Sławomir Gajewski, Małgorzata Gajewska, Ryszard Katulski,
Andrzej Marczak, Marcin Sokół
Gdansk University of Technology

Janusz Staniszewski
Provincial Police Headquarters in Gdansk, Traffic Department

RADIO SYSTEM FOR MONITORING AND ACQUISITION OF DATA FROM TRAFFIC ENFORCEMENT CAMERAS – FEATURES AND ASSUMPTIONS OF THE SYSTEM

Abstract: The study presents the architecture and selected functional assumptions of Radio System for Monitoring and Acquisition of Data from Traffic Enforcement Cameras (RSMAD). Ultimately, the system will be used for transmission and archiving image data of traffic offenses, but can also perform other duties related to traffic safety. Implementation of the RSMAD system will facilitate, inter alia, issuing the fine process and supervision of the traffic enforcement cameras network on Polish territory. Data transmission will be implemented using the networks based on GSM, UMTS or TETRA systems, and through the Internet. The study also discusses some aspects concerning the structure of RSMAD system security.
Keywords: GSM/UMTS, RSMAD, VPN, enforcement camera.

1. INTRODUCTION

Radio System[1] for Monitoring and Acquisition of Data from Traffic Enforcement Cameras will be an innovative, integrated, extensive information and communication system used primarily for transmission, archiving and exploring of data concerning traffic offenses. Furthermore, the system will be able to perform other duties with greater relevance to road safety. RSMAD is designed for the police and it is supposed to cover whole area of the country [1].

[1] The concept of the system must be understood as a physical object, creating certain compact structure, in which we can distinguish some interrelations and relations.

RSMAD system aims to improve to work of the police and other authorities empowered to control traffic in the field of supervision and maintenance of traffic enforcement cameras (portable and stationary), supplied by various manufacturers and distributed throught the country. Above all, the implementation of the RSMAD system is to improve road safety by reducing the number of offenses and by that accidents.

2. FUNCTIONAL ASSUMPTIONS OF THE SYSTEM

RSMAD system will provide the possibility of concurrent use of shared data resources by multiple users. In this context, RSMAD system will have features of transactional system. Central point of the system will be a Data Acquisition Center (DAC), which will be automatically supplied with image data from multiple sources of information distributed over wide areas [2, 3]. Data transmission will be realized through a variety of telecommunications systems, including radio communications and using any transmission technology. RSMAD system will also allow speed remote configuration of traffic enforcement cameras based on the graphical user interface. Access to the system resources will be possible only for authorized users.

The main features of the system are: complexity, breadth, integration of data and procedures, functional and structural flexibility, openness to different techniques and technologies, and security of transmission.

The key assumptions of functional RSMAD system include:

- ***the system's compatibility with traffic enforcement cameras and software from different manufacturers*** − structure and functionality of the system will enable the co-operation with traffic enforcement cameras of various parameters and performance provided by independent producers, compliance will be ensured only by adjusting the functional software modules,
- ***the possibility of a simple connection to the new traffic enforcement camera system*** − the system will be equipped with a feature which allows the system administrator simple connection of new traffic enforcement cameras, without interference in the source code of the application,
- ***monitoring and reporting system status*** − a system administrator will have the opportunity to monitor the current state of the system and to detect possible malfunctions in its operation,
- ***the possibility of remote configuration of traffic enforcement cameras*** − depending on the type of devices the remote management of traffic enforcement cameras and configuration of their parameters will be possible,
- ***configuration of processing and data sending modules*** − functioning of data-processing modules, and modules sending blocks to the DAC will be configurable,
- ***flexibility and system development*** − system architecture will enable its further development and, flexible and easy maintenance,
- ***direct access to system parameters configuration*** − manual configuration of selected devices and modules will be possible through a virtual network VPN

(Virtual Private Network) and via remote video transmission system VNC *(Virtual Network Computing)*,
- ***security of information*** − data transmission (both utility and maintenance) will be realized via encrypted links,
- ***integration with external systems*** − the system will provide integration with public telecommunications networks, primarily mobile and landline and a CDVaD system *(Central Database of Vehicles and Drivers)* for reading data.

3. THE ARCHITECTURE OF RSMAD

RSMAD system's architecture will be open and distributed. This means that from the perspective of end users, the system will create an impression of a centralized system [2, 3].

