Research on the Integrated Attack-Defense Simulation Platform Architecture of the large-scale oil and gas gather-transferring SCADA system

Jie Li[1, a], Xiedong Cao [2, b] ,Li Yang [3, c]

[1] School of Electrical Engineering and Information ,Southwest Petroleum University, Chengdu, 610500, P.R. China

[2] School of Electrical Engineering and Information ,Southwest Petroleum University, Chengdu, 610500, P.R. China

[3] School of Computer Science,Southwest Petroleum University, Chengdu, 610500, P.R. China

[a]email: googleli757@163.com, [b]email:cowyco@126.com, [b]email:scncyl@126.com

Keywords: SCADA; Dynamic Simulation; HYSYS;OPNET

Abstract. In this paper,We analyse the difficulty of the large-scale oil and gas gather-transferring SCADA system process simulation and dynamic simulation and give a new simulation architecture for the large-scale oil and gas gather-transferring SCADA system, which bases on middleware technology and sets dynamic simulation, fault diagnosis, safety assessment of network attack and defens and semi-physical simulation platform in one. By integrating the HYSYS simulation platform to realize network physical modeling, solving process simulation, dynamic simulation, and the evaluation of the effect of offensive and defensive problems such as;Using network simulation technology of large-scale network running status of the simulation, to study the influence of network attack of large-scale oil and gas pipeline network.Combining semi-physical simulation method to simulate the actual station, studies the influence of different offensive and defensive method of business process.This study to explore security defense algorithm validation method have positive significance.

Introduction

The fusion of industrialization and informatization brings enormous security challenge to ICS (Industrial Control System). Viruses, trojans and other threats began to spread to the industrial control system, information security problem increasingly prominent. Different from that of traditional information system,the object of ICS is to provide corresponding security protective measures while ensuring its high usability[1].

Foreign scholars devoted to build real test environment SCADA system, simulated attacks, analysised the security of SCADA system through simulation and modeling[2]. For example, since 2008, the U.S. department of energy (doe), by combining its six subordinate national laboratory technical force,such as Idaho, began building SCADA test platform plan (2008-2013), Canada Wurldtech Achilles test tool using vulnerability scanning and fuzzy test method, test equipment in industrial control system and software security problems.

However, People who want to clone a complete set of oil and gas gather-transferring SCADA system ,will face huge investment.On the other hand, Developing and testing information security products directly in The real production environment need to take a great risk.

Therefore, in this paper, we propose a new simulation method for the large-scale oil and gas gather-transferring SCADA system, it can use of a small amount of resources for researchers to construct a general integrated support environment, real-time distributed simulation test ,this method can be applied to web-based/SCADA information based on host defense system demonstration, development, testing, validation, assessment and training and so on each link.

Related Work

This study is based on the following work :

Law AM, who proposed the system dynamic simulation model of seven yuan group, $S = (T, X, \Omega, Q, Y, \delta, \lambda)$,Where:T for time base, describe the system change of time coordinate, T as an integer becomes discrete time systems, T for real number becomes continuous time systems.X for the input set, on behalf of the external environment on the system. Usually X is defined as an Rn, among them, the X represents n values of input variables. Ω Set for the input segment, is used to describe a certain interval between input mode, is a subset of the (X, T).Q for internal state set, is the core of the system internal structure modeling. δ As the state transition function, defined within the system state is how to change, it is a map, namely: $\delta : Q \times \Omega \to Q$, the meaning is: if the system is in the state of q in t0 time, and exert an input $\omega : < t0, t1 > \to X$, so $\delta(q, \omega)$ indicates the system is in t1 status.Y for the output set. System through its effects on the environment. λ For the output function, it is a mapping $\lambda : Q \times Y \times T \to Y$: output function is given a set of output section ,and then the system dynamic model is divided into continuous-time and discrete-time model [3]. Transfer equation, Bo Yi, Yang Yang, who build oil and gas pipelines steady-state simulation model and dynamic simulation and optimization model for the system to achieve a computer-based model of state pipe network model of discrete time dynamic simulation [4-5].In 2000, Lei Y, Wu CG et al build a network simulation environment and the virtual device model, the network business model [6-7], Xiang Y, Wu XH limited resources and other proposed use of the laboratory simulation of real-world computer network attack methods [8-9].

