Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

Critical Infrastructures: from risk assessment to identification of improvement priorities

Decision making methodology and tools for an integrated management of water utilities

S.Olivero, M.Migliorini, F.Stirano
SiTI
Torino, Italy

olivero@siti.polito.it,
migliorini@siti.polito.it,
federico.stirano@siti.polito.it

N.Bazzurro
IRIDE Group
Genova, Italy

Nicola.Bazzurro@iride-acquagas.it

D.Savic
University of Exeter
United Kingdom

D.Savic@exeter.ac.uk

Abstract—**Drinking water networks are critical infrastructures for human communities. The strategic importance of case studies in the field of water networks is enhanced by the fact that in general water systems are considered an ideal laboratory to study, apply and test security solutions. The assessment of all potential vulnerabilities, which have to be clearly understood and modeled, is indispensable for the definition of appropriate preventive and corrective countermeasures. Moreover, the continuous risk management of these infrastructures is fundamental for maintaining adequate levels of protection for securing the effectiveness of the countermeasures. Manage the risk of a critical infrastructures means basically 1) to understand organization's information security requirements and the need to establish policy and objectives for information security, 2) implement and operate controls to manage an organization's information security risks in the context of the organization's overall business risks and 3) monitor and review the performance and effectiveness of the system. To ensure an adequate safeness level to the population, it is necessary to study and analyze not only the physical components of a water distribution network, but also the ICT components. For example, computer systems that control the whole infrastructure play a relevant role in guaranteeing the security and safeness of the system and assuring the health of the associated economies. Risk Assessment must include all these aspects to be valuable tool to enable an effective management of water networks.**

Keywords— water networks, risk assessment, water supply chain, integrated security framework, critical infrastructures, cyber threats, process automation control system, integrated management

I. INTRODUCTION

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. Consequently, the failure of these infrastructures can result in critical damage with direct effects on the population.

Examples of critical infrastructure are:

- electricity generation, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunication;
- water supply (drinking water, waste water/sewage, stemming of surface water (dikes and sluices));
- agriculture, food production and distribution;
- heating (natural gas, fuel oil, district heating);
- public health (hospitals, ambulances);
- transportation systems (fuel supply, railway network, airports, harbours, inland shipping);
- financial services (banking, clearing);
- security services (police, military).

Drinking water networks are critical infrastructures for human communities. Large urban areas are becoming more and more vulnerable to a series of threats, both man-made and natural, that are capable of causing major short-term and medium-term catastrophic effects.

Regarding the need to optimize security and protection of networked systems, it is worth saying that the processes of liberalization and deregulation are creating relevant business opportunities. However, one of their organizational effects is the segmentation of the "water supply chain" into a series of domains that are independently owned and managed by private Companies. This state of undefined ruling of the supply chain may result in an increased vulnerability of water networks to events such as maintenance problems, lack of coordination and attacks on specific "rings" along the chain. For this reason, analysis of organizational and cooperation issues are very relevant among different actors, owners and utilities.

The strategic importance of case studies in the field of water networks is enhanced by the fact that in general water systems are considered an ideal laboratory to study, apply and test security solutions. Since they are contexts in which collaboration among the various organizations is required and forced, large amounts of money and resources are allocated, with risks being multiple and interrelated.

The assessment of all potential vulnerabilities, which have to be clearly understood and modeled, is indispensable for the definition of appropriate preventive and corrective countermeasures. Moreover, the continuous risk management of these infrastructures is fundamental for maintaining

978-1-4244-2794-9/09/$25.00 ©2009 IEEE

adequate levels of protection and for securing the effectiveness of the countermeasures.

A crucial point in the system modeling process is represented by the identification of the economical impact of each asset on the whole system. One of the most promising methodologies to effectively assess this process has been presented in [8]. The methodology, called GAasset, aims to optimize the engineering activities and the timing of investment in order to maintain the service level over acceptable thresholds. The goal is reached by means of optimization techniques that represent an efficient way of modeling large multi-dimensional problems and determining the true optimum.

Even if the final goal of the GAasset methodology is different from the risk analysis, it can be useful to perform an economical analysis in order to identify which asset needs to be protected, as a failure could have a significant economical impact.

Unfortunately, this methodology has a major drawback. As with most mathematical models, it is based on a deterministic approach. That is, the impact analysis is conducted assuming that the input variables are known with 100% certainty. However, in real life this hypothesis is too strong, as all real problems include risk and uncertainty in one way or another. Typical uncertainty can be found in field measurement, in the parameter definition or in the model definition. Reference [9] presents an improvement of the GAasset methodology that takes into account the conditions of uncertainty of the real systems.

