Design of a Test Bed for evaluating a Intrusion Detection System (IDS)

Jae Kwang Kim *, Jung Soo Kim
Truth hall in ICU Munji-dong Yu-sung gu, Daejon, KOREA, 305-732,
Korea Institute of Nuclear Nonproliferation And Control (KINAC)
Corresponding author: jgwang@kinac.re.kr

1. Introduction

Intrusion detection system (IDS) in domestic nuclear installation should be established in consideration of environmental and site-specific factors. Prior to this, a guidance of the IDS based on those factors at the specific nuclear facility should be provided. We have designed a concept of a test bed, which consists IDS and CCTV system, in order to execute several performance tests.

The ultimate purpose of this study is to establish a test bed in which IDS could be evaluated and developed.

2. Components and elements of a Test Bed

2.1 Intrusion detection system

There are several considerations for installing the system: 1) detection zone should be taken into account according to characteristics of sensors such as infrared, E-field, H-field, optical fiber, microwave sensor. To provide excellent detection, sensors require that the grade be planar and even, especially for good crawl detection. One example for microwave sensors installation from Sandia experiments will be shown as follow: The terrain should be flat, with no more than +0, -15cm deviation from a plane drawn through the offset points or crossover points directly in front of the transmitter and receiver of the zone. 2) Weather condition should be taken into account according to all the sensors' characteristics. The major factors which can induce the problem in health detection are snow, rain, wind and can be generating the nuisance alarm. The sensitivity of the sensors also should be reduced to get rid of these nuisance alarms. 3) Periodic performance testing should be taken into account. It is very good for guard to do small test on petrol of the PPS such as touching and walking at the near detection zone to make sure the good detection. The following performance tests of zone should be conducted while monitoring the output relay for the presence of an alarm condition: Initial walk, Run, Shuffle walk, Normal walk, Crawling intruder, Sphere target test. These tests will be performed more than once a year on spot because the sensors will be degraded as the environmental conditions are changed [4, 5, 6].

2.2 CCTV system (Video alarm system)

The purpose of a CCTV system is assessment which is essential to identify the cause of an alarm and to determine if an alarm is a threat or nuisance. The system should be cooperated with the intrusion detection system to cover the detection zone against intruders. The components of a CCTV system are shown in Figure1.

It is necessary to consider the relationships between the CCTV, the intrusion sensors and the display system.

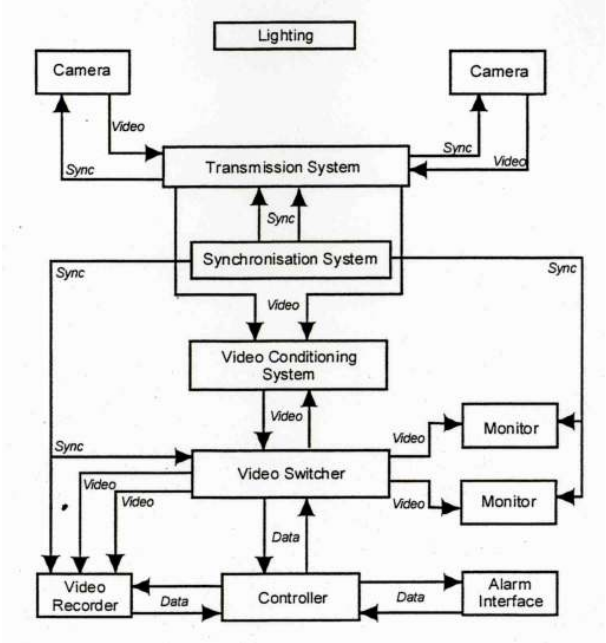

Figure 1. Components of alarm assessment systems.

One requirement of a