International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Review on PLC SCADA Based Automated System Control Applications and Challenges

Pooja Rai
Electrical Dept
MMMUT, India
pooja1307rai@gmail.com

Dr. Awdhesh Kumar
Electrical Dept
MMMUT, India

Abstract: Application of PLC SCADA in industrial plants is getting very common with the advancement of automation and sensor applications. Due to high rate of increase in demand with high quality and precision all the conventional control systems are being replaced by automated supervised control system. Thermal power plants are the example of very large systems which are based on the PLC and SCADA system. Not only the large system but small plants in local operations are also using PLC SCADA based control in temperature, pressure etc. This paper presents the review on the PLC SCADA systems history, development and security. This review is helpful is understanding the present applications of automation in various industrial systems.

Keyword: PLC, SCADA, Power Plant, Automation

1. Introduction:

In thermal power plant the demand for higher reliability & efficiency is increasing. Power plant requires continuous inspection & monitoring after regular intervals. There may be chances of errors while measuring at various stages by human workers. In order to increase reliability the automation is needed so that overall efficiency of power plant gets improved. The automation is developed by using PLC & SCADA which reduces the errors caused by human workers .PLC is programmable logic control. It is used for implementing various function such as sequencing, timing, counting, logic, mathematic control through analog and digital input output modules. In order to store the programme in PLC it must be interfaced to computer via interfacing unit. The programmed can be implemented through various languages. In this paper ladder logic is used for programming .SCADA system is used to supervise a complete process. The output of different sensors is given to the PLC which takes necessary action to control the parameter. SCADA system consist of subsystem such as human machine interface, remote terminal unit, and programmable logic control and communication cable. The alarm system is also provided to inform the operator. SCADA is used to monitor water level, temperature, pressure using different sensors and corresponding output is given to the PLC. For controlling these parameter. In coal conveyer belt the belt tear up, overloading and moisture content is sense by different sensors. The sensor used are IR sensor, temperature sensor, and humidity sensor.

Critical Infrastructures (CI) are often described as the infrastructures which provide essential services and serves as the foundation for any nation's security, economy, and healthcare systems. Cyber-Physical Systems (CPS)/ Internet of Things (IoT), are supplementing traditional CI with data-rich operations. The list of sectors under critical infrastructure varies from country to country. It generally includes sectors like agriculture, healthcare, nuclear reactor, transportation, energy sector, civil and chemical engineering, water plants, research etc. as depicted in Fig. 1. Supervisory Control and Data Acquisition (SCADA) systems, an Industrial Control Systems(ICS), have a pivotal role in managing and controlling of the CI. SCADA systems control and monitor geographically distributed assets. Historically, SCADA frameworks were limited to power transmission, gas conveyance, and water appropriation control frameworks. Advancements in technology have led to SCADA being deployed in steel making, chemical processing industries, telecommunications, experimental and manufacturing facilities [1]. With Industries 4.0 / Industrial Internet of Things (IIoT) evolution, modern SCADA systems have adopted CPS/ IoT, cloud technology, big data analytics, Artificial intelligence (AI) and machine learning. Integration of these technologies has significantly improved interoperability, ease the maintenance and decreased the infrastructure cost. Therefore, leading to a near real-time environment. SCADA systems improve the efficiency of the operation of the industrial critical system as well as provide better protection to the utilised equipment. Moreover, it improves the productivity of the personnel. SCADA frameworks give valid identification and prompt alert warning to the observing stations by using an attested monitoring stage, advanced communications, and state-of-the-art sensors. SCADA systems were designed to work in a standalone way and relied on air-gapped networks and proprietary protocols for securing the system. Therefore, initial designs of SCADA never incorporated security features [2, 3]. However in recent years, due to the expansion of business and need of central monitoring of distributed software, SCADA systems have evolved into sophisticated, complex open systems, connected to the Internet using advanced technology. Associating SCADA system to the web has helped numerous SCADA systems to work from topographically inaccessible areas. However, this has lead the SCADA system more vulnerable for attackers to target from anywhere in the world [4].

The modernisation of the SCADA system, standardisation of communication protocols and growing interconnectivity have drastically increased the cyber-attacks on SCADA system over the years. These type of attacks are becoming more sophisticated to commit the more traditional cyber espionage and sabotage in addition to cyber crimes. The smooth and genuine operation of SCADA framework is one of the key concern for the enterprises, because the outcome of break down of SCADA system may range from financial misfortune to natural harm to loss of human life [5]. A cyber-attack on a nuclear plant will have a global impact. Moreover, the security spillage in small networks can lead to a loss of services and financial loss to the utility company.

