THE INTEROPERABILITY OF THE PCCN LEVEL SUBSTATIONS

Olivier JARAY (1) Jean-Pierre THOMESSE (1),
Jean-Philippe TAVELLA (2)
(1) LORIA-INPL, 2 av. de la Forêt de Haye, 54516 Vandoeuvre lès Nancy, France
Tel : 33-3-83-59-55-76, Fax : 33-3-44-07-63
email : {ojaray,thomesse}@loria.fr
(2) EDF-DER, 1 av. du Général de Gaulle, 92141 Clamart
Tel : 33-1-47-65-35-61, Fax : 33-1-47-65-46-88
email : { jean-philippe.tavella}@der.edfgdf.fr

ABSTRACT

The development and the performances of networking and computing technologies leads to the definition of distributed applications rather than centralised ones.

A given system may then be composed of sub-systems provided by different vendors. Although technically and economically attractive, such a solution can only be used if the interoperability between the different sub-systems is guaranteed and verified.

This paper deals with those problems and proposes a solution based on formal modelling.

KEYWORDS

Interoperability, formal modelling, conformance tests, automatic generation.

1. INTRODUCTION

Open systems, heterogeneity, interoperability, interworking are the key words in the field of distributed systems. The move towards open systems, in conjunction with the new possibilities offered by communication networks, is leading electrical utilities to design substations with open architecture and digital technology. EDF's PCCN project [5], [6] is a typical example. PCCN is an acronym standing for "digital protection and control-command system for HV/MV substations", featuring an architecture divided into five sub-systems established using both technical and economical criteria.

The aim of the PCCN project is to bring a new technological generation into use for the HV/MV substation protection and control-command systems. The project arose from the need to replace the current EDF's substations with fully digital facilities, mainly in order to improve their reliability, reduce their maintenance costs and compensate equipment obsolescence.

The essential purpose is to reduce costs as a result of the vendors automatically being in competition [9]. This must be set against a certain number of additional difficulties as compared to the acquisition of a turnkey proprietary system.

This is because the policy of openness obliges the owner to carry out design work before construction and acceptance and integration work afterwards. With an open system, it is up to the user to verify the interoperability of sub-systems of different origins. The PCCN project is indeed now at this stage. The five sub-systems have been entrusted to different suppliers, with two or three sub-systems to each, and it will be up to EDF, as owner, to integrate them, assess their interoperability and settle any cases of non-interoperability. In such cases, EDF must be capable of determining which sub-system is responsible.

This paper deals with these problems and with their solutions which are also properties of heterogeneous sub-systems. In order to explain the proposed solution, the second section will describe the PCCN system architecture, regarding the communication features, and stating the real problem to be solved. In a subsection the new protocol called " M-PCCN " will be briefly presented.

The third section present the approach defined by EDF and the tests that should be realised. The last section will develop the method, based on formal description, used to realise the tests described in section three.

We will conclude on the advantages and drawbacks of such a method.

2. CONTEXT

2.1. System architecture

The following diagram shows the architecture of the control-command system for HV/MV substations represented as sub-systems connected to the substation communication network. Each sub-system consists either of a single item of equipment or several items of equipment connected to an internal network specific to the sub-system (and its manufacturer).

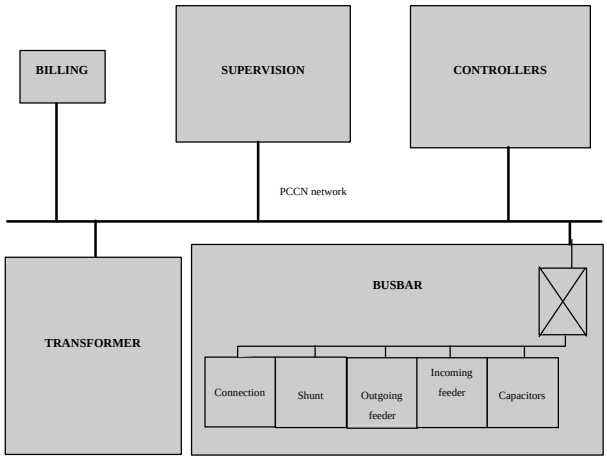

Figure 1 : System architecture

The functionalities of the different sub-systems are briefly the following :

- Supervision : to record all system events and to ensure the local control (including network management) and a remote control (interface with a long distance network);
- Controllers : to support distributed functions as automatic permutation of transformers or Var control;
- Busbar : to detect faults and ensure busbar protection;
- Transformer : to ensure transformer protection, high impedance fault detection, auxiliaries ground protection and transformer tank ground protection.

