Cristian Silviu BANACU
Bucharest University of Economic Studies
Emilian Cristian IRIMESCU
Bucharest University of Economic Studies

SCADA AND SECURITY DISPATCHES ACCORDING TO PRESENT LEGISLATION IN ROMANIA

Methodological article

Keywords:
Security
Management
SCADA
Dispatch

JEL Classification
M19, M10

Abstract

SCADA is an old term, older than twenty years, used for defining systems that acquires data from industrial networks and / or critical infrastructure networks and process them for operational and security purposes. Its importance is growing simultaneously with the development of technology's interference in our lives (social life, economical life, etc.).
Although they are not defined as SCADA systems, Security dispatches (and their structure) have a lot of similarities with the general architecture of SCADA systems.
Taking into consideration the security dispatches, as they are accepted by the actual Romanian law, we will draw a parallel between them and SCADA architecture, identifying the similarities and the differences between them, and also the points where some changes could be made.

1. INTRODUCTION – SECURITY AND SCADA

The past ten years are characterized by an important transition in our life, in our social and economic life, from the classical ways of doing things to automatized and technological ways. These days, technology is everywhere, and almost all aspects of today life are computerized.

If we say that security is not an exception, SCADA systems are the expression itself of technology penetrating our day by day life and business.

While first security activities took into consideration clear and local sites, with SCADA the security operations move to the next level, taking into consideration industrial networks and critical infrastructure networks, with a major impact for the life and society from many points of view (Radvanovsky, 2013).

1.1 Security, security systems and Security dispatches to SCADA

In the security history, electronic security is the first recorded step after the first classical security approach. If security is a term that exists (in various forms) from the beginning of civilization, electronic security is a term that is more present in our lives starting with the 80's and 90's. The first video cameras and the beginning of television coincide with the first CCTV systems (Close Circuit Television).

Moving forward, based on electronic security systems and new telemetry technologies, and also based on first SCADA systems, we have the onset of the SCADA used for security purposes.

In fact, based on SCADA architecture, the industrial networks and critical infrastructure networks operators started to develop tools that also protect them, in parallel with monitoring the networks. After that, that principle was also developed to other applications, not only for industrial and critical infrastructure networks (in fact the industrial network term, as presented in literature (Knapp, 2011) was extended to other commercial activities – video surveillance based on IP technology is an example for that). Another result of this is the Security dispatches, both for alarms and video surveillance.

Security dispatches, as they are accepted by our legislation, are central stations, based on servers and databases (the hardware and software components) that communicate all over the country, with secured protocols over some communications mediums (internet, wired, radio, etc.) with alarm control panels installed in remote locations (control panels connected to various detectors). Maybe this definition seems quite unclear at this moment, but it will be clearer when we will analyze the SCADA general structure.

1.2 SCADA - general notions

SCADA is a general technical term that defines a system which acquires data from several terminals and processes them in a central station. The name came from Supervisory Control and Data Acquisition.

First, SCADA systems were used in industrial processes. Now, there are a lot of applications for SCADA, like infrastructure networks (water, oil, gas, etc.), facility processes (heating, security, access, energy consumption, etc.). In fact, today SCADA systems are part of the industrial networks, as they are defined in the literature (Knapp, 2011).

Each SCADA system has several general components, as shown in the next image – figure 1.

Later (in this paper) we will use this architecture to draw the parallels between SCADA systems and Security Dispatches.

In general terms, the four main components represent:

- Sensors: various types of sensors, specific to the activity that is monitored by the SCADA system. For example, there can be temperature sensors, pressure sensors, flow sensors, etc.
- Automation: devices that can automatic control different processes (temperature, fluid flow, etc.);
- Remote control units or Programmable logic controllers: here we refer to electronic devices that convert data from sensors into digital information, information that will be sent to the control center.
- The control center (also called master control system (Radvanovsky, 2013)) is the brain of the SCADA system. Here all information is centralized, and decisions are made based on logical criteria.
- Human interface: with the human interface (generally PC units) operators can administrate the control center and also operate it.

Communication between sensors and remote control units and the communication between remote control units and the control center can be wired or based on a telemetry system. In the second case we can talk about SMS, GSM or GPRS technology (or other communication solutions).

SCADA systems have some general features. We nominate here some of them:

- SCADA systems are centralized systems, which have a central hardware and software platform and a variety of sensors (inputs) and automation (output action);
- Technically speaking, SCADA systems are systems based on a data base. This fact is direct linked to the centralized aspect of SCADA and is a technical reflection of it;
- SCADA systems are built to cover large areas (long or wide);
- SCADA systems are open systems, which can be modified in time, updated or modified according to new necessities or problems. For this we consider physical modification (quantitative)

and / or structure modification (logical actions from the control center);

- SCADA systems are reactive systems, which can in an automatic way react to some detected situations (according to the rules from the control center). In some cases, SCADA systems can also be proactive systems, but only in case in the control center is used a heuristic approach and not a logical one. In this case we have systems with initiative, term that is frequent used in correlation with the heuristic approach (Golu, 1975);

According to last trends in technology more and more specialist talks about Next Generation SCADA. This is a hybrid between SCADA and cloud computing. In fact the system is quite the same, only the servers and the data base (complete or partial) being in cloud.

