# 21st CENTURY SECURITY

## Understanding

## High Security Contacts

WHITE PAPER

It is apparent that many older specifications for government and military security contacts were based around the misconception that Balanced Magnetic Switches (BMS) or Triple balanced reed switches provide the highest possible security.

While it is true that BMS / Triple balanced reed devices do provide "better" security than standard door contacts, it has been demonstrated for years that these too are easily disarmed using the placement of simple tamper magnets. In addition, reed switch technology is extremely prone to permanent contact welding due to power surges (lightning, stun guns, etc.).

Steps to correct these vulnerabilities were addressed in the in the early 2000's when the Army's Technical Support Working Group (TSWG), Sandia Labs, and Underwriter's Laboratories (UL) came together to create specifications for security devices that met specific performance criteria rather than settling for off the shelf products that manufacturers claimed to be "high security" devices, because they used balanced magnetic reed switches.

The result was the publication in 2007 of the 9th edition of the UL634 Standard for Connectors and Switches used with Burglar Alarm Systems, which addressed improved performance by creating two distinct Levels for high security contacts. Specifics for these Levels are included in the attachments, but the condensed explanation is as follows:

> All existing UL listed BMS/Triple Balanced reed devices, that had previously been recognized as high security, but were known to be vulnerable to magnetic tamper by someone with access to the device (i.e. from the inside) were listed as LEVEL 1 high security devices.

- Originally these previously listed devices were "grandfathered" by UL to Level 1.
- Subsequent re-testing by UL of many of these devices to the new Level 1 test criteria has resulted in the de-rating of these old devices – they no longer meet Level 1 criteria for High Security Contacts (see attachment 3).
- A new, higher level standard for devices that could resist internal magnetic tamper, and meet other higher security performance criteria were listed as LEVEL 2 High Security Contacts.

In 2010 the Government's Intelligence Community through the Office of the Director of National Intelligence (ODNI) updated its standards for high security contacts for sensitive secure areas via publication of the ICD 705. It should be noted that the ICD language does not reference BMS or Triple reed devices, but rather requires High Security Switches (HSS) that meet specific performance requirements, rather than devices that are just marketed as "high security".

It would be prudent for all military branches and government agencies to follow the lead of the DNI / ICD 705 and define and specify the requirements for high security switches based on the UL634 Level 2 criteria for any areas where high security devices would be used.

The supporting documentation provides the important details regarding the classification of high security contacts when used with IDS and ACS systems.

**ATTACHMENTS:**

1. Understanding UL634 & Level 1 - Level 2
2. UL634 – ICD 705 – White Paper
3. UL Letter, de-rating Level 1 concealed devices

# Underwriters Laboratories Testing Criteria UL-634 Connectors and Switches for Use with Burglar-Alarm Systems

There are 40 standards that must be met to achieve listing to UL-634, which covers basic contacts, including Balanced Magnetic Switches, defined by UL-634 Section 3, Glossary, as: 3.2 BALANCED MAGNETIC SWITCH (BMS) - A switch that is constructed in such a manner or that includes additional components that increase resistance to magnetic, electrical and mechanical tampering or defeat.

It should be noted that while devices made with BMS provide "higher security" than standard contacts, they are not considered HIGH SECURITY CONTACTS until criteria listed below is met.

In addition, **there are 8 testing criteria that must be met to achieve UL-634 Level 1 HIGH SECURITY.** They are included in these categories:

- Mechanical Protection Against Tampering
- Electrical Protection Against Tampering
- Compromise Test – Mechanical and Mercury Switches
- Compromise Test – Magnetic Switches
- Compromise Test – Enclosures
- Detection Test – Measures Activation Distances

Beyond the UL-634 Level 1 listing, **there are 8 additional requirements that must be met to achieve UL-634 Level 2 HIGH SECURITY:**

- Made with Balanced Magnetic Switches (BMS)
- Nuisance Alarm Test
- Cover or Enclosure Tamper Test (When Applicable)
- Magnet Assembly Cover Removal Alarm Test (When Applicable)
- Switch Assembly Removal Tamper Test (When Applicable)
- Foreign Magnetic Field Tamper Alarm Test
- Foreign Magnetic Field Compromise Tests
- Extended Endurance Test

# HIGH SECURITY STANDARD

# UL634

Level 1

vs.

