Using Internet Protocols to Implement IEC 60870-5 Telecontrol Functions

Gemma Sánchez, Isabel Gómez, *Member, IEEE*, Joaquín Luque, *Member, IEEE*, Jaime Benjumea, and Octavio Rivera

***Abstract*—The telecommunication networks of telecontrol systems in electric utilities have undergone an innovation process. This has removed many of their technical restrictions and made it possible to consider carrying out telecontrol tasks with general standard protocols instead of the specific ones that are used currently. These are defined in the standards 60870-5, 60870-6, and 61850 from the International Electrotechnical Commission, among others. This paper is about the implementation, using the services of general standard protocols, of the telecontrol application functions defined by the standard IEC 60870-5-104. The general protocols used to carry out telecontrol tasks are those used in the Internet: the telecommunication network-management protocol SNMPv3 (simple network management protocol version 3), the clock synchronization protocol network time protocol and Secure SHell. With this new implementation, we have achieved, among others, two important aims: 1) to improve performance and, above all, 2) to solve the serious security problems present in the telecontrol protocols currently being used. These problems were presented by IEEE in an article published in the website of the IEEE Standards Association. In this paper, the use of general standard protocols to perform the telecontrol of electrical networks is justified. The development of this paper—its achievements and conclusions and the tools used—is detailed.**

***Index Terms*—Computer network-management protocols, International Electrotechnical Commission (IEC) 60870-5 series, internet protocols, performance, security, telecontrol.**

I. Introduction

IN THE field of electrical network telecontrol, the protocols traditionally used are either vendor specific or a result of standardizing efforts in this specific area [for instance, the telecontrol protocols from the International Electrotechnical Commission (IEC)]. These types of solutions make sense in applications with strong real-time restrictions and slow transmission speeds. However, although real-time restrictions are still present, speed restrictions are not.

In different European electrical networks [1], the communication networks of the telecontrol systems have undergone a generalized innovation process, since the 1990s. This innovation process has made many of the private aspects of these networks more open and standard. The following changes were introduced:

- use of digital technologies with broader bandwidth: optical fiber, digital radio links, digital power-line communications (PLC), mobile phone, etc.; this has removed speed restrictions prevailing until some decades ago;
- use of standard protocols: specifically those defined by IEC 60870-5 series for the communication between control centers (CCs) and remote terminal units (RTUs), by IEC 60870-6 series for communication between control centers and by IEC 61850 for communication inside a substation;
- use of standard reference models: open system interconnection (OSI) [2]–[5]; enhanced performance architecture (EPA) [6] and transport control protocol/Internet protocol (TCP/IP) [7]–[9];
- use of more intelligent RTUs, relieving network and control centers from the load.

The features of the telecommunication networks, as a result of this evolution, make it possible to carry out the telecontrol tasks by using general standard protocols that are not characteristic of the telecontrol field, such as the case of the network-management protocol Simple Network Management Protocol version 3 (SNMPv3) [10]–[12], the clock synchronization protocol network time protocol (NTP) [13] and Secure SHell (SSH) [14], members of the TCP/IP architecture. These solutions are more flexible and have a higher rate of commercial penetration and standardization. This approach opens up a new field of solutions that permits the exploitation of all the rich and dynamic experience of other fields which are constantly evolving, such as network management as well as time and session protocols for electrical networks.

These protocols have the advantages derived from their widespread use, such as reliability (since they are fully debugged), continuous update, and cost-effectiveness produced by the independence from vendors (since free implementation is available). Some IEC key standards for power systems, such as the 61850 set, are still under development or in an early stage of production compared with these protocols. Furthermore, the serious security problems of the protocols in the IEC 60870 series have been solved by using these protocols. These security problems have been highlighted and faced by IEEE, as can be seen in an article published in the website of the IEEE Standards Association [15].

To sum up, the purpose of this paper is to perform power system telecontrol by means of general standard protocols instead of the specific telecontrol protocols currently used. In this way, it is possible to take advantage of the features of the new communication networks of the telecontrol systems. These gen-

eral standard protocols have important advantages, such as reliability, robustness, security, continuous update, and saving. This paper improves performance and solves the security problems present in the telecontrol protocols that are currently used.

In Section II, the telecontrol functions defined in the IEC 60870-5 series are outlined, while Section III focuses on the Internet protocols used for implementing these functions. Section IV describes in detail the implementation of these telecontrol functions over the services of SNMPv3. Section V studies security issues related to power systems telecontrol networks. In this section, we expose the security threats that can affect these networks, the security models of SNMPv3, other alternatives to achieve security and the repercussions of using open or closed protocols in the security. Section VI shows the outcomes of the performance analysis and compares the performance of our implementation with that of another using TCP/IP services, ruled by the standard IEC 60870-5-104. Conclusions by the authors are presented in Section VII.

II. Telecontrol Functions of the IEC 60870-5 Series

This series [6], [16]–[22] defines a set of protocols to regulate the communications between control centers and RTUs.

The standard IEC 60870-5-104 deals with the interchange of telecontrol messages between control centers and RTUs connected via data networks, using TCP/IP. It adds a transport and a network layer to the EPA model. It sets the correspondence between the telecontrol functions defined by the document 5 of this series and the services supplied by TCP/IP. The application functions we have implemented by using SNMPv3, SSH and NTP services will be briefly described.

Station Initialization (SI): This function sets the involved station in a correct state of operation and has three categories: 1) initialization of the primary station (SI-IPS), 2) local initialization of the secondary station (SI-LISS), and remote initialization of the secondary station (SI-RISS).

Data Acquisition by Polling (DAP): The control center polls RTUs for updated information. The standard 104 advises against using this function because of the overload it generates.

Cyclic Data Transmission (CDT): This is a low priority function by which RTUs can take the initiative in sending data to the control center.

Acquisition of Events (AE): The RTU informs the control center about important and unexpected events. This is a high priority function.

General Interrogation (GI): This function is executed by the control center after a data loss or an internal initialization to ask the RTU for the updated values of all of its process variables.

