USING PROTOCOL ENGINEERING TECHNIQUES TO IMPROVE TELECONTROL PROTOCOL PERFORMANCE

VERÓNICA MEDINA[1], ISABEL GÓMEZ[2], GEMMA SÁNCHEZ [3], ANTONIO BARBANCHO [4], SERGIO MARTÍN[5]
Department of Electronic Tecnology
University of Seville
Facultad de Informática y Estadística
Avda Reina Mercedes s/n 41012
Seville, SPAIN
Phone/Fax: 95 455 27 64
anamed@cica.es[1], igomez@cica.es[2], gemma@acebuche.fie.us.es[3], ayboc@cica.es [4],smartin@cica.es[5]

Abstract.- This article describes the need of using Protocol Engineering techniques to study current telecontrol protocols and this way improve their performances by setting them up or changing for others, such as standardised ones (testing their implementations).

Keyword: Substation and Distribution Automation, Protocol Engineering, Testing

I. INTRODUCCTION

In the last few years, the role of Power Utilities in the world of telecommunications has undergone rapid changes, which affect not just technological aspects but also issues of regulation, access to new markets, creation of new services, etc. This situation creates urgent technological demands that have to be satisfied to be able to keep on competing successfully [1], [2], [3], [4], [5], [6], [7], [8], [9].

One of the most important aspects for updating technology is to manage the operation of a Power Utility Network. That is why, several telecontrol systems have been applied to operate on that network in a safety and economical way from the 60´s on [10], [11], [12]. Until recently, competition in the utility sector only has existed between suppliers of equipment. This resulted in the development of vendor-proprietary, closed product lines. Buyers were "tied-in" to a specific supplier. The liberalisation and de-regulation in the energy market has stimulated the buyers of energy as well as the energy production and distribution companies to adopt three main driving forces for their strategic decisions [13]:

- better use of the assets.
- better staff utilisation.
- better customer focus.

Data communications, tele-metering and substation automation are ways to achieve these objectives. Data communication must be supported by an open communication architecture when applying component for telecontrol automation. These telecontrol systems are based on a processor architecture allocated through the equipment of the Power Utility Network. The processors are mainly located in both the energy generation plant and the energy distribution and transformation stations. These plant processors are called "remotes" (also called RTU´s: Remote terminal Units) and make it possible to work on the Power Network. Remotes communicate with one or several centres (also called control centres), sending the network status information and receiving commands. Communication protocols, that are applied to control these Power Networks, have to be thoroughly studied, because the expense of setting up such systems can be reduced just by optimising them. These protocols are called telecontrol protocols.

In this article we describe the need of using protocol engineering techniques not only to automatically calculate performance but to implement and test telecontrol protocol in order to adopt communication standards in telecontrol systems. We also present different tools that are available to develop and test protocols and our experiences in the subject.

II. PROTOCOL ENGINEERING

Protocol design is related to several subjects such as operating systems, computer networks, and data transmission. However, the designing of a protocol whose correctness can be proved is a challenge and, sometimes, a desperate task.

Communication software is a special kind of software developed to be used in telecommunication or computer network to provide a set of well-defined services. This software is allocated in different network nodes, so it is required some protocols that make the interaction among components easy. Protocols supply their services co-ordinating and synchronising distributed components.

Although the main protocols used in computer networks have been standardised by International Organisations, the software that implements them is difficult to design and to test, because of [14]:

- standards make use of informal text in formal descriptions.
- formal descriptions are not adequately validated.
- standards do not include some details that depend on the machine where protocols are implemented.

Application of formal methods and software engineering methodologies to protocol design has given rise to a new interdisciplinary that is called "protocol engineering"[15]. Protocol engineering allows achieving efficient and reliable communication software.

