Hardware protection of metallic loops against sabotage

Václav Mach

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

v2mach@fai.utb.cz

ABSTRACT

This article deals with the protection of metallic loops against sabotage. Basic hardware solutions are examined as an essential element that can protect the Control and Indicating Equipment (CIE) against brute force attacks like overvoltage. To increase the security level, a new possible design of loop protection is designed. Assembled electronic device is then measured and discussed. Part of these issues is described in images that contain labels and values of the used components.

INTRODUCTION

The most common way how to connect detectors to the CIE is by using a digital bus. Several detectors can be connected to the bus. This provides many advantages such as smaller length of cable, better communication, and connectivity. Despite of these advantages, there are still some situations where metallic loops can be used. Due to the specialization of this article, any weaknesses of detectors are disregarded. This article is focused only on the possibilities of protection of the loop and evaluating circuits. [1,3,5]

Basically, protection of the metallic loops can be divided into Hardware and Software type. Hardware protection means selection, application, and wiring of electronic components. Used components can address undesirable conditions which can occur, such as overvoltage or short-circuit.

Companies do not provide their schematics to the public. But own testing proved that every CIE has some kind of basic protection against destruction. Basically, only high overvoltage can destroy the CIE. Due to this problem, every input of the loop has at least a fuse installed. But these are only single-use fuses. [5] The main goal of this article is to design a new concept of possible protection of metallic loop.

The new concept should consist of completely new schematics which must be in principle compatible with commercial CIEs. It means that should be possible to use the design in any possible manner of commercial connection. Moreover, the design should be able to protect the CIE without any damage. This new concept of protection is described in the following chapter and measurement with results of the design solution is listed in the last chapter.

HARDWARE METHODS OF PROTECTION

The actual state of the loop is determined by voltage level, which is measured at the input terminal. This voltage can be affected by a set of several resistors connected into the loop. This is typically done by the resistor which is bypassed by the Normal Closed (NC) contact. [5,6] When the detector activates the contact, the bypassed resistor is connected to the loop and it causes a voltage drop, which can be measured.

All modern CIEs operate in digital form. So, the analog signal from the loop must be converted using an Analog to Digital Convertor (ADC). This causes the first problem. If overvoltage occurs, additional components must be used to protect the CIE against destruction.

For purposes of this research, the own model of CIE was created. Every CIE contains a microcontroller which can measure and evaluate the actual state of the loop. The ATmega2560 microcontroller is chosen for this situation because it has enough pins to connect several loops just like in commercial CIEs. But the microcontroller operates at 5 V and every commercial detector operates at 12 V. So there must be a voltage divider, which reduces the voltage. A basic voltage divider is shown in the following figure. The Equation (1) describes this schematic.

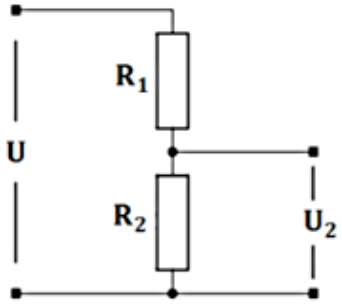

Figure. 1. Voltage divider [1]

An additional diode is added to the loop to protect also the power part. According to the datasheet, the protection diode consumes 1.1 V. It means that operating voltage should be 10.9 V. The diode is dimensioned up to 10 kV, so it is protected against high voltage very well. After that, the values of resistors can be evaluated using the formula listed in Equation (1).

$$U_2 = U \cdot \frac{R_2}{R_1 + R_2} \tag{1}$$

$$U_2 = 10.9 \cdot \frac{10k}{12.4k + 10k} \tag{2}$$

$$U_2 = 4.87\ V \tag{3}$$

The main goal is to achieve maximum voltage U_2 under 5 V. From the previous Equation (2) it is evident that resistors with values R_1=12.4 kΩ and R_2 = 10 kΩ fit well in this situation. By using these values, even a direct short-circuit does not destroy the connected ADC. The tens of kΩ used help to keep power consumption at a low level, which is also needed.

The new electric circuit should protect the microcontroller against overvoltage, which can be applied directly to it. This protection is done by the component called Transient Voltage Suppression (TVS) and resettable fuse. TVS is a normal diode, with a threshold

voltage set to 12 V in this case. When this voltage is exceeded, TVS switches to short circuit mode and voltage is passed to Ground (GND). At the same time, the short-circuit current turns the fuse off. This situation can be seen in Figure 2.

