

LIMITATION OF THE ADVANCED TECHNOLOGY ZONE

Václav Mach, Milan Adámek, Jan Valouch and Miroslav Mušálek



This Publication has to be referred as: Mach, V[áclav]; Adamek, M[ilan]; Valouch, J[an] & Musalek, M[iroslav] (2018). Limitation of the Advanced Technology Zone, Proceedings of the 29th DAAAM International Symposium, pp.0719-0724, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-20-4, ISSN 1726-9679, Vienna, Austria

DOI: 10.2507/29th.daaam.proceedings.104

Abstract

This article deals with the limitation of the Advanced Technology Zone (ATZ) which is one of the common methods of connecting analogue alarm detectors to the Control and Indicating Equipment (CIE). The ATZ model can handle up to three independent detectors. The modern alarm system can have thousands of detectors. However, the standard ATZ mode is not able to provide the sufficient number of alarm detectors. The new design should determinate and increase the maximal number of connected detectors to the CIE by using the low-tolerance bypassing resistors. All created ideas come with the technical details and the design was tested to ensure flawless and reliable operation in real time.

Keywords: intruder alarm system; control and indicating equipment; advanced technology zone; detector

1. Introduction

The Intruder Alarm System (IAS) is a part of technical security which can indicate the intrusion to the protected building or area. According to the [9] 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 concept is driven by the standard CSN EN 50131. The standard is divided into several parts that describe single areas. [5] The most important standard for this article is the CSN EN 50131-1 Control and indicating equipment, which consists of information and parameters which every product must accomplish. The CIE is the main component of the IAS. It consists of several components which are responsible for each function. These functions are:

- It receives and evaluates the signals from the detectors.
- It provides the power to the connected detectors and other equipment
- It allows system diagnostics
- It controls signaling, transmission, recording, and other functions that indicate the current conditions.

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. The author [8] stated that each CIE must be manufactured according to the mentioned standard EN 50131-3.

According to the evaluation of incoming signal, the commercial CIE can be divided into two groups. First group using digital interface and second using analogue interface. Digital CIE using only one bus which typically consists of four cables. This manner allows to connecting several detectors to one bus. Detector evaluates actual state which is then sent to the CIE in binary form. [1] CIE using analogue loops evaluates actual state of each zone. Each loop has the maximum amount of connected devices according to used mode. These modes are Normal Closed (NC), End of Line (EOL) and ATZ. The most used mode is ATZ because it provides the biggest amount of possible connected detectors from all mentioned modes. Even nowadays ATZ mode is still commonly used in many applications.

ATZ mode still has many disadvantages and possible threats. One of the biggest disadvantages is the number of connected devices which is limited usually up to three devices. [2] This is given by a huge tolerance of terminating resistor which is usually 30%. It means that states between each other must have a huge gap. This situation helps with the selection of terminating resistor but it inefficiently uses the working range. The biggest threat is that every commercial CIE has only basic protection against overvoltage which can destroy CIE by the potential intruder. This protection is done using one-use fuse which is installed in each loop. [3] When higher voltage passes the fuse it becomes interrupted. The interrupted loop is not working anymore. In this case destroyed fuse must be replaced.

This article deals with mentioned disadvantages and it tries to bring a new solution. For purposes of this research, a prototype of new CIE was created. The sub goal is to increase the number of connected detectors to the maximum. This design can bring the ATZ mode to the same level as the digital manners.

2. Advanced technology Zone

ATZ mode uses different values of resistors. Different values can very precisely distinguish between individual detectors. Each detector has a resistor with a unique value. In real operation, multiple detectors are connected into several groups. Each group uses the same value of resistors. In general, the ATZ variant has three detectors, but each individual group can be distinguishable. It can be done by using different values of resistors. This variant is limited by the final numbers of used groups. Usual ranges of values are $R_A = 3k9 \Omega$, $R_B = 10k \Omega$ and $R_C = 18k \Omega$. Adding more resistors can result in difficulties in distinguishing between groups. Each group can contain up to three detectors. Described mode can be found in the following figure.

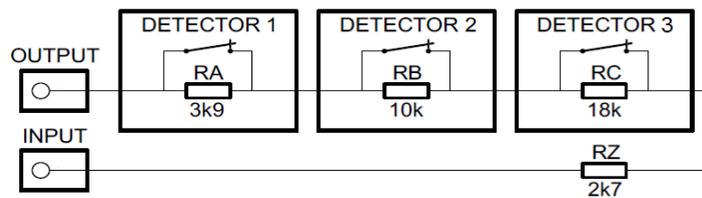


Fig. 1. Advanced Technology Zone loop.