The main activities that have to be done in Protocol Engineering are:

- Synthesis. A formal description is made from an informal description of the communication requirements. Protocol and service specification is described in this activity.
- Validation and verification. These two activities try to find out possible faults in the formal description of the communication protocol.
- Performance Analysis. Protocol specification is analysed to optimise its performance.
- Automatic Generation. An executable code is generated from the specification of the protocol.
- Conformance Testing. The protocol implementation is tested to check its correctness and its conformance with the specification.

A Formal Description Technique (FDT) is chosen when a protocol has to be specified in a formal way. Although there are many FDTs, just three of them are the most popular. These are ESTELLE [16] (Extended State-Transition Language) and SDL [17] (Specification and Description Language), based on extended finite state machines, and LOTOS [18] (Language for Temporal Ordering Specification), based on process algebra. All three are international standards and the selection of one or the other depends on the specific needs of the user or designer. No FDT satisfactorily fulfils all requirements.

Several studies have shown [4][19][20] that ESTELLE adapts better to the electrical sector than the other specification languages, since it does not require much learning or specialisation effort. ESTELLE is particularly suited for describing communication protocols and services. Each component of communication protocol is specified by a module whose functional behaviour is described as a finite state machine. In ESTELLE, a protocol system is specified as a hierarchically structured system of modules that interchange messages (called interactions) through bi-directional links between their ports (called interaction points). Both the hierarchy of modules and the structure of links may change over time, thereby making the system a dynamic one.

There are different tools that are able to analyse performances, validate, verify and test protocols specified in ESTELLE as shown next section.

III. ESTELLE TOOLS

The only tool specifically designed to implement, measure performance and integrate a telecontrol protocol from its specification in ESTELLE [21]is the CUP tool -it was financed by the Electrotechnical Investigation Program of the Spanish Ministry of Industry and Energy and developed as a whole by the power utility CSE (Compañía Sevillana de Electricidad) and our Department at the University of Seville-. This tool is a propietary software and is an acronym for the spanish words "**C**onversor **U**niversal de **P**rotocolos"(Universal Protocol Converter) and its first application was the protocol conversion by services adaptation [19]. The performance of telecontrol protocols can be analysed from its specification in ESTELLE with this tool and, then, made an efficient implementation of them. To achieve it, some specific primitives are added to the specification in ESTELLE of a telecontrol protocol [22]. This method studies the performance of a telecontrol protocol without using neither analytical solution nor simulating solution [23]. We specify in ESTELLE the performance analysis model of the telecontrol protocol (existing or new one) including the performance primitives and then the performance measures are automatically calculated. The performance analysis model is needed because it is possible to study a part of a whole protocol (only one layer in line with the OSI [24] -Open System Interconnection Model- or a similar one). In order to validate this method, we study successfully the same telecontrol protocol analysed in the work done in [25] and [26], where the performance was calculated by both an analytical and simulating solution.

For example, Figure 1 compares[1] our results of efficiency to those achieved at the aforementioned work by means of a simulating solution for a set of speeds (300 bps , 600 bps, and 1200 bps) and Figure 2 shows the same but comparing ESTELLE solution to both analytical (exact and

[1] We made the same conjecture as in work [25], i.e., each RTU generates messages exponentially (a Poisson process) with an average time of 4 seconds, and the control center generates command message exponentially with a average time of 8 seconds. The probability that a RTU generates an event message is less than a measurement message. The switching time is 10 milliseconds. The length of measurement and event messages is 380 bits and the length of command message is 60 bits. The simulating time is an hour and the maximum number of RTUs is 28.

approximate) and simulating solution.