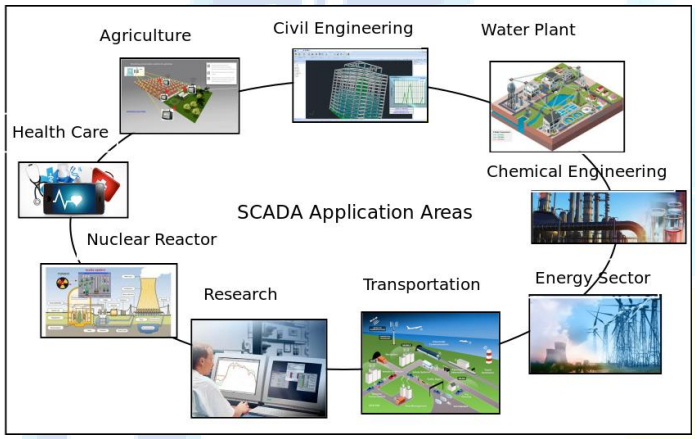

Fig. 1: SCADA Application Areas

2. Related Work:

K. Gowri Shankar (2008) [1] outlines the various stages of operation involved in the conversion of a manually operated boiler towards a fully automated boiler. Over the years the demand for high quality, greater efficiency and automated machines has increased in this globalised world. The initial phase of the paper focuses on passing the inputs to the boiler at a required temperature, so as to constantly maintain a particular temperature in the boiler. The Air preheater and Economizer helps in this process. And the paper mainly focuses on level, pressure and flow control at the various stages of the boiler plant. Thus the temperature in the boiler is constantly monitored and brought to a constant temperature as required by the power plant. The automation is further enhanced by constant monitoring using SCADA screen which is connected to the PLC by means of communication cable. By means of tag values set to various variable in SCADA the entire process is controlled as required. At the automated power plant, the boiler is controlled by Variable Frequency Drive (VFD) to put in action the required processes to be carried out at the boiler. Thus the entire cycle is carried out as a paper and at various stages each phase is detailed out. This paper has proved to be very efficient practically as the need for automation grows day by day.

The most important aspect of any power plant is the boiler control. Several techniques can be implemented to control the boiler in power plant. The method that has to be used relies on varied objectives like superior quality, increased efficiency, high profit and other such points depending upon the purpose of the company that implies it. With the prime objective of catering to these necessities and the needs of the industrial sector, significance has been given here to automation.

K. Gowri Shankar (2008) [1] presented here has kept in mind, the ceaseless changes that are relentlessly taking place in the contemporary scenario of the industrial segment. Emphasis has been given to the automation process that is now rapidly taking its place in all the power plants across the globe. The Paper has furnished itself to study the integral parts of the entire process involved, their implementation and the problems that may show up have also been given their due importance. The future work deals with the purification of water to the boiler and the air circulation for the boiler to burn the fuel using same automation technique.

Over the last decade, efforts from industries and research communities have been made in addressing the security of Supervisory Control and Data Acquisition (SCADA) systems. However, the SCADA security deployed for critical infrastructures is still a challenging issue today. **Ning Cai et. al., (2008) [2]** given an overview of the complexity of SCADA security. Products and applications in control network security are reviewed. Furthermore, new developments in SCADA security, especially the trend in technical and theoretical studies are presented. Some important topics on SCADA security are identified and highlighted and this can be served as the guide for future works in this area.

The security of SCADA systems has been the subject of research, standardization and industrial practices for several years. However, the attacks on SCADA system is getting more frequent due to the openness of the SCADA network platforms, the advancement of hacking techniques and the increased availability of hacking tools. It will rise to a significant level in the future according to the investigation and study by the Committee on Homeland Security [2]. The cooperative efforts from control/automation and IT specialists are the key to combat the threats facing the SCADA systems. New protocols, standards and products are expected to strengthen the security levels of various existing and future SCADA systems. In this paper, we have briefly discussed the major differences between control network security and traditional IT network security. The complexity of SCADA system security is presented. The progress on SCADA system security researches and developments is reviewed. Efforts on the SCADA security from governments, international standardization bodies and research communities are summarized. Some representative products, proposed protocols, and applications are presented. The technical trend and direction on the SCADA security research are discussed, A few research topics, such as high speed real time intrusion detection, artificial immune system for SCADA system, and SCADA security vulnerability assessment, are identified as promising research areas.

