University of Nevada

Reno

The Jackson High Security Switch
and
Radio Frequency System

by

John T. Jackson, Jr.

A thesis submitted in partial fulfillment of the requirements
for the degree of Master of Science in Electrical Engineering

Dr. Bruce Johnson, Thesis Advisor

The thesis of John T. Jackson, Jr. is approved:

____

Thesis Advisor

____

Department Chair

____

Dean, Graduate School

University of Nevada

Reno

1997

ABSTRACT

Prior magnetic proximity high security switch technology is discussed and a novel technology based upon the Jackson Switch is introduced as a replacement. The analysis of reed switch technology, upon which the prior high security switch technology is based, covers magnetic materials, electrical contacts, and hermetic seals. The limitations and deficiencies of the prior technology are illustrated including defeat mechanisms. Many variations of the Jackson high security switch are shown in three dimensional illustrations and schematics. Many variations of a novel radio frequency system which incorporate high security switches are also introduced and shown in three dimensional illustrations and schematics. The combination of a Jackson high security switch and the radio frequency monitoring system is shown to be undefeatable and to have the highest reliability. Four patents, both foreign and domestic, are pending on the Jackson high security switch technology.

TABLE OF CONTENTS

The Jackson High Security Switch

and

Radio Frequency System

1. DESCRIPTION OF HIGH SECURITY SWITCHES

The generic term "security switch" includes security switches and high security switches, most generally of the magnetically actuated types. Security switches are frequently used as the primary level of security in complete electronic security systems. Often, this is the only level. They are the simplest and most effective method of indicating whether or not a door or window has been breached. The on or off information from each switch may be sent by wire to a central processing unit which is usually a relay box connected to an alarm. A facility or building may have one or more such devices guarding entry ways. Some home units integrate a radio transmitter with each switch that transmits the information to a central receiver which controls an alarm. Security switch, and particularly high security switch, applications for protecting doors, windows, and cabinets include, but are not limited to, airports, medical facilities, government buildings, research centers, factories, warehouses, controlled or hazardous materials, banks, and data processing centers. Industrial versions are available for controlling machinery safety barriers and other moving assemblies.

Security switches are typically one magnetic proximity switch that is actuated into the electrically closed position when in the proximity of an actuator that is comprised of one permanent magnet. The magnetic proximity switch assembly is usually mounted in or about the frame surrounding a doorway, window or access panel and may have conductors leading out from it to the security or machinery monitoring control unit. The actuator is usually fixed to the moving member such as a door or window. A single magnetic proximity switch in combination with a single permanent magnet is most prevalent in home security systems. They may be seen most often on department store, restaurant, and super market doors near the top of the door frame on the inside. Security switches represent a trivial obstacle to any intruder with a single permanent magnet and a piece of tape or a very powerful permanent magnet from the outside.

High security switches typically consist of a fixed switch assembly and a movable actuator assembly. The switch assembly comprises some combination of two or more magnetic proximity switches and the actuator assembly comprises some combination of two or more permanent magnets. The purpose of the multiple magnetic proximity switch combination is to make the switch assembly difficult to defeat with a single permanent magnet. Ideally, the high security switch should be immune to defeat by its own actuator and specially designed lock picking magnet assemblies. All of the prior technology is susceptible to defeat by single permanent magnets, their own actuator assemblies, or some form of lock picking mechanism.

All high security switches of the prior art are based upon reed switch technology which has reliability problems. Due to constraints imposed by the inherent structure of reed switches, the incorporation of electrical contacts is compromised. Consequently, life expectation is extremely sensitive to operating conditions. Their sensitivity to magnetic fields makes them susceptible to extraneous fields generated by electric motors, transformers, lightning, etc. This characteristic is further exacerbated by the introduction of biasing permanent magnets to polarized the reed switches and increase sensitivity. The combination of unpredictable operating conditions and environmentally induced currents and fields results in unreliable performance, false alarms, and catastrophic failure. Response to false alarms are expensive, reduce the sense of urgency or confidence in the system, and create a psychological disadvantage to the responding individuals. Catastrophic failures often go unnoticed producing a false sense of security. Elaborate schemes are available as options in high security switches, at additional cost, to detect these failures.

The reed switch glass envelopes, which are used to create a hermetic seal, are fragile and prone to breakage. Improper bending of the leads or improper packaging and potting techniques tends to break the hermetic seal resulting in several failure modes of the electrical contacts. In addition, they are highly susceptible to shock which may alter the magnetic operating characteristics or also damage the hermetic seal.

Reed switches have large actuation lobes in response to magnetic fields even after the introduction of biasing permanent magnets. This renders single reed security switches, in combination with their sensitivity, easily defeatable. High security switches with combinations of two or more biased reed switches (polarized) for the purposes of coding are vulnerable. Consequently, magnetic shields may be introduced into the design. Effective magnetic shielding is cost prohibitive and dramatically increases the size of the security switch. High security switches that use a more cost effective magnetic shielding means are still vulnerable (see section 2.3.1).

It is apparent that a need exists for a more advanced high security switch technology. The present material addresses this need and relates to magnetically actuated proximity switches consisting of novel combinations of permanent magnet proximity switches of the type referenced in the U.S. provisional patent [41], hereafter referred to as the Jackson Switch, as part of an electronic physical security system or machinery control system for detecting and monitoring the opening or closing of panels, windows, doors or the like.

Security switches, including high security switches, which are connected by wires to a physical security monitoring system, are vulnerable to defeat if access can be gained to the connecting wires. One method to defeat a wired security switch is to discover the appropriate pairs of wires and electrically short them, thereby defeating the system. Armored cables and conduits are sometimes used to limit access to the connecting wires. However, these protective means do not actively monitor the integrity of the cables, nor do they provide any indication that such means have been breached. The present material overcomes this limitation and relates to a radio frequency, magnetically actuated, proximity switch system for use in physical security monitoring systems, machinery control systems, and the like.

2. PRIOR TECHNOLOGY

An example of a prior art high security switch is the "MSS-100-17 High Security BMS Contacts" available from Flair Electronics, Inc. of Glendora, California. Another example is the ADM-30/31 High Security Switch available from AMSECO referred to as "ADM-30/31 Anti-Defeat High Security Contacts". Further examples of magnetic security switches of the prior art may be found in the numerous patents referenced in the bibliography. The two most significant examples of high security switches are those manufactured by Sentrol of Portland, Oregon [32] and Securitron of Sparks, Nevada [40], which will be discussed later on in detail.

The single most distinguishing characteristic of the prior art is the use of reed switches. The most advanced models use combinations of two or more reed switches that are magnetically biased by permanent magnets. From this perspective, the prior art may be thought of as a collection of novel combinations of the same ingredients. And, the limitations and deficiencies thereof are essentially those of the reed switch. The description of reed switch technology that follows will summarize the theory of operation and elucidate those limitations and deficiencies.

2.1 REED SWITCH THEORY

There are three basic reed switch types [4], the dry reed, the mercury wetted reed, and the mercury wetted contact switching capsules. The magnetic behavior of reed switches as a class of device is similar. However, switches of the mercury type are restricted to certain mechanical orientations for successful operation due to gravitational affects. They also represent an environmental disposal hazard and are much more expensive than the dry reed type. Consequently, only the dry reed is appropriate in modern applications of security switches. Therefore, the following discussions of magnetic properties will apply to reed switches in general, but the overall scope will be restricted to the dry reed type.

Referring to FIG. 1, a three dimensional view of a glass encapsulated reed switch comprised of, a magnetic electrically conducting lead wire **1** to which a flexible magnetic electrical contact member **1A** is fixed, a nonmagnetic electrically conducting lead wire **2** to which a nonmagnetic rigid electrical contact member **2A** is fixed, another lead wire **3**, which may optionally be magnetic, to which a magnetic rigid electrical contact member **3A** is fixed, and hermetic glass envelope **4** is shown. In the absence of a magnetic field of sufficient strength, the magnetic electrical contact **1A** is in electrical contact with the nonmagnetic electrical contact **2A** as a consequence of the spring action by the contact member **1A** as shown. The lead and electrical contact elements **1**, **1A**, **3**, and **3A** are composed of high permeability magnetic electrically conducting alloys such as Mu-Metal [22] or the like for optimum performance. For proper operation of the switch, at least the electrical contact **2A** must be nonmagnetic so that no magnetic forces may be developed therewith.

In the presence of an appropriate magnetic field, virtual magnetic poles of opposite polarity are produced on the magnetic electrical contact members **1A** and **3A**. The resulting magnetic force of attraction overcomes the opposing spring force and the electrical contact **1A** bends to make electrical contact with the electrical contact **3A** as shown in FIG. 2. The magnetic force of attraction between them is a very complex function of the regional flux density vectors [9]. When the regional magnetic field drops below the actuation threshold or is absent, the electrical contact **1A** returns to its original position of electrical contact with the member **2A**.

2.1.1 ACTUATION AND BIASING

Actuating a reed switch is accomplished by bringing a permanent magnet into the proximity of the reed switch. Although the reed switch is not sensitive to magnetic polarity, there are certain positions within the permanent magnet field in which the reed switch will not actuate because virtual magnetic poles are

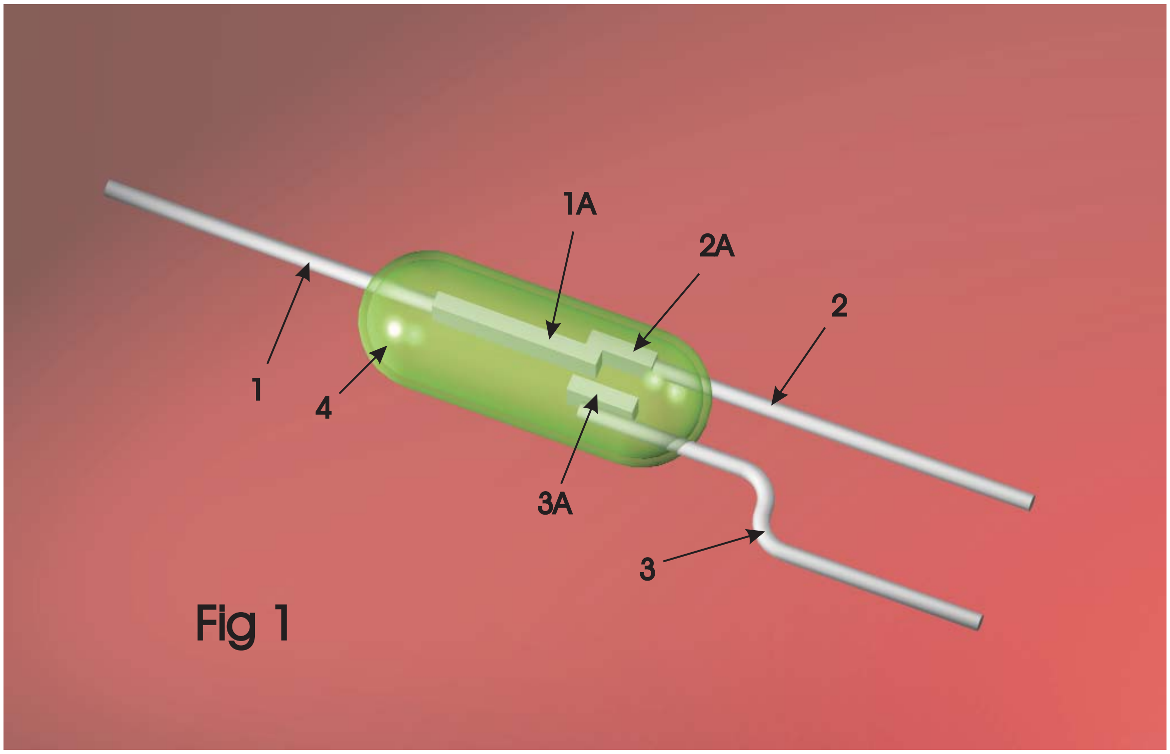


Fig 1

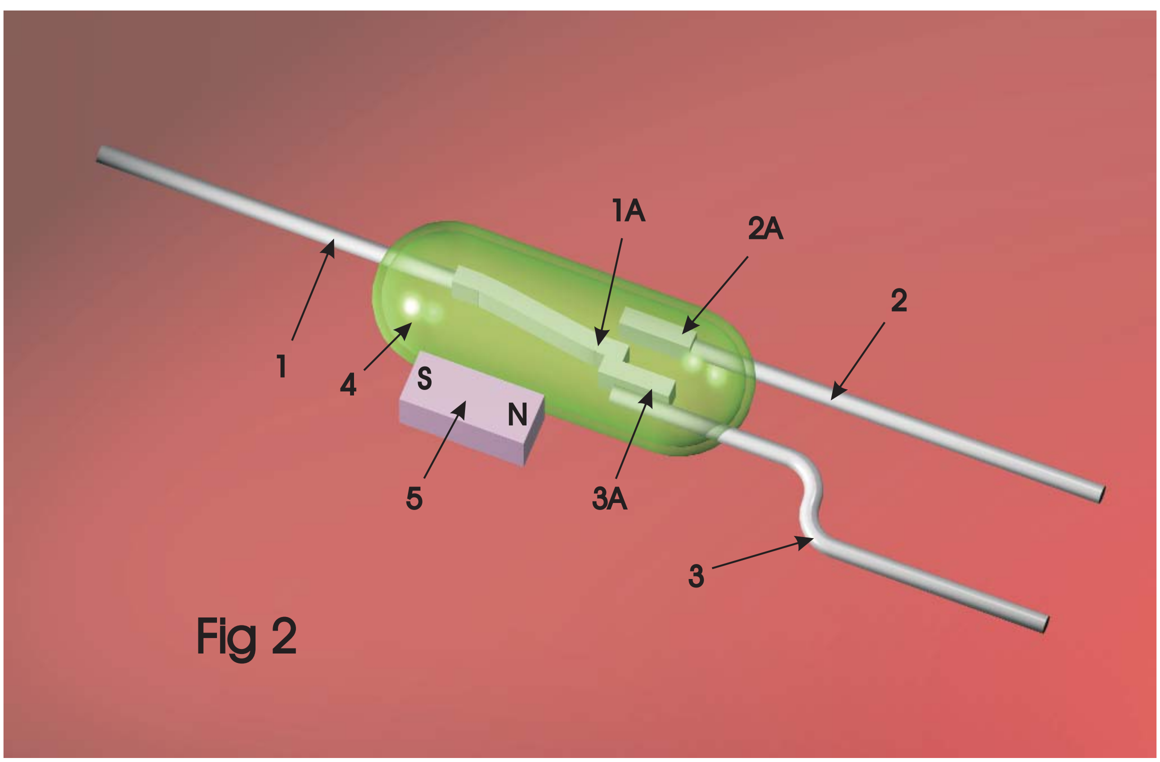


Fig 2

not developed on the magnetic electrical contacts. All of the reed switch manufacturer catalogs, some of which are listed in the bibliography, show illustrations of the actuation zones depending upon the permanent magnet orientations.

The magnetic force between two magnetic poles of opposite polarity is attractive. Physics books show certain idealized cases where opposite magnetic poles are attracted to one another by the square of the magnetic flux density and by the inverse square of the distance of separation. In practice, the only useful method of predicting forces between reed switch electrical contacts is by the use of finite element methods on a computer after a particular configuration has been designed from experience [9]. To further complicate matters, the properties of the magnetic lead and contact materials vary so widely in production that predetermined ranges of actuation or "pull in sensitivity" are not possible to produce economically. This means that for any single production run, the statistical distance between a reed switch and a permanent magnet for first actuation under optimum conditions may vary 300% or more. Consequently, reed switches are test selected for pull in sensitivity from large production lots. Once the reed switch is actuated, the permanent magnet may be pulled away much further than the first actuation distance (hysteresis), that distance being called "drop out". Reed switch manufacturers do not specify drop out because it is not predictable or controllable.

Referring to FIG. 2, a three dimensional view of a glass encapsulated reed switch magnetically biased by a permanent magnet **5** is shown. This is one of many ways to magnetically bias a reed switch. Some other means may be found in the book by Moskowitz [5] and in many of the issued patents listed in the bibliography. It is clear that magnetic biasing actuates the reed switch. Moving the bias permanent magnet along the axis of the reed switch envelope adjusts the pull in sensitivity and polarizes the combination [32]. The biased reed switch has greater pull in sensitivity, is directional to some extent, and the actuation lobes become distorted. This increase in pull in sensitivity makes the assembly more susceptible to extraneous magnetic fields which results in a statistical increase in false alarms. Actuation of the biased assembly will be described in Section 2.2 (the Sentrol High Security Switch).

The difficulty with any bias technique with permanent magnets is obtaining accurate adjustment. Due to the small size of the components, their relative mechanical tolerances, wide magnetic property variations, and the complication of magnetic hysteresis, highly specialized fixtures with micrometers for adjustment are required. Because the magnetic behavior of the adjusted assembly is nonlinear, the adjustment points appear to migrate from one test to the next. And, specifying the operational characteristics takes on a statistical nature. Some biasing techniques [40] are easier to adjust than others, however, they all increase manufacturing complexity and cost.

2.1.2 ELECTRICAL CONTACTS

Electrical contact engineering is not well understood and there is not very much literature published in this field. Some understanding of electrical contacts behavior can be gained from the book by Jones [3]. Knowledge in this field is mostly gained from empirical measurements on particular combinations of electro-mechanical circumstances and materials, and is considered arcane. The success of any electrical contact design is measured on a statistical basis rather than parametrically.

The general principles of operation involve electrical arcing at the moment of making contact or breaking contact. This results in wearing of the electrical contacts which leads to an inevitable failure by welding or mechanical interlock which may be preceded by momentary or temporary sticking. The enormous electrical gradients at the moment of make or break cause ionization of the material which is pulled into the gap as a plasma. Resistive heating at the points of contact and through plasma bridges raises the temperature of the contacts to the vaporization point [3]. Material transfer occurs. Pitting and erosion result.

Materials with the highest melting points and highest mechanical hardness in combination with low conductivities tend to wear the least. However, materials with the highest melting points and hardness, such as refractory metals, do not have the lowest conductivity. Alloys of low conductivity materials with refractory metals make improvements, but many combinations are not miscible. As a result, composite materials are becoming popular in which materials with high melting points and high mechanical hardness are combined with materials with less favorable properties but having low conductivities through sintering processes, which would not otherwise be possible.

Reed switch electrical contact members, as previously mentioned, are made from magnetic alloys consisting of materials from the ferromagnetic triad [22]. These magnetic alloys make some of the poorest electrical contacts. These electrical contacts must be hermetically sealed to prevent atmospheric corrosion which could result in an inoperable switch within hours [12]. Occasionally, optimal electrical contact materials are welded or brazed onto the magnetic members [4]. But this widens the magnetic gap reducing the pull in sensitivity and alters the magnetic properties of the magnetic members in the bond zone which further reduces the pull in sensitivity in unpredictable ways. Electro-plating of refractory metals, such as Rhodium [15] or Ruthenium, onto the electrical contact members is advertised by reed switch manufacturers to compensate for the poor substrate materials.

Electrical contacts have optimum ranges of contact force [2]. Most combinations will not conduct or have excessively large resistances near zero or at very light contact pressure [10]. Gold electrical contacts require a minimum of a 5 gram force and preferably a 10 gram force to conduct. And, the contact surfaces must be metallurgical clean to obtain these results and can only be maintained in a hermetic environment. Reed switch contact forces are typically in that range at the maximum pull in range. Many electrical contact materials require much higher contact forces. So, if a contact material is selected for favorable electrical characteristics which have a high contact force requirement, and it is bonded to the reed contact members, the magnetic gap will have been enlarged which reduces the magnetic force of attraction between them. The consequences are obvious.

All reed switches require some combination of materials for the actuation of magnetic members or reeds and electrical contacts. With known materials, these two requirements are the antithesis of one another. Reed switch manufacturers generally favor optimization of the magnetic properties and use a “Band-Aid” approach by electro-plating the electrical contact area with Rhodium or Ruthenium. This combination is particularly sensitive to failure as a consequence of electrical arcing. Additionally, hermetically sealed glass envelopes filled with inert gases are absolutely required to prevent corrosion of the electrical contacts [12] [13].

2.1.3 ELECTRICAL POWER

Magnetic materials are not good electrical conductors. The electrical conductivity of iron is roughly five times lower that copper. This limits the electrical current handling capabilities of the reed switch. The electro-plated materials, such as Rhodium and Ruthenium, have electrical conductivities three and four times lower than copper, respectively. Even with electroplating, the resistivity of the magnetic materials is the dominant affect. It is trivial to show that the reed switch has no more than one half the energy density of other devices. Even if the reed switch life could be extended by optimum selection of electrical contacts, the power density and the pull in sensitivity would be severely limited. The reason reed switches are not usually manufactured in sizes larger than thirty watts is that classical relays offer a greater selection of electrical contacts, are more sensitive to electro-magnetic actuation with large electrical contacts, have higher power densities, and are more economical to manufacture at that power break point.

2.1.4 SIZE

Current high security switches embodying the prior technology are already using the smallest “Form C” reed switches manufactured. The size of their basic mechanisms is not easily scaled to smaller reed switches even if such reed switches could be economically manufactured. Further, scaling them to a smaller size would diminish either the actuation gap range or increase the false alarm rate. Manufacturing procedures already involve sensitive adjustments which may require the use of micrometers. Any significant reductions in size would escalate the production costs to unfeasible levels.

2.1.5 RELIABILITY

Dropping a reed switch from 30 centimeters above a hard surface will permanently degrade the magnetic performance [24]. The hermetic seal between the glass envelope and the lead wires may also be compromised. Special care must be taken in production to bend the lead wires without putting “any” mechanical stress on the hermetic seal joint [12]. Encapsulating or potting the reed switch results in thousands of kilogram force per square centimeter on the glass envelope and the hermetic seal joint. The detrimental affect of this may be seen by removing the potting compound from a reed switch assembly with methylene chloride. The glass envelope is often shattered. If the reed switch assembly has been potted and the hermetic seal has been compromised, hydrocarbons from the potting compound may enter the envelope. The Platinum series elements used for electro-plating the electrical contacts may catalytically convert the hydrocarbons to a monolayer on the electrical contacts. This renders the reed switch inoperable. Oxygen may also leak into the glass envelope and corrode the contacts which has the same result [19].

