Estimation of Cluster Sensors' Probability of Detection for Physical Protection Systems Evaluation

W. I. Zidan

Nuclear and Radiological Regulatory Authority, Nuclear Safeguards and Physical Protection Department, P.O. Box 11762, Cairo, Egypt, najzidan@yahoo.com

Abstract

Cluster sensors are vital components of physical protection systems, and are used extensively to detect intrusion. It is essential to insure that a particular sensor will meet the design criteria of the physical protection system. In this paper, performance evaluation and operational procedures of Glass Breakage (GB) and Open Door (OD) sensors are presented and discussed. Several intrusion tests were carried out inside the detection areas of the sensors in order to evaluate their performance during a particular intrusion process. Experimental results are presented here. The probabilities of detection for both GB and OD sensors were estimated.

Keywords: *Physical Protection Systems, Intrusion Detection, Cluster Sensors, Security Sensors, Intrusion Detection.*

1. Introduction

Nuclear security focuses on prevention and detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities. It aims to protect persons, property, society, and the environment from harmful consequences of a nuclear security event.[1] One of the main pillars of nuclear security is physical protection which is an integral part of nuclear security. Physical protection systems (PPSs) for nuclear facilities are necessary to achieve the desired protection, and they

are based on a combination of personnel, hardware, procedures, and facility design.[2] All PPSs must be subjected to vulnerability assessments or tests, to judge how effective they will be in warding off attacks from adversaries.

This paper is concerned with protection of nuclear facilities using hardware, specifically electronic hardware. Because the evaluation of the performance of equipment used in PPS is an important element in designing and maintaining PPS, we applied a method for evaluating the performance of intrusion detection systems (IDSs). The IDSs used in this study were Glass Breakage (GB) and Open Door (OD) sensors. This evaluation can be used to compare the performance of intrusion detectors, and to evaluate performance goals for them. The operational procedures and probability of detection (PD) for the tested sensors were investigated and are discussed in this paper.

2. Physical Protection Systems

A PPS is an integrated set of physical protection measures intended to prevent the completion of a malicious act.[3] The purpose of a PPS is to prevent an adversary from successful completion of a malevolent action against a facility or its personnel. The primary PPS functions are detection, delay, and response. For a system to be effective, there must be awareness that there is an attack underway (detection), and slowing of adversary progress to the targets (delay), thus allowing the response force enough time to interrupt or stop the adversary (response).[4] PPSs at different sites are seldom identical because of the differences in facilities, targets, and threats. The basic design for PPSs is quite well established, though considerable engineering and design fine-tuning is usually required for each site.[5]

The physical protection sub-system first encountered by adversaries in any facility should serve as a substantive deterrent by presenting a difficult obstacle to penetrate. The obstacle usually involves non-electronic systems such as steel gates, but in recent times, there has been an increased use of electrified fences and armored floodlights as the first line of defense.[6] In designing PPSs, several criteria have to be taken into

consideration; this includes such things as the characteristics of PPSs, functional conformity, vulnerability assessments, and the nature of adversaries.[7]

Detection—which is the discovery of an intrusive action at any point in the protection system—is usually reported by an intrusion sensor and announced through the alarm communication sub-system. The intrusion alarm must then be followed by an assessment; if appropriate, the response force will then be notified. The detection of an intrusion or an attempted intrusion into a protected area is one of the basic functions of a PPS. It is important to make this detection as early as possible after the start of the intrusive action in order to provide the maximum time for assessment and response. Maximum delay usually requires detection as far from the target as possible.[5]

3. Intrusion Detection Systems

Attempts to breach a protected area have to be detected by a PPS, and this is mostly achieved by the use of electronic sensors. These are typically devices that detect changes in a physical quantity (heat, motion, vibration) and convert them to electrical signals. These signals are then made readily available for indication and/or annunciation at the central alarm station (CAS) via transmission sub-systems. Providing a supplementary means of indication at the point of detection may also serve as a deterrent.