II. PROCESS AUTOMATION CONTROL SYSTEM

To ensure an adequate safeness level to the population, it is necessary to study and analyze not just the physical components of a water distribution network. For example, computer systems that control the whole infrastructure play a relevant role in guaranteeing the security and safeness of the system and assuring the health of the associated economies.

Control processes typically employ real-time computer systems, with different characteristics and priorities than standard data exchange networks. Typical data exchange applications put the focus on security and confidentiality of the communication, while a real-time system is specifically designed to give priority to performance and reliability, while security is not a primary requirement.

These differences derive from past installations of the control network, where they were completely separated from office networks and their development run in parallel with respect to other types of data communication. However, the emerging need for remote access capabilities and economical considerations has led to the integration of both infrastructures, introducing new serious vulnerabilities into operational system components.

Cyber attacks on a critical infrastructure control network could provoke damage not only to the infrastructure itself or to its company managing, but they could put in danger a lot of economies depending on it. In the specific case of systems that manage public water, a cyber attack could endanger public health and safety as well as invoking serious damage to the environment.

A typical process automation control system is described in Figure 1 [3]. Measurement variables are transmitted to the controller from the process sensors. The controller interprets the signals and generates corresponding control signals that it transmits to the process actuators. Process changes result in new sensor signals, identifying the state of the process, which are again transmitted to the controller. The Human Machine Interface (HMI) allows a control engineer or operator to configure set points, control algorithms and transmit parameters to the controller. The HMI also provides displays of status information, including alarms and other means of notifying the operator of malfunctions. Diagnostic and maintenance tools often made available via modem and Internet enabled interfaces, allow control engineers, operators and vendors to monitor and change controller, actuator and sensor properties from remote locations. Following this schema, a malicious agent could attack any of the elements described above. Due to the various interconnections the consequences could spread throughout the entire system causing a great deal of damage to all the controlled process and, indirectly, to the population served by the water distribution center.

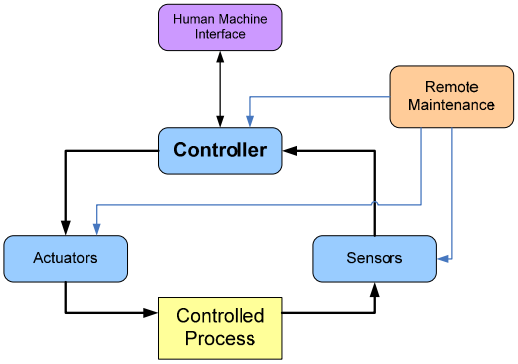

Figure 1. Example of a process automation control system.

During the last ten years, several international bodies have been working hard to provide a standard, or at least some guidelines, in order to improve the overall security level of the critical infrastructure control systems. Among them, the most active bodies seem to have been the International Society of Automation (ISA) and the International Organization for Standardization (ISO).

The ISA99 Committee tries to provide some guidelines to follow to improve the cyber security level of the control network in an industrial automation process. In its Technical Reports ([4][5]), it is stated that the security plans for industrial production and control can be developed using experiences, plans and practices adopted in standard IT systems. However, they have to take into account a series of

differences that, for example, could prevent the adoption of strong encryption measures on the transmitted data. A strong data encryption could introduce too much delay with respect to the time constraints tolerated by a real-time system, such as a control network for water distribution systems.

The ISO/IEC 27000 family has been specifically prepared to provide a model for establishing, implementing, monitoring, reviewing and improving an Information Security Management System (ISMS). Using this approach, the security is studied at process level, where a process is defined as any activity using resources and managed in order to enable the transformation of inputs into outputs. The Standard employs the "Plan-Do-Check-Act" model, based on four basic operations performed cyclically:

- Understanding an organization's information security requirements and the need to establish policy and objectives for information security;
- Implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;
- Monitoring and reviewing the performance and effectiveness of the system;
- Continual improvement based on objective measurements.

III. HUMAN AND NON-HUMAN THREATS

The research permitted the construction, application and validation of a methodology for the assessment of the risk of drinking water supply infrastructures.

