# SCALA

# Surveillance Continue d'Activité et Localisation d'Agressions

Francis CAMPAN[1], Van Long DO[2], Patrick NADER[2], Paul HONEINE[2], Pierre BEAUSEROY[2], Lionel FILLATRE[4], Philippe CORNU[2], Igor NIKIFOROV[2], Guillaume PRIGENT[3], Jérôme ROUXEL[3]

[1] ONDEO SYSTEMS, 38 Avenue du Président Wilson 78230 Le Pecq

[2] UTT, ICD - LM2S, UMR STMR – CNRS, 12 rue Marie Curie BP2060 10010 Troyes Cedex

[3] DIATEAM, rue Yves Collet, 29200 Brest

[4] Laboratoire I3S, UMR7271 - UNS CNRS, Sophia-Antipolis

Francis.campan@suez-env.com, igor.nikiforov@utt.fr

**Résumé** –Les systèmes SCADA (Supervisory Control And Data Acquisition) interviennent dans de très nombreux secteurs d'activité : de la production industrielle à la signalisation ferroviaire en passant par les systèmes de traitement et de distribution d'eau. De nombreux opérateurs d'importance vitale (OIV) (si ce n'est tous) sont concernés. Que ce soit par malveillance ou dans une perspective terroriste, prendre la main sur un système SCADA est en général la garantie d'avoir une capacité de nuisance avec un impact maximal. Ce risque est accru par l'architecture distribuée du process et de son architecture associée avec de très nombreux sites dont certains sont contrôlés à distance. De très nombreuses solutions existent pour la protection des infrastructures informatiques des entreprises, mais ces solutions ne sont pas utilisables directement pour des systèmes industriels car ne prenant pas en compte les spécificités de ces systèmes. Ces systèmes industriels contrôlent des process physiques hors du champ des systèmes informatiques de l'entreprise, traditionnellement capables d'opérer de manière indépendante avec des équipements très spécifiques optimisés pour le process et des logiciels développés pour des matériels « contraints » (en terme de capacité de traitement ou de stockage). Dans ce contexte, les systèmes ne sont pas assez protégés et la conception de ces systèmes et des processus opérationnels associés sont encore peu concernés par la sécurité des systèmes d'information (SSI). Dans ce contexte global de protection des infrastructures et des réseaux, nous envisageons d'explorer des moyens de protection économiquement justifiable et d'améliorer la détection d'intrusions pour réduire et minimiser substantiellement le risque résiduel.

**Abstract** – SCADA (Supervisory Control And Data Acquisition) systems are used in many business sectors such as transportation, energy, telecom or water distribution. Most of these sectors are defined in Europe as mission critical sectors and, as a consequence, critical installations have to be protected. For malicious action or terrorism purpose, enter in a SCADA system allows capability to control the system with a wide impact on the process. This risk is increased by the distributed architecture of the process and the associated infrastructure: there are lot of sites and most of them are remotely controlled. There are plenty of solutions to protect a legacy infrastructure of an information system, but these solutions are not useful for industrial systems, because not taking into account the specificity of those systems. These industrial systems are controlling physical processes outside the IT systems, traditionally able to operate as autarkic systems with very dedicated equipment technology optimized to local process efficiency and software developed for constrained devices (in terms of capability of processing, storage or communication). In this context, the systems are not protected enough, and system design and operational processes were only marginally impacted by IT security concerns. In this global context of protection of the infrastructure and the networks, we plan to explore economically justifiable protection and improve the detection of intrusion to reduce and minimize remaining risks substantially.

# 1. Context and positioning

SCADA (Supervisory Control And Data Acquisition) systems are used in many business sectors such as transportation, energy, telecoms or water distribution. Most of these sectors are defined in Europe as mission critical sectors and, as a consequence, critical installations have to be protected.

For malicious action or terrorism purpose, enter in a SCADA system allows capability to control the system with a wide impact on the process. This risk is increased by the distributed architecture of the process and the associated infrastructure: there are lots of sites and most of them are remotely controlled.

Studies in IT security have been made and are going on to protect these systems against intrusion and vulnerabilities exploit. The packaging of solutions used initially for the protection of legacy information systems has been adapted to be used in industrial environment.

