A design of integrated alarm system for modern households

Václav Mach[*], *Jan* Valouch, and *Milan* Adámek

Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic

Abstract. This paper aims to design an Integrated Alarm System which has the same features and properties as commercially made alarm systems. The system should be able to communicate with all commercially-made alarm detectors, and it should be able to control other devices in the house. It also consists of the Ethernet interface which allows connecting the system to the Internet of Things. The alarm system is based on the Atmel platform, and it is built according to the standardization EN 50131-3: Control and indicating equipment. All components are described, and the function is in detail listed in the individual chapters.

1 Introduction

The Intruder Alarm system (IAS) is becoming one of the most important parts of the electronic part of each modern house. The system protects the possession and the life of the owner, and it is a part of the technical security which replaced the physical security. The physical security in the form of the real person is not reliable, and it is very economically inefficient to employ a person as physical security. According to the [6] “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 these problems, technical security with the alarm systems is nowadays prevalent.

The system can be combined with other systems such as fire system or with the smart house system. Intruder Alarm System with the combination of the smart house can be defined as an Integrated Alarm System. According to the author [5] “A smart home is one that incorporates advanced automation systems in order to provide its inhabitants, the sophisticated monitoring and control facilities over us various functions. For example, a smart home may have automated facilities for controlling lights, fans, air conditioners, temperature, multimedia systems such as home theatre systems etc., security, window, door operations, curtains.” In this case, the Intruder Alarm System is the main system which controls other devices. Very often The Intruder Alarm System is integrated with the Fire Alarm System. According to the [1] “Heat or Thermal detectors are most primitive one’s which works based on fixed temperature only. These detectors get activated based on a predefined temperature or in some case if there is an abnormal rise in temperature.”

Every Intruder Alarm System should consist of main components which can detect the intrusion into the protected object or area. The system also should be able to evaluate and process the incoming alarm signal from alarm detector, and the system must cause a reasonable response to the signal. According to mentioned information, every Intruder Alarm System should consist of following components:

- Control and Indicating Equipment
- Alarm detectors
- Uninterruptible Power Supply
- Communication interface

The author [4] also mentioned that “designed and implemented system to detect fire outbreak using camera image processing. Although this is a novel approach, it is not as efficient and accurate in detecting fire as a sensor-based system.” It means that cameras can be used by the Intruder Alarm System, not in the Fire Alarm Systems.

1.1 Control and Indicating Equipment

The Control and Indicating Equipment is the main part of the whole system. It periodically scans the inputs where the detectors are connected. The mainboard usually consists of the microcontroller which controls the whole system. To this microcontroller is also connected others chips which are responsible for the other communication such as Ethernet connection, Global Position System or programming USB port. Commercially made mainboard usually has the interface to the second board where other chip is responsible for the communication between connected detectors. The customer can have different requirements for the number of connected detectors. That’s the reason why commercially made mainboards have separated board for the detectors. The author [7] stated that “Each CIE must be manufactured according to the standard EN 50131-3: Control and indicating equipment.” All components such as detectors, must be constructed according to this standard.

[*] Corresponding author: v2mach@fai.utb.cz

1.2 Alarm detectors

There are many alarm detectors on the market. The detectors can be divided according to its application to many categories. Each category has a different usage in the alarm systems. Each detector must be connected to the CIE. There are several ways how the detector can be connected to the CIE:

- Wireless connection
- Wire connection
    - Analogue connection
    - Digital connection

The digital connection is usually provided using a common bus for several detectors. Each detector has a unique address which is saved in the CIE. This address is also saved in the detector. The biggest advantage of the digital connection is that several detectors can be connected into one buss. The analogue connection is much more complicated. The analogue connection is based on the voltage loop where several detectors are connected in one loop. The difference between detector is ensured by the resistor which has a different value for each detector. This difference is evaluated by the CIE.