Clock Synchronization (CS): This function is executed by the control center after an initialization and periodically to synchronize its clock with the RTUs. It can be carried out only if the maximum delay of the network is smaller than the required time accuracy.

Command Transmission (CT): By means of this function, the control center can execute actions in the RTUs. There are two categories: 1) "Direct Commands" (CT-DC) and 2) "Select and Execute Commands" (CT-SEC). "Select and Execute Commands" allow the control center to prepare RTU for the execution of an action, check if it is ready, and after the verification execute that action.

Transmission of Integrated Totals (TIT): The control center obtains values from the RTUs counters. This function can be initiated locally by the secondary (TIT-S) or remotely by the primary station (TIT-P) and has two categories: 1) transmission of integrated total and 2) transmission of incremental information, depending on whether the counters are reset or not.

Parameter Loading (PL): This function allows the control center to modify RTUs parameters, such as limits of measures, timer values, etc. Generally, the parameter loading is carried out in two phases: 1) parameter loading and 2) activation of the previously loaded parameters. This function can be initiated by primary (PL-P) and secondary (PL-S) stations. There are three kinds of parameters: 1) A; 2) B (PL-X-AB); and 3) C (PL-X-C), where X is the abbreviation of the initiator station.

Test Procedure (TP): The control center tests the connection with an RTU.

File Transfer (FT): When the volume of information to be transferred is too big to fit in an application service data unit (ASDU), it is transferred in files. This file transfer is bidirectional and has three categories: 1) file transfer from primary to secondary station (FT-PS); 2) file transfer from the secondary to primary station initiated by primary station (FT-SPP); and the file transfer from secondary to primary station initiated by the secondary station (FT-SPS).

III. Protocols

This section is about the protocols used to implement the telecontrol application functions defined by IEC 60870-5-104. These protocols are SNMPv3, SSH and NTP.

A. SNMPv3

The simple network management protocol version 3 is a de-facto standard and a member of the TCP/IP architecture. Most of the telecontrol functions mentioned (all except CS and the final phase of FT) were implemented by using the services provided by this protocol. This section is about this standard, its network-management model, and Net-SNMP (the implementation of SNMPv3 used to implement these functions).

1) Internet Network-Management Model: A network-management system can be defined as the set of elements that allow the supervision, analysis, and control of the resources and activities of a communication network in an effective and efficient way.

To carry out our implementation, the internet network-management model has been taken as the basis and adapted to the architecture of a telecontrol system. Their components have been related, identifying the role played by each element of a telecontrol system as a component of a management system.

The architecture of a network-management system based on SNMP (Fig. 1) includes a set of management stations and the elements managed by them. The management stations (or managers) run management applications that monitor and control the elements of the network; their main task is polling

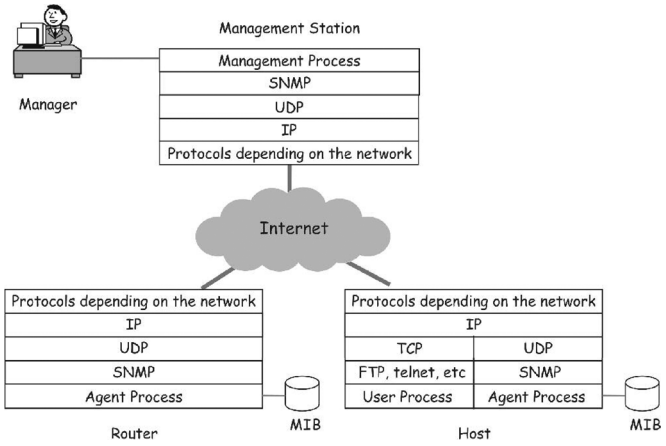

Fig. 1. Internet network-management model.

the agents present in those elements to demand necessary information to manage the network. The managed elements are devices (routers, gateways, servers, hubs, hosts, etc.) running agent software which responds to the information and action requests from a manager and can provide it with important and nonrequested information by an asynchronous mechanism called traps.

The managed elements and their attributes are represented by variables belonging to a management database, or management information base (MIB). The manager monitors the network by reading and writing the values of the MIB objects.

The communication between the manager and the agents is ruled by the network-management protocol SNMPv3 operating in the application layer.

When studying the Internet network-management model, we must deal with the management protocol and the information handled by it.

Regarding information, the MIB specifies which data must be stored by the agent and the access permission of the manager to these data. The structure of management information (SMI) [23] determines the rules used to define the variables of the MIB. These rules determine the valid types for MIB variables and specify how to define new types.

SNMP is the protocol used for managing the elements of the network. It defines the format and the meaning of the messages exchanged by SNMP entities. SNMP is a very simple protocol which satisfies network-management requirements and consumes very few resources from the network wherein it is installed. This protocol allows the manager to read and write the values of objects represented as variables in the agent's MIB. SNMP is based on the fetch-store paradigm. Conceptually, SNMP has only two commands, allowing a manager to get and set an object value. All of the remaining operations are defined by using these two commands. Another advantage of SNMP is that these days, it is the most widespread network-management protocol, supported by almost all of the devices.

SNMPv3 is the version of the protocol that has been used to implement the telecontrol functions determined by the standard IEC 60870-5-104. This protocol is defined in the request for comments (RFCs) 3410 to 3415. It presents a very high level of security, regarding both access control and message security (replay protection, data integrity, authentication and data confidentiality via encryption). This has been a key factor in our implementation, as we will expose later.

Its PDUs are:

- GetRequest, GetNextRequest, and GetBulkRequest: the manager gets the values of one or more variables from the agent's MIB;
- SetRequest: the manager sets the values of one or more variables from the agent's MIB;
- InformRequest: by means of this PDU, a manager notifies another of which information from its own MIB is accessible;
- Response: this is the response to the request PDUs; it contains either the requested information or the result of the requested operation;
- SNMPv2-Trap: by means of this PDU, the agent can asynchronously notify the manager of the occurrence of an event; this PDU is a heritage from SNMPv2.

