication services such as data transport, Internet access or voice over IP (Internet Protocol). These utilities can use the same solution for telecommunications management and energy management, which may help in reducing purchase, implantation, training and maintenance costs, by using well-known telecommunications management platforms and tools. Nevertheless, configuration and management of both domains can be done separately though the same kind of systems have been implanted for them, in order to delegate these tasks to different departments and increase security at the same time.

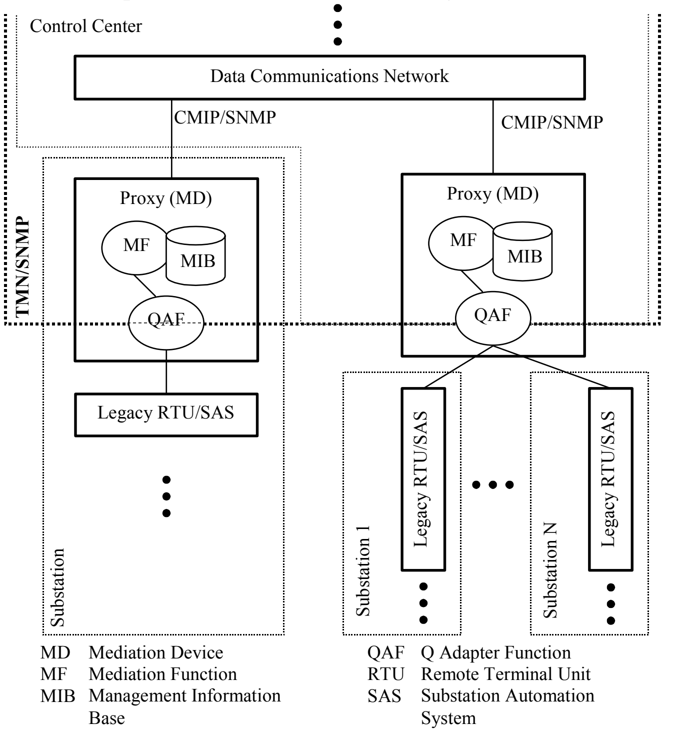


Fig. 6. Integrating legacy RTUs to a TMN/SNMP environment.

This paper introduces the fundamentals behind the adaptation of TMN/SNMP standards for power system telecontrol, leaving open several topics for further discussion. These topics include the development of a complete GDMO/SNMP SMI specification of power devices, maybe using IEC 61850-7 as a guide (like the example in Section V); the implementation of gateways for the integration with traditional telecontrol systems; the evaluation of security mechanism; and the analysis of CMIP/SNMP efficiency as real-time protocols. Also, communications network design is an essential issue which must be dealt with great care because it has a high impact on both performance and costs. In particular, if a utility decides to offer telecommunications services, the most appropriate solution would be an IP-based network. Therefore, if a management solution is needed for the power system control, it is natural to profit from having an IP network and implanting a CMOT (CMIP over TCP/IP) and/or SNMP-based management environment. Nevertheless, some critical requirements must be met in order to use of IP for telecontrol tasks [10].

VIII. References

[1] Introduction to Version 3 of the Internet-standard Network Management Platform, RFC 2570, Apr. 1999 [Online] Available: http://www.rfc-editor.org/rfc/rfc2570.txt

[2] Principles for a Telecommunications Management Network, ITU-T Recommendation M.3010, 2000

[3] Structure of Management Information Version 2 (SMIv2), RFC 2578, Apr. 1999 [Online] http://www.rfc-editor.org/rfc/rfc2578.txt

[4] Information Technology – Open Systems Interconnection – Structure of Management Information – Guidelines for the Definition of Managed Objects, ITU-T Rec. X.722, 1992

[5] Telecontrol Equipment and Systems – Part 6-505: Telecontrol Protocols Compatible with ISO Standards and ITU-T Recommendations – TASE.2 User Guide, IEC 60870-6-505, 2002

[6] Communications Networks and Systems in Substations – Part 7-2: Basic Communication Structure for Substations and Feeder Equipment – Abstract Communication Service Interface (ACSI), IEC (draft) 61850-7-2, 2002

[7] Communications Networks and Systems in Substations – Part 7-3: Basic Communication Structure for Substations and Feeder Equipment – Common Data Classes, IEC (draft) 61850-7-3, 2002

[8] Communications Networks and Systems in Substations – Part 7-4: Basic Communication Structure for Substations and Feeder Equipment – Compatible Logical Node Classes and Data Classes, IEC (draft) 61850-7-4, 2002

[9] S. Díaz, “El uso de arquitecturas de gestión de comunicaciones en el telecontrol de redes eléctricas,” Dpto. de Tecnología Electrónica, University of Seville, Spain. Rep. TESP-0202-022, Mar. 2002.

[10] C. Samitier, J. Darné. The Use of the IP Technology to Deploy a Modern Telecontrol Network. Presented at Distributech 2001. [Online]. Available: http://www.gne-eng.com/Files/IP_TC_2001_paper.pdf

IX. Biographies

S. Díaz received his degree in Computer Engineering in 1999 from the University of Seville (Spain). At present he is working in his Ph. D. thesis in Power System Control.

Since 1999 he has worked in several research projects focused on telecommunications network management, protocol engineering and power systems telecontrol at the University of Seville. In 2000 he became Associate Professor and began his teaching work in the School of Computer Engineering, University of Seville.

J. Luque received his degree in Industrial Engineering in 1980 and his Doctorate in Industrial Engineering in 1986 from the University of Seville (Spain).

Since 1980 he has worked for several companies in the area of SCADA systems for electrical networks, participating in some of the primary EMS projects in Spain. He is currently Professor of electronic engineering at the University in Seville, and is a member of the IEEE.

M. C. Romero received her degree in Computer Engineering in 1999 from the University of Seville (Spain). At present she is working in her Ph. D. thesis in Multimedia Control of Power Systems.

Since 1999 she has worked in several research projects focused on telecommunications network management and power systems telecontrol at the University of Seville. In 2001 she became Associate Professor and began her teaching work in the School of Computer Engineering, University of Seville.

J.I. Escudero received his Physics degree in 1979 and his Doctorate in Physics in 1995 from the University of Seville (Spain).

He has held several teaching positions. He has been Professor of electronic engineering at the University of Seville since 1989. Dr. Escudero has focused his research activity on the study of telecommunications network performance.