The output of each loop is connected to the optocoupler which is used for voltage shifting from 5 V to 12 V. It also serves as a protection of the microcontroller against overvoltage. There are several possibilities how loops can be designed. Each mode needs a special composition of used resistors. But the most used mode is Advanced Technology Zone (ATZ), which is described in the following chapter. [1]

ADVANCED TECHNOLOGY ZONE

This mode allows distinguishing which detector in the loop has been activated. It is based on the different values of used resistors. Every resistor has its own bypassing switch, which can be activated by the connected detector. Using different values of resistors causes a step in the level of current. Such steps can be evaluated and distinguished later. The voltage levels differ approximately by 1 V between steps, as can be seen in Table 1. [1] The following figure describes the functional schematics which was created. It is composed of protective components such as an optocoupler, diode, TVS, resettable fuse and voltage divider.

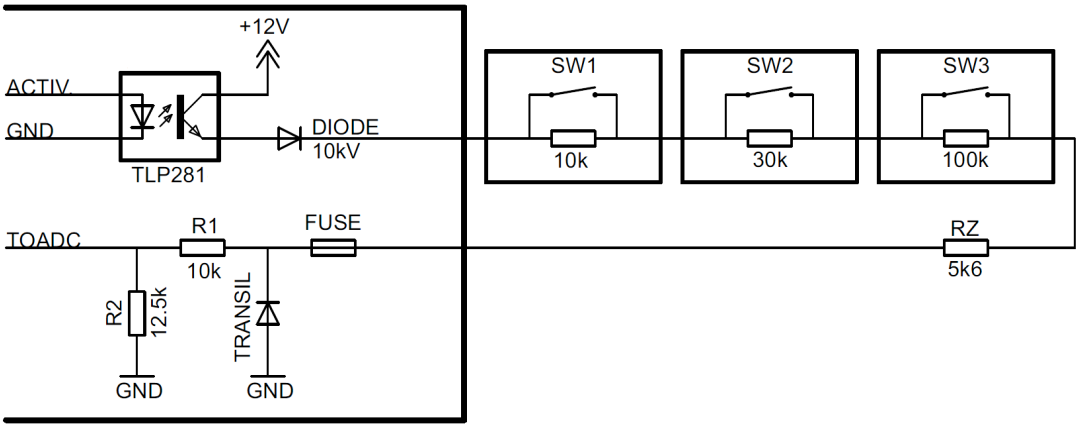

Figure. 2. Advanced Technology Zone wiring [1]

In common situations, the loop can be divided into three independent zones according to voltage level shifting. For proper function, these resistors are selected in exponential order as 10 kΩ, 30 kΩ, and 100 kΩ. [1] No components and no measuring systems are perfect, so there must be a tolerance in the chosen values. Input voltage must be converted in 10-bit ADC. The following table shows the range of all of these values.

State	Max Value	Min Value	U max	U min
-	-	-	[V]	[V]
Short-circuit	1023	972	4.87	4.67
Serenity	852	768	3.69	4.09
Active -1	639	556	3.07	2.68
Active -2	433	350	1.68	1.08
Active -3	218	135	1.05	0.65
Sabotage	41	0	0.2	0

Table. 1. Calculated threshold values

The previous table also shows that states have a 5% tolerance total and the level between each state is 11%. That really helps with distinguishing between the states. The final evaluation is explained in the following chapter. ATZ is one of the most used modes. It is capable of distinguishing all the possible states which can occur in the mode. There are at least 6 states which are listed in the previous table. This mode can provide more states by decreasing tolerance between levels and states. Basic states of the loop are the following:

- Serenity
- Alarm
- Short-Circuit
- Failure

The Serenity and Alarm state are very easy to identify. These states can be very easily evaluated with calculated values and compared with created tolerance. Different values of resistors help to distinguish between each detector in the current loop. Short-Circuit can occur when an intruder attempts to connect an external wire right into the terminal in the CIE. This state must be detected as Alarm by Short-Circuit. The same situation comes with Sabotage when the intruder attempts to cut the loop. This situation must be evaluated as Alarm by Sabotage. The last state, which is not in the previous table, is Failure. Failure occurs when neither state corresponds to the measured value. [1,2]

SOFTWARE EXTENSION

The used ATmega2560 contains an ADC, so the circuit in Figure 2 can be directly connected to the input pins. The output can also be connected to the ADC. In this case, additional software must be created. The program should consist of conditions which can distinguish between the values from the Table 1.