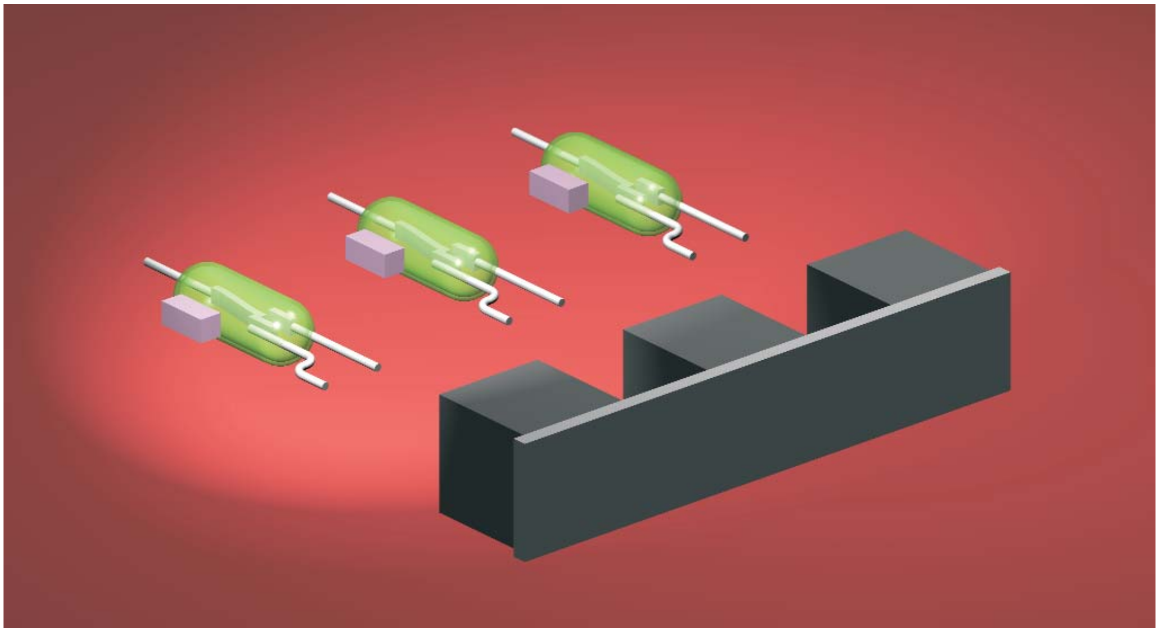
Reed switches are extremely vulnerable to electrical conditions [16] [21]. Switching inductive loads should be avoided. Electrical arcing will occur. The thin electro-plated layer can be immediately breached and the contacts may weld. If there is inductance in the switched circuit, auxiliary circuits must be placed around the switch to minimize the arcing. Surge currents must also be avoided, such as those associated with the turning on of electric light bulbs or switching high capacitive loads. Ideally, the reed switch only wants to switch a pure resistive circuit. Any other condition can reduce its life expectation by orders of magnitude. If the reed switch is expected to switch any load except a purely resistive one, a variety of auxiliary circuits are available to minimize the detrimental affects.

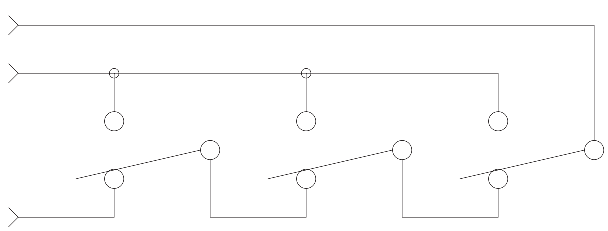
Due to their extreme magnetic sensitivity, reed switches should never be placed near electric motors, transformers, heaters, or any equipment that radiates electro-magnetic fields. A single stroke of lightening can destroy every reed switch in the vicinity by induction. Biasing reed switches with permanent magnets increases their sensitivity to induced fields. The false alarm rate of security devices that rely on them should not be any surprise.

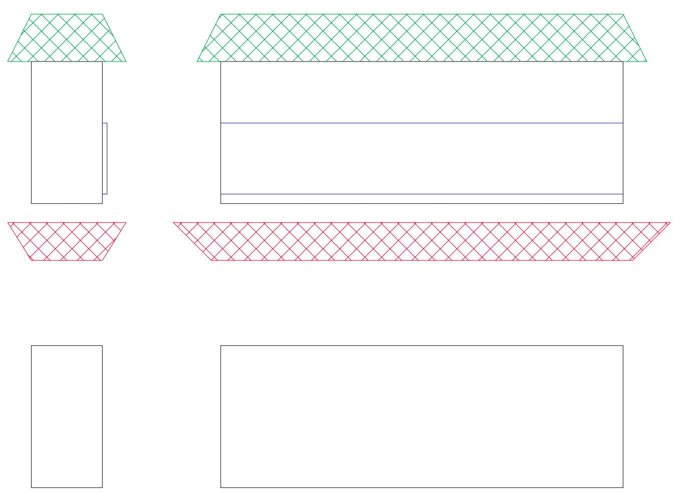
Compared to other technologies, the reed switch is not very reliable and should not be considered in a new design if there is any reasonable alternative.

2.2 THE SENTROL SWITCH

The Sentrol High Security Switch [32] is considered a first generation switch. It is referred to as a triple biased switch but should be more accurately called a triple coded switch. Referring to Figure 3, the switch which is comprised of a switch assembly in which three magnetically biased reed switches **1**, **2**, **3**, as shown in Figure 2, are arranged side by side, parallel to each other, is shown. The biasing magnets are oriented with alternating polarities as shown. The switch assembly is actuated by an actuator assembly comprised of a combination of three permanent magnets **4**, **5**, **6** arranged with their axes of polarity parallel to one another, and spaced apart from each other by distances corresponding to the spacing between the reed switches of the switch assembly. The magnetic metal strap **7** in this invention is not sufficiently substantial to constitute a magnetic yoke. It is an assembly fixture whereby the actuator







permanent magnets are held in position during a subsequent potting process. The individual permanent magnets of the actuating assembly oppose the polarities of their corresponding biasing magnets of the individual reed switches, as shown. When the actuating assembly is sufficiently proximate to the switch assembly, the magnetic field vectors of the individual biasing magnets in the vicinity of their corresponding reed switch contacts are rotated such that the reed switches release. The permanent magnet polarities of the entire switch and actuator assemblies, as shown in Figure 3, may be reversed without effect. Figure 4 shows a typical basic electrical schematic of the reed switch interconnection.

The switch assembly is adjusted in production by moving each biasing magnet along the longitudinal axis of its particular reed switch to a position where the switch is magnetically closed, that is, until a magnetic reed of the switch is attracted into minimum contact with a magnetic fixed contact as described in Section 2.1.1. The actuator is subsequently brought into a predefined maximum actuation distance. If the reed switches release, then the switch assembly is too sensitive. The actuator is removed and the process repeated until satisfactory results are obtained. The actuator assembly is then brought to a closer predefined actuation distance. If the reed switches do not release, then the switch assembly is not sensitive enough. The actuator is removed and the process repeated until satisfactory results are obtained. This process may be repeated many times until satisfactory results are obtained and then the bias magnets are glued to the reed switch glass envelope.

An interesting feature of this high security switch results when the actuator assembly is brought very close to the switch assembly. The actuator permanent magnet field, that had previously neutralized the bias permanent magnetic field, is now dominant. An actuation range is produced. This is an artifact of the technique, and not a design feature, for which there are no positive or negative attributes.

2.2.1 DEFEAT MECHANISMS

Figure 5 shows a top and side view of a Sentrol high security switch in an anodized aluminum housing. The actuator is drawn outside of the actuation range which is shown in cross-hatched red. Single permanent magnets can defeat this switch, but the technique is difficult and unreliable. There are three other ways to defeat the switch that are very simple and very reliable. Two of the ways involve the actuator from another switch of the same series or design and the third involves specially designed lock picking actuators.

Actuator assemblies for any particular Sentrol switch series are interchangeable. So, if such an actuator is placed between the blue lines in Figure 5, the original actuator may be removed without altering the state of the switch assembly. Figure 6 shows a three dimensional example of this. The alternate actuator **3** is placed on the top surface of the switch assembly **1**. The original actuator **2** can now be removed along the line of the arrow in either direction without setting off the alarm and the system has been breached.

The red cross-hatch actuation range of the switch assembly shown in Figure 5 is quite broad. Figure 7 shows an example of an alternate actuator **3** being placed on top of the original actuator **2**. Both actuators are moved in the direction of the arrow as a single unit until the alternate actuator **3** is directly under the switch 1. The original actuator **2** can now be removed without setting off the alarm and the system has been breached.

The green cross-hatch in Figure 5 shows the actuation range of specially designed lock picking actuators. The design of such lock picking devices is beyond the scope and intent of this material.

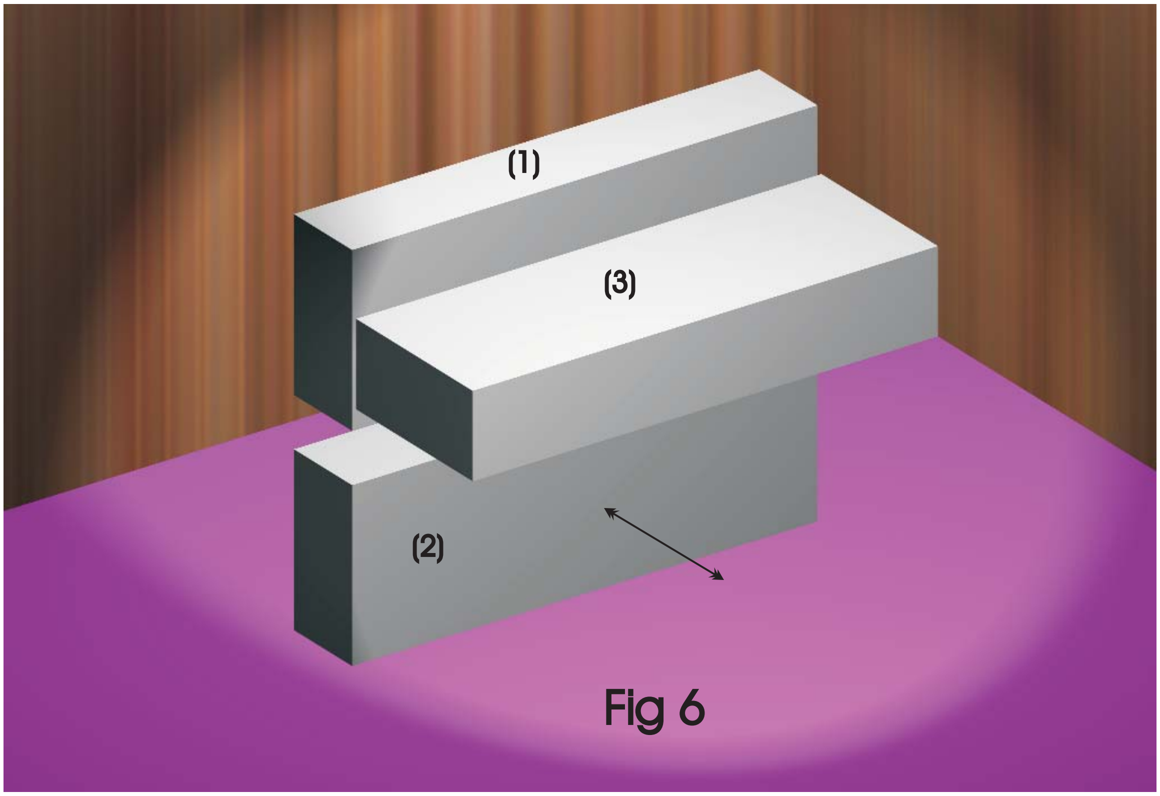


Fig 6

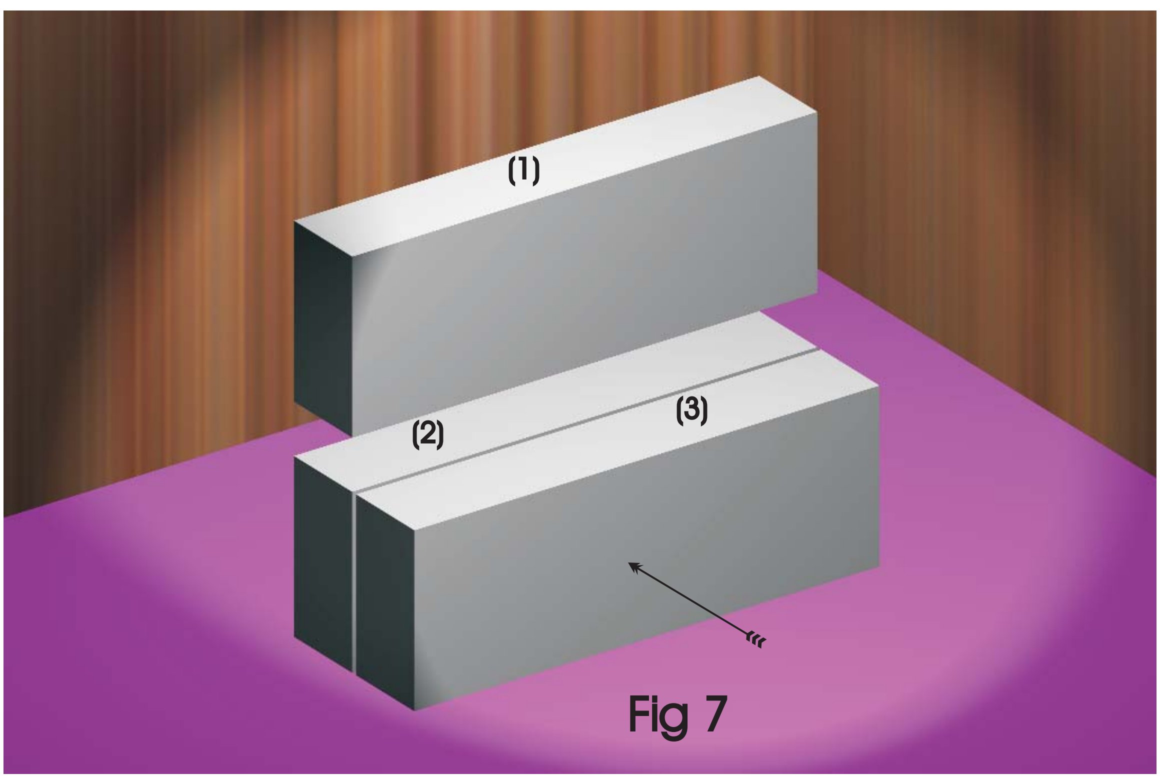


Fig 7

2.3 THE SECURITRON SWITCH

The Securitron high security switch [40] is considered a second generation switch. Figure 8 shows the switch that includes a switch assembly comprised of two permanent, high coercivity, biasing magnets **3**, **4** arranged in a row with their magnetic axes alternating and coincident with an imaginary line connecting their centers and that are mechanically fixed in position so that the repulsive forces acting between them cannot alter their locations. This thereby creates a number of “apparent” or “consequent” magnetic poles in a field which is interactive such that interference with the field of one of the magnets effects all of them. Two reed switches **1**, **2** disposed in predetermined locations within that field are magnetically switched when the actuator assembly is sufficiently removed and are released when the actuating magnets **5**, **6** are moved to a predetermined range or distance relative thereto. The external fields of the actuating magnets **5**, **6** act to sufficiently cancel the fields within the switch assembly, thereby releasing the reeds. The actuator comprises two or more permanent magnets **5**, **6** connected by a magnetic metal strap **7**. The magnetic metal strap **7** in this invention is not sufficiently substantial to constitute a magnetic yoke. It is an assembly fixture whereby the actuator permanent magnets are held in position during a subsequent potting process.

The permanent magnet polarities of the entire switch and actuator assemblies, as shown in Figure 8, may be reversed without effect. The reed switch lead wire symmetry as depicted in Figures 8 and 10 are necessary for successful operation of the switch assembly. Here again, we find the same interesting actuation range as was found in the Sentrol high security switch. Figure 11 shows a typical basic electrical schematic of the reed switch interconnection.

The switch assembly is adjusted in production by locating the reed switches away from their respective actuation positions along their mounting axis and then bringing an actuator assembly into a

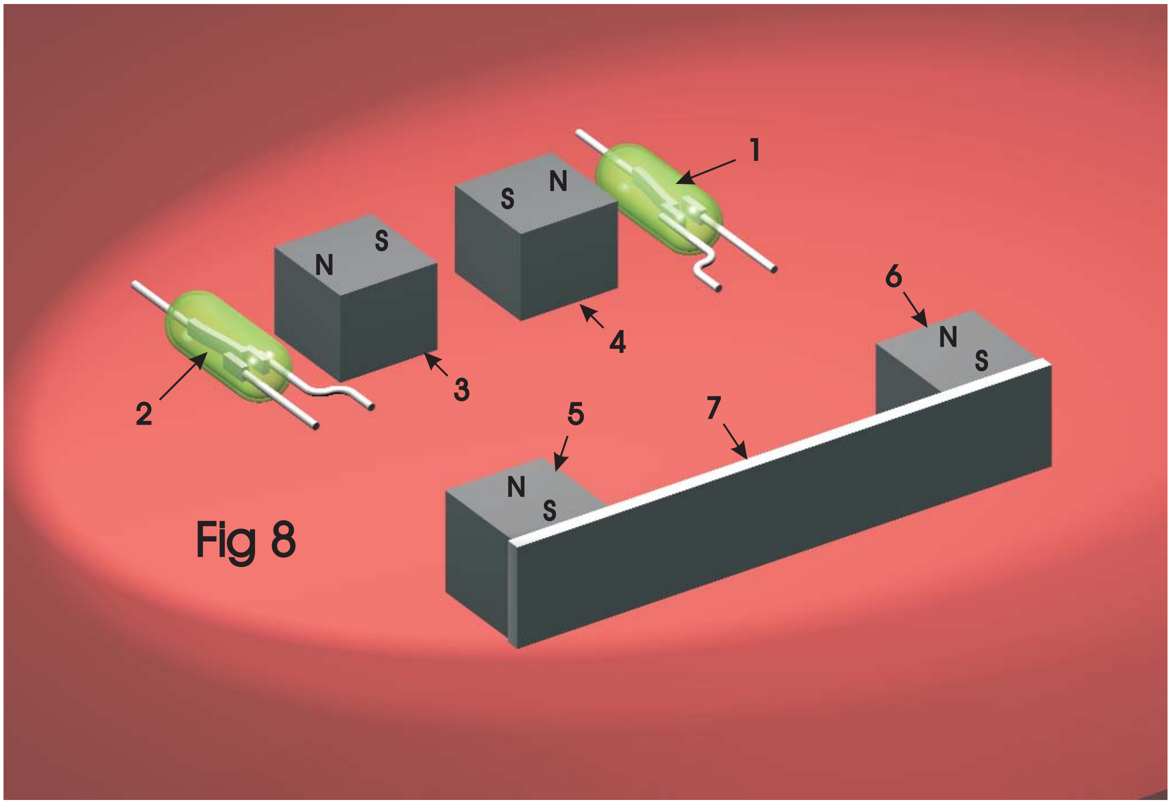


Fig 8

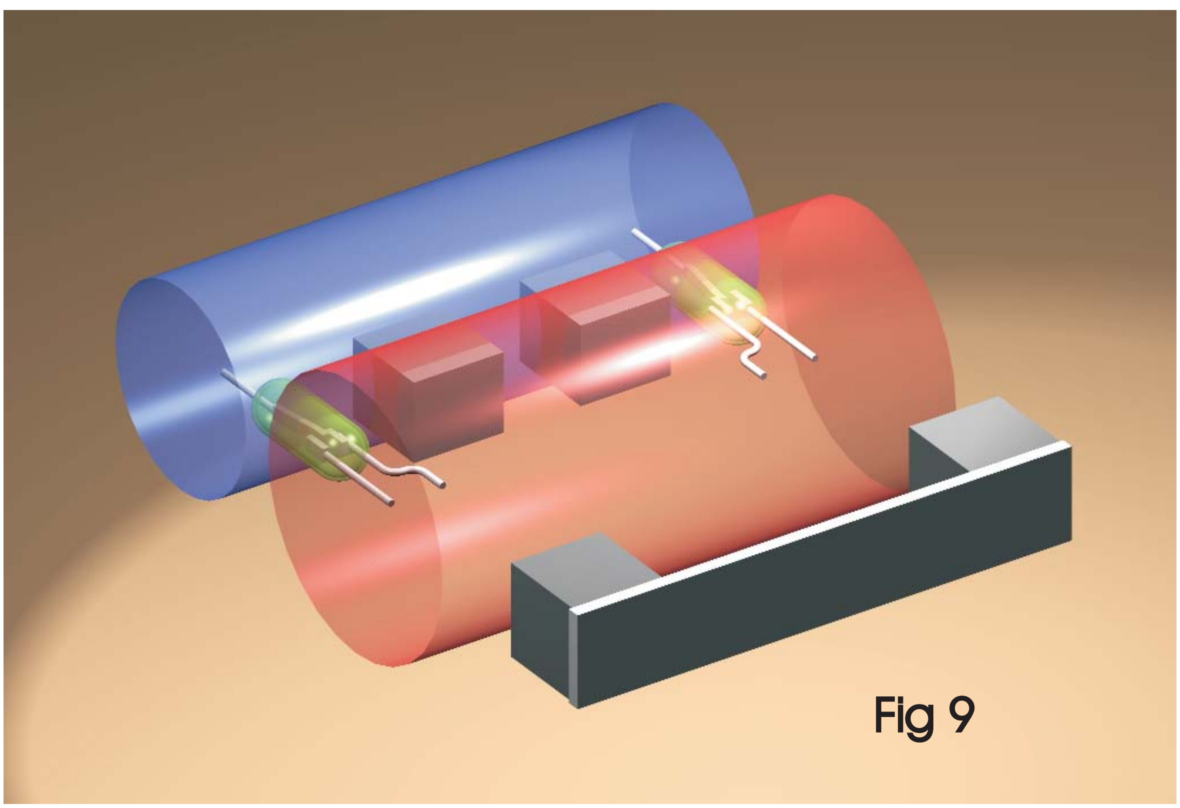


Fig 9

predetermined maximum actuation range. The reed switches are moved towards the actuator magnets along their mounting axis by the use of micrometers until they are actuated and soldered.

