Computer Aided Risk Management of Large Combustion Plants

ENESCU, Marian
Faculty of Economics and Business Administration
University of Craiova
enescu.marian@yahoo.com

Abstract

This paper considers the risk management of Large Combustion Plants (LCP) by specialized information systems. A Computer Aided Risk Management System (CARMS) based on SCADA systems and data management procedures, Human Resources Management, and Security Management is proposed. Data models about risks, and their treatment are recorded by special registers/directories. This paper describes the CARMS-LCP requirements and features to be implemented in order to assist top management of LCP based enterprises.

Keywords: *LCP, SCADA, computer aided risk management, data modelling, information systems modelling*

AMS Classification: Primary 68U35; Secondary 68N01.

1. Introduction

The activity optimization of the business agents operating LCP (Large Combustion Plants) under risk factors is important not only from the perspective of economic efficiency, but also in terms of security and environment protection. The LCP organization's performance management is a process designed to improve both the performance of each employee, each decision-maker of the team involved in analysis or decision group, effectively the entire organization, and is led by the hierarchical management.

This paper considers the risk management of Large Combustion Plants (LCP) by specialized information systems. A Computer Aided Risk Management System (CARMS) is proposed based on SCADA systems and data management procedures, Human resources management (HRM), and Security management (SM). Data models about risks, and their treatment are recorded by special registers/directories. The proposed data models and described in the next sections. The HRM component is common to any Computer Aided Risk Management system and is not detailed here. The LCP Security management is considered in the third section due to the Information and Communication Technology Risks associated to SCADA Systems, and general software systems.

2. **LCP Risk Register Data Models**

The implementation of a risk management system based on ISO 31000 [8] for LCP requires both a clear specification of objectives and their description in the Register of objectives (LCP.RO), identifying risks and maintain registration in a register of risk and decision makers. Identification of decision is part of the general management.

Risks will be analyzed in all structures of the organization, as literature recommend [2, 4, 6, 10], each risk is studied by establishing consequences and plausibility in order to assess the impact on objectives [7]. Monitoring LCP risks is based on LCP Risk Register (LCP.RR). Obviously, the content of LCP.RR is established by the identification of those threats that could lead to failure of objectives, if they materialize.

Risks are identified from anywhere before there exists dangers in meeting objectives and specific measures can be taken to resolve the issues raised by those risks [5, 6]. Setting registry entries, as far as possible, requires the temptation of establishing indirect causality.

Risk register is based on the data contained in the Risk Alert Sheet (RAS) and Risk Monitoring Sheet (RMS) which are described below.

The results shall be recorded in the RAS to cover [7]:

- the RAS.ID of ID.TYPE,
- the risk identification code [RAS.RIC of RIC.TYPE],
- the description of the identified risk [RAS.DESCRIPTION of DESCRIPTION.TYPE],
- the circumstances that favour the emergence of risk [RAS.CIRCUMSTANCES of CIRCUMSTANCES.TYPE],
- the description of the impact[RAS.IMPACT of IMPACT.TYPE],
- the assessment of inherent risk (*impact*: low, medium, high, *probability*: low, medium, high; the exposure, *the risk profile*: ignorance, prudent, action) [RAS.RINHERENT of RISKEVAL.TYPE],
- the description of the treatment risk preventive actions [RAS.TREATMENT of TREATMENT.TYPE],
- the presentation of control instruments [RAS.TOOLS of TOOLS.TYPE],
- the responsible person for managing risk [RAS.RESPONSIBLE of RESPONSIBLE.TYPE],
- the deadline to start working [RAS.DEADLINE of DEADLINE.TYPE],
- the description of secondary risks [RAS.SECONDARY of SECONDARY.-TYPE].

As an example RISKEVAL.TYPE is a structure (record) having three fields: def(type) RISKEVAL.TYPE as record { ptype probability in {1, 2, 3}; itype impact in {1, 2, 3}; etype exposure; }, but other data types mentioned above are intuitive and will be not detailed in this paper.

Risk profile is obtained as the product of probability and score points attributed to impact [2]. Risk register is used during risk monitoring. Action monitoring has the effect that it had on the risk measures and the results shall be recorded in RMS.