Nevertheless, the security cannot be perfect. The hypothesis that the conventional security measures can be bypassed by intruder seems to be realistic. In this context, the SCALA project has three main goals:

- Monitor the network and the system components to display an unusual status through an inspection system;
- Detect/isolate: define an algorithm to detect and to isolate (identify)as soon as possible actions made by an intruder using anomaly detection technique;
- Protect: improve the protection of the system against exogenous attack.

Two types of results are expected, methodology and prototype of product:

- Create a methodology for risk analysis dedicated to industrial system used for process control : define the security concepts for industrial system;
- Prepare an awareness and educational training kit for operational and technical staff in order to improve operational processes by taking into account the security commitments;
- Identify and develop the instruments able to protect the integrity of the production system;
- Development of solutions for detection of abnormality of the behaviour of the system.

In order to demonstrate the capabilities of the results, operators will be involved in the project. These operators operate sites in water and energy domains.

As required by the call 2011, partnership has been made between German and French partners. The following chapters are focused on the French tasks of the project.

# 2. State of the art

## 2.1 SCADA system: a special case of cyber-physical systems

The SCADA system is a special case of cyber-physical systems (CPS). A CPS is a system featuring a tight combination of, and coordination between, the system's computational and physical elements. Unlike more traditional embedded systems, a full-fledged CPS is typically designed as a network of interacting elements with physical input and output instead of as standalone devices. A real world SCADA system can monitor and control hundreds to hundreds of thousands of Input/Output (I/O) points. As an example, a very simplified water distribution SCADA application would be to monitor water levels at various water sources like reservoirs and tanks and when the water level exceeds a preset threshold, to activate the pumping system to transfer water to tanks to low tank levels.

The SCADA Host is usually industrial PC running sophisticated SCADA with treatment and HMI (Human Machine Interface) software. This software is used to exchange data with the remote sites and store the collected data in its centralized database. Logic can be configured in the SCADA Host software which then monitors and controls plant or equipment. The control may be automatic, or initiated by operator commands.

SCADA systems have to monitor and to control two types of signals:

- Analog signals: levels, temperatures, pressures, flow rate, motor speed, etc.
- Digital signals: level switches, pressure switches, generator status, relays, motors, etc.

There is typically another layer of equipment between the remote sensors/instruments and the central computer. This intermediate equipment (existing on the remote side) is used to digitalize and packetize the sensor signals so that they can be digitally transmitted via an industrial communications protocol over long distances to the central site. Typical equipment that handles this function is PLC's (Programmable Logic Controllers) and RTU's (Remote Terminal Units). SCADA systems cover much larger geographic areas. RTUs differ from PLCs in that RTUs are more suitable for wide geographical telemetry, often using wireless communications, while PLCs are more suitable for local area control (plants, production lines, etc.) where the system utilizes physical media for control.

## 2.2 Main characteristics of SCADA systems

Detecting an intrusion and/or a failure in the SCADA system is a difficult task because CPS (including SCADA systems as a particular case) has specific characteristics:

- Input and possible feedback from the physical environment;
- Distributed management and control;
- Real-time performance requirements;
- Wide-distribution geographically, with components in locations that lack physical security;
- Multi-scale and systems of systems control characteristics.

Feedback and input from the physical environment means the existence of communication channels which need to be "secured". This characteristic is one that is specific to CPSs. An attacker does not need to break into the computer to affect such a system, but could cause a coordinated streak of physical actions that are sensed and which cause the system to respond in an unexpected manner. To protect efficiently such systems from this kind of attack requires an understanding of the system from the process point of view and not from the security point of view

Large-scale CPSs involve management by multiple parties. The utilities manage their own parts of the whole system. Global decisions (induced by interconnections between utilities) affect the whole system. Many of the changes that need to be made across the system as whole must occur increasingly on small time-scale, meaning automation of local actions based on input from other organizations in other parts of the system. The structure of such systems is like a federation: systems are interconnected and control is distributed.

CPSs have real-time requirements. Some actions must be made locally to take into account failure transmission elsewhere. The delayed reaction on the initial failure will result in cascading failures and possible permanent damage to equipment. Over time, these interactions have become more complex, and require reaction on smaller time-scales. This requires automated response, sometimes based on remote inputs from sensors and commands originating with other members of the federation. The real-time requirement also implies a requirement for performance (no overload of the whole system).

CPSs are often geographically dispersed, with components in the field where they lack appropriate physical security. Such physical dispersion also makes it difficult to physically reset, or reload the software on a compromised device. Security solutions in such an environment must be tied in part to resilience of the application in spite of such compromise, rather than focus solely on preventing compromise of the component in the first place.