IDSs are usually considered as the second line of defense; they can protect with high accuracy against internal attacks. This mechanism allows detecting abnormal or suspicious activities on the relevant target, and triggers an alarm when intrusion occurs. Many studies in the application of the IDS technology in *ad hoc* networks have been done, in contrast to wireless sensor networks where few studies have been undertaken. The reason is probably the limited energy and computing storage capacity for wireless sensor networks.[8] In practice, IDSs are needed to detect both known security exploits and novel attacks that have yet to be experienced.[9] Reliable intrusion sensors are used extensively as single units and in multiple-unit networks in detection systems of all sizes. Intrusion detectors are often used in overlapping arrays for mutual protection

and reliability.[9] IDSs consist of exterior and interior intrusion sensors, video alarm systems, entry control, and alarm communication system all working together. Interior sensors are those used inside buildings and usually involving the use of a different set of sensors from exterior sensors, which are used in an outdoor environment and are usually mounted on the walls, windows, or doors of a building.[10]

Interior intrusion sensors, when integrated into a system using administrative procedures, access control, and material monitoring, can be highly effective against insider threats. Using interior intrusion sensors that can be correctly placed, installed, maintained, and tested, an alarm can be generated with the occurrence of unauthorized acts or the unauthorized presence of insiders as well as outsiders. There are three main applications for interior sensors [4]:

1- Boundary penetration sensors for detecting penetration of the boundary of an interior area.
2- Interior motion sensors for detecting the motion of an intruder within a confined interior area.
3- Proximity sensors for detecting an intruder in the area immediately adjacent to an object in an interior area, or when the intruder touches the object.

Boundary penetration sensors include vibration, electromechanical, infrasonic, capacitance, proximity, and passive sonic sensors. "Cluster sensors"—distributed arrays of networked sensors—are widely used in PPSs and installed in huge numbers inside nuclear facilities to detect intrusion. They may include Glass Breakage sensors (GBs), Balanced Magnetic Switches (BMSs), or Open Door Sensors (ODs).

A GB sensor is any device intended to detect the breakage of protected glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. GB sensors use microphone transducers to detect the glass breakage and listen for frequencies associated with breaking glass. A processor filters out all unwanted frequencies and only allows the frequencies at certain ranges to be analyzed. The processor compares the frequency received to those registered as being associated with glass breakage. If the received signal matches frequencies characteristic of breaking glass, then an alarm will be generated. The sensor element is often equipped with a

light emitting diode (LED) activation indicator. The LED should be kept lit until it is turned off.[11]

OD sensors are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other structural devices that can be opened to gain entry. When using a BMS, a magnetic unit is mounted on the movable part on the door or window adjacent to switch unit. Typically, the BMS has a three-position reed switch and an additional magnet (called the bias magnet) located adjacent to the switch. When the door is closed, the reed switch is held in the balanced or center position by interacting magnetic fields. If the door is opened or an external magnet is brought near the sensor in an attempt to defeat it, the switch becomes unbalanced and generates an alarm. See Figure 1. A BMS must be mounted so that the magnet receives maximum movement when the door or window is opened. BMSs provide higher level of protection for doors and windows than either magnetically or mechanically activated contacts or tilt switches.[4]

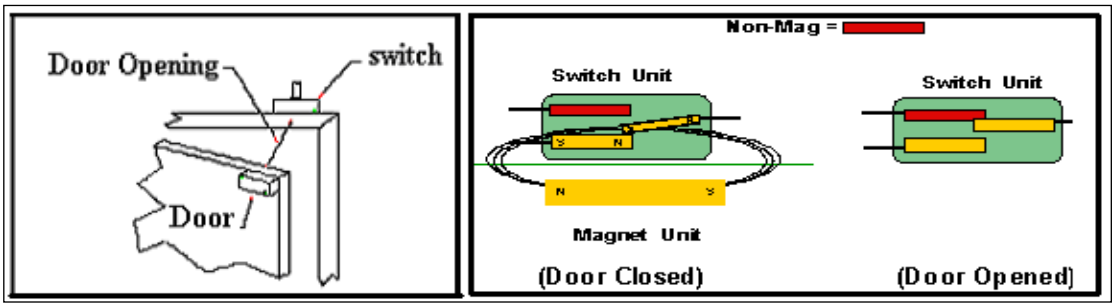

Figure 1 - Schematic diagram of the Balanced Magnetic Switch (BMS).