Every detector has connected in parallel the resistor. When the detector is triggered, the switch opens and the resistor is not bypassed anymore. This change can be measurable by the CIE and then evaluated. The evaluation is made by the program which has threshold values to detect current state. Threshold values for this article are shown in Table 1. Every loop should be able to distinguish between basic states. These states for every variant are Serenity Alarm, Failure and Sabotage.

Serenity and Alarm state are very easy to identify. The tricky part comes with the detection and subsequent distinction between Failure and Sabotage. In the NC variant, it is almost impossible to distinguish between them. In such case, Failure must be detected as Alarm. The connected detectors can have some additional outputs like tamper or anti-masking. These connections must be wired in the correct way according to the device manual and also an appropriate version must be used.

3. Designed Hardware

Every analogue CIE consists of Analog to Digital Converter (ADC) which converts the analogue signal to the binary form. Usually, this converter is already embedded into the microcontroller. Designed protection consists of output part and input part. Input part should process not only the continuous signal but it also should process binary pattern. This pattern provides better protection against sabotage because is almost impossible to imitate random binary signal which is generated by the CIE. Due to this situation, every output of the CIE can be controlled. The control part is galvanically separated using an optocoupler to protect CIE from any other threats.

The diode in the forward direction is placed in the circuit to protect also the power supply against overvoltage. The diode is dimensioned up to 1 kV. Another active protection is the Transient Voltage Suppression (TVS) diode in combination with the resettable fuse. [4] TVS diode acts as a normal diode with the threshold voltage. In this case threshold voltage is set to 11 V. When this voltage is exceeded diode becomes to the short circuit mode and voltage is passed to the Ground (GND). [5] In the same time resettable fuse disconnects the circuit due to the big current from the external power supply. TSV diode can turn back from the short circuit state after the voltage drops back under 11 V. Also the resettable fuse can turn back to the connected state. It means that this protection is non-destructive.

The input part consists of a twin set of TVS diode and resettable fuse as well as the output part. Before voltage gets to the ADC it passes through the voltage divider. Operating voltage of the circuit is 10,9 V. But the maximal voltage level which can be applied to the ADC is only 5 V. The entering voltage must be lowered using the voltage divider.

Voltage divider uses resistors with values 10k Ω and 12k5 Ω . It means that output voltage of the voltage divider is 4,84 which is safe for the ADC built in the microcontroller. This precise value is used to evaluate short circuit state of the loop. All modes use NC contact and resistor in the loop. When the detector is activated, it opens the NC contact. It causes that connected resistor is no long bypassed and the resistor is connected to the loop. [4] ATZ mode uses several resistors with different values to identify, which of these resistors were connected to the loop. The total value of the resistor in the loop is changing by adding more resistor to it. This change is detected and evaluated in the CIE.

Before final evaluation, entering voltage must be converted using ADC. Used ATmega2560 the microcontroller has a built-in 1024-bit converter. It means that range of entering voltage is converted into numbers from 0 to 1023. This conversion is critical because it must consist of all states and tolerances. Selected values of used resistors should have an exponential rising tendency. This tendency helps to achieve a linear order of resulting voltage. Created design needs also software extension.

4. Extension

One of the biggest disadvantages is the limited amount of connected detectors. Every commercial made CIE has 30% tolerance of the resistor which is connected to the bypassing switch. This tolerance is given by the environmental influence which can cause the unexpected change of the resistor. It means that only three detectors can be connected into one loop. This problem can be solved by using lower tolerance with considering the environmental influence. Considering must cover the temperature differences, loop length, and other physical influence.

The most common influence is by the temperature difference which can rapidly change the resistor value. New design using 5% tolerance instead of 30%. This reduction brings more detector which can be added to the loop without any interference. According to the [6] and [7], average resistor deviance to the changing temperature is 1% in both directions. It means that the real value of each resistor can change during the temperature shift. This tolerance must be included in the final program. Following table shows the values of calculated resistors.