The RMS component of LCP.RR covers the following data:

- the RMS.ID of ID.TYPE,
- the LCP organization [RMS.ORGANISATION of ORGANISATION.TYPE],
- the description of monitored risk [RMS.DESCRIPTION of DESCRIPTION.TYPE],
- the responsible person for monitoring risk [RMS.RESPONSIBLE of RESPONSIBLE.TYPE],
- the interval time of monitoring [RMS.DURATION of DURATION.TYPE],
- the list of initial actions [RMS.INITIALLIST of LIST.TYPE],
- the impact of initial actions [RMS.INITIALIMPACT of INITIALIMPACT.TYPE],
- the risk reevaluation [RMS.RISKEVAL of RISKEVAL.TYPE],
- the list of corrective actions [RMS.CORRECTIVELIST of LIST.TYPE],
- the list of RMS register responsible staff [RMS.CHECK of CHECK.TYPE],

where the CHECK.TYPE is a table containing details on staff participating in the elaboration, verification, and approving of RMS. Other data types are quite intuitive and will be not detailed here.

If it is found a modification of the risk profile then the new profile will be recorded in LCP.RR. At the management level of the organization the responsible for maintaining LCP.RR has the following responsibilities and competence [7]:

- To collect data for alert to risks and risk monitoring sheets, the RAS and RMS.
- To record data on risk alert data sheet and risk monitoring sheet.
- To keep track of received and archived documents.
- To make available the Risk Register for auditing activities.

3. LCP Security Management

The quantitative risk analysis, extended to LCP security, involves the following steps:

1. Identification and evaluation of assets of operators LCP organization;
2. Identifying and assessing vulnerabilities for each asset individually;
3. Identify and evaluate threats for each vulnerability;
4. Estimate the probability of manifestation of threats, namely the faults;
5. Calculation of expected annual losses;
6. Analysis of security measures;
7. Calculate the return on investment in security.

The following section will highlight the above elements and relations. This section describes a specific asset of LCP computerized systems: SCADA system.

According to [3, 9], a SCADA system can be defined either as a technology of data acquisition processes / equipment / remote stations and remote control devices, either as a real-time operating system to control terminals remote (RTU – Remote Terminal Unit).

The basic modules of any SCADA system are [9]:

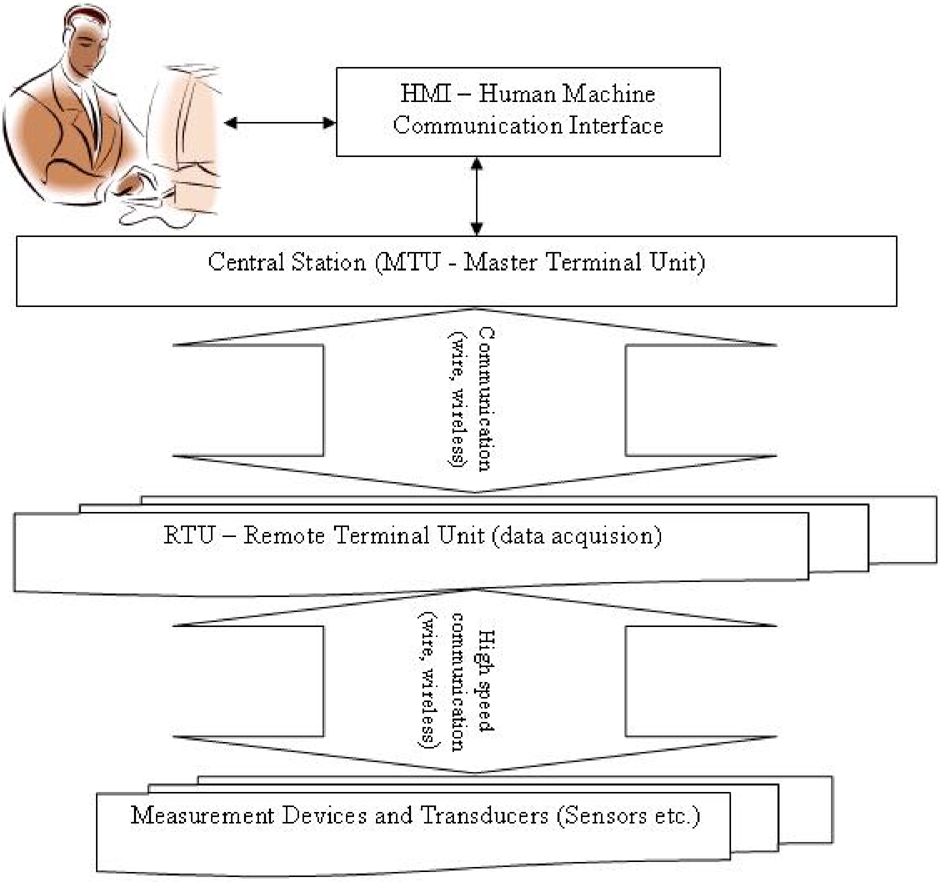
HMI – Human Machine Communication Interface
Central Station (MTU - Master Terminal Unit)
Communication (wire, wireless)
RTU – Remote Terminal Unit (data acquision)
High speed communication (wire, wireless)
Measurement Devices and Transducers (Sensors etc.)