SYSTEM ARCHITECTURE

I Map relations of SCADA systeminput/output data

In real system, the I/O point set of the field PLC stations and the system input set X and output set Y is in a injective relation, namely $f : I \cup O \to X \cup Y$, functions f correlations with acquisition frequency, network status and so on.System input point set I uplink data set (or data collection data sets, such as temperature, pressure, flow rate, etc.), the output point set O constitute system downstream data set (or control signal set). In hardware-in-the-loop simulation system ,we set up small-scale DCS network environment (no live-fire equipment, such as pipeline, valve), the system input/output sets can be calculatied in process simulation software HYSYS, again through the signal generation system/control reverse mapping to the I/O command set, so its mathematical description form for $h : X \cup Y \to I \cup O$, functions of h is related with response time, network status and so on. Virtual node is used to represent SCADA control node in the network system, the nodes can be a PLC or RTU, whereas virtual node set can be said more yard or upper PC, as shown in Figure 1. In the simulation system, attacking virtual node or node set simulatie the situation in which local area network (LAN) and even the area of network are attacked in the real system, It's mathematical description: $g_v : V_{node} \to \{x_d \mid x_d \text{ in tgt arc}\}$, g_v is a functions which is related to virtual node/collection operation state variables , x_d is the disturbance on the x.

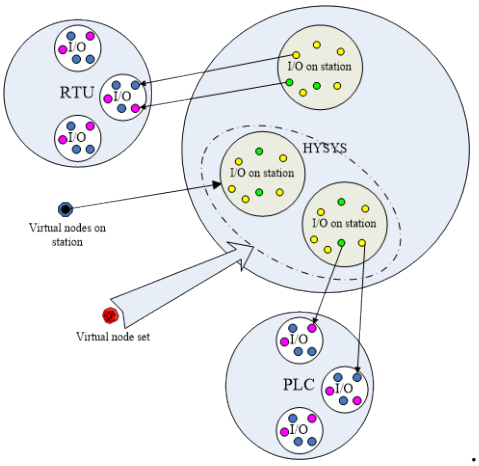

Figure 1. The relationship between the system input/output set and I/O

II Fundamental architecture of simulation platform

Integrated simulation platform is a three layer structure system,it is composed of the simulation application system layer, platform operation support middleware layer and Attack and defense walkthrough layer as shown in Figure 2.

Among them, the simulation application system layer have the integration of business process simulation software HYSYS and management tool, by HYSYS we can establish the station P-F network model and pipe network model, platform management tools mainly complete system initialization parameter setting, simulation network general control center and data statistical analysis, etc;

Platform operation support middleware layer is a core control for the operation of the platform and data interactive hub, simulation middleware libraries realize the interactions with the data of the other two layers, See Part III platform specific data process; In Attack and defense walkthrough layer by OPNET, we can build large-scale SCADA network layered structure model, simulate the network running status, and integration of all kinds of network attack and defense tools, support the attack plan, offensive and defensive modeling and simulation scenarios, Attack and defense walkthrough layer contain DCS system at the same time, it is because the industrial control system is different from general computer network system, studies its information security needs for different manufacturers DCS system security vulnerabilities.

