Bulletin of Electrical Engineering and Informatics
Vol. 9, No. 2, April 2020, pp. 729~738
ISSN: 2302-9285, DOI: 10.11591/eei.v9i2.1753

Control and indicating equipment communicating via the peripheral component interconnect express bus

Vaclav Mach[1], Milan Adamek[2], Jan Valouch[3], Karla Barcova[4]
[1,2,3]Faculty of Applied Informatics, Tomas Bata University in Zlín, Czech Republic
[4]Faculty of Safety Engineering, VSB-Technical University of Ostrava, Czech Republic

Article Info

Article history:

Received Aug 25, 2019
Revised Oct 12, 2019
Accepted Jan 23, 2020

Keywords:

Control and indicating equipment
Interconnect-express
Peripheral component
Personal computer
Technical security

ABSTRACT

Nowadays, the Intruder Alarm system is commonly used to protect the life, health and the possession of people in big companies. However, these systems have limited options for managing and remote control. This lack is very often criticized by big companies which want to use the Intruder Alarm System with other applications like Access and Attendance control. The aim of this article is to design a Control and Indicating Equipment which can be implemented into commercially made Personal Computer as expansion card. The designed card provides the main function of the Intruder Alarm system which can be further extended by other applications. The system consists of external communication like Universal Serial Bus, Ethernet and General Packet Radio Service interface. Each individual part of the system is driven by a single microcontroller ATmega328P which can handle communication and evaluation of the current state obtained by devices connected to it. The design can offer all alarm and non-alarm visualization of smart control like irrigation, lights control, audio system, etc. The whole design is driven by the proper standardization and the design consists of every schematic which comes with the explanation.

Corresponding Author:

Václav Mach,
Faculty of Applied Informatics,
Tomas Bata University in Zlín,
Nad Stráněmi 4511, 760 05 Zlín, Czech Republic.
Email: v2mach@utb.cz

1. INTRODUCTION

The main topic of this article is the Intruder Alarm System (IAS) which is a main part of the technical protection. The main purpose of the IAS is to protect the life, health, and possession of the person. The concept is driven by the standard CSN CLC/TS 50131 Alarm systems-Intrusion and hold-up systems which is divided into several parts that describe single components. The physical security done by a real person is not reliable, and it is very economically inefficient to employ a person as physical security [1]. According to the author [2] when a person stares at a screen for more than 20 minutes, his attention drops by 30%; and for periods over an hour, this drop can reach 70%. Due to this problem, technical security with alarm systems is nowadays very popular.

Every alarm system must have assigned a Level of Security. It depends on the device which has the lowest level of security. Each Level of Security specifies the equipment of the expected intruder. This standard is given by the CSN EN 50131-1 ed. 2 Alarm systems-Intrusion and hold-up alarm systems Part 1: System requirements. Every detector has the number which specifies the maximal Level of Security

where it can be applied. [3] Common rules for the application of mechanical and electronic alarm systems enable to optimize the security of property for specific risks or to assess the level of specific security or to determine requirements for security of the protected object. The security levels are as follows:

- Level 1: Low risk It is assumed that the intruder or burglar has little knowledge of the system and has a limited range of readily available tools available.
- Level 2: Low to Medium Risk It is assumed that the intruder or burglar has limited knowledge of the system and the use of common tools and portable devices.
- Level 3: Medium to High Risk It is assumed that the intruder or burglar is familiar with the system and has an extensive range of tools and portable electronic devices.
- Level 4: High Risk Used when security has priority over all other aspects. It is assumed that the intruder or burglar is capable or able to prepare a detailed intrusion plan and has a complete range of equipment including means to replace critical system components [4, 5].

According to mentioned standardization, every Intruder Alarm System should consist of the Control and Indicating Equipment, Alarm detectors, Uninterruptible Power Supply, and the Communication interface. All manufacturers of the IAS come to the market as an independent and closed device without any remote user-friendly interface. The setting of the system is usually done by the technical person during the installation, and further managing is very limited [6, 7]. However, the information from the system can be used in other application as well. The author [8] also mentioned that the external connection usually via the Ethernet is the only way how to manage the system and the manufacturers do not provide any additional software for further managing. Most of the people using a personal computer for mentioned external managing of the system. The main goal of this research is to design the Control and Indication Equipment which can be placed as an expansion card into the Peripheral Component Interconnect Express bus (PCI-E).

As mentioned before, there are four main components of the Intruder Alarm System. The first one is Control and Indicating Equipment, which periodically evaluates all data from connected devices. This part usually has a microcontroller for the real-time evaluation, external communication interface such as USB or Ethernet, and the internal communication interface. The second are detectors, which are detecting the person in restricted room or area based on the application. There are detectors which have a sensor focused on the light (Passive Infra-Red), sound (Microwave) contact (Magnetic contact) or vibration (Glass-break). Each category is suitable for different purpose and location. The third is the Uninterruptible Power Supply (UPS) which every IAS must-have when a power failure occurs. The UPS must have a battery which can distribute the power during the power failure for a given time. This time is based on the Level of Security and the number of connected devices. The last on is the internal interface usually done by the RS-485 or RS-232 [9].