2.3.1 DEFEAT MECHANISMS

Figure 9 shows the Securitron switch assembly and actuator of Figure 8 with the actuation range of that switch shown in red and with the actuator **2** outside of that range. An actuator with the magnetic poles reversed will actuate the switch assembly in the blue range. A magnetic shield is necessary to alter both actuation ranges.

2.3.2 SHIELDING

Magnetic shielding does not mean that magnetic fields are eliminated inside the shielding mechanism. Magnetic shielding only attenuates the exterior magnetic fields to some acceptable level on the interior. Layers of shielding where each layer has a different magnetic composition are common. For the shielding to be effective, the shielding material can not saturate. At that point, the effective magnetic permeability becomes equivalent to air and no further attenuation occurs.

The amount of attenuation depends upon the shape of the shield and its material composition. The following is quoted from a brochure published by Magnetic Shield Corp. [25]:

> "The optimum shield is a closed, spherical configuration. In practice, effective shields can be cans, open-ended cylinders, five-sided boxes, U- or L-shaped brackets and even flat plates. A flat plate is effective if both the length and width of the shield exceed the distance separating the source and receiver of interference."

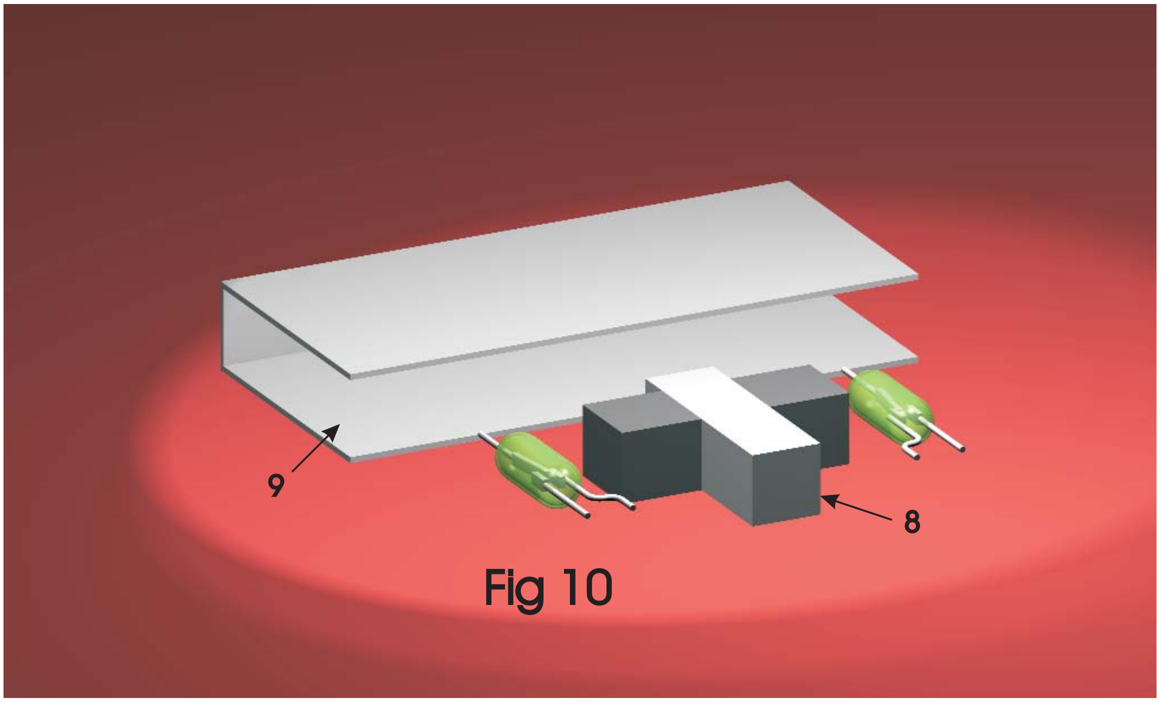


Fig 10

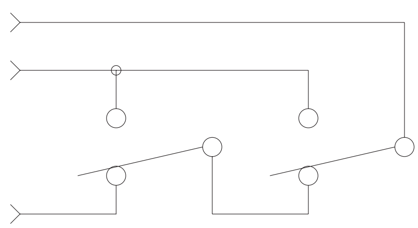


Fig 11

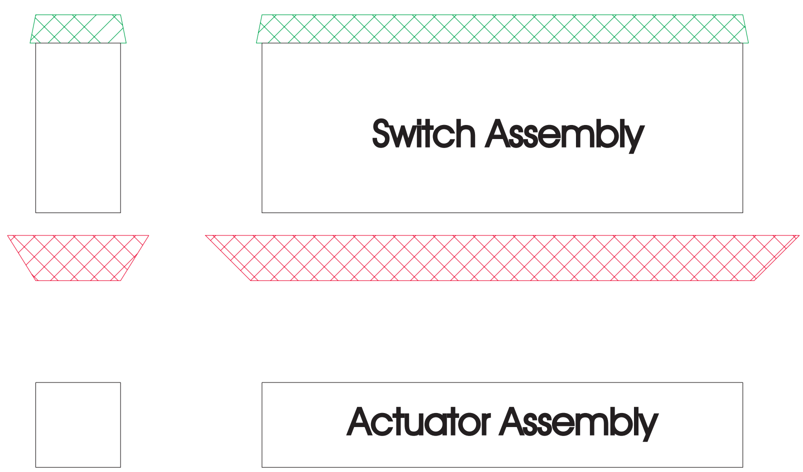


Fig 12

The following equation [24] [25] produces a useful magnetic field attenuation approximation for some purposes:

$$A := \frac{\mu \cdot t}{D}$$

where:

A = the attenuation ratio,

μ = the shield material magnetic permeability,

t = the shield thickness,

D = the shield diameter or diagonal of the shield.

Figure 10 is an exploded view of the Securitron switch assembly of Figure 8 outside of its U-shaped shield **9**. The switch assembly will not function correctly if the iron slug **8** is not present. The bottom of the U-shaped shield is not required for magnetic shielding of the switch assembly. In combination with the L-shaped shield of the top and back, it makes a convenient U-shaped enclosure for packaging. This combination has been referred to as “co-planar”.

Figure 12 shows a top and side view of a Securitron high security switch in its U-shaped housing. The actuator is drawn outside of the actuation range which is shown in cross-hatched red. There are two known ways to defeat the switch that are very simple and very reliable. The first involves the actuator from another switch of the same series or design stacked as shown in Figure 7. The other involves specially designed lock picking actuators.

It is not known at the time of this writing whether or not the top shield can be effectively penetrated by a special lock picking actuator. If such is the case, then, Figure 12 would look substantially like Figure 5 and the method of Figure 6 would be applicable. However, the back of the L-shaped shield can be penetrated with a special lock picking actuator. The green cross-hatch in Figure 5 shows the actuation range of specially designed lock picking actuators. The design of such lock picking devices is beyond the scope and intent of this material.

2.4 SUMMARY

Current high security switches embodying the prior technology are a collection of novel combinations of reed switches and permanent magnets. Whatever can be said about reed switches is then true of high security switches. Therefore, high security switches of the prior art are fragile sensitive devices. Their reliability is lower than other passive devices serving a similar function. They are prone to damage in production. They do not survive electrical or mechanical abuse well. Their sensitivity to extraneous electro-magnetic fields and shock result in high false alarm rates. Even with magnetic shields, they are still vulnerable to defeat by their own actuators or special lock picking actuators. These security switches have been based upon reed switch technology because there was no reasonable alternative.

Also, these high security switches rely on a multiplicity of conductors between the switch and the monitoring system to thwart attempts at shorting out the switch conductor pair. A skilled technician with hand held equipment can easily determine the character of the lines and short out the appropriate pair which bypasses the high security switch and breach the system.

3. THE JACKSON HIGH SECURITY SWITCH AND SWITCH SYSTEM

The Jackson high security switch is a magnetically-actuated, proximity switch system for use in physical security monitoring systems, machinery control systems, and the like, including a stationary assembly and an actuator assembly moveable relative to the stationary assembly. The actuating assembly includes at least three permanent magnets or their functional magnetic circuit equivalent arranged such that alternating magnetic poles of either the real or apparent (or consequent) type are produced. The stationary assembly includes at least three electrically-interconnected permanent magnet proximity switches of the type referenced in the U.S. provisional patent [41] arranged such that their polarities alternate resulting in snap action attraction mode switching when used in combination with the actuator assembly. Magnetic shields or magnetic field decouplers are placed between the individual permanent magnet proximity switches [42] to neutralize the interactive switch fields which might otherwise be detrimental to successful electrical contact of said switches. This combination cannot be defeated by a single permanent magnet, its own actuator assembly, or a special lock picking actuator due to the inherent directionality of the permanent magnet proximity switches [41] which require no shielding to manifest said directionality. An additional permanent magnet proximity switch [42] may be included as a tamper switch for the detection of removal of the stationary element from the mounting surface. Additionally, an electro-magnet spring magnet may be substituted for one or more of the spring magnets in accordance with the technology for the purposes of remote testing of the device. Voltage, current, and power handling of the device is limited only by the physical size and choice of electrical contact materials.

This technology may be used in combination with a radio frequency, magnetically actuated, proximity switch system for use in physical security monitoring systems, machinery control systems and the like [43]. This proximity switch system includes a stationary assembly, an actuator assembly moveable relative to the stationary assembly, and a radio frequency monitoring system to which the stationary assembly is connected by a coaxial cable or transmission line. The stationary assembly and the actuator assembly may be any magnetic proximity switch of the security or high security types, balanced or unbalanced, based upon, but not limited to, reed switch technology or the security switch technology referenced in a U.S. provisional patent [42], hereafter referred to as the Jackson Security Switch, or the types referenced in a U.S. provisional patent [41] of which all of the aforesaid types will hereafter be referred to collectively as Security Switches, without any limitations thereto, that are modified to include either a matched electrical load, a matched radio frequency generator, or a matched radio frequency generator in combination with a band pass filter and matched to a transmission line which is also matched to monitoring circuits. The monitoring system monitors the integrity of the switch and its associated coaxial cable or transmission line. An additional proximity switch, including reed switch technology, mechanical switches, or Jackson Switches, may be included as an anti-tamper switch for detecting the removal of the stationary element from the mounting surface. In this configuration, the anti-tamper switch is connected along with any security switch within the same housing and coupled to the coaxial cable or transmission line by such means that both said switches may use the same coaxial cable or transmission line without interference between the direct current voltages associated with each switch or the radio frequency signals. This also applies to any other combination of devices within said switch assembly that use direct current voltage and radio frequency signals jointly or separately. Said radio frequency monitored, magnetically actuated proximity switches, connected to a monitoring system by a coaxial cable or transmission line as part of an electronic physical security system or machinery control system for detecting and monitoring the opening or closing of panels, windows, doors or the like, will trigger an alarm state if any attempt is made to alter, modify, tamper, or interrupt said connecting coaxial cable or transmission line.

3.1 THE JACKSON HIGH SECURITY SWITCH

Referring to FIG. 13, a top view of the armature **5** and two sets of electrical contacts, set one consisting of elements **1** and **2**, and set two consisting of elements **3** and **4**, is shown hermetically sealed in a glass envelope **6**. The spring magnet and actuator magnet are not shown. The direction of permanent magnet magnetization is shown by the arrow.

FIG. 14 is a three dimensional view of FIG. 13 showing the two sets of electrical contact leads extending through the glass envelope **6** for easy circuit board mounting.

Referring to FIG. 15 and 16, a top view and a three dimensional view respectively, of a high security switch comprising three Jackson Switch modules, elements **7**, **8**, and **9**, as defined in FIG. 13 and 14 with corresponding spring permanent magnets, elements **15**, **14**, and **13**, respectively are shown. The spring magnets, elements **15**, **14**, and **13** are mounted on a magnetically soft material or yoke **16**, such as iron, which strengthens the magnet fields resulting in a stronger spring force and a more economical use of materials. The interactive fields between the switch modules, elements **7**, **8**, and **9** are decoupled by the shields, elements **17**, **18**, **19**, and **20** which eliminates the detrimental affect of said interactive fields upon switching action. All of the components are mounted on a printed circuit board **22**.

The actuator assembly consists of three permanent magnets, elements **10**, **11**, and **12**, which are fastened to a magnetically soft material or yoke **21**, such as iron which strengthens the magnet fields resulting in a stronger actuating force and a more economical use of materials.

The polarities of all of the permanent magnet elements are clearly marked on the top view in FIG. 15 by N for north and S for south. The entire combination is operated in accordance with the Jackson Switch