The detectors have several states which must be evaluated by the CIE. These states are Idle, Alarm, Failure, Short-circuit, and the Antimasking. According to [2] “Anti-masking is a motion ability to detect if an intruder has attempted to defeat the detector by blocking it with a material that blocks infrared energy, such as paper, tape, film, or spray.” When the detector is triggered, it automatically sent the signal to the CIE.

2 Hardware Design

The design of the CIE is based on the common commercially made system which can be found on the market. The system is divided into the Main-board which is responsible for the controlling connected devices, and the Zone-Board which is responsible for the reading from connected detectors. Both boards are based on the ATmega2560 the microcontroller which is used in the Arduino MEGA board. Boards have own design with the same function to ensure easy programming via the Arduino interface.

2.1 Main-board

The main-board is composed of two ATmega2560 the microcontrollers. The author [10] mentioned that “ATmega2560 the microcontroller has 256kB Program Space, 4 UARTs, 14 PWM, 16 Analog Inputs, 54 Digital I/O ports.” The first one is responsible for the whole system, and it has the highest rights in the system. The second one is responsible for the communication via the Ethernet. This communication is established by the W500 which is used in the Arduino Ethernet board. According to the [9] “Ethernet board makes possible to link the data with a router through an IP address that is within the range of addresses unused. Thus, it was possible to incorporate features in the prototype server that allow the user to manipulate the system from anywhere as long as access to the Internet or a local area network is obtained” Author [9] also mentioned that “For the design of the website, information from Arduino was used as a reference for the web servers, where, using HTML, details are presented to create a web page from analogue readings.”

The main board also has pinheads which can be used to connect standard Arduino boards. In this case, the GSM board is mounted on the main-board. Author [8] mentioned that “GSM board is based on the controller SIM900 by SIMCOM. It supports GSM/GPRS standards and operates at the frequencies of 850, 900, 1,800 and 1,900 MHz. The shield can be connected directly to the board of Arduino Uno by a set of pins mounted at the bottom of the printed circuit board.”

On the sides of the board, there are placed others pins that are used to communication between other boards. On the right side, there are serial communication interface for the Zone-Board (ZONE-TX, ZONE-RX), GPS-Board (GSM-TX, GSM-RX), Keypad-Board (KEY-TX, KEY-RX), and the optional board (OPT-RX, OPT-TX). Each board can be connected to the USB hub which can be used for the programming, or it can also be used for the direct communication with the connected computer. In the corner is situated the power connected to the 12 V/DC. On the left side of the board are situated state signals for the Ethernet chip. These signals are representing the current state of the Ethernet communication. On the top is placed standard pinhead for the Arduino boards. Any of the standard Arduino boards can be used as an extension of the current system. The design of the Main-board can be found in the following figure.

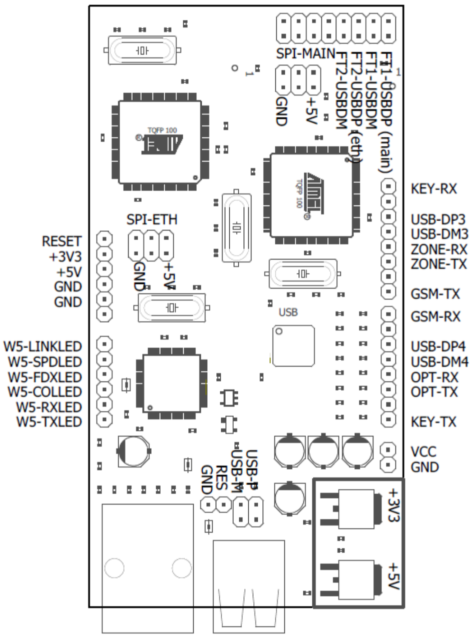


Fig. 1. Design of the Main-Board

The board also consist of headers which can be used to connect other devices. Connected devices should communicate via the serial interface, which is implemented on the main board. The board has USB hub which allows to connect up to four devices by one cable placed on the side of the board.