The most important standard for this article is the CSN CLC/TS 50131-1 Control and Indicating Equipment, which consists of information and parameters which every product must accomplish [10]. The CIE is the main component of the IAS and it consists of several components which are responsible for the main function. The main function of the CIE is periodically scanning detectors and the evaluation of states. According to the authors [5] and [10], commercial CIE can be divided into two groups. First group using digital interface and second using analog interface. Digital CIE using only one bus which typically consists of four cables (Ground, Power Voltage, Data+, Data-). This manner allows to connecting several detectors to one bus. Detector evaluates actual state which is then sent to the CIE in binary form. There is another type of connection called an analog loop. However, this type is outdated and it is not recently used.

The incoming signal from the connected detector is the essential information for the whole system, and the CIE must be able to distinguish between basic states [11]. These states for every CIE are Serenity, Alarm, Failure, and Sabotage. Serenity and Alarm states are very easy to identify. The tricky part comes with the detection and distinction between Failure and Sabotage. Failure must be detected as Alarm. All mentioned states must be implemented into the final model. The connected detectors can have some additional outputs like tamper or anti-masking.

According to the author [12] and [13], every component of the alarm system which comes to the market must be constructed according to the standardization. Every device must be tested according to the standard CSN EN 61000-4-4 ed. 2 Electromagnetic compatibility (EMC)-Part 4-4: Testing and measurement techniques-Electrical fast transient/burst immunity test. This document describes unified standards and limits of the maximum permitted interference level for specific types of equipment or accurate and reproducible conditions for the measurement and verification of the electromagnetic susceptibility equipment.

The Peripheral component interconnect express is a high-speed serial computer expansion bus standard, which has characteristics of high speed, low power, and high protocol efficiency [14]. This standard is widely used as a standard I/O interface for connecting processors, and I/O system devices. High speed,

low power, and high efficiency are the salient properties of the PCI-E; because of additional properties, PCI-E is considered as good alternatives to the existing network structures [15].

It also uses a bus topology to enable communication between other devices on the bus, and it supports multiple lanes of 1x, 2x, 4x, 8x, 16x, and 32x per link. Data rates are 2 Gb/s per lane in PCI-E Gen 1, 4 Gb/s per lane in PCI-E Gen 2 and 8 Gb/s in Gen3, the bandwidth is 128 Gb/s, and the clock speed is 8 GHz based on the PCI-E Gen3 16x lane [16, 17]. Every PCI-E slot has a switch which is a collection of logically connected PCI-PCI bridges. After connecting the additional PCI-PCI bridges downstream, one PCI-PCI bridge is upstream. It means that switching appears as a hierarchical structure of logical PCI bridges [16].

PCI-E is one example of the general trend toward replacing parallel buses with serial interconnects like USB. PCI Express is a serial connection that operates more like a network than a bus. Instead of one bus that handles data from multiple sources, PCI-E has a switch that controls several point-to-point serial connections [18]. The physical card must be manufactured by a strict dimension which is listed in Figure 1.

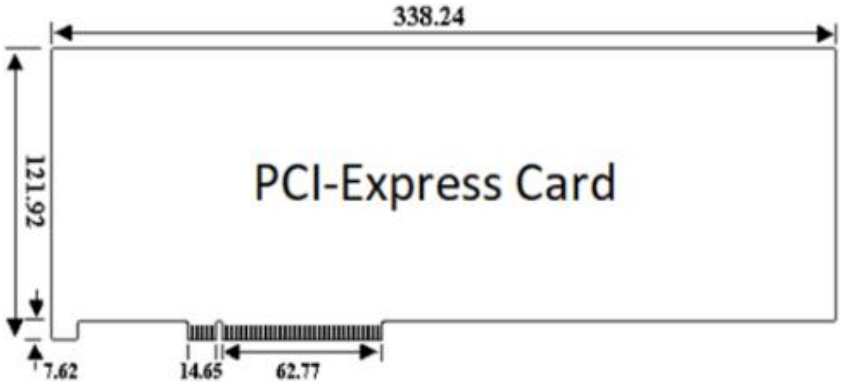

Figure 1. Maximal dimensions of the PCI-express card

2. RESEARCH METHOD AND MATERIALS FOR THE DESIGN

The main goal of this article is to design a functional prototype of Control and Indicating Equipment which has a PCI-E connection. The system should be built from the same components and built according to techniques as a common certificated CIE on the market. These elementary components and features are described in the following individual section.

2.1. The main microcontroller ATmega328P

The main microcontroller is on the top of the created hierarchy of the system. It can receive data from other devices like detectors or keyboards and it is also able to transmit data to other microcontrollers or devices. The ATmega328P microcontroller was chosen as the main microcontroller because it has embedded channels for the UART interface for serial communication. Moreover, the first channel is reserved only for communication via USB with the computer. However, the microcontroller can handle also function Software Serial, which can be implemented on any pin and it can provide more serial channels for serial communication [19, 20].

