SAFE LOCKER – A SECURE CARGO TRANSPORT CONTROL SUPPORT IT SYSTEM

ARTUR ANUS[1] AND PAWEŁ BUCHWALD[2]

[1] *ICONITY Sp. z o. o., Cicha 20, 40-116 Katowice, Poland*

[2] *WSB University, Faculty of Applied Sciences,*
Department of Rail Transport and Information Technology,
Cieplaka 1c, 41-300 Dąbrowa Górnicza, Poland

(received: 23 November 2018; revised: 21 December 2018;
accepted: 26 December 2018; published online: 3 January 2019)

Abstract: The article presents the assumptions and architectural implementation of a cargo transport control support system, as well as the preliminary results of tests of the operation of this system in environmental conditions identical with the conditions of natural operation. The aim of the article is the publication of the research results collected during the design, implementation and operation of the system, which relate to the proposed solutions for selected problems that emerged during the development of the system by the research and development team. The article also presents the completed development work and possibilities in the field of the system improvement due to security reasons through integration with modern data processing systems based on a block chain (Blockchain).

Keywords: GPGPU, GPGPU, PDE

DOI: https://doi.org/10.17466/tq2019/23.1/b

1. Functionality of the implemented cargo transport control support system

Remote monitoring systems are widely used in rail transport [1]. The basic functionality of the system includes monitoring and notification of unauthorized access to cargo, at the same time not including physical protection – *i.e.* the system is to notify about the occurrence of an undesirable situation, while not attempting to prevent the occurrence of such. For this reason, the critical parameter for the system is the rate of propagation of the alarm information, which determines its architecture. The basic functionality (violation detection) is supported by the aggregation and transmission of additional data such as location, power status, signal strength, *etc.*, which means that the system not only detects violations of the integrity of the cargo, but also offers monitoring of its condition and location.

2. System design and implementation including development of a cargo transport monitoring device

The system architecture is based on the use of radio technologies for transmission and a fiber optic technology for security purposes (Figure 1). The security component (called “seal”) has a fiber optic loop threaded through a secured element (railcar drain valves, transport container buckles, *etc.*) through which random data is transmitted. In the event of breaking the loop continuity or an unintentional attempt to interfere with the transmitted data (*e.g.* by opening the cover, which changes the degree of illumination and disrupts the transmission), this state is detected as an attempt to impair the integrity of the cargo and an alarm is initiated, and a message concerning this event is sent to the server immediately via the GSM network. Even when there is no tampering, the seals send data on their location and status in a cyclical manner, including, for example, the GSM signal strength, the battery level, the temperature inside the enclosure, the housing condition (it has not been tampered with), *etc.*, which allows monitoring both the devices and, indirectly, the train set. In addition, the system is complemented by a mobile application which, with the use of the RFID technology, enables the activation of the seal in the system after the protection device has been installed, as well as its deactivation before disassembly – which limits the alarm messages only to situations where such information corresponds to the actual state and is not connected with assembly/disassembly.

Transport depots are logically mapped on the server side, where the data provided by devices is also collected. By providing the appropriate API, the server allows the use of client terminals with various functionalities – allowing graphical tracking of the train route or notification of failures and emergency situations, depending on the client’s rights and wishes.

The security device consists of three main modules – a power module, a management module and a communication module. The first one is responsible for the power supply service provided by the configurable sets of lithium-ion or lithium-polymer batteries. The voltage is adequately stabilized and filtered, and then fed to the voltage rails. The protection device monitors the charge level to protect the circuits, if necessary, informing about battery depletion and switching into the economy mode.

The management module is the heart of the device, coordinating the work of the other two modules and supporting the fiber optic loop. The transceiver system integrated in the module operates in the infrared band and consists of a transmitting diode, photosensitive elements and signal conditioning. Random data is transmitted via the loop using the binary ASCII code representation, and in the case of non-compliance of data received with the data sent, the alarm notification procedure is started. Data to be transmitted via the communication module is transmitted thereto using a serial bus. The communication module itself can have an integrated structure (GPS and GSM module in one) or a shared one, however, its functional scope (reading the position using satellite navigation and communication with the data transmission over the GSM network) remains unchanged.

