International Journal of Computer Applications (0975 – 8887)
Volume 128 – No.8, October 2015

A Survey on Generic Scada Simulators

Ahmad Almadhor
University of Denver

ABSTRACT

SCADA acronym for supervisory control and data acquisition, a computer system for gathering and analyzing real-time data. SCADA systems are used to monitor and control a plant or equipment in industries such as water and waste control, telecommunications, oil and gas refining, transportation, energy. As these systems monitor critical and industrial infrastructures, so evaluation of their execution or performance and security is crucial. They are complex systems passed on over wide domains, from now on their modeling and simulation is far from piddling. Really, consistently it requires the co-simulation of the processes directed, furthermore the network communication between components of SCADA. Selecting the best possible modeling and simulation tool is segregating, because the blend of domain specific simulators with network simulators while considering the basic piece of time synchronization, engages the plan of dependable diversion circumstances. We outline here in this research article the SCADA network structural design, evaluate the widespread network simulators distinctiveness and study the on-hand simulator realizations in multiple or manifold SCADA application realms.

Keywords

SCADA, Networks, Architecture, Simulators

1. INTRODUCTION

Supervisory control and data acquisition (SCADA) [A. Daneels et al][Z. Ma et al] have transform into the essential development for monitor and control of significant scale critical and industrial infrastructures in the midst of the latest decades. They are dependably used as a piece of oil and gas refineries and pipelines, water treatment and allotment, rail lines and electrical power generation and transmission. The word SCADA is frequently brought into play to delineate computerized control systems whose field devices are geologically spread, sometimes past the country edges. These field devices are joined with their control centers by method for Wide Area Networks (WANs) utilizing diverse protocols by employing wired or wireless channels. The SCADA systems regularly cover wide district and are comprised of different, habitually abundance components likewise, as communication modes between them. They are passed on over, and expected that would stay operational for an extensive timeframe giving high openness (availability). Thusly, they are really multifaceted while hoping to stick to stringent availability, munificence, extendibility and routinely security limitations. SCADA simulators are utilized to lend a hand with various those errands, comprising orchestrating/planning, resource optimization, security checks, and workforce get ready, liveliness to disaster circumstances and demand forecast. Legacy associations routinely incorporate non-standard architectures and tailored software's. Front line associations or deployments hold quickly to Industry rules and standards, regardless, in view of high necessities, even they may be exceedingly revamped. SCADA systems standardization and in particular of SCADA networks has in like manner helped the reusability of components for SCADA simulators. Towards this heading [J.S Dahmann et al] energizes the change of simulator environments, giving the nonexclusive structure to merge various simulation stages. Regardless, when laying out any simulator it is significant to consider where and how it will be utilized.

2. OVERVIEW OF SCADA

Since Supervisory control and data acquisition (SCADA) are control systems where availability is key essential, they routinely incorporate practically tight close control loops that allow the structure or system to work for endless time periods even without external joint effort. Distributed Control Systems (DCS) really, are tinier, close loop systems that cover a confined zone and topographically constrained methods not surpassing the breaking points of a foundation or installation. Distributed Control Systems are moreover used as a piece of industrial applications to screen and control passed on equipment without human intercession for its normal operation. For broad operations, Distributed Control System is functioning as a part of SCADA and is interconnected with it, thusly allowing manager coordinated effort. The field equipment is connected with the Distributed Control Systems control center through LAN, offering higher constancy and what's more modestly higher physical and computerized security stood out from a level SCADA structural design. In the first place of SCADA systems, they continue running on gave networks holding up simply prohibitive (proprietary) protocols with confined connectivity. Security was in light of physical region separation and likewise the offered by the inconclusive nature of shipper/vendor specific programming software's and hardware. Among other constrained limits, this reason versatility and interoperability issues. How-ever, most current gateway devices reinforce different standard protocols over IP and are frequently remote/wireless. Forefront SCADA systems by and large offer generous or vigorous communication utilizing diverse communication channels with fluctuating trustworthiness, throughput, and absence of movement traits. Ordered and fast control of multiple ranges thinks seriously about speedier and more correct reactions that alter the operation of the system. On the other hand, meanwhile the multifaceted way of the structure/system amplifies. Field devices, for instance, Remote Terminal units (RTUs) or Programmable Logic Controllers (PLCs) are connected with recognizing or sensing equipment and switch-boxes or valve actuators spread in the process field. The RTUs in remote territories gather data and send them by method for a communication link with the SCADA master station. The SCADA server arranges the data, trades alarms and events to the Human Machine Interface (HMI) and stores the assembled data in a gigantic database called historian. The historian logs and archives time-based methodology data allowing execution monitoring, example auditing and trend investigation. The HMI is utilized to give an interface to the operators. It indicates data to the operators and grants them to screen the state of the strategy and to correspond with the field devices giving information shapes, when an action is required.