M. N. Lakhoua, (2010) [3], presented the applications of a supervisory control and data acquisition (SCADA) system in thermal power plants (TPPs). In fact, a supervisory system must take into account the physiological and cognitive features of the supervisory operator. The paper briefly discusses on the one hand the different steps of the application of a SCADA system and the difficulties to manage and on the other hand it presents three examples of the application of a SCADA system in a TPP in Tunisia and the instrumentations and the measurements used. The first application is related to a counting system of the natural gas, the second one is related to the supervision of pumps vibrations and the third one is related to the supervision of heavy fuel oil.
The SCADA system is used for monitoring and controlling industrial processes from remote areas. It allows an operator to make a set point changes on remote controllers, to open/close valves/switches, to monitor alarms and to gather instrument information from a local process to a widely distributed process, such as oil/gas fields, pipeline systems, or hydroelectric generating systems. In the context of SCADA, it refers to the response of the control system to changes in the process and makes them similar to real-time control system in the virtual environment.
In this paper, an example of a SCADA system in a TPP is studied and some applications are presented. First, we presented the supervision of a counting system of the natural gas of a TPP. This application was permitting the branching of counters of the natural gas to a SCADA system of the TPP in the one hand, and requires the programming and the configuration of the counting system, on the other hand. Second, we presented the supervision of a system of vibratory surveillance in a TPP. This application enables us the creating and the maintaining dynamics of updating the pumping process displays. Finally, we presented the supervision of heavy fuel-oil tanks of a TPP. This application allows us to assure the connection between the ultrasound sensor and the post of surveillance in the control room of the TPP. However, the paper discusses the need to monitor the process and possibly control the operation of TPPs from virtually anywhere.

Boiler is one of the most important equipment in any power plants which require continuous monitoring and inspection at frequent intervals. There are possibilities of errors at measuring and various stages involved with human workers. So a reliable monitoring system is necessary to avoid catastrophic failure, which is achieved by Programmable Logic Controller & Supervisory Control and Data Acquisition system. **S.Kalaivani, M.Jagadeeswari, (2015), [4],** outlined the design and development of boiler automation system using PLC, SCADA and sensors. PLC and SCADA interfaced via communication cables. The initial phase of the paper focuses on passing the inputs to the boiler at a required temperature, so as to constantly maintain a particular temperature in the boiler. SCADA is used to monitor the boiler temperature, pressure and water level using different sensors and the corresponding output is given to the PLC which controls the boiler temperature, pressure and water level. If the temperature and pressure inside the boiler exceeds the predefined value then the entire system is shut down. In case of emergency different automated check valves are used to release pressure, steam and inform the concerned authority through alarm. Boiler automation ladder diagram is designed using WPL soft and SCADA design is done by Intouch wonderware.
In this paper, Boiler Automation using PLC and SCADA was designed and implemented. Different sensors are used to measure the temperature, pressure and water level. SCADA is used to monitor the parameters and PLC used to control the operation. If the temperature and pressure exceed predefined value then the entire setup will shut down and automatic check valves are opened to release the steam and pressure. In case of emergency alarm was energized and automatic check valves are opened to avoid catastrophic failure. Ladder diagram of Delta PLC is simulated using WPL soft and the SCADA design of boiler automation is simulated using Intouch wonderware software. The future research is to focus on the application oriented implementation of remote monitoring of boiler Automation by SCADA internet access.

Comprehensive historical perspectives of different boiler automation techniques are discussed below. This survey provides critical reviews and highlights the concepts, advantages and disadvantages among survey results. This contribution adds more thoughtful ideas in the design and development of boiler automation techniques. In present situation conventional PID control is being used for boiler control. These conventional controllers in power plants are not very stable when there are fluctuations and, in particular, there is an emergency occurring. Continuous processes in power plant and power station are complex systems characterized by nonlinearity, uncertainty and load disturbances. The conventional controllers do not work accurately in a system having nonlinearity in it. So, an intelligent control using PLC& SCADA is developed to meet the nonlinearity of the system for accurate control of the boiler steam temperature and pressure level. Embedded system based boiler automation system consist of GSM (Global System for Mobile Communication), PIC (Peripheral Interface Controller) and different sensors which is capable of monitoring the entire boiler temperature and pressure. The obtained temperature and pressure measured data are transferred through the PIC microcontroller. The microcontroller read the available data and processed.
If the temperature and pressure exceeded the maximum value then the user will be able to get information about the current temperature in any boiler by simply sending a boiler identification number [5], [7].