2) Net-SNMP: Net-SNMP is the package used to implement the telecontrol functions defined by IEC 60870-5-104. It comes from the Carnegie-Mellon University—Simple Network Management Protocol (CMU-SNMP) and dates back to 1992 at Carnegie-Mellon University, Pittsburgh, PA. It began as an implementation of SNMPv1. Later, its source code was made publicly available and so, is open to individuals and companies for their use and modification. Since 1995, this project was adopted, enhanced, and made easier to use by universities and private people from several countries under the coordination of University of California at Davis and giving rise to the University of California, Davis—Simple Network Management Protocol (UCD-SNMP). Finally, UCD-SNMP became an open-code project with the concurrent versions system (CVS), and at the end of 2000, the project changed its name to Net-SNMP since collaborators were spread all over the world. It was moved to SourceForge so that administrative tasks were shared out.

The current version of Net-SNMP includes a set of tools:

- command-line applications to read and write information from an SNMP agent, remotely configure it, and handle different formats of MIB object identifiers;
- graphical MIB browser;
- daemon for receiving and managing SNMP notifications;
- extensible agent for responding to SNMP queries for management information; this includes built-in support for a wide range of MIB modules and can be extended by using dynamically loaded modules, external scripts, and commands;
- library implementing SNMP services for developing new applications, with both C and perl application programming interfaces (APIs).

The security model used by Net-SNMP is a user-based security model (USM), which is discussed in Section V.

B. NTP

The clock synchronization function, just as it is defined by IEC 60870-5-104, can be carried out only if the maximum delay

of the network is smaller than the required time accuracy. However, we cannot ensure it within a wide-area network (WAN). The solution adopted as an alternative to the clock synchronization defined by IEC 60870-5-104 is the implantation of an NTP synchronization system over the telecontrol network.

The network time protocol (NTP) [24], [25] was designed to keep synchronization among the elements of a distributed system by sharing time information in a large and diverse Internet system operating at any speed. The used version of the protocol is 3.

The Internet standard protocol NTP is able to provide a time accuracy of 10 ms over the Internet, even in the presence of attacks or failures in clocks, time servers, or the network. This time accuracy is achieved by a global approach of the system design, integrating primary time references, time servers, synchronization subnets, protocols, and synchronization mechanisms.

The architecture of a synchronization system based on NTP consists of a distributed subnet of time servers operating in a self-organizing and hierarchical configuration, synchronizing local clocks within the subnet and to national time standards. These time servers and their clients exchange synchronization information by means of NTP, over the user datagram protocol/Internet protocol (UDP/IP).

NTP works correctly in a wide range of computers, from personal workstation to mainframes. It minimizes the load over the operative system. Since it is a connectionless protocol, it minimizes latency and simplifies implementations. NTP is tolerant to numerous faults of different types, such as communications, clocks and servers. Furthermore, it includes mechanisms of protection against hackers. It also makes up for the effects of the variable transmission delays between a client and a server within WAN. All of these reasons make this protocol appropriate for electrical network telecontrol systems.

These days, NTP is the most spread protocol for distributed system synchronization, and it works perfectly. As a curiosity, we can say that NTP is the synchronization protocol used by NASA spacecrafts [26].

C. SSH

File transfer is carried out by means of SNMPv3 and SSH. The first protocol is used for exchanging information about the files to be transferred and the second carries out the transfer of the files using the command secure copy (SCP).

SSH is defined in the RFCs 4250 to 4256. It allows accessing remote hosts through a network by means of a secure channel. It uses public-key cryptography to authenticate the remote computer and to allow this to authenticate the user. SSH provides confidentiality and integrity of data exchanged between the two computers using encryption and message authentication codes.

IV. Implementation of the Telecontrol Applications Functions Defined by the Standard IEC 60870-5-104 Over the Services of SNMPv3

This section describes the implementation of those telecontrol functions by using the services of the network-management protocol SNMPv3.

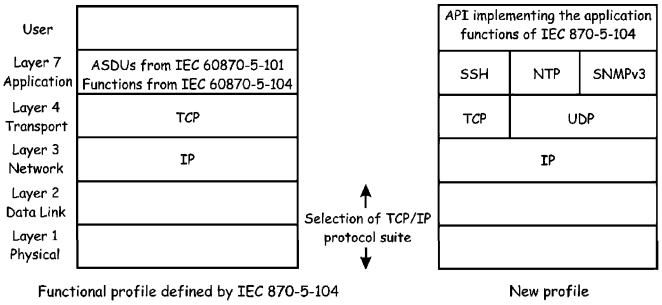

Fig. 2. Comparison of protocol stacks.

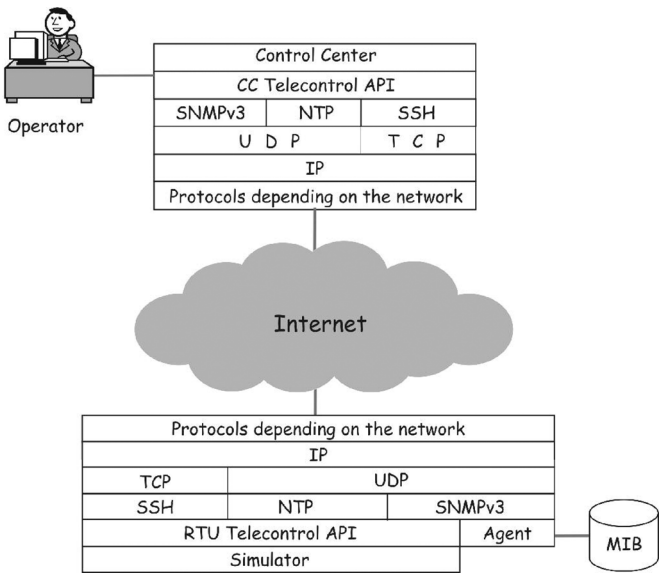

Fig. 3. Adaptation of the Internet network-management model to telecontrol systems.