2.2. Sub-system architecture

The communication network is a 10 Mbps Ethernet network with a fibre optic medium to avoid ECM problems. The communication protocols selected to fulfil the digitally-controlled substation requirements are those detailed in the following diagram :

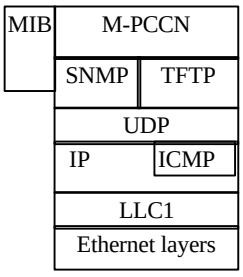

Figure 2 : Stack of protocols

All the sub-stations on the network must have this stack of protocols. The application layer contains all the application processes communicating thanks to the M-PCCN layer based on SNMP and TFTP standards.

All the objects are defined and structured according to the rules of the SNMP MIB (Management Information Base).

This communication system must transmit MIB data for reading, writing or updating actions. These data are states (called double TSs or permanent single TSs in remote operation), events (called transient TSs), commands (called TCs), readings (called TM) or files. Communication network control and distributed data base integrity are also required.

The data exchanged in real time can be divided into two categories :

- evolving data whose value depends on the real time system and the electrotechnical process and which can be characterised as a function of time. In the digitally-controlled substation, binary states are managed (value 0 or 1 corresponding to open or closed, enabled or disabled, set or tripped etc.) as well as numerical readings;
- ad hoc data represented with timestamp occurrences. Such data can be a transient data (event of "momentary" interest), a command (invocation of an action to perform a state change on an element of the process or the control-command system), a request (like a command but without acknowledgement), a setpoint or a file.

Each M-PCCN entity plays then the role of an SNMP Agent or Manager according to its position of client or server, producer or consumer regarding the services.

To exchange those objects, the following services have been defined :

- CDE : to control a remote organ or function
- EF : to transmit a transient event
- ETAT : to signal a state change
- CONS : to transmit a setpoint
- LCONS : to read a remote setpoint
- MES : to update a local reading
- LMES : to read a remote reading
- DOWNLOAD : to transfer a file
- UPLOAD : to bring back a file
- REQ : to transmit a request
- CNX/DNX : to establish the connection or the disconnection of a sub-system on the network and permanently control the connected remote sub-systems.

Those services have been defined in the M-PCCN layer to fill out the missions defined above.

3. EDF APPROACH

For the PCCN project, EDF has defined three steps for a complete validation of the system. These steps are presented and illustrated in this section.

3.1. Qualification

As a sub-system can be seen as a set of components, each of them is firstly and separately tested. The communication stack (refer to section 2) is one of these components and will be considered alone in this subsection.

As a postulate, we suppose the protocol implementation of the stack except the M-PCCN layer fully conform to the standards (SNMP, TFTP, ..).

In this context, the qualification phase includes two goals, the conformance and the robustness tests of the protocol M-PCCN implementation.

The conformance testing is divided into two steps. The first one is the MIB validation. It consists on checking that all objects are correctly structured and accessible through read and write services. The second step must validate the services one by one. We have to be sure that the sub-system reacts as defined in the specifications.

The robustness tests goal is related to some critical behaviour. In this case, the test suites are directly deduced from the knowledge of the sub-system and of the application. We realise a burst of SNMP services to be sure that the sub-system correctly reacts. For example, we send ten SETs or GETs to the sub-system and we verify that they are all taken into account.

3.2. Acceptance

Acceptance tests are defined to be sure that a single sub-system is able to communicate and to interoperate with a test bench which is in fact a model of the other sub-systems and of the electrotechnical process.

The acceptance phase must verify that the sub-system is able to exchange correctly the right PDUs with the tester. It is composed of two steps :

- the choice of a test suite is made and the IUT (Implementation Under Test) is set in the right state;
- a specific application process which may be considered as an automaton is started, and the exchanges are recorded.

For each test, the result may be “success” or “failure”. In the standardised conformance testing methods, the result may be “success”, “fail” or “inconclusive”. In the M-PCCN acceptance testing approach, an inconclusive result is considered as a failed one.

3.3. Integration

The integration tests goal is the verification that a given sub-system is able to interwork with one or several real other ones. At the positive end of the acceptance tests, a sub-system is considered as “accepted” regarding the simulated environment of the tester. At the integration stage, several real and accepted sub-systems are tested together. The integration is organised in a progressive way, in the sense that simulators are gradually replaced by real sub-systems. Nevertheless, except for the final trial (including exclusively real sub-systems), the test bench is still required for simulation.

3.4.Test bench architecture

The test bench is the same for acceptance and integration tests. It is composed of :

- a set of simulators of the sub-systems;
- a simulator of the electrotechnical process;
- an observer;
- a test manager.

The following illustration shows the global architecture of the test bench. A simplest one without electrotechnical process simulation and without any sub-system simulator is used for the communication stack qualification.

