

# Software and hardware in the loop component for an IEC 61850 Co-Simulation platform

Mohamad Haffar  
Euro System, GIPSA-lab  
(UMR 5216)  
Grenoble-France  
Email: mohamad.haffar@euro-  
system.fr

Jean Marc Thiriet  
GIPSA-lab (UMR 5216), UJF  
Grenoble-France  
Email: jean-marc.thiriet@ujf-  
grenoble.fr

Mohamad El-Nachar  
Université Libanaise Faculté Génie  
Branche1, GIPSA-lab  
Tripoli-Lebanon, Grenoble-France  
Email: mohammad.el-  
nachar@gipsa-lab.grenoble-inp.fr

**Abstract**— The deployment of IEC61850 standard in the world of substation automation system brings to the use of specific strategies for architecture testing. To validate IEC61850 architecture, the first step consists in validating the conformity of the object modeling and services implementation inside devices. The second step consists in validating IEC61850 applications compliance according to the project specifications. A part of the architecture can of course be tested “physically”; however in the design phase or when the actual architecture cannot be checked directly, modeling is helpful. In our research study we propose a co-simulation approach based on several components allowing the realization of advanced tests. This paper describes the need and the design implementation of software and hardware in the loop components as well as the object modeling concept of IED models.

## I. LIST OF ABBREVIATION

The following table 1 contains the definition of acronyms used in this paper.

TABLE I.  
ABBREVIATION LIST

<u>Acro- nym</u>	<u>Definition</u>
IED	Intelligent Electronic Device
SAS	Substation Automation System
FAT	Factory Acceptance Test
HITL	Hardware In The Loop
SITL	Software In The Loop
UCAIUG	Utility Communications Architecture International Users Group
GOOSE	Generic Object Oriented Substation Event
MICS	Model Implementation Conformance Statement
PICS	Protocol Implementation Conformance Statement
ICD	IED Configuration Description
MX	Measurand analogue value X
SCL	Substation Configuration language
RTG	Run Time Generation

## II. INTRODUCTION

In the early 1990s communication technologies and protocols began to appear in SAS application. In 2004, a new worldwide standard of communication IEC61850 was introduced in the majority of substation automation systems car-

rying out new innovation prospects. The interoperability between devices from different manufacturers as well as the insurance of the overall security of SAS architecture through its communication network becomes now attainable with this new communication standard [1]. In addition, object data modeling is used inside IEC61850 equipments to replace the aspect of non significant addresses. The standard provides a stack of services in order to obtain a self description of the internal objects and communication capabilities of the device; this leads to reduce the time of developing supervision control and data acquisition applications.

IEC61850 authorizes the distribution of functionalities between devices. This aspect permits the exchange of real time inter-equipment messages over the communication network to provide advanced services for electrical substation process which was done previously via hardwiring (e.g. interlocking, load shedding, auto transfer switch, etc...). The real advantage behind consists in reducing the amount of cables inside a substation which can be very long due to the distance between the substations (i.e. installation price). However this new aspect of configuration relies on a peer to peer device messages sent over the communication network. Thus it must be well verified before any implementation [2].

Being the unique standard used in the SAS network, devices from different manufacturers are able to dialog in order to exchange information and services. This feature brings to the engineering staff more liberty in choosing their IED (e.g. protection relay, power meter ...). However, the heterogeneity of IEDs inside SAS architecture yields complexities to the FAT which becomes difficult to realize due to the dispersed location of the switchboards suppliers. An exhaustive FAT must be provided with each project development in order to minimize time of site commissioning. This point is an essential key demanded by the end users.

End Users must have a realistic view about the demanded SAS architecture tests according to their desired requirements. Thus they should comprehend the limitation scope of the conformance tests provided by the international certification organizations such as Kema [3] versus a complete successful implementation of IEC 61850 SAS architecture which should be well coordinated by all involving parties.

