In this article I present a novel design of a testing device for the hardwired zone control panel or zone expander input of a burglary alarm systems.

In the hardwired zone input, the contact or switch of the sensing device, usually combined with two resistors, is connected to the zone input of the burglary control unit or to the input of the zone expander of the burglary control unit.

The activation of a contact or switch shorts or opens one of the serial resistors and thus changes the overall loop resistance. The changes in loop resistance will cause a burglary control panel's status change from Normal to Alarm, if burglary system is Armed, or to Trouble, when the system is Disarmed.

Additionally, abnormal events such as when the zone loop wires between contact or switch and the zone input device become shorted or cut, will also generate Alarm signal.

The greatest advantage of the hardwired zone input type is that any changes of the zone loop resistance will generate adequate burglary alarm status immediately within the time limits described by the burglary alarms systems Standard ,so that the hardwired connections are constantly supervised.

However, a serious disadvantage of the hardwired connection is that it is really easy to compromise or default the zone loop. This will be discussed below.

Because the hardware zone loop is powered by a constant voltage level delivered by the burglary control unit or a zone expander, it is very easy to apply devices that can read and remember the voltage level in the zone loop, and later, on a request, they feed it back to the zone loop.

When, for example, this voltage level represents the status of “closed door” (window or other barrier), after applying the compromise technique is applied, opening the door, (window or other barrier) will not affect the zone loop voltage level, because a burglary control unit sees the zone loop status as not changed . In this way someone can access a protected area without being noticed.

Figure 1 shows a simplified example of compromise tactics and a device, and a way of taping it to the zone loop wires. These types of device allow to compromise the protected zone loop for a time frame up to 30 minutes, or even longer.

