Federative SCADA – Solution for Evolving Critical Systems

I. Stoian*, E. Stancel*, S. Ignat* , Sz. Balogh*

*IPA – R&D Institute for Automation – Cluj – Napoca Subsidiary, Romania (Tel: 040-264-596155);
e-mail: *ioan_stn@yahoo.com;eugen_stancel@yahoo.com;sorin_ign@yahoo.com;bszabolcs@yahoo.com*)

Abstract: This article intends to introduce the concept of federative SCADA systems in order to fulfill the requirements of evolving critical systems. The SCADA Federation is a cooperative system which ensures more than the individual assigned functions of each entity, but also provide some envelope functions created by the mechanism implemented into each federative SCADA systems member. It defines the structure, the conceptual model of the federation, the set of rules imposed to the federation members, the global tasks of the federation, the envelope functions and the offered services, preserving in the meantime all the individual systems functionally which are improved by integration synergy.

The federation assures the management support of interconnected individual critical systems, using different technologies and methods to enable the participation of existing stand-alone SCADA systems to the federation, in order to provide an added value, the interoperability of the resulted enhanced-system.

The concept may be prospectively exploited in order to carry out the integration among several evolving critical SCADA systems. To all types of critical systems: safety critical, mission critical, business critical and security critical, the federative SCADA systems offer a support to decrease their level of criticality. The topic of coordination and interoperability involves system of systems (SoS) approaches.

Keywords: SCADA federation, cooperative systems, evolving critical systems.

1. INTRODUCTION

The rapidly evolving demands and scale of SCADA (Supervisory Control and Data Acquisition) systems determine their overall/ increasing feature but in the meantime they become more and more critical systems. The computing resources integrated into the SCADA system structure are more powerful, more data must be exchanged to meet the information demands of more powerful and high diversity users spread in a wide geographical area.

So the systems are becoming more complex as they must cover a wide diversity domains of activity and meet the requirements imposed by different management level (large and very large hardware structures, new updates appearing in shorter periods of time for application software, increasing the number and types of the connected sensors and actuators which are becoming more and more complex). The continuous demands of faster and more secure SCADA systems in a day by day changing business environment impose a rapid/ quick change for expanding the capabilities.

There are many factors driving the evolution of the modern SCADA systems, more hardware platforms and software products help SCADA users cope with that change in short time.

Serving different users, the SCADA systems become heterogeneous by design, representing various domains and fields of activities and adopt a specific architecture. They are deployed in many fields of activity: manufacturing companies, public utilities (power, water, gas supply for large geographical areas) and corporate business networks, health system, environment survey and protection, risk evaluation, management of disaster) expressing and revealing the ubiquity of SCADA systems.

The requirements and the need for greater computing power, rapid development and expansion of hardware determine an increased evolution tempo. New types of networks are accessible today and the SCADA systems must operate over new and increasing types of networks with high data transfer rate and more capabilities. Considering the above mentioned issues related to SCADA systems (large and very large scale, heterogeneous features, ubiquity), we conclude they are exposed to an increasing system criticality (Lorcan, 2010).

2. SCADA SYSTEMS

Critical systems are systems where failure, or malfunction will lead to significant negative consequences (Lyn, 1996). These systems may have strict requirements for security and safety, to protect the users and some other entities (Leveson 1986). Alternatively, these systems may be critical to the organization's mission, product base, profitability or competitive advantage.

Many of the SCADA systems in use today belong to one of

the following critical system types: safety – critical, mission-critical, business-critical or security-critical .

Types of Critical Systems are defined by (Lorcan, 2009).

Safety critical system – may lead to loss of life, serious personal injury or damage to the natural environment.

Mission critical system – may lead to in ability to complete the overall system or project objectives.

Business- critical system – may lead to significant tangible or intangible economic costs.

Security critical system – may lead to loss of sensitive data through theft or accidental loss.

Many SCADA systems have overlapping aspects of criticality.

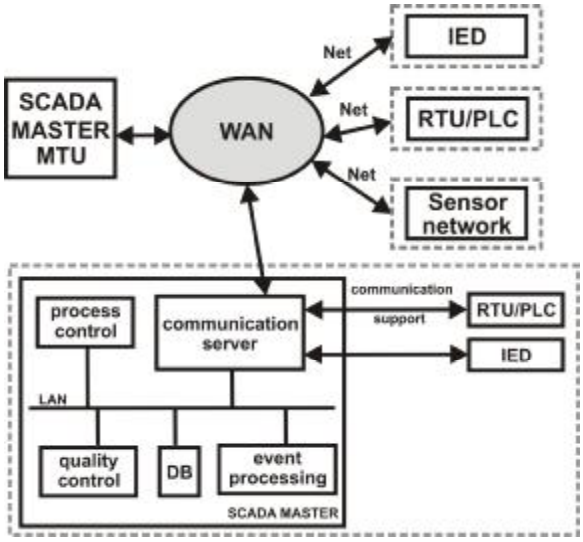

Fig. 1. Networked SCADA Systems.