A. Protocol Stacks

The proposed approach replaces the protocol stack established in the standard IEC 60870-5-104 (specific of telecontrol) that drives the telecontrol communications between RTUs and control centers by a stack of protocols nonspecific of telecontrol. To be exact, the services of SNMPv3, SSH, and NTP are used to implement the telecontrol application functions defined by that standard.

Fig. 2 shows protocol stacks and compares them by equating their equivalent layers. It can be observed that, in our development, the services of the application protocols SNMPv3, SSH, and NTP are used for implementing the telecontrol application functions defined by IEC 60870-5-104. In this standard, these functions are defined to work directly over TCP/IP.

B. Architecture of the New System

To implement the telecontrol application functions defined by the standard IEC 60870-5-104 using the services supplied by the network-management protocol SNMPv3, the Internet network-management architecture was adapted to that of a telecontrol system, as shown in Fig. 3.

Three programs have been developed to test the implemented functions:

1) Control center: It is an SNMP manager playing the role of control center (primary station in the nomenclature of the IEC standard). This process calls the telecontrol functions initiated by this station.
2) RTU simulator: It is also an SNMP manager implemented to face with the lack of a real RTU to work with. This process simulates the behavior of an RTU, generating different kinds of faults and events with a certain probability and frequency, and reflecting the effect of commands on the RTU. This process calls the functions initiated by the RTU.
3) SNMP agent: This process, together with the simulator, plays the role of secondary station (or RTU). For this purpose, the agent has been extended, including new variables in its MIB, and giving them a dynamic behavior.

C. RTU's MIB

The MIB is a fundamental component in this new telecontrol system. All of the implemented telecontrol functions are carried out or initiated by means of the MIB. Through it, the control center and RTU send and receive all of the information they need to carry out the telecontrol functions. It is stored in the RTU.

Every telecontrol function has an associated variable of status in this MIB. The transitions in the state machines of each function are implemented by changes in its variable of status. These changes can be caused by the control center and the RTU.

Those telecontrol functions that entail telecontrol data exchange (DAP, CDT, AE, GI, TIT, PL, and FT) have an additional variable. This variable is an array of DisplayStrings. The maximum length of this array is configurable. All of the telecontrol data that the control center and the RTU want to exchange are written in this array.

In addition, every variable in the MIB has a timetick variable recording the time of its last change.

D. Implementation of the Functions

This section describes the implementation of the telecontrol functions defined by the standard IEC 60870-5-104 over SNMPv3. The philosophy ruling the implementation of all these different functions is quite homogeneous. For this reason, the implementation of one of the most used functions, Data Acquisition by Polling, is shown as a representative example.

As mentioned, the implementation of the telecontrol functions has been carried out by using the MIB. Data Acquisition by Polling uses the data structure implemented by the subtree *dapIEC* in the MIB. The structure of this subtree is shown next:

```
+–dapIEC(17)
      |
      +– -RW- EnumVal dapState(1)
      | Values: nodata(0), data(1), locked(3)
      +– -R– TimeTicks dapStateTT(2)
      +– CR– INTEGER dapNDS(3)
      |
      +–dapDSTable(4)
            |
            +–dapDSEntry(1)
                  | Index: dapDSInd
                  |
                  +– —- INTEGER dapDSInd(1)
                  +– CR– String dapDS(2)
                  | Textual Convention: DisplayString
                  | Size: 0..1492
                  +– CR– EnumVal dapDSStatus(3)
                        Textual Convention: RowStatus
                        Values: active(1), notInService(2),
                        notReady(3), createAndGo(4),
                        createAndWait(5), destroy(6)
```

The object dapState is an enumerated value reflecting the state of the RTU with regard to the Data Acquisition by the Polling function. It can contain the values nodata (there are no data to reply to a data poll), data (there are some data) and locked (data are being read or written, so the access to them is locked). Reading this object while containing the value data causes it to be assigned the value locked.

The object dapStateTT is the time tag that records the moment in which dapState was last modified.

The object dapNDS records the number of Display Strings from the table dapDSTable that must be read by the manager to obtain the requested data.

The last object of this subtree is the table dapDSTable. It consists of three columns. The first one, called dapDSInd, is the index identifying the row being accessed. The second, called dapDS, is a Display String with a maximum length of 1492 B that contains the necessary information to reply to a Data Acquisition by Polling request. The data that the RTU must send to the control center are stored in as many dapDS objects as necessary. This information is stored by the RTU in the MIB. The third column dapDSStatus is an administrative object, necessary for creating and erasing rows in the table.

The state machines of the processes implementing the control center (manager) and the RTU (agent and simulator) are achieved by means of the variable of status. Figs. 4–6 show the state machine of these processes.

E. Operation in a Real System

This implementation is being installed in a trial system. The program corresponding to the CC will operate in a PC, while the one corresponding to the RTU will run in an RTU implemented in an embedded system [27], [28]. This system is based on an open core hardware in which Linux has already been installed.

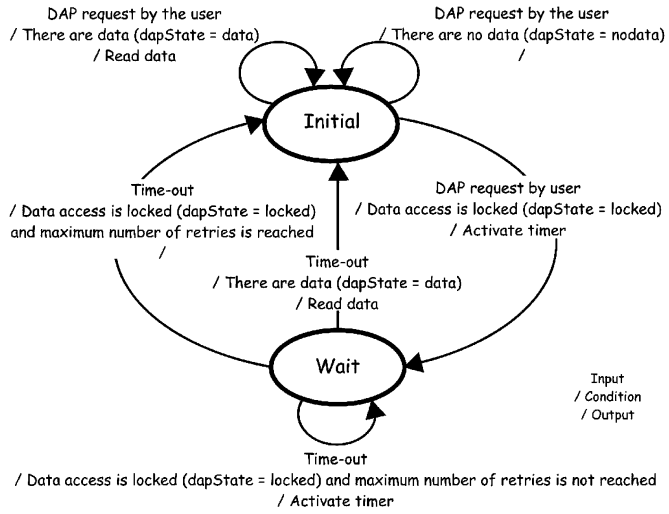

Fig. 4. State machine of the control center for data acquisition by polling.