This work was supported by Euro System Company and GIPSA Laboratory

### III. LIMITATIONS SCOPE OF STANDARD CERTIFICATION TESTS

A generic testing plan for an IEC61850 SAS architecture shall include four testing categories: the conformance testing of a device, the distributed functionalities testing, the interoperability testing and the global system performance evaluation [4]. Witness and hold points shall be specified in the testing plan for carrying out inspections that verify the quality of tests.

UCAIUG has established a conformance testing program for IEDs which permits the certification of the internal object data modeling, communication oriented services and the global configuration online testing.

These conformance tests could be considered as parts of the device conformance testing. Therefore distributed functionalities, interoperability and global system performance evaluation tests are still left unanswered. Guidelines are given by the international certification organization to accomplish these advanced tests.

New tools and advanced models should be provided to fill the gap of tests. These tools should also permit the cohabitation of real devices of a switchboard supplier with virtual device of the missing switchboard to ensure an advanced FAT in a heterogeneous SAS architecture.

Based on the guidelines of advanced tests proposed by international certification organization, our work deals with a Co-Simulation Platform to accomplish a complete IEC 61850 advanced test. This platform is constituted of a simulation software and other additional components. Virtual IEDs will be modeled inside the simulation platform by implementing real communication IEC61850 services and data objects. The additional components are used in order to ensure the overall utility of the simulation platform. As shown in Fig. 1 additional component are divided into three categories: the standard simulation configuration component, external process interface component and Hardware in the loop component.

The major purpose of the Standard simulation configuration is to generate and configure any IED model by importing its device configuration file. Using this component our simulation platform will be able to simulate an heterogeneous architecture containing IEDs from different suppliers.

In this paper we show the purpose and the implementation detail of the external process interface and hardware in the loop component.

### IV. OPNET NETWORK SIMULATOR

Modeling and simulating a networked system requires a network simulator that takes into account all major contributions including protocols, medium access control technology, network load, communication imperfections, timeouts and packet losses etc. Popular network simulators include NS2, OMNET, Qualnet, OpNet etc. OpNet Modeler is chosen in our research because it implements a large number of libraries of standard equipment (e.g. switches and link models) as well as proprietary models, which is useful for simulation and reduces the development time [5]. Object oriented modeling approach fitted into many programming editors is

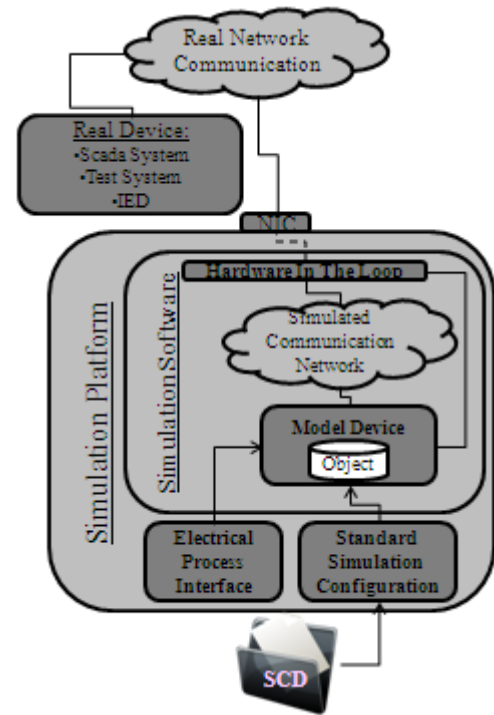


Fig. 1 Co-Simulation platform architecture

used in OpNet in order to facilitate the construction of models (Fig. 2).

A network device is modeled as a node which is composed of many modules connected by packet streams or static wires. Each module aims to represent specific aspect of the node's behavior such as data creation, data storage, data processing or routing (IP layer), data transmission (Transport layer), etc. Thus the modeling of each layer of the TCP/IP stack is made in OpNet modules.