CPSs may be multi-scale systems and systems-of-systems. Since components in the systems of systems are necessarily part of multiple systems, with different ownership, management, and security requirements, what we once thought of as non-critical infrastructure can have critical consequences.

CPSs are often using large networks. Any large network is a very "noisy" environment[1] even at the packet level [1]. Such noises may affect the performance of an Intrusion Detection Systems (IDS) by adding ambiguities into physical "analog" and "digital" sensing. Moreover, noise is also referring to the diversity of legitimate network traffic [2]. Zachary et al. [3] further argue that discerning between normal and malicious traffic is an ill-posed problem. Some of the mostly common used SCADA-specific protocols are byte-coding, such as ModBus, DNP3. When these protocols are tunneled over IP and used in conjunction with TCP, the security implication of the envisioned problem due to ambiguities would be more potentially damaging, if no proper attention is paid on.

## 2.3 Exploiting physical interactions to improve security

The design of applications for security is crucial for a SCADA system. The common approach consists of using myriad of security mechanisms such as encryption, authentication, authorization, intrusion detection, and firewalls. One needs to define the authorized and unauthorized information-flow, control-flow, and availability requirements of the application, taking into account the physical consequence as well as the cyber consequences of a breach of any of these requirements. In CPSs, this enumeration must take into account a domain specific including the physical and external-process channels that are part of the system. By physical channel, we refer to physical inputs from sensors, and external-process channels include the reactions by human operators of the system, or control activities initiated by outside parties based in part on data from the system under design.

As a second line of defence, work is needed in modelling the security implications of physical interactions in CPSs. Physical interactions with components of a system must be modelled as control and data channels. Security testing should model these physical interactions in addition to the purely cyber-attacks. Such modelling of physical interactions is likely to be application domain specific, e.g. modelling the effect of flow constraints within a water distribution system. A framework for integrating such modules and visualizing the effects of the physical aspects of such a system would be useful. Security for sensors and actuators in the field needs to be considered. Techniques for detecting tampering, and validating the inputs provided by these sensors is important to prevent these control inputs to the CPS from being recruited by adversaries.

[1] refers to the messiness of benign and innocuous yet non-ideal system and network data due to unintentional interference from natural and technical sources.

## 2.4 Attacks on SCADA systems

Cyber intrusions on SCADA systems can be grouped according to their possible target-based manifestation channels, e.g.:

- Data historian, HMI, controller: what data and control functionality have been stored in memory or disk ?
- Network link between sensors and HMI or controller: what is seen by controller/operator including ID, address, value and time ?
- Network link between controller and actuators: what is being sent to actuators including ID, address, action, value and time ?
- Modify sensors threshold values and settings through cyber means;
- Modify or sabotage actuators normal settings through cyber means.

## 2.5 Methods for SCADA intrusion detection

Many methods are proposed in literature to detect an intrusion. The detection of a failure, once the system is affected, is a less studied problem. Each method can be applied to at least one of the above mentioned group of attacks.

### 2.5.1 Signature detection IDS for SCADA

In the early days of IDS research, two major approaches known as signature detection and anomaly detection were developed [4], [5]. The signature detection [11], [12] matches traffic to a known misuse pattern of the intrusive process and its characteristic traces regardless system normal behaviour. Namely, we are watching for known intrusion. Supplied with a well-craft intrusion signature and the absence of its variants in real operations, this approach can theoretically achieve high detection rate and low false alarm rate simultaneously.

### 2.5.2 Anomaly detection IDS for SCADA

While in anomaly detection [10], [13], [14] we do not watch for known intrusion but rather the abnormalities in the observed data in question and alert when something "extremely unusual" is noticed. It's usually based on learning with certain statistical profiling of the usual behaviour of the overall SCADA system over time without regard to actual intrusion scenarios. Namely, we identify deviation from the learned normal system model and decide whether it's within acceptable range. This approach faces the difficulty to find a snag fitting model for the usual behaviour that is comprehensive enough to avoid false alarms yet tight enough to escape false negatives. Ideally, a faithful model can detect novel attacks as well.