Current State	Value of ADC	Input voltage	Active resistor
-	[-]	[V]	[k Ω]
Short-circuit	1024	4,84	0
Serenity	915	4,33	2k7
Active - RA	851	4,02	1k9 + RZ
Active - RB	792	3,75	3k9 + RZ
Active - RC	718	3,40	6k9 + RZ
Active - RD	655	3,10	10k + RZ
Active - RE	588	2,78	14k + RZ
Active - RF	534	2,52	18k + RZ
Active - RG	469	2,22	24k + RZ
Active - RH	410	1,94	30k + RZ
Active - RI	338	1,60	43k + RZ
Active - RJ	284	1,34	56k + RZ
Active - RK	213	1,01	83k + RZ
Active - RL	159	0,75	120k + RZ
Sabotage	0	0	Infinity

Table 1. Calculated values of resistors.

Own values of resistors were used to achieve the satisfying number of the possible detectors connected to the loop. Presented values are not very common but all these values can be found in the market. Listed values of the resistor must have only 1% tolerance to achieve maximal states without interference or overlapping. Resistors with this tolerance are very usual and it can be very easily found in the market.

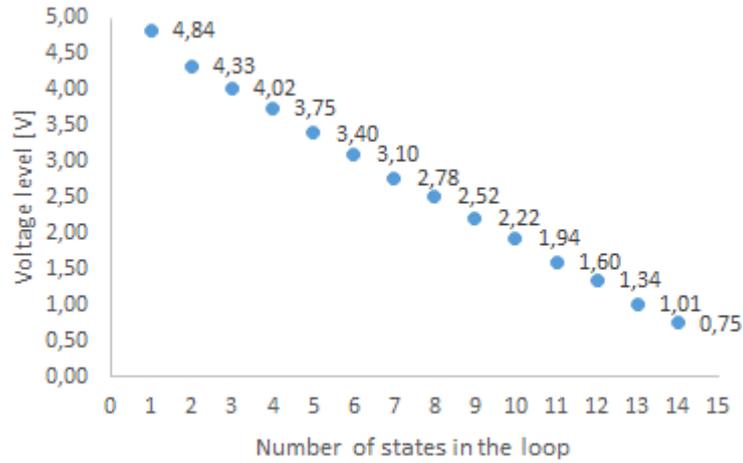


Fig. 2. Graphical representation of the calculated resistors.

Presented values can create up to twelve unique detectors which can be added to the loop without any distortion. Every value was tested using the formula to ensure that even with temperature influence will not change the resulting value. The formula for the temperature dependence of the resistance is shown below.

$$R = R_0 \cdot (1 + \alpha \Delta t) \tag{1}$$

- R - Resulting resistance
- R₀ - Influenced resistor
- α - Temperature coefficient of electrical resistance
- Δt - Temperature difference

All resistor can be checked using the previous formula to check temperature drifting. The common temperature of the resistor should be 22°C. According to the CSN EN 50131 [5] temperature range for the alarm device should be from -25°C to +60°C. Due to this standard, every value of the resistor was checked. Shifting resistance of each resistor can be found in the following table.

Current State	Minimal -25 °C	Normal +22 °C	Maximal +60 °C
-	[kΩ]	[kΩ]	[kΩ]
Short-circuit	0	0	0
Serenity	2,8	2,7	2,6
Active - RA	4,7	4,6	4,5
Active - RB	6,7	6,6	6,4
Active - RC	9,8	9,6	9,4
Active - RD	12,9	12,7	12,4
Active - RE	17,0	16,7	16,3
Active - RF	21,1	20,7	20,2
Active - RG	27,2	26,7	26,1
Active - RH	34,3	33,7	32,9
Active - RI	46,6	45,7	44,6
Active - RJ	59,8	58,7	57,3
Active - RK	87,3	85,7	83,7
Active - RL	125,0	122,7	119,8
Sabotage	-	-	-

Table 2. Resistance shifting.

The previous table shows the tolerance which must be considered in the evaluating process. Calculated values must be converted to the ADC levels mentioned before. Created voltage levels are shifted from each other by 0,3 V. Created gap and 5% tolerance helps against any overlapping or distortion.

5. Measurement

The experiment was done in the laboratory of Tomas Bata University in Zlin at the Faculty of Applied Informatics. Used components are listed below.

- ATmega2560 the microcontrollers
- Digital multi-meter M-3900
- Power supply LBN-303 0-30V/0-3A
- Designed PCB

The Printed Circuit Board (PCB) was created, to confirm that designed system is working. Tested PCB was connected to the power supply. The pin named OUT was set to logic 1 using the test program. This change causes that optocoupler activated the loop. Each resistor was added to the loop and by the ADC in the microcontroller entering voltage was measured and displayed. Every detector in the experiment was represented by the switch. Also, the temperature impact was applied to ensure flawless operation. The measurement was primarily focused on the independent states, which can occur. Measured levels are presented in the following Figure 3. The measurement shows designed levels of each state. Presented states are given by the resistor values in Table 1.