SCADA systems in use belong to three generations: monolithic, distributed and networked systems.

SCADA systems, whether belonging to the latest hardware and software technology or to systems that have been commissioned years ago but still in operation, representing different generations, should adopt high speed communication equipment and networks in order to be integrated into the federation. Using the newest technology, the risks of remote attacks (increasing criticality) is present to all the system levels. Heterogeneous communication equipment and protocols determine one of the critical aspect of SCADA systems (need to verify their compatibility).

The increasing use of SCADA systems in various domains of activity, distributed in wide geographical area, determine the use of various physical support (telephone lines, radio, FO, satellite) and multitude of communication standards. The interoperability between equipment from different producers depends on their compatibility *(Letia, 2005)*. They become much more involved in the environment security management .

SCADA federation concept has the computational support of the third generation SCADA systems as they are based on an open software and hardware architecture, and their functionality is distributed across a WAN. This generation use open standard communication protocols for data transfer. The networked SCADA systems integrate new generation of RTUs/PLCs. Huge volume of data must be stored in a safe way and this lead to the possibility of loss of sensitive data – SCADA systems become security – critical.

The SCADA systems are used by more and more companies organizations, local and state authorities. They use the data provided by more operational SCADA systems implemented in various domains for safety impact assessment. When variously interconnected heterogeneous systems that operate with several common information or data fail, there is a need for complementary support to substitute the missing information. As SCADA systems are used by important companies, they expose the business in case of partial failure to don't complete the main objective– the aspect of mission critical systems overlaped with bussines – criticality. There is a certain data redundancy between different such SCADA systems and the federation aims to use it for the benefit of all of his constituents. Even each one investigates some common critical parameter is a waste or inefficient use of distributed computing resources in normal operating conditions but much more in un usual situations.

Having no general rules to conform with the models implemented in various SCADA systems can't be complement each other because they are working insulated having no information regarding the other systems capabilities. We conclude that SCADA systems become more and more critical systems by evolving technologies and their wide variety, communication support resources exposed to attacks as they a spread in a wide area interconnecting different equipment belonging to various technological generation.

SCADA vulnerability or criticality involve the following associated issues: remote access, various networks configurations and topology, third party security holes in operating systems, commercial databases and other applications lack of protection, legacy communication protocols not encrypted, missing redundancy at the sensing level.

3. SCADA FEDERATION CONCEPT

The rapid evolving characteristics and magnitude of SCADA systems determine their increasing criticality. An effective solution to this challenge could be the SCADA System Federation - a concept based on the information technology management methods.

The SCADA federation is a cooperative system which ensures more than the individual assigned functions of each entit,y but also provides some new created envelope functions based on various specific mechanism implemented into each federative SCADA systems member.

The SCADA federation responds to the individual system's required tasks as well as to the continuing growing of all criticality processes specific to various SCADA system, to

their operations and procedures, and addresses and try to find real solutions to the challenges of the above mentioned critical type systems.

The SCADA federation concept defines the main global characteristics needed for the integration of the individual systems. It realizes the inter operability among the federation members and provides informational support to mitigate the data loss risk during the critical situation. It aims to create new added value to the individual SCADA systems and to all the public authorities which are interested to join the federation . It is designed to meet the management needs of a every federative organization which accept and are submitted to the the cooperative set of rules, respect the individual access rights to the federation resources and are submitted to the global coordination of the local authority tasks imposed during critical situations. Because of its flexibility and extensibility, the SCADA federation has great benefit to all the members. Using the envelope model functionality implemented by federative SCADA systems, the federation offer the support for the realization of its global tasks and ensures the possibility to all the entities to share the benefits offered by the envelope created features. The resources of federative SCADA systems represent real solution to lower the criticality that characterises the individual SCADA systems. It provides all of these added values by the inter operability main functions which characterise some specific advantages as: redundant resources exploitation, fault tolerant control/processing control, complex event processing system techniques, the new extended informational envelope models created by the integration of various models owned by the various individual SCADA systems. The new multi model is a support for proactive actions, risk assessment and management of critical systems. The SCADA federation concept exploits the synergy of the cooperative based approach (multi-level model, runtime model, and proactive control).