Various HMIs may exist with contrasting access rights depending upon the necessities of differing customers. In case of corporate infrastructure layer (Fig 1) that takes in Enterprise Resource Planning (ERP) systems for operational management, production scheduling, business planning and logistics. Normally, the business management layer contains distinctive servers, has, network devices giving web services, for instance, web, FTP, and messages. Furthermore, this layer generally speaking supports remote customer access demonstrates all together allow far away customers to take a gander at the state of the SCADA system. Regardless of the way that this is not endorsed for security reasons, some affirmed and advantaged remote customers could participate with the SCADA control devices. Nevertheless, the corporate infrastructure layer is considered un-trusted as a result of its presentation to the web. Thusly, remote access should be restricted just in emergency circumstances. The correspondence or communication between the field devices and the control center is given by the control network. Obviously, SCADA networks have been committed networks employing restrictive protocols. That provoked complex sorts and systems with no sponsorship for interoperability. Numerous those prohibitive protocols exist. Things being what they are, during the time the industrial control associations started grasping general open standard protocols and after the augmentation of IP networks the example is to encapsulate SCADA packets into TCP/IP frames. The most no doubt understood industrial protocols are Modbus-TCP, Ethernet/IP, Profibus, DNP3 et cetera. In addition, to address interoperability through the creation and maintenance of non-selective open measures subtle elements, the [opcfoundation] added to an Application Programming Interface (API); the OPC protocol. OPC energizes the data trade between the present day control systems, the HMI, the understudy of history and the Enterprise Resource Planning (ERP) structures. More starting late, the stage free OPC UA protocol [S. Lehnhoff et al] was familiar all together with withdraw from the Microsoft COM based OPC classic. SCADA powerfully moves towards extensively valuable information propels, for instance, Ethernet and TCP/IP for both essential and non-separating trades/communications. In any case, while the use of essential protocols is seen as supportive and fiscally adroit, it revealed the fundamental operational methodology to threats starting from the outside world. A couple sorts of strikes reaching out from unapproved customer access (hacking) and spying to data catch and denial of services (DoE) attacks reveal SCADA systems in high peril. The best make preparations for these threats is to absolutely separate the network from the outer world. Regardless, this can't be totally done; therefore additional technique for redesigning security [K. et al] should be well thought-out. Toward directing these advanced perils, one frequently prescribed practice is to detach the SCADA and system control networks from the endeavor network and the web through the plan of firewalls, making differing zones of trust. Architectures that allow the communication between the un-trusted enterprise networks to the trusted SCADA network just by method for Demilitarized Zones (DMZ) give the best security game plan. It has been subsequent to a long time prior pushed to apply the standard of scarcest advantage which gives a customer or process only the base plan of rights totally expected to perform a task whilst deny everything else. Besides, when the architectures have a need of the association of diverse firewalls, it is significantly endorsed to draw on firewalls from various dealers to improve the security.