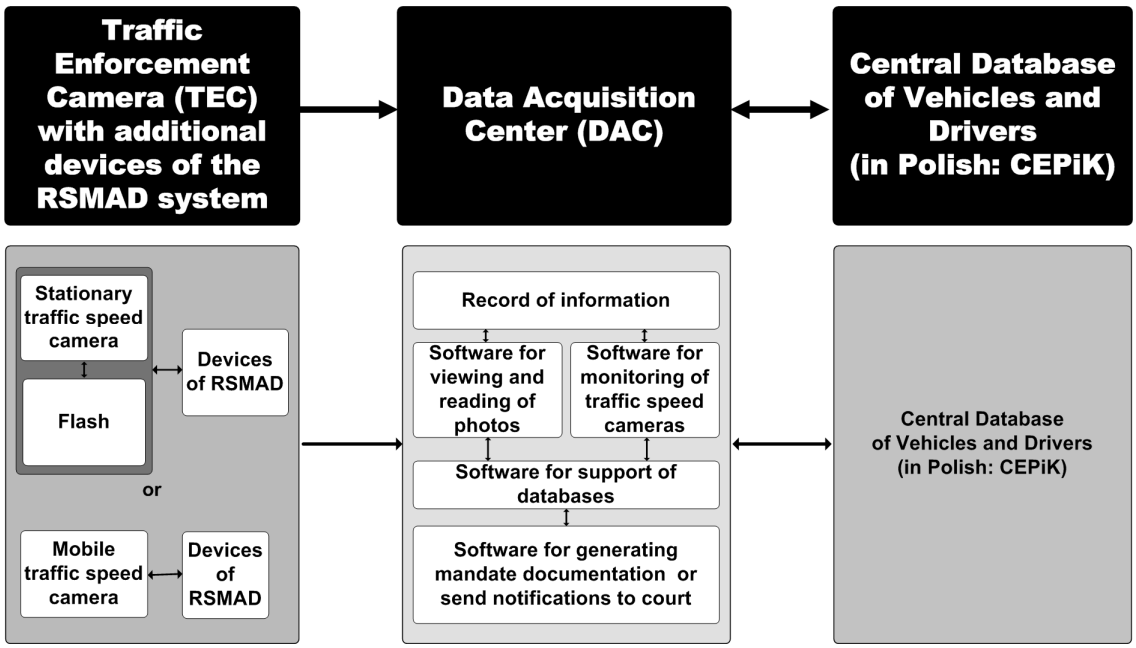

Fig. 1. Conceptual block diagram of RSMAD system.

RSMAD system will be equipped with a features which allow it to communicate with the database of the Central Register of Vehicles and Drivers (fig. 1). Fast and reliable access to data stored in registration database of CDVaD will enable effective finding traffic offenders, through immediate identification of the vehicle, its owner and driver. Integration with DCVaD system will be realized via web services.

The source of image data in the system will be adequately equipped traffic enforcement cameras, with installed software and a dedicated communications module. Data transmission will be implemented through a network-based systems:
- **GSM/UMTS** − the basic variant (all available subsystems to transfer data, including the future of LTE),

− **TETRA** (or other networks) − the additional variant.

Transport blocks containing image data of traffic offenses will be formed and secured at the level of traffic enforcement camera and then sent by radio to the CAD, which is composed of: Management Center (MC), Services Delivery Center (SDC) and the Data Center (DC) (fig. 2).