The main microcontroller takes advantage of CISC and RISC architecture. Microcontrollers use up to 120 instructions and process the entire instruction in one clock cycle. The combination of these architectures provides a good implementation of any programs. ATmega328P also consists of an 8-bit processor that contains two types of memory-data memory that stores the variables and program memory that stores the program. Data memory is typically Static RAM (SRAM), and the program memory is stored in the Flash memory [19]. The microcontroller also equipped with 14 pins which can be used for the output or input and some of these pins support PWM, analog inputs, and connection of a 16 MHz crystal [21].

Every ATmega328P are able to communicate with the computer via UART. For easy and comfortable communication via the PCI-E, a special integrated circuit called FT232RL is used which can convert UART communication to USB. This circuit does not require any other special settings. The data from the USB connector are connected to the USB-DM and USB-DP pins. The converted UART interface is able on RXD and TXD pins. The _DTR reset pin must be connected to the master reset circuit and all of the power lines according to the official datasheet.

2.2. The ethernet chip ENC28J60

One of the sub-goal of this article is to integrated easy and suitable Ethernet interface for external and technical communication. Using another microcontroller which provides the Ethernet communication makes it very easy to add user interface via a website. It can be reached from all devices connected to the Ethernet network. At the same time, the connection can be used as an interface to send the alarm signal to the Alarm Receiving Center (ARC).

Ethernet communication itself is performed by the microcontroller ENC28J60. It is a single-chip Ethernet controller and no separate operating system is required. The ATmega328P, which is connected as the command microcontroller, is able to communicate via the SPI. In order to simplify SPI wiring, it was decided to use this method of communication. [15] The hardest part of this connection is the Ethernet connector. Physical pins for the Ethernet connection are TPIN+, TPIN- for the receiving and TPOUT+, TPOUT- for the transmitting part. These pins are directly connected to the Ethernet connector which contains the isolating transformers. A special filter is added between the parts to protect against electromagnetic interference. The schematic part of the Ethernet connection with the ENC28J60 is shown in Figure 2.

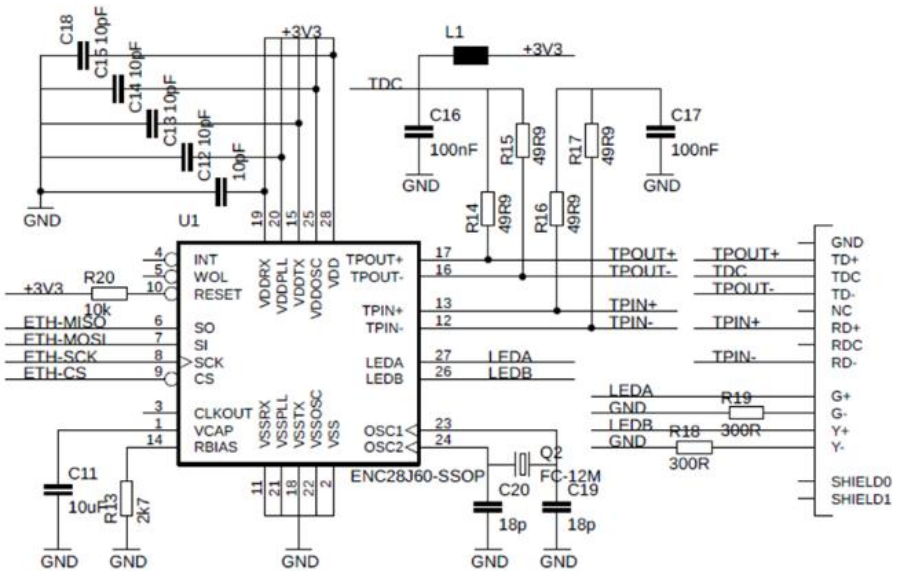

Figure 2. Schematic part of the ethernet connection via the ENC28J60

2.3. GPRS communication via the SIM900

Another microcontroller was used to control the GPRS communication via the microcontroller SIM900 using the UART. It allows communication using so-called AT commands which means that text strings are used for sending commands. No other library is necessary to achieve maximum flexibility. Physical pins for serial communication are (SIM-TX and SIM-RX). Pin for SIM-TX can be any free pin for sending AT commands, but the SIM-RX must be connected to the pin which can handle the internal interrupt. There is a special pin called SIM-PWRKEY which can be used for the starting sequence. The main usage for this part is to allow sending SMS and email as a notification to the customer. It can be also used as an input to control temperature, lights or any other devices. The schematic part of the SIM-900 is listed in Figure 3.

SIM900 is widely used in GSM and is has a complete Quad-band GSM/GPRS module. It has a very powerful single-chip processor AMR926EJ-S. The chip also has a 32-bit ARM processor-based LPC2148 microcontroller which is connected to LPC2148 through a USB to RS232 driver. [22] As mentioned before, the communication is done using the AT command set that is specific to the GSM technology. This communication includes SMS-related commands like AT+CMGS (Send SMS message), AT+CMSS (Send SMS message from storage), AT+CMGL (List SMS messages), and AT+CMGR (Read SMS messages) and more [23].