The intrusion detection evaluation problem and its solution usually affect the choice of the suitable intrusion detection system for a particular environment, depending on several factors. The most basic of these factors are the false alarm rate and the detection rate.[12] IDS accuracy involves evaluating the performance of the IDS and determining the best configuration.[13] Sensor performance testing is usually performed to determine whether a particular sensor will be acceptable for a particular design. These tests permit the user to evaluate the current status of the overall PPSs. It helps to identify shadowed areas from uneven terrain that result in weak (low

detection) spots. Performing a few tests near the sensor head is usually done to determine the optimum offset.[14-15]

Intrusion sensor performance is described by three fundamental characteristics: probability of detection (PD), nuisance alarm rate, and defeat vulnerabilities.[16] An understanding of these characteristics is essential for designing and operating an effective intrusion sensor system. Thus, the present study focuses on determining the probability of detection for certain intrusion detectors in order to evaluate their performance and the appropriateness of their use in the current PPS for a nuclear facility.

4. Experimental Work

4.1. GB sensor performance measuring procedures

I determined the PD by undertaking 10 intrusion trials.[17,18] The sound created by knocking metal keys on the glass windows from outside the building was used to test the GB alarm to see if it generated an alarm or not. All trials were performed on different areas and many fields of sensors.

4.2. GB sensor technical specifications and hardware description

The following are the sensor spectificaitons. Type: VISONIC GFD-20 GLASS BREAK audio discriminator and detector; Detection range: 15 m radius adjustable; Coverage Area: up to 500 m^2; Cut out frequency: 4 kHz; Detection Current: 20 mA; Alarm period: 2-3 Sec; Power supply voltage: 9 to 16 VDC; Working ambient temperature: -20C to 60^oC.

The GB detector board was tested using the MSP430F2274 board, which is a 16-bit microcontroller (MCU). The supply voltage required for the microcontroller spans a broad range from 1.8 V to 3.6 V. The MCU is capable of operating at frequencies up to 16 MHz. The CPU has a 16-bit RISC architecture with a total of 51 instructions (27 core

and 24 emulated). It supports a single-cycle shift and single-cycle add/subtract instructions. This enables efficient multiplication in the absence of a hardware multiplier.[18] The MCU also has an internal very-low-power, low-frequency oscillator (VLO) that operates at 12 kHz at room temperature. This oscillator eliminates the need for an external onboard crystal for the operation of the device. However, an option has been provided on the board to use external crystal/resonators of up to 16 MHz. The MCU has two 16-bit timers (Timer A and Timer B), each with three capture/compare registers. An integrated 10-bit analog-to-digital converter (ADC10) supports conversion rates of up to 200 kilo samples per second (ksps). The ADC10 can be configured to work with to on-chip operational amplifiers (OA0 and OA1) for analog input signal conditioning. The memory model supports up to 32 kB of flash memory and 1 kB of RAM in addition to 256 bytes of information memory. This device comes with four 8-bit I/O ports that can be used to control external devices. The current consumption of 0.7 mA during standby mode and active mode current of just 250 mA at 1 MHz make this device an excellent choice for battery-powered applications. Figure 2 shows the setup for the Glass Breakage detector using this device. The microphone captures the analog input, and a buzzer or LED indicates detection of glass breakage. The op amps internal to the MSP430 are connected to a few external passive components as part of the design of active analog filters.

4.3. GB sensor's on-site experimental steps and evaluation procedures

1. Turn off the GB sensor power.
2. Open the front cover.
3. Use a screwdriver to short the operation mode pads on the PC board.
4. Connect an oscilloscope device to the output terminal of GB sensor.
5. Connect two digital voltmeters to the output terminal of amplifier 1 (QA1) and the output terminal of amplifier 2 (QA2).
6. Close the front cover.
7. Turn on the GB power and wait until the detector’s green LED blinks approximately once per second to indicate that it has entered operation mode.
8. Stand within 4.6 m (15 feet) of the detector.

9. Generate a flex signal by carefully striking the glass with a cushioned tool (or by vibrate a collection of metal keys. For high amplitude excitation a loud sound above 2 kHz is used. The GFD-20 responds with a burst of glass break audio or from the audio generated by the metal keys. If the detector receives both the flex and audio signals properly, its red alarm LED lights.
10. Measure the output currents at the output connection port, and record the alarms which generated as the intruder breaks the glass and high frequency sound is generated.
11. Repeat the intrusion process several times (10 trails). After each test, ensure that the GB sensor is ready, and then generate the sound. Adjust all setting after each test.
12. Record the output signals and alarms generated by AQ1, AQ2, output terminals of GB sensors and LED flashing, and then determine PD.

4.4. OD sensor performance measuring procedures

The PD was measured using at least 10 intrusion trials.[19] The intrusion process included multiple opening and closing of one selected door inside a certain nuclear facility. The OD sensor was installed at the top of the door and it depended on an open circuit during the opening process of the door, and closed circuits in case of closing of the door.