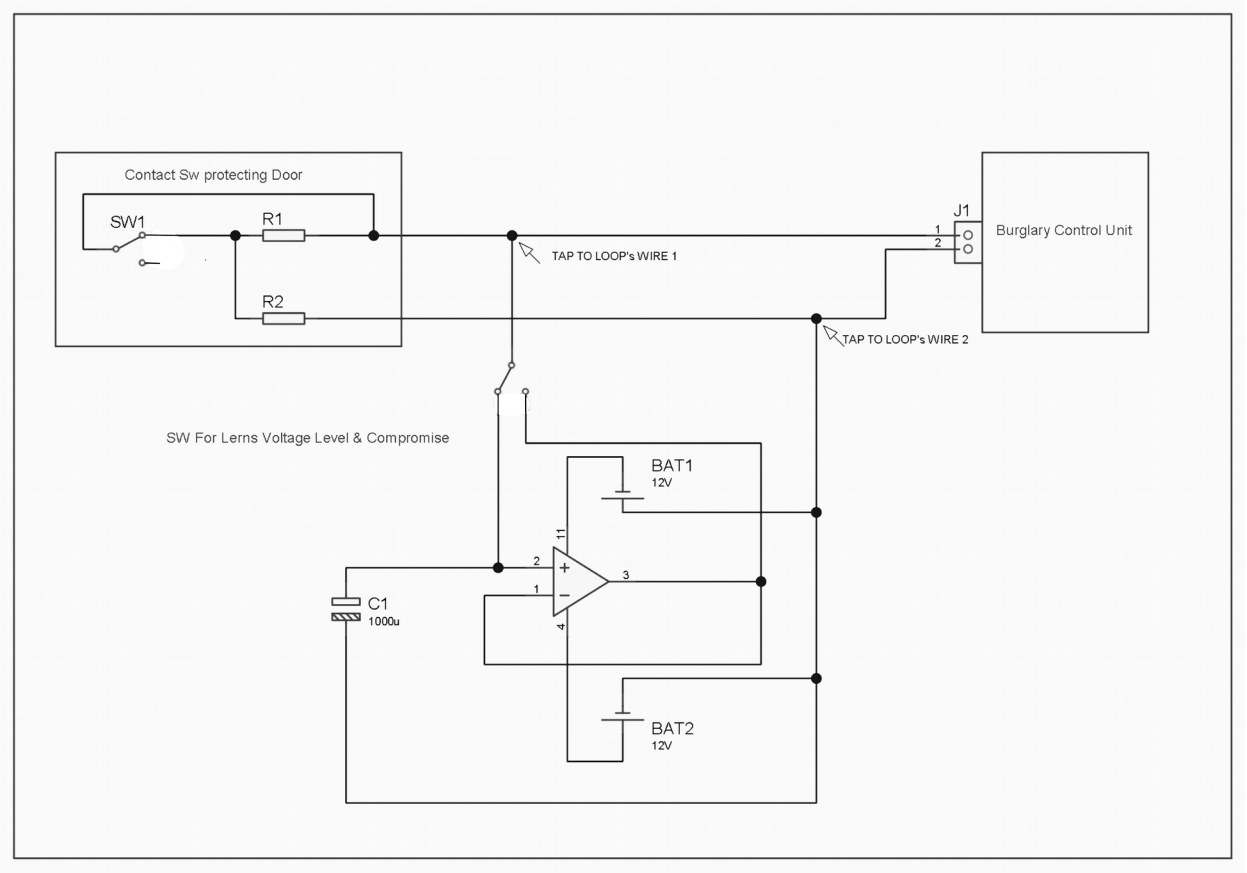


Fig. 1

To be more precise, based on Thevenin's theorem, if an external compromising voltage equals the voltage level presented when the door is closed, and if during the compromise attack this voltage is applied to the zone loop, then opening the switch or contact that usually changes the serial zone loop resistance will have no effect on the loop parameters seen from the zone loop input terminal, as the compromising voltage compensates for the loop resistance changes.

In the case where more than two wires count in a zone loop, more compromising devices may be used to connect to the wires in a circular pattern, in order to

monitor and the substitute all voltages presented in the zone loop circuits.

Fig. 1A presents a full schematic of a device that can be used to successfully compromise a burglary alarm system zone loop powered by a constant voltage level.