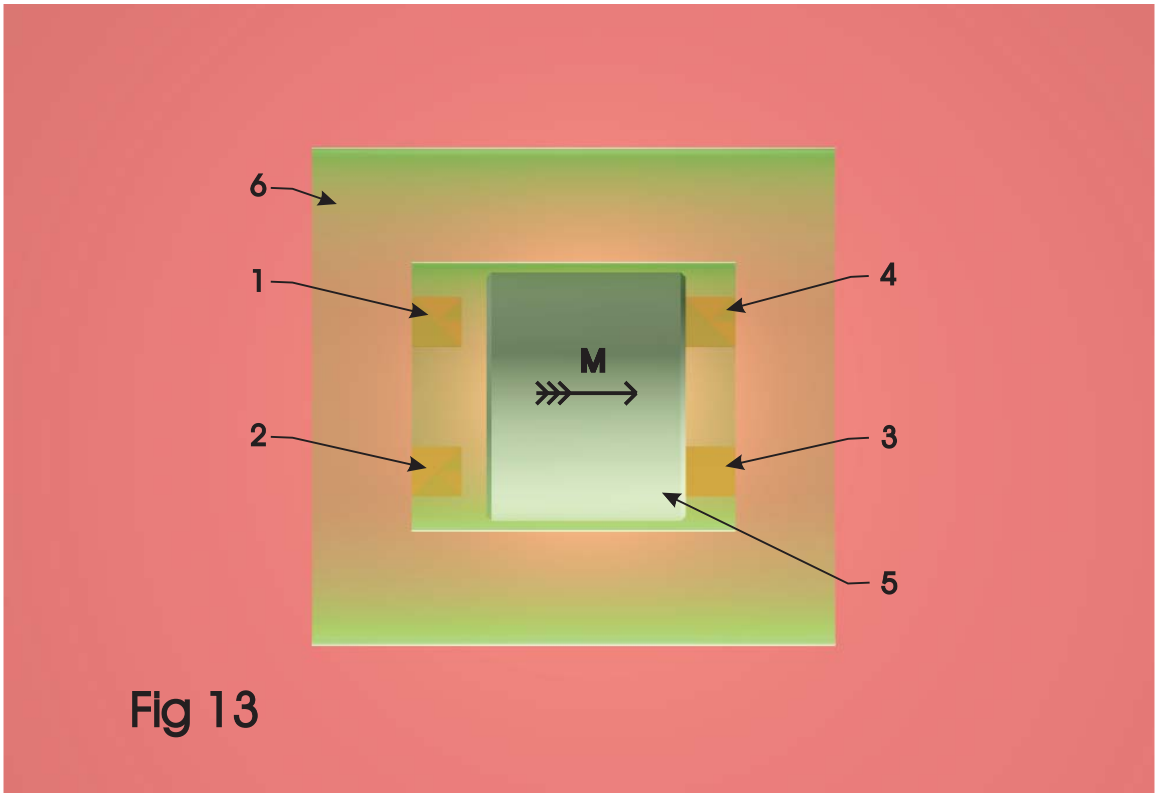


Fig 13

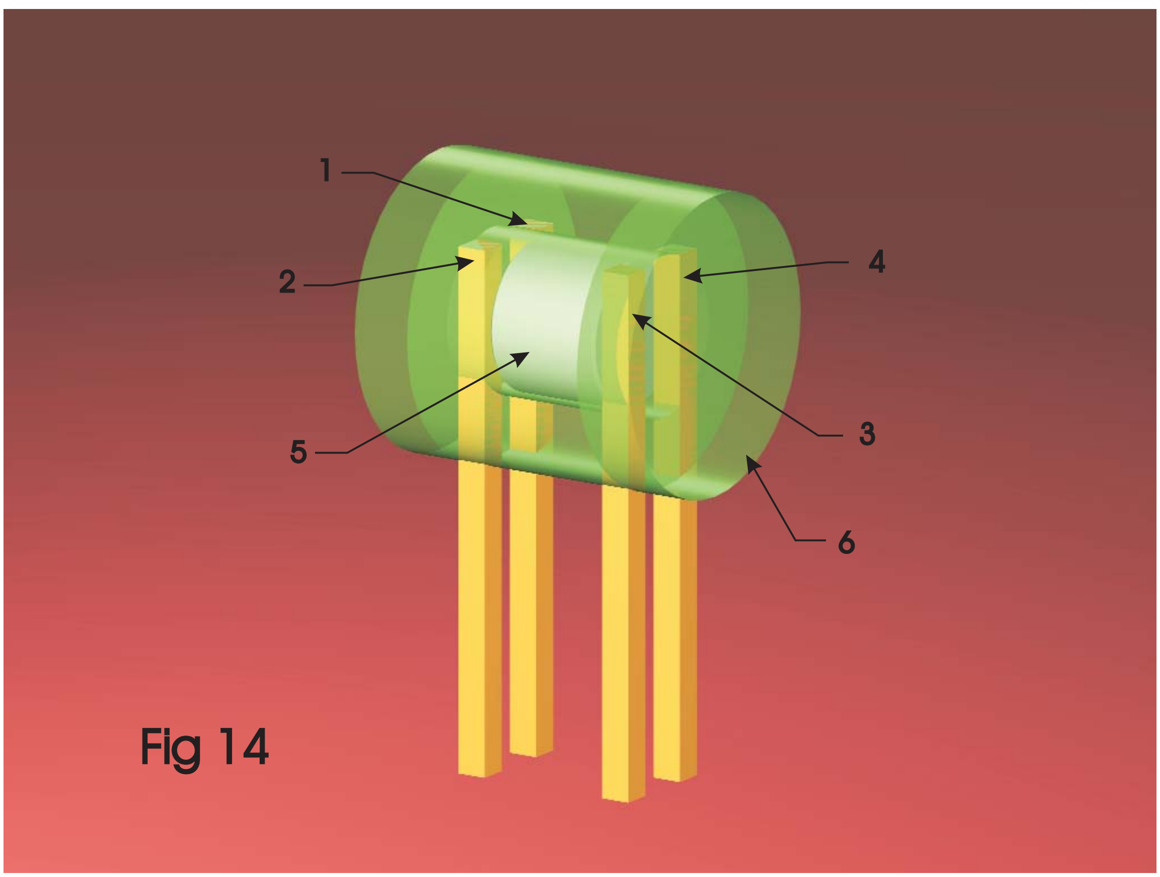


Fig 14

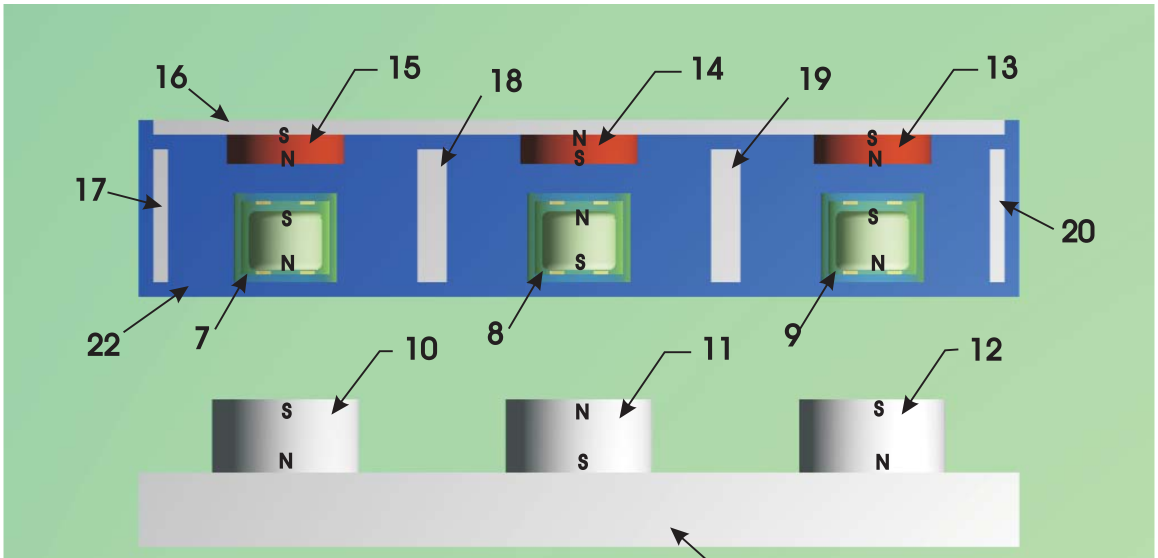

16
15
18
14
19
13
S
N
N
S
S
N
17
S
N
N
S
S
N
20
22
7
8
9
10
11
12
S
N
N
S
S
N
21

Fig 15

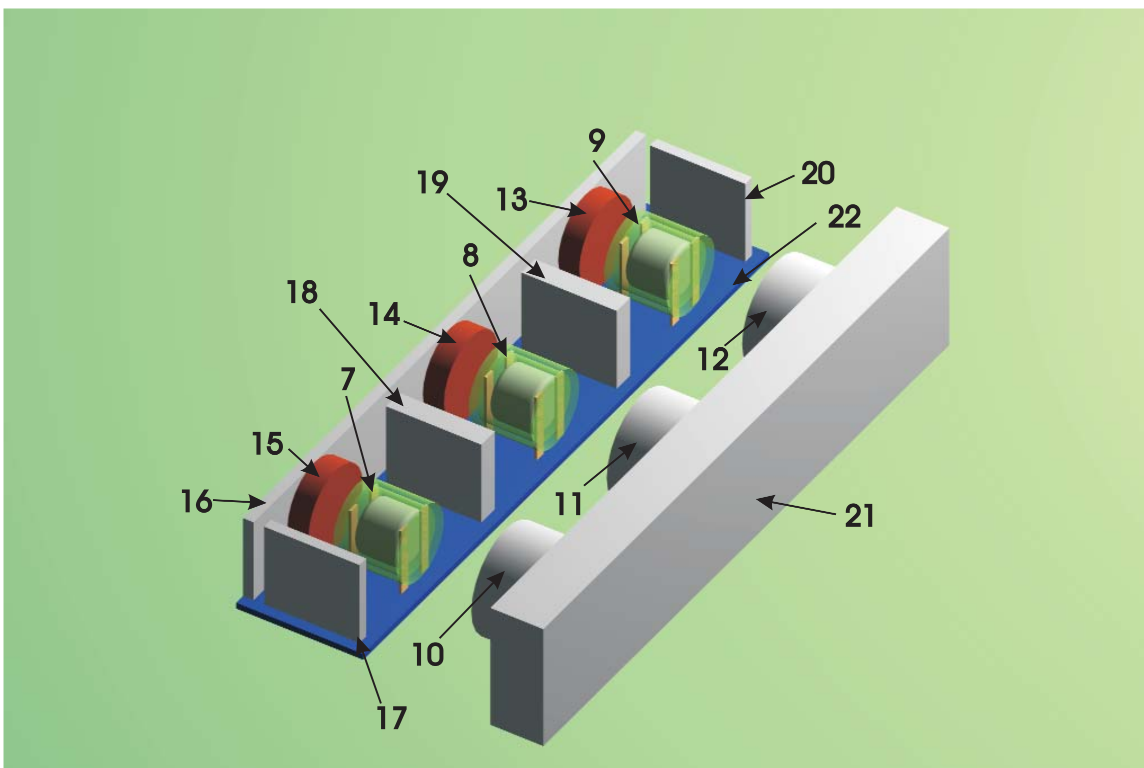

9
20
19
13
22
8
18
14
12
7
15
16
11
21
10
17

Fig 16

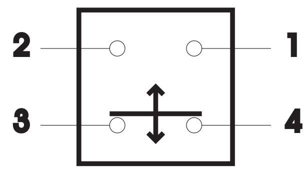


Fig 17A

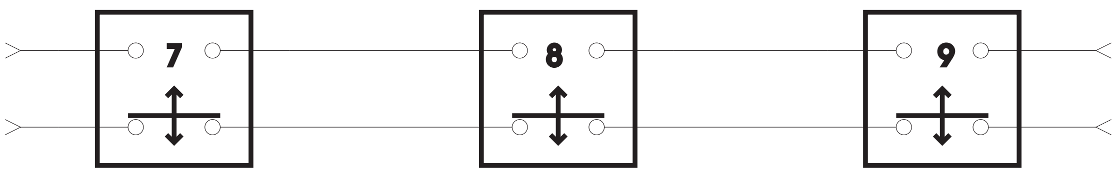


Fig 17B

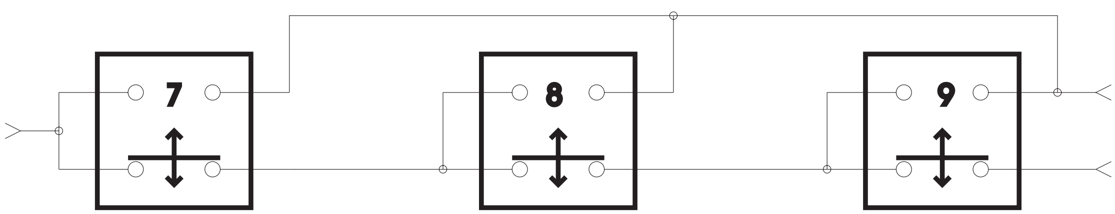


Fig 17C

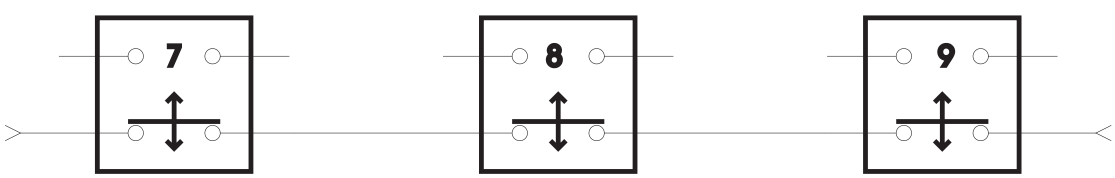


Fig 17D

technology snap-action attraction mode. Of course, the polarities of all of the permanent magnets may be reversed with completely equivalent operation. This mode of operation regarding permanent magnet polarities is hereafter assumed without further reference unless otherwise stated.

Referring to FIG. 17A, B, C, and D, electrical schematics of a Jackson Switch with two sets of electrical contacts, a high security switch wired double pole double throw (DPDT), a high security switch wired single pole double throw (SPDT), and a high security switch wired single pole single throw (SPST) are shown respectively. The high security switch in FIG. 15 and 16 may be wired by any suitable means but are not limited to the said schematics B, C, and D.

Referring to FIG. 18 and 19, a top view and a three dimensional view respectively, of a high security switch comprising three permanent armature magnets, elements **23**, **24**, and **25**, and three corresponding permanent spring magnets, elements **26**, **27**, and **28** respectively are shown. The permanent armature magnets are enclosed in a single integrated armature block **37** consisting of any suitable non-magnetic dielectric material or insulator such as plastic, glass, or ceramic. The actuation gap of the switch is set by the thickness of the integrated spacer **38** consisting of any suitable non-magnetic material such as plastic, glass, ceramic, or metal to which the permanent spring magnets are fastened. The magnetically soft screws, elements **29**, **30**, **31**, and **32**, extend through the printed circuit board **52**, as defined in FIG. 20, the armature block **37**, and the spacer **38** and decouple the interactive fields between permanent armature magnets, elements **23**, **24**, and **25**, which eliminates the detrimental affect of said interactive fields upon switching action. The magnetically soft plate or yoke **39**, consisting of any magnetically soft material such as iron, strengthens the spring magnet fields, resulting in a stronger spring force and provides a more economical use of materials. This high security switch is wired single pole single throw (SPST) as shown in FIG. 26. The entire assembly may be fastened together by such suitable means and in combination with appropriate materials to produce a hermetically sealed unit.

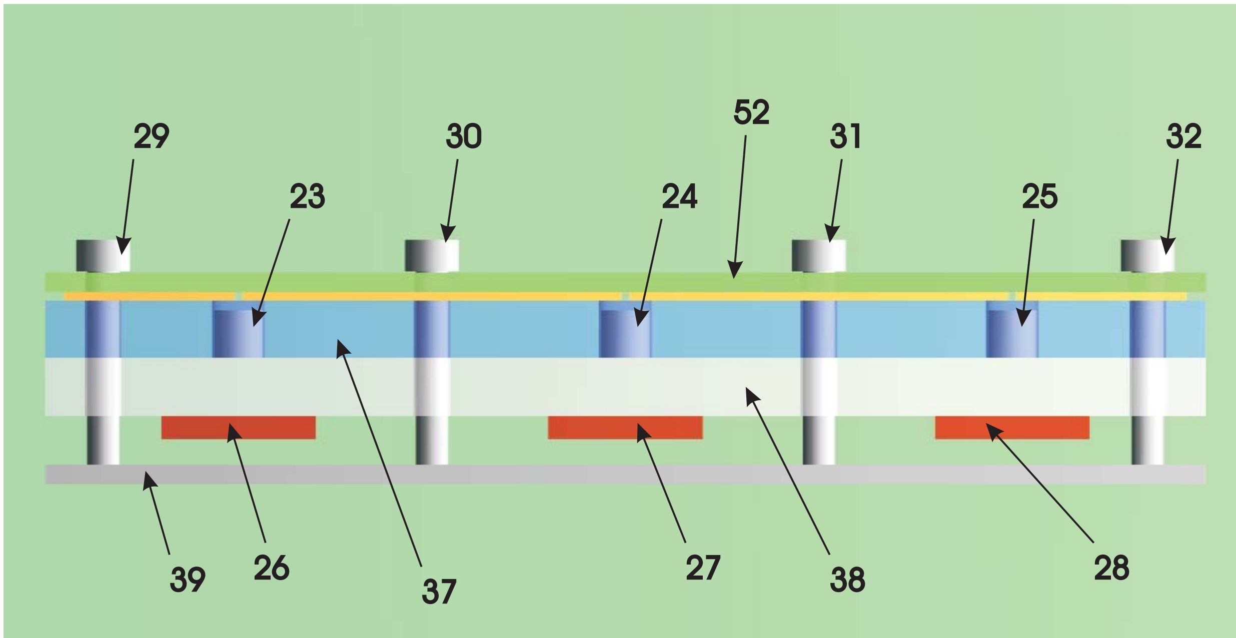

29
30
52
31
32
23
24
25
39
26
37
27
38
28

Fig 18

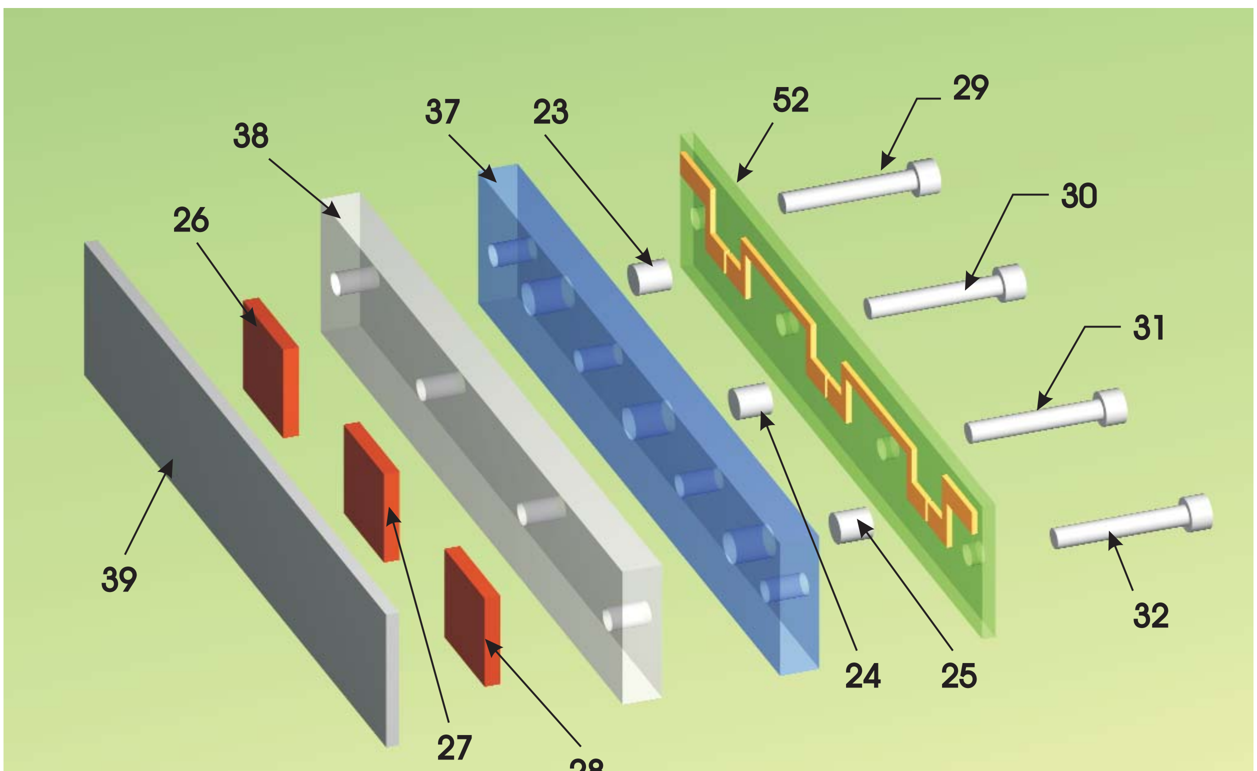

29
52
37
23
38
30
26
31
39
32
24
25
27
28

Fig 19

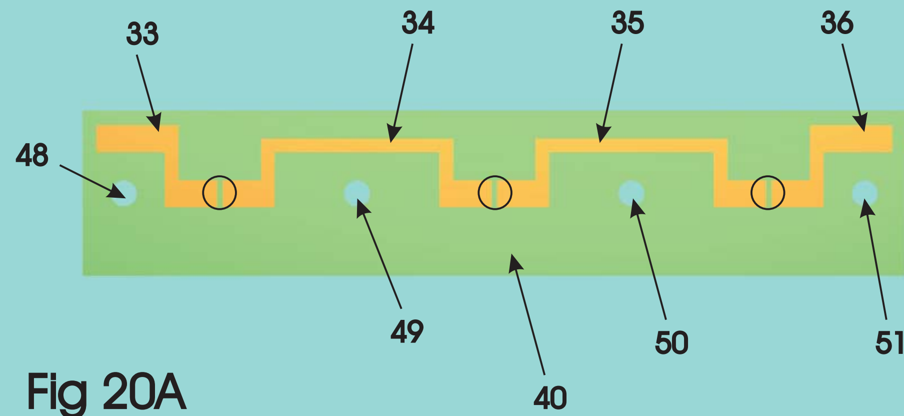


Fig 20A

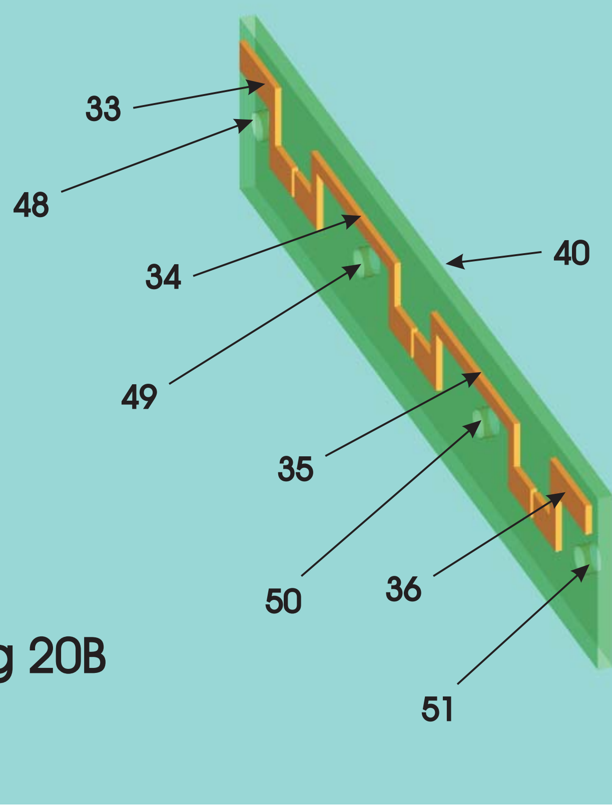
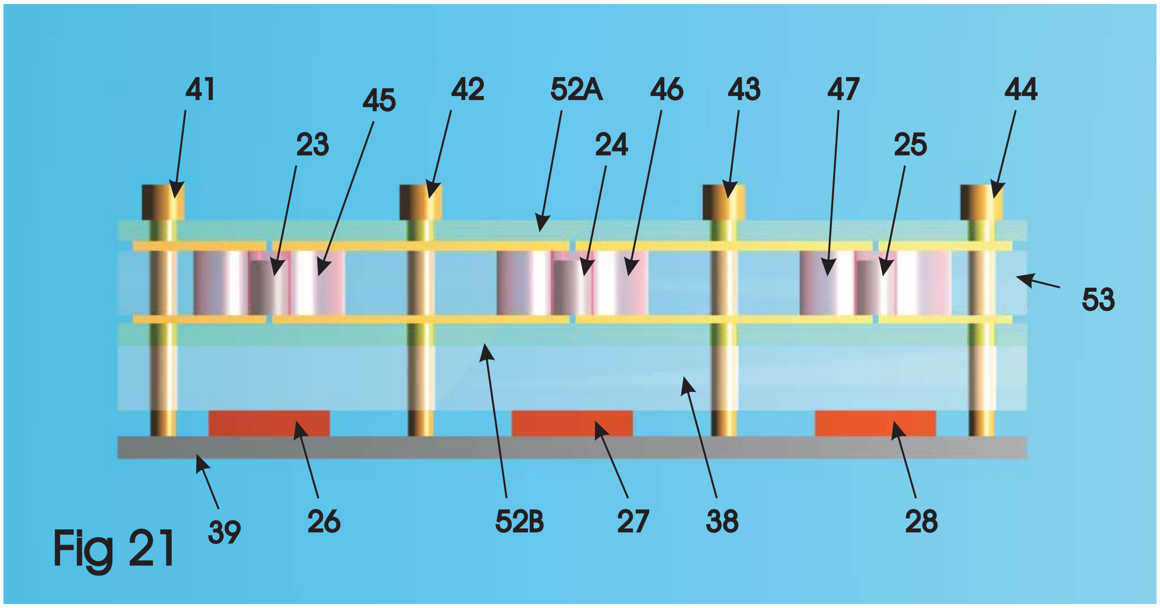
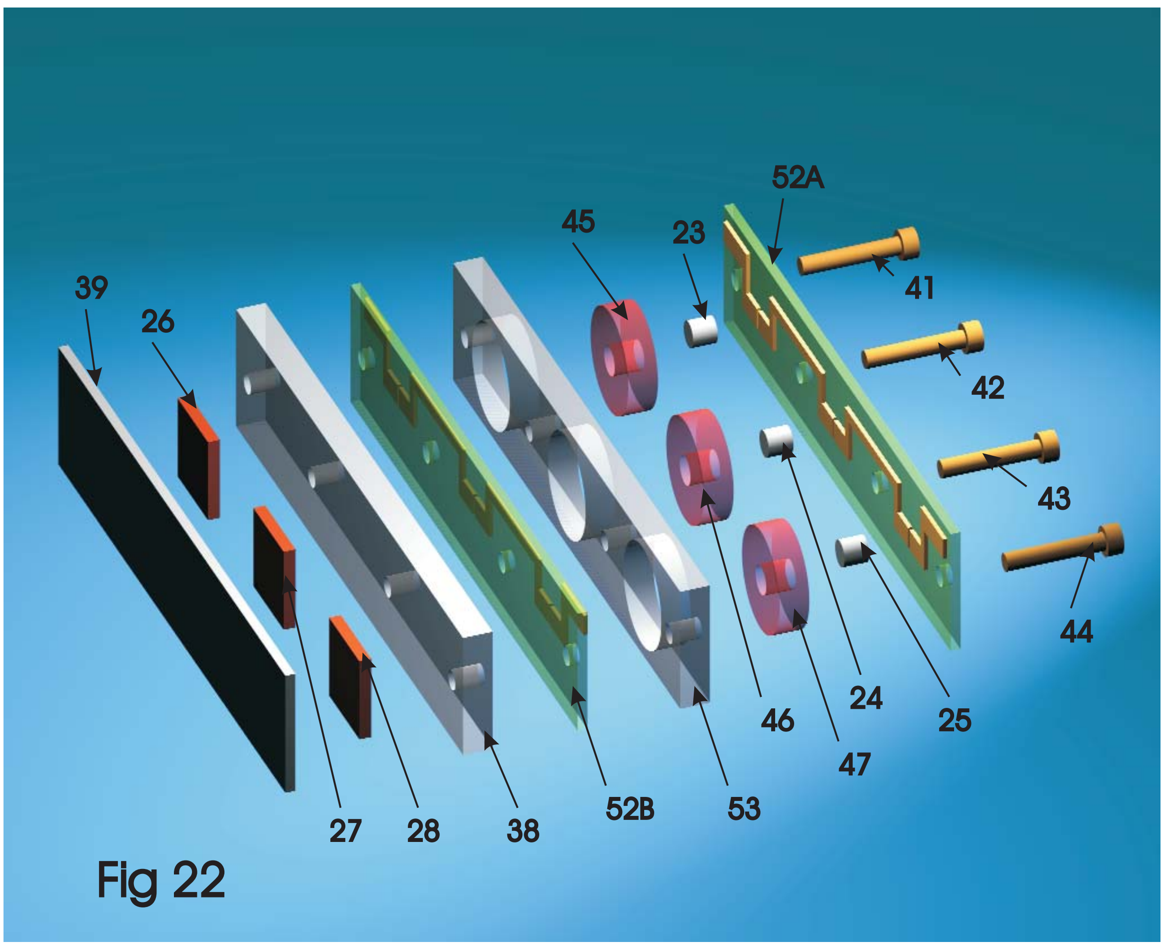


Fig 20B

Referring to FIG. 20A and B, a top view and a three dimensional view respectively, of three sets of electrical contacts and connecting traces integrated onto a printed circuit board made out of any suitable material, for example epoxy glass or ceramic, are shown. The left circle drawn on the top view shows the electrical contact area between traces **33** and **34** made by the permanent armature magnet **23** from FIG. 18 and 19. The central circle drawn on the top view shows the electrical contact area between traces **34** and **35** made by the permanent armature magnet **24** from FIG. 18 and 19. The right circle drawn on the top view shows the electrical contact area between traces **35** and **36** made by the permanent armature magnet **25** from FIG. 18 and 19. All of the permanent armature magnets must make contact for electrical continuity across the board. The elements **48**, **49**, **50**, and **51** are through holes for the magnet field decoupling screws.