Criteria for identification and classification of assets of water supply infrastructures, such as physical sites, catchments, conveyors, treatment plants, distribution, control centres and laboratories, were defined. Threats against water systems were identified, considering categories including:

- *Man-Made Non Deliberate*: accidents, malfunctions, urban wastes, industrial wastes, agriculture wastes;
- *Antagonist*: Malicious CBRNE (Chemical Biological Radiological Nuclear and Explosive) carried out by both insiders and outsiders, hacking attacks against ICT control & telemetry systems, sabotage on distribution networks;
- *Technology*: electricity failure, pipeline break, system failure;
- *Natural*: floods, earthquakes, landslides, fires, extreme weather condition;
- *Other*: maintenance problems due to the segmentation of the supply chain related to privatization processes, procedures & operating rules, organization, personnel behavior.

Emphasis was placed on human-related threats, but the approach could easily be extended to non-related ones.

For each of the above mentioned threats, criteria to assess severity levels were defined, assessing the potential entity of damages from economic, logistic and socio-cultural points of view.

A vulnerability assessment has been performed, identifying the level of protection of assets against each of the identified threats and characterizing the level of effort (resources and capabilities) required by the Water Utility to re-activate the asset.

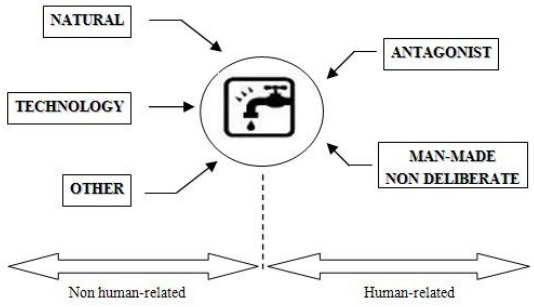

Figure 2. Human and Non-Human threats.

IV. CYBER THREATS AND VULNERABILITIES

Because of the increasing sophistication of computer attack tools, an increasing number of actors are capable of launching nationally significant assaults against critical infrastructures. Water distribution systems can be considered valuable targets, as an attack does not solely affect the infrastructure itself, but the consequences can directly effect the population.

Cyberspace provides a means of organized attack on infrastructure from a distance. These attacks require only commodity technology and enable attackers to obfuscate their identities, locations and path of entry. Not only does cyberspace provide the ability to exploit weaknesses in critical infrastructures, but it also provides a fulcrum for leveraging physical attacks. This is done by allowing the possibility of disrupting communications, hindering defensive or offensive response, or delaying emergency responders who would be essential following a physical attack ([6]).

Sandia National Laboratories has conducted a pervasive vulnerability assessment for IT systems with the main focus on control and automation systems used in critical infrastructures ([7]). Most security vulnerabilities in infrastructure include failure to adequately define security sensitivity for automation system data, identify and protect a security perimeter, build comprehensive security through defense-in-depth and restrict access to data and services by authenticated users based on operational requirements. Many of these vulnerabilities result from deficient or nonexistent security governance and administration, as well as budgetary pressure and employee attrition in system automation. Finally, automation administrators themselves cause many security deficiencies, through the widespread deployment of complex modern

information technology equipment in control systems without adequate security education and training.

Following the classification provided in [7], the vulnerabilities can be divided into five categories:

- *System Data*: Data is the fundamental element in any information architecture. System security is applied to preserve data attributes such as availability, authenticity, integrity and confidentiality, which ensure the reliable operation of the overall information system.
- *Security Administration:* The cardinal element is the system security policy, which prescribes the goals and responsibilities for security. The security policy is the genesis for every other requisite administrative component, which subsequently prescribes procedure for system implementation, operation and maintenance.
- *Architecture:* The architecture for the distribution of automation functionality is critical for reliability of the functional whole. At one extreme, totally centralized authority for automation means that remote stations function as little more than boundaries for analog and digital control and measurement signals (such as the traditional model in industrial automation). At the other extreme, completely decentralized authority resembles the agent model, where operations depend on the emergent behavior of smaller entities with limited capabilities and viewpoints
- *Network:* Control systems networks include all data transmission elements wholly owned and administered by the utility, in addition to data transport functionality of external networks traversed by data. Networking devices can include lower-level end communications equipment, advanced networking devices and the link equipment itself. Network functionalities include the capability of the network to deliver messages securely and reliably to support system operation.
- *Platforms:* These are the computing hardware (inclusive of specific industrial platforms) and software (applications and operating systems) in control systems.