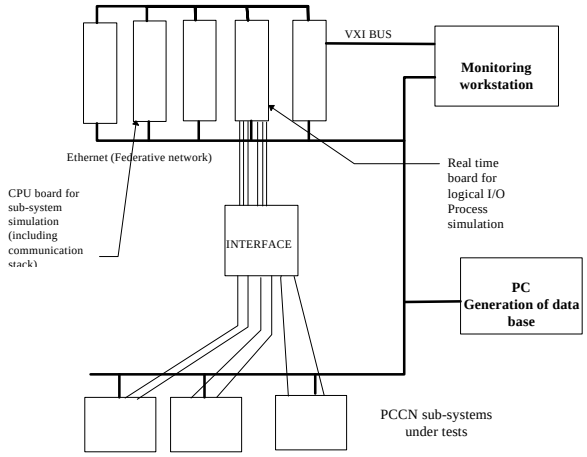

Figure 3 : Test bench

The IUT is a real sub-system with its communication stack and its application processes. As in a real substation, it is connected to the tester through the real Ethernet network and the electrotechnical process simulator with its own inputs and outputs.

The electrotechnical process is modelled by an automaton with a set of real analogue and digital inputs and outputs.

A sub-system simulator is a black box exchanging PDUs with its environment like any real sub-system. But in addition, it can communicate with the tester directly through an ad-hoc communication system for programme transfers and test scheduling.

The observer records and analyses all the frames exchanged between the IUT and the simulators.

3.5. PICS and PIXIT

To carry out the implementation of the tests suites, we have written two documents which have been distributed to the manufacturers. The first one, called PICS (Protocol Implementation Conformance Statement), groups together the list of the services implemented by the manufacturers and all the parameters and timers defined in the specifications. For those objects, meaning, range of values, unit and step are given. The second document, called PIXIT (Protocol Implementation eXtra Information for Testing) states how services can be stimulated or observed.

3.6. Conclusion

The EDF approach to verify the sub-systems and the global system has been presented.

The qualification tests include the conformance testing [7]. But it is more complete since some robustness tests are added.

The acceptance tests are relevant of the interoperability and interworking testing [1], [8]. And the tests are managed as for conformance checking since a single sub-system is concerned at a time. Indeed, the tests include the application processes of the sub-system. In this sense, they verify for each sub-system some interoperability without any distinction between application dependent and application independent aspects [10].

The acceptance tests include also a robustness test.

The integration tests are really an interworking test.

The test suites are the same in both cases. Their generation with the help of the formal method used is studied in the next section.

4. FORMAL METHOD PRINCIPLES

4.1. Specification and description

The specifications of all the PCCN system (called STB at EDF) are described in a natural language (French). The use of a formal method presents a first interest in decreasing the risk of misunderstanding among manufacturers because ambiguities inherent in any natural language are suppressed.

We have first described each independent function thanks to an array representation of states/transitions and actions. The following figure presents a very reduced example of this representation :

Init. state	Event	Action	Next state
CNX	CDE.ind	SET.req	Wait
Wait	Get_Response.ind	CDE.cnf	CNX

Figure 4 : Automaton representation

This formal specification is not contractual but is given to the manufacturers so that they get very rapidly a global view of the system (especially for sub-systems the development of which they are not in charge). Then, to validate the dynamic side of the system, we have chosen the language SDL (Specification and Description Language) [2], [4].

SDL is a language allowing the definition of state/transition communication systems through send and receive primitives and including the management of delays. It isn't the most formal but it has the advantage to be very easy to read and understand.

4.2. Validation

Starting from the previous specifications and models, we now lead their validation and their checking using the following method.

At first we use the simulator tool of the ObjectGeode software [11] in order to simulate the model step by step. We can thus check the model on which all the following steps depend on.

To validate the formal specification, we realise a simulation of the SDL model and we compare the results to the specifications. If they correspond to the expected ones, the formal specifications are validated.

Finally, we use the checking tool to detect automatically the possible deadlocks, livelocks and so one of the STB. The following scheme summarises this methodology :

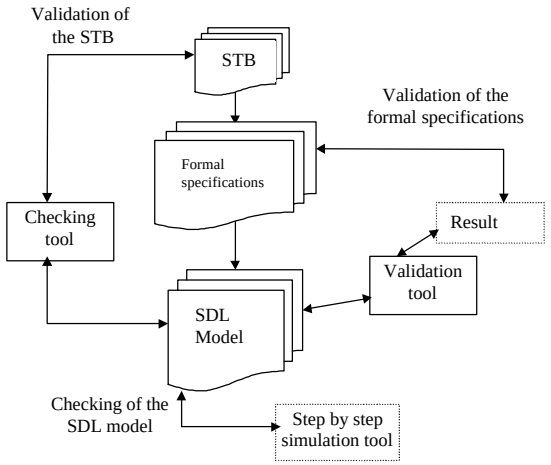

Figure 5 : Principles of validation

After this validation, we can use the SDL model as a validated equivalent (but simplified) representation of the specifications to generate the tests suites.