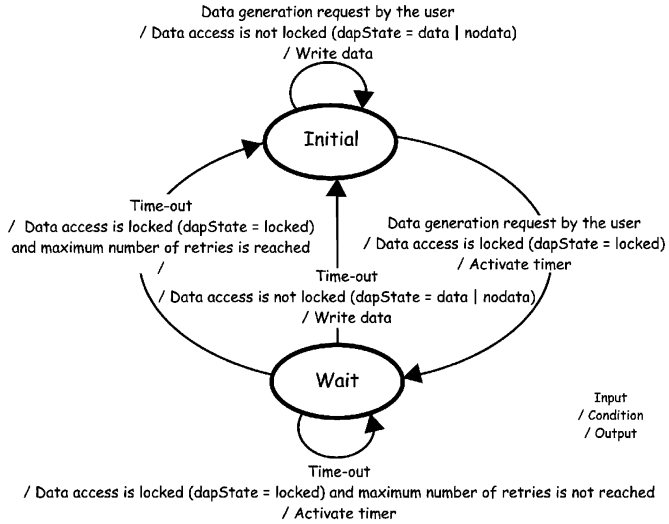

Fig. 5. State machine of the RTU simulator for data acquisition by polling.

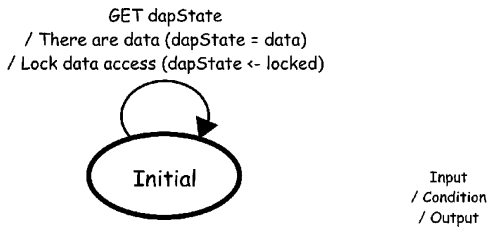

Fig. 6. State machine of the SNMP agent for data acquisition by polling.

V. Security

Security is an important issue in any network, even in an isolated one such as the telecontrol network of a power system. This kind of network is so large that it is impossible to ensure that no one will ever be able to physically access wires or even an RTU. Given the fact that an unauthorized access to the network is possible, it is important to be aware of the risks.

A. Security Threats in Telecontrol Networks

This section outlines the different security threats that can affect a telecontrol network of a power system. Computer network literature [29] may help to classify these attacks:

Passive Attacks: The main kind of passive attack is eavesdropping on transmissions. This does not directly harm because data traffic on the network is not modified. However, the information obtained when eavesdropping could be useful by itself or might be used to gather information to launch an active attack.

Active Attacks: These involve actively interfering in network activity, and in most cases, having physical access to some point in the telecontrol network. Traffic forgery is an active attack which means that an unauthorized entity is able to modify, insert, or remove traffic from the network. This allows, for example, changing orders issued by a control center, or sending a false alarm to it, or a shutdown command to an RTU. One kind of traffic forgery is traffic replay. It consists in resending unauthorized traffic previously captured by a passive attack.

Eavesdropping and traffic forgery (excepting traffic replay) can be solved by using cryptography, which includes encryption and hash algorithms. This usually means sharing a secret key between the CC and the RTU. This key allows them to communicate securely, even if the network has been tapped. Encryption renders eavesdropping almost useless because no entity (with the exception of the real RTU and CC) will be able to understand the traffic. In this situation, traffic forgery is not possible because it is not feasible to create a valid message without knowing the encryption key. Hash algorithms, in combination with encryption, prevent the unnoticed modification of the traffic.

However, encryption alone is not enough to avoid traffic replay. Traffic replay is possible because an attacker is able to store encrypted traffic and send it later. Even if the attacker does not know what kind of traffic it is, it will be cryptographically valid provided that nothing is changed in the stored message. This means that an attacker could store a shutdown command and replay it at any moment. If protection against traffic replay is needed, some kind of timestamp or nonreusable numbering must be added to the encrypted message so that duplicated messages could be detected.

B. Security in SNMPv3

SNMPv3 modular design allows choosing a security model independent of the rest of the architecture. Several security models [30]–[33] have been proposed for use with SNMPv3, but only the user security model (USM) has been implemented in frameworks such as Net-SNMP. The others are either still in the drafting stage or have been dropped.

USM is defined in RFC3414 and is usually implemented in many SNMP-capable devices (both software and hardware based). This security model allows using SNMP with insecure channels by providing user identity verification, integrity verification (verifying that the message has not been modified by a third party), and protection against disclosure of information. USM also provides protection against replay attacks.

USM allows user-based authentication and access control. Administrators can create specific accounts for each SNMP user and grant privileges through those user accounts. This has a significant impact on the security by increasing accountability

for user actions. It also facilitates the exclusion of a user from the system without requiring the reconfiguration of all SNMP devices.

Although USM has been implemented, some concerns have arisen with its use. These have been studied by an Internet Engineering Task Force (IETF) Working Group (WG) [34]. In accordance with this WG, USM lacks proper user and key management, meaning that key and user distribution among the network (CC and RTU) is inefficient. There are also some concerns with replay protection, but it is not considered a serious problem because it can be easily circumvented by adding nonreusable numbering in messages, as the WG itself states in [34].

Given the concerns with USM, this WG seeks to deploy a security module for SNMPv3 capable of integrating an efficient user and key management. Although External USM (EUSM) [31] was initially considered to be "the right direction for the Integrated Security Model for SNMP (ISMS) WG" [35], it was dropped afterwards [36]. So this WG moved to use the secure Transport Subsystem [37] and SSH in tunnel mode as the security model [38]. As work is still in progress, no final proposal has been made so far and, as a result, USM is still in use.

Even though USM is not a perfect solution, it is one of the security models implemented in Net-SNMP. Since the most serious concern with USM is its inadequate key management, USM applicability will depend on the complexity and the size of the telecontrol network. If the number of users (operators) and keys (RTUs and CCs) in use is acceptable, it would be possible to use USM. As the number of operators and CCs is significantly lower than that of the RTUs, the latter is decisive. Finding out how many RTUs are acceptable requires further analysis and is beyond this paper.