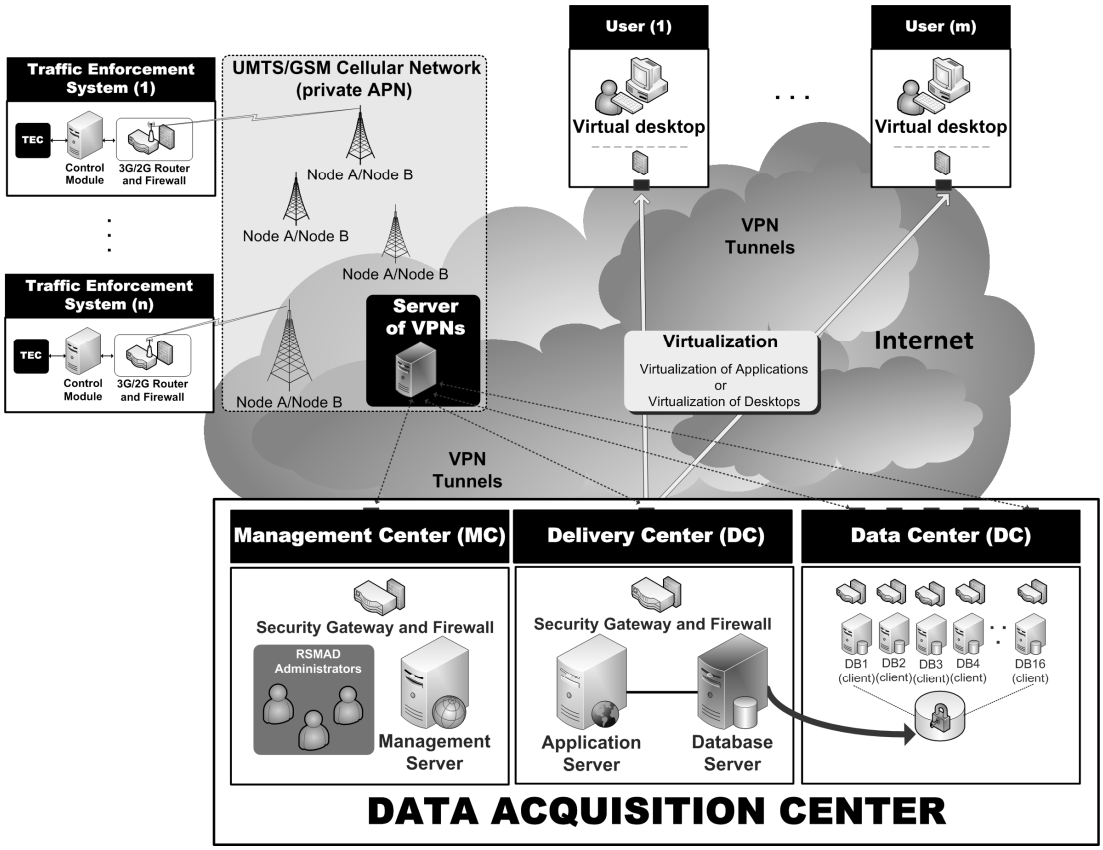

Fig. 2. Simplified architecture of RSMAD system.

As it is shown in fig. 2, an access of authorized persons to RSMAD database will be executed using appropriate client applications. Any of those applications will be delivered to end users in the form of virtual services. This means that instead of the applications installed directly on the client terminals, users of the system will get the application to generate fines documentation as a virtual digital service, made available on request from the modern CAD level. This solution will provide greater system scalability, flexibility and security, because the centralized access control effectively prevents unauthorized use of the application. Software updates and new applications can also be implemented more efficiently than it is in the traditional model. Thanks to it, the efficiency and reliability of the entire system will be improved.

The specificity of the RSMAD system, current regionalization of police work and other services, forces the architecture of the system to consider also these conditions. Therefore, the distributed database system will be used in RSMAD system. Thus, the RSMAD system Data Center will consist of several local database servers with data processor (creating the

so-called database nodes network) and the global node. The RSMAD system database will the base with so-called horizontal fragmentation due to the mentioned before regionalization of the system. This will allow the storage of data from different regions on the local servers in the headquarters of the various provinces or other regions. That is why backup process will not be centralized and the responsibility for it will fall on the individual field units. This will allow the dispersal of reporting mechanisms on the many smaller centers, which will significantly influence the processing of data.

4. SECURITY OF RSMAD

Communication between traffic enforcement cameras [3, 4] and the DAC will be implemented basing on the IPsec VPN (IP Security Protocol) and a private subnet APN (Access Point Network). In particular, the transmission of data via IPSec VPN tunnels, will take place between the network of the GSM / UMTS operator and: MC, SDC, and all DC nodes.

IPsec protocol will be implemented in a way ensuring the broadcast: confidentiality, authentication, integrity, non-repudiation and protection against attacks by repetition. Security of the connections will be provided by the appropriate encryption algorithm and using a cryptographic hash function. However, ability of easily migration to other solutions will be preserved. Use of these algorithms in the IPsec protocol brings very tangible benefits: on the one hand it ensures a sufficiently high level of security, on the other hand, it ensures proper system performance.