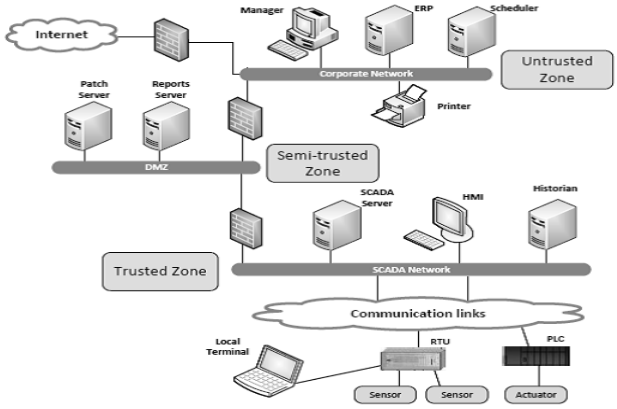

Fig 1: Architecture of SCADA [K. Mathioudakis et al]

3. COLLABORATION OF EMULATION AND SIMULATION

The guideline differentiation between a normal IT establishment and a SCADA structure is the operational congruity that a SCADA system must hold up. This infers that even the most secure, trusted and tried and true update can't be expeditiously joined without exhaustive testing in some bit of the authentic or real system. Any potential glitch that happens in the midst of the installation of novel software may meddle with the separating/critical operation system bringing on loss of openness/availability and accordingly immense mischief to the operation. Much more, as SCADA consolidated with charge and control structures/systems are brought into play for checking of major operations they can't be particularly utilized for diverse activities, for instance, patch management and software testing, advanced security testing, network execution evaluation or training. Regardless of the way that the acquisition of a full monotonous structure/system for having a tendency to such non-operational activities is in all probability the ideal game plan, it may not be the achievable. A SCADA system is contained a couple of units in diverse regions and that makes the plan of redundant equipment inconceivable or expense incapable. Considered this the exploitation of a trustworthy simulation milieu that adheres to all the SCADA necessities is the most reassuring way for watching out for the beforehand expressed dilemmas. Also, the cooperation of communication networks and the field specific systems, for instance, electric system parts would be clumsy to study without the aide of careful models and versatile milieu simulations. The examination of complex strategies which take in fused, discrete or reliable schedules oblige fitting simulation models and methods. In this perspective, power grid modernization tries call for successful simulation and generation instruments for hybrid structures. In addition, in power grid applications or more wide in wide range checking circumstances the use of present day communication advancements is seen as mandatory; in this way, the allocation of forefront network simulators is the principle conceivable way to deal with examination and evaluate these networks. Hence, it is essential to build up a simulation framework that will consider modeling and simulating the differing parts in diverse circumstances. A SCADA simulator should be made out of direct yet reusable parts and should reinforce extensibility and straightforward interconnection with other simulating and/or honest to goodness or real modules. Meanwhile, it should not display more unconventionality than required for the present workload. The best choice depends on upon the specific system the SCADA is controlling, the typical circumstances, the rate of changes in the system and their relative speed to that of network correspondences, furthermore the accuracy we have to get. As we portray in the going hand in hand with paragraphs a general structural design of a SCADA simulation environment is constituted from four different layers. In the base we get together the range specific models or genuine field devices if we target holding up hardware in the loop. In the second layer there is a totally delineated coordination module which is accountable for the interconnection and furthermore the fundamental time synchronization between the models and the network simulator. The late lies on the third layer while on top there is an interface that allows the customer to chip in with the made stage. Ordinarily the customer interface is united in the network simulator.

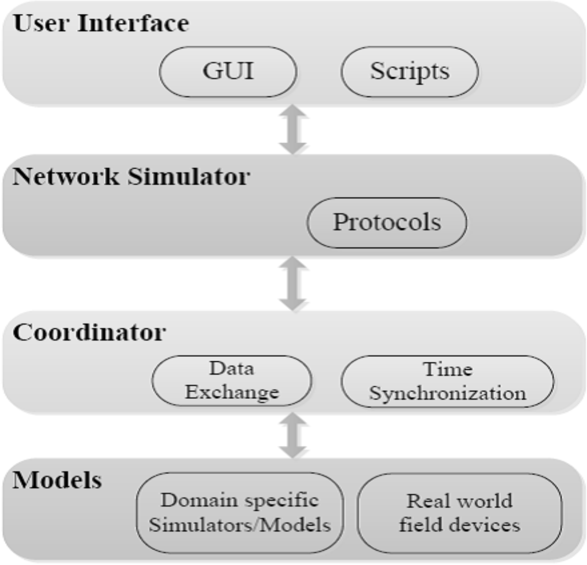

Figure 2: SCADA Simulation Environment (Design Structure) [K. Mathioudakis et al]