Another trend in today's technology is mobility. SCADA also adopted this new feature, integrating new portable devices (smartphones, tablets, etc.) into the human interface category (Figure 1).

1.3 Legislative framework and organizations

The main law governing security activities and also security dispatches in Romania is Law no. 333 from 2003, regarding guarding of objectives, good, valuables and personal protection. This law was completed in time by some additional acts, like Law no. 40 from 2010, Government decision no. 301 from 2012 and some other minor decisions.

The main Government decision that defines the security dispatches activity is decision no. 301 from 2012. In Chapter VI we have full details about the functionality of this activity.

Strictly regarding the SCADA systems, we do not have in Romania any law to regulate this technology.

The main European standard regarding security dispatches (alarm monitoring and receiving center) is SR EN 50518:2011 (requirements for the location and construction, technical requirements, procedures and requirements for operation). This standard is also adopted as a Romanian standard.

In Romania, the most important association for security technology is ARTS (Romanian Association for Security Technique) and another security association (this time an international one) is ASIS International. Regarding SCADA there is no professional associations directly linked to this domain. Generally, IT & C associations also approach this domain.

Internationally we can find some standards regarding SCADA systems, but mostly for critical infrastructure systems, and not necessarily with a security approach. Examples are NERC Standards, which practically refer to critical infrastructure and how to protect it. The Nord American non-profit organization standards refer to Physical Security, Incident Reporting, Personnel & training, etc.

Also regarding SCADA we can talk about ISA – 99, an important set of automation standards, issued by The International Society for Automation. Its role is to protect SCADA (and indirect the industrial network or the critical infrastructure network) and to create a mainframe for this activity.

2. KNOWLEDGE STAGE

2.1 Knowledge stage in security systems

Thegoalof this paper is to underline the involvement of technology in security. Therefore, we will outline some works about electronic security from other countries, because in our country this type of literature practically doesn't exist.

Unfortunately, there are not too many international books about Security dispatches either. Generally, we find books about video surveillance and security, like Closed Circuit Television by Joe Cieszynski and Digital Video Surveillance and Security by Anthony C. Caputo, and books about general surveillance, like Surveillance and Threat Detection: Prevention Versus Mitigation by Richard J. Kirchner, Jr. Obvious, all these are the base of security dispatches. Unfortunately they are not considered as a whole and presented from an integrated approach.

2.2 Knowledge stage for SCADA

If Romanian literature is very weak developed regarding SCADA systems, international literature abound in books about SCADA and SCADA with security applications and security interference. Handbook of SCADA/Control Systems Security, by Radvanovsky and Brodsky is an example that presents SCADA notions, starting from information security, but with references to Physical Security Management, Risk Management, etc. The book also presents the security treats for the SCADA system itself, this being a major operating issue.

Another book, but better focused on security for critical infrastructure than on its security is Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems by Eric Knapp. The book underlines an approaches directly the importance of securing industrial networks.

From what could be seen from the international literature, we can observe a double way between security and SCADA: security with SCADA and security for SCADA. Both approaches are very important and only with them together there could be a satisfying result for big industrial networks.

3. A PARRALEL BETWEEN SCADA AND SECURITY DISPATCHES

To understand how SCADA systems and Security dispatches interferes, we will analyze this topic from two points of view. First, we will try to identify from the structure approach how Security

dispatches as accepted by our actual law are similar with SCADA systems and second we will analyze how the functionality of Security Dispatches is similar with general SCADA functionality structure.

3.1 Structural approach

As described in the previous chapter, SCADA systems have some main components (parts). These parts are: sensors and automations, remote control units, a control center and one or more human interfaces. Next we will analyze for each of these components the correspondent of a Security dispatch.

Sensors: for this category we have for Security dispatches a lot of detectors, based on many technologies. For example, we have presence detectors, based on infrared or Doppler technology, infrared barriers based on infrared technology (infrared beam), pressure sensors, glass break sensors based on sound detection, smoke detectors, etc.

Automation: this is the part where SCADA is not very well represented. We have only a few devices used to action remotely (in case of smoke detection to open some smoke windows, unblock doors, etc.).

Remote control units: the correspondent for this SCADA component is the alarm control panel. Its function is to transform the information from the detectors in analogical information and to transmit it (wired or on telemetry system) to the control room. Also, the alarm control panel can command some automation like unblocking doors, opening windows in case of smoke, etc.

Regarding telemetry system, even the communication medium is a classical one (radio, internet, LAN, etc.) in both cases (standard SCADA systems and Security dispatches) the structure design assume protocols for communication. These protocols can be standard or customized communication protocols.

Control center: for this term we have a high similitude between general SCADA systems and Security dispatches. In both cases we talk about servers, with backup features, running with software built on databases structures.