Figure 1: Typical SCADA system

1. The main module (MTU – *Master Terminal Unit*) with the role of presenting the information collected and the transmission of signals to remote units;
2. The local (RTU – *Remote Terminal Unit*) which transmits signals to the devices they control, acquires data and sends them to the main module (MTU);
3. The lines of communication (Internet, wireless or wired telephone network) used for communication between the station MTU and RTU stations. These can be monitored and can act by sending the wrong message by malicious people;
4. The operator interface (HMI – *Human Machine Interface*) through which the operator has access to control and visualization functions through menus, device interaction and graphical viewports; operator – the supervisory role of the SCADA system and the weak link where can be the victim of social engineering.

SCADA software components of any system is, along with the communication, real hazards under control facility, if they contain vulnerabilities. The software architecture of a standard SCADA system, as in [9], is based on a master module (HMI, alarm management, monitoring events, special applications, ActiveX controls or Java) and a slave mode (real-time management system, applications data processing, generating reports, alarms management, drivers and interfaces for control components, spread sheets, logging the transactions, archiving, production of charts and predictions).

Transmission of information by means of specific channels based on the use of specific protocols must not be vulnerable.

Evolution of SCADA systems from proprietary hardware and software platforms for data acquisition systems and data processing in real time using communication protocols on the network (wired or wireless) made it possible to identify, for the latter category of systems, vulnerabilities that favour attacks. Of the many known cases in the literature ew mention penetration from the outside, using a laptop computer, the control system of a power unit by employees of consulting firms (Paul Blomgren) employed to assess the cybersecurity of this unit [9]. Because SCADA systems uses the most current computer equipment and communication networks, in Table 1 are highlighted the performance requirements of SCADA/LCP compared against standard systems (SIS).

The common risks of LCP are described in [6, 7]. The list of risks is updated to cover the major risk elements to SCADA systems: connections to vulnerable networks, the usage of hardware platforms and/or software with known vulnerabilities, real-time requirements affected by delays of information security controls.

The list of threats to SCADA systems covers the following items: improper application of software patches, malware (autonomous worms, viruses, trojans, etc.), attacks (Distributed-denial-of-service, terrorists), electromagnetic interference, accidents, human errors, disruption of utilities, radio frequency interference, noise on power lines, improper maintenance actions, natural disasters, etc.

LCP Security management is based on procedures, information files, and hardware and software tools. For the aim of this paper only software aspects are detailed. Based on a procedure in 21 steps, described in [9] the cybersecurity of SCADA systems can be continuously improved and managed using the LCP.SM component:

1. Develop a rigorous risk management process based on principle of defence-in-depth to meet the security requirements along various configurations [LIST.OF.PRINCIPLES, LIST.OF.SECURITY.REQUIREMENTS, LIST.OF.CONFIGURATIONS].

2. Identify and evaluate every connection to SCADA networks: LAN, WAN, Internet, wireless, modem, dial-up, other types [LIST.OF.NETWORKS].

3. Optimize the set of connections by removing unnecessary connections, but maintaining the availability of services according to the requirements [LIST.OF.CONNECTIONS].

