How to improve zone protection in burglary alarms

Abstract.

In this article I present a novel design of a hardwired zone control panel or zone expander input of a burglary alarm, which provides an enhanced security level against compromise attack attempts or problems with the zone loop.

Burglary alarm systems in question feature zone input connections with RF sensors and hardwired sensors. Herein I review the positive and negative properties of such zone inputs and the degree of susceptibility toward a variety of attacks compromising the secured zones. A simplified schematic of a device for testing a sensor's hardwired connections against compromising attack attempts is presented.

Do modern designs of alarm burglary systems properly and reliably protect objects or zones?

The above question will be answered by discussing a particular subsystem of a burglar alarm, the zone input, and its contact or switch that controls the status of a door, window, PIR (Passive Infrared Sensor) or other mechanical sensor barriers.

Modern designs of burglary alarm systems.

Modern designs of the above sub-circuits provide two main technical solutions: 1- the hardwired zone inputs. 2- RF (Radio Frequency) zone input. Each of them has their advantages and weaknesses.

In the case of a 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. These zone input devices can be placed at a distance of several meters apart and thus may increase the installation costs.

The activation of a contact or a 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.

Compromise of the RF type zone devices.

The RF type zone input is an over the air type connection utilizing a sensor with a magnetic contact, or a switch like a PIR, or a door device with a built in RF transmitter, that sends its status to the RF zone receiver of the burglary control unit or the RF zone expander.

These types of connections generally are less expensive to install, however these connections have some disadvantages.

The basic problem comes from the fact that the RF device has to periodically send a supervision signal within a maximum time frame of a few minutes, as defined in a particular Standard. When a system uses several dozen of RF devices, a situation may occur when two or more RF sensors concurrently send supervisor or status change signals, and the receiver sees the messy signals and does not know how to interpret the received information. In such a case, the RF receiver needs to wait for the next cycle of signal transmission in order to correctly interpret it. Then the time limits designated for supervision of the RF device may be longer than the limits defined in the Standard requirements for such a check performed in a supervision cycle.

A serious problem may occur when the RF receiver is overloaded by external RF signals, having wide spectrum of noise frequencies, and becomes jammed. During this time, the Alarm signal of the RF sensor device cannot be received and properly decoded by the RF receiver, it just becomes blocked.

In consequence, the burglary alarm system generates a general Alarm or a jammed type Alarm and sends this information to the Central Station, and a proper procedure takes place - someone needs to be dispatched to the site to check the situation.

The worst scenario could happen when in the same time frame, a few or more secured sites located in different locations, or at a large location such as an airport, power plant or a water plant, become jammed, and as consequence, there will be no more staff available to check the next alarming site, that might be actually attacked and sends a real Alarm. The seriousness of above situation increases when we consider the danger from potential terrorist attacks on the variety of important objects.

Typically, the RF sensor's device signal is predetermined in its pattern, thus applying proper RF

devices and sniffing/spoofing techniques, a false substituting signal can sent with a status "OK" right after the original RF sensor is physically destroyed. However, these compromising techniques require access to proper RF equipment and people with adequate knowledge and experience.

All of above problems are the consequences of the fact that the RF signal may be visible to anybody with appropriate devices.

Compromising hardwired connections

Considering all the above, hardwired type connections seem more reliable and safe in securing a wide variety of sites. However, in order to make a hardware type connection safe, we need to solve the problem of compromising it.

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, the applied compromising voltage level represents the status of “closed door” (window or other barrier), then 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 devices and tactics, and a way of taping it to the zone loop wires. These types of devices allow to compromise the protected zone loop for a time frame up to 30 minutes, or even longer.