Microcontroller is programmed with the fuzzy knowledge base rule to control the boiler temperature. The temperature sensor is interfaced with the microcontroller to monitor the steam temperature and a level indicator circuit is used to indicate the water level inside the boiler chamber which is interfaced with the microcontroller and the corresponding

outputs are given as the two inputs for the Fuzzy Inference System. After fuzzification of the inputs and applying suitable rules and defuzzifying the output the microcontroller generates appropriate control signals [6].

Fuzzy PID controller is used for temperature superheated steam of boiler based on the fuzzy control methodology. The control process is simulated through the Simulink MATLAB software. It shows that the system can demonstrate good control ability and dynamic effects even in large delay and stochastic disturbance circumstances [8]. From the literature works that are discussed; it is evident that have several disadvantages. In the proposed system the previous papers disadvantages are overcome by using PLC & SCADA for boiler automation to monitor and control the boiler temperature, pressure and water level in thermal power plant.

As the need of automation increases significantly, a control system needs to be easily programmable, flexible, reliable, robust and cost effective. **Ephrem Ryan Alphonsus et. al. (2016) [9]** reviewed on the application of programmable logic controller (PLC) in our current market is discussed. Investigations on the applications of PLCs in energy research, engineering studies, industrial control applications and monitoring of plants are reviewed in this paper. PLCs do have its own limitations, but findings indicate that PLCs have more advantages than limitations. This paper concludes that PLCs can be used for any applications whether it is of simple or complicated control system.
PLC was first conceivedinlate60's and now has become a major player in automation system. Generally from the review that has been done, PLCs can be fully adaptable for any research, industry applications, control of simple or advanced system, monitoring and even joint control with any other controller in the market such as PID, PICMCU, PLA, PAL and fuzzy controller to name a few. As more advancement of PLCs in the current market, either if its in the hardware of software application, we can see that more people are coming to terms in using PLCs as their main controller in their applications. Programming system using ladder diagram comparing with other type of programming languages are very much beneficial since even an electrician with limited knowledge of programming would be able to understand and program a PLC base on his knowledge of electrical system. Programming is no more for programmers but simple layman can involve in programming machines.

Thermal power plant consist of many important equipment which is required for the generation such as boiler ,coal conveyer belt ,ash handling plant ,cooling system etc. These equipment requires continuous inspection and monitoring . **Akash R. Jaiswal et.al. (2016) [10],** outlined the automation of boiler &coal conveyer .Automation leads to greater efficiency &reliability .The automation is achieved by using PLC&, SCADA. PLC & SCADA is connected through communication cable .This paper focuses on passing the inputs to the equipment so that equipment operation must not get affected .SCADA is used for monitoring the operation of equipment and PLC is used to control the operation . The different sensors are used to sense different parameter such as temperature, pressure, tearing of belt, overloading, water level etc. If the parameter exceed the predetermined value the n it is informed by SCADA system to the operator. in order to automate the boiler and coal conveyer belt the ladder logic is developed. The SCADA screen shows the status of equipment so that operator can take necessary corrective action. In case of emergency different automated check valves are used to release pressure, steam and inform the concerned authority through alarm. The most common Faults in coal conveyer belt are belt tear up fault, moisture content and overloading fault.
In this paper Boiler, Coal conveyer belt, Ash handling plant ladder are developed in PLC. Different sensors are used to measure pressure, temperature and water level. Different sensors are used to the monitor and measure the parameter and PLC used to control the system operation. SCADA system are developed to estimate and monitor current operation states and to collect, analyze and diagnose fault alarm.