Other tools can be consulted at [27]. NIST (National Institute of Standards and Technology) has developed ESTELLE tools called "Pet Dingo". They are

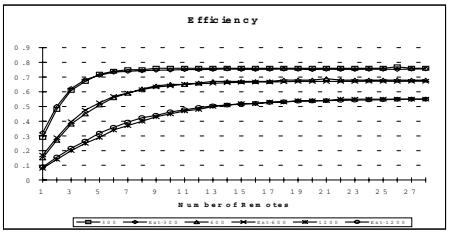

Figure 1.- Protocol efficiency (simulating and ESTELLE)

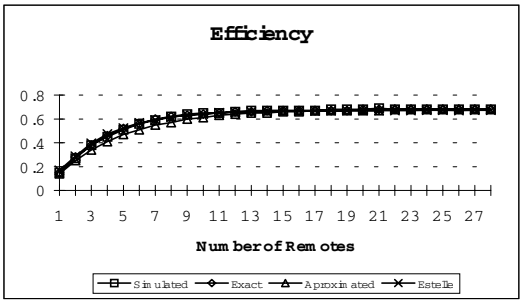

Figure 2.- Protocol efficiency (analytical, simulating and ESTELLE)

freeware software and are available via anonymous ftp from the NIST site ftp://snad.ncsl.nist.gov/pub/petdingo/. Their last version dates from 1996.

Institut National des Telecommunications in France distributes the ESTELLE Development Toolset (EDT) comprising a compiler, a simulator and debugger, a state/event table generator and a test driver generator. Versions of the EDT software with X11 Windows interface are available for Sun, HP and PC platforms under corresponding (SunOs4.1.3 and Solaris 2.5, HP-UX 9.01 and Linux 2.0) UNIX systems. Versions on IBM RS6000 and Bull DPX20 under AIXx.x, DEC/Alpha under OSF1 and PC under SOLARIS 2.5 (5.5) can be compiled on special request. An evaluation version of the EDT package and about licensing conditions can be download using the following address: http://www-lor.int-evry.fr/edt/. Now we are trying the application of this toolset to telecontrol systems. The US Army has applied this toolset to evolve the MIL_STD 188-220 [28].

The University of Kaiserslautern, Germany, is expected soon to release the eXperimental ESTELLE Compiler (XEC) (http://rn.informatik.uni-kl.de/activities/Estelle/XEC/) [29], which was developed to build a platform for the testing, performance-evaluation, and optimisation of implementation methods for ESTELLE. XEC is a fully operational and well tested ESTELLE compiler, which is "experimental" merely concerning its applicability as platform for experiments with implementation methods.

Another example of application of ESTELLE can be examined at the paper [30]. It describes how the ISO RTSE protocol [31] can be modelled using ESTELLE and the process of analysing such specification. The analysis is done by first transforming the ESTELLE specification into NPNs (Numerical Petri Nets) using the techniques they have developed, and then the NPN specification is analysed by a proven automated verification tool, PROTEAN [32].

IV. ADOPTING STANDARDS

The IEC (International Electrotechnical Commission) Technical Committee 57 (TC57), “Power Systems Control and Associated Communications” is in charge on international level of the technical aspects and realisation of world-wide standardisation of communication protocols for use in the energy sector. The relevant communication standards are IEC 61850 (standard draft) [33], IEC 60870-5 [34], IEC 60870-6 [35] and their level of application are respectively achieving interoperability of Intelligent Electronic Devices in substation, specification of protocols that are mainly based on the EPA (Enhanced Performance Architecture) and dealing with the definition of protocols for communication between control centres conforming to the 7 layer OSI stack.

These standards are all well defined and thoroughly described. Yet it turns out that if a manufacturer implements such a standard in one of his products, at a detailed level deviations from the standard may occur due to differences in interpretation between manufacturers. Also different subsets from the same standard may be implemented. Experiences show that this situation is not unusual.

Therefore, a solid testing strategy is necessary, it is presented one in the article [13] that should consist of the following elements (CIR):

- **C**onformance testing. The process of verifying that a protocol implementation is in accordance with a particular standard.
- **I**nteroperability testing. Different manufacturer products that implement the same protocol exchange information to test if a user of these products may use the functions provided in the protocol implementation to transfer data.
- **R**egression testing. It is applied to introduce errors on each layer of the protocol standard and verify that the system under test continues to communicate in a stable, conforming manner.