Referring to FIG. 21 and 22, a top view and a three dimensional exploded view respectively, of a high security switch comprising three permanent armature magnets, elements **23**, **24**, and **25**, and three corresponding permanent spring magnets, elements **26**, **27**, and **28** respectively are shown. The permanent armature magnets are enclosed in individual armature blocks, elements **45**, **46**, and **47** respectively, consisting of any suitable non-magnetic dielectric material or insulator such as plastic, glass, or ceramic which are inserted into an integrated magnetic field decoupler **53,** made from any suitable magnetically soft material such as iron, to decouple the interactive fields between permanent armature magnets, elements **23**, **24**, and **25**, which eliminates the detrimental affect of said interactive fields upon switching action. The actuation gap of the switch is set by the thickness of the integrated spacer **38** consisting of any suitable non-magnetic material such as plastic, glass, ceramic, or metal to which the permanent spring magnets are fastened. The non-magnetic screws, for example brass, elements **41**, **42**, **43**, and **44**, extend through the printed circuit boards **52A** and **52B** as defined in FIG. 20, the armature block **53**, and the spacer **38**. The magnetically soft plate or yoke **39**, consisting of any magnetically soft material, such as iron, strengthens the spring magnet fields resulting in a stronger spring force and provides a more economical use of materials. This high security switch is wired double pole double throw


41
45
42
52A
46
43
47
44
23
24
25
53
39
26
52B
27
38
28
Fig 21


52A
45
23
41
39
26
42
43
44
24
25
46
47
27
28
38
52B
53
Fig 22

(DPDT) as shown in FIG. 17B. The entire assembly may be fastened together by such suitable means and in combination with appropriate materials to produce a hermetically sealed unit.

Referring to FIG. 23 and 24, a top view and a three dimensional view respectively, of a high security switch comprising three permanent armature magnets, elements **23**, **24**, and **25**, are shown. The permanent armature magnets are enclosed in a single integrated armature block **37** consisting of any suitable non-magnetic dielectric material or insulator such as plastic, glass, or ceramic. The actuation gap of the switch is set by the thickness of the integrated spacer **38** consisting of any suitable non-magnetic material such as plastic, glass, ceramic, or metal to which the permanent spring magnets are fastened. The magnetically soft screws, elements **29**, **30**, **31**, and **32**, extend through the printed circuit board **52**, as defined in FIG. 8, the armature block **37**, and the spacer **38** and decouple the interactive fields between permanent armature magnets, elements **23**, **24**, and **25**, which eliminates the detrimental affect of said interactive fields upon switching action. The magnetically soft plate or yoke **39**, consisting of any magnetically soft material such as iron, acts as an integrated spring magnet for a more economical use of materials. This high security switch is wired single pole single throw (SPST) as shown in FIG. 26. The entire assembly may be fastened together by such suitable means, and in combination with appropriate materials, to produce a hermetically sealed unit.

Referring to FIG. 25A, a top view of a complete single Jackson Switch without the actuator magnet configured for use as a tamper switch is shown. The permanent armature magnet **56** is enclosed by a single armature block **55** consisting of any suitable non-magnetic dielectric material or insulator such as plastic, glass, or ceramic. A permanent spring magnet **54** is fastened to the armature block **55**. The electrical contacts, elements **57** and **58**, are traces on a printed circuit board **59** made out of any suitable material, for example epoxy glass or ceramic. Electrical continuity is achieved when the permanent armature magnet **56** is in physical contact with the two said electrical contacts. The entire assembly may

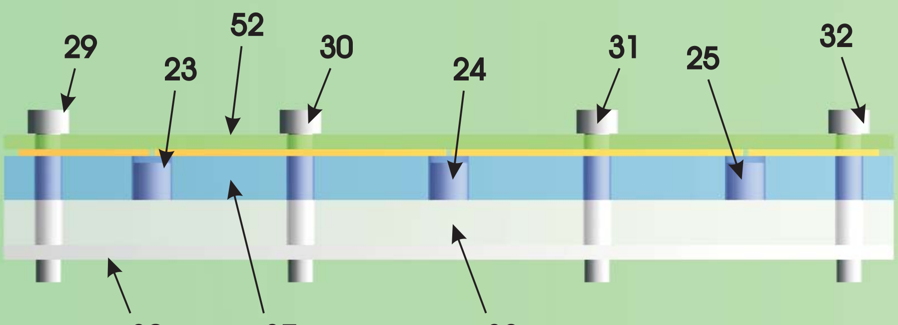


Fig 23

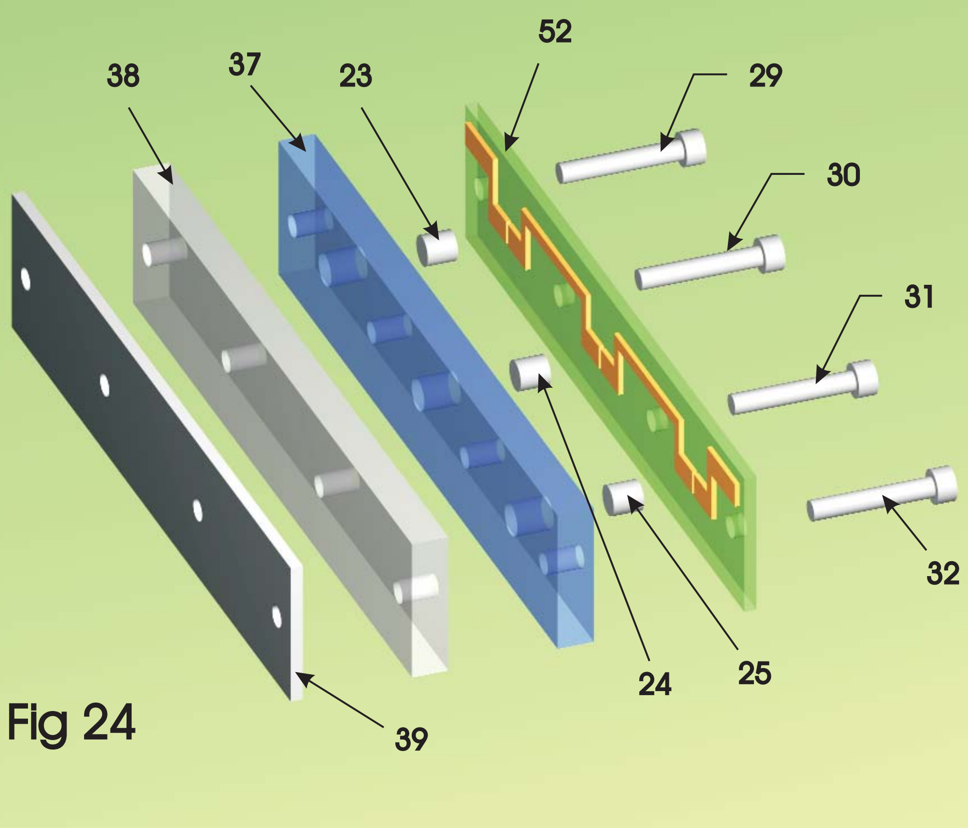


Fig 24

be fastened together by such suitable means, and in combination with, appropriate materials to produce a hermetically sealed unit.

Referring to FIG. 25B, a electrical schematic of the Jackson Switch in FIG. 25A is shown.

FIG. 26 is an electrical schematic of a high security switch consisting of three integrated Jackson Switches wired single pole single throw (SPST).

Referring to FIG. 27, a three dimensional exploded view of FIG. 25A is shown with the actuator magnet **60** in its respective actuating position.

Referring to FIG. 28, a three dimensional view of a high security switch in combination with a tamper switch and its actuator and the mounting method are shown for which one possible electrical schematic is also shown in FIG. 28. The high security switch **62** and the tamper switch **61** are shown enclosed in a housing **63** that is pulled away from the door frame or wall revealing the tamper switch actuator magnet **60** and its mounting hole **64** in the door frame or wall. The high security switch actuator **65** is shown attached to the partially open door in its appropriate position. If the switch housing is removed from the door frame or wall an alarm condition results when the tamper switch opens.

FIG. 29 is one possible electrical schematic of Figure 28.

Referring to FIG. 30 and 31, a top view and a three dimensional exploded view respectively, of a high security switch comprising three permanent armature magnets, elements **23**, **24**, and **25**, and two permanent spring magnets, elements **27** and **28** are shown. An electro-magnet comprising an electrical coil **69** and a magnetically soft core **68** act as the spring magnet for the permanent armature magnet **23**. When the switch is actuated to be in the alarm safe condition and a voltage of the appropriate polarity is

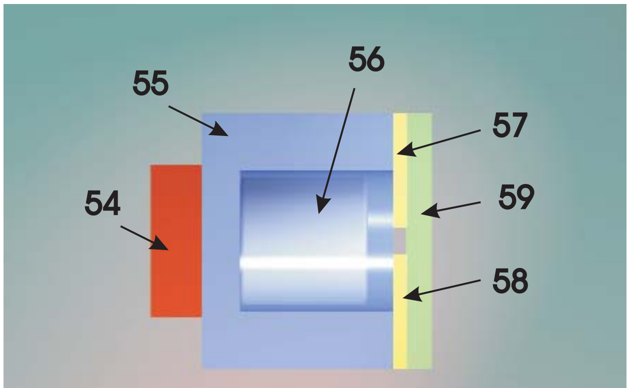


Fig 25A

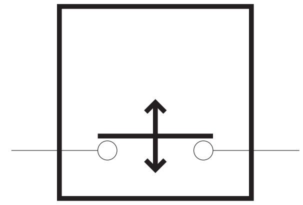


Fig 25B

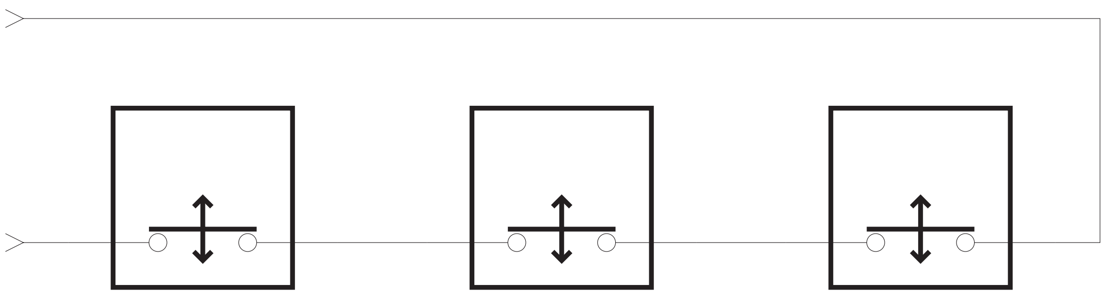


Fig 26

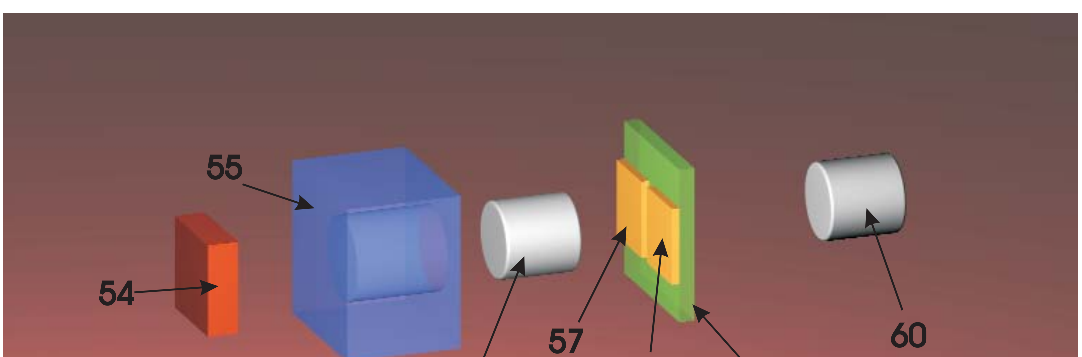


Fig 27

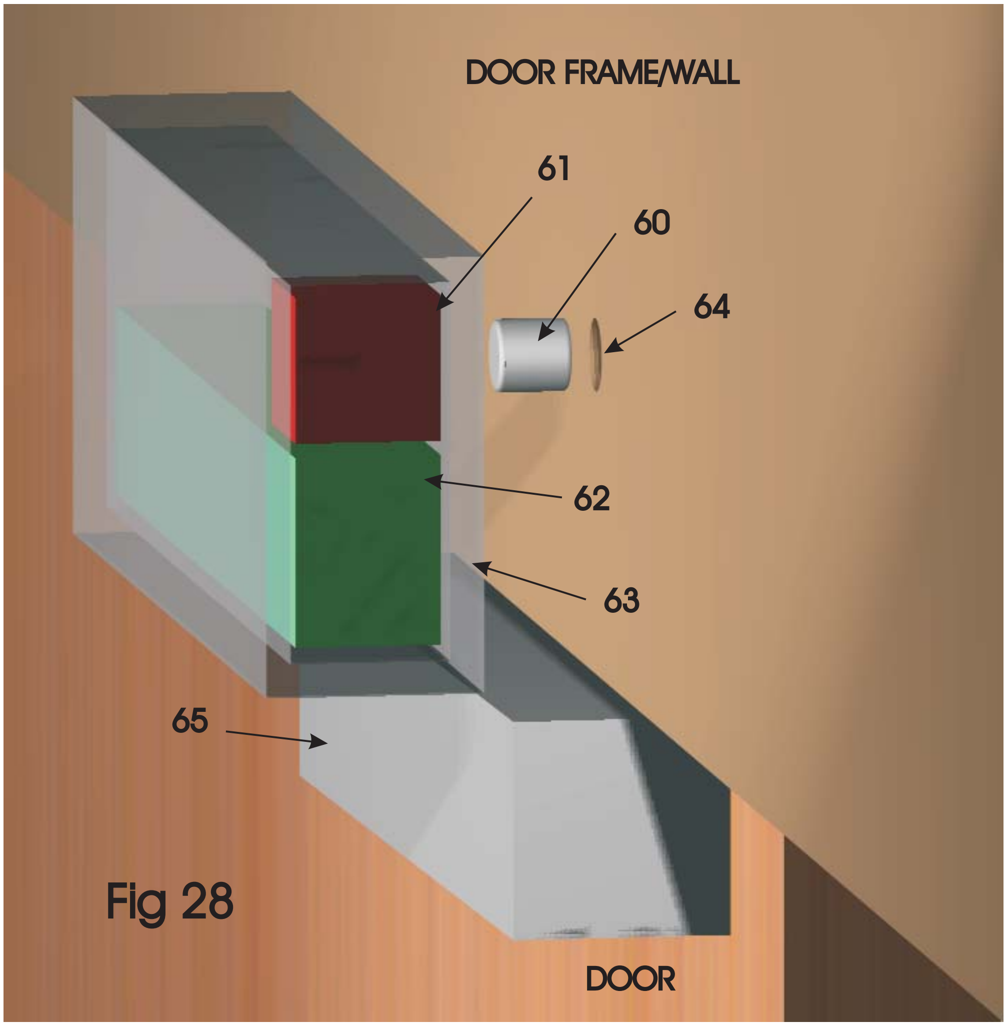


Fig 28

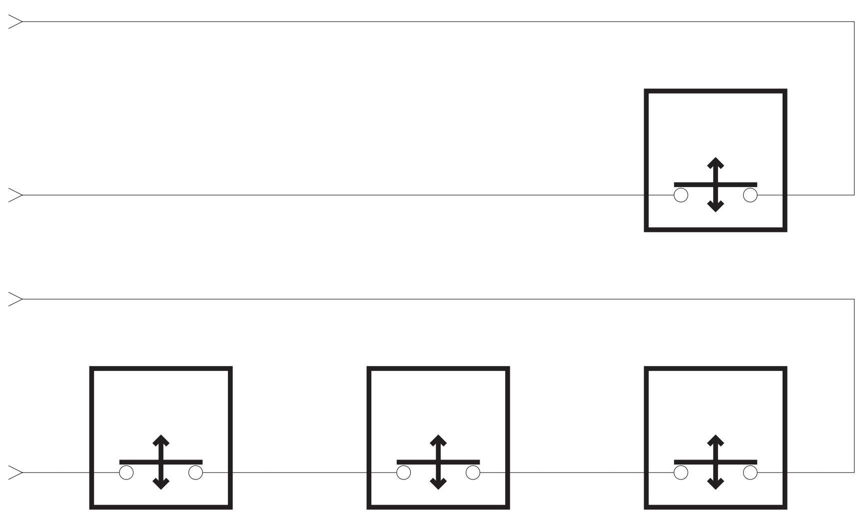


Fig 29

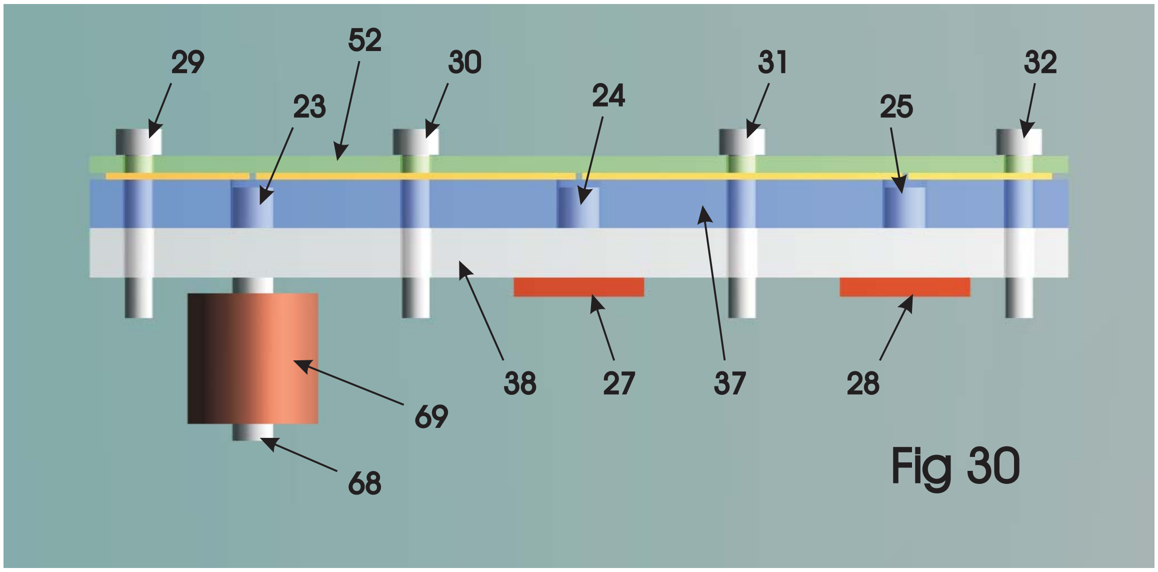

29
52
30
31
32
23
24
25
38
27
37
28
69
68

Fig 30

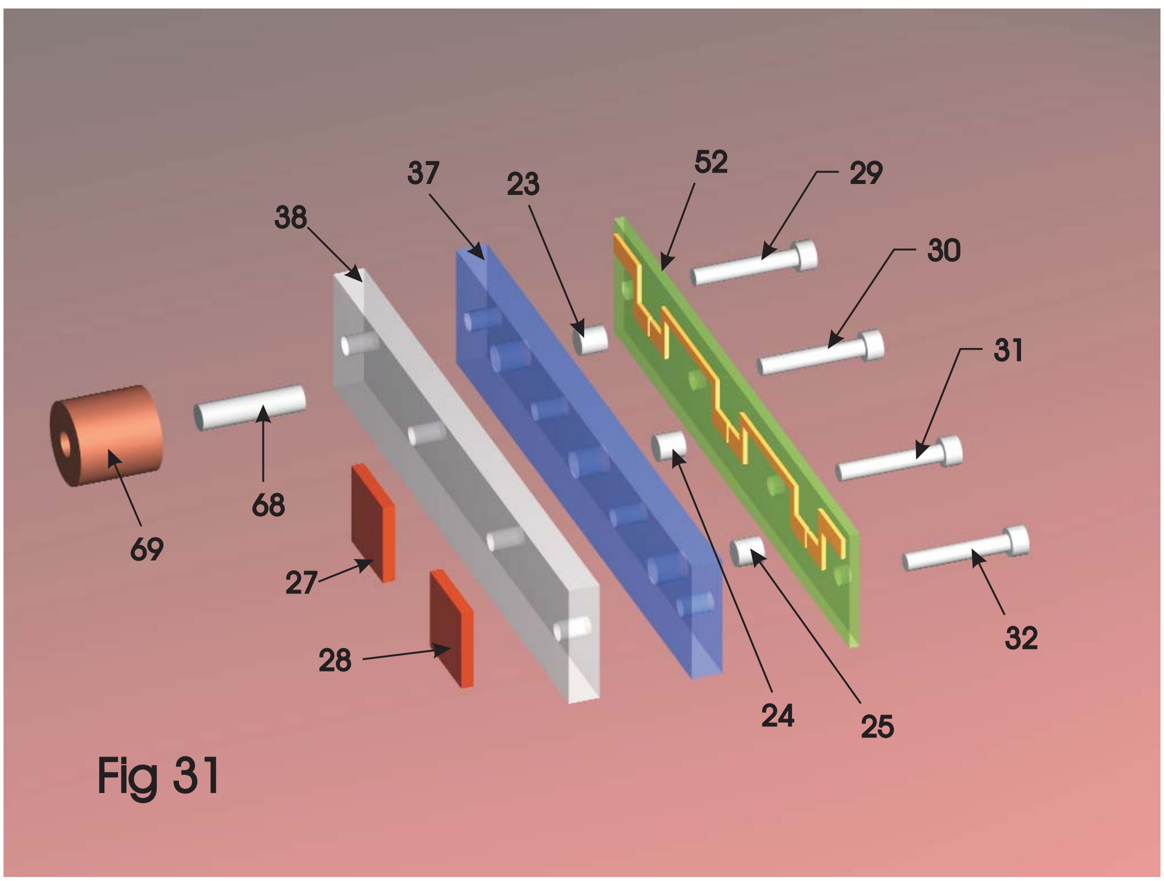

37
23
52
29
38
30
31
69
68
27
28
24
25
32

Fig 31

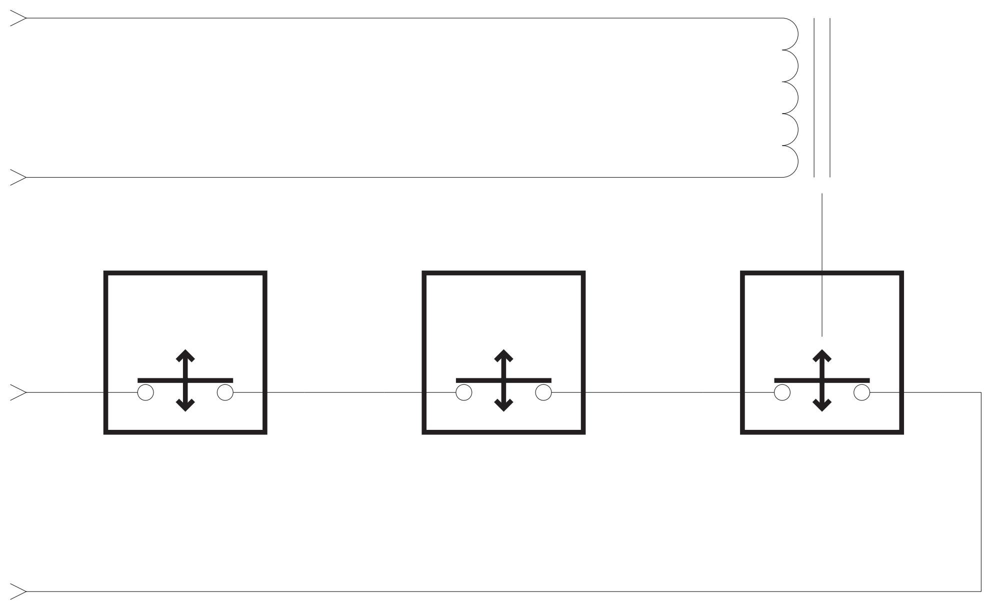


Fig. 32

applied to the coil, the permanent armature magnet will move producing an alarm condition. The permanent armature magnets are enclosed in a single integrated armature block **37** consisting of any suitable non-magnetic dielectric material or insulator such as plastic, glass, or ceramic. The actuation gap of the switch is set by the thickness of the integrated spacer **38** consisting of any suitable non-magnetic material such as plastic, glass, ceramic, or metal to which the permanent spring magnets are fastened. The magnetically soft screws, elements **29**, **30**, **31**, and **32**, extend through the printed circuit board **52**, as defined in FIG. 20, the armature block **37**, and the spacer **38** and decouple the interactive fields between permanent armature magnets, elements **23**, **24**, and **25**, which eliminates the detrimental affect of said interactive fields upon switching action. This high security switch is wired single pole single throw (SPST) as shown in FIG. 26. The entire assembly may be fastened together by such suitable means and in combination with appropriate materials to produce a hermetically sealed unit.