C. Other Alternatives for Security

Using SNMPv3 security extensions is not the only way to achieve security in a network. There are protocols such as IPsec [39] or transport-layer security (TLS) [40] which also offer security services to a network. In these cases, protection is achieved at the network and at a socket-layer level. This means that application protocols do not need to support security, because it is provided by lower-layer protocols. However, since our proposal is to use SNMPv3 to perform telecontrol functions, we do not see a significant advantage in using either IPsec or TLS because standard SNMPv3 implementation already includes the security services described before.

If we use either an implementation of the telecontrol functions over TCP/IP or some mixed scenario (not only SNMPv3), it would be appropriate to evaluate the use of other security protocols, such as IPsec or TLS.

D. Concerns With the Use of Open Protocols

The proposal is to use Net-SNMP, NTP, and SSH, open-source software installed in an open-source operating system (such as Linux), using well-known cryptographic and authentication protocols. Therefore, some concerns might arise because our framework may be the object of the same kind of attacks as those used in the Internet. Some people might think it would be better to continue using closed protocols in order to keep telecontrol systems secure. While it is true that our framework might be attacked in the same way as the Internet, it is untrue that a closed environment will provide more security to our telecontrol networks.

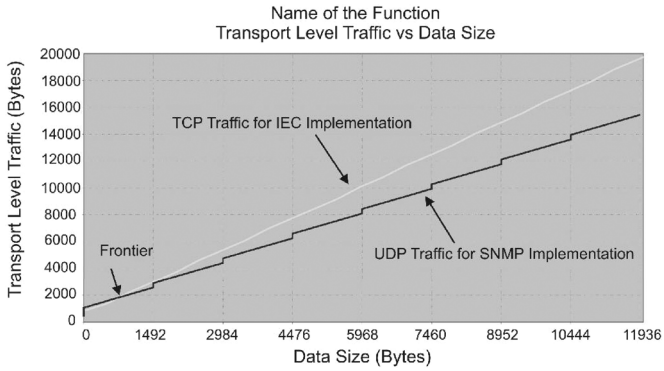

Fig. 7. General format of transport-level traffic comparison for both implementations of functions bearing telecontrol information.

The question is what kind of framework is more secure: one using open protocols or other using closed ones? The answer is none of them. A system, framework, or protocol will be secure only if it is designed to be secure (i.e., prepared to be attacked); it does not matter if an open or a closed environment is being used. In fact, open protocols and, more specifically, open-source software are considered to be advantageous by certain groups because the source code may be inspected by everybody and, thus, be subject to some kind of communitarian audit. However, this communitarian audit should not be considered as a guarantee that a piece of software is secure; it only means that it may be inspected by anyone.

To summarize, using an open protocol or software does not increase the threat of being successfully attacked. Improperly designed software or protocols can be found in open and closed environments.

VI. Performance Analysis

In this section, the results of the performance analysis are summarized. To determine the quality of the proposed implementation (called SNMP implementation from now on), the analyzed performance measurements are compared with those obtained from another implementation by using TCP/IP services, ruled by the standard IEC 60870-5-104 (called IEC implementation from now on).

The analyzed measurements are the transport-level traffic generated by the execution of a particular function and the fraction (percentage) of this traffic bearing telecontrol information (called useful percentage, from now on). This last measure can be analyzed only for those functions that entail the exchange of telecontrol information.

To carry out this performance analysis, the telecontrol application functions have been considered in two groups: those bearing telecontrol information and those which do not. Data acquisition by polling (DAP), cyclic data transmission (CDT), acquisition of events (AE), general interrogation (GI), transmission of integrated totals (TIT), parameter loading (PL), and file

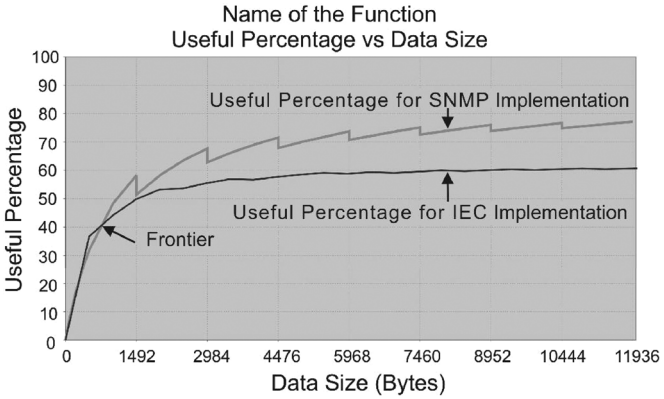

Fig. 8. General format of useful percentage comparison for both implementations of functions bearing telecontrol information.

TABLE I
FRONTIER AND ASYMPTOTIC VALUES OF USEFUL PERCENTAGE FOR BOTH IMPLEMENTATIONS OF FUNCTIONS BEARING THE TELECONTROL INFORMATION

Function	Frontier	Asymptotic value (%)	
		SNMPv3	IEC
DAP	800 bytes	78	61
CDT	300 bytes	76	58
AE	500 bytes	76	60
GI	700 bytes	79	62
TIT-P	0 bytes	80	60
TIT-S	0 bytes	80	61
PL-P-AB	0 parameter	45	0.55
PL-P-C	0 parameter	45	0.74
PL-S-AB	1 parameter	80	0.94
PL-S-C	1 parameter	80	1.25
FT-PS	850 bytes	94	12.4
FT-SPP	3 Kilobytes	94	12.3
FT-SPS	3 Kilobytes	94	12.3

transfer (FT) are included in the first group. Station initialization (SI), command transmission (CT), and test procedure (TP) are included in the second group.

Fig. 7 represents the general format of transport-level traffic comparison for the first group of functions. This shows the transport-level traffic generated by the execution of a function for both implementations.

Fig. 8 represents the general format of useful percentage comparison for the first group of functions. This shows the useful percentage for both implementations of a function.

In these two graphics, we can observe that traffic and useful percentage present steps for multiples of 1492-B data sizes. This is a result of the encapsulation of telecontrol information into MIB variables to transfer it. These MIB variables are *Display Strings* with a maximum length of 1492 B, which implies that every time data size exceeds a multiple of 1492, a new variable has to be transferred, with the overload in protocol information needed to request and transfer it. The more data that are contained in this variable approach 1492 B, the higher the useful percentage that is obtained. This is a configurable size that could be adapted to specific systems' necessities. It must minimize the possibility of transmission error, and should be big enough to maximize the performance of the protocol.