4. SIMULATORS

Adding to a SCADA simulator can be time serious and extravagant. Just because of the multifaceted way of the issue and the distinctive parts of a cutting edge control system, a single simulator is lacking to recreate or simulate the whole SCADA process. Neither one of the as stand-alone space specific simulation/simulation nor a stand-alone network simulation is tasteful to model a totally equipped and interconnected system. Accordingly, there is a huge investigation push to unite unmistakable territory specific and network simulators into co-simulation stages. Right when brining into play a simulator, the goal is to delineate in adequate unpretentious component the state of a system that is a collection of components [A.M Law et al]. It should recollect that this is not by any methods the main way it can go about and to be sure distinctive schedules or techniques incorporate attempting diverse things with the certified system, using a physical model of the system on a consistent game plan. A valid example, to reproduce network development we can choose to bring into play a clear connectivity system, unless sensible estimations for delay and latency are required, in which case a packet level network simulator would be all the more fitting. Simulating Reproducing a SCADA system incorporates showing at given levels of inconspicuous component the state of the SCADA components, the communications amidst them and the state of the controlled operation henceforth called environment. Making a strong simulator for these entire eventual radical, and also would convey inefficient results, since selecting the right level of unpretentious component for each of those depends on upon our necessities. To be perfectly honest, a couple of systems may have a bit of them not simulated,but imitated or partially executed using a physical model. As an outline, a simulator used for orchestrating future needs or approximating operational costs ought not detail normal operations on anomalous state. Then again, an simulation used to demo a particular capacity, or to train staff might truly have not completely executed the facets of the SCADA system that unite with workforce. Plus, when arranging a simulator, we should mull over how the environments states work together with each other. Consider as a case the cases of a SCADA for an electric grid, versus that of one for checking a game plan of dykes. In the first case, any alteration in the electric load will impact the system in nano, little scale, or miliseconds depending upon the marvel. In the second, an irregularity may be seen a couple of days preceding the dyke truly breaks. This suggests that a simulator of environment may in the first case need to have a nanosecond inconspicuous component, while in the second minutes or hours. Instantly consider a normal communication network where events have milisecond compass. Going along with it to environment simulator may not look good. It may be perfect to run the two simulations separate and give a connectivity matrix, or a plan of possible system states and their Probability Distribution Functions (PDFs). Displayed by the US Department of Defense, HLA [J.S Dahmann et al] was made to ensure the interoperability and reusability of models and aspects of simulation. It is a standard procedure to consider joining specific simulations into a solidified co-simulation stage. Its point is to bestow a structure, which will enable the reuse of a couple of capacities successfully available in distinctive simulations, concentrating on cost and time diminish. A computer simulation or a manned simulator can go about as a associate, which is identified with as object. In addition, the Runtime Infrastructure (RTI) goes about as the distributed operating system of the association/federation. It is a collection of services that sponsorship the relationship between assorted unites. Its genuine service is seen as the time management which goal is to ensure the time synchronization among all brings together. A couple business and open source RTIs are available. Finally, the runtime interface specific portrays how the relationship amidst unites and the RTI is coordinated. Each individual simulator ought to fit in with HLA's standards and an interface determination to be joined with distinctive unites/federate. Also, each unites or federates or alliance document should be clearly open and conform to the standard open model template. Tragically, it may be complex to alter formally existing generations to take after HLA's determination. But there is a credibility to add a wrapper to these simulators, it is ambling due to the amount of modifications and expands that should be finished with a particular deciding objective to acclimate to the HLA.