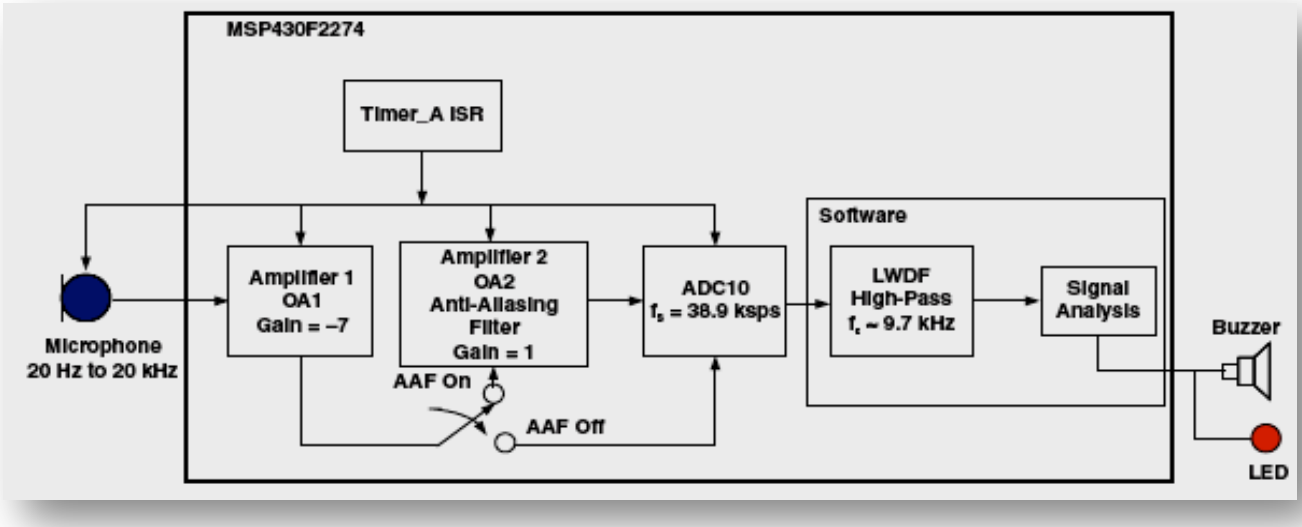

Figure 2 - Glass Breakage detector setup.

4.5. OD sensor technical specifications and hardware description

The sensor used for the OD measurements consisted of an actuating magnetic assembly and switch assembly that detects 6 mm (0.25”) of relative movement between the magnet and the switch housing. Upon detecting such movement, it transmits an alarm signal to the alarm annunciation system. The switch mechanism is of the balanced magnetic type. Each switch is provided with an overcurrent protective device, rated to limit current to 80 percent of the switch capacity. The housings of the surface mounted switches and magnets were made of nonferrous metal and are weatherproof. The housings for the recess-mounted switches and magnets need to be made of nonferrous metal.

4.6. OD sensor's on-site experimental steps and evaluation procedures

1. Ensure that the card reader, open door sensor, TL unit and electrical lock are working.
2. Turn off power to all electronic units of the door (card reader, comparator TL unit, main PAU unit). See Figure 3.
3. Open the front cover of the OD sensor.
4. Connect a digital voltmeter to the output terminal of the OD sensor
5. Adjust the voltmeter to measure the output signal.
6. Close the front cover.
7. Turn on power to the TL device and the OD, and wait.
8. Stand at the front of the door and open it rapidly
9. Measures the output volts using the digital voltmeter at the output terminals of OD sensor (at input terminals of TL unit), and record the generated alarms when the intruder opens the door.
10. Close the door again.
11. Repeat the intrusion process several times (10 trial). After each trial, ensure that the OD sensor is working properly.
12. Record the results and then determine the PD.