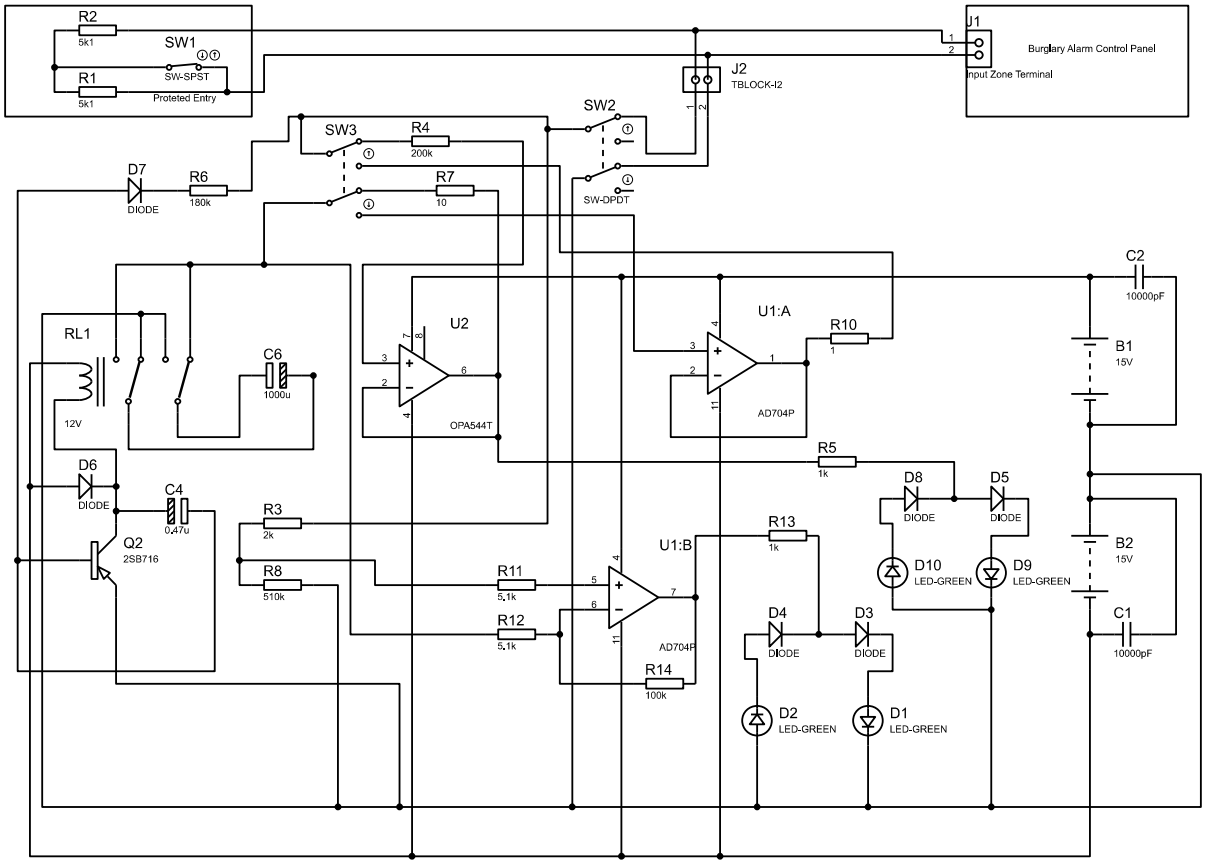


Fig. 1A

The device's Terminal J2 is used to connect to the zone loop wires to measure the

voltage level presented on the burglary alarm systems zone loop input Terminal J1. Measurements are done through the switch SW3 to the input of a operation amplifier U2, model OPA544T or of the similar parameters.

This operation amplifier has a large output current that quickly charges the capacitor C6.

When C6 is charged up to the voltage level presented in the zone loop, then the one of the two Green Led Diodes (LED 1 or 2) will light with constant luminescence to indicates, that C6 is charged to a proper voltage level.

The LED1 or LED 2 is powered from the operation amplifier U1-B, it switches its output power voltage as voltage level on C6 becomes similar to loop zone voltage. One LED activates on a positive voltage level, the second one on a negative voltage level as referenced to the zone loop polarity.

If the zone loop polarity measures as a negative voltage, then the contacts of the relay RL1 switch in order to maintain proper polarity charges of the capacitor C6.

The RLI coil is controlled by the transistor Q2, that switches on when a negative voltage powers its base through the resistor R6 and diode D7.

Capacitor C4 provides a small delay for switching status on or off of Q2. When switch SW3 changes the device mode from reading the loop zone voltage to the compromise mode, the Q2 small delay helps to maintain its constant status.

The time frame for charging C6 may take up to 30 seconds for a large capacitance of C6.
Depending of how long the compromise time frame should last, C6 may have the capacitance up to 100000 uF. Then the testing time frame may lasts as long as 60 minutes, when using a very good quality capacitor of large capacitance.
For a such long compromise time frame, it is important for the capacitor C6 to have an extremely low leakage current, and uses the operation amplifier U1-A, model ADT704P or similar, with a low input bias current, of a pA range.

The U1-A output supplies the zone loop with the compromising voltage presented on C6, however with each second passed, these voltage decreases a little. It is assumed that when voltage drops to around 300 mV, the compromise time frame should be ended.

Switching the SW3 it starts the counting the time elapse for the compromise event.
Before the compromise time frame is completed, the protecting contact of the zone loop has to be brought to the original status i.e. the door needs to be closed and the SW3 switched again to the measure mode. When C6 charge is complete, another compromise attract can be conducted.
By adding the RF receiver to the these device, the SW3, SW2 could be remotely controlled.

In a case when the zone loop has a couple of pairs of wires, then couple of devices may be used, one per a pair of wires.

