ENHANCING SMART HOME SECURITY WITH 3D MAGNETIC SENSORS

By Joseph Hollins
Allegro MicroSystems

INTRODUCTION

Household electronic systems with higher levels of integration are quickly being adopted to enable an improved user experience. As consumers find new ways to outfit their living spaces with simple-to-use smart home and Internet of Things (IoT) products, they may be unaware of certain vulnerabilities and security features commonly found in these and other electronic devices.

Many household security and access control devices [1] such as electronic locks, cameras, intrusion sensors, garage door openers, control hubs and panels contain increasing levels of smart electronics that enable automated access to permitted users while restricting access to intruders. The fusion of these electromechanical devices with a security-based role poses a risk that should be addressed by using magnetic tamper detection sensors.

What Is The Vulnerability Mechanism?

One of the many methods employed in tampering with electronics is using strong magnets to disrupt the device's ability to operate in a closed loop. As these magnets are brought in close proximity to the device, they begin to expose the smart device's internal electronics to high magnetic fields. Security and access control personal electronics are commonly equipped with magnetically sensitive components but are seldom designed to compensate or ignore the influence of an external "stray" magnetic field.

[1] The security principle discussed here applies directly to other critical-function electronic systems as well, such as medical instruments and utility meters.

Hall-effect and magnetoresistive (xMR) magnetic sensors, along with various other integrated circuits commonly used in security electronics, are susceptible to saturation and malfunction. During these conditions, the disruption to the magnetically sensitive components may prevent the system from knowing critical information such as how much power is flowing through it or the exact status of a mechanical position. In the smart lock example, shown in Figure 1, the tamper mechanism may inadvertently trigger an unlock condition due to a stray magnetic field.

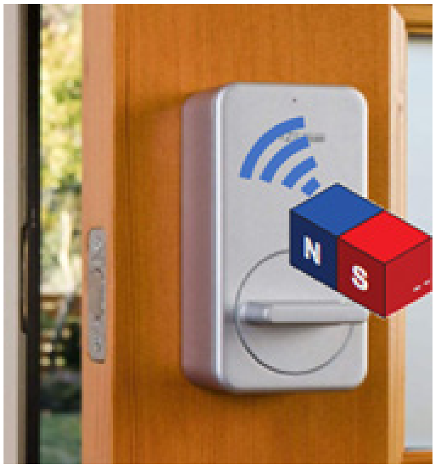

Figure 1: Smart Lock Vulnerability Mechanism

What Is a Stray Field?

An often uncharacterizable external magnetic field is referred to as stray magnetic field. This is an applied magnetic field that is either intentional – the method of a nefarious tamper perpetrator – or unintentional – such as interference from a large current or magnetic source nearby. Sources such as a permanent magnet or electromagnet can vary in polarity, frequency, direction, and strength. Permanent magnets used for tampering are typically very strong, may be relatively large and heavy, and can be purchased online or salvaged from discarded electronics and computers.

How Secure Are Smart Locks?

A smart lock is a prime example of a smart home security product. According to Littelfuse Inc. (Littelfuse, n.d.), 7 million smart lock units shipped worldwide in 2019, and annual shipments are anticipated to rise to 23 million units within 5 years. With the growing adoption rate of smart locks and other personal electronic security and access control solutions, manufacturers in parallel must address hardware and software security susceptibilities.

The internal electronics materializing these access control systems use voltage and current references which are often sensitive to external magnetic fields. An interference event of this nature can potentially cause the system to become blinded or tricked into performing an operation when it should remain secured. In the case of a smart lock, a very high magnetic field applied may allow an intruder to enter a secure space if proper tamper safeguards are not implemented as part of the product design.

Criteria for Successful Tamper Detection

Although it may be challenging for manufacturers to prevent magnetic tampering at the point of use, it is quite possible to detect attempts at tampering. In the very least a log can be recorded, or a remedial action can be taken such as an alert, disabling critical parts of the system or notifying an administrator. Multiple organizations worldwide are working toward defining smart home access control system regulations that include the requirement for smart home and personal electronic security peripherals to detect and log attempted tampering.

To be effective, a magnetic sensor used to detect tampering must have the following features:

- High Sensitivity: Even though the magnet applied to the outside of the system may be strong, the magnetic field strength of a magnet decays exponentially as you move farther away; the field strength at the internal location of the sensor may be much lower than the field at the surface of the magnet (see Figure 2); certain metallic components used in the system may distort the magnetic field, resulting in "shadows" or "holes" in the sensor's detection region if the sensitivity is not high enough.

- High Dynamic Range: Some magnetic sensing technologies have upper bounds on the magnetic field strength that is allowed to be applied to it, and exceeding those limits can cause permanent damage. Unlike xMR, Hall-effect technology has no upper limit on applied magnet fields.

- Omnipolar Sensitivity: It is unlikely that the perpetrators of a tampering attempt will pay much attention to which pole of the magnet is applied to the system's case, or they may simply try all options to find one that is effective; the sensor should be capable of detecting north and south polarity magnetic fields and be insensitive to the magnet's pole orientations.

- Omnidirectional Sensitivity: Many legacy magnetic sensors are only sensitive to fields in a single direction or plane; since the external magnet may be applied in any orientation to any exposed point on the component's surface (front face, top, bottom, back or sides), the sensor should be equally sensitive in all three directions (X, Y, and Z). Examples of true 3DMAG™ Hall-effect magnetic sensor devices include the ALS31300 low-power 3D linear sensor and the ALS31313 low power 3D linear sensor from Allegro MicroSystems.