The CIR testing could be achieved using protocol

engineering techniques. The tools shown above test protocol implementations and they also automatically implement and analyse performance using the telecontrol protocol specification in ESTELLE.

Besides, protocols converter could be developed to operate vendor-proprietary telecontrol protocols with the standards. This could reduce the standard implantation costs.

V. CONCLUSIONS

The use of a communication infrastructure that is based on the IEC communication standards suited for telecontrol systems and substation automation can guarantee inter-connectivity. A number of alternatives are available, however, standards in general and open communication infrastructures in particular do not only have a strong positive effect on utility business and service (like cost reduction and decreasing implementation period).

Standard-based component have become a prerequisite for the modular and flexible control and substation automation systems which are demanded by the new, changing environment of the utility. It is in this point where the protocol engineering techniques could be applied to help the development of such an implementation.

ESTELLE is the FDT that adapts better to the electrical sector than other and we have applied it (performance analysis, protocol conversion, protocol integration). The tools presented in this article have to be deeply studied to try which one make suitable for telecontrol systems.

VI. REFERENCES

[1] David R. Ambrose. *"Inter-Utility Communications within WSCC"*. IEEE Transactions on Power Systems. Vol. 6, nº4. November 1991.

[2] Anindo Barnegea, Domenico Ferrari, Bruce A. Mah, Mark Moran, Dinesh C. Vernaand Hui Zhang. *"The Tenet Real-Time Protocol Suite: Design, Implementation and Experiences"*. IEEE/ACM Transactions on Networking. Vol.4, nº 1. February 1996.

[3] J.P. Bernard, D. Durocher. *"An Expert System for Fault Diagnosis Integrated in Existing SCADA Systems"*. IEEE Transactions on Power Systems. Vol.9, no.1. February 1993

[4] Dpto. Tecnología Electrónica. *"Convertidor Universal de Protocolos de Telecontrol"*. PIE nº 132.181. October 1992.

[5] T. E. Dy-Liacco. *"Modern Control Centres and Computer Networking"*. IEEE Computer Applications in Power. October 1994.

[6] Göran Ericson, Anders Johnsson. *"Examination of ELCOM-90, TASE.1, and ICCP/TASE.2 for Inter-Control Centre Communication"*. IEEE Transactions on Power Delivery. Vol.12, nº2. April 1997.

[7] Gerard Glijnis. *"European Utilities Open Lines of Communications"*. IEEE Computer Application in Power. Vol.9, nº4. October 1996.

[8] Y. H. Kim, N. Fukushima y T. E. Dy Liacco. *"KEPCO's National Control Center with an Advanced Energy Management System* ". IEEE Transactions on Power Systems. Vol. 5, nº 4. November 1990.

[9] H. Lee Smith. *"Substation Automation Problems and Possibilities"*. IEEE Computer Application in Power. October 1996.

[10] J.I. Escudero, J. Luque and F. Gonzalo. *"Quality of Service in the NOMOS TMN System"*. International Conference on Power Sector Telecommunication System for 21st Century. Nueva Delhi. (India). January 1997.

[11] J.I. Escudero, F. Gonzalo, J. Luque. *"The Challenge of Managing New Communications Technologies"*. SC35 CIGRE Colloquium. Beijing (China). September 1997.

[12] Carlos León, Juan B. Casado, Joaquín Luque, Fernando Gonzalo. *"SER: Expert System in the Fault Management of a Radio-Delay Network"*. IEEE Stockholm Power Tech. June 1995.

[13] Working Group 35.13. *"Telecontrol Protocols and The Importance of Testing Protocol Implementations Against The Standards"*. Electra Nº 188, pp 89-99, February 2000.

[14] Fuchun Joseph Lin, Ming T. Liu. *"The Rise of Protocol Engineering"*. IEEE Sotfware, pp. 14-15. Enero, 1992.