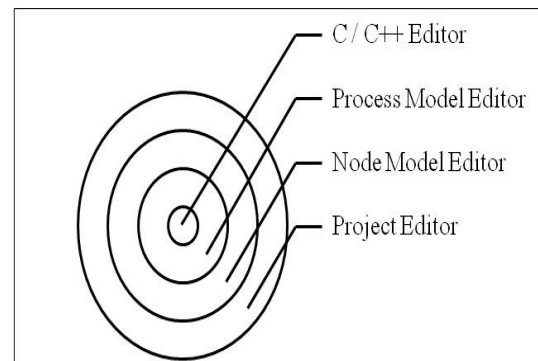


Fig. 2 Simulation software editors

The process is programmed using the finite state machine (FSM – Technology). This approach facilitates the supporting of the implementation of applications, algorithms and queuing policies. States and transitions graphically define the progression of a process in response to events. Each state in process model contains embedded C/C++ code, supported by an extensive library of functions designed for network programming.

Two kinds of states are used in OpNet Modeler: red states and green states.

A red state in the process model is an unforced state. Unforced states allow a pause between the enter executives and exit executives, and thus can model true states of a system. After a process has completed the enter executives of an unforced state, it blocks and returns control to the previous context that invoked it. When an interrupt occurs and invokes the process, the exit executive will be treated as well as the test of the transition to the next state.

A green state in the process model is a forced state. Forced states are so called because they do not allow the process to wait. In other words, the exit executives of a forced state are executed by a process immediately upon completion of the enter executives.

## V. CO-SIMULATION COMPONENTS

This paragraph shows the importance of the presence of the external process interface and the hardware in the loop components inside our Co-Simulation platform in different phase of IEC61850 project.

### A. Typical architecture of an IEC 61850 switchboard under test

Each IEC61850 server (i.e. device or model) is delivered with its Model Implementation Conformance Statement ‘MICS’ and Protocol Implementation Conformance Statement ‘PICS’. MICS documentation describes the capabilities of the device in term of functionalities described in object format. However PICS is another documentation which describes the IEC61850 services supported by the device. The conformance tests of a device [6] is based on tests that cover the conformity of object data modeling as well as the conformity to IEC 61850 Abstract Communication Services Interfaces ‘ACSI’ according to PICS and MICS documentations.

Three types of services can be found inside each IEC61850 server:

- Client/Server pooling services which are initiated by the IEC61850 client.
- Peer To Peer services (via IEC61850 GOOSE message). These services are generated by the server on event. It provides the sharing of functionalities between devices.
- Reporting services which are heavy load generated periodically or on event by the server. This kind of services permits to decrease the network load by reducing the number of pooling services.

It is shown in Fig. 3 an image of a typical IEC61850 future substation. The substation is divided into three switchboards including each a group of IEDs coming from different device supplier. The switchboard S1 is the one under test inside S1 factory placement. The switchboard S2 shares functionalities with the switchboard S1. This switchboard is considered absent in our architecture for the fact that it comes from another device supplier. The last switchboard S3 doesn’t share any functionality with the other switchboards but is connected to the same communication net-

work. IEDs of the switchboard S3 are also missed during FAT of S1 thus it can be considered that all physical IEDs that belong to S2 and S3 will be replaced by their models inside the simulation platform.

In order to validate the functionalities of the switchboard S1 two different kinds of tests should be provided:

- Test of the functional part of the switchboard’s IED,
- Test of the communication part of the switchboard’s IED.

Functional part aims to test all the protection and control parameters of IED inside S1. This is done by connecting an electrical process board to S1 and injecting the process values on the inputs of its IEDs.

The most critical point in the communication test consists to verify the exchanging of peer to peer messages between switchboards that shares functionalities. Therefore three different tests should be provided:

- Testing the publisher part of the peer to peer messages from the switchboard S1 to S2 according to the configuration of S1 IEDs.
- Testing the subscriber part of peer to peer messages from S2 to S1 which consists to verify that the IEDs inside S1 accept the peer to peer messages coming from the S2.
- Verifying that the end to end time of the peer to peer message doesn’t exceed the time specified in the specification of the project.