Human interface: this part is more important on Security dispatches than on SCADA systems. The difference appears from due to human factor. On Security dispatches, human factor is still very important, and sometimes is very important in decision making. For SCADA systems, the human factor is not so important in decisions, generally decisions are automatically taken, and human factor is more present with an observer role and as operator for the logical rules for the server.

3.2 Functional approach

Regarding functionality, we will focus on the features presented in chapter about general notions.

- centralized systems: both general SCADA and Security dispatches are centralized systems, based on a server running a database application;
- open systems: on Security dispatches we can monitor as many alarm control panel we want. The structure is open, also from a quantitative approach, regarding the type of the control panel and regarding the communication type (wired or telemetry);
- reactive systems: based on a logical approach (and not a heuristic one) Security dispatches react to different sensors via alarm control panels;
- communication protocols: also SCADA systems and Security dispatches use standard or customized protocols to communicate between the controllers (or alarm control panels) and the central station;

4. ECONOMIC ADVANTAGES OF SECURITY DISPATCHES AND SCADA SYSTEMS

When we talk about the advantages of using SCADA systems we practically refer to the advantages of using automatic control and commands instead of using human interface systems with human surveillance and decision.

If the advantages of automatic control and decision are hardly quantifiable, the advantages of automatic data acquisition, almost in real time and from a wide geographical area are incontestable and with an important economic impact.

To understand that we will use a short example provided by the electric energy industry. A good example can be the photovoltaic networks, with 20 or 30 sites spread across hundreds of kilometers. In the case, for the maintenance engineers the challenge is to find as soon as possible all the power failure alarm notifications and to diagnose and fix the problems. The best solutions for this situation is to integrate all this sites in a SCADA system, to have real time monitoring and also remote diagnose for the Programmable Logic Controllers. In this case the photovoltaic network problems will be found almost instant and all the losses from the power failure will be reduced. Same time, all the cost with the labor of service engineers will be reduced.

In parallel with SCADA systems, Security dispatches have the same economic advantages. We can talk here about substituting labor (guarding services) with remote surveillance, a change with huge cost impacts. Also, from a technical approach, the remote monitoring of many parameters of the alarm control panels and sometime even remote trouble-shooting can be cost saving.

These two examples underline in a general manner the economic advantages of using SCADA and Security dispatches.

5. CONCLUSIONS

Taking into consideration the general structure of SCADA and the general structure of a Security Dispatch, we can extract a first conclusion, according to witch Security dispatches, as they are accepted by our actual law, can be defined like SCADA systems. Their structure and also their functionality are highly similar, in proportion of about 90%.

On the other hand, looking to the complexity of a SCADA system, applied for example on critical infrastructure networks, we can observe a lower complexity at Security dispatches than at SCADA systems.

These conclusions can be also applied to other security dispatches, for example at national video surveillance dispatches (not local dispatches).

An important issue that can be improved based on the SCADA example is the limitation of the human factor. At this moment, the human factor is still very important for Security dispatches. It would be desirable that, in a few years, the legislation and also the technology to minimize the interference of the human factor.

6. REFERENCES

[1] ARTS.(n.d.).*Legislatie*, Retrieved November 11, 2014, from http://www.arts.org.ro/pagini/legislatie.php

[2] ASIS Online.(n.d.).*Standards & Guidelines*, Retrieved November 11, 2014, from https://www.asisonline.org/Standards-Guidelines/Pages/default.aspx

[3] AUTOMATION.(n.d.).*Reducing Labour Costs and Increasing Investor Confidence with Real-Time Monitoring of Photovoltaic Energy Network,* Retrieved November 13, 2014, from http://www.automation.com/pdf_articles/controlmicrosystems/SE-SUCCESS_STORY-_POWER-PHOTOVOLTAIC-V001.pdf

[4] Caputo, A. (2010). *Digital Video Surveillance and Security.* Burlington: Butterworth-Heinemann

[5] Cieszynski, J. (2007). *Closed Circuit Television.* Manchester: Butterworth-Heinemann

[6] Golu, M., (1975). *Principii de psihologie cibernetică*. Bucuresti: Editura Stiintifica si Enciclopedica, 166

[7] ISA.(n.d.).In*ISA – The International Society for Automation*. Retrieved November 09, 2014, from https://www.isa.org/

[8] Kirchner, R. (2014). *Surveillance and Threat Detection: Prevention Versus Mitigation.* Waltham: Butterworth-Heinemann

[9] Knapp, E. (2011). *Industrial Network Security.* Waltham: Syngress, 7, 8

[10] NERC.(n.d.).In*NERC*. Retrieved November 09, 2014, from http://www.nerc.com/Pages/default.aspx

[11] Radvanovsky, R. & Brodsky, J. (2013).*SCADA / Control Systems Security*. Boca Raton: CRC Press, 31, 33

[12] SCADA.(n.d.).In*Wikipedia*. Retrieved November 10, 2014, from http://en.wikipedia.org/wiki/SCADA

[13] TELEMETRY.(n.d.).In*Wikipedia*. Retrieved November 12, 2014, from http://en.wikipedia.org/wiki/Telemetry

Figure 1, Structure of SCADA