In the RSMAD system the following areas of information security, has been defined:

- ***teleinformatic network security*** − all elements of the RSMAD teleinformatic network will be protected,
- ***the protection of access to transmitted data*** − all transmitted, stored and processed data in the RSMAD system will be under the cryptographic protection; transport blocks are sent in encrypted form, and digitally signed[2],
- ***authorization of access to system resources*** − access to RSMAD system resources will be based on strict control of access to each of the areas of its activities,
- ***firewalls[3] and advanced gateway security with control mechanisms of virus detection and intrusion prevention*** − the RSMAD system firewall and security gates will ensure the control of access to network devices (commonly referred to as hosts) and confidentiality of data transmitted in networks,
- ***verification of data*** − the RSMAD system will be provided with cryptographic protection of data in relation to their non-repudiation and integrity,
- ***security of data stored in RSMAD*** − the RSMAD system will be equipped with technical and technological resources which will ensure the increase of the reliability and availability of the system.

[2] ***digital signature*** – a cryptographic transformation of data which enables the recipient to verify the authenticity and integrity of data and ensuring the protection of the sender against forgery.

[3] ***firewall*** - the term referring to a specific software or hardware with appropriate software deployed, which aims to protect systems and networks from attacks of intruders.

It is also important that implementing an extensive cryptographic security structure in the RSMAD system does not hamper or in extreme cases entirely unable users to execute their duties under normal conditions. Therefore it is important to define policy and security architecture so that, as far as possible, reach a compromise between optimizing the efficiency of the system and reaching the required level of security. However, in order to ensure secure transmission of data between applications and network services, basing on a SOAP[4] mechanism *(Simple Object Access Protocol)* the secured HTTPS *(Hypertext Protocol Secure)* is to be used. Each call to the network service is also associated with the calling party's authorization.

5. CONCLUSION

This study was entirely devoted to discussion of the architecture, assumptions, functional and safety issues in the ICT system of RSMAD, mainly in terms of the system. Due to the very wide range of topics only the most important aspects were presented in the paper.

Running a system demonstrator, which primary objective is to demonstrate that the proposed scheme can successfully operate in real conditions is also planned in the project. The concept RSMAD system demonstrator's architecture will be based on main and target concept of RSMAD system in each of its areas: the system, network and application.

The project is realized under the research-development grant R02 N 0034 06 in years 2009-2012 in the Department of Radiocommunication Systems and Networks, Faculty of Electronics, Telecommunications and Informatics at Gdansk University of Technology and is funded entirely by the National Centre for Research and Development.

References

1. Gajewski S.: *Future-Oriented Directions of Research on New Generation Cellular Technologies and System Application Solutions* (in Polish). Przeglad Telekomunikacyjny i Wiadomosci Telekomunikacyjne, no. 2-3/2010, Poland, 2010.
2. KSSR RT 05.900 v. 1.0.0: *Architecture and technology stack of application layer of RSMAD system* (in Polish), Gdansk University of Technology, Poland, 2009.
3. KSSR RT 02.901 v. 1.1.0: *Security architecture of RSMD* system (in Polish), Gdansk University of Technology, Poland, 2009.
4. Rutkowski D., Sokół M., *Data security in IPsec VPN network based on AES-Rijndael cipher* (in Polish), Krajowa Konferencja Automatyzacji i Eksploatacji Systemów Sterownia i Łączności, Jurata 2009.
5. Pieprzyk J., et al., Fundamentals of Computer Security, Springer-Verlang Berlin Heidelberg, 2003.
6. Microsoft Corp., *Assessing Network Security*, Microsoft Press, 2005.

[4] ***SOAP*** – protocol which enables the exchange of data and communication regardless of technology used in XML *(Extensible Markup Language)*.

RADIOWY SYSTEM MONITOROWANIA I AKWIZYCJI DANYCH Z URZĄDZEŃ FOTORADAROWYCH – CECHY I ZAŁOŻENIA FUNKCJONALNE SYSTEMU

Streszczenie: W pracy omówiono architekturę oraz wybrane założenia funkcjonalne Radiowego Systemu Monitorowania i Akwizycji Danych z Urządzeń Fotoradarowych (RSMAD). Docelowo system będzie służył do transmisji i archwizacji danych obrazowych o wykroczeniach drogowych, choć będzie mógł także pełnić inne funkcje, związane z bezpieczeństwem ruchu drogowego. Wdrożenie systemu RSMAD usprawni m.in. proces mandatowania oraz nadzór nad siecią fotordarów na terenie Polski. Transmisja danych będzie realizowana w oparciu o sieci, bazujące na systemach GSM, UMTS lub TETRA oraz poprzez sieć Internet. W pracy omówiono także niektóre aspekty związane ze strukturą zabezpieczeń systemu RSMAD.
Słowa kluczowe: GSM/UMTS, RSMAD, VPN