The automation control of a boiler superheated steam temperature is considered. It is important to keep the superheated steam temperature at the given level. In case of discrepancy, the boiler operates inefficiently and emergency situations can occur. Namely, the boiler water is flooded alongside steam into a turbine set. A system of multistage cooling of boiler superheated steam through a condensate injection is described by **Olga V. Kolesnikova et. al. (2018) [11]**. The system of automatic control over the temperature of superheated steam for the boiler with three-tier steam cooling system is considered. A regulating algorithm rests on a cascade control method with the temperature error correction based on a force signal. The force signal is a speed of steam temperature change after the condensate injection. A mathematical model of boiler steam cooling is described. The model takes into account a nonlinear nature of the shut-off and control valves of a real boiler. The model was implemented in Simulink (Matlab) and tested on actual data of a steam boiler. The simulation results demonstrate that the method for control over the boiler superheated steam temperature has good quality characteristics, which imply effective control.
The system of superheated steam temperature control on the basis of cascade control and force signals recording is
suggested. The model of the controlled object was developed in the program Simulink (MATLAB). This model takes into account all the complexity of the control loop of boiler superheated steam temperature. This model contains a three step system of a desuperheater and nonlinearity, such as looseness, level and time quantization, hysteresis, dead zone. This model operation was checked on actual data. The results show that the developed model for control is effective as it has good quality parameters.

Supervisory Control and Data Acquisition system facilitates the monitoring and control of industrial process from the designated control station. The cost investment for

implementing the SCADA system is expensive and is not in approach of small and medium scale industries these days. Developing the customized SCADA system helps to reduce the cost in software components and becomes more close approach to the small and medium scale industries. In this research **Sudip Phuyal et. al. (2020) [12],** presented a SCADA software developed in C# environment and successfully tested in industrial process monitoring and control. The developed SCADA software is capable of remotely supervise, control and data monitoring facility and is also capable of data logging in the IoT server. This approach has been found to be efficient in both aspects, technically and economically.

By using the platform of C# environment and using Schneider M221 series PLC as RTU, we successfully tested the performance of low-cost SCADA system in in the milling and roller unit of Mayos Noodles plant in Banepa, Kavre. The setup was installed in the existing running unit of the industry by adding the infrared sensors to detect the flow of materials in the roller, ultrasonic sensors to detect the materials available in the mixer unit, PLC for logical controls and a SCADA interface to monitor and supervise the entire plant process. Additionally, the necessary electrical safety was provided by protection devices like MCCB, MCBs, overload relays, contactors and the add-in blocks, fuses etc. wherever required.

The setup includes the wireless control and supervision of the plant process through the use of internet and the plant process is made to be accessible to monitor and control through mobile applications and the web interface.

This can be easily implemented in small and medium scale industries, isolated and hybrid microgrid systems very easily with very low-cost investment compared to the commercial products.

All types of power generation, transmission and distribution system, industries and all types of process monitoring purpose, the emerging technology of supervisory control and data acquisition (SCADA) is being implemented and also the cloud-based control systems are also emerging in this field for the advanced monitoring and control of the process from the supervisory level. This reduces the workforce required, less time of action for decision taking, easy planning of system task, easy and proper visualization of the system process.

As the commercial SCADA products available in the market is expensive and higher in budget size for small and medium industries, we implemented a low-cost SCADA software developed in C# environment and tested successfully in the process monitoring and control of Mayos noodles industry in Banepa. The test of this system has proved that we can reduce the cost investment in purchasing the software to monitor the industrial process and can run the industry in fully automatic and monitored environment. The product implemented has a huge possibility of upgrade and can be used in commercial industries to reduce their production costs by increasing the machines utilization, reduction in workforce requirement and can also improve the quality of products by monitoring the process more precisely.

The results obtained in this work can be implemented in the commercial and educational purpose to produce SCADA software and hardware for the monitoring and control of full industry. For more facilitated and expanded service, the SMS alerts can be sent to system administrators of any critical notifications, the user-interface can be developed more user friendly so that it can be operated from the webpage directly from using the selector switches and input data.

Table 1: Comparison Table

Protocol Use	Data Use	Behavioral Model	Simulated Data	References
No	Protocol, Source IP, Destination IP, Source Port, Destination Port	No	Simulated Data	[6]
Yes	Packets PDU	Yes		[12]
No	Features extracted by sliding window over a sequence (n-gram)	No	Real Data	[13]
Yes	Master ID, Slave ID, Function Code, Transaction Status, Operation Data, Access Type, Memory Contents, Memory Address	No	Simulated Data	[15]
No	Number of different packets in a time period, Number of packets, between two specific types of packets, Relative difference in the packet rates, Number of different source addresses in a time period.	No	Simulates Data	[16]
Yes	Modbus protocol fields, service discovery	Yes	Simulates Data	[10]
No	Features extracted by sliding window over a sequence (n-gram, invariant induction)	No	Simulates Data	[18]
No	Link utilization, CPU usage, Login failure	Yes	Simulates Data	[19]
Yes	Modbus protocol fields, service discovery	Yes		[17]