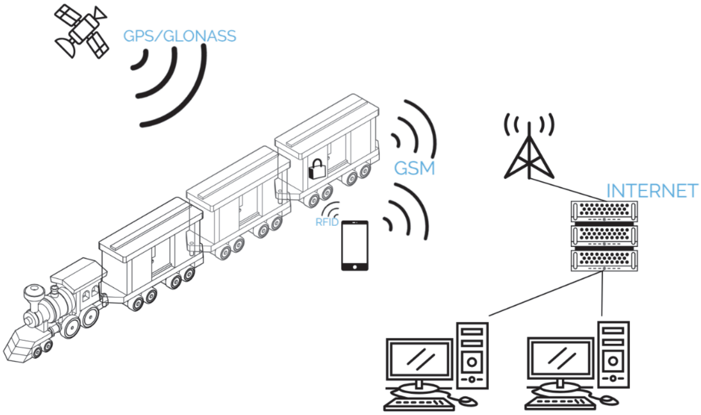

Figure 1. System architecture concept (own work)

3. Performance tests of the cargo data acquisition system carried out in conditions of natural operation

The proposed solution was subjected to a pilot process under real conditions. Within its framework, it covered railway routes of various nature (urban, rural, mixed, high-speed, low speed, *etc.*), with cards of various mobile operators and in various power configurations. In addition, some copies were additionally equipped with the ability to write data on an SD card, which allowed any problems with the GSM communication to be detected. Sample results of a pilot crossing on the Czechowice-Dziedzice to Zduńska Wola Karsznice route (railway lines no. 93, 138, 161 and 131) are presented in Figures 2–4. As can be seen, there is a progressive drop in the supply voltage in the system, which is consistent with the discharge curves for the lithium-ion technology used [2]. While maintaining the pace of discharge, the device could continue to operate incessantly for the next three days, before it reached the warning level (6.4V, with a safety voltage of 5.8V, which is safe for a pair of rechargeable batteries) and go into the power saving mode [3].

In turn, as shown in Figure 3, the offered signal quality significantly differs depending on the cellular network operator – differences in quality The signal (expressed in a unit of the unit obtained with the standard AT "CS +" command) can reach even a dozen or so units, and even individual networks may not have coverage at all, while others are characterized by a satisfactory signal quality. In turn, the GPS signal does not cause such problems – usually the lack of a report

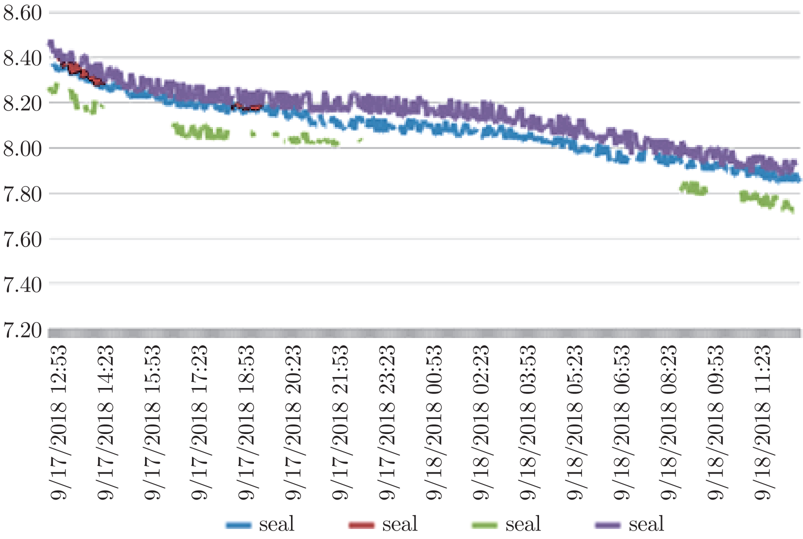

Figure 2. Power supply voltage of protective circuits (own work)