As author [24] mentioned, the SIM900 is developed for Appliances Automation and Security Control System using the Arduino platform. The developed system is decomposed into two separate entities. First, the hardware is designed using Arduino with other required electronic components which

is programmed using embedded C language. Second can be an Android app which provides freedom to the user to control and access the electronic appliances and the security system without the internet.

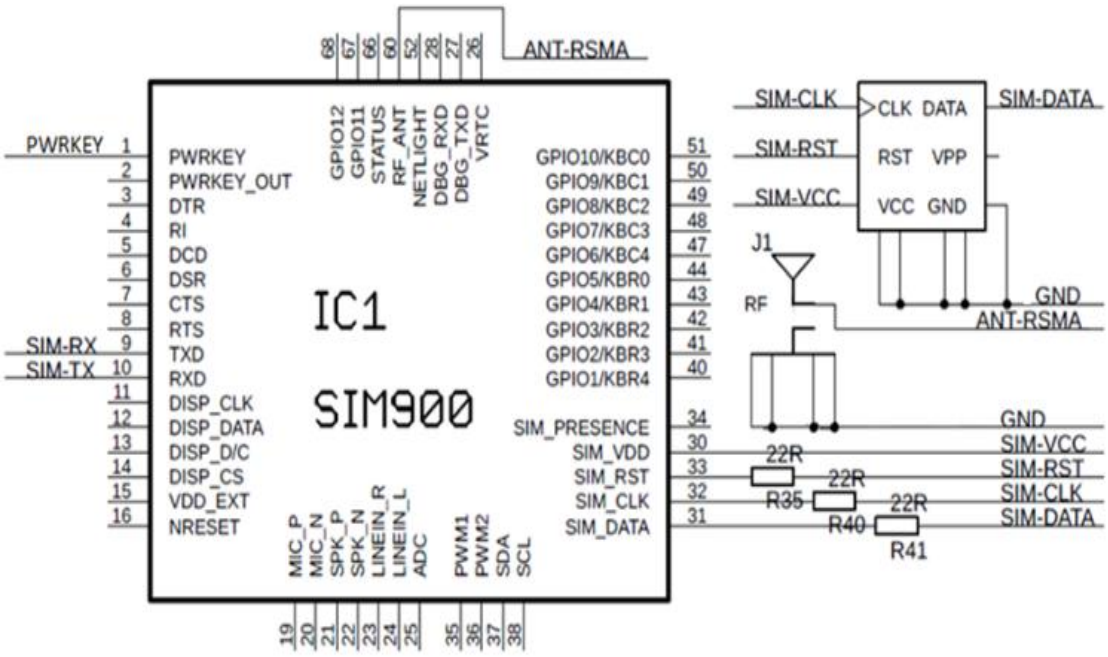

Figure 3. Schematic part of the GPRS connection via the SIM900

The antenna for external communication with the Base Stations is needed. On the final board is installed an antenna connector compatible with GSM, GPRS, UMTS, and 3G. It is ideal to extend the coverage quality, move the antenna to areas of better coverage, have a better quality of the signal. The frequency of the antenna is 824-960 and 1710-2170 MHz which is the exact frequency of the SIM900 module. The schematic part is shown in the following Figure 4.

2.4. PCI-express communicator with the USB hub

On the board must be a communication interface which can communicate with the program via the PCI-E. The standard interface for the communication is done via the USB which is used in this scenario. The PCI-E slot has complete USB interface using all USB 3.0 features. The pins HSOp(0) and HSOn(0) are responsible for the transmitting part of the channel and the pins HSIp (0) and HSIn (0) are responsible for the receiving part. There are also pins for the USB 2.0 REFCLK+ and REFCLK-. All mentioned pins can be used for further communication via the PCI-E.

All mentioned microcontrollers are connected to the USB bus. The USB 2.0 interface was used due to a small amount of information that is passing through the line. However, there is only one USB 2.0 line on the PCI-E 1x, three active microcontrollers, and each one must be connected to the separate line. Due to this problem, a USB Hub was installed on the board to provide enough lines for all microcontrollers. In this case, the TUSB2046 USB hub was used. This device can make four independent USB 2.0 lines.

Each line has also termination resistor which helps with the stability. The PCI-E connector has also the power pins for the power supply. These pins are +12V and +3V3 and it can be used as a power supply for all components on the board. However, these pins have limited power consumption of 10 W. It means that there must be an external power supply on the board. The card will be placed inside of the common PC case which has the power supply with the power cables. Classical Molex connector was added to the board to power all devices on the board. Only the power voltage +3V3 must be stabilized from the +5V using a stabilizing device.

The chip itself contains overcurrent circuits that can detect overload of each line. This protection is very often used for the protection of an unknown connected device. However, this design is not used due to the concept where all components are connected and there is no possible way to connect other devices which can cause overload. The schematic part of the USB hub TUSB2046 can be found in Figure 4.