V. RISK ASSESSMENT METHODLOGY IN THE WATER NETWORKS AREA

Research activities were performed to address the question of how to evaluate the risk exposure to all the possible threats (natural threats as well as malicious threats). The research takes into account the whole supply chain: catchments, conveyors, treatment plants, distribution, control centers, laboratories, etc, also analyzing the issues related to communication and interoperability. The aim is to set the basis for an integrated framework for risk assessment and risk management for water infrastructures, connecting major security aspects such as risk analysis, protection against malicious attacks and crisis management. Risk models have been applied, allowing to perform an accurate risk analysis and identify the most important vulnerabilities in the water distribution system. Risks related to all categories of possible threat (deliberate and due to errors and technological failures, natural and human made) were analyzed, looking at both the prevention of unsafe situations and the management of consequences. Where feasible, some possible countermeasures were checked, investigating criteria to define technological and organizational approaches to increase security.

The risk assessment methodology was developed through six activities.

A. TASK 1: Asset identification and classification

In this task, an as detailed as possible description of the global infrastructure is provided. The description must include all the elements that play a relevant role during the working operations of the infrastructures. We need to evaluate the physical elements, including for example, valves and water pumps that regulate the water flow in the distribution system for the population.

In addition, we need to provide a detailed description of the control network, with the identification of the network elements, the connections with the outside and the software employed for running the control actions on the systems. It is very important to include the configurations of the different elements, as an operator can install the best security measure against malicious actions, but, if this solution is not properly configured, the system can be even more vulnerable.

To better identify the relevance of an asset inside a system, proper evaluation of its impact in a normal state and in a case of failure is required. To do so, [9] suggests the definition of a series of *Key Performance Indicator* (KPI), associated with individual or groups of assets. Examples of performance indicators commonly used for water distribution systems are: leakage, interruptions to supply, water quality and pressure level (too high or too low). Each indicator is characterized by a series of parameters and actions that can be performed to modify the value of the indicator, aimed at improving the overall system performance. It is important to note that each action has a cost associated with it. Typically, when modeling a critical infrastructure system, we need to consider capital costs, operating costs, direct costs related to normal operations and maintenance operating costs.

In addition to a fully detailed description of the system for security analysis, a similar model also allows performance of simulations in order to define proper maintenance and investment plans.

B. TASK 2: Threats identification

With reference to Paragraph III of the present paper, five categories of threats were identified, paying attention to separate non-human related and human related.

C. TASK 3: Criteria to assess severity level

Criteria were defined taking into account territorial, economical and social impacts, in order to evaluate the level of security of the effects of threats. This evaluation implies the estimation of time and costs of restoring disrupted asset.

D. TASK 4: Vulnerability assessment

This typology of assessment takes into consideration also the inventory of existing measures put in place to protect assets with respect of identified threats. Major relevance is played by control and emergency procedures that influence the capability of organization system to cope with threats.

E. TASK 5: Risk assessment

Multi-dimentional risk indexes are created, defining the theoretical risk level of each asset with respect to each threat. These indexes are represented on a GIS (Geographic Information System) Platform, in order to enable an user-oriented operational decision support tool. ("Theoric Risk Analisis").

F. TASK 6: Quantification of probability of threats

The knowledge of the Probability of threats depends upon the availability of reliable intelligent data: only authorized Bodies and agencies own these data. The Decision Support tool up to Task 5 is a neutral instrument that can be fed with sensitive information in order to produce actual risk scenarios. ("Effective Risk Analysis").

The instruments used to perform the project were:

- Technical documentation of water plants;
- Maps of the area;
- On-Site Valutation;
- Research of historical data-set;
- Interviews with plant staff;
- Software for data elaboration.

VI. APPLICATION OF THE METHODOLOGY TO A REAL CASE

A risk assessment methodology and related software tool based upon indicators and mathematical indexes have been developed, linking all types of potential threats to all possible targets, according to a multi-layer likelihood and severity scale. Two levels of output are available. The first level is a security scenario analysis of the water network showing vulnerabilities of assets to each of the identified threats, independent of their probability of occurrence. The second level takes into consideration the possibility of threat occurrence and combines it with the output of the first level to determine the effective level of risk for each asset against each threat.

Clearly only authorized Bodies and Authorities (who own classified information) can insert information that determine the probability of occurrence of specific threats into the tool: the tool allows them to perform this activity in a totally independent way, generating multi-dimensional indexes of risk to be use for prevention.

This methodology can help create a standard risk assessment approach for water critical infrastructures at a wider level.