The integration of various information and metadata, content offered by different entities, may increase the overall efficiency of individual and global process management based on federative rules and its relevant outcomes.

4. SCADA FEDERATION ARCHITECTURE

The conceptual model of SCADA federation determines what data each individual system is allowed to offer to other members, and what are the sharing resources to be imported from the partners. When one SCADA misses some information, another SCADA system - as component of the federation may supply the needed data accessing the federation resources database and models.

Each SCADA in the federation will define the data and parameters available for sharing with all other SCADA systems according to the federative rules in order to not interfere with the real-time local control critical tasks. Each SCADA system is able to access the models owned by all the other SCADA for obtaining the missing information due to the failure of its sensing modules.

Required services are organized hierarchically, based on certain priority mechanisms. Federation participants exchange aggregated information between them according to specific rules (Gordon, 2004) and determine the way information should be aggregated by the complex events analysis (figure 2). SCADA federation provide some proactive action that can be elaborated for the benefit of all the partners using the knowledge accumulated by a certain member in similar condition. The federation ensures a cost-effective use of several models implemented into individual systems which become a common resource for all of them.

Basic principles for the federative SCADA system concept are the support to define specific ways how all the integrated systems will cooperate to ensure the overall functionality.

Observability.

If a certain zone of a SCADA system is not observable, the observability analysis module will further determine the pseudo-measurements that need to be added to make the system observable. The observability investigations are used to qualify a system that has this capability, based on the information related to the federation topology and the SCADA parameters evaluation.

Controllability. Each SCADA system is characterized by a partial overall controllability. In order to obtain total controllability at the inferior levels of SCADA system, should integrate the third generation SCADA components. At the superior control levels, SCADA systems assure proactive/ predictive controllability using the process models.

Observability and controllability features depend rigorously on SCADA systems capabilities, like: master re-initialization, master clock synchronization, universal watch master, functions like pooling, parameters configuration.

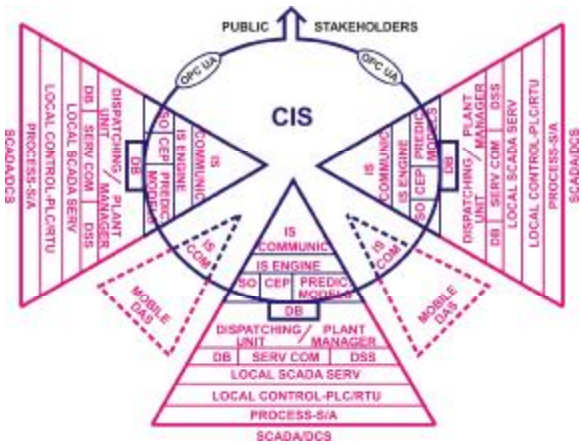

Fig. 2. SCADA federation architecture

The Common Information Space contains all the higher hierarchy levels from all the SCADA systems. The Integrated Supervisor - IS Engine, the IS Communication support, the SO (Sensing optimisation techniques), Complex Event Processing - CEP, Prediction Models and the databases DB owned by all the members of the federation are

interconnected by means of OPC UA protocol. In this way the aggregated data are offered to the different users as the public authorities, stakeholders, high level management entities.

Main components of SCADA federation

The SCADA federation is based on integration strategies involving development of mechanisms structured on Common Information Space (CIS) concept, including an Integrated Supervisor (IS) (figure 3) for systems, in order to provide pro-activeness, functionality, accuracy, reliability and resilience.

The federation defines the functional modules and the integration tasks:
- definition of a system integration mechanism (peer-to-peer, plug&play), system open re-configurability, adjustable group membership, reconfigurable interoperability, complex multi-modal behaviour assessement, assigned right for common resources exploitation, common multi-models identification, common complex event analysis;
- standardization premises for federative integration;
- definition of a certain test application in large-scale management systems, conceptual novel models based on exploitation of multi-sources embedded information, specific data streams analysis and complex event processing recognition, sensing optimization, adapting the multimedia content transmission standardization through OPC UA support.

CIS provides simultaneously data, models and resources merging which belong to different information spaces, complex event processing, pro-activeness methods, structured on novel predictive multi-level models. IS manages all operations in an open standardized framework based on end-to-end approach.