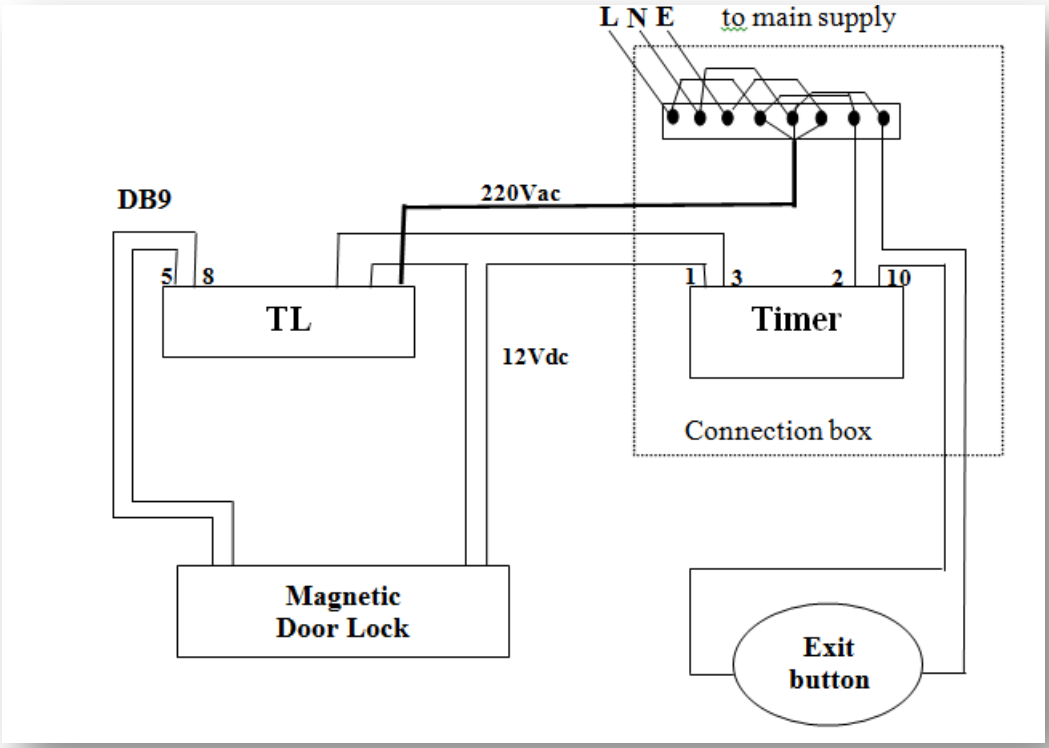

Figure 3 - Magnetic door sensor circuit diagram.

5. Results and Discussion

While designing a PPS, there a number of kinds of attacks which should be considered. These include [20]: ***False Alarming***: which refers to the situation where the adversary induces random, multiple false alarms in a system in order to undermine its usefulness and the confidence placed in it. ***Fault analysis:*** which refers to the situation where an adversary, typically exploiting technical savvy, makes a system function in an abnormal manner by altering its operational parameters, in order to obtain useful information that can be exploited, e.g., changing the ambient temperature around a sensor. ***Poke the System:*** which refers to the situation where an adversary probes the system without tampering with it and observes its responses, in order to obtain useful information, e.g., taking note of how near one can get to a motion sensor before it detects a presence.

5.1. GB sensor evaluation results

The GB detector was equipped with two LEDs **indicators**, a green event LED and a red alarm LED. When the LEDs are enabled, they light in a variety of patterns to convey the detector's operational status. Table (1) summarizes the LED messages obtained during the intrusion process.

Table 1 - GB LED output messages.

Condition	Green LED	Red LED
Normal	OFF	OFF
Normal, event detected	Flicker	OFF
Normal, break detected	OFF	ON 5 seconds
Normal, alarm latched	OFF	ON
Power up	ON (1 second)	ON (1 second)
Low voltage	Flash ON/OFF	Flash ON/OFF
Operation mode	Flash once per second	OFF
Test mode, event detected	Flicker	OFF
Test mode, alarm	Flash once per seconds	ON 5 seconds

The output results and the GB timing diagram obtained from an oscilloscope are illustrated in figure 4. It was noted that in three trials (trials 3, 4, 9), the GB sensor failed to detect the glass breakage, and the output current was 0 mA, 3 mA, 8 mA; these values were not considered as alarm values. One trial (trial 6) recorded 13 mA, which was considered as a fraction of the alarm value (20 mA). In the remaining six trials, the GB sensor succeeded in recording alarms and the output current was 20 mA. See figure 5. The tests and recorded data and all results obtained during intrusion process are shown in table 2.