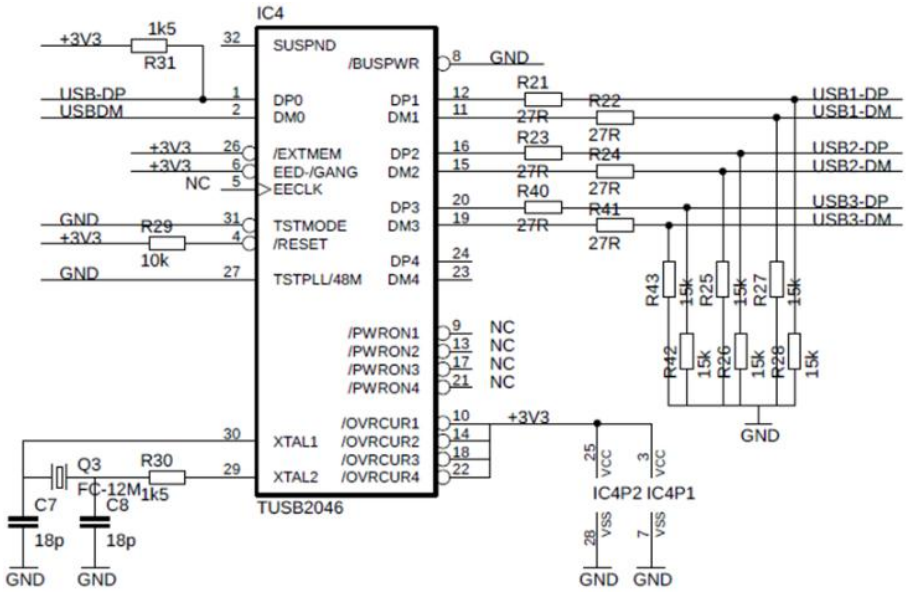

Figure 4. Schematic part of the USB hub TUSB2046 connection

2.5. The schema of the UPS

According to the mentioned standardization, every IAS must have a UPS in case of power failure. During this event, the UPS must power the whole system from the battery in it. The battery must be able to power CIE and also all connected devices. The capacity of the battery is calculated from the total power consumptions which must be available during the failure. All needed information can be found in the standardization and every scenario can have different capacity of the battery. The final schema of the UPC can be found in Figure 5.

This simple UPS schema can deliver 12V unregulated, 5V regulated, and 3.3V regulated. The power from the PC Power Supply is smoothed by the capacitor C33. When the PC supply is available the battery will be charged via diode D2 and the regulator gets supply via diode D1. Voltages 5V and 3.3V will be available at the output terminals. When the PC Power Supply is not available the battery supplies current to the regulator and the 12V terminal through diode D3. Also, the diode D2 blocks the reverse flow of current during battery mode. Capacitors C2 and C3 act as filters.

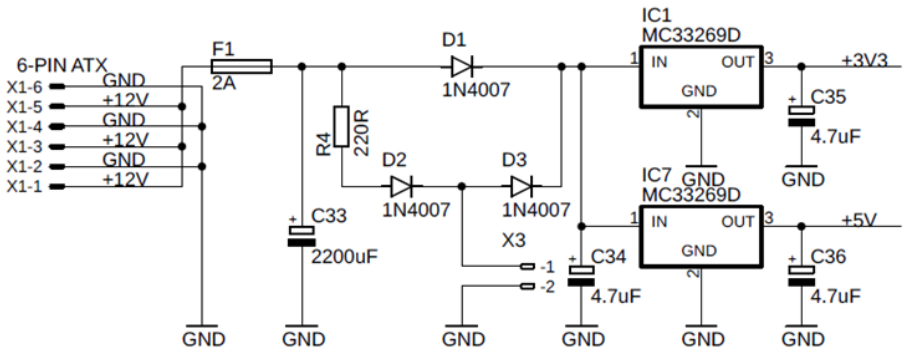

Figure 5. Schematic part of the UPS

3. REQUIREMENTS FOR THE DESIGN

Every section of the final schematic must be designed according to all mentioned standardization. The final product of this paper should be an independent board which can be connected to the mainboard via the PCI-E interface. The system should be also protected against the power failure by the UPS module on the board. All main requirements for the system are the following:

- final IAS placed in a PC case as PCI-E card
- programming and communication via the PCI-E
- external communication via the Ethernet, USB, and the GPRS
- internal communication with the detectors using the RS-485 and RS-232
- a UPS installed on the board

The board should consist of three independent microcontrollers each for one main function like GPRS communication, Ethernet interface, and the evaluation of connected devices to the system. Each microcontroller should be able to communicate with others using the serial interface like Serial Peripheral Interface (SPI). This organization can help with overloading the microcontroller with a time-consuming task which can lead to total system failure. The overload can be caused for example by the internet connection and if the system operates only on a single chip, the Ethernet communication can affect for example the evaluation of the alarm messages. The same applies to the GPRS communication. The block schema for better understanding is shown in Figure 6.