2.2 Zone-Board

The Zone-Board also consist of the ATmega2560 the microcontroller. This board is focused only on the analogue detection. It means that only detectors which are connected by the analogue loop can be connected to this board. Board provides 16 independent loops, and each loop can hold up to three detectors. This makes it possible to connect 48 analogue detectors to the Zone-Board. This number is sufficient for most households.

Each loop also has the protection against the sabotage by the intruder. The combination of the Transient Voltage Suppression (TVS) diode and the resettable fuse protects the main processor against the overvoltage which can be applied the vires. This protection is effective up to 1 kV and 10 A. [11] Each loop can be programmed independently using standard modes such as Normally Closed (NO), End of Line (EOL), Double End of Line (DEOL) and Advanced Technology Zone (ATZ). Each mode comes with some advantages and some disadvantages. The most used mode in the analogue loops is the ATZ mode which has the biggest possible number of connected detectors in one loop, and it is still possible to distinguish between each detector in the loop. This function is caused by using different values of the resistors which are bypassing each detector. The connection between the Zone-Board and the Main-board is established using the serial interface. The board with the labels can be found in the following figure.

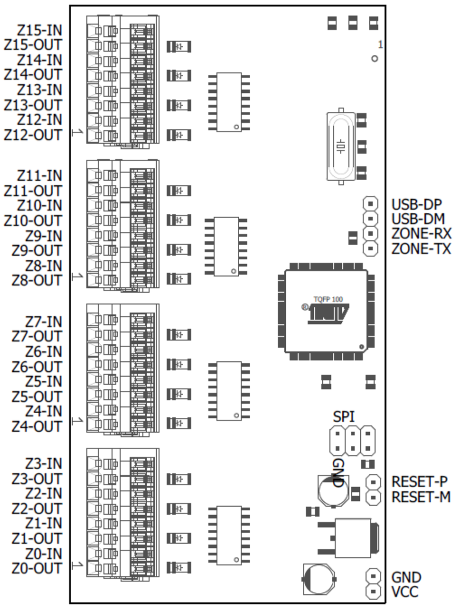


Fig. 2. Design of the Zone-Board

Each loop has its socket which consists of two terminals maned IN for input and OUT for output. The socket also has the power terminals for the connected detector. Common power voltage of the alarm detectors is 12V/DC. This voltage is connected to the UPS in case of power failure. On the opposite side of the terminals are situated pins for communication with the main board. There also programming pins which can be connected to the USB hub. The connection of the detector must follow the specified standard which guarantees flawless operation. As mentioned before, each loop can handle several modes which are used in the alarm systems. The most common mode for the analogue connection is the ATZ. The schematic can be found in the following figure.

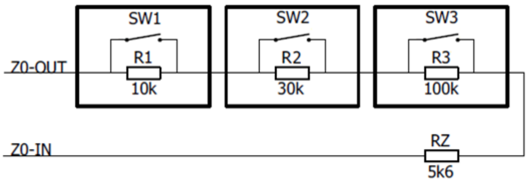
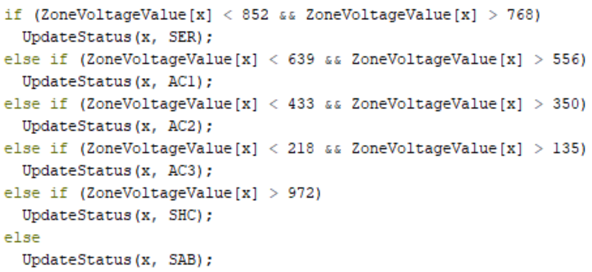


Fig. 3. Design of the Advanced Technology Zone [11]

The mode consists of three independent detectors. When commercially made alarm detector detect the intruder, it activates the switch which is bypassed by the resistor. This cause that the resistor in the loop is changed according to the activated detector. This change can be measured by the CIE. Each detector has different value; it causes that resistors can be distinguished from each other by the CIE. A special resistor is added at the end of the loop. This resistor allows for distinguish between the idle and the sabotage state. The previous study [11] found that this concept can be extended by using the logarithmic scale of the resistors to increase the maximal possible states up to 12 to one loop.