4.1. Simulators

Network simulators when all is said in done endeavor to duplicate and model veritable networks. The cost of a complete execution of a present day communication network just for testing and looking at is prohibitive appeared differently in relation to the headway of a simulation framework. In spite of the way that network simulators are not faultless, they can give a vital comprehension into the attempted/tested network, and how changes will impact its operation.

4.1.1. Network Simulator 2 (NS2)

The Network Simulator 2 is an open source event driven simulator expected for investigation in computer communication networks. It can reenact or simulate existing network protocols, for instance, TCP, UDP, coordinating and multicast protocols over both wired and remote/wireless networks. It allows the arrangement of diverse communication circumstances employing explicit protocols and simulating the behavior of these protocols under varying conditions. NS2 utilizes C++ to describe the simulation objects and Object-oriented Tool Command Language (OTcl) to schedule the discrete events and to set up the simulations. NS2 is particularly vital to industrial simulations since there is an example to encapsulate prohibitive protocols packets into TCP operational over Ethernet networks.

4.1.2. Network Simulator 3 (NS3)

This Simulator has procured thoughts and realizations from a couple open source simulators and it is seen as that will legitimately supplant NS2. Then again, NS3 is not a redesignd version of NS2 and it is not in converse immaculate with NS2. It is expected to improve flexibility and measured quality and is formed is C++ however offers similarly a Python scripting interface. Furthermore, it reinforces virtualization, software and testbed blend, and it focuses its respect for legitimacy supporting key interfaces, for instance, connections (sockets) and network devices, diverse interfaces per node and addresses usage.

4.1.3. OPNET:

This simulator is a gadget to imitate the behavior and execution of any kind of network. It is in light of discrete system event instrument which simulate the behavior of system by showing the events of the circumstances that the customer has set up. Its principal segment is that it gives distinctive honest to goodness network setup or configuration limits that make the simulation environment close to reality. It in like manner gives graphical editors (GUI interface) and a comprehensive library of network protocols and models. It uses object-oriented programming techniques to make the mapping from the graphical layout to the use of the bonafide or real time systems. Finally, it allows the change of customer's own networks, protocols and format of packets by giving the vital programming credentials and tools.

4.1.4. OMNeT++

It is in like manner a discrete event simulator altered in C++. It is a fragment or component based structural design and comprises modules that interact with each other utilizing message passing. The portions tweaked in C++ can similarly be combined in a pecking or hierarchy request of levels allowing the making of complex simulation parts. It also gives a GUI interface and in view of its modular structure design, the simulation kernel can be embedded into an extensive variety of unmistakable customer’s applications. Furthermore, by giving modules developments (plug-inns), it allows the change of the default behavior of the simulation engine.