### 2.5.3 Probabilistic approaches

Between the two above mentioned approaches, there lie the probabilistic and specification-based methods for intrusion detection. A probabilistic approach is also termed as a statistical or a Bayes method [6] with probabilistically encoded models of misuse. It has some potential to detect unknown attacks. A specification-based approach constructs a model of what is allowed, enforces its predefined policy and raises alerts when the observed behaviour is outside this model. It has a high potential for generalization and leverages against new attacks [7]. This technique has been proposed as a promising alternative that combines the strengths of signature-based and anomaly-based detection. Instead of finding the deviation and unknowns, specification-based method [7], [8] defines what's allowable in terms of network and system traffic behaviour/patterns. This method sounds promising but it might be tedious to enumerate all possibly allowable patterns.

### 2.5.4 Configurable Embedded Middleware-Level Detection

Næss and al [15] present a configurable Embedded Middleware-level Intrusion Detection System (EMISDS) framework that is application specific. EMISDS comes with IDS-aware middleware tools to embed IDS sensors and detectors into an application's middleware layer instead of directly interacting with the low-level system and network interface. The system model is comprised of anomaly and misuse detection. EMIDS uses interval-based and procedural-based IDS sensors and misuse-based IDS detectors. Interval-based sensors are responsible for identifying whether parameter values and method invocation frequencies fall within their predefined ranges or not. Procedural-based sensors embedded at the entry or exit points of application monitor its execution patterns. Misuse-based detectors reside within the application's source code at those locations where known vulnerabilities exist. By exploiting this application specific information, EMIDS provides reusable security policies such as predefined ranges for interval-based sensors and stored profiles of acceptable behaviour for procedural-based sensors. This approach integrates intrusion detection in the middleware layer which does the resource intensive job of unmarshalling network packets thus saving the IDSs in the embedded components of the SCADA networks from doing it.

### 2.5.5 Intrusion Detection and Event Monitoring in SCADA Networks

Complementary to the above direct knowledge based classification; there are also behavioural detection approaches [16]. They capture behaviour patterns associated with certain attacks, which are not necessarily illegitimate in the direct semantic sense but wrong in a

contextual setting thus may require secondary evidence. They may abstract allowable normal interaction as well. Such methods are quite promising, especially used in conjunction with other methods [9].

#### 2.5.6 Modeling Flow Information and other Control Systems Behaviour to Detect Anomalies

Moran and Belisle [19] use a commercially available Network Based Anomaly solution to passively monitor the flow between routers and other network devices. They apply a quite comprehensive combination of anomaly-, behavioural- and specification- based techniques to detect a deviation from normal behaviour. Since it's flow-based, this solution focuses more on network layer detection and cannot investigate attacks specifically crafted at application layer. No analysis on false alarm or missed detection rate is available.

#### 2.5.7 Model for Cyber-Physical Interaction

One approach which uses a physical model to detect an intrusion is proposed by Rrushi and Campbell [17]. The authors set out to probabilistically build a profile of legitimate data flows plant (a nuclear power plant in the paper) along with the main characteristics of the substation information exchanged between devices. As noted by the authors, their intrusion detection rules are implementable in all construction provided that attack-effects are based on known failure models.

Another approach is proposed by Xiao and al [18]. The SCADA system is decomposed into a physical layer and a cyber-layer and the authors propose a separate workflow layer above it. They consider that each essential component in the physical layer has a corresponding node in the workflow. Mathematically speaking, a workflow models both essential functionalities of the underlying physical layer and attack patterns derived domain specific security knowledge. This work leverages the presumably existing survivability-related knowledge and protection scheme to incorporate the detections of both known attack patterns and known unsafe states. A simplified water treatment system is studied through simulation to illustrate the idea.

# 3. Scientific program

## 3.1 Specification

1. The concepts, tools and other techniques usually used or under development in the Information Communication and Technology (ICT) security area are to be also reviewed in order to take into account any latest development which are already applied in the industrial domain.
2. In order to avoid scattering of effort, we must describe the typical industrial system used for process control.
3. Based on the two first tasks, it aims to formalize the specification of the target system from the security point of view. Taking into account the critical context of an operational system and therefore the performance requirements, the specification includes the definition of the protocols for validation and qualification of the system.

## 3.2 Security and risk analysis

Security analysis of the industrial system is based on the system description (structure, interfaces, etc.). The purpose is to determine where to harden the system regarding exogen disrupting.

SCADA systems are complex. To assess vulnerabilities and identify possible points of interest for penetrating a system like this, we wish to use an analysis approach from the attacker's point of view.