FIG. 32 is an electrical schematic of FIG. 31.

3.2 THE RADIO FREQUENCY SYSTEM

Referring to Fig. 33A and 33B, a top view and a three dimensional view respectively, of a high security switch comprising three permanent armature magnets, elements **1**, **2**, and **3**, are shown. The permanent armature magnets are enclosed in a single integrated armature block **4** consisting of any suitable non-magnetic dielectric material or insulator such as plastic, glass, or ceramic. The actuation gap of the switch is set by the thickness of the integrated spacer **5** consisting of any suitable non-magnetic material such as plastic, glass, ceramic, or metal to which the permanent spring magnets are fastened. The magnetically soft screws, elements **7**, **8**, **9**, and **10**, extend through the printed circuit board **14**, as defined in FIG. 34, the armature block **4**, and the spacer **5,** and decouple the interactive fields between the permanent armature magnets, elements **1**, **2**, and **3**, which eliminates the detrimental affect of said

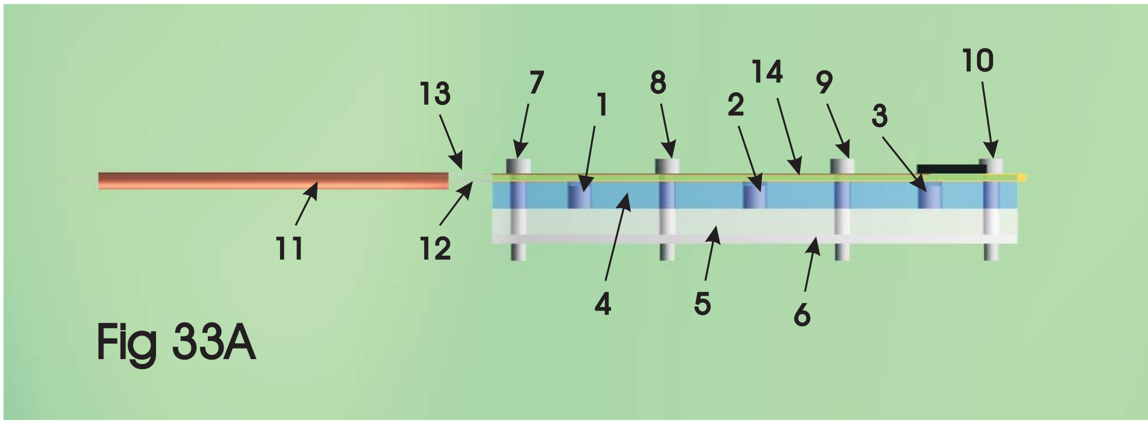


Fig 33A

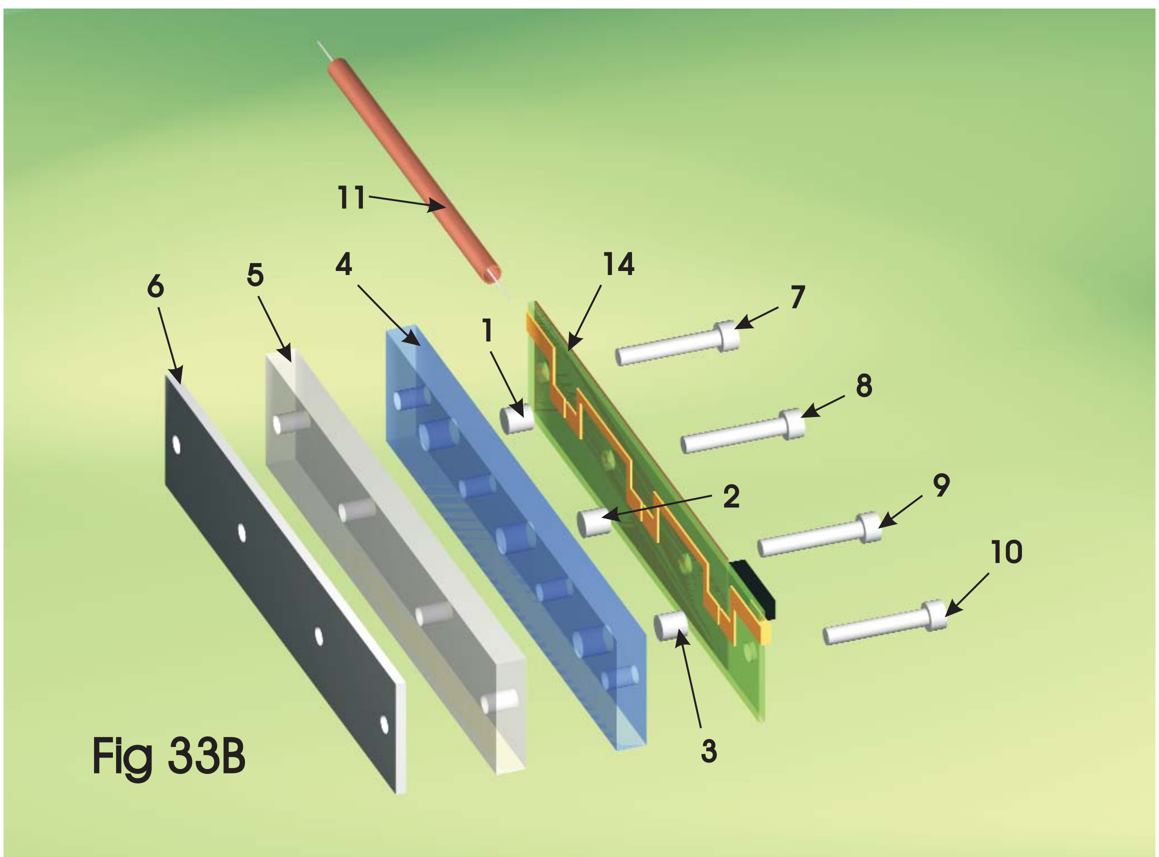


Fig 33B

interactive fields upon switching action. The magnetically soft plate or yoke **6**, consisting of any magnetically soft material such as iron, acts as an integrated spring magnet, resulting in a more economical use of materials. A coaxial cable or transmission line **11** connects to the high security switch circuit board **14** such that the center conductor of the transmission connects to the trace **16** of the circuit board shown in Fig. 34A, and the outer conductor or shield connects to the ground plane **25** of the circuit board shown in Fig. 34B. This high security switch is wired, but not limited to, single pole single throw (SPST) as shown in FIG. 35. The entire assembly may be fastened together by any suitable means and in combination with appropriate materials may produce a hermetically sealed unit.

Referring to Fig. 34A and 34B, a front view and a back view of the circuit board **14** in Fig. 33 respectively, the gaps in the three sets of traces between **16** and **17**, **17** and **18**, and **18** and **19,** are shorted out by the armature magnets **1**, **2**, and **3** respectively when actuated by the actuator assembly. Trace **19** is shown wrapping around the edge of the circuit board substrate **15**, which is made, for example, from epoxy glass, Teflon, ceramic, or other suitable material, to the back side where a load resistor **24**, preferably 50Ω, designated as LOAD in Fig. 35, connects said trace to the ground plane **25**. There are four holes **20**, **21**, **22**, **23** through the circuit board substrate **15** to accommodate said magnetic field decouplers.

Referring to Fig. 35, one preferred embodiment of the invention is a security monitoring system comprising a radio frequency oscillator, designated OSC, which sends a radio frequency signal through the MISMATCH DETECTOR and down the transmission line as shown. The radio frequency signal travels through the Jackson Security Switch when actuated, shown by the three switch icons, and terminates in the LOAD. The electrically grounded box surrounding the switch assembly is an electrically conductive housing that is grounded to the transmission line's outer conductor. When the oscillator, MISMATCH DETECTOR, transmission line, Jackson Security Switch, and LOAD are substantially matched, there will be a minimal reflection of the radio frequency signal. The MISMATCH DETECTOR

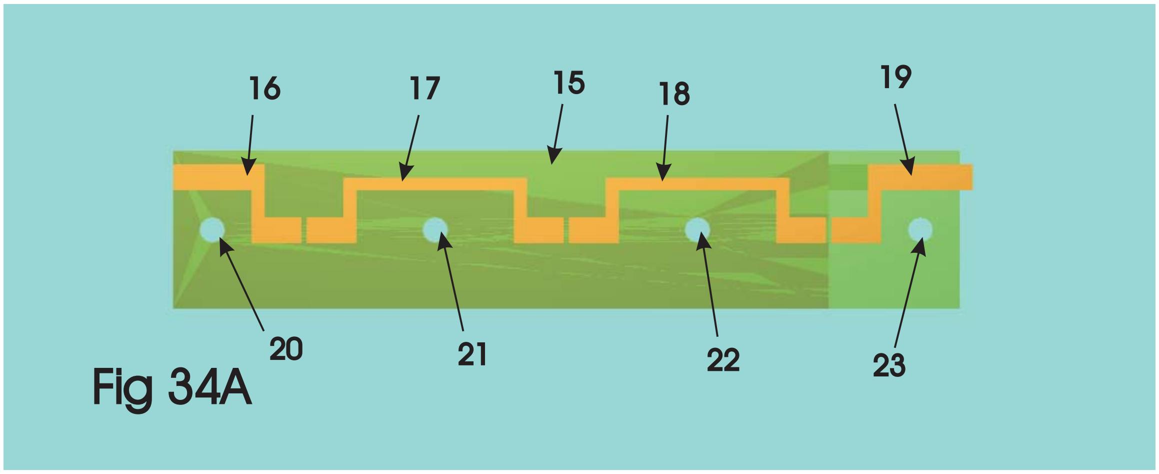


Fig 34A

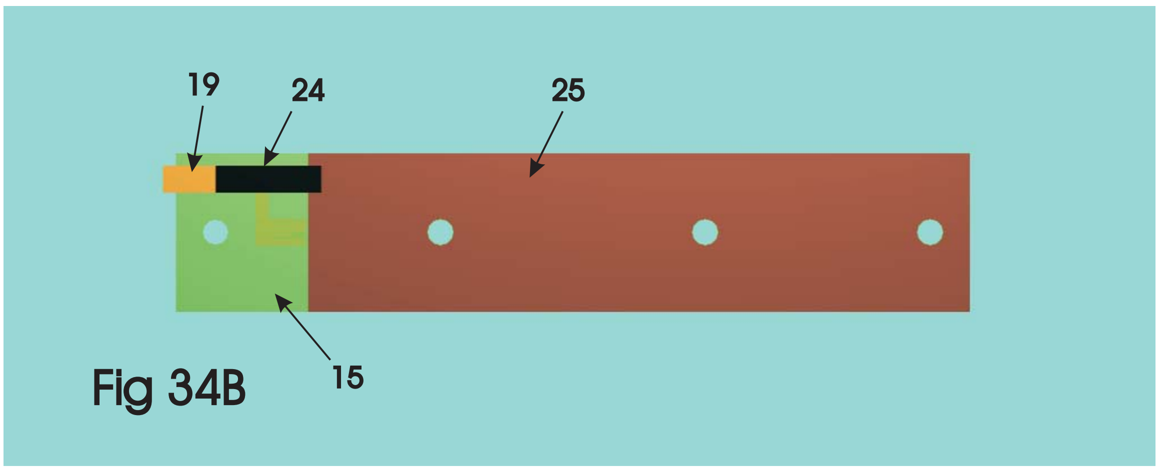


Fig 34B

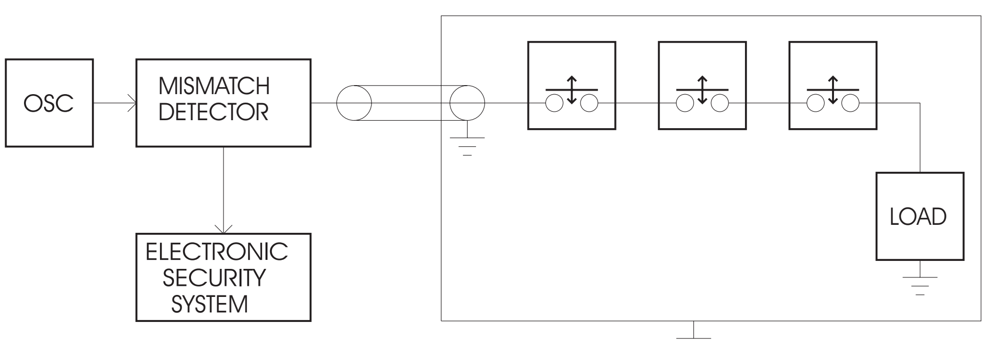


Fig 35

may be a VSWR (voltage standing wave ratio) circuit which reads a VSWR of 1.5:1 or better when the said matched condition exists. If the transmission line is cut into or tampered with, the system will no longer be matched and will exhibit a VSWR of much greater than 1.5:1 which is communicated to the ELECTRONIC SECURITY SYSTEM as a fault. Alternatively, the combination of the oscillator and MISMATCH DETECTOR may be a network analyzer or any other suitable circuit to accomplish the afore said purpose.

Referring to Fig. 36A and 36B, a top view and a three dimensional view, respectively, of another high security switch, comprising three permanent armature magnets, elements **1**, **2**, and **3**, are shown. The permanent armature magnets are enclosed in a single integrated armature block **4** consisting of any suitable non-magnetic dielectric material or insulator such as plastic, glass, or ceramic. The actuation gap of the switch is set by the thickness of the integrated spacer **5** consisting of any suitable non-magnetic material such as plastic, glass, ceramic, or metal to which the permanent spring magnets are fastened. The magnetically soft screws, elements **7**, **8**, **9**, and **10**, extend through the printed circuit board **26**, Fig. 36A and 36B, (further shown in Fig. 37A and 37B), the armature block **4**, and the spacer **5,** and decouple the interactive fields between permanent armature magnets, elements **1**, **2**, and **3**, which eliminates the detrimental effect of said interactive fields upon switching action. The magnetically soft plate or yoke **6**, consisting of any magnetically soft material such as iron, acts as an integrated spring magnet for a more economical use of materials. A coaxial cable or transmission line **11** is shown which connects to the high security switch circuit board **26** such that the center conductor of the transmission connects to the black box **36** of the circuit board as shown in Fig. 37A, and the outer conductor or shield connects to the ground plane **38** of the circuit board as shown in Fig. 37B. This high security switch is wired, but not limited to, single pole single throw (SPST) as shown in FIG. 38. The entire assembly may be fastened together by any suitable means, and in combination with, appropriate materials may produce a hermetically sealed unit.

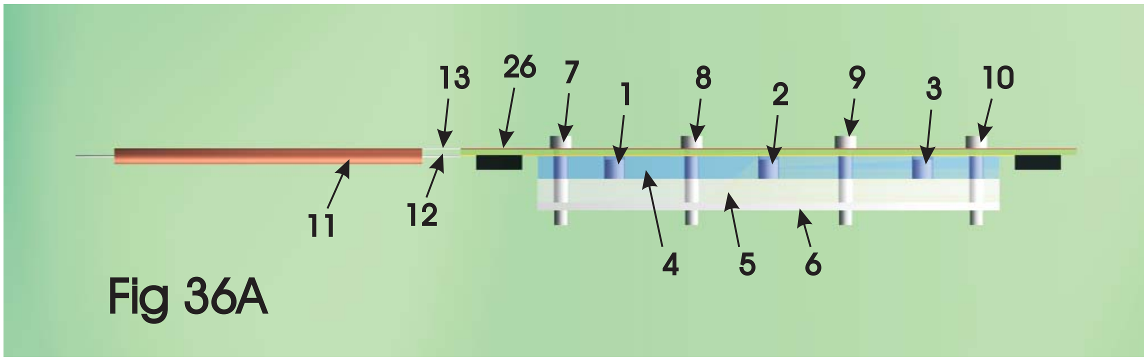


Fig 36A

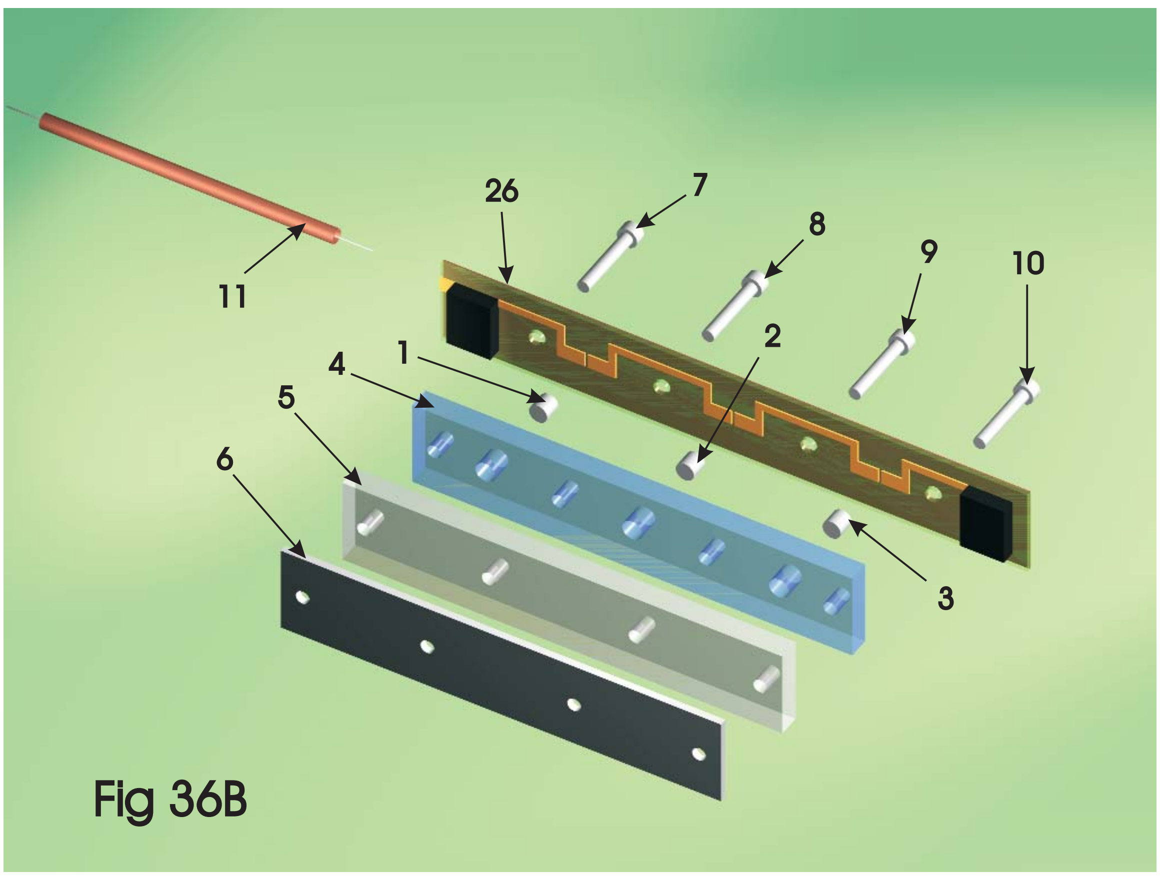


Fig 36B

Referring to Fig. 37A and 37B, a front view and a back view of the circuit board **26** in Fig. 36 respectively, the gaps in the three sets of traces between, **28** and **29**, **29** and **30**, and **30** and **31,** are shorted out by the armature magnets **1**, **2**, and **3,** respectively, when actuated by the actuator assembly. There are four holes **32**, **33**, **34**, **35** through the circuit board substrate **27**, made for example from epoxy glass, Teflon, ceramic, or other suitable material, to accommodate said magnetic field decouplers. The first black box **36** may be any electronic bandpass filter, designated as BP FILTER in Fig. 38, and the second black box **37** is the load, designated as LOAD in Fig. 38.