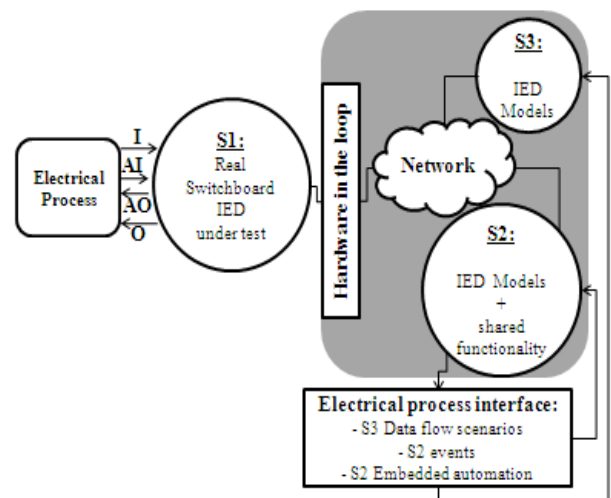


Fig. 3 Typical IEC61850 architecture under test

### B. Hardware and software in the loop during FAT

To test the publisher part of S1, an electrical process board must inject real inputs to the IEDs inside S1 in order to publish the peer to peer messages. Hardware in the loop component is developed in our study in order to route the real network message from the real world into the simulation platform. Once arrived to the simulation world, the peer to peer message enters the simulation network and reaches at the end to the virtual IED subscribing to this message.

In the factory acceptance test stage, a punctual study of the end to end time parameter of the peer to peer messages must be given for the reason that these messages are used to solve time critical electrical applications. The dynamicity of this parameter comes from the network delays due to the data flows sharing the same network. Real IEC61850 data flows scenarios must be generated as configured inside the IEDs of S1, S2, and S3. Therefore it is crucial to have an electrical process interface inside the simulation platform which corresponds to the electrical process board inside the real world. This component is connected to the simulation platform in order to produce real IEC61850 data flow scenarios for S3 and generate planning events to test the peer to peer message sent from S2 to the switchboard under test S1 (Fig. 3).

### C. Hardware and software in the loop during platform development

Our Co-Simulation platform is based on the modeling of device communications. The increase of confidence in the platform is an important point in our research study. To accomplish this point, compliance tests should be provided to IEDs models according to the IEC 61850 flowchart tests. Thus, in order to test the compliance of IED services according to PICS documentation, the software in the loop and hardware in the loop component must be used with the simulation platform. The software in the loop will be used in this case in order to generate Inputs/ Outputs simulated process value (e.g. voltages and currents exceeding values, status trip and default) to the IED model and check its behavior (i.e. reports and peer to peer message transmission). However the hardware in the loop component will be used in order to connect the model under test to a test external system to validate the services declared in its PICS documentation.

## VI. HARDWARE IN THE LOOP MODULE IMPLEMENTATION

A HITL node is based on an edge Router interface which is used inside the simulation platform in order to provide the workflow for exchanging packets between simulated and real devices. The detailed of this workflow is shown in Fig. 4.

The first important job of the edge interface router is the mapping of external network interface of the simulation machine to the network interface of the appropriate device model. HITL allows multiple interfaces to map different network addresses in the simulated network.

The HITL module has many associated attributes that permit to describe the HITL behavior. One of these attribute is used for filtering packets received by HITL in order to reject unexpected packets and allocate memory for expected real world packets. If the packet is accepted, the edge router enter the creation phase where it constructs the skeleton of the simulated or real packet weather if the packet received is real or simulated.

To succeed in the phase of copying the contents of packet fields between the two formats, HITL requires a predefined well-known protocol format included in the Standard Model

Library. Otherwise, if the packet received is not a part of the library, a custom code must be written for providing the conversion of the unsupported protocol format packets else it will be dropped by the edge router and will not enter the simulation world. The protocols format packets supported or partially supported by HITL are the ones associated to standard TCP/IP layers as shown in Fig. 5.