3. Conclusion:

The systems based on PLC SCADA are the subject under standardization, research, and industrial applications from

many years. However, the use of SCADA system is getting frequent due with the growth of wireless network platforms, the advancement of techniques and the availability of sensors networks. It is rising to a significant level day by day. The efforts from control/automation and IT specialists are the key support in the systems based on PLC SCADA. New protocols, standards and products are strengthening the modern PLC SCADA control mechanism. In this paper, review is presented on control network security and traditional systems. The complexity of SCADA system is presented. The SCADA system progress in research and developments has been reviewed. Use of the SCADA for international standardization bodies, governments and research fields is summarized. Applications, protocols, and challenges are discussed in terms of technical trend and security is discussed.

References:

[1] K. Gowri Shankar, "Control of Boiler Operation using PLC – SCADA", International MultiConference of Engineers and Computer Scientists 2008 Vol II.
[2] Ning Cai et. al.,"SCADA System Security: Complexity, History and New Developments", DOI: 10.1109/INDIN.2008.4618165 · Source: IEEE Xplore, · August 2008.
[3] M. N. Lakhoua, "SCADA applications in thermal power plants", International Journal of the Physical Sciences Vol. 5(6), pp. 1175-1182, June 2010.
[4] S.Kalaivani, M.Jagadeeswari , "PLC & SCADA Based Effective Boiler Automation System for Thermal Power Plant", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 4, April 2015.
[5] T.Karuppiah, Sivasankaran V, Azha , Periasamy, Muruganand S—Embedded System Based Industrial Power Plant Boiler Automation Using GSM Technology‖ IJARCCE Vol. 2, Issue 8, August 2013.
[6] Anabik Shome, Dr. S.Denis Ashok —Fuzzy Logic Approach for Boiler Temperature & Water Level Control‖ International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012.
[7] K. Ghousiya Begum Mercy D, Kiren Vedi H, Ramathilagam V —An Intelligent Model Based Level Control of Boiler Drum‖ IJETAE Volume 3, Issue 1, January 2013.
[8] Chuntanman, Jia Li,Lanying Wang,Yantao Chi —The fuzzy PID control system for superheated steam temperature of boiler‖ Strategic Technology (IFOST) , IEEE International Conference ,Volume 2, pp. 967-970, June-2011.
[9] Ephrem Ryan Alphonsus et. al., "A review on the applications of programmable logic controllers (PLCs)", Renewable and Sustainable Energy Reviews 60 (2016) 1185–1205.
[10] Akash R. Jaiswal et.al., "Study Of PLC & SCADA Controlled Thermal Power Plant", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 04, Apr-2016.
[11] Olga V. Kolesnikova et. al., "Method of Automation Control of Boiler Steam Temperature", International Russian Automation Conference (RusAutoCon), 2018.
[12] Sudip Phuyal et. al., "Design and Implementation of Cost Efficient SCADA System for Industrial Automation" I.J. Engineering and Manufacturing, 2020, 2, 15-28.
[13]. Düssel P, Gehl C, Laskov P et al, "Cyber-Critical Infrastructure Protection Using Real-time Payload-based Anomaly Detection" Critical Information Infrastructures Security, 2010. 85-97
[14]. Lawrence Berkeley National Laboratory, "Bro intrusion detection system" http//www.bro-ids.org. Accessed 17 September 2010
[15]. Papa M, Gonzalez, "Passive Scanning in Modbus Networks" International Federation for Information Processing Digital Library. 2007, 175-187
[16]. Cucurull J, Asplund M, Nadjm-Tehrani S, "Anomaly detection and mitigation for disaster area networks", Recent Advances in Intrusion Detection. 2010 339-359.
[17]. Porras P A, Neumann P G, "EMERALD: Event monitoring enabling responses to anomalous live disturbances", Proceedings of the 20th National Information Systems Security Conference. 2007, 353–365.
[18]. Bigham J, Gamez D, Lu N, "Safeguarding SCADA systems with anomaly detection", Computer Network Security, 2003, 171-182
[19]. Yang D, Usynin A, Hines J W, "Anomaly-based intrusion detection for SCADA systems", 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies. 2005, 12-16.