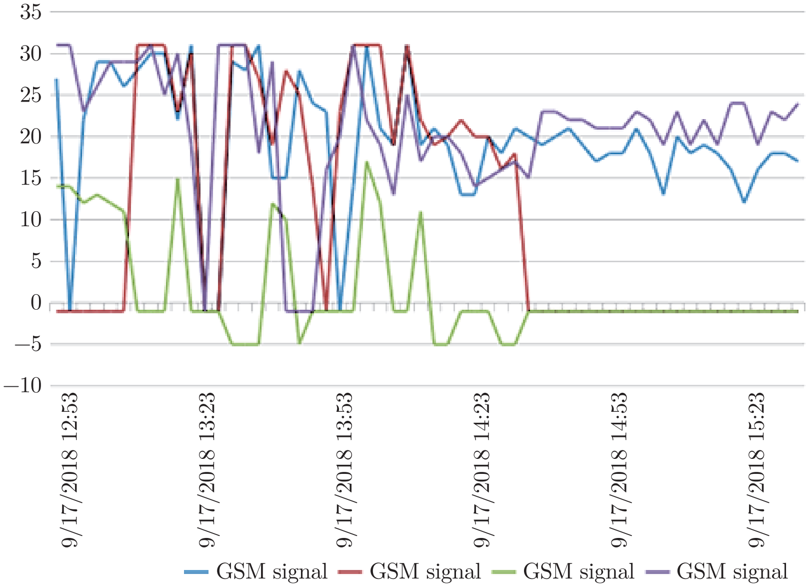

Figure 3. Signal quality of different networks during pilot passages (own source)

on the position of the device is not triggered by the lack of a GPS signal, but the lack of the reporting possibility due to the breaking of the GSM connection.

4. Using the system in real-life conditions

The device is a proprietary solution and does not rely on any ready-made cargo tracking systems. The innovation of the project emphasizes the method of

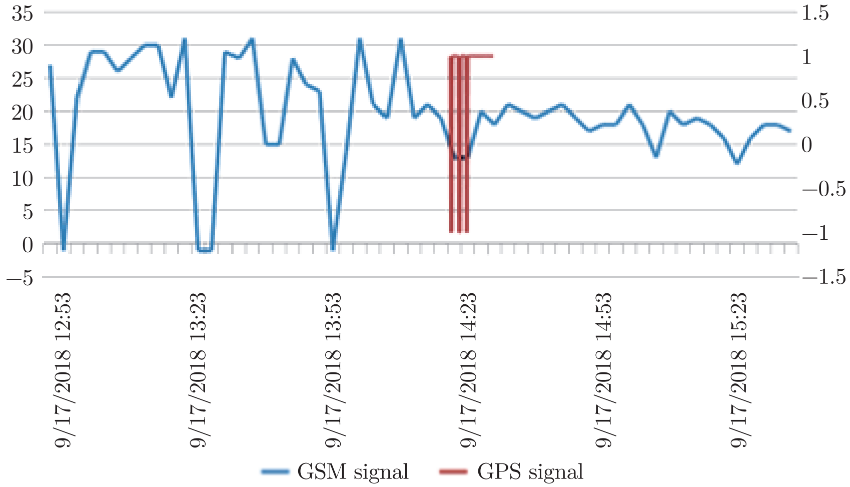

Figure 4. GPS and GSM signal quality for one device (own work)

controlling unauthorized access to the device, which is very important especially when monitoring the transported cargo. The device is vulnerable to destruction especially when the train is not in motion. A fiber loop is used to detect opening of the door. Access to the transported cargo by an unauthorized person causes the loop to unfasten.