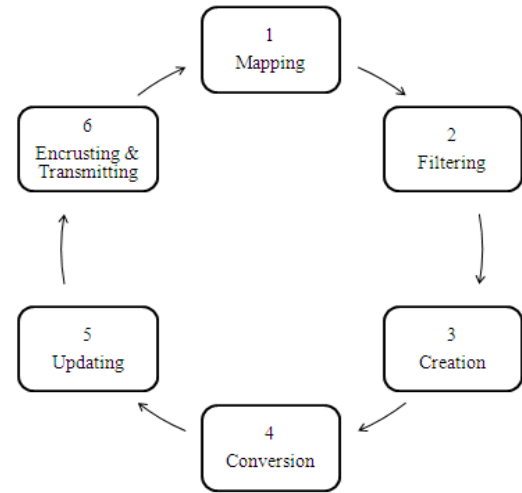


Fig. 4 Hardware in the loop workflow

As described in the introduction, the Simulation Platform is used for solving Power Management System ‘PMS’ issues, thus HITL must provide conversion of protocols associated to PMS more particularly the IEC 61850 standard. IEC 61850 packets format and other industrial protocols are not included inside the Standard Model Library Packets thus the conversion of application layer packets are not provided with a nominal HITL.

Our customized user code is developed to provide the conversion of protocol application packets. In addition, the code is also used to fill in uncompleted conversion points of transport packets by updating (i.e. phase 5 of the HITL workflow shown in figure 6) TCP missing fields which are associated to the application (e.g. data length field).

A surplus point of our custom code is that it has been developed in a way to make use of HITL with any industrial hardware device taking into consideration that it is possible to have heterogeneous power management architecture combining the IEC 61850 and other industrial protocols such as Modbus or others.

After a successful conversion and updating of partially supported packets format, the HITL encrusts real or simulated packet into a SITL conversion block and routes it finally to the appropriate model if the original packet is real or to the external world if the original packet is simulated.

## VII. SOFTWARE IN THE LOOP MODULE

### A. OPNET Problematic

In OpNet modeler, C functions can be placed in three different placements:

- Process model states,

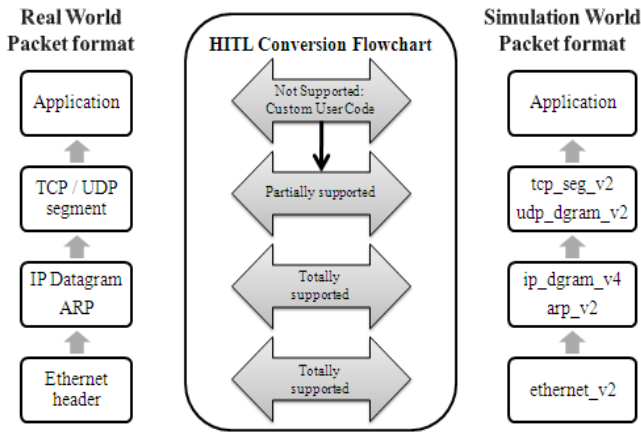


Fig. 5 Hardware in the loop conversion supported packets

- Function blocks attached to a process model,
- External OpNet Library.

When a function is defined inside a function block, it can only be used by the process associated to the function block. External OpNet libraries differ from the function block because when a C function is defined in an external library it can be shared with different process models. Finally if the C function is defined inside a state, only the state can have access to this function.

Three types of variables can be found for particular use inside the OpNet process model: the state, the temporary and the global variable. The table 2 shows which kind of functions can have access to these variables.

TABLE II. VARIABLES VISIBILITY INSIDE SIMULATION

		Visibility			
		Opnet State executive	Opnet Function block	Opnet External Library	External application
Type of variables	Temporary	X			
	State	X	X		
	Global	X	X	X	

What should be concluded is that only OpNet functions can have access to the simulation variable environment. Electrical process interface is considered as an external application to the simulation software. Therefore as shown in the table 1 this application will not be able to exchange variable values with the simulation on run time. For this reason a software in the loop package [7] is developed in this study in order to make this point feasible.

B. Software in the loop package constitution

Software in the loop consists on a package associating three different modules: C predefined research library, Data base, electrical process software. The purpose of this package is to provide an access method which authorizes the electrical process interface to exchange information with the simulation variables.