4.2 Related simulator frameworks of SCADA*:*

The joining of unmistakable simulation frameworks for heterogeneous systems is customary in examination. Regardless, simulating SCADA systems and networks utilizing open source devices is by and large novel. The reason behind that is a direct result of the need of genuine modeling instruments/tools, the communication traits must be reworked and simulations must be considering essential postulations that may impact the last result. The [W Li et al] make use of the OPNET limits for simulating the communication network and they bring into play the Virtual Test Bed (VTB) for component simulation of the power system. The VTB is a software tool that used for power devices and power systems. For the data exchange between the two simulators, a co-simulation coordinator was made which moreover is accountable for the time synchronization. The coordinator gives a customer interface and through it the customer can set the overall time step. The general goal of this effort is to study and separate the communication network of the power system and to check the quality of the power system as a segment of the network execution. Their multiplication results show enormous issues in delay and packet dropping when they dissected the inspecting period and the data rates of communication. [C.Queiroz et al] Propose a SCADA simulation gadget (SCADASim) that sponsorships the fuse of external devices and applications. Their objective is to examine the effect of ambushes in real devices and applications by using simulating milieus. Strikes that are maintained comprise denial of service (DoE), man in the middle, listening in, and satirizing or spoofing. Moreover, they plan to amass an extensible, versatile and specific SCADA simulation framework with in the meantime compromise of outside portions and devices. They bring into play the OMNeT++ to simulate the network and they abuse the connection based mix of OMNeT++ to allow the compromise of the outside devices. Regardless, with a particular final objective to handle the issue that just connection based protocols are maintained, they pass on entryways. These entrances go about as communication ports that execute protocols for talking with external parts. The synchronization between the OMNeT++ and the outside devices is dealt with by the SSScheduler module, which is responsible for synchronizing the relating clocks. Finally, they pass on malicious strikes circumstances to evaluate the framework, and they display how the ambushes are affecting the strategy of utilize authentic requests. The [W. Chunlei et al] propose a reference structural design. It comprises a couple layers and parts that identify with the enterprise network, the OPC server and client, the SCADA protocols analyzer, the RTUs, the field sensors and actuators and the cutting edge establishment. Their model implementation concentrates on the security examination and assessment of SCADA systems. It is extensible and flexible and it is basically in perspective of NS2. Additionally, in order to allow the joining with certifiable networks desires they mishandle the capacities of emulating component of NS2. The later can implant development from the simulator into a live network and to simulate a looked for network between veritable applications continuously. For the simulation network they use real PLC/RTUs and sensors/actuators, and what's more industrial and open source systems for OPC client/server execution. Finally, for the appraisal of the simulation network they executed attack circumstances that exchange off the security of SCADA system and they made techniques to to examine and survey the effect of these assaults on the network. Regardless, there is no much information available with respect to the aftereffect of the trials. In [K. Hopkinson et al] the authors fuse various investigation and commercial of-the-shelf (COTS) structures to gather an administrators based simulation network for the electric power grid. In perspective of HLA framework [J.S Dahmann et al] they made a merged simulation system which exploits the capacities of a couple of the individual simulators; a mix of the PSCAD (Power System Computer Aided Design) and EMTDC (Electromagnetic Transients including Direct Current) [James Nutaro et al] where the first offers a graphical interface and the later is an electric power simulator, the PSLF (Positive Sequence Load Flow) for electromechanical transient simulations, used also as a piece of elecro-mechanical security circumstances, and the NS2 for the simulation of network communication. Each one of these simulators changes in accordance with the HLA's rules, interface subtle element, and documentations models. Additionally, the interface between the individual simulators is performed by a central part, the RTI. The RTI is accountable for packet routing and the time-wandered synchronization between the units or federates. This synchronization strategy is the most frequently utilized when various simulators are taking part. A preset simulation time must be come to by all the parts before a data exchange between them is allowed. Beside the distinctive simulators the makers added to the AgentHQ module which goes