CIS environment

There are many different practical reasons for making field instruments intelligent through CIS environment. They depend on type of instruments and the conditions they are used. Furthermore the sensing elements used should have the potential to be upgraded as intelligent ones using the federative aggregation. The CIS environment will provide automatic optimization of the sensitivity, enhancement of the dynamic range and accuracy by filtering algorithms.

The following issues are considered to be the general reasons for the provision of intelligent field instruments:

CIS improvements operational capability and maintenance

- Remote sensors maintenance support functions (zero-point and span adjustments, measurement range, etc.)
- Integration of different range sensors by widening sensor's measurability (flexibility features regarding user's specification changes, reduction of the inventory diversity for maintenance service, etc.)
- Storage and readout of sensor data and process control data (tag, domain, historical maintenance data, set-point);
- Self-check and self-learning functions;
- Emergency event detection and alarm setting (out of range, unusual environmental conditions).

CIS improvements in measurement accuracy is obtained through advanced linearization of signals, automatic zero-point calibration, error compensation and adaptive compensation of errors.

Improvements in communication functions and reduction of system failure:

- Open standard communication support with upper level system and the inter-connected systems

-Fault detection and fault prediction features of control system, based on IS Engine characteristics:
- A feature of fault detection is that the targets of detection or recognition are "states" of the devices, equipment, machines or local systems. The fault detection systems use different techniques, such as information processing, detection of physical signals and digital signals status.
- The "state" is extracted from physical data by means of techniques, based on knowledge acquired during the time of operation or from experimental results.
- The final aim of a fault detection system is to discriminate the abnormal "states" of the monitored system or equipment from the normal states; moreover, discrimination between types and degrees of abnormal states is required frequently.

The fault detection systems require some clarifications that are divided roughly into two groups as follows:
- Assessment of abnormality, its category and its degree which are derived from the signals offered by the usual sensors, which are not specially developed. Since the discrimination between states is based on human experience or experimental facts, processing techniques combined with knowledge engineering, such as application of the neural network, or expert systems for waveform analysis, have been recently developed.
- The difficulties to access the usual sensors - real difficulties arising in fault detection systems, in many cases, have been caused by the difficult/limited access created by physical hazards, or by the inadequacies of the sensors themselves with respect to the discrimination of parameter value against the false information.

The IS have access to various types of data collected from the RTUs/PLCs belonging to different SCADA systems; data can be viewed from anywhere in the federation.

The IS (Integrated Supervisor) Engine integrates features as: real-time complex event processing, democratic sensing access, proactive management conceptual model and common resources management.

The IS engine is able to exploit information embedded in the models implemented into each entity and take the appropriate decisions concerning the optimum management of the whole distribution chain. CIS provides the virtual environment for high level decision tasks, develops the appropriate interfaces between the IS and the various entities of the distribution chain, so that decisions taken by the IS will be transformed into the appropriate lower level control signals for each entity: system, module/equipment, tool, etc.

The IS supports the interoperation between a number of entities to provide data and multimedia content delivery with a given QoS, respecting the owners contents rights.

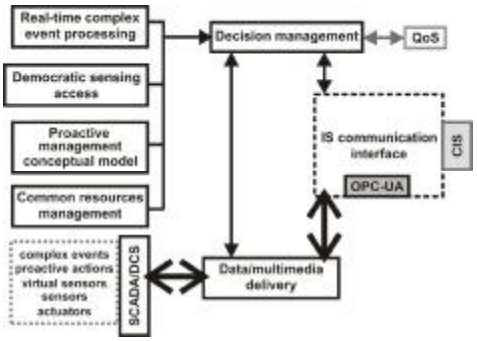

Fig. 3. IS Engine structure and interactions.

Such entities will provide directory services, registration support and access rights to available resources, distributed data management, etc. The interoperation between the decision units is ensured through the adoption of the OPC UA and open standard protocols. OPC UA protocol involves multimedia elements, video streams, mobile sensing elements, that could be included in an ad-hoc federation, assuring exchanging of complex measurements to all entities.

The IS provides different capabilities for confederation: flexible communications architecture programming that supports multimedia content delivery, democratic access to sensing entities, complex event processing, and complete management model.

Sensor networks exploitation advantages offered by the federation are: compensation for the lack of certain sensors, sensors calibration, virtual sensor creation through synthesis information from actual sensors or simple easy replacement.

SCADA federation ensures optimal management of huge data sets by CEP technology, integration of run-time models, real-time information for external decision factors in case of a disasters/abnormalities.