Level 2

**ICD** Replaces **DCID**

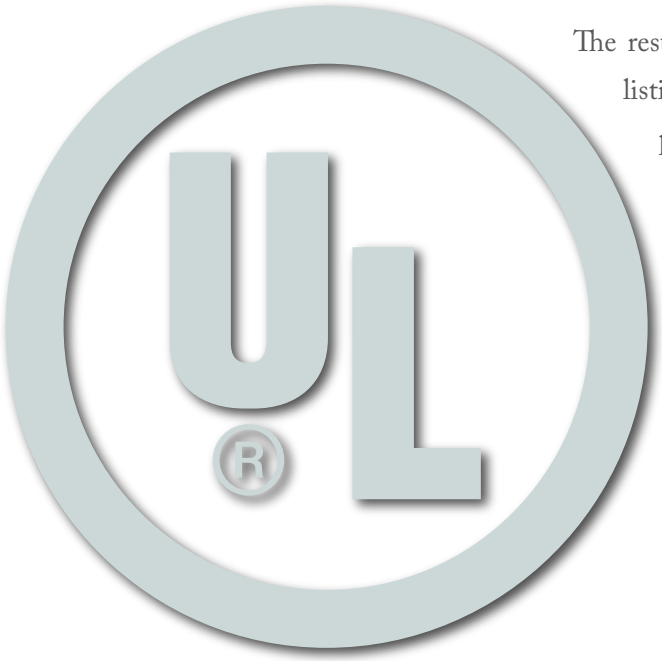
WHITE PAPER

## BACKGROUND

The UL 634 Standard for Connectors and Switches for use with Burglar Alarm Systems sets the UL requirements for all magnetic sensors (commonly called contacts – installed on doors, windows, cabinets, safes, etc.) used for all alarm systems - from the lower end residential devices to the High Security devices used in government and other high level intrusion detection systems (IDS).

Prior to 2007 the highest level of device recognized by UL634 was the BMS (Balanced Magnetic Switch) high security contact. The test for magnetic defeat and tamper established by UL to rate devices to this level was outdated, and many devices were designed to circumvent this test, and thus able to acquire the High Security listing. It was widely known in the government security community that these BMS High Security contacts were easily defeated – even though they met the UL requirements.

Funded by the Army's Technical Support Working Group (TSWG) through Sandia Labs, the government wanted to develop security devices that met performance standards. Sandia enlisted Underwriters Laboratories to be the standards facilitator and together they developed new test parameters to better define performance for these devices to be used on these high level secure installations. The 9th edition of UL634 was published in October of 2007.



The result was that the old UL634 BMS High Security contact listing was re-named Level 1 High Security. Some test procedures were changed or improved, but all devices that were previously listed to that level, were "grandfathered" in as Level 1 devices.

A new Level 2 High Security Standard was established that was based on much more stringent performance criteria that had been developed through the Sandia / UL collaboration.

## FUNCTIONALITY:

### Level 1 Vulnerabilities:

1. Magnetic tamper and defeat. During the workday, when IDS systems are off, virtually undetectable defeat magnets can be placed on the Level 1 devices that render it useless when the IDS system is activated, allowing an intruder undetected access to the area.

2. Magnetic defeat of removal tamper circuits. All Level 1 and Level 2 devices require a 24 hour supervised circuit to detect removal of the device from its location. This tamper circuit on Level 1 devices is easily defeated with a magnet, which allows undetected removal from its location allowing undetected access to the secure location at any time.

