The Social Sciences 10 (2): 201-205, 2015
ISSN: 1818-5800

On Information of Security Risk Management for GPS/GLONASS-Based Ground Transportation Monitoring and Supervisory Control Automated Navigation Systems

[1]Pavel Viktorovich Botvinkin, [1]Valery Anatolevich Kamaev,
[2]Irina Sergeevna Nefedova and [2]Alexey Germanovich Finogeev
[1]Volgograd State Technical University, 400005 Avenue, 28 Volgograd Lenin, Russia
[2]Penza State University, Krasnaya Street, 440026, 40 Penza, Russia

Abstract: In developed countries, the creation and usage of satellite navigation systems for ground transportation monitoring has been helping to solve various problems for a long time whereas in Russia similar systems based on GLONASS have been introduced relatively recently. Satellite monitoring is widely used to supervise ground transportation for solving logistical tasks, control of passenger and cargo traffic, optimization of courier services, providing the safety of passenger and freight transportation. Attackers in the case of gaining access to a system with read-permissions can illegally obtain information about the location of monitored objects. If attackers can access with write-permissions, they can affect the data in the system, intercepting or sending false data. Both of these options may entail serious negative consequences and even cause casualties. The study describes the purpose and typical structure of such systems; the necessity of their information security risk management. The necessity of development a new approaches of risk management for such systems is also noted.

Key words: Information security, risk management, satellite navigation systems, monitoring and supervisory control of ground transportation, automated information-measuring systems, SCADA, GPS, GLONASS

INTRODUCTION

Modern civilization is largely dependent on automation of production processes. Functioning of the automated control systems in various branches of public and private sector, science and industry is based on computer technology and from the protection of these systems depends not only on the companies' profits but also the national security (Botvinkin *et al*., 2014; Bosenko *et al*., 2013; Tyukov *et al*., 2012).

Global navigation and positioning systems are parts of automated navigation systems for ground transportation monitoring and supervisory control which have complex structure and include a variety of different software and hardware solutions. Data communication between their nodes is performed by a variety of protocols. Breach of information security of such systems can lead to serious negative consequences but this problem is not analyzed in sufficient details.

Over the past few years in Russia such systems have been being systematically implemented at the federal and municipal levels. The first city in Russia where public transport was equipped with navigational monitoring equipment based on GLONASS (GLObalNAvigation Satellite System) became Sochi. In order to control transportation flows, GLONASS equipment was installed on 250 buses in Sochi by company "M2M telematics".

The purpose of this study is to explain the importance of development and usage of information security risk management for ground transportation monitoring and supervisory control GLONASS-based automated navigation systems.

BRIEF INFORMATION ABOUT GLOBAL NAVIGATION AND POSITIONING SYSTEMS

The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all weather conditions anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

Correspoding Author: Pavel Viktorovich Botvinkin, Volgograd State Technical University, 400005 Avenue, 28 Volgograd Lenin, Russia

The system provides critical capabilities to military, civil and commercial users around the world. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver.

The GPS project was developed in 1973 to overcome the limitations of previous navigation systems, integrating ideas from several predecessors, including a number of classified engineering design studies from the 1960s (Anonymous, 1995). GPS was created and realized by the United States (US) Department of Defense (DoD) and was originally run with 24 satellites. Currently there are 31 in-orbit and healthy satellites.

GLONASS-GLObalNAvigation satellite system is the Russian satellite navigation system designed for operative support of quick navigation. The system is intended for an unlimited number of users. GLONASS satellite monitoring can be carried out on a land, sea, river and air transport. Access to civil GLONASS signals at any point on the globe is provided on the basis of presidential decree granted to Russian and foreign consumers at no cost and without restrictions.

GLONASS can provide not only navigation but also satellite monitoring of transport (Finogeev *et al.,* 2014). Which allows monitoring ground transportation on purpose to solve logistical problems to control cargo traffic, to optimize courier services, to ensure safety of passenger and freight transportation to perform survey and cadastral works.

Russian authorities doesn't have jurisdiction on GPS and unlike GLONASS, stable access to it on country's territory cannot be guaranteed.

Russian GLONASS as well as USA's GPS is used both in civil and military (army vehicles movement, fire coordination, etc) purposes. It means that at any moment civil access to these systems may become limited or even completely restricted by military orders.

Parts of these systems may become objects of political show downs as it happened at Summer 2014 Russian government decided to shut down all 11 American-run GPS stations within its territory.

LEGISLATIVE CONTROL

At the moment, the Russian government has adopted a series of regulations and laws that establish the basic concepts, procedures and standards of installation and operation of GLONASS-based automated navigation systems for ground transportation monitoring and supervisory control and has aimed at stimulating their implementation and use.

According to Resolution of the Russian government on August 25, 2008 #641 "About equipment transportation, technical facilities and systems by satellite navigation systems based on GLONASS or GLONASS/GPS", the following vehicles, devices and systems should be equipped by facilities, based on GLONASS or GLONASS/GPS:

- Space devices
- State aircraft, civil and experimental aviation planes
- Sea, river and mixed ("river-sea") vessels
- Road and rail vehicles used for the transportation of passengers, special and dangerous freight
- Apparatus and equipment used to carry out geodetic and cadastral works
- Time synchronization system

Although, the law does not directly limit the application of the navigation equipment, based on GPS on these types of devices, it does so indirectly by only allowing the use of devices based on GLONASS or GLONASS/GPS combination.