This "bottom up" white box audit approach will allow us to develop attack trees specific to the studied business domain.

The ultimate goal of this study is to be able eventually to formalize a methodology for "bottom up" risk analysis based on the motivations of the perpetrator (external and/or internal) and define a first methodological range of interest points to secure in order to block or prevent the most critical attack scenarios.

In the longer term, the idea is to complement this "penetration test" approach by a traditional risk analysis in order to lead to a genuine reproducible method of cross-sectional analysis of the security of SCADA systems.

To help operational team, guidelines and training packages will be delivered.

## 3.3 Instruments for protection and monitoring

Two ways of research will be followed :

- Develop a protection device and monitoring probe to capture and record the traffic and the system behaviour.
- Define a target system to mimic the actual system. This system could operate as a decoy and could indicate there is an attack on the actual system.

Adam and Byres [20] presented an interesting high level analysis of the possible threats to a power plant system and in the Chandia, Gonzalez, Kilpatrick, Papa and Shenoi [21], the authors describe two possible strategies for securing SCADA networks, underlying that several aspects have to further improved.

Such control system communication protocol like Modbus, Profibus, DNP, ... are still widely used in control system networks, even though some more secure protocol or version are developed. Existing so vulnerable protocols will continue to be used in the future by reason of economy and backward compatibility.

What is evident today is that communication protocols used in such systems were absolutely not conceived for dealing with typical ICT legacy threats. To our knowledge, to date no operational solution is proposed for intrusion detection on industrial networks and that is why we propose to realize a dedicated hardware and software component for detecting network intrusion in SCADA protocol environments (NIDS approach).

This component will enable the acquisition of network frames in a distributed manner (by a collection of sensors) for subsequent or delayed analysis on specific equipment (correlation engine, aggregation, statistical analysis) and be capable of detecting abnormal behaviour locally and specifically block certain traffic (as a proactive safety device).

There is a plethora of SCADA standards and protocols overseas that can be currently used within the SCADA industry. But on the other side, SCADA networks have some special characteristics not present in traditional IT networks:

- Fixed number of devices;
- Fixed number of protocols;
- Regular traffic patterns.

Our goal is to design, build and test a prototype in-line proactive SCADA network sensor whose first vocation is issuing alerts. The main task of this manageable equipment is to collect and monitor traffic in real-time in order to, initially, apply a simple rule-set to:

- Generate alerts;
- Optionally block certain traffic.

The level of protection offered by this future IDS agent will be primarily focused on:

- Topology discovery tool scans;
- Use of known vulnerabilities;
- Denial of Service attacks by flooding;
- The impromptu appearance of new protocols;
- The impromptu appearances of new devices (rogue PLC or rogue RTU).

## 3.4 Detection of possible intrusions

The goal of this part of the project is to design the statistical methods of intrusion detection/isolation. Two alternative approaches will be developed in the project:

- model-based statistical anomaly detection and isolation methods;
- nonparametric methods based on the learning theory and pattern recognition

For the first approach it is necessaryto get a model of system. The purpose is to be able to define a space of “nominal states” of the system. This model is designed by using the data and knowledge provided through the specification task. We will try different ways of research to set a system model :

- Design a logical scheme of the whole system architecture: this may be difficult because the industrial systems are complex, heterogeneous, real time and must be available all the time;
- When the industrial system controls a technological process, a lot of process data are stored. A track is to define “normal states” of the process and therefore normal states of the system;
- One of the results of the project will be a probe to record and analyze the network traffic, the behaviour of critical components of the system. We could use the large amount of stored data to determine a space of normal behaviours inside the whole system.

At this stage, we do not know if it will be possible and necessary to define the global state space of the entire system. We think that we will be able to define at least the state space of local subsystems.

## 3.5 Test and demonstration

The project developments will be tested by using off-line and restricted on-line demonstrators, based on process control systems in Germany and in France, in water and energy distribution domains. There will be different steps in this work package:

- Preparation of a test bed with simulation of the process environment based on the real process and system context from the pilot sites;
- Demonstrator for the validation of each component;
- Definition of test scenarios;
- Definition of tests to be carried out;
- Definition of test evaluation criteria and evaluation grid;
- Integrated test on the simulation platform;
- Pilot site for the demonstration of components (the way to do such kind of test will be defined carefully, and will be studied in detail with the operational teams in Germany and in France);
- Return on experience.