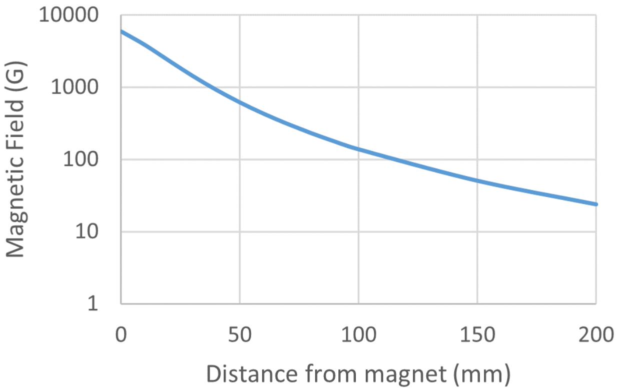

Figure 2: Magnetic Field vs. Distance from Magnetic Surface (mm) for 50 mm^3 N45 Neodymium Magnet

Tamper Prevention

There are options to choose from as discussed earlier when addressing a detected tamper event. Tamper prevention can only be realized at the point of the end equipment's use, by having the proper safeguards in place like detection, lockout and notification, or a form of compensation when continuing with operation.

For instance, the system may intentionally disable itself for a short period of time if a very strong stray field tamper attempt is detected, or it may log and disregard the stray field if it is considered weak enough. Ultimately a tamper prevention mechanism is used when critical sensitive electronics are present and their malfunction could cause a hazard, or in the case of the smart lock – a security breach.

Two different 3D magnetic sensor types from Allegro are compared in Table 1. The A1266 3D micropower Hall switch and the ALS31300 3D Hall linear sensor both meet the criteria discussed in the previous section for successful tamper proximity detection solutions, and each offer a unique approach to tamper mitigation and prevention.

	A1266	ALS31300
Package	SOT23	DFN
Footprint	2.9 mm × 3mm	3 mm × 3 mm
Operation Mode	Threshold Switch	Calibrated Linear
Sensing Mechanism	3D Hall-effect	3D Hall-effect
Output Protocol	Open Drain	I^2C
Sensing Range	±40 G (4mT)	±500 G, ±1000 G, and ±2000 G (±50 mT, ±100 mT, and ±200 mT)
Features	Individual X/Y/Z Outputs, Single OR Output of X/Y/Z, Fixed Low Power Cycling	EEPROM (W/ Customer Space), Adjustable Low Power Cycling, Interrupt Pin, Adjustable Interrupt Settings, Temperature Sensor

Table 1: Comparison of Hall-effect switch and linear sensor features and capabilities

To learn more about the Allegro 3DMAG™ family of products and to explore available design resources, visit allegromicro.com/3DMAG.

CONCLUSION

Magnetic tamper detection is a critical function required for the confident adoption of smart home security and access control devices by consumers. This feature prevents malfunctions and enables a system-level response to a hazardous magnetic field exposure event, enhancing the overall security and performance of these and other electronic devices.

Magnetic sensor ICs such as the A1266 3D Hall switch and the ALS31300 3D Hall linear are able to detect magnetic tampering over a large region from a footprint smaller than 9 mm^2. The 3DMAG™ sensor solutions from Allegro ensure highly accurate, versatile sensing design by using the fewest number of ICs to achieve high reliability tamper detection.

Be sure to read Allegro's companion application note, discussing the technical advantages of true 3D sensors for use in tamper detection, *3D Hall-Effect Sensors Reduce the Cost and Complexity of Magnetic Tamper Detection for Smart Home Systems*.

REFERENCES

Littelfuse Inc.. 2020. “IoT Smart Locks and Access Control.” https://info.littelfuse.com/hubfs/Electronics/Documents/LFUS_BLD_IOT_Smart_Locks_Spotlight.pdf.

Allegro MicroSystems, LLC. “ALS31300 3-D Linear Hall-Effect Sensor with I^{2}C Output and Advanced Low Power Management.” Last modified October 20, 2021. https://www.allegromicro.com/-/media/files/datasheets/als31300-datasheet.ashx.

Allegro MicroSystems, LLC . n.d. “ALS31313 Automotive Grade, 3-D Linear Hall-Effect Sensor with I2C Output and Advanced Low Power Management.” Accessed November 16, 2021. https://www.allegromicro.com/en/products/sense/linear-and-angular-position/linear-position-sensor-ics/als31313.

Allegro MicroSystems, LLC. “A1266 Micropower Ultrasensitive 3D Hall-Effect Switch.” Last modified February 4, 2020. https://www.allegromicro.com/-/media/files/datasheets/a1266-datasheet.ashx

Allegro MicroSystems, LLC.“3D Hall-Effect Sensors Reduce the Cost and Complexity of Magnetic Tamper Detection for Smart Home Systems.” Last modified July 29, 2021. https://www.allegromicro.com/-/media/files/application-notes/an296223-3d-hall-tamper-detection.ashx.

Revision History

Number	Date	Description	Responsibility
–	November 16, 2021	Initial release	Joseph Hollins

The information contained in this document does not constitute any representation, warranty, assurance, guaranty, or inducement by Allegro to the customer with respect to the subject matter of this document. The information being provided does not guarantee that a process based on this information will be reliable, or that Allegro has explored all of the possible failure modes. It is the customer's responsibility to do sufficient qualification testing of the final product to insure that it is reliable and meets all design requirements.

Copies of this document are considered uncontrolled documents.

MCO-0001163
P-0173