3 Software Design

The critical program of the whole system is the detection program which is responsible for the proper reading the values from each loop. The main evaluation is done in the Zone-Board, and the alarm message is then sent to the Main-board. The program itself does not need any special library or special implementation. It only uses the built-in function for reading the analogue values from each loop. The basic program can be found in the following figure.



```
if (ZoneVoltageValue[x] < 852 && ZoneVoltageValue[x] > 768)
  UpdateStatus(x, SER);
else if (ZoneVoltageValue[x] < 639 && ZoneVoltageValue[x] > 556)
  UpdateStatus(x, AC1);
else if (ZoneVoltageValue[x] < 433 && ZoneVoltageValue[x] > 350)
  UpdateStatus(x, AC2);
else if (ZoneVoltageValue[x] < 218 && ZoneVoltageValue[x] > 135)
  UpdateStatus(x, AC3);
else if (ZoneVoltageValue[x] > 972)
  UpdateStatus(x, SHC);
else
  UpdateStatus(x, SAB);
```

Fig. 4. Program for the Zone-Board [11]

The previous figure shows the program for the ATZ mode. This mode compares the measured voltage level with the threshold values which are calculated according to used resistors. Each state has some tolerance which can be found in the previous figure. According to the standard EN 50131 - General requirements, the CIE must be able to capture alarm signal which lasts longer than 400 microseconds. The frequency of the reading on each loop is only 10 microseconds.

Zone-Board only detects the intruder by the connected alarm detectors. The alarm message is then sent to the Main-Board which the evaluates the received message. The final alarm triggering depends on the internal conditions in the program. These conditions are based on the zones, time, and the arming. All information must be imported into the system, and it should be changed by the user. The system also consists of the Ethernet connection which allows creating the web sides. The setting can be changed by the user, or it can be changed by the certificated person via the Ethernet connection. The Ethernet connection can also be used for transmitting the alarm message to the Alarm Receiving Centre (ARC).

4 Conclusion

This research proved that Intruder Alarm System could be controlled by the Atmel platform. The introduction consists of all needed information and standardization. The system is composed of two boards. The Main-board is responsible for the whole system, and it also provides a connection via USB and the Ethernet. This board meets the standard EN 50131 - General requirements. The Zone-Board is responsible for the flawless connection of the detectors. The designed CIE can address up to 48 detectors. The whole system can be connected and controlled by the Internet of Things via the Ethernet connection.

The system can be extended by other non-alarm application such as lighting, heating, air conditioning, blinds, irrigation, sound. This feature can be achieved by the extended relay board, and it can also be extended by the GSM module. The further research can be focused on special extending board and software implementation for the non-alarm system.

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Programme project No. LO1303 (MSMT-7778/2014) and also by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089 and by the Internal Grant Agency of Tomas Bata University under the project No. IGA/CebiaTech/2018/004

References

1. S. Suresh, S. Yuthika G. Vardhini. ICTBIG. (2016).
2. Ch. Song-Shyong, K. Wang, W. Li, W. Chen. ICAMSE. (2016).
3. J. Valouch. CASEDRBCCCIS. (2012).
4. A. Imteaj, T. Rahman, M. Hossain, M. Alam, S. Rahat. ECCE. (2017).
5. M. Shariqsuhail, G. Viswanathareddy, G. Rambabu, C. Dharmasavarni, V. Mittal. ICACCI). (2016).
6. J. Landa, Ch. Jun, M. Jun. ICMTMA, (2017)
7. J. Valouch. AMM. (2015)
8. M. Pospisilik T. Smekal, M. Adamek, P. Neumann, T. Dulik. CSCC. (2016)
9. C. Algarín, J. Cabarcas, A. Llanos. E **6**(4) (2017).
10. S. Umbarkar, G. Rajput, S. Halder, P. Harname, S. Mendgudle. ICCASP. (2017).
11. V. Mach. Hybrid. T. **5** (2), (2016)