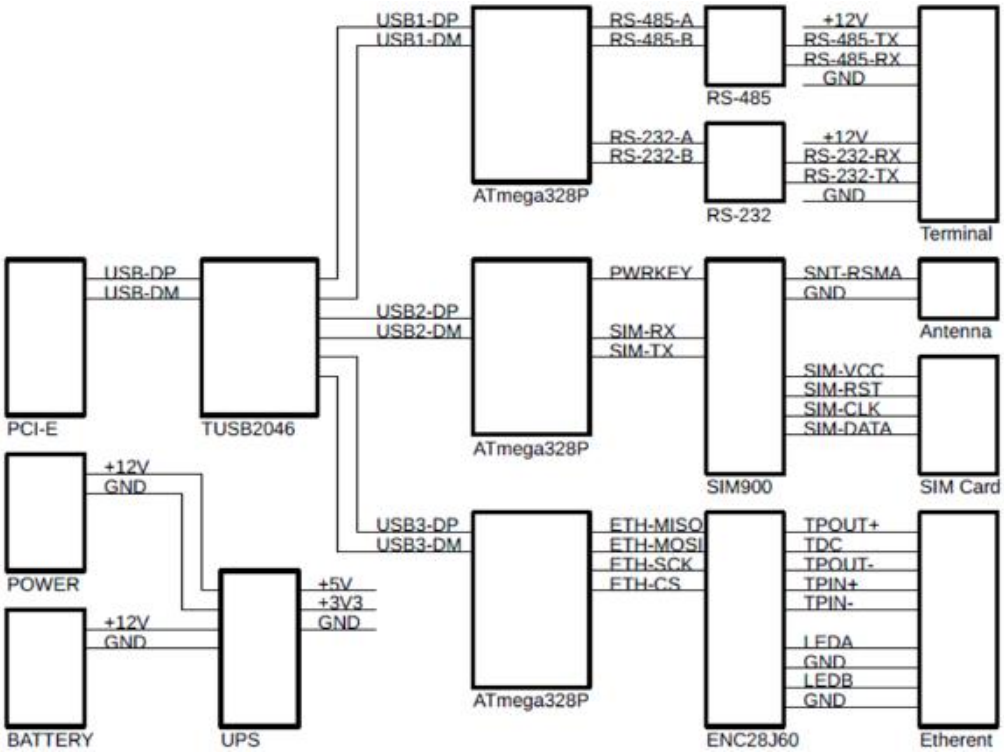

Figure 6. Block Schematic diagram of the designed system

As mentioned before, the main communication interface with the computer is done by the USB standard which can be directly used from the PCI-E interface. Just one data lane for the USB cam be used due to the relatively small amount of the exchanged data between the PC and the board. However, there are three microcontrollers and just one USB line, which cannot be physically divided. This problem should be solved by the USB bus which can extend the one line in three more needed by the microcontrollers. In case of the power failure, the system must operate normally using the UPS with the battery.

4. THE FINAL DESIGN OF THE PCI-E-CARD

The whole card must fit in a common PC case which has a limited amount of the space in it. Due to this limitation, the dimensions of the card are strictly limited. However, the number of components is not very huge and there was no problem with space. The communication interface will be transmitting only the string of the text which can be handled by the USB 2.0 though the PCI-E interface. The PCI-E 1x connector was used in this design, and the card can be plugged in any version of the PCI-E connector. The final design of the card can be found in Figure 7.

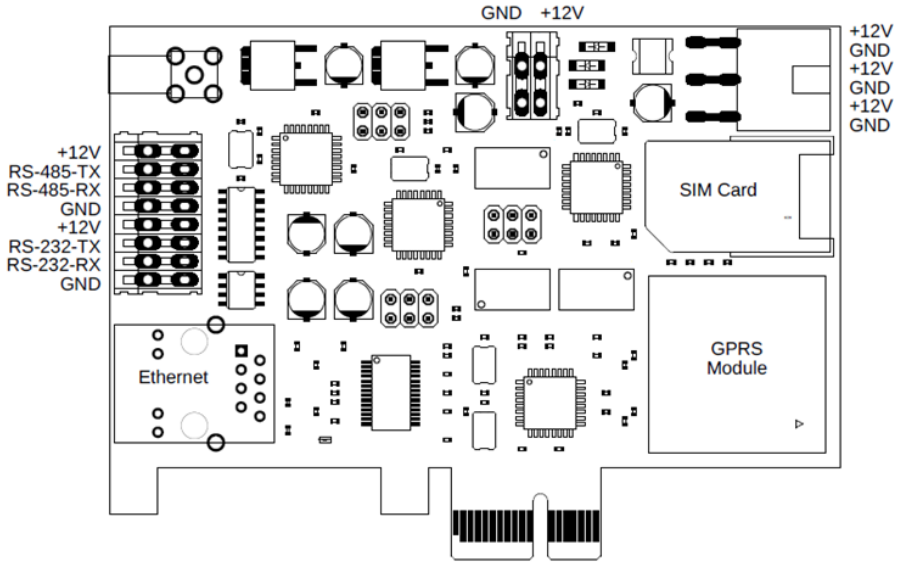

Figure 7. The final design of the PCI-express card for IAS applications

The final card is very compacted and small. Typical design with the components on top and the copper lines on the bottom was used. On the board is a slot for the classic SIM card, on the side of the board is installed an RSMA antenna connector, and there is also installed the Ethernet connector (RJ45). There must be placed a terminal where interface for alarm detectors and other alarm devices can be connected. All microcontrollers must be separately programmed via the In-System Programming using the 6-pin- header on the board.