Table 1: SIS/LCP Performance Requirements

No.	Type Performance requirements
1	SIS : Tolerance data loss and disruptions (back-up procedures and restarts) is permitted. LCP: packet loss and communication interruption can not be tolerated. There is a risk of destruction of facilities and loss of lives.
2	SIS: Although recommends enhanced data transfer performance, any delay can be allowed and compensated. LCP: systems work and time loop forced response; sensors and various subsystems must respond in real time; delays or failures are not tolerated.
3	SIS: recovery from damage can be done by rebooting, possible failures do not have major consequences. LCP: systems must be fault-tolerant through specific techniques, any failures can have major consequences.
4	SIS: the usage of antivirus scanning programs and programs with abnormal behaviour is accepted. LCP: the usage of monitoring software (including antivirus) can lead to delays in system response, and these delays are not acceptable.
5	SIS: standard computer systems are using cryptography methods. LCP: SCADA systems do not use cryptographic methods.
6	SIS: the usage of the usual tests on penetration. LCP: penetration tests can not be used or rarely used to not introduce delays in the normal functioning of the system.
7	SIS: software packages that are used to repair any defective functionalities. LCP: not use repair software packages, and if this is done only by using the cooperation with suppliers of SCADA system components.
8	SIS: security audit system is performed periodically. LCP: not use security audit procedures.
9	SIS: information system components are replaced at the latest every five years. LCP: SCADA systems operate without replacing components for long periods of time.

4. Optimize the set of services to be active during operation [LIST.OF.ACTIVE.SERVICES].
5. Check the trustability of communication protocols [LIST.OF.PROTOCOLS].
6. Set all security features of SCADA subsystems to assure the maximum level of security [LIST.OF.SCADA.SUBSYSTEMS.SECURITY.LEVELS].
7. Implement strong mechanisms for secure communications [LIST.OF.MECHANISMS].
8. Implement two level intrusion detection system (IDS) and full incident monitoring [EXTERNAL.IDS, INTERNAL.IDS].

9. Complete auditing of SCADA devices and networks [LIST.OF.SCADA.DEVICES, LIST.OF.SCADA.NETWORKS].
10. Evaluate the physical security of SCADA networks [LIST.OF.NETWORKS].
11. Identify and evaluate possible attack scenarios by a group of experts in field [LIST.OF.SCENARIOS].
12. Define LCP.SM.ROLES, LCP.SM.RESPONSIBLES, LCP.SM.MANAGERS, LCP.SM.ADMINS, LCP.SM.USERS.
13. Document the information security architecture and the security levels in order to assure the maximum protection [SECURITY.DASHBOARD].
14. Implement system backups and disasters recovery plans [LIST.OF.PLANS.AND.CALENDAR].

The above architecture support both the application of OCTAVE approach [1] for LCP, and the requirements of ISO 27001 [11].

5. **Conclusions**

This paper considered the risk management of Large Combustion Plants (LCP) and proposed adequate data models according to ISO 31000 requirements to support security management when SCADA systems are used. The proposed information system, called CARMS, will be an efficient tool able to assure the activity optimization of the business agents operating LCP.

References

1. Alberts C., Dorofee A., *Managing Information Security Risks: The OCTAVE Approach*, Addison Wesley, 2002.
2. Aven T., *Foundations of Risk Analysis. A Knowledge and Decision – Oriented Perspective*, John Wiley & Sons Ltd, 2003.
3. Barnes K., Johnson B., *Introduction to SCADA Protection and Vulnerabilities*, Idaho National Engineering and Environmental Laboratory, INEE/EXT-04-01710, 2004.
4. Bârsan-Pipu N., Popescu I., *Managementul riscului: concepte, metode, aplicaţii*, Editura Universităţii Transilvania, Braşov, 2003.
5. Directive 2001/80/EC, http://eur-lex.europa.eu/ LexUriServ/ site/ en/ consleg/2001/L/02001L0080-20011127-en.pdf, http://eur-lex.europa.eu/ LexUriServ/ LexUriServ.do? uri = CELEX: 02001L0080 - 20070101: EN:NOT
6. Enescu M., *Risk Management Associated to the Environmental Management of Large Combustion Plants (LCPs)*, "Analele Universităţii din Craiova", 1, 61-68, 2012.

7. Enescu M., *On the Evaluation of LCP Associated Risk Management*, "OptimumQ", 1, 2014 (in press.)
8. ISO, *ISO 31000: 2009 Risk Management – Principles and Guidelines*, International Organization for Standardization, 2009.
9. Krutz R.L., *Securing SCADA Systems*, Wiley Publishing, 2006
10. Larsson T.J., *Computer-Aided Risk Assessment: Claims Data as Expert System Support for Industrial Safety Management*, "Safety In Action Conference", http://www.diva-portal.org/smash/get/diva2:429902/FULLTEXT01.pdf, 2001.
11. Vasudevan V. et al., *Application Security in the ISO27001 Environment*, IT Governance Publishing, 2008.