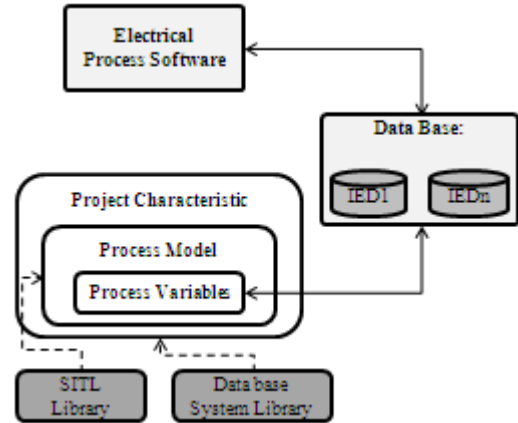


Fig. 6 Software in the loop package

The data base shown in Fig. 6 is used as an intermediate component between the OpNet process and the electrical process interface. Each IED electrical process values is included as a table inside this database in order to have at the end all the electrical process values of all the IEDs integrated inside the modeled switchboards.

In order to ensure a real time exchange between the OpNet process variables and the data inside the database, two libraries are integrated inside the simulation software. The first one is a system library which is implemented in the project properties to provide a communication language between simulation software acting as a data base client and the data base server. The SITL library is developed in our research in order to authorize the simulation to read and write values inside the data base. The read procedure is programmed in a periodical mode in order to collect the changes of the process values. The period of generation will depend on the cycle time of the real IED which will be modeled. On each process value changes, this library generates the appropriate OpNet process interrupt to invoke the state that corresponds to the changes. The collected values will be then placed inside the simulation environment variable. The writing procedure is programmed in event mode. This function is invoked by the library when an external client sends a writing request to an IED model inside the simulation.

VIII. HARDWARE AND SOFTWARE IN THE LOOP TEST

The simulation test described in this paragraph shows how HITL module is used in order to test the compliance of data modeling inside an IED model.

A. IEC61850 modeling concept

The IEC61850 includes a comprehensive set of data models for substation (and beyond) functionality. The models

are, in general, constructed from a set of common data classes (defined in part 7-3 of the standard). The common data classes are used to build data objects, which are then clustered in logical node classes. Each logical node class represents some basic application function. Instances of the logical node classes are then combined to construct logical devices. A physical network device may contain an arbitrary number of logical devices. The set of classes (common data classes, data objects, and logical node classes) define the network visible data types (network interface), along with some standardized behavior, definitions, and configuration parameters [8]. One of the most important points in testing a physical or model device is to verify the compliance of its data object modeling. The paragraph below describes how HITL module is used for accomplishing this point.

### B. Hardware in the loop for testing object modeling

When a physical or a model IED is developed, it is delivered with its PICS and MICS documentation which describe the capability of the IED in term of functionalities and services. Before delivering the IED, it is crucial to verify the conformity of these two documentations according to the IEC61850 specification to increase confidence in implementation (i.e. interoperability). Verifying the MICS of the IED consists to check:

- The existence of the functionalities defined in the MICS
- The compliance of the object modeling according to IEC 61850 standard dictionary (i.e. part 7.3 and 7.4)

The testing of IEC 61850 implementations is potentially a large task, given the large scope of the standard services and data models. IEDScout is a universal IEC 61850 test systems [9] that can be connected to any IEC 61850 device (server) and provides many useful functions for verifying data model, reading and writing data, reporting, along with GOOSE publishing and subscribing.

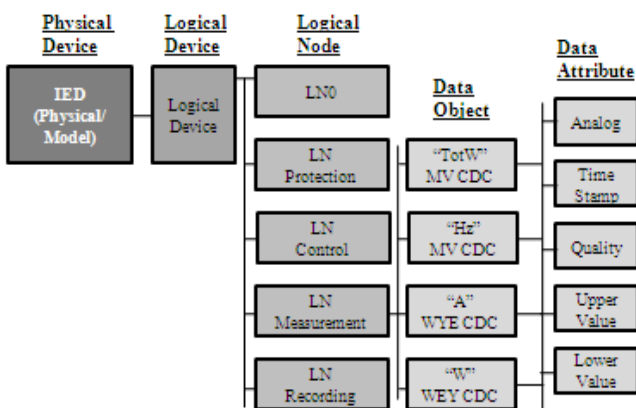


Fig. 7 Simple server MICS representation

A simple IEC 61850 measurement unit functionality has been implemented in our IED model to test the data object implementation. The model IED does not implement the functionality, but it is important to note that even unmapped model elements are implemented in the IEC61850 side of

the model. The MX logical node contains four standard measurement unit data objects: TotW, A, W, Hz which permits to calculate the energy, current, power and frequency. Fig. 7 shows the MICS representation of the IED model.