STRUCTURE OF AUTOMATED NAVIGATION SYSTEMS FOR GROUND TRANSPORTATION MONITORING AND SUPERVISORY CONTROL

Thus, due to the growing number of GLONASS-based automated navigation systems for ground transportation monitoring and supervisory control (it varies up to few hundreds of such systems in each administrative region of Russia in civil sector), issues of information security has become extremely important.

The typical structure of such Regional Navigational and Informational System (RNIS) is shown on the scheme in Fig. 1.

Attackers in the case of gaining access to a system with read-permissions can illegally obtain information about the location of monitored objects. If attackers can access with write-permissions, they can affect the data in the system, intercepting or sending false data. Both of these options may entail serious negative consequences and even cause casualties.

To contemplate the possible security issues of such systems, it's necessary to analyze the elements of their typical structure (Fig. 2).

Stability of system's measurements mainly depends on the space satellites: their amount, on-line status, coverage zones, stability of firmware, etc. To properly calculate the position of object it's necessary to have communication with at least four available satellites at once (three satellites are enough for two-dimensional measure without of altitude parameter) but more satellites will improve accuracy of calculations (Karouby, 1994).

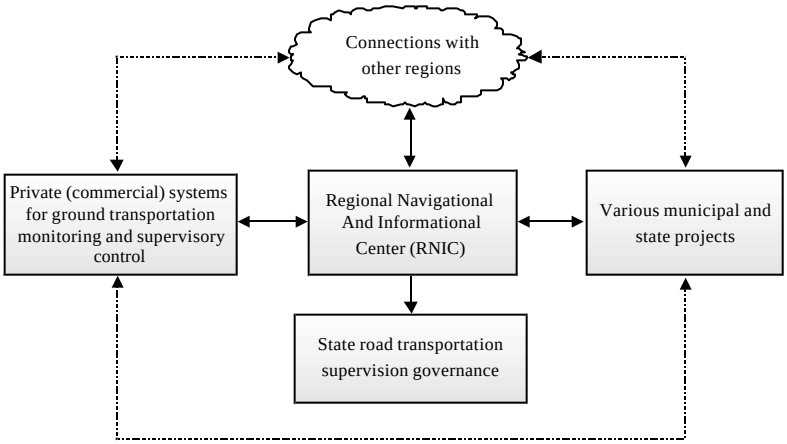

Fig. 1: The structure of regional navigational and informational system

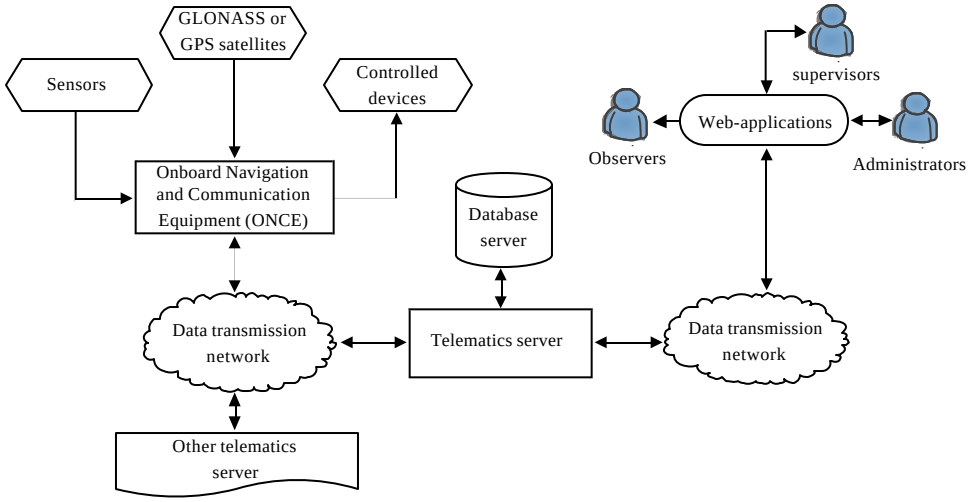

Fig. 2: A typical structure of automated navigation system for ground transportation monitoring and supervisory control

As seen, automated navigation systems for ground transportation monitoring and supervisory control by their functions and structure can be considered as Systems for Control and Data Acquisition (SCADA).

Without the analysis and taking measures to prevent these vulnerabilities, malicious attackers can cause serious damage to the system and to dependent from it organizations and individuals. Most of the attacks can be prevented but in such systems there are still some vulnerabilities. Therefore, prevention methods should be found and it is an urgent task.

The ways to manage information security risks for such systems should be found. At the first, it's important to define the basic terms.

Information security is a state of information, information resources and information systems in which the required information shall be protected with a necessary probability against leakage, theft, loss, unauthorized destruction, mutilation, modification (forgery), copying. Risk is a combination of the probability and consequences of adverse events.