In real operating conditions the device itself will be exposed to attempts of breaking in and destroying. For this reason, the electronic seal design has a housing opening detection module. In the case of a force test to destroy the housing, all shocks will be received by the accelerometer sensor connected to the main control module by means of the I2C bus. Thanks to this, it is possible to detect shocks of the casing, which take place during a stoppage and may indicate an attempt to destroy the device. Inside the housing, there is a lighting sensor based on a photoresistor. This sensor detects the change in resistance caused by lighting, which can also be used to monitor the physical opening of the device housing. The availability of analog converter inputs in the device itself allows further extensions in the field of detecting attempts to destroy the seal, *e.g.* by introducing contractor sensors signaling the opening of the housing. The laboratory version of the device tested the use of ambient sound spectral analysis to detect a burglary attempt. The ambient sound detected by the piezoelectric microphone underwent a Fourier transformation. This allowed detection of the application of a grinding machine or a cutter in the vicinity of the sensor of a working power tool – which may also indicate a burglary attempt. However, this method was been implemented in the device tested under operating conditions due to the requirements of the electronic seal power supply efficiency.

While the transported cargo was in motion, the GSM and GPRS signal quality tests revealed temporary deficiencies in the network coverage. Due to the existence of such breaks, data on geolocation and possible events is additionally saved to the SD card in the device and transmitted when the GSM network is available. In the version of the device based on the ESP8266 system, the internal Flash memory was used to save this data.

The prototype was implemented on the basis of generally available electronic components. A patent application was submitted for the solution with a particular reference to the fiber optic loop. The completed implementation allowed testing the operation of the devices. The hardware devices used to control the transport of cargo are shown in Figure 5.

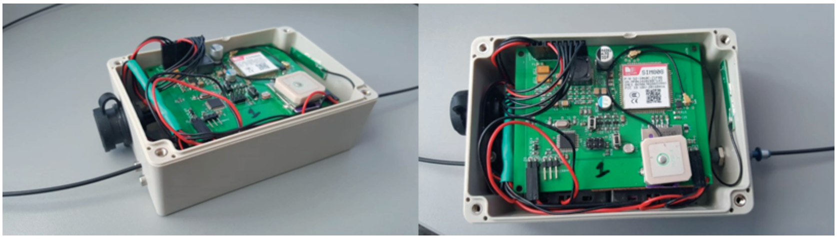

Figure 5. Electronic device tested in real conditions

Costs related to produce a prototype device and its operation are presented in Table 1.

The estimated costs of servicing the seals must take into account the costs of assembly and disassembly. Assuming that the seal requires to be assembled and disassembled once a day, and calculating the total time of these activities, which was 10 minutes on average – the cost of one-year maintenance was 60 hours. At an hourly rate of PLN 20, the overheads related to providing man-made maintenance of the system are PLN 1200. The monthly cost of providing access to the Internet using a SIM card for telemetry applications in Poland is at the level of PLN 20, which gives a total cost of PLN 240 per year. According to the above analyses, the TCO (Total Cost of Ownership) is 240+430+1200 = PLN 1870, which corresponds to daily costs of about PLN 5. Table 1 shows the cost of the system operation. Analysis of the implementation costs of the presented solution allows stating that it is profitable in practical applications.

5. Possibilities of system integration with Ethereum platform for secure distributed infrastructure management

The blockchain is one of the solutions classified under the distributed register technology. These concepts are often mistakenly treated as interchangeable. The distributed register is a distributed database in which each node has a replicated copy of the entire data. Each node updates the data independently and the system as a whole is responsible for its synchronization. The main assumption of a system based on distributed registers is the lack of a central computer – a server that manages access to data. The update correctness is verified by groups of nodes which, using dedicated methods of achieving consensus, confirm the correctness and security of transactions.

Table 1. Costs of equipment production and operation

Unit production costs		Annual operation costs	
Cost description	Value	Cost description	Value
Installation cost	PLN 100	Staff costs	PLN 1200/year
GSM system	PLN 70	Data transmission costs	PLN 240/year
Batteries	PLN 80		
Antennas	PLN 40		
Charging connectors with protection	PLN 40		
Electronic board and passive electronic components	PLN 100		
Total	PLN 430	Total	PLN 1440
TCO	PLN 1870		

From the point of view of IT systems analysis, a blockchain is a database with a decentralized architecture in which data storage uses blocks combined into chains. The connection is based on computationally complex cryptographic algorithms, which ensures consistency and security of the system due to unauthorized modification attempts.