Referring to Fig. 38, a second preferred embodiment of the invention, comprising a radio frequency voltage controlled oscillator, designated VCO, that sends two or more distinct radio frequency signals through the MISMATCH DETECTOR and down the transmission line, is shown. At least one of said frequencies or spectral components must fall within the bandpass of the BP FILTER. The radio frequency signals travel through the Jackson Security Switch when actuated, shown by the three switch icons, and terminate in the LOAD. The electrically grounded box surrounding the switch assembly is an electrically conductive housing grounded to the transmission line's outer conductor. When the oscillator, MISMATCH DETECTOR, transmission line, BP FILTER, Jackson Security Switch, and LOAD are substantially matched, there will be minimal reflection of the radio frequency signal which is passed by the BP FILTER and no match at the other frequency or frequencies. The MISMATCH DETECTOR may be a VSWR (voltage standing wave ratio) circuit which reads a VSWR of 1.5:1 or better for said matched signal and much greater that 1.5:1 for all other frequencies. If the transmission line is cut into or tampered with, the system will no longer be matched and will exhibit a VSWR of much greater than 1.5:1 at the bandpass radio frequency, and will be communicated to the ELECTRONIC SECURITY SYSTEM as a fault. If the security switch is cut from the cable and a dummy resistive matched load is connected thereto, all radio frequencies will be matched which is also communicated to the ELECTRONIC SECURITY SYSTEM as a fault. Alternatively, the combination of the VCO and MISMATCH DETECTOR may be a network analyzer or any other suitable circuit to accomplish the afore said purpose.

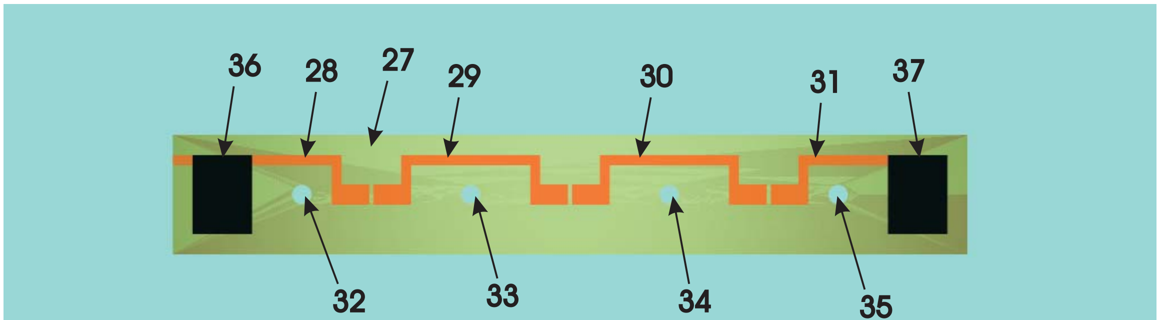


Fig 37A

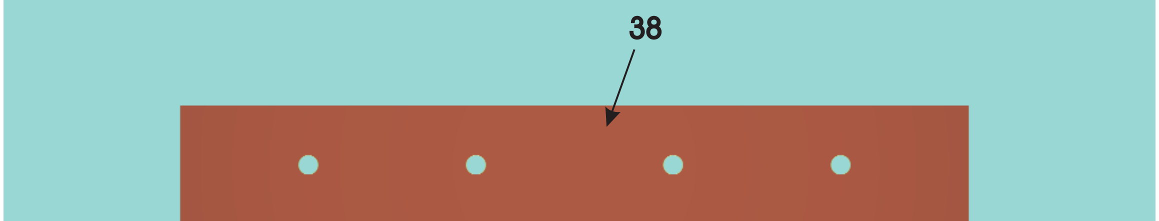


Fig 37B

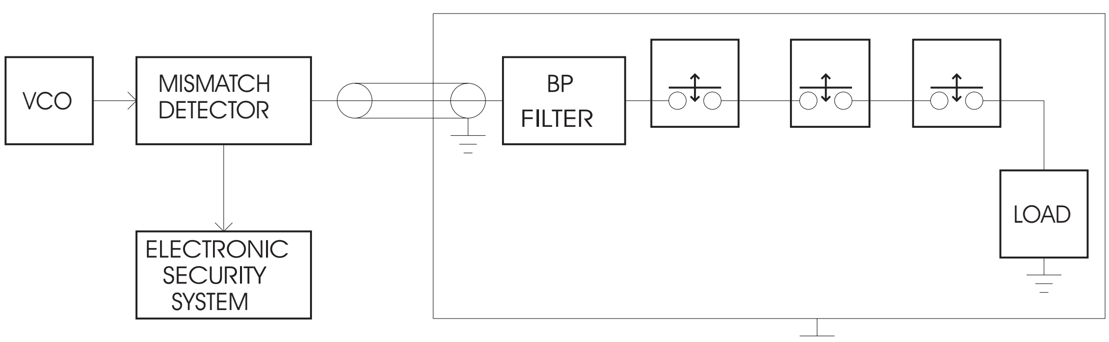


Fig 38

Referring to Fig. 39A and 39B, a top view and a three dimensional view, respectively, of another high security switch comprising three permanent armature magnets, elements **1**, **2**, and **3**, are shown. The permanent armature magnets are enclosed in a single integrated armature block **4** consisting of any suitable non-magnetic dielectric material or insulator such as plastic, glass, or ceramic. The actuation gap of the switch is set by the thickness of the integrated spacer **5** consisting of any suitable non-magnetic material such as plastic, glass, ceramic, or metal to which the permanent spring magnets are fastened. The magnetically soft screws, elements **7**, **8**, **9**, and **10**, extend through the printed circuit board **39**, as further defined in FIG. 40, the armature block **4**, and the spacer **5** and decouple the interactive fields between the permanent armature magnets, elements **1**, **2**, and **3**, which eliminates the detrimental effect of said interactive fields upon switching action. The magnetically soft plate or yoke **6**, consisting of any magnetically soft material such as iron, acts as an integrated spring magnet for a more economical use of materials. A coaxial cable or transmission line **11** is shown which connects to the high security switch circuit board **39** such that the center conductor of the transmission connects to the black box **49** of the circuit board as shown in Fig. 40A, and the outer conductor or shield connects to the ground plane **52** of the circuit board as shown in Fig. 40B. This high security switch is wired, but not limited to, single pole single throw (SPST) as shown in FIG. 41. The entire assembly may be fastened together by suitable means and in combination with appropriate materials may produce a hermetically sealed unit.

Referring to Fig. 40A and 40B, a front view and a back view of the circuit board **39** in Fig. 39A and 39B, respectively, the gaps in the three set of traces between, **41** and **42**, **42** and **43**, and **43** and **44,** are shorted out by the armature magnets **1**, **2**, and **3,** respectively, when actuated by the actuator assembly. There are four holes through the circuit board substrate **40**, made for example from epoxy glass, Teflon, ceramic, or other suitable material, to accommodate said magnetic field decouplers. The first black box **49** consists of the decoupling elements a capacitor, C2, and an RF choke, L2. The capacitor, C2, decouples direct current voltage from the Jackson Security Switch and passes radio frequency signals. The RF choke, L2,

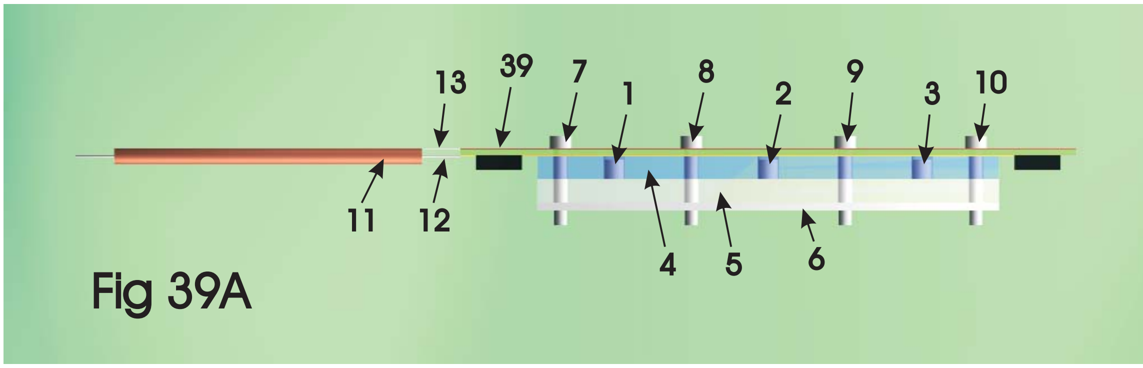


Fig 39A

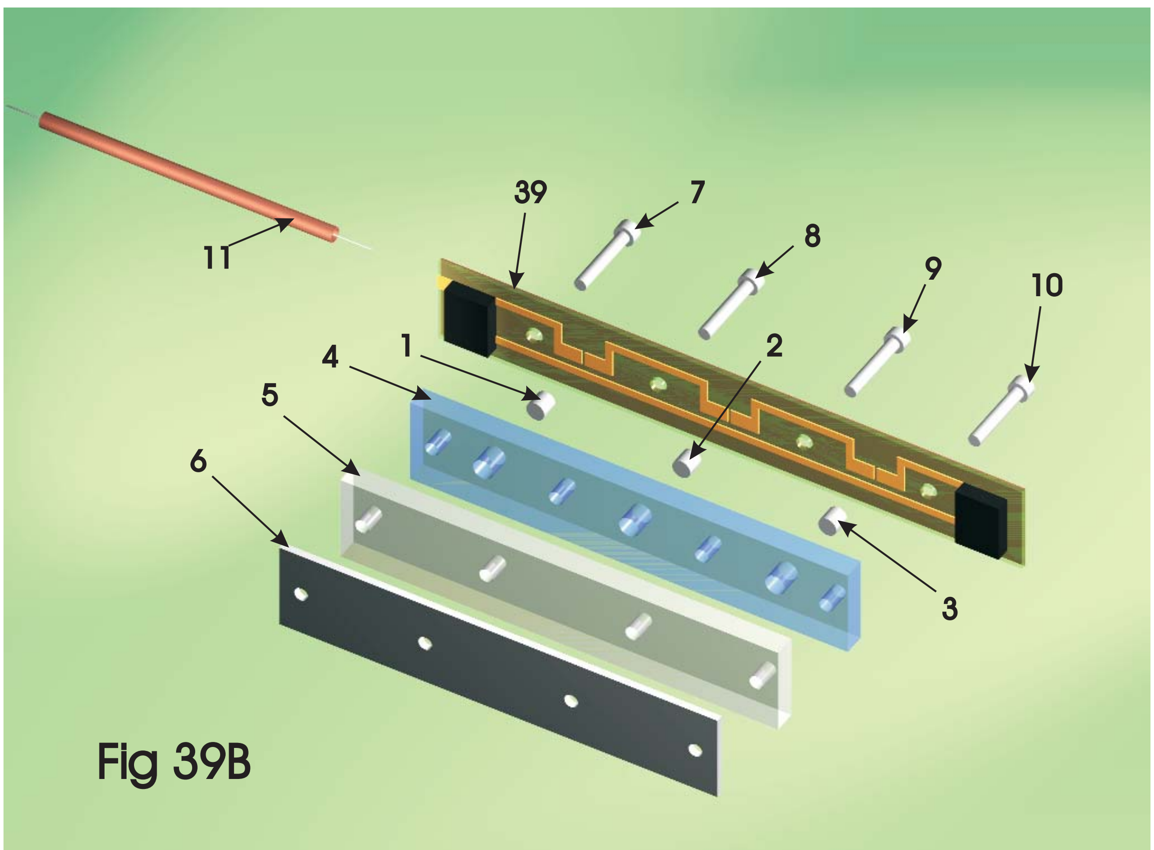


Fig 39B

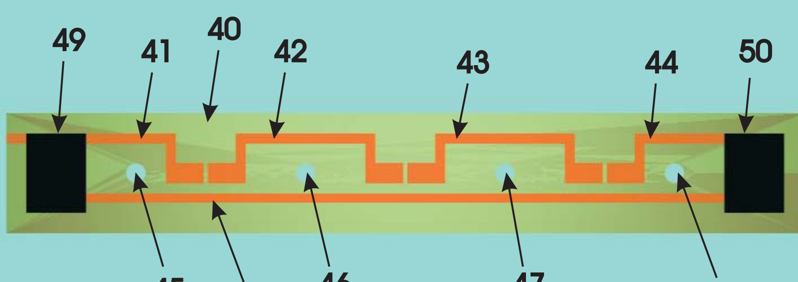


Fig 40A

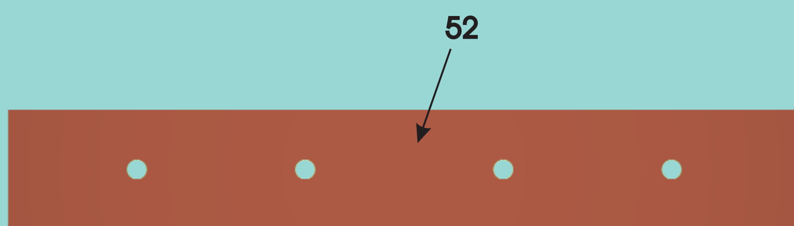


Fig 40B

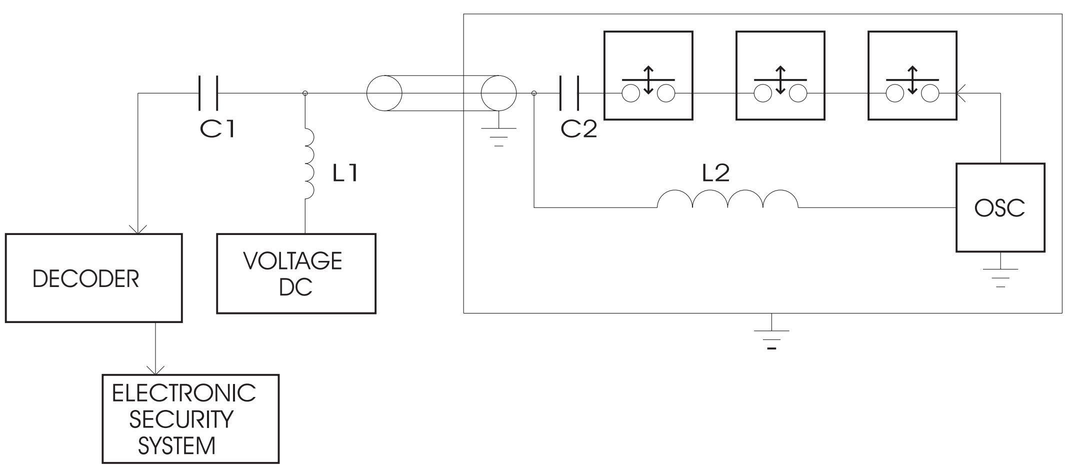
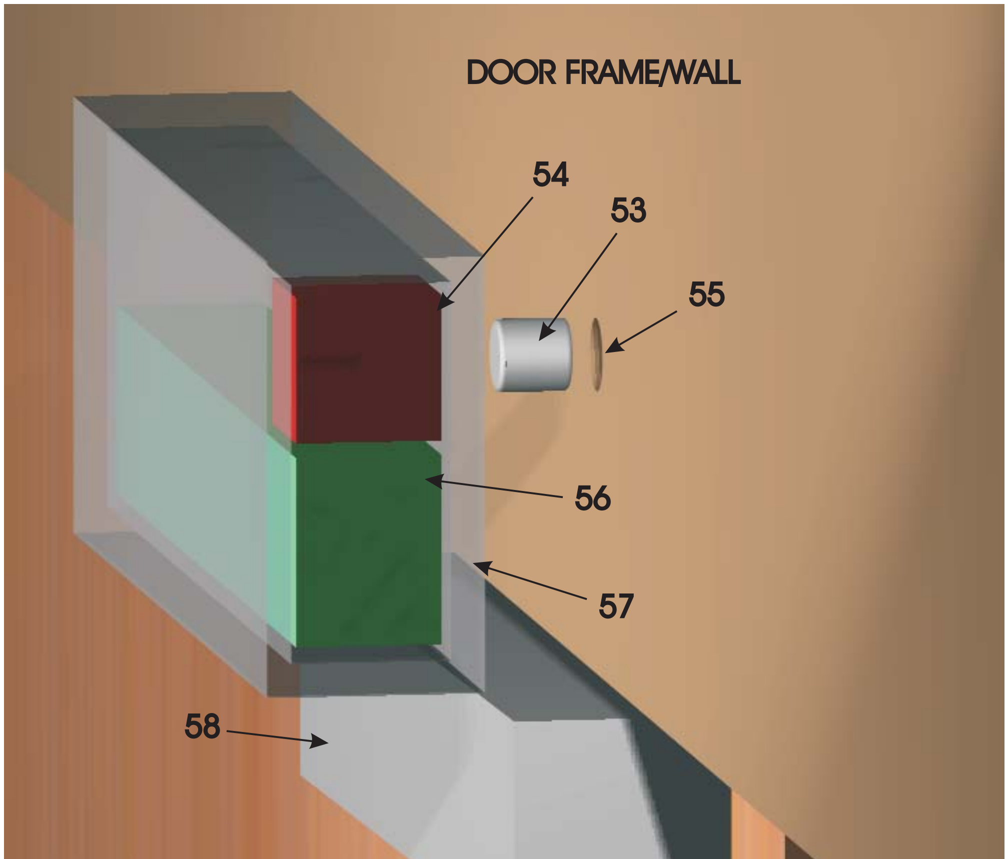


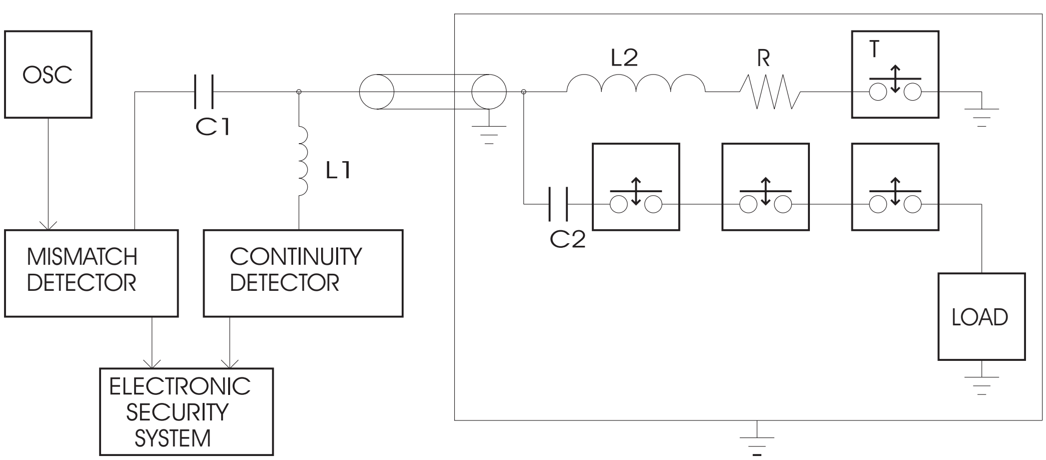
Fig 41

decouples radio frequencies from the oscillator power input and passes direct current voltage. The second black box **50** is a radio frequency oscillator, designated as OSC in Fig. 41.

Referring to Fig. 41, which is another preferred embodiment of the invention in which a direct current voltage, designated VOLTAGE DC, is passed through an RF choke, L1, down the transmission line and through the RF choke, L2, into the power input of the oscillator. The oscillator may originate single or multiple radio frequencies that are sent through the Jackson Security Switch, back down the transmission line, through the decoupling capacitor, C1, and into the decoder. Multiple frequencies can be used as device identification. The electrically grounded box surrounding the switch assembly is an electrically conductive housing grounded to the transmission line's outer conductor. If the transmission line is cut into or tampered with, the system will no longer be matched and will exhibit a VSWR of much greater than 1.5:1 which is communicated to the ELECTRONIC SECURITY SYSTEM by the DECODER as a fault. If the security switch is cut from the cable and a dummy resistive matched load is connected thereto, the coded radio frequencies will not be present, which is also communicated to the ELECTRONIC SECURITY SYSTEM as a fault.

Referring to FIG. 42, a three dimensional view of a Jackson Security Switch in combination with a tamper switch (Jackson Switch) and its actuator and the mounting method are shown, for which two possible electrical schematic variations are shown in FIG. 43 and FIG. 44. The Jackson Security Switch **56** and the tamper switch **54** are shown enclosed in a housing **57** that is pulled away from the door frame or wall revealing the tamper switch actuator magnet **53** and its mounting hole **55** in the door frame or wall. The Jackson Security Switch actuator **58** is shown in its appropriate position attached to the partially open door. If the switch housing is removed from the door frame or wall a fault condition results when the tamper switch opens.


DOOR FRAME/WALL
54
53
55
56
57
58
DOOR
Fig 42


OSC
C1
L1
L2
R
T
C2
MISMATCH DETECTOR
CONTINUITY DETECTOR
ELECTRONIC SECURITY SYSTEM
LOAD
Fig 43

Referring to Fig. 43, another preferred embodiment of the invention, comprising a radio frequency oscillator, designated OSC, which sends a radio frequency signal through the MISMATCH DETECTOR, through the decoupling capacitor, C1, and down the transmission line, is shown. The radio frequency signal continues to travel through the decoupling capacitor, C2, and through the Jackson Security Switch when actuated, shown by the three switch icons, and terminates in the LOAD. The electrically grounded box surrounding the switch assembly is an electrically conductive housing grounded to the transmission line's outer conductor. When the oscillator, MISMATCH DETECTOR, transmission line, Jackson Security Switch, and LOAD are substantially matched, there will be minimal reflection of the radio frequency signal. The MISMATCH DETECTOR may be a VSWR (voltage standing wave ratio) circuit which reads a VSWR of 1.5:1 or better when said matched condition exists. If the transmission line is cut into or tampered with, the system will no longer be matched and will exhibit a VSWR of much greater than 1.5:1, which is communicated to the ELECTRONIC SECURITY SYSTEM as a fault. Alternatively, the combination of the oscillator and MISMATCH DETECTOR may be a network analyzer or any other suitable circuit to accomplish the aforesaid purpose.

A direct current voltage is generated by the CONTINUITY DETECTOR and sent through the decoupling RF choke, L1, down the transmission line, through the decoupling RF choke, L2, and the resistor, R, terminating with the tamper switch (Jackson Switch) marked T in the icon. Interruption of the direct current is detected by the CONTINUITY DETECTOR when the tamper switch opens, which is communicated to the ELECTRONIC SECURITY SYSTEM as a fault.