about as a mediator or proxy when agents need to collaborate with the unites. Through it, it is possible to arranged and get the power system values and to exchange data. Finally, they show different exploratory results exhibiting the upsides and drawbacks of an agent based remarkable security arrangements, while they don't oversee concerns of security. In [Hua Lin et al] the makers charged by [K. Hopkinson et al] and [James Nutaro et al], developed a co-simulation framework concentrating on sharp system applications. Their dedication was the facilitating of the synchronization overhead issue that could realize data jumble between the simulation sections, by introducing asynchronous practices. Their key focus is to clear the gathering goofs exhibited by the synchronization network. Subsequently they run the diversion comprehensive in a discrete event driven route rather than using relentless time simulation schedules to simulate a discrete event system. An overall scheduler is responsible for the synchronization while the differing simulators have the same timetable. For the utilization they impact the limits of the PSLF simulator for power system dynamic simulation and the NS2 for the communication network simulation. Additionally, an authorities based exchange affirmation arrangement is investigated within this framework. Each relay has its own master and slave agent which go about as interface for data exchange. Finally, for the approbation they essentially take a gander nearby off or relay dissatisfactions without overseeing the concerns or problems of security. [P.Palensky et al] Plot the simulation platform DAVIC (Distributed Automation via Implicit Channels) which is in perspective of OMNeT++. The objective of this use lies on the making of speedy and strong simulation stage to be used for the appraisal of unmistakable energy management algorithms, for instance, peak interest/demand. Interestingly, they didn't employ of-the-shelf territory specific simulators, notwithstanding they used synthetic load profiles which are the reference use profiles, and their own specific considers so to model the demand. That saved them from synchronization challenges however obliged the convenience of the platform. The objective in [Rohan Chabukswar, et al] is to demonstrate the use of C2WindTunnel [O.Anaya-Lara et al] [K. E Roth et al] platform with the arrangement to simulate DDOS-like ambushes on a plant and its control system and notwithstanding inspect the results for particular routers. The C2WindTunnel platform is in perspective of HLA and it was expected to support the progression of considerable scale simulations. It uses the Generic Modeling Environment [G.Hemingway et al] and uses model-based design networks and graphical interface to allow integration of diverse simulation engines. The inventors use the NetworkSim, which is in perspective of OMNeT++ to simulate the communication protocols and the Simulink to model the field specific strategies. Also, they developed a Simulink ability to synchronize the model with the Run-Time Infrastructure granting the Simulink to progress exactly when the RTI licenses it. They bring into play timed-stepped synchronization, while keeping the time-size low in order to minimize event timing goofs introduced by exchanging events amidst Simulink and HLA. Another work that is in perspective of the C2WindTunnel is shown in [Himanshu Neema et al]. This work follows the troubles experienced in setting up simulation platforms that are used to duplicate the command and control circumstances. As most of the past works the makers used OMNeT++ and as a piece of solicitation to secure the synchronization between the OMNeT++ and the RTI they made, which called the NetworkSim scheduler. For their experimentation they realized Unmanned Aerial Vehicles (UAVs) models using the Simulink X4 with the objective to test the mission execution when a network attack is happened. Especially, they focused on DDOS attacks depicting the outcomes on the way of got data and the correspondence between the charge and control center and the UAV. A hybrid simulation tool was developed for modeling the correspondences and the control of the electric system [K. Mathioudakis et al][James Nutaro et al]. The vital objective of the makers is to spare the hybrid simulation definition by using both discrete and continuous systems. The communication processes are exhibited using NS2 and the discrete continuous processes are executed using ADEVS (A Discrete EVent Simulator). ADEVS is a C++ library for building discrete event simulators in perspective of parallel DEVS and Dynamic DEVS formalism. The ADEVS software is epitomized in a NS2 TclObject and it is summoned by the NS2 when required. In the experimentation stage they exhibit how the communication network impacts the solicitation of load shedding furthermore how the information transmission and the dormancy impact the controller behavior. Most of the software that was utilized by the experts is free or if nothing else an academic grant is available. Things being what they are, a couple devices were fabricated concentrating on mechanical or business applications, thusly the obtaining of a license is seen as fundamental.