On the top of the board is installed the UPS terminal where the battery can be connected. The typical capacity of the battery is about 2000 mAh which can power a small system for tens of hours. This problem must be considered with the Level of Security if the Security which has a minimal time of charging and discharging of the battery in the system. The battery can be placed inside of the PC case due to small dimensions. When the power failure occurs, the PC shut down and the battery powers only the CIE and connected devices.

5. COMPARISON WITH JABLOTRON JA-82K

Hybrid control and Indicating Equipment of the electronic security system with a maximum capacity of 50 loops of which up to 14 wires. The control panel has 2 subsystems, 4 outputs, up to 50 users identifying PIN codes or RFID chips. The memory of the JA-82K is 256 events. Meets standardization safety 2 according to mentioned EN 50131. Power supply JA-82K is 230V, reserve. power supply max 700 mA, battery compartment max. 12V/2,6Ah. The system can be extended by wireless module JA-82R and by the JA-82C wired input module connector. It uses the common communication bus based on the RS-485. The physical design of the Jablotron JA-82K can be found in Figure 8.

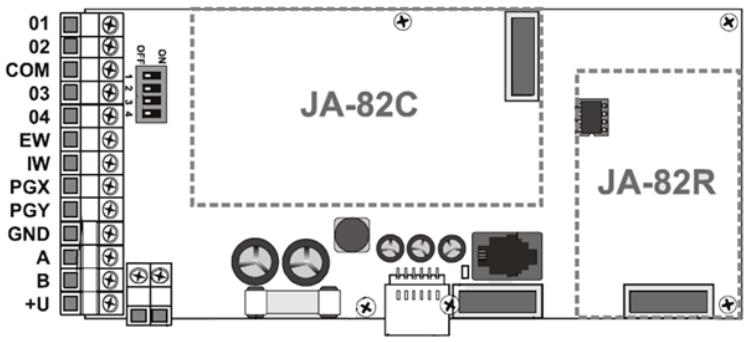

Figure 8. The model of the control and indicating equipment Jablotron JA-82K [25]

As mentioned before, the commercially made CIE cannot support any external interfaces like Ethernet, GPRS or USB. Several interfaces can be added to the system using the expansion slots, however, this number is very limited. The installation and the management of the system can be done only by the external keypad which has only the numerical keypad and the 16x2 LCD. This type of management is very limited, complicated and it does not provide any external connectivity with other devices or applications.

6. RESULTS AND DISCUSSION

The designed system is assembled as a common CIE which can be found on the marketplace and it is constructed according to the standardization. The final board has dimension and connection for the placement into standard PCI-E expansion slot in the PC. Compared to the mentioned CIE JA-82K, the new design has the microcontroller ATmega328P for the main evaluation of the alarm messages which is an equivalent to the microcontroller used in JA-82K. It uses the same communication bus for the alarm detectors, However, the new design intentionally lacks the terminal for the analog loop connection which is outdated. The communication interface is extended by the Ethernet, GPRS and USB standard. The power supply is already placed inside of the PC case and the battery can be connected to the board in case of the power failure.

The USB hub can be deleted from the design in case of using at least PCI-E 4x where three independent USB lines can be found. Moreover, the PCI-E 4x can also help with the stability inside of the case. However, the used PCI-E 1x connector can be placed in any PCI-E connectors despite the numbers of lines, which makes PCI-E 1x the most universal. The biggest advantage of the designed system is the integration of all needed communication interfaces which are not places in others CIEs on the markets. The capacity of the supporting battery must be calculated before the real-time operation. The battery must have the voltage 12V and this type of the battery have small dimensions which can fit inside of the standard PC case. By using simple construction, the battery can be mounted in a 3.5-inch frame.

7. CONCLUSION

The main goal of this article was to design a functional model of the Control and Indicating Equipment in for of the PCI-E which can be placed in a common PC case. This concept should help with the remote managing and integrating other non-alarm application to the system. The design is driven by the current standardization CSN CLC/TS 50131. Alarm systems-Intrusion and hold-up systems. At the beginning of the study, the idea of the IAS and all needed part of the system are presented. The PCI-E interface which is used as a communication interface with the PC is described further in the article. The following sub-sections are focused on the design and schematic of each part of the system. This system consists of the main part which deals with the alarm connection and further evaluation. The system has several external communication interfaces such as USB, Ethernet, GPRS, RS-232, and RS-485 interfaces.

One of the chapters consists of the physical design of the system in the form of the Printed Circuit Board and the last one shows the final design of the system. The board has dimensions and connectors compatible with the PCI-E standard and it can be placed in any common PC case which has the PCI-E interface. Further research can be focused on the programming of the interface for the user which can be used as application management for Integrated Alarm Systems. The designed system also has the UPS which automatically activates when the power failure occurs. The design was compared witch the real CIE which can be found on the marketplace.