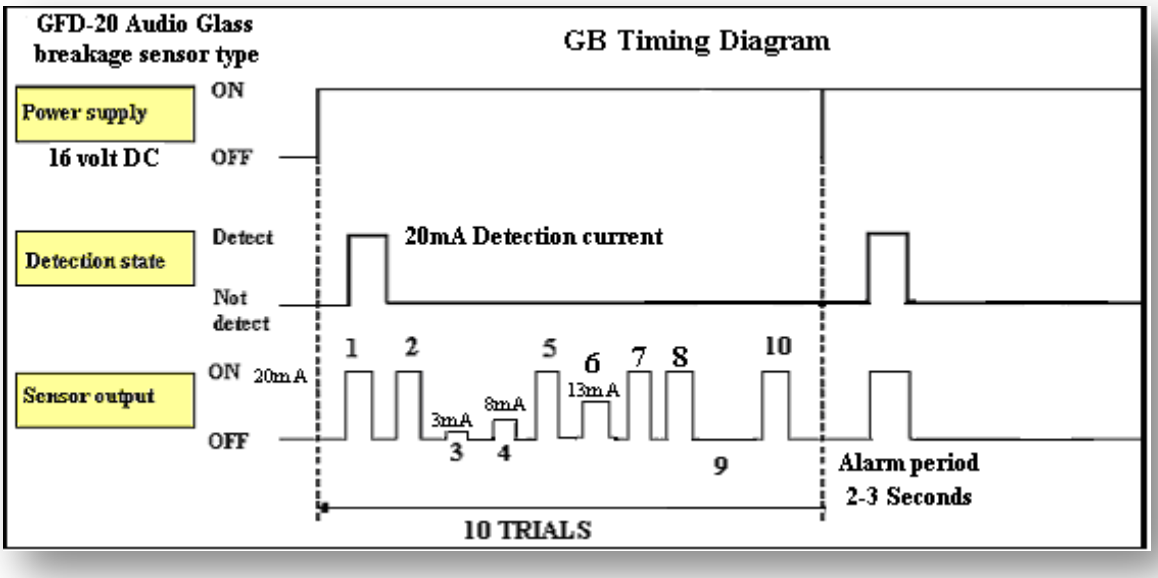

Figure 4 - GB Timing Diagram.

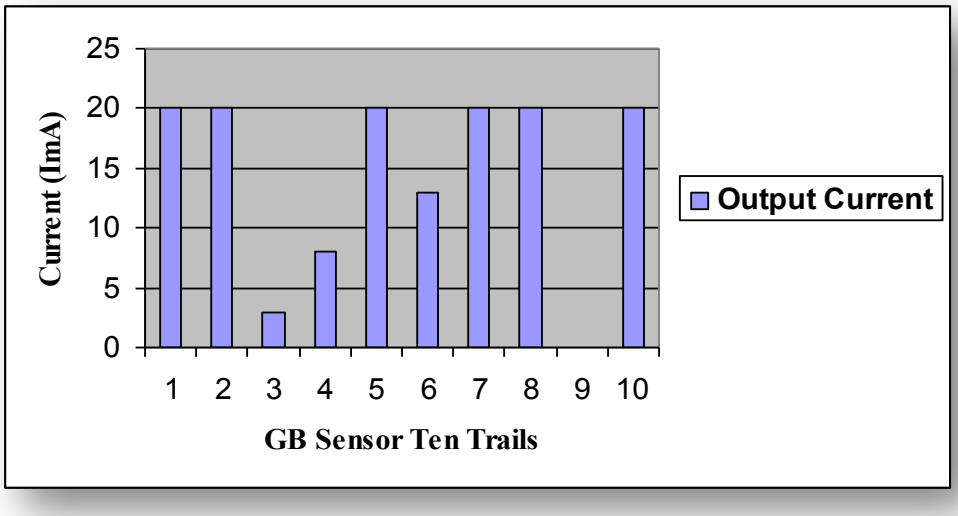

Figure 5 - GB sensor's test output current results.

5.2. OD evaluation results

Good access control systems should be capable of controlling the physical barrier at the entrance/exit point automatically by preventing access until authorization is

granted, thus contributing to the delay function. This is mostly achieved by electromechanical sub-systems such as door strikes and rotating doors.[7] The access control/anti-intruder system described in this paper uses a microcontroller chip to achieve the coordination function.

After finishing the intrusion process for the OD sensor and recording the alarms which had been generated from the OD sensor during the intrusion process, the OD sensor's test output voltage results are listed in table 2. As previously stated, 10 trials had been undertaken. In two trials (trials 4 and 8), the OD sensor failed to detect the intrusion process while it succeeded in recording alarms in the remaining 8 trials and the output voltage across the two output terminals was the nominal value.