4.3. Test generation

To generate the tests suites of the qualification step, we have modelled in SDL the stack of protocols under M-PCCN with the only objective to convey correctly a message, to lose it, to delay it or to generate errors.

Then we have applied the checking tool on the SDL model of the system and the communication stack to automatically generate test scenarios. Then, we have transformed them in an MSC (Message Sequence Chart) standard representation in order to model the messages exchanged between the different entities. The following figure stands for an example of such a representation :

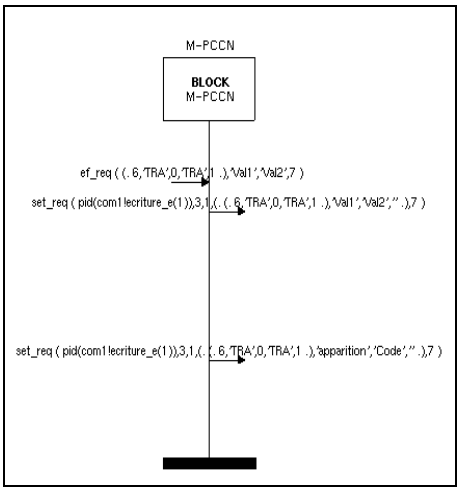

Figure 6 : MSC representation

The requested services are coming from the left of the vertical line and the exchanged messages are on the right side.

For the acceptance and integration step, a small but significant part of the PCCN application has been modelled in SDL. This study focused on the control of permutation of transformers in case of failure.

As they are based on state/transition formalism, the SDL models describing this application behaviour lead to an explosion of the number of states. Some simplifications have been made in order to reduce the number of states and transitions. But in spite of these simplifications, the number of generated test suites stay so great that a generalisation to all the PCCN system does not appear credible with this approach.

Nevertheless, we have shown that among the numerous tests found, some were relevant and not obvious even for electrotechnical specialists.

5. CONCLUSION

In this paper, the methodology chosen by EDF to qualify and verify control-command sub-system implementations has been presented. This methodology has also been briefly compared with general purpose test methods.

This paper has shown :

- the interest in SDL use for validation of the M-PCCN protocol and for generation of tests (refer to the qualification step but also to a possible future standardisation [5], [20]);
- the same interest for the application validation in spite of the limits due to the explosion of the number of states;
- the fact that the formal specification has led to solve several ambiguities in the initial specification written in natural language.

More generally, the EDF methodology could be extended to other networks and applications.

The work has also shown the necessity for a theoretical research on mathematical reduction of complex models maintaining the same semantic or properties than the original specifications. But such a research was not compatible with the constraints of the PCCN project in terms of delays and budget.

Another way for research could be in a more modular specification and design of the applications definitely avoiding natural language specification.

Finally, it could be interesting to research how to model the application in a simplified way rather than simplifying a complex model.

6. REFERENCES

[1] Y. Benkhellat and J.P. Thomesse "Validation of timing properties for interoperability in distributed real time applications". Proc 13th PSTV, IFIP, Chapman and Hall, 1994, pp331-338.

[2] R. Braek "*SDL Basics* Computers Networks and ISDN Systems 28", 1996. Elsevier Science B.V.(Editeur). p1585-p1602

[3] E. Brinksma (1988). "A theory for the derivation of tests". In PSTV VIII, IFIP, Elsevier Science Publisher, pp 235-247.

[4] ITU Z100 SDL 92, "Secification and Description Language", ITU Geneva, 1994

[5] P. Godfrin, WY. Thang, G. Barssoff, "Digital protections and control-command system of HV/MV substations specification of an open architecture". DASM Europe, 1996, Vienna

[6] P. Godfrin, WY. Thang, M. Poncin, JF. Brisset, "a digital parcelled-out protection and control system of HV/MV substation". Power Delivery, 1997, Madrid.

[7] ISO IS 9646-1 to IS 9646-5. "Open Systems Interconnection OSI conformance testing methodology and framework". 1988.

[8] O. Rafiq "Sur la vérification de l'interconnexion des systèmes". In CIM'90. Bordeaux, France, 1990, pp 557-564.

[9] W.Y. Thang, JY. Boussion, B. Peruzzo, R. Hubner, “An approach for an open control system for substations”, CIRED 1997, Birmingham.

[10] J.-P. Thomesse “Interoperability, an overview, SICICA”, 3rd IFAC Symposium on Intelligent Components and Instruments for Control Applications. L. Foulloy Ed., 1997, Annecy, France, pp473,478.

[11] several documents on the ObjectGeode software tool :

- ObjectGeode ProjectOrganiser : Reference Manual. Version 1.3.
- ObjectGeode Method Guidelines Version 1.0.
- ObjectGeode Tutorial.
- ObjectGeode Training : Analysis and Design of Real-Time Systems.
- Verilog, 52 avenue Aristide Briand, 92220 Bagneux.