Item	Description
Major Achievements	Contribution in the building of an integrated framework for risk assessment and risk management for water infrastructures, helping connecting major security aspects such as risk analysis, situation awareness, protection against human and non-human related attacks, crisis management. The study of the security problems related to the use of embedded ICT systems for the control and monitoring networks (investigation of the conditions that can favor security–relevant events) and the production of recommendations on security criteria and best practice for the protection of ICT systems.
Steps for the future	One of the main future objectives is the extension of the experience gained to other kinds of critical infrastructures (e.g. pipelines, energy distribution networks).

Table 1. Result summary table.

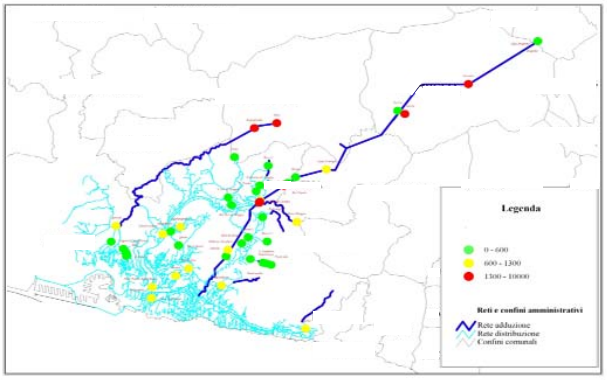

Figure 3. First level output: SECURITY SCENARIO ANALYSIS

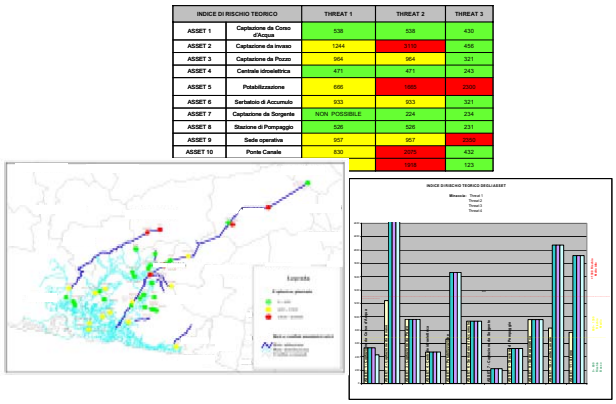

Figure 4. Second level output: EFFECTIVE RISK ANALYSIS

VII. CONCLUSIONS

A risk assessment methodology for drinking water supply infrastructures has been defined and applied to actual contexts in water utilities in Northern Italy. The assessment linked all type of potential threats to all possible targets, according to a multi-layer likelihood and severity scale.

The research sets the basis for an integrated framework for risk assessment and risk management for water infrastructures, helping connect major security aspects such as risk analysis, situation awareness, protection against human and non-human related attacks and crisis management.

Risk Assessment is therefore a valuable tool to enable an effective management of water networks.

REFERENCES

[1]. S. Olivero, F. Fulcini, "Vulnerability & risk assessment of drinking water distribution networks for Genova Acque S.p.A. (AMGA Group): decision support systems for risk reduction and emergency management", *World Water Forum – Italian Local Actions for Global Challenges – March 2006, Mexico City, Mexico.*

[2]. S. Olivero, M. Migliorini, "Risk Assessment of Critical Infrastructures", *IDRC 2008, International Disaster and Risk Conference, 25-29 August, Davos, Switzerland*

[3]. J. Falco, J. Gilsinn, K. Stouffer, IT Security for Industrial Control Systems: Requirements Specification and Performance Testing, *NDIA Homeland Security Symposium & Exhibition, Crystal City, Virginia, May 25-27, 2004*

[4]. ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems: Concepts, Terminology and Models, Part I

[5]. ANSI/ISA-TR99.00.01-2007 Security Technologies for Manufacturing and Control Systems

[6]. National Strategy to Secure Cyberspace, (http://www.whitehouse.gov/pcipb*)*

[7]. Common vulnerabilities in critical infrastructure control systems (http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf)

[8]. *I. Miller, Z. Kapelan, D. A. Savic*, GAasset: Fast Optimisation Tool for Strategic Investment Planning in the Water Industry, *4th International Conference on Water Pipeline Systems*, *28-30 March 2001, York, United Kingdom*.

[9]. *D. A. Savic*, Risk and Robust Strategic Investment Planning in the Water Industry, *4th International Conference on Decision Making in Urban and Civil Engineering, 28-30 October 2004, Oporto, Portugal*.