The overall federation QoS is increased, based on CIS capabilities. SCADA federation deals with specific issues:

- federation scalability: is not equivalent with simply totalizing facilities from the component SCADA systems (there are a lot of redundant capabilities);
- data fidelity and integrity; all the information is gathered from databases only (avoiding direct access to sensors). Data integrity is evaluated at multiple levels. Data integrity provided at the level of SCADA systems, have to be reflected at the superior hierarchical level.
- data aggregation from different sources using a great variety of communication protocols and giving access mechanism to the programs of another federation member.

5. SCADA FEDERATION vs. CRITICAL SYSTEMS

The SCADA federation brings benefits for all types of critical systems and represent a solution to decrease the criticality of all the members using the envelope functions:

- Sensing optimization;
- Complex Event Processing (CEP);
- Run-time models.
- Critical systems proactive approach;

Sensing optimization: creating a tool for democratic access to all the federation sensors involves the definition of the metadata categories (XML based) for each sensor, publishing the sensors features/parameters and enabling a query mechanism to inform about their availability.

The federative tool involves coordinating and scheduling tasks for errors detection, optimizing the use of capabilities and resources, managing the sensor data aggregation and correlation, assessing the situation, adapting sensor networks and reducing operator intervention.

The sensing optimization allows the members of the federation to borrow a sensor or his data from a valid system when their own are not accessible or is damaged. It assures the data for specific sensor auto-calibration, linearization, errors compensation.

Sensing optimization offer the possibility to create a virtual sensor using virtual measurements collecting data from other existing sensors and using the resources of the available models shared between the federation members. Virtual sensing technology provides improved monitoring and control by virtual measurements, predictive capability, robustness to sensor failure.

The sensing optimization function determine the decreasing of criticality by substitution of some sensors that are not valid using the interpolation methods, algorithms and existing data and models own by an other valid measuring system member of the federation. As a federation envelope function, it provides redundancy of data and enables each SCADA system owner to address relevant issues, imposed by critical events. Sensing optimization contributes to SCADA system interoperability and to the systems mission-critical aspects reduction by processing the available data of the operational infrastructure and sharing the results to all the federation members substituting the missing data or sensors failure own by a certain system.

Complex Event Processing (CEP)

The CEP system “collect the events data from numerous SCADA/DCS entities on ongoing base and use algorithms and rules to determine in real time the interconnected trends and patterns that combine them into complex event”.

The SCADA federation represent an effective support to implement CEP procedures by providing the following premises:

- multiple surveilling leyers and directly real time connection of data streams from sensors;
- modular and flexible communication infrastructure;
- each SCADA systems included into the federation ensures the model of its controlled process and through the federation multiple model enhanced capabilities are available to be shared to all the members

The added value provided by CEP implemented at the federation level decrease the criticality of the systems by the

detection of some complex events which can not be observable by a single SCADA system (Luckham, 2002). The difference between traditional SCADA post-processing techniques and the new CEP is that all the functional components of the engine run in a single analytic generation process.

The federation CEP features enhances the pro activeness of the system, and on the other hand facilitates the real-time analysis of continuous growing data volume.

The ability to incorporate real-time information and complex event patterns into federative decisions is a critical task. CEP solutions, together with significant historical information (from analytics processing), can be used to enable the predictive capabilities, decreasing considerably the critically degree of the entire SCADA federation using the synthesis of complex events offered by a certain SCADA system for an other member of the federation. CEP techniques decrease the criticality, preventing loss of sensitive information, assuring the context for proactive decisions.

Run-time models. SCADA systems are distributed in large area, operating in heterogeneous and rapidly changing environments. The remote surveillance and the need for consistency of data impose to these systems to be flexible, adaptable, reconfigurable, and to implement a self test and self-managing procedures. All of this requirements or attributes make systems increase the risk to failure. The implementation of appropriate mechanisms for runtime monitoring offer better visibility for the system and help to avoid damage determined by the sensing failure which are substituted by adopted run time models. The federation structures have to evolve at runtime among existing configuration and a new one, during a secure transition (activated by signals as: context changes, user choices).

The run-time model offers a valuable semantic support for real time operation and critical decision linked to system parameters adjustment with positive influence on safety critical systems management.

The systems implemented in large area having impact on environment should have effective adaptation, and reactivity to the parameter changes. The adaptation feature of the system represent a model transformation, that become an adaptive runtime model, in order to determine the final results. In this way federation which integrate metamodels offer a support to decrease the mission-critically aspects of the member systems (from a software point of view), by the ability to accomplish the global objectives.