The main difference between a typical distributed information system and a Blockchain-based system is the implicit trust for nodes in the case of traditional distributed information systems. The Blockchain system is characterized by the fact that no trust is assumed by default for all nodes. It can only be assumed that most of the nodes (over 50%) are certified devices for which there is trust.

One of the features of a Blockchain distributed base is its existence in many identical copies. Each copy contains a set of data in the form of interconnected blocks. The Blockchain-based system guarantees the irreversibility of entries made on a distributed database. An attempt to change one block entails the need to modify the whole chain, which is extremely difficult to implement due to the necessary computing power. The technology is based on point-to-point networks, without central computers, which does not cause a single element of failure in the form of a server storing data. The system of distributed registers is much more limited in terms of the ability to perform operations on data compared to distributed databases. When using block-based systems, the implementation of a single data modification transaction is much slower. The use of Blockchain-based systems is a remarkable solution when the overriding task is to maintain security rather than the time efficiency of the processed data [4].

In an Ethereum network, as in the case of traditional cryptocurrency systems, successive blocks are created in the mining process. The block will record the list of transactions that took place since the last transaction saved in the previous block and the value of the hash function representing the new state of the tree after the implementation of the approved transactions. The creator of the newly created block gets a reward from the system for acquiring the so-called block

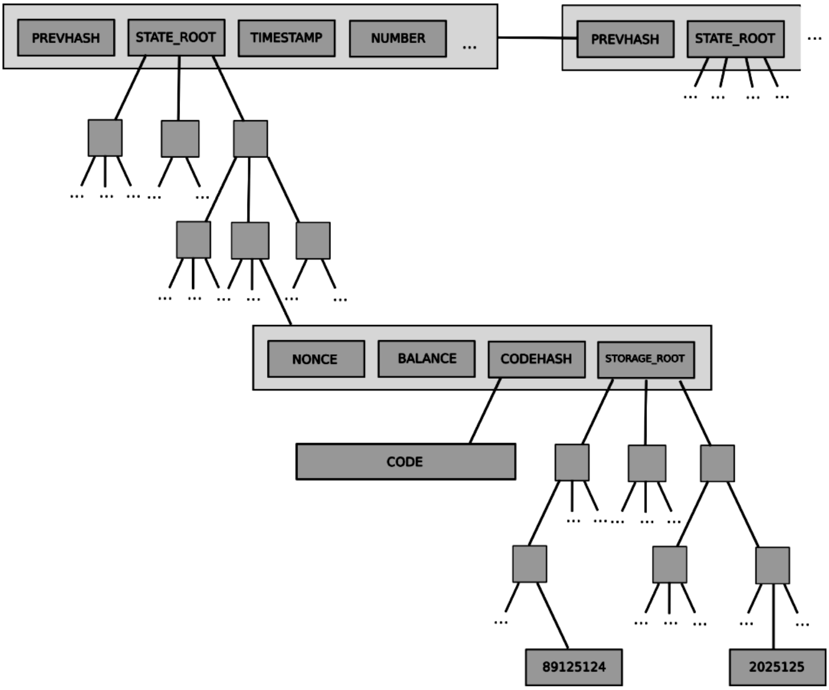

Figure 6. Structure of distributed block register source [5]

digging. The blocks are connected together to form a specific chain (Blockchain). The concept of data stored in such a block is shown in Figure 6.

Currently, the Ethereum platform can be understood as a block chain system that supports a high-level Java script to create embedded business logic elements. It should also be noted that the Ethereum platform introduces a virtual machine to run a code of distributed applications. The virtual machine operates on many distributed nodes and is based on maintaining the security of the code being launched by means of algorithmic methods of reaching consensus by the nodes belonging to the network.

The Ethereum Virtual Machine (EVM) can change its state under the influence of the triggered actions to allowing launching a function implemented in the Java script language which is called a contract [3].