ACKNOWLEDGEMENTS

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Program Project No. LO1303 (MSMT-7778/2014) and also by the European Regional Development Fund under the project CEBIA-Tech ED2.1.00/03.0089 and by the Internal Grant Agency of Tomas Bata University under the project No. IGA/CebiaTech/2019/003.

REFERENCES

[1] K. Ljubymenko and M. Adámek, "Security personnel of new generation," *In: Proceedings-International Carnahan Conference on Security Technology*, Montreal: Institute of Electrical and Electronics Engineers, 2018.

[2] L. Jiang, *et al.*, "Implementation of a Remote Real-Time Surveillance Security System for Intruder Detection," *9th International Conference on Measuring Technology and Mechatronics Automation*, 2017.

[3] CSN EN 50131-1 ed. 2 (334591), "Alarm systems-Intrusion and hold-up alarm systems-Part 1: System requirements," Prague: The Office for Standards, Metrology and Testing, 2013.
[4] CSN CLC/TS 50131, "Alarm systems-Intrusion and hold-up systems," Prague: The Office for Standards, Metrology and Testing, 2011.
[5] J. Hart, and V. Hartova, "Testing of combined space detectors in intrusion and hold-up alarm systems," *Engineering for Rural Development*, pp. 905-909, 2018.
[6] J. Hart, *et al.*, "Intrusion and Hold -Up Alarm Systems and Their Reliability Glass Break Detection," *6th International Conference on Trends in Agricultural Engineering*, pp. 171-174, 7-9 September 2016.
[7] M. Blahová and M. Hromada," The Soft Targets in the Czech Republic and Their Security," *Trilobit*, vol. 10, no. 2, 2019.
[8] M. Pospisilik, *et al.*, "Remote controlled gate controller using a GSM network and Arduino platform," *MATEC Web of Conferences*, pp. 02036, 2016.
[9] E. I. Davies, and V. E. I. Anireh, "Design and Implementation of Smart Home System Using Internet of Things," *Advances in Multidisciplinary & Scientific Research Journal Publication*, vol. 7, no. 1, pp. 33-42, 2019.
[10] J. Valouch, "The Proposal of Methodology for Evaluating the Effectiveness of Alarm Systems," *Applied Mechanics and Materials*, vol. 736, pp. 183-188, 2015.
[11] A. Hanacek, and M. Sysel, "The Methods of Testing and Possibility to Overcome the Protection against Sabotage of Analog Intrusion Alarm Systems," *Intelligent Systems in Cybernetics and Automation Theory*, pp 119-128, 2015.
[12] H. Urbančoková, *et al.*, "Testing of an intrusion and hold-up systems for electromagnetic susceptibility," *International Journal of Circuits, Systems and Signal Processing*, vol. 9, pp. 40-46, 2015.
[13] S. Kovář, *et al.*, "Electromagnetic compatibility of arduino development platform in near and far-field," *International Journal of Applied Engineering Research*, vol. 12, pp. 5047-5052, 2017.
[14] A. Gabrielli, *et al.*, "A Multi-Channel Pci Express Readout Board for Fast Readout of Large Pixel Detectors," *Nuclear Instruments and Methods in Physics Research Section A*, vol. 924, pp. 279-281, 2019.
[15] Ch. Shim, *et al.*, "Compatibility Enhancement and Performance Measurement for Socket Interface with Pcie Interconnections," *Human-Centric Computing and Information Sciences*, vol. 9, no. 1, 2019.
[16] M. Ravindran, "Cabled PCI express-a standard high-speed insterument interconnect," *2007 IEEE Autotestcon*, Baltimore, MD, 2007, pp. 410-417.
[17] R. Neugebauer, *et al.*, "Understanding PCIe performance for end host networking," *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, pp. 327-34, 2018.
[18] T. Du, and Q. Jia. "Design of Universal PCIe Interface Module Based on Vs," *IOP Conference Series: Materials Science and Engineering*, pp. 449, 2018.
[19] M. Mazidi, *et al.*, "The Avr Microcontroller and Embedded Systems: Using Assembly and C," Upper Saddle River, N. J.: Prentice Hall, vol. XIV, pp. 776, 2016.
[20] D. Q. R. Elizalde, R. J. P. Garcia, M. M. S. Mitra and R. G. Maramba, "Wireless Automated Fire Detection System on Utility Posts Using ATmega328P," *2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM)*, Baguio City, Philippines, 2018, pp. 1-5.
[21] Y. Patil, *et al.*, "Basic Logic Gate Detector Using Atmega328P and Android App," *HELIX*, vol. 9, no. 3, pp. 4937-4940, 2019.
[22] T. Nasution, *et al.*, "Electrical appliances control prototype by using GSM module and Arduino," *4th International Conference on Industrial Engineering and Applications*, pp. 355-358, 2017.
[23] V. Bharathkumar, *et al.*, "Microcontroller based digital meter with alert system using GSM," *11th International Conference on Intelligent Systems and Contro*l, pp. 444-448, 2017.
[24] K. Memon, *et al.*, "GSM based Android Application Appliances Automation and Security Control System using Arduino," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 2, pp. 206-210, 2017.
[25] Jablotron Alarms a.s., "Installation manual of JA-82K control panel," 2014.