The main program is written in the C language and for simplicity, only the main basic functions and conditions are used. Part of the program can be found in the following figure.

```
case ATZ:
  if (ZoneVoltageValue[x] < 852 && ZoneVoltageValue[x] > 768) // Serenity
    else if (ZoneVoltageValue[x] < 639 && ZoneVoltageValue[x] > 556) // Active-1
      else if (ZoneVoltageValue[x] < 433 && ZoneVoltageValue[x] > 350) // Active-2
        else if (ZoneVoltageValue[x] < 218 && ZoneVoltageValue[x] > 135) // Active-3
          else if (ZoneVoltageValue[x] > 972) // ShortCircuit
            else // Sabotage
```

Figure. 3. Program with threshold values for ATZ mode [1]

The part of the program in Figure 3 shows how it created states can be evaluated. Before evaluation, the signal must be read from the pin of the microcontroller and then put into the ***ZoneVoltageValue[x]*** variable. Each condition can send a different signal to CIE.

MEASUREMENT RESULTS

To prove the designed circuit, a simple Printed Circuit Board (PCB) was created for testing. The most important values are shown in Figure 4. All measured values should be in tolerance with the range listed in Table 1. Figure 4 shows a regularity in the levels of each state.

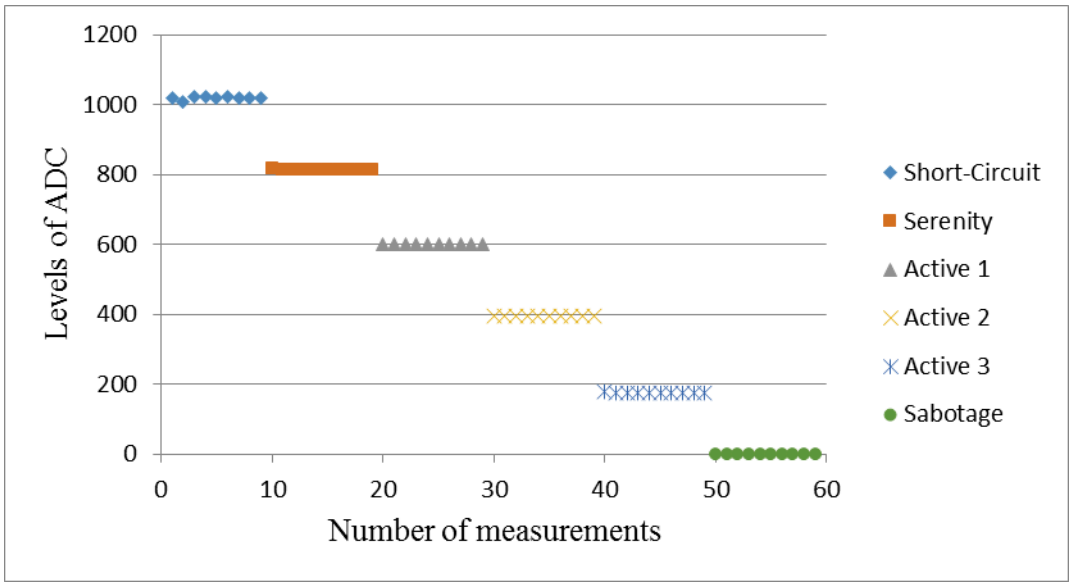

Figure 4. Measurement results

CONCLUSION

A prototype of the protective circuit that can protect the internal components against any kind of external sabotage was created. It has also maintained the designed levels very well between each state. Overvoltage was tested only at 24 V to ensure personal safety. The designed circuit shorted high voltage to GND in order to protect the internal logic. All tests were successful. The 11% gap between states can be made much smaller to achieve more states.

More research can be done using an extension of this design. With more components, there can be added some digital signal to avoid sabotage. That received signal can be also evaluated and compared with the transmitted. Another way can be in increasing the levels of the loop.

REFERENCES

[1] MACH, V. An Integrated Alarm System. Zlin, 2016. Tomas Bata University in Zlin, Faculty of Applied Informatics

[2] CAPEL, Vivian. Security systems and intruder alarms. 2nd ed. Boston: Newnes, 1999. ISBN 075064236X

[3] BROOKS, David J. Intruder alarm systems: Is the security industry installing and maintaining alarm systems in compliance to Australian Standard AS2201 Security Journal. 2011, 24(2), 101-117. DOI: 10.1057/sj.2009.12. ISSN 0955-1662

[4] HANÁČEK, A. Security methods of wired central ESS against sabotage. Zlin, 2010. Tomas Bata University in Zlín. Faculty of Applied Informatics

[5] MACHEK, O. Microprocessor Based Security System. Brno, 2009. Brno University of Technology.