## References


[1] Ross Anderson, *Security Engineering – A Guide to Building Dependable Distributed Systems*, Wiley, 2001.

[2] Thomas H. Ptacek and Timothy N. Newsham, *Insertion, Evasion, and Denial Of Service: Eluding Network Intrusion Detection*, Secure Networks technical report, 1998.

[3] John Zachary, John McEachen and Dan Ettlich *Conversation Exchange Dynamics for Real-Time Network Monitoring and Anomaly Detection*, Proceedings of the Second IEEE International Information Assurance Workshop (IWIA04), 2004.

[4] Carl Endorf and Jim Mellander, *Intrusion Detection & Prevention*, McGraw-Hill Professional, 2004.

[5] Stefan Axelsson *Intrusion Detection Systems: A Survey and Taxonomy*, Technical Report, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, 2000.

[6] Christopher Kruegel, Darren Mutz, William Robertson and Fredrik Valeur, *Bayesian Event Classification for Intrusion Detection*, in Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003).

[7] Ivan Balepin, Sergei Maltsev, Jeff Rowe, and Karl Levitt *Using Specification-Based Intrusion Detection for Automated Response*, in the Proceeding of the 6th International Symposium, RAID 2003, Recent Advances in Intrusion Detection, Pittsburgh, PA, September 8-10, 2003.

[8] Calvin Ko, *Execution Monitoring of Security-critical Programs in a Distributed System: a Specification-based Approach*, Dissertation, Department of Computer Science, University of California at Davis, 1996.

[9] Stefano Zanero, Behavioral *Intrusion Detection*, in Proceedings of 19th International Symposium on Computer and Information Sciences - ISCIS, pp. 657-666, October 2004.

[10] Dayu Yang, Alexander Usynin, and J. Wesley Hines, *Anomaly-Based Intrusion Detection for SCADA Systems*, International Atomic Energy Agency (IAEA), Technical Meeting on Cyber Security, Idaho, 2006.

[11] Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, Alfonso Valdes, *Using Model-based Intrusion Detection for SCADA Networks*, SCADA Security Scientific Symposium, 2007.

[12] Martin Roesch, Snort - *Lightweight Intrusion Detection for Networks*, Proceedings of LISA '99: 13th Systems Administration Conference, USENIX.

[13] Keith Whisnant, Kenny Gross, Natasha Lingurovska, *Proactive Fault Monitoring in Enterprise Servers*, in Proceedings of the 2005 International Conference on Computer Design, pp. 3-10, June 2005.

[14] Chi-Ho Tsang, Sam Kwong, *Multi-Agent Intrusion Detection System in Industrial Network using Ant Colony Clustering Approach and Unsupervised Feature Extraction*, In Proceeding of IEEE International Conference on Industrial Technology Page 51- 56, ICIT 2005.

[15] Eivind Naess, Deborah A. Frincke, A. David McKinnon, David E. Bakken, *Configurable Middleware-Level Intrusion Detection for Embedded Systems*, The 25th ICDCSW, 2005.

[16] Paul Oman, Matthew Phillips, *Intrusion Detection and Event Monitoring in SCADA Networks*, book chapter of Critical Infrastructure Protection, Pages 161-173, Springer Boston, 2007.

[17] Julian Rrushi and Roy Campbell, *Detecting Attacks in Power Plant Interfacing Substations through Probabilistic Validation of Attack-Effect Bindings*, in Proceeding of S4: SCADA Security Scientific Symposium, Miami, FL, January 2008.

[18] Kun Xiao, Nianen Chen, Shangping Ren, Limin Shen, Xianhe Sun, Kevin Kwiat, Michael Macalik, A Workflow-based *Non-intrusive Approach for Enhancing the Survivability of Critical Infrastructures in Cyber Environment*, in Proceedings of Third International Workshop on Software Engineering for Secure Systems (SESS'07).

[19] Brian Moran, Rick Belisle, *Modeling Flow Information and Other Control System Behavior to Detect Anomalies*, in Proceeding of S4: SCADA Security Scientific Symposium, Miami, FL, January 2008.

[20] Creery, A., Byres, E.J. *Industrial Cybersecurity for Power System and SCADA networks*,IEEE Paper No. PCIC-2005-DV45, 2005

[21] Chandia,R., Gonzalez, J., Kilpatrick, T., Papa,M.,Shenoi,S. *Security Strategies for Scada Networks*. In : Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, March 19-21 2007.