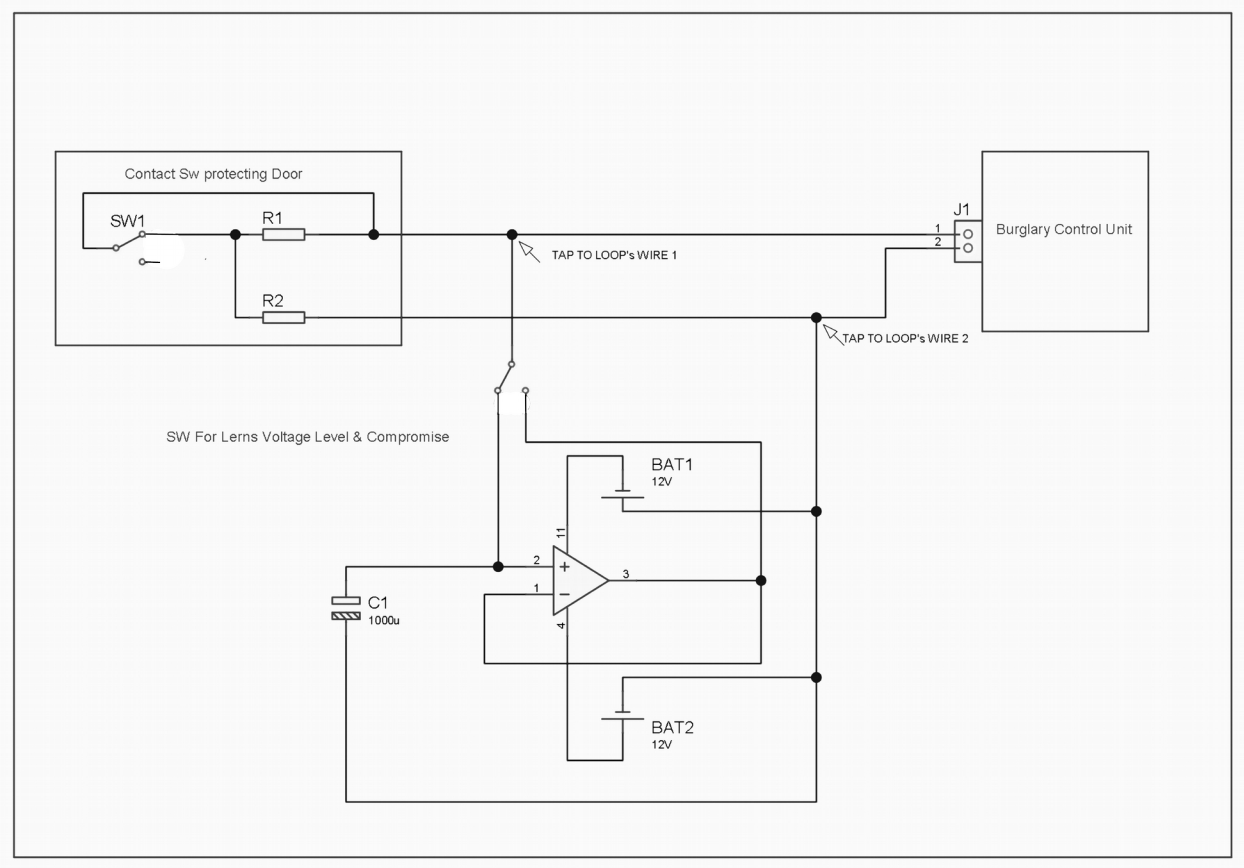

Figure 1: Simplified device used for compromising a hardwired zone loop

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 then substitute all voltages presented in the zone loop circuits.

How to prevent compromise attacks on a hardwired zone loop.

The case presented above is of such importance, that it needs to be prevented. This can be accomplished by changing the way the zone loop is powered, from a DC with a constant voltage level to a random variable voltage level constantly changing over time.

As the results of 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.

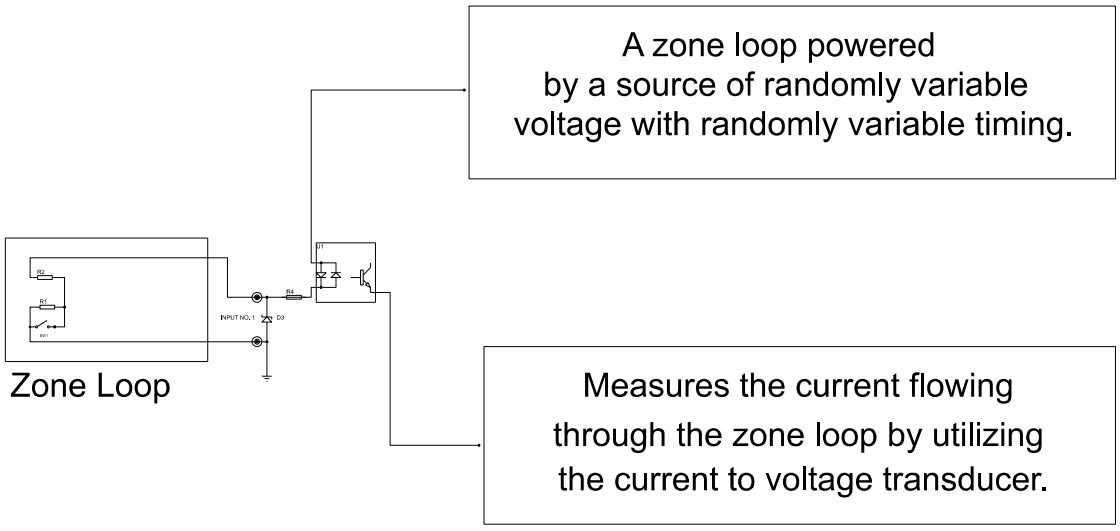

Figure 2: A wired zone loop powered by random variable voltage and timing

In practice, the easiest way to protect a hardwired zone loop 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.

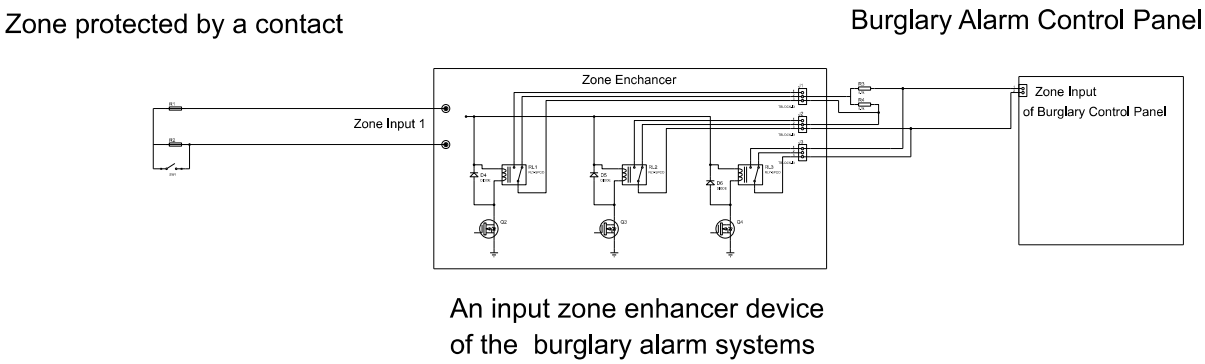

Figure 3: Burglary Alarm Zone Enhancer

The device named Burglary Alarm Zone Enhancer described above has a Patent Pending status.

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

PEO Cezary Jaronczyk
email: cjjconsultant4@gmail.com
phone (416) - 972-0069