[15] Behçet Sarikaya. *"Principles of Protocol Engineering and Conformance Testing"*. Ellis Horwood. 1993.

[16] International Standard. *"Estelle- A Formal Description Technique based on an Extended State*

Transition Model". ISO-OSI 9074. First edition, 1989.

[17] *CCITT*. *"Specification and Description Language (SDL)"*. Z.100 *CCITT*. 1992.

[18] International Standard. *"LOTOS- A Formal Description Technique based on the Temporal Ordering of Observational Behaviour"*. ISO-OSI 8807. 1989.

[19] Joaquín Luque, Fernando Gonzalo, Francisco Pérez y Manuel Mejías, *"Formal Techniques Improve Connectivity in Supervisory Systems,"* IEEE Computer Applications in Power Magazine, April 1994.

[20] Pöschmann Axel, Hintze Elke, Hähniche Jörg and Dübner Ralf. *"Formal Methods –Quality insurance in communication and information technology"*. Copyright 1998 by the ifak e. v. Magdeburg, last changed 07/26/99. http://www.ifak.fhg.de/kommunik/english/Spec.htm

[21] A.V. Medina, I. Gómez, F. Pérez, J. Luque and S. Martin. *"Code Generator to Integrate Telecontrol Protocols"*. MELECOM'989. Tel-Aviv (Israel). 1998.

[22] Verónica Medina, Isabel Gómez, Sergio Martín,, Joaquín Luque, *"Applying Estelle to Automatically Determine the Performance of Telecontrol Protocols in SCADA Systems"*. CIGRÉ (Conférence Internationale Des Grandes Réseaux Électriques a Haute Tension) Cracovia (Polonia) 1999.

[23] Averill M. Law, W. David Kelton. *"Simulation Modelling and Analysis"*. McGraw-HILL International Editions. 1991

[24] OSI Reference Model. *"Information processing systems - Open Systems Interconnection- Basic Reference Model"*. ISO-7498. 1984.

[25] J. Luque, I. Gómez and J. I. Escudero. *"Determining the Channel Capacity in SCADA Systems Using Polling Protocols"*. IEEE Transactions on Power Systems. Vol.11, nº 2. May 1996.

[26] J. Luque, I. Gómez. *"The Role of Medium Access Control Protocols in SCADA Systems"*. IEEE Transactions on Power Delivery. Vol.11, nº 3. July 1996.

[27] Tenney Richard. *"Estelle Information"*. Updated 25 april 2000. http://www.cs.umb.edu/~rlt/estelle/.

[28] Paul Amer, Adarshpal Sethi, Mariusz A. Fecko. *"Using Estelle to Evolve MIL-STD 188-220"*. Estelle'98 Workshop, Paris, November 1998.

[29] J. Thees. *"Protocol Implementation with Estelle - from Prototypes to Efficient Implementations"*. ESTELLE'98, Evry, France, 2 November 1998.

[30] Jirachiefpattana Ajin and Richard Lai. *"Application of Estelle to Modelling and Analysis the ISO RTSE Protocol"*. January 1997. http://www.journal.au.edu/ijcem/jan97/doc2.htm.

[31] ISO/IEC 9066-1, *"Information processing systems - Text communication - Reliable Transfer Service Element. Part 1: Model and service definition"*. 1989.

[32] Billington J., Wheeler G. R. and Wilburham M.C. *"PROTEAN: A High-level Petri Net Tool for the Specification and Verification of Communication Protocols"*. IEEE Transactions on Software Engineering 14(3) (1988), 301-316.

[33] Draft IEC 61850-1 (1999). *"Ed.1: Communication networks and systems in substations - Part 1: Basic principles"*.

[34] IEC 60870-5-2 (1992-04). *"Telecontrol equipment and systems - Part 5: Transmission protocols - Section 2: Link transmission procedures"*.

[35] IEC 60870-6-502 (1995-12). *"Telecontrol equipment and systems - Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - Section 502: TASE.1 Protocol definitions"*.