Another general characteristic of these graphics is that during a first little interval, the traffic generated by SNMP implementation slightly exceeds that of the IEC implementation. Therefore, the useful percentage of the IEC implementation is higher during this interval. The upper frontier of this interval varies between 0 and 800 B, depending on the specific function. For file transfer to primary station (FT-SPP and FT-SPS), the traffic of SNMP implementation is bigger than that of the IEC implementation, up to a file size of 3 kB.

For all data sizes over the frontier, the SNMP implementation performance is always better than that of the IEC implementation.

For both implementations, the useful percentage of each function grows to almost stabilize around an asymptotic value. Table I shows the mentioned frontier and the asymptotic values of a useful percentage for the functions of the first group.

In this table, we can observe that this asymptotic value is between 16 and 20 percentage points higher for the SNMP implementation of DAP, CDT, AE, GI, and TIT. For PL, the difference is bigger, about 44 points when the PL is initiated by the primary station (PL-P) and about 79 when it is initiated by the secondary station (PL-S). For file transfer, the difference exceeds 81 percentage points.

The group of functions that do not bear telecontrol information includes station initialization (SI), command transmission (CT), and test procedure (TP). The only analyzed measure for these functions is traffic. Fig. 9 represents the general format of traffic comparison for them. This shows the traffic generated by the execution of a function for both implementations. The three columns on the left represent traffic for the SNMP implementation and those three on the right for IEC implementation. Inside every group of three columns, the outgoing traffic from the primary station, the incoming traffic for the primary station, and the total traffic (sum of both) are represented.

Table II shows the total traffic obtained for every function of the second group.

In this table, we can observe that the traffic for IEC implementation exceeds that of the SNMP implementation for every function, ranging from 110 to 321% depending on the function, expect for the remote initialization of the secondary station (SI-RISS), where IEC implementation traffic is 72% of that of the SNMP implementation.

VII. CONCLUSION

As a result of this work, the following conclusions can be obtained:

- Electrical network telecontrol systems, in their evolution, tend to the use of standard protocols to carry out their

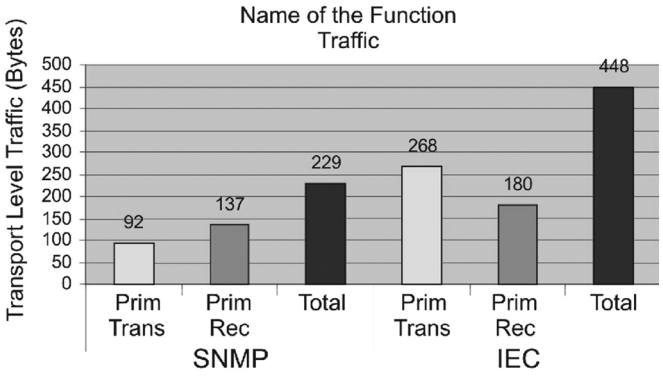

Fig. 9. Transport-level traffic comparison for both implementations of function not bearing telecontrol information.

TABLE II
TOTAL TRAFFIC OBTAINED FOR BOTH IMPLEMENTATIONS OF THE FUNCTIONS NOT BEARING TELECONTROL INFORMATION

Function	Total Traffic (bytes)		Relation between IEC and SNMP traffic
	SNMPv3	IEC	
SI-IPS	229	292	128 %
SI-LISS	96	308	321 %
SI-RISS	663	480	72 %
CT-DC	615	890	145 %
CT-SEC	1102	1215	110 %
TP	344	615	179 %

functions. Specifically, European electrical companies are adopting the standards of IEC 60870-5 series to rule the communications between control centers and RTUs, and those of IEC 60870-6 to communications between control centers.

- As its name suggests, SNMP is a very simple protocol. Its installation is easy in large networks and the management information needing exchange takes a few network resources.
- SNMPv3 services allow implementing upper functions, adapting them to the fetch-store paradigm, and to the use of .
- Since SNMPv3 is really an extended protocol, present in most of the network systems, its use is not costly in terms of installation of new applications. In fact, many telecontrol networks are managed by SNMPv3. The wide experience in it makes it robust and well-known since there are many groups analysing and improving it, in view of its importance in the right operation of the networks in many organizations.
- The use of Net-SNMP has entailed all the advantages of mature and extended software, endorsed by a wide and active community of users and programmers, willing to cooperate in the presence of any problem or doubt. Furthermore, the use of a free implementation of SNMP dissociates us from vendors.
- SNMPv3 provides security facilities, such as authentication, encryption and timeliness checking. The implementation of telecontrol application functions using SNMPv3 services solves completely and satisfactorily the serious problems of security that IEC 60870-5-104 presents.
- The performance analysis determines a higher performance for SNMPv3 implementation in most cases.
- This approach could be applied to other fields of telecontrol besides electrical networks, such as industry or intelligent home.

REFERENCES

[1] J. M. Selga, R. Baumann, L. Björk, B. Richardson, and H. Spelt, "Technical brochure on communication concepts for control systems," presented at the CIGRE SC35-WG13-TF13.03 Colloquium, Paris, France, 1998.

[2] *Information Technology. Open Systems Interconnection. Basic Reference Model. Part 1: The Basic Model*, ISO/IEC Std. 7498-1, 1994.

[3] *Information Processing Systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture*, ISO/IEC Std. 7498-2, 1989.

[4] *Information Technology. Open Systems Interconnection. Basic Reference Model. Part 3: Naming and Addressing*, ISO/IEC Std. 7498-3, 1997.

[5] *Information Processing Systems. Open Systems Interconnection. Basic Reference Model. Part 4: Management Framework*, ISO/IEC Std. 7498-4, 1989.

[6] *Transmission Protocols. General Structure of Application Data*, IEC Std. 60870-5-3, 1992.