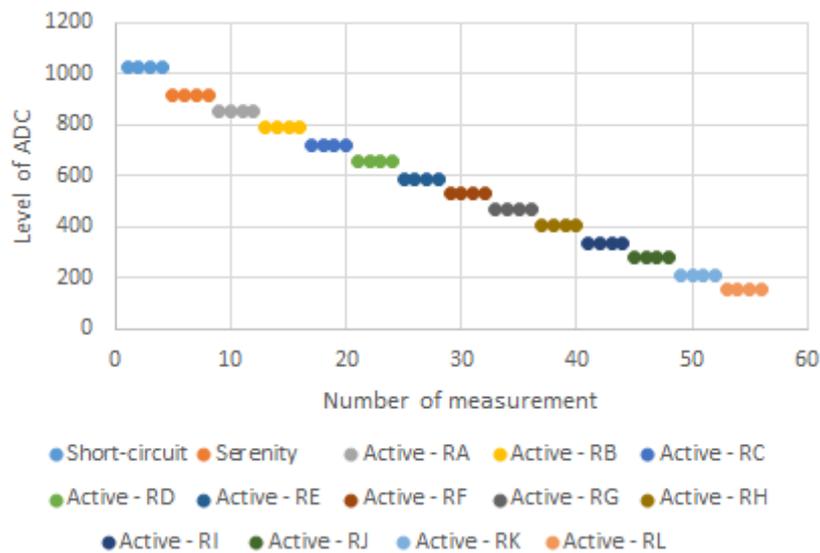


Fig. 3. Measurement results of each state.

Several measurements of each state were taken to obtain a satisfactory amount of data. Even with this amount of values, states are very stabilized according to calculated values from Table 1. From Figure 3 can be seen the gap between each state to ensure minimal possible distortion or overlapping. This gap is also sensitive to the length of the loop. According to this problem, before real-time operation, the resistance of the cable must be considering and subtracted from the RZ.

6. Conclusion

The aim of this paper was to increase the number of connected detectors to the ATZ. Existing CIEs provides only three detectors. However, presented design provides up to twelve independent detectors in a single loop. This growth causes, that the ATZ can keep up with the modern digital connection. Presented design using the low-tolerance resistor to achieve maximal detectors connected to one loop. The design also considering the environment influence. With this design, the ATZ mode can be still used in the alarm application. All measurements were done using the 8-bit ADC embedded in ATmega2560 the microcontroller. Future research can be focused on the rising of the operating voltage over 12 V which can ensure more possible levels for the alarm detector.

7. Acknowledgement

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

8. References

- [1] Mach, V. (2016). Hardware Protection of Metallic Loops Against Sabotage, Trilobit, pp 1804-1795.
- [2] McLaughlin, R. Brooks, D. (2006). A study of the compliance of alarm installations in Perth, Western Australia: Are security alarm systems being installed to Australian Standard AS2201.1, Australian Information Warfare and Security Conference, pp. 0955-1662.
- [3] Hanacek, A, Sysel, M. (2015). 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.
- [4] Hanacek, A, Sysel, M, (2016). Design and Implementation of an Integrated System with Secure Encrypted Data Transmission, Automation Control Theory Perspectives in Intelligent Systems, pp 217-224.
- [5] CSN EN 50131-1 ed. 2. (2007). Alarm systems - Intrusion and hold-up alarm systems - Part 1 System requirements. Prague.
- [6] Shahnewaz, A. (2016). Embedded Home Surveillance System, 19th International Conference on Computer and Information Technology (ICCIT), pp 42-47
- [7] Juhana, T; Anggraini, V, (2016). Design and Implementation of Smart Home Surveillance System, 10th International Conference on Telecommunication Systems Services and Applications (TSSA), pp 2372-7314
- [8] Valouch, J. (2015). The Proposal of Methodology for Evaluating the Effectiveness of Alarm Systems. Applied Mechanics and Materials. pp 183-88. doi:10.4028/www.scientific.net/amm.736.183.
- [9] Landa, J, Chu J, and Miao J. (2017). Implementation of a Remote Real-Time Surveillance Security System for Intruder Detection. 9th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), doi:10.1109/icmtma.2017.0032.