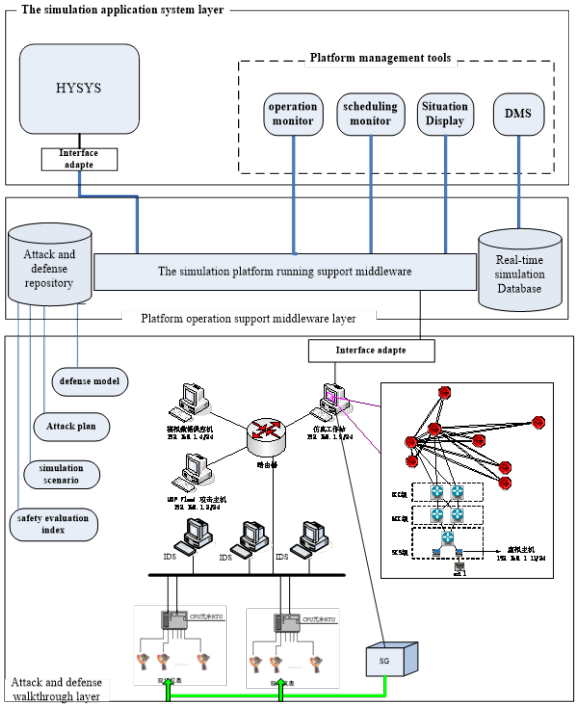

Figure 2. System architecture

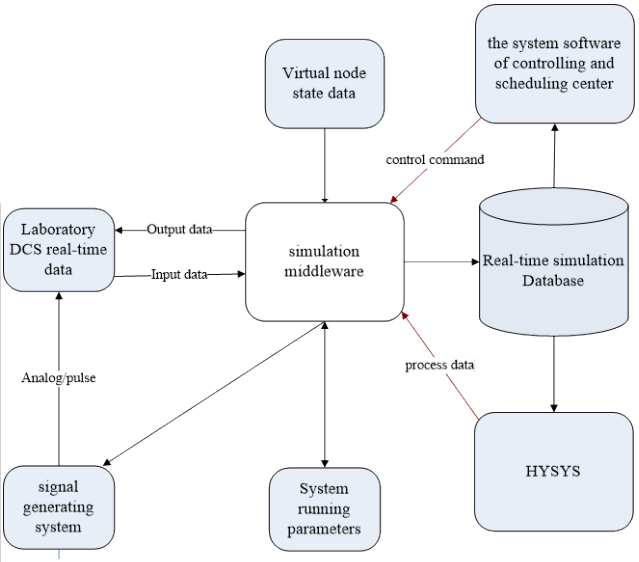

Figure3. System data flow

III System data flow

System running entrance initial parameters are combined with HYSYS dynamic process data by Simulation middleware. They have contributed towards the normal production data flow of simulation system, then transmitted to the real-time simulation database, real-time simulation database not only provide the input data set for oil and gas gathering and transferring dynamic process simulation software HYSYS through dynamically linked methods, as well as real-time data storage HYSYS dynamic simulation process data, all such data dispatching center monitoring system of data source, as shown in Figure3.

System running entrance initial parameters are combined with HYSYS dynamic process data by Simulation middleware. They have contributed towards the normal production data flow of simulation system, then transmitted to the real-time simulation database, real-time simulation database not only provide the input data set for oil and gas gathering and transferring dynamic process simulation software HYSYS through dynamically linked methods, as well as real-time data storage HYSYS dynamic simulation process data, all such data dispatching center monitoring system of data source, as shown.

At the same time, Dispatching center's control signals transfer into the real-time simulation database through the simulation middleware. if the control signals are corresponding to I/O set of the laboratory DCS system, also need to further transfer to them. For synchronous laboratory sensors collect data at the same time, need to transform HYSYS dynamic simulation process data through the signal generator for electricity signal, and through the laboratorial DCS system to upload the middleware by comparing calculation result with HYSYS,which can be used to judge equipment failure, communication interrupt or hijacking attack.

To see this platform can not only simulate the data uplink channel, at the same time also can simulate data downlink control channel.

On the other hand, the simulation middleware can also adjustment data sending frequency, superposition disturbance, etc.according to the virtual node dynamic real-time running state, system running parameters.

Test results

We assume an attacker to launch middle attack or attacks against virtual flood oil station, then observed the vessel pressure, throttle pressure changes.

Hardware configuration, we use 3 PCS (OS: Windows xp sp3, each running process of the virtual machine) and two RTU (each containing 32 ~ 40 I/O point) and the system structures, station DCS system, the signal between RTU and PC using MODBUS RTU communication protocol.One database server (OS: Windows server 2003 DB: SQL server2005), one simulation server (Windows 7 ultimate) installation configuration HYSYS2006, opnet 14.5 and run middleware, 1 and 1 switch attack hosts.