Table 2 - Glass Breakage and Open Door sensor results.

Test Type	Sensor Type	No of Trials	Success (Alarm)	Failed (No-Alarm) & Current	Small Current "Alarm"	Probability of Detection (PD)
Intrusion Sound	Glass Breakage	10	six IO/P=20mA	three ; I1O/P=8mA I2O/P=3mA I3O/P=0mA	One trial IO/P=13mA	**65%**
Intrusion	Open Door	10	8	2	--	**80%**

6. Conclusion

The probability of detection for intrusion detection sensors is an important factor for evaluating physical protection systems. This work determined the probability of detection (PD) for Glass Breakage (GB) and Open Door (OD) cluster sensors. These are widely used in nuclear facilities. The GB and OD sensors were found to have a PD of 65%, and 80% respectively.

7. References

1. IAEA-Nuclear Security Series no. 20, *Objective and Essential Elements of a State's Nuclear Security Regime*, Vienna, Austria (2009).

2. IAEA- INFCIRC/225/ Rev.3, *The Physical Protection of Nuclear Materials and Facilities*, Vienna, Austria (1993).

3. IAEA- INFCIRC/225/ Rev.5, *Nuclear Security Recommendation on Physical Protection of Nuclear Materials and Facilities*, Vienna, Austria (2011).

4. Mary Lynn Garcia, *Design and Evaluation of Physical Protection Systems*, Butterworth-Heinemann (2008).

5. Lionel S. Johns, *Technology Against Terrorism: Structuring Security*, OTA-ISC-511, Washington (1992).

6. *Enhanced Physical Protection Measures and the Agency's Plan of Action for Protection Against Nuclear Terrorism*; T. Rauf, presented at the 2003 NPT PrepCom, 6th May (2003).

7. B. Nkom, I.I. Funtua, and L.A. Dim, "Design of an Access Control System: A Paradigm for Small Nuclear Facilities", *Journal of Physical Security* 7 (2) (2014).

8. Hichem Sedjelmaci, and Mohamed Feham, "Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network", *International Journal of Network Security & Its Applications* 3(4) (2011).

9. Chong Eik Loo, Mun Yong Ng, Christopher Leckie, and Marimuthu Palaniswami, "Intrusion Detection for Routing Attacks in Sensor Networks", *International Journal of Distributed Sensor Networks* 2 (4) (2006).

10. Robert L Barnard, *Intrusion Detection Systems*, Butterworth-Heinemann, (1988).

11. James D. Williams, *Physical Protection System Design and Evaluation*, IAEA-CN-68/29, Vienna, 10-12 November (1997).

12. M.E. Elhamahmy, Hesham N. Elmahdy and Imane A. Saroit, **"**A New Approach for Evaluating Intrusion Detection systems**"**, *CiiT International Journal of Artificial Intelligent Systems and Machine Learning*, Vol 2, No 11, November (2010).

13. Alvaro A. Cardenas, John S. Baras, and Karl Seamon, "A Framework for the Evaluation of Intrusion Detection Systems", *Proceedings of the 2006 IEEE Symposium on Security and Privacy* (2006).

14. Headquarters, Department of the Army, *Physical Security Field Manual no.3-19-30*, Washington, DC, 8 January, USA, (2001).

15. KUBE Electronics Ltd, Garstligweg 2, *SF389 PIR Circuit IC Passive Infra-Red Alarm Preliminary Datasheet*, 8634 Hombre-chtikon, Switzerland, Revision 1.1, January (2003).

16. John J. Fay, *Encyclopedia of Security Management*, 2nd edition, Butterworth-Heinemann (2007).

17. Safety Analysis Report (SAR) of Safari Reactor of South Africa, *SECURITY SYSTEM BASIC DESIGN*, (1999).

18. 18th International Training Course, *Physical Protection of Nuclear Facilities and Materials*, Sandia National Laboratories, Albuquerque, New-Mexico, USA, (2004).

19. J.C. Beef, J. Josiak, S.F. Mahmoud, and V. Rawat, "Continuous access guided communication (CAGC) for ground-transportation systems; *Proc. IEEE*, vol. 61, pp. 562–568, May (1973).

20. R.G. Johnston, et al., "Effective Vulnerability Assessments for Physical Security Devices, Systems, and Programs"; *NUMAT Conference Proceedings*, Salzburg, Austria, 08–13 September (2002).