3. Nuisance / false alarms. Level 1 devices use a decades old glass switch technology called reed switches. When these devices are installed, they require a minimum separation distance between the sensor portion (typically installed on a door frame) and the actuation magnet (installed on the door). Often, over time, doors will sag (typically unevenly), which can cause the magnet portion on the door to move up toward the sensor, violating the minimum separation distance, and causing the sensor to false alarm

4. Reed switches (used in Level 1 devices) are prone to permanent contact welding from power surges such as lightning, or activation with a stun gun. When reed switch contacts weld in this closed position, they are failed SECURE, which means the device is always in the secure state, and an alarm would not be sent when the door opened – even with the Intrusion Detection System armed.

5. Level 1 devices are tested to a life cycle of 100,000 operations.

### Level 2 Solutions:

1. More stringent performance parameters to eliminate magnetic tamper and defeat of the devices. Eliminating the potential of defeat by an insider or the "inside job". Test parameters have been significantly enhanced.

2. Tighter performance and protection tolerances for 24 hour removal tamper circuits.

3. Tighter performance and installation requirements to help eliminate false or nuisance alarms.

4. Most Level 2 devices use the newer Magnasphere switch technology which is designed to be resistant to contact welding, magnetic tamper / defeat, and breakage. Any potential failure of this technology will be in the fail SAFE mode, which does not render the device inoperable.

5. Level 2 devices are tested to a life cycle of 1M operations.

## ICD 705-1 REPLACES DCID 6/9 FOR SCIF IDS INSTALLATIONS

### BACKGROUND

With the creation of the Office of the Director of National Intelligence (ODNI), which consolidated the intelligence agencies, the old DCID (Director of Central Intelligence Directives) were re-written as ICD / ICS (Intelligence Community Directive / Standard) regulations.

In May of 2010, the last of these ICD's, ICD 705 for Sensitive Compartmented Information Facilities (SCIF) was signed by then Director of National Intelligence (DNI), Dennis Blair. Approximately one year later, on May 5th, 2011, the Technical Specifications (IC Tech Spec for ICD / ICS 705) were released, and Version 1.3 was published on September 10, 2015 amended to read:

### ICD TECH SPEC FOR ICD / ICS DOCUMENT LANGUAGE

Chapter 7. **Intrusion Detection Systems (IDS)**

A.2 (d) Areas of a SCIF through which reasonable access could be gained, including walls common to areas not protected at the SCI level, shall be protected by IDS consisting of UL 639 listed motion sensors and **UL 634 listed High Security Switches (HSS) that meet UL Level II requirements** and/or other AO-approved equivalent sensors. **All new SCIF accreditations shall use UL Level II HSS.** Existing UL Level I HSS are authorized **until major IDS modifications/upgrades are made.**

December 20, 2013

Rick Kirschman
Magnasphere Corp.
N14 W23777 Stone Ridge Dr.
Suite 160
Waukesha, WI 53188

Subject: UL Listed Level 1 & Level 2 High Security Devices

Dear Mr. Kirschman:

All High Security devices (Level 1 or Level 2) Listed to the UL Standard 634 are required to be equipped with a tamper circuit that supervises removal. This requirement applies to both surface-mount and recessed/concealed mount contacts. This requirement is stated in Section 51 of UL 634:

> 51 Electrical Protection Against Tampering
>
> 51.1 A high security switch shall be provided with an electrical circuit that supervises removal of the switch from the mounting surface or removal of the enclosure (if any). See the Test for Electrical Protection Against Tampering, Section 56.
>
> *Exception: The switch need not be electrically supervised if repositioning the switch mounting or removing the switch enclosure does not result in a risk of the switch being compromised (for example, exposure of current-carrying parts of field-wiring leads).*

There is currently a review in process to confirm that UL Listed devices without this provision be brought into compliance to earn or to maintain Listing to UL 634 High Security. Any UL Listed devices that do not comply with the above requirement will continue to be UL Listed but will not eligible for the Level 1 rating.

If you have any questions regarding this issue, please contact the undersigned.

Sincerely,

Senior Market Surveillance Engineer
Market Surveillance Dept.
UL LLC
Ph: 847-664-2350
Email: Lee.R.Cetrone@us.ul.com

Security, Principal Engineer
Product Safety
UL LLC
Ph: 847-664-3238
Email: Louis.Chavez@ul.com