When device connects to two wires that are a common point of inputs of a burglary control panel, the LED 9 and LED 10 will be in the off states and when a connections are done correctly, one of LED's light on.

Also it does not matter to which loop wires the device is connected, because all the wires refer to each other in a circular connection and each of the compromising devices is powered individually, having a floating type power sources, and thus are isolated form each other.

Fig1C shows a example of compromising three zone loops using three devices.

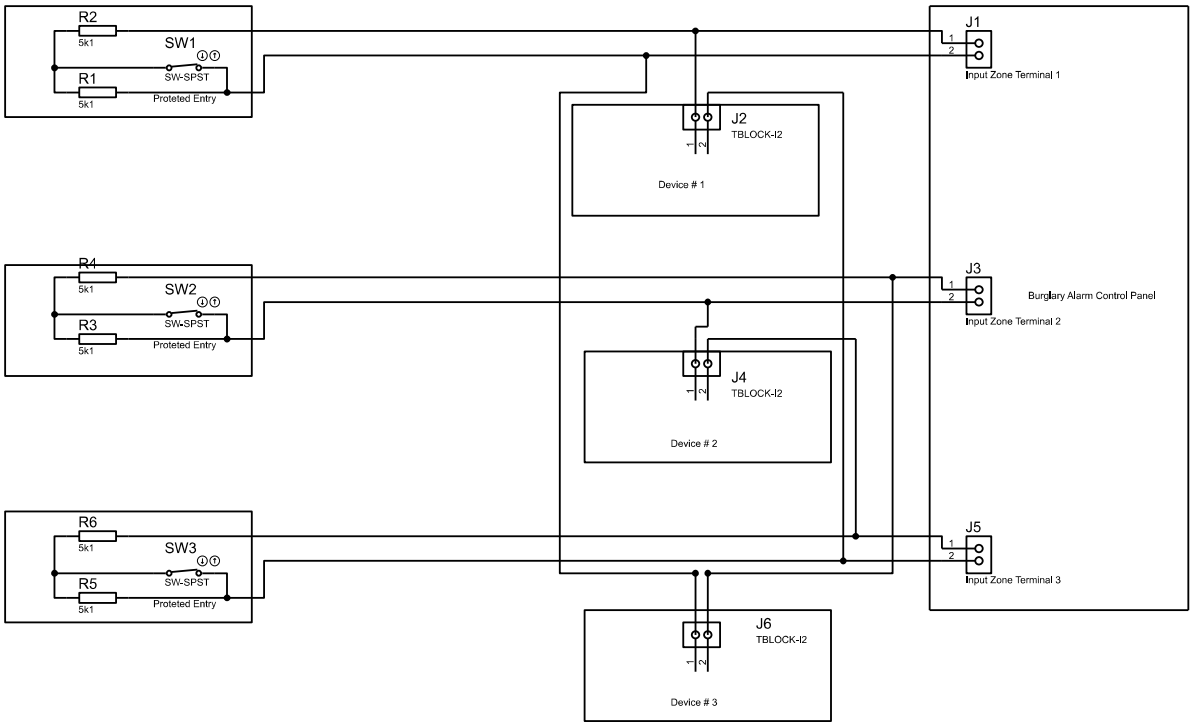


Fig. 1C

By applying a random variable voltage power to the wired zone loop, as shown Figure 2, it will be extremely difficult to successfully perform any of the above discussed compromise techniques in order to disable the protected zone.