Fig. 8 is explained that the generation of IEC61850 dictionary relies on the implementation of essential points:

- An ICD configuration file which describes the content of the server (i.e. simple server in our example). This file is generated by the SCL standard editor that produces IEC61850 configuration files.
- SCL RTG Library which includes predefined IEC 61850 code that aims to generate on run time the IEC61850 object dictionary according to the ICD configuration file and to implement the auto discover functionality.

For testing the conformity of implementing the server data model, HITL is used to connect the real IEDScout test system to the IED model using real to simulated scenario. The aim idea consists on showing the content of the IED model and identifying the object included in the model that are conformed or not to the standard dictionary. The test system sends an auto discover query to the configured IED model in order to discover the content of its standardized data object. This query passes through the HITL component as shown in Fig. 8. At its turn, the IED model sends back a file transfer response containing its entire data object content, the response reaches the real world also through the HITL component. In our example, the test system shows clearly the content of the simple server included in Fig. 8. This allows us to certify the implementation of simple server data object.

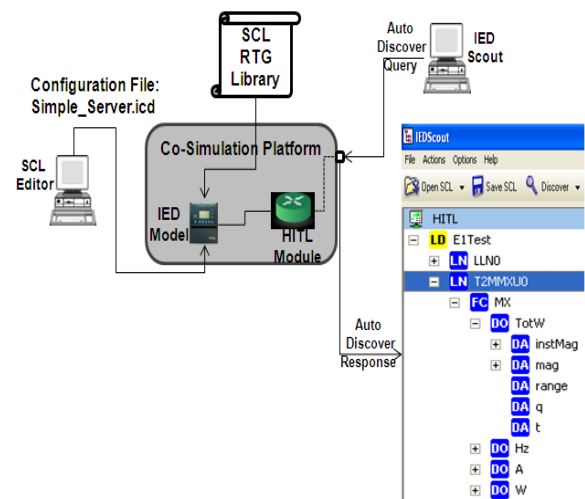


Fig. 8 Object modeling testing platform

### C. Software in the loop Test

In order to validate the functionality of the SITL package, a small application is developed in our study. Inside this application, the electrical process software is developed in order to support 1 IED containing 4 categories of process values: Current, voltage, frequency measurements and finally the status position.

In order to validate the SITL package, a simple OpNet modeler node is developed. This node contains a simple module that implements one process model. This process model will be further implemented inside the application OpNet module of the final IED IEC61850 model. The first state 'red' is an unforced state which waits for an interruption coming from the process in order to execute the output transitions. This interrupt will be generated periodically from the SITL library. On the exit executive of the initial state, many states can be invoked depending on the condition calculated by the SITL Library. The activation of a condition depends whether the process value has changed or not. Each process measurement (i.e. current, voltage, frequency, and status) is associated to a forced state in order to run the control procedure associated to the measured value. In order to give a demonstration of the SITL package, the measurements are printed in the OpNet debugger console 'ODB' inside each forced state. As shown in the OpNet Debugger Interface 'White Window' in Fig. 9, when the voltage value changes to 220kV, this value is inserted inside the data base and printed on the OpNet debugger 'Output Console of OpNet'.

IX. CONCLUSION

The paper shows the development of a co-simulation platform, for the evaluation of IEC61850-based architectures. The use of OpNet Modeler, which is an event-based simulation tool for networks, is interesting in such a context. A HITL/SITL gateway has been developed, allowing interfacing physical actual components, and virtual components, altogether to constitute a whole "hybrid" architecture.