Threat is a possible cause of the unwanted incident which may result in damage to the system or organization. Information security risk management is a process of ensuring the identification, assessment and minimization of risks of exploiting information security threats aimed at the system and its components.

The following directions of protection of GLONASS-based automated navigation systems for ground transportation monitoring and supervisory control can be denoted:

Table 1: Risk management methodologies

Methodology name	Percentage of references in analyzed literature	Country of development
Qualitative		
OCTAVE	78	USA
CRAMM	50	United Kingdom
CORAS	42	Greece, Germany, Norway
FRAP	35	Canada
COBRA	14	United Kingdom
Quantitative		
ISRAM	28	Turkey
CORA	14	USA
Risk watch	14	USA
IS	7	South Korea

- Protection from natural factors: climate, sunlight, extreme temperatures, rain, high relative humidity, high atmosphere pressure, dust, sand, etc.
- Protection from biological agents (insects, rodents, etc.)
- Protection from technogenic effects
- Protection from malicious human intervention: mechanical intrusions, software and hardware hacking

There are many methodologies which are used for risk management of organizations and systems. All can be divided into two groups quantitative and qualitative (Table 1) (Behnia *et al*., 2012). Information security risk management is aimed at:

- Identification of risks
- Risk assessment
- Studying of probability of risks and their potential consequences
- Priority order setting for risks procession
- Prioritization of measures to eliminate existing risks
- Involvement concerned persons into decision making in risk management and keeping them informed about the state of affairs in this area
- Improvement the effectiveness of risk monitoring
- Regular monitoring and review of risk management process
- Collecting information to improve the approach to risk management
- Training managers and staff in the field of risk management and necessary actions which should be taken to reduce them

Quantitative risk assessment uses two basic elements: the probability event and the losses to which it may lead.

The most of risk management methodologies define risk as multiplication of the probability of a threat and damage from this threat.

Problems of quantitative risk assessment are usually associated with unreliable and inaccurate data. Probability is rarely accurate in most cases being an approximate estimate.

Different methodologies are aimed to manage risk in different ways and sometimes contradict to each other. Quantitative methodologies are mostly used to assess economical parameters and can barely be applied for informational security

This, combined with the lack of informational security research of GPS/GLONASS-based ground transportation monitoring and supervisory control automated navigation systems shows the necessity of development of a new approach to information security risk management for such systems.

CONCLUSION

Automated navigation systems for ground transportation monitoring and supervisory control currently receive active development on the territory of Russia. Such systems may be considered as complicated information-measuring systems and they have many potential vulnerabilities because of their complex structure.

In general, the task of such systems' protection involves the use of special technical, technological, software and hardware solutions and should be developed and implement as a set of measures to comply with the constitutive and legislative standards, rules and regulations. The most important parts with the weakest security gradesare information transmission channels and software solutions.

The most of owners of such systems do not aware of existing and possible risks they don't care about importance of providing proper security measures and thus, they don't spend money on it. These expenses may vary of system's structure and complexity but anyway they're lower than possible damages from possible system failure.

The most of existing risk management methodologies are sometimes contradict to each other. Quantitative methodologies are mostly used to assess economical parameters and can barely be applied for informational security.

It's necessary to manage risk of such systems and develop a new approach to information security risk management for them.

ACKNOWLEDGEMENTS

This researchers was supported by Russian Foundation for Basic Research (project 14-37-50693 mol-nr) and the Ministry of Education of Russia within the base part of state task (project 2586 task No. 2014/16).

REFERENCES

Anonymous, 1995. The Global Positioning System: A Shared National Asset. Recommendations for Technical Improvements and Enhancements. National Academies Press, USA., ISBN-13: 978-0-309-05283-2 pp: 16.

Behnia, A., R.A. Rashid and J.A. Chaudhry, 2012. A survey of information security risk analysis methods. Smart Comput. Rev., 2: 79-84.

Bosenko, V.N., A.G. Kravets and V.A. Kamaev, 2013. Development of an automated system to improve the efficiency of the oil pipeline. World Applied Sci. J., 24: 24-30.

Botvinkin, P., V., Kamaev, I.S. Nefedova, A.G. Finogeev and E.A. Finogeev, 2014. Analysis, classification and detection methods of attacks via wireless sensor networks in SCADA systems. Life Sci. J., 11: 384-388.

Finogeev, A.G., I.S. Nefedova, E.A. Finogeev, Q.V. Thuy and P.V. Botvinkin, 2014. Analysis and classification attacks via wireless sensor networks in SCADA systems. Manage. High Technol., 1: 12-23.

Karouby, P., 1994. Method of estimating the error in the calculation of the position of a mobile by a GPS receiver and GPS receiver for implementing this method. Patent US5373298. https://www.google.com/patents/US5373298.

Tyukov, A., A. Brebels, M. Shcherbakov and V. Kamaev, 2012. A concept of web-based energy data quality assurance and control system. Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services, December 3-5, 2012, Bali, Indonesia, pp: 267-271.