Referring to Fig. 44, another preferred embodiment of the invention, comprising a radio frequency oscillator, designated OSC, which sends a radio frequency signal through the MISMATCH DETECTOR, through the decoupling capacitor, C1, and down the transmission line, is shown. The radio frequency signal continues to travel through the decoupling capacitor, C2, and through the tamper switch (Jackson Switch) when actuated, shown by the icon marked T, and terminates in the LOAD. The electrically

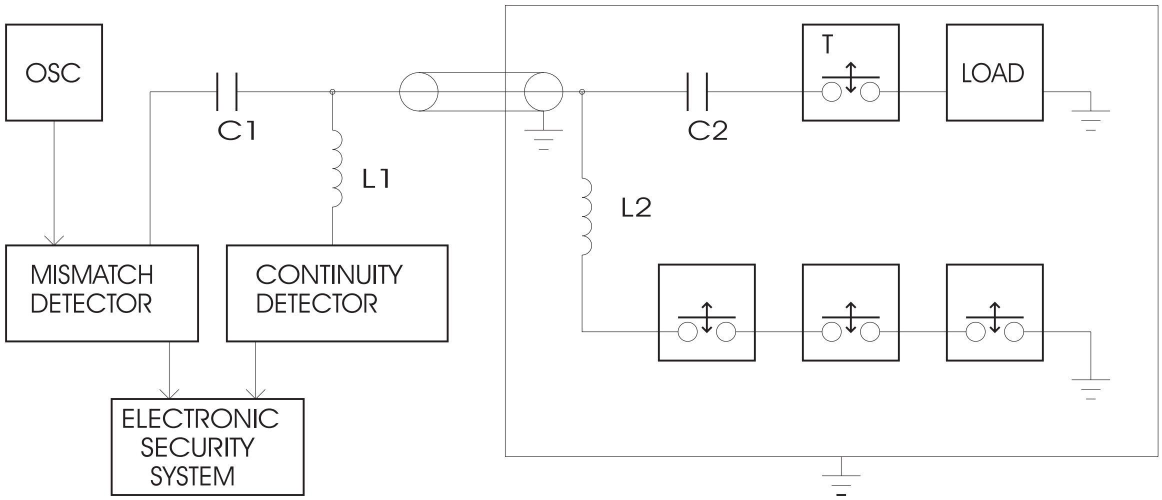

OSC
C1
L1
T
LOAD
C2
L2
MISMATCH DETECTOR
CONTINUITY DETECTOR
ELECTRONIC SECURITY SYSTEM

Fig 44

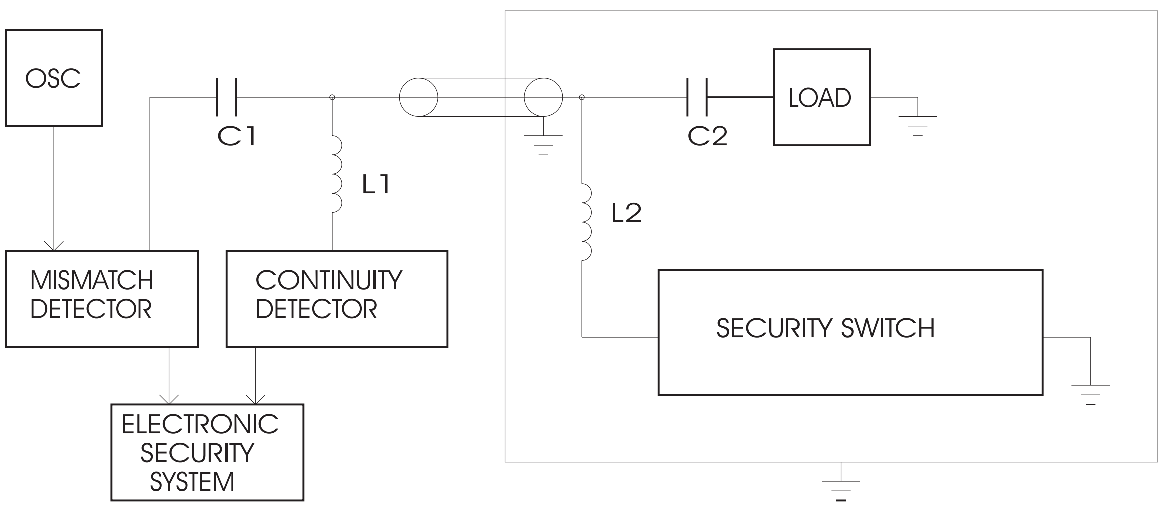

OSC
C1
L1
LOAD
C2
L2
MISMATCH DETECTOR
CONTINUITY DETECTOR
SECURITY SWITCH
ELECTRONIC SECURITY SYSTEM

Fig 45

grounded box surrounding the switch assembly is an electrically conductive housing grounded to the transmission line's outer conductor. When the oscillator, MISMATCH DETECTOR, transmission line, Jackson Switch, and LOAD are substantially matched, there will be minimal reflection of the radio frequency signal. The MISMATCH DETECTOR may be a VSWR (voltage standing wave ratio) circuit which reads a VSWR of 1.5:1 or better when the said matched condition exists. If the transmission line is cut into or tampered with, the system will no longer be matched and will exhibit a VSWR of much greater than 1.5:1, which is communicated to the ELECTRONIC SECURITY SYSTEM as a fault. Alternatively, the combination of the oscillator and MISMATCH DETECTOR may be a network analyzer or any other suitable circuit to accomplish the afore said purpose.

A direct current voltage is generated by the CONTINUITY DETECTOR and sent through the decoupling RF choke, L1, down the transmission line, through the decoupling RF choke, L2, terminating with the Jackson Security Switch shown symbolically by the three switch icons. Interruption of the direct current is detected by the CONTINUITY DETECTOR when the security switch opens which is communicated to the ELECTRONIC SECURITY SYSTEM as a fault.

Referring to Fig. 45, another preferred embodiment of the invention comprising a radio frequency oscillator, designated OSC, which sends a radio frequency signal through the MISMATCH DETECTOR, through the decoupling capacitor, C1, and down the transmission line, is shown. The radio frequency signal continues to travel through the decoupling capacitor, C2, and terminates in the LOAD. The electrically grounded box surrounding the switch assembly is an electrically conductive housing grounded to the transmission line outer conductor. When the oscillator, MISMATCH DETECTOR, transmission line, and LOAD are substantially matched, there will be minimal reflection of the radio frequency signal. The MISMATCH DETECTOR may be a VSWR (voltage standing wave ratio) circuit which reads a VSWR of 1.5:1 or better when said matched condition exists. If the transmission line is cut into or tampered with, the system will no longer be matched and will exhibit a VSWR of much greater than 1.5:1

which is communicated to the ELECTRONIC SECURITY SYSTEM as a fault. Alternatively, the combination of the oscillator and MISMATCH DETECTOR may be a network analyzer or any other suitable circuit to accomplish the afore said purpose.

A direct current voltage is generated by the CONTINUITY DETECTOR and sent through the decoupling RF choke, L1, down the transmission line, through the decoupling RF choke, L2, terminating with any security switch shown symbolically as SECURITY SWITCH. Interruption of the direct current is detected by the CONTINUITY DETECTOR when the switch opens and is communicated to the ELECTRONIC SECURITY SYSTEM as a fault.

Referring to Fig. 46, another preferred embodiment of the invention, in which a direct current voltage, designated VOLTAGE DC, is passed through an RF choke, L1, down the transmission line and through the RF choke, L2, into the power input of the oscillator designated OSC, as shown. The oscillator may generate single or multiple radio frequencies that are sent through the decoupling capacitor, C2, and back down the transmission line, through the decoupling capacitor, C1, and into the decoder. Multiple frequencies can be used as device identification. If the transmission line is cut into or tampered with, the system will no longer be matched and will exhibit a VSWR of much greater than 1.5:1, which is communicated to the ELECTRONIC SECURITY SYSTEM by the DECODER as a fault. The electrically grounded box, surrounding the switch assembly, is an electrically conductive housing which is grounded to the transmission line outer conductor. If the security switch is cut from the cable and a dummy resistive matched load is connected thereto, the coded radio frequencies will not be present, which is also communicated to the ELECTRONIC SECURITY SYSTEM as a fault.

The direct current voltage generated by the CONTINUITY DETECTOR and sent through the decoupling RF choke, L1, down the transmission line, through the decoupling RF choke, L2, also terminates with any security switch shown symbolically as SECURITY SWITCH. Interruption of the direct current is detected

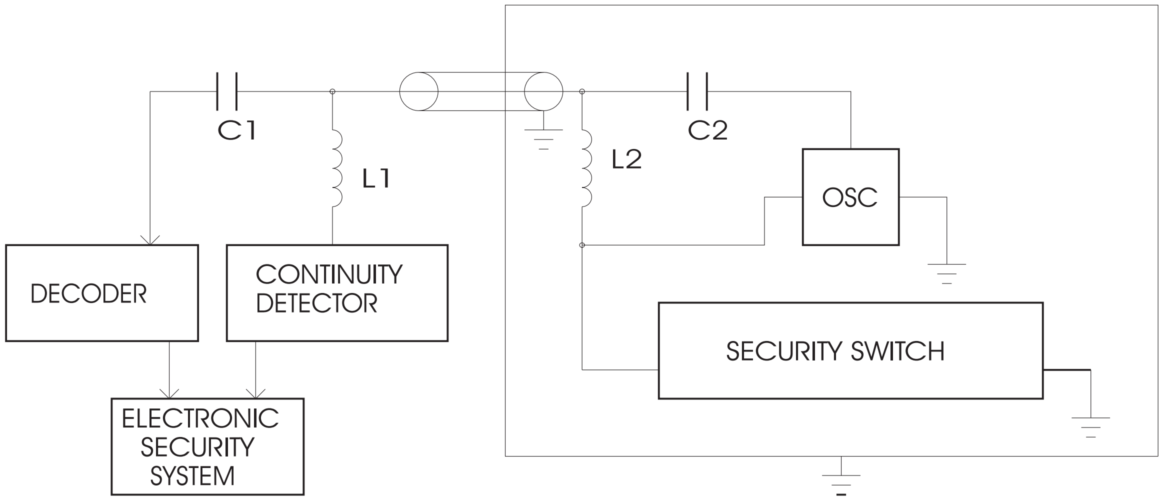

C1
L1
L2
C2
OSC
DECODER
CONTINUITY
DETECTOR
SECURITY SWITCH
ELECTRONIC
SECURITY
SYSTEM

Fig 46

by the CONTINUITY DETECTOR when the switch opens and is communicated to the ELECTRONIC SECURITY SYSTEM as a fault.

3.3 FEATURES

The Jackson High Security Switch and Radio Frequency System features may be tailored to meet commercial to full military environmental and electrical specification requirements. The switch, which may be constructed from as few as six parts, is ideal for "no adjustment" fully automated assembly. Enormous design flexibility allows creative system construction with the highest reliability and security.

3.3.1 RELIABILITY

The reliability of the Jackson High Security Switch is equivalent to or exceeds the reliability of electrical contact state of the art in conventional relays. Shock and vibration will not alter the magnetic operation, pull in sensitivity, or any other operational characteristic. Electrical arcing is partially suppressed by the intense magnetic fields present in the electrical contact gap. This reduces the load requirement on auxiliary arc suppressing circuitry when handling inductive loads. There is no sensitivity to the inrush currents associated with light bulbs or capacitive circuits.

3.3.2 ELECTRICAL POWER

The electrical power handling capability of the Jackson High Security Switch is equivalent to the electrical contact state of the art electrical power handling capability. The Jackson High Security Switch energy density can be easily shown to be thirty (30) times that of a reed switch. There are no limitations on use of materials for conductors or lead wires. Hermetic sealing of the switch depends upon the application and the electrical contact material chosen.

The Jackson High Security Switch in combination with the Radio Frequency System can handle alternating or direct current (AC or DC power) and low level radio signals, including video signals, simultaneously.

When designed within standard guidelines, the complete system does not generate electro-magnetic radiation. The system, although continuously active, does not betray its presence or radio frequency spectral signature.

3.3.3 SIZE

The Jackson High Security Switch has no size limitations. Preproduction runs show ±10% variations in pull in sensitivity with "no" adjustments. Consequently, down sizing presents no adjustment problems in production. There is no dependence on glass envelopes to create an economical hermetic seal.

The transmission lines connecting the Jackson High Security Switch to the Radio Frequency monitoring equipment are two wire coaxial conductors. They do not occupy any more space than existing multi-wire systems. Armored cable or metal conduits are no longer required because tampering with the transmission lines is immediately detectable.

3.3.4 DEFEAT MECHANISMS

A novel variation of the Jackson High Security Switch actuator assembly [44] has removed the "slide by" defeat mechanism characteristic of the prior art as shown in Figure 7. The device is "not" sensitive to its own actuator or any special lock picking actuator. Therefore, the Jackson High Security Switch is undefeatable. When used in combination with the Radio Frequency system, the entire system is undefeatable. The Jackson High Security Switch Radio Frequency System is analogous to a biological nervous system - one small cut anywhere, and pain is immediately experienced in the central nervous system.

3.3.5 SHIELDING

The Jackson High Security Switch technologies are sufficiently directional that magnetic shielding is not necessary nor is it desirable. The cost of expensive magnetic shielding has been eliminated. The entire mechanism can be injection molded or made from injection molded parts without compromising security. The Jackson High Security Switch used as a retro-fit in an existing security system can be potted in aluminum tubes without injury for aesthetic purposes or if it adds to a general feeling of increased security. When used in a Radio Frequency System, it must be sealed in a non-magnetic metal can that is grounded to the outer conductor of the coaxial cable to prevent electro-magnetic radiation from betraying its presence or spectral signature.

3.4 SUMMARY

The Jackson high security switch is based upon a novel switch technology that replaces the reed switch. It constitutes a combination of permanent magnets arranged and decoupled so that balanced or coded actuation is achieved providing superior performance over the traditional reed switch high security switches. Any combination of electrical contacts is possible in these designs. Consequently, the necessity for a hermetic seal has been removed. These switches are substantially immune to electro-magnetic interference and mechanical vibration or shock resulting in potentially false alarm free environments. Magnetic shields as well as all known defeat mechanisms have been eliminated. The huge increase in reliability alone makes the prior art obsolete.

It is obvious from the detailed descriptions that many variations are possible. The sizes, configurations, and operating characteristics may be tailored for any particular situation. Further, fabrication and automated production from few parts is very simple and does not require any adjustments of any kind to obtain consistent performance characteristics. Designs may vary from fully automated mass produced components to full military and space oriented systems.

The Radio Frequency System provides many alternatives to the traditional system. Armored cables and electrical conduits have been replaced with a two conductor radio frequency transmission line. Although any high security switch may be incorporated into this system, the Jackson high security switch is much more reliable and can handle radio frequency signals directly which further increases the possibilities. This system will detect any attempt to alter the cables connecting the security switch to the central monitoring system providing a level of security unachievable with the prior art.

4. CONCLUSION

The existing security switch technology based upon reed switches exhibits all of the characteristics of the reed switch including its limitations. Reed switch construction is restricted to combinations of certain materials to achieve functionality. The choice of materials selection usually constitutes a compromise between magnetic behaviors and electrical contact performance with magnetic behaviors being favored. Consequently, the base material for the electrical contacts is most often an iron alloy. This further necessitates the use of hermetically sealed glass envelopes with inert gases in the envelope to prevent immediate degradation of the electrical contacts. So, given the state of the art in glass reed switch technology, these components are mechanically fragile, have electrical contacts that are inferior to available alternatives in other applications, and are highly sensitive to extraneous electro-magnetic fields and mechanical shock. They are prone to damage in manufacturing operations that incorporate them. And, their operating characteristics are highly variable from switch to switch which makes consistent performance in any assembly that uses them impossible without extremely sensitive adjustments in production.

High security switches that use combinations of reed switches suffer further from their omni-directional activation characteristics. It has been shown that these switches are easily defeatable, even with magnetic shielding. To complicate matters further, achieving any functionality in the final product requires extremely sensitive adjustments in production. Additionally, current production processing techniques often violate the hermetic seal and alter the magnetic properties of the materials which further degrades the reliability of the device. The existence of frequent catestrophic failures and false alarms should not be surprising.

The Jackson high security switch, a triple balanced third generation high security switch, represents the most advanced, coded, passive, magnetic proximity security device known. It's novel switching action replaces reed switch technology of the prior art and consequently renders all reed switch based security devices obsolete. The inherent directional magnetic behavior of the Jackson high security switch outperforms co-planar devices that are achieved by the use of magnetic shields. Further, this novel technology removes size and power constraints imposed by reed switch limitations. Defeat mechanisms that can be used against all other existing high security switches are ineffective against the Jackson high security switch. One variation of this switch has been installed in the laboratory and connected to an electronic monitoring system for testing and security purposes.

When using the undefeatable Jackson high security switch retro-fitted into existing systems, the weakest link is the cables between the switch and the central monitoring system. The Radio Frequency System eliminates any threat to the connection between the Jackson High Security Switch and the central monitoring system while offering a cost effective alternative to multiple conductor armored cable and electrical conduits.

The Jackson high security switch is simple to construct from very few parts and is ideal for "no adjustment" automated production. And, the Radio Frequency System is more cost effective than the prior art. This complete cost-effective system offers rugged, trouble free, undetectable operation with the maximum possible security.

5. BIBLIOGRAPHY

BOOKS

[1] Bozorth, Richard M., "Ferromagnetism", Van Nostrand, 1951.

[2] Holm, Helm, "Electrical Contacts - Theory and Application 4th Edition", Springer- Verlag, 1967

[3] Jones, F. Llewellyn, "The Physics of Electrical Contacts", Oxford University Press, 1957.

[4] Magnecraft Electric, Co., "Designers' Handbook & Catalog of Reed and Mercury Wetted Contact Relays", Magnecraft Electric, Co., 1966.

[5] Moskowitz, Lester R., "Permanent Magnet Design and Application Handbook", Cahners Books International, Inc., 1926.

[6] Peek, R.L., Wagar, H.N., "Switching Relay Design", Van Nostrand, 1955.

[7] Vines, R.F., "The Platinum Metals and Their Alloys", The International Nickel Company, Inc., 1941.

JOURNALS

[8] An Analysis of Life Limiting Factors for Medium Sized Reed Switches, S. Mitan, G. Kamoshita, K. Oho, T. Tanii, Relay Conference, 1968.

[9] Analysis of a Magnetic Field and Operational Parameters of a Two-Reeds Relay, V.N. Shoffa, B. Miedzinski, Relay Conference, 1994.

[10] Contact Resistance As It Affects Dry Circuit Relays, J.W. Scannel, Relay Conference, 1958.

[11] Dry Reed Contacts Operated by Permanent Magnets, H.J. Wierzba, International Conference on Electrical Contacts, Electro-Mechanical Components and Their Applications, Japan, 1986.

[12] The Effect of Cracks in Glass-to-Metal Seals on Performance of Hermetically Sealed Relays, H.N. Staats, Relay Conference, 1954.

[13] Factors Determining the Selection of Gases for Hermetically Sealed Relays, W. Brown, Relay Conference, 1956.

[14] Fallacies in Life Testing, F.F. Yanikoski, Relay Conference, 1962.

[15] High Reliability Reed Switches with Rhodium Plated Contacts, T. Yokogawa, C. Kawagita, Relay Conference, 1973.

[16] Life Expectancy of a Form C Dry Reed Switch as a Function of its Operating Environment, W.J.Fontana, Relay Conference, 1966.

[17] A Mathematical Analysis of the Magnet Reed Switch, A.R. Le Blanc, Relay Conference, 1964.

[18] Predicting Early Failure of Dry Reed Contacts, E.F. Sutherland, Relay Conference, 1977.

[19] Predicting Gas Mixture Changes Due to Leakage in Hermetically Sealed Units, J.L. Hartley, C.Z. Stuart, Relay Conference, 1977.

[20] A Realistic and Dynamic Life Test for Reed Switches, D.H. Fox, Relay Conference, 1968.

[21] Relay Contact Load Switching Design Guidelines, Michael Baldwin, Relay Conference, 1994.

[22] Selection of Magnetic Materials for a Design of Hard Reed Switches, J. Cornu, O. Demeyer, Relay Conference, 1975.

[23] A Study on the Soft Sticking of Rhodium Contact Reed Switches, T. Yokokawa, T. Yano, C. Kawakita, K. Hinohar, A. Nagai, Relay Conference, 1986.

CATALOGS & BROCHURES

[24] Reed Switches, Aleph International, CA.

[25] Reed Switches, 0991/01 F 3 E, Gunther, Germany.

[26] Reed Switches and Proximity Sensors, Hermetic Switch, Inc., OK.

[27] Magnetic Shielding , 811217, Eagle Magnetic Company, IN.

[28] Magnetic Shielding Lab Kit with AC Probe, LK-2F, Magnetic Shield Corp. IL., 1989.

U.S. Patents

[29] 2,912,540 (Sawicki)

[30] 3,305,805 (Tann)

[31] 3,974,469 (Nicholls)

[32] 4,210,889 (Holce)

[32] 4,339,747 (Maybee)

[33] 4,544,903 (Grant)

[34] 4,945,340 (Brill)

[35] 5,057,807 (Longly et al.)

[36] 5,128,641 (Krizman et al.)

[37] 5,233,322 (Posey)

[38] 5,233,323 (Burkett el al.)

[39] 5,293,523 (Posey)

[40] "High Security Balanced Type, Magnetically Actuated Proximity Switch System", (Jackson et al.), assigned to Securitron Magnalock Corp. on 02/02/94

[41] "Magnetic Proximity Switch", patent pending, (Jackson)

[42] "Balanced-Type Magnetically-Actuated Proximity Switch System", patent pending, (Jackson)

[43] "Balanced Type Magnetically Actuated Proximity Switch and Radio Frequency Monitoring System", patent pending, (Jackson)

[44] "Slide-By Anti-Defeat Mechanism", patent pending, (Jackson)