Experiment 1: under the normal production of the dynamic pressure in the separator V - 101 about 164 kPa, throttle valve opening VLV - 103 35%, middle attack by taking RTU first place machine, the communication protocol between the fake PC control command changes of the opening of the throttle valve VLV - 103 was 80%, as shown in figure5, separator internal pressure, rose to 189.5 kPa pressure fall at the same time the throttle VLV - 105 kPa from 16 to 39.54 kPa.

Experiment 2: attack of the host IP address is 192.168.1.4, supply machine IP Settings for 192.168.1.6 simulated data, the simulation workstation (192.168.1.8) on OPNET running in a virtual host (192.168.1.12) is attacked host.In the simulated data supply machine set the data interval to 1000 ms, set up to collect statistics on the simulation workstation.

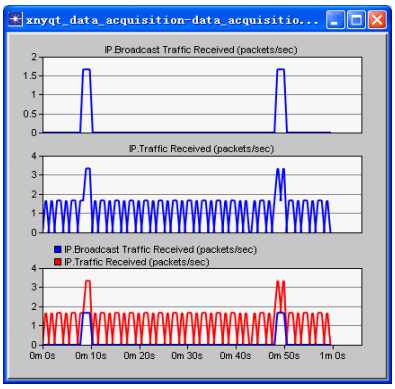

Figure 4. Normally receive IP business

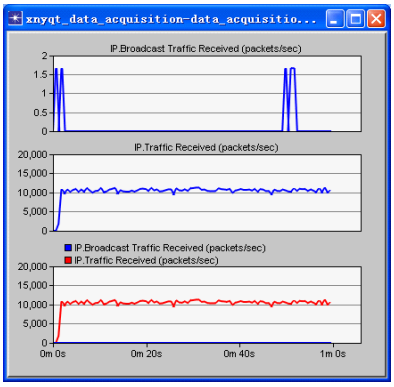

Figure 5. After being attacked

As shown in Figure4,5 can be seen after the flood attacks of virtual nodes, a significant change in virtual node IP data service, at the same time,the I/O set of the virtual nodes refresh rate becomes slow on surveillance images.

Conclusion

In this paper, we studied the simulation method of the large-scale oil and gas gather-transferring SCADA system respectively from the business model, network model, the relationship between the input/output data aspects such as the theoretical basis of the simulation is analyzed, design the hardware-in-the-loop simulation platform integration system structure and data flow, and experimental verification. Simulation experiment shows that the system can not only inside the yard small-scale network/host defense effect, at the same time, due to the introduction of virtual node based on virtual node/set, can simulate for multiple station SCADA networks and even the whole offensive and defensive posture; For this system, on the other hand, offensive and defensive effect is ultimately reflected in the business model, therefore, can be more realistic assessment of real system damage. This system can be widely used in business training, system testing, network optimization, the vulnerability assessment, etc.

Acknowledgement

In this paper, the research was sponsored by National Natural Science Foundation Project (Grant No. 61175122).

References

[1] Wang S.L, Yin Y.H, Security Protection of Industrial Control System. Communications Technology.2014(2) pp.205~209

[2] Wang.M. Industrial control system, information security testing and protection technology trends. Automation Panorama.68-71(2014.9).

[3] Law A M,Kelton W D.Simulation Modeling and Analysis.3rd ed.New York;McGrawHill,2000

[4] Bo Y. Optimal Analysis and Emulation of Natural Gas PIPe NetWork in west Sichuan. SWPU, 2004.

[5] Yang Y. The Study of Dynamic Simulation of Operation Conditions and Operation Optimization of Yonghuning Oil Pipeline.China University of Petroleum, 2009 .

[6] Lei Y， Wang X G.Computer network simulation method and tool].Journal on Communications，2001，22(9)：84-90.

[7] Wu C G.Emulation Technique.Beijin：Kluwer Academic Publishers，2000.

[8] Xiang Y X,Xiang X X.Application of method based on hypothesized target in network attack and defense experimental teaching .Computer Engineering and Design，2009 30(4) pp.855-857.

[9] Wu X H.Design and Implementation of Simulation Environment of Network Attacking and Defence.Xidian University，2005.