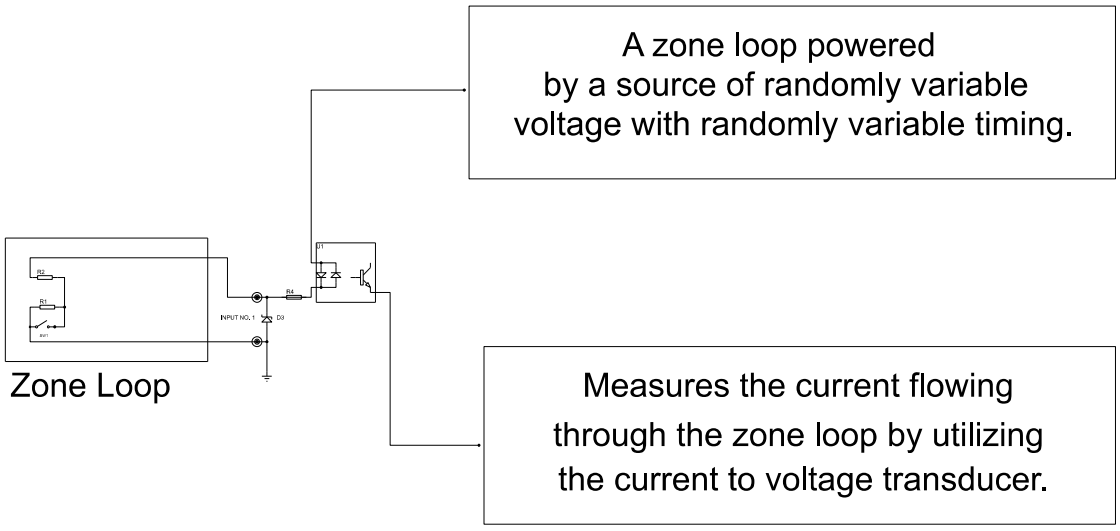
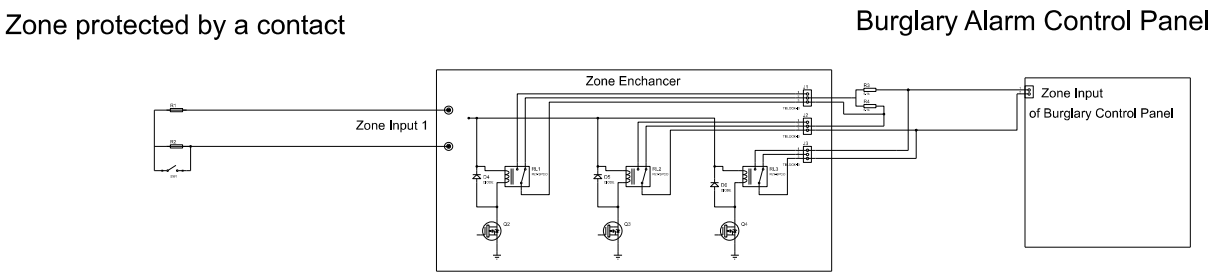


Figure 2.

In practice, the easiest way would be to insert, between the zone loop and the burglary control panel, a device called here a Burglary Alarm Zone Enhancer, which will power the zone loop with random variable voltage level and will process the status changes of the contact or switch and pass the result to the input of the control unit as shown in Figure 3.



An input zone enhancer device
of the burglary alarm systems

Figure 3.

Bill Of Materials

Quantity	References	Value
2	C1-C2	10000pF
1	C3	300pF
3	C6-C8	1000u
	R1, R2	As per Installation Manual
Quantity	References	Value
2	R11,R12	5k1
1	R3	2k
1	R6	180k
1	R7	10
1	R8	510k
1	R4	200K
1	R10	1
2	R5,R13	1k

Quantity	References	Value
1	U1	AD704P
2	U2-U3	OPA552PA

Quantity	References	Value
1	Q2	2SB716

Quantity	References	Value
2	D10-D2	LED-GREEN
5	D3-D8	DIODE any 50V/50 mA
2	D9-D1	LED-RED
Quantity	References	Value
2	B1-B2	Battery pack 15V
2	RL1	RELAY 12V
1	J1	TBLOCK-I2
2	SW2-SW3	SW-DPDT
1	SW1	Door Switch

If you are interested in this subject, feel free to contact me.

Cezary Jaronczyk

email: cjjconsultant4@gmail.com
home page: http://cjj-consultant.ca
phone 1 (416) 972-0069