In the Ethereum platform created using distributed applications, the contract serves four basic functions:

- Storage in the status memory of useful data that may be relevant from the point of view of other contracts or external applications. An example of such information could be a contract representing the state of the ETH portfolio, but also information regarding ownership of a given physical resource.
- Conducting conditional operations while meeting additional requirements. This is called a forwarding contract. This type of a contract allows sending a message to the target object if additional conditions are met which can be verified using

a code snippet. An example is the implementation of a conditional ETH transfer if the ownership or access to a resource is modified. Conditional operations can also be used to implement the functionality of a multilateral signature. If the message is confirmed, for example, at least three out of five selected private keys, another contract can be started.
- Management of the status of other contracts. This type of contract may be useful for the implementation of a financial agreement controlled by external entities, or during insurance transactions. This type of contract allows specifying the target object later. For example, it is possible to implement the bidding functionality. The EOA account that will propose the largest value will be the target of the contract transferring the ownership information for the resource.
- It fulfills the functions of the module and library provider for other contracts.

Interaction between contracts takes place on the message exchange principle. Sending a message may be initiated in a programmatic manner from the level of a contract or from the Ethereum platform user's account when making a payment transaction using a cryptocurrency [6, 7].

6. Summary and further development work

One of the additional aspects of using the Ethereum network is to facilitate the execution of tasks related to electronic payments. A distributed register Ethereum platform can store information on the status of selected nodes of the cargo control system along with financial and billing information regarding the operation of the equipment. Development works of the presented system will concern further use of the Ethereum system to improve data security as well as store information on the quality of distributed measurements. This will allow the use of a redundant data acquisition channel in the form of a communication channel between the Ethereum platform and the access control system [7]. This approach gives the opportunity to ensure authentication of sending messages through a secure cryptographic key system, whereby a redundant data exchange platform [8] can be used to exchange public keys. The Ethereum platform is tested in cryptocurrency applications and can be considered as a system that meets the security requirements of message acquisition.

Acknowledgements

The research on the presented cargo transport control support IT system, Save Locker, was implemented as part of the project *Implementation of research and development works on the creation of an innovative monitoring system and remote notification of unauthorized access to cargo in transport*. The project was co-financed from the European Union funds.

We want to greatly acknowledge the European Union funds obtained as part of the project *Implementation of research and development works on the creation of an innovative monitoring system and remote notification of unauthorized access to cargo in transport* for supporting this work.

References

[1] Bocciolone M, Caprioli A, Cigada A and Collina A 2007 *Mech. Syst. Signal Process.* **21** (3) 1242

[2] Source: Li-Ion & LiPoly Batteries Discharge, [online] `https://learn.adafruit.com/li-ion-and-lipoly-batteries/voltages`

[3] Gord M 2016 *Smart Contracts Described by Nick Szabo 20 Years ago Now Becoming Reality*, Bitcoin Magazine [online] `https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751` [accessed: December-2017]

[4] Wood G 2018 *Ethereum A secure decentralized generalized transaction ledger EIP-150 Revision*, [online] `https://gavwood.com/paper.pdf` [accessed: September-2018]

[5] Ethereum platform technical documentation, [online] `https://www.ethereum.org/`

[6] Nowakowski M 2017 *Ethereum Smart Contracts: Security Vulnerabilities and Security Tools*, Norwegian University of Science and Technology, [online] `https://brage.bibsys.no/xmlui/bitstream/handle/11250/2479191/18400_FULLTEXT.pdf` [accessed: September-2017]

[7] Bagchi R 2017 *Using Blockchain Technology and Smart Contracts for Access Management in IoT Devices*, University of Helisinki [online] `https://helda.helsinki.fi/handle/10138/228832/blockchain_thesis_RupshaBagchi.pdf?sequence=2&isAllowed=y` [accessed: December-2017]

[8] Buchwald P, Rostański M and Mączka K 2014 *Theoretical and Applied Informatics* **26** (3.4) 177