5. SUMMARY

loads of defies are faced when building up an assorted simulation platform for SCADA systems. Disregarding the way that the framework of HLA bestows the key APIs to diminish the multifaceted way of making simulations, there are still concerns that must be taken care of in the midst of the progression stage. Three levels of integration are regularly requisite in order to stick together a simulation framework to a general simulation milieu; the API level, the level of collaborations or interactions, and the level of model semantics. The begin with offers some principal services, for instance, management functionality and message passing. The second and most basic manage the time synchronization and coordination among the erratic command and control simulation platforms, whereas the third is genuinely optional and depends on upon the objective of the simulation setting. But vast bits of the self simulation frameworks give a rate of the obliged services and are great with the HLA reference structural design; they don't have a comprehensive coordination and coordination approach among diverse stages/platforms. Reducing the exertion and time mandatory for simulation progression can be done through joining of multiple suitable field specific instruments, which will provoke more adaptable SCADA simulation circumstances. Completing up, the combination of viably passed on and sanction far reaching scale field specific models is a key for the competent hybrid systems progression.

6. REFERENCES

[1] ”Rohan Chabukswar, et al..”,, “Simulation of network attacks on scada systems,” in Proceedings of the First Secure Control Systems Workshop, Cyberphysical Systems Week, Stockholm, Sweden, 2010.

[2] ”J.S Dahmann et al..”,, “The department of defense high level architecture,” in Proceedings of the 29th conference on Winter simulation. IEEE Computer Society, 1997, pp. 142–149.

[3] ”Himanshu Neema et al..”,, “Rapid synthesis of multi-model simulations for computational experiments in c2,” 2009.

[4] ”W. Chunlei et al..”,, “A simulation environment for scada security analysis and assessment,” in Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference on. IEEE, 2010, vol. 1, pp. 342–347.

[5] “http://www.opcfoundation.org,” last access: July 2013.

[6] ”K. Hopkinson et al..”,, “Epochs: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components,” IEEE Transactions on Power Systems, vol. 21, no. 2, pp. 548–558, 2006.

[7] ”S. Lehnhoff et al..”,, “Opc unified architecture: A service-oriented architecture for smart grids,” in Software Engineering for the Smart Grid (SE4SG), 2012 International Workshop on. IEEE, 2012, pp. 1–7.

[8] ”O.Anaya-Lara et al..”,, “Modeling and analysis of custom power systems by pscad/emtdc,” Power Delivery, IEEE Transactions on, vol. 17, no. 1, pp. 266–272, 2002.

[9] ”G.Hemingway et al..”,, “Rapid synthesis of high-level architecture-based heterogeneous simulation: a model-based integration approach,” Simulation, vol. 88, no. 2, pp. 217–232, 2012.

[10] ”W Li et al..”,, “Vpnet: A co-simulation framework for analyzing communication channel effects on power systems,” in Electric Ship Technologies Symposium (ESTS), 2011 IEEE. IEEE, 2011, pp. 143–149.

[11] ”A. Daneels et al..”, “What is scada,” in International Conference on Accelerator and Large Experimental Physics Control Systems, 1999, pp. 339–343.

[12] ”Z. Ma et al..”,, “Towards a layered architectural view for security analysis in scada systems,” arXiv preprint arXiv:1211.3908, 2012.

[13] ”C.Queiroz et al..”,, “Scadasim - a frame-work for building scada simulations,” Smart Grid, IEEE Transactions on, vol. 2, no. 4, pp. 589–597, 2011.

[14] ”Hua Lin et al..”,, “Power system and communication network co-simulation for smart grid applications,” in Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES. IEEE, 2011, pp. 1–6.

[15] ”K. et al..”,, “Guide to industrial control systems (ics) security,” NIST Special Publication, vol. 800, pp. 82, 2008.

[16] ”P.Palensky et al..”,, “A simulation platform for distributed energy optimization algorithms,” in Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on. IEEE, 2008, pp. 342–347.

[17] ”James Nutaro et al..”,, “Integrated hybrid-simulation of electric power and communications systems,” in Power Engineering Society General Meeting, 2007. IEEE. IEEE, 2007, pp. 1–8.

[18] ”K. E Roth et al..”,, “Command & control wind tunnel integration and overview,” in Proceedings of the 2009 SISO European Simulation Interoperability Workshop. Society for Modeling & Simulation International, 2009, pp. 45–51.

[19] ” K. Mathioudakis et al..”,, Towards generic SCADA simulators: A survey of existing multi-purpose co-simulation platforms, best practices and use-cases, AGT Group (R&D) GmbH, Hilpertstrasse 35, 64295 Darmstadt, Germany

[20] ”A.Ledeczi et al..”,, “The generic modeling environment,” in Workshop on Intelligent Signal Processing, Budapest, Hungary, 2001, vol. 17.

[21] ”James Nutaro et al..”,, “Integrated modeling of the electric grid, communications, and control,” International Journal of Energy Sector Management, vol. 2, no. 3, pp. 420–438, 2008.

[22] ”A.M Law et al..”,, “David: Simulation modeling and analysis,” Mac Graw Hill, Boston, Burr Ridge, ua, 2000.