Critical systems proactive approach - SCADA integration process generates a sequence or pattern of possible data security lacks, essential for both safety and business continuity assessment. Critical events are frequently expanded at large-scale; that is why it is necessary to develop practical strategies which assure security of critical systems infrastructures.

The vulnerabilities are connected with the following aspects: remote access; network configurations; security holes, patches, viruses; not encrypted communication protocols; lack of incident reporting.

One challenge in guaranteeing right and predictable federation behaviour is defining a specification for standard behaviour. This involves identification of the important aspects of federation operation, and developing proactive techniques for achieving these properties.

The safety requirements assure that the federation converges to a stable state, implying that infrastructure updates actually correspond to topological changes.

Proactive approach is related to and provides:

§ a model that is scalable to various federation size and easily deployable;
§ methods for identifying the root causes - effect managing root causes rather than the symptoms;
§ an appropriate quantification of the key factors (allows to prioritize the events without introducing errors);

Proactive measures deal with critical situations and business tasks and opportunities, whereas reactive management approach to failure is critical; The pro active measures have a major impact in decreasing overall federation criticality (safety-critical aspect), at the software level, providing tools and strategies for implementation and expansion of systems or new features in a safe way and to secure SCADA systems even though not all utilities make use of these tools.

System reputation involves the degree of trust regarding the system reliability (availability) and data authenticity. The federation reputation is given by the most vulnerable system (being a drawback for the federation). To all types of critical systems: safety critical, mission critical, business critical and security critical, the federative SCADA systems offer a support to decrease their level of criticality.

6. CONCLUSION

The federative mechanisms will enable the safety - critical systems to avoid failure that can lead to risk/ danger or loss of life or real damage to the social or natural environment by the implemented mechanism that enable the partners to borrow resources when they face a real risk situation.

The SCADA federation features offer a solution to the individual mission – critical system to complete its overall system or project objectives when it is in a dangerous position. It receives o real help from the federation that ensures the substitution of the particular system mechanism needed to achieve the objective during a period of time when it is not able to manage the tasks.

The systems that are business-critical systems type which are leading to loss of money or even the business, have find a solution when they join to the federation by the possibility offered to all of the confederated systems, to borrow some data from the database of the partners, by the synergy of the different systems having different functions and capabilities and share their own resources. The security-critical systems which may lead to major loss of sensitive data and exposure at terror attack can have an improved capabilities by the data redundancy as the critical data are stored and protected in multiple access data bases created by partners, and special

mechanism to protect them against attack of the unauthorized operators.

REFERENCES

Azzedine Boukerche, Algorithms And Protocols For Wireless Sensor Networks, *Wiley Series On Parallel And Distributed Computing*, New Jersey, 2009.

Blair Gordon, Bencomo Nelly, Models@Run.Time, IEEE Computer, vol. 42, no. 10, pp. 22-27, Oct. 2009.Professionals, October 2009.

Cohen Bernard, Boxer Philip– Why critical systems need help to evolve, *Computer IEEE Computer Society* – May 2010, http://www.computer.org

Gordon Clarke, Deon Reynders, Practical Modern SCADA Proto-cols: DNP3, 60870.5 and Related Systems, IDC Technologies, 2004.

Jamshidi Mo, System of Systems Engineering: Innovations for the 21st Century, John Wiley & Sons, 2009.

Leavitt N., "Complex-Event Processing Poised for Growth", IEEE Computer, vol. 42, no. 4, pp. 17-20, Apr. 2009.

Letia T. S., Hulea M., Sisteme de control distribuit, Ed. Mediamira, Cluj-Napoca, 2005.

Lorcan Coyle, Mike Hinchey and Bashar Nuseibeh, Jose Luiz Fiadeiro, Evolving critical systems – Computer IEEE Computer Society– May 2010 , http://www.computer.org

Lorcan Coyle, Mike Hinchey, Evolving critical systems – University of Limerick, Ireland, Lero Technical Report Lero-TR-2009-00– July 2009.

Luckham David, The Power of Events - An Introduction to Complex Event Processing in Distributed Enterprise Systems, Addison-Wesley, May 2002.

NCS TIB 04-1, Technical Information Bulletin 04-1, National Communications System, SCADA systems, October 2004.

Stoian I., Stancel E., Ignat S., Balogh Sz., Dancea O. - "Federative SCADA Consideration", IEEE Catalog Number: CFP10AQT-PRT, ISBN: 978-1-4244-6722-8, 2010 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR 2010), THETA 17th edition 28th -30th May, Cluj-Napoca, Romania.