[7] J. Postel, *Internet Protocol Handbook* RFC-774, 1980.

[8] Information Sciences Institute. University of Southern California, Internet Protocol. DARPA Internet Program. Protocol Spec. RFC-791, 1981.

[9] Information Sciences Institute. University of Southern California, Transmission Control Protocol. DARPA Internet Program. Protocol Spec. RFC-793, 1981.

[10] J. Case, R. Frye, and J. Saperia, *SNMPv3 Survival Guide*. New York: Wiley, 1999.

[11] W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, 3rd ed. Reading, MA: Addison-Wesley, 2000.

[12] S. Díaz, J. Luque, M. C. Romero, and J. I. Escudero, "Power systems monitoring and control using telecom network management standards," *IEEE Trans. Power Del.*, vol. 20, no. 2, pt. 2, pp. 1349–1356, Apr. 2005.

[13] D. L. Mills, Network Time Protocol Ver. 3 (NTP, V.3): Specification, Implementation and Analysis. RFC-1305, 1992.

[14] D. J. Barrett and R. Silverman, *SSH, The Secure Shell: The Definitive Guide*. Sebastopol, CA: O'Reilly Media, 2001.

[15] IEEE Standards Assoc.: News and Information, Apr. 18, 2006, IEEE Begins Work on Cyber Security Standard for Electric Utilities. [Online]. Available: http://www.standards.ieee.org/announcements/pr_P1689_P1692.html

[16] *Transmission Protocols. Transmission Frame Formats*, IEC Std. 60870-5-1, 1990.

[17] *Transmission Protocols. Link Transmission Procedures*, IEC Std. 60870-5-2, 1992.

[18] *Transmission Protocols. Definition and Coding of Application Information Elements*, IEC Std. 60870-5-4, 1993.

[19] *Transmission Protocols. Basic Application Functions*, IEC Std. 60870-5-5, 1995.

[20] *Transmission Protocols. Companion Standard for Basic Telecontrol Tasks*, IEC Std. 60870-5-101, 1995.

[21] *Transmission Protocols. Companion Standard for Basic Telecontrol Tasks*, IEC Std. 60870-5-101, 2000, amendment.

[22] *Transmission Protocols. Network Access for IEC 60870-5-101 Using Standard Transport Profiles*, IEC Std. 60870-5-104, 2000.

[23] K. McCloghrie, D. Perkins, and J. Schoenwaelder, Structure of Management Information Ver. 2 (SMIv2) RFC-2578, 1999.

[24] L. Lamport and P. M. Melliar-Smith, "Synchronizing clocks in the presence of faults," *J. ACM*, vol. 32, no. 1, pp. 52–78, Jan. 1985.

[25] T. K. Srikanth and S. Toueg, "Optimal clock synchronization," *J. ACM*, vol. 34, no. 3, pp. 626–645, Jul. 1987.

[26] D. L. Mills, 2004, Network Time Protocol (NTP). General Overview. [Online]. Available: http://www.cis.udel.edu/~mills/database/brief/overview/overview.ppt

[27] A. Muñoz, E. Ostúa, M. J. Bellido, A. Millán, J. Juan, and D. Guerrero, "Building a SoC for industrial applications based on LEON microprocessor and a GNU/Linux distribution," in *Proc. IEEE Int. Symp. Industrial Electronics*, 2008, pp. 1727–1732.

[28] J. Benjumea, V. Medina, I. Gómez, E. Dorronzoro, G. Sánchez, and S. Martín, "Choosing the right protocol stack for an open and flexible remote unit," in *Proc. IEEE Int. Symp. Industrial Electronics*, 2008, pp. 1668–1673.

[29] W. Stallings*, Cryptography and Network Security*, 4th ed. New York: Pearson-Prentice Hall, 2006.

[30] U. Blumenthal and B. Wijnen, User-based security model (USM) for Ver. 3 of the simple network management protocol (SNMPv3) RFC 3414, 2002.

[31] K. Narayan, K. McCloghrie, and J. Salowey, 2005, External user security model (EUSM) for ver. 3 of the simple network management protocol (SNMPv3). [Online]. Available: http://www.tools.ietf.org/html/draft-kaushik-snmp-external-usm-02

[32] W. Hardaker and D. Perkins, 2004, A Session-Based Security Model (SBSM) for ver. 3 of the Simple Network Management Protocol (SNMPv3). [Online]. Available: http://www.tools.ietf.org/html/draft-hardaker-snmp-session-sm-03

[33] D. Harrington and J. Schoenwaelder, 2004, Transport Mapping Security Model (TMSM) for the Simple Network Management Protocol Ver. 3 (SNMPv3). [Online]. Available: http://www.tools.ietf.org/html/draft-schoenw-snmp-tlsm-01

[34] IETF ISMS Working Group, 2008, Integrated Security Model for SNMP (ISMS). [Online]. Available: http://www.ietf.org/html.charters/isms-charter.html

[35] U. Blumenthal, L. Dondeti, R. Presuhn, and E. Rescorla, 2005, Comparison of Proposals for Integrated Security Model for SNMP. [Online]. Available: http://www.tools.ietf.org/html/draft-ietf-isms-proposal-comparison-00.txt

[36] IETF ISMS Working Group, 2006, Minutes of the ISMS session at IETF 62. [Online]. Available: http://www.tools.ietf.org/wg/isms/minutes?item=minutes62.html

[37] D. Harrington and J. Schoenwaelder, 2007, Transport subsystem for the simple network management protocol (SNMP). [Online]. Available: http://www.tools.ietf.org/html/draft-ietf-isms-tmsm-08

[38] IETF ISMS Working Group, 2007, Minutes of the ISMS session at IETF 68. [Online]. Available: http://www.tools.ietf.org/wg/isms/minutes?item=minutes68.html

[39] S. Kent and K. Seo, Security architecture for the internet protocol. RFC-4301, 2005.

[40] T. Dierks and E. Rescorla, The transport layer security (TLS) protocol version 1.1. RFC-4346, 2006.