The whole set of tests, required by the IEC 61850 standards, can be executed on this hybrid architecture, which allows the evaluation of architectures, in the design phase, as well as existing architectures but which require off-line validations.

The preliminary tests of the approach are promising; the next stage will be the validation of the approach on an actual existing architecture.

ACKNOWLEDGMENT

We are thankful to OpNet Technologies, Inc. for their active support under OpNet University Program (OUP).

REFERENCES

[1] M. Haffar, J.M. Thiriet, E. Savary - Modeling of substation architecture implementing IEC 61850 protocol and solving interlocking problems - 7th IFAC International Conference on Fieldbuses & Networks in Industrial & Embedded systems, Toulouse, France (November 7-9, 2007), pp. 291-294.  
 [2] IEEE C37.115-2003, "IEEE Standard Test Method for Use in the Evaluation of Message Communications Between Intelligent Electron-

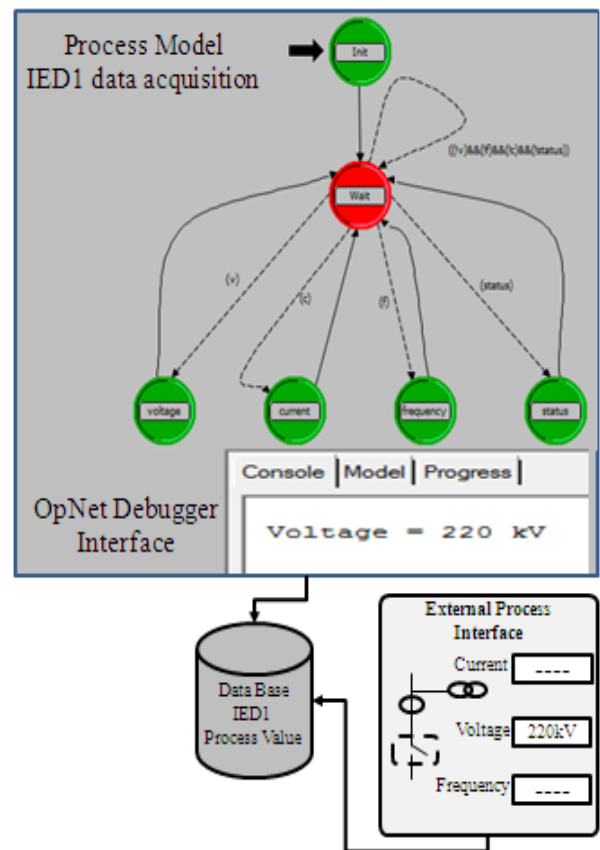


Fig. 9 Software in the loop package validation

ic Devices in an Integrated Substation Protection, Control, and Data Acquisition System," IEEE Power Engineering Society, New York, June 2004  
 [3] E. A. Udren, D. Dolezilek, "IEC61850: Role of Conformance Testing in Successful Integration"; KEMMA T&D and Schweitzer Engineering Laboratories 2006  
 [4] IEC; IEC61850 Communication Networks and Systems in substations, part 10: Conformance Testing (IEC61850-10), 2005; http://www.iec.ch  
 [5] J.Guo, W.Xiang, S.Wang ; "Reinforce Networking Theory with OPNET Simulation," Journal of Information Technology Education, MI, USA, 2007.  
 [6] C. Jiongcong, R.Yanming, G. Xinhua, J. Yangjun, "The research on Conformance Testing Platform of Numerical Substation," Elec. Dist., CIGED 2008, Decembre 2008  
 [7] R. Martinez, W. Wu, K. McNeill, "hardware and software-in-the-loop techniques using the opnet modeling tool for jtrs developmental testing," MILCOM, Monterey, October 2003.  
 [8] A.P. Apostolov, "Modeling Systems with Distributed Generators in IEC 61850," Power Sys. Conf, PSC '09. Clemson, SC, March 2009.  
 [9] A. Apostolov, B. Vandiver, "Functional Testing of IEC 61850 Based IEDs and Systems," Power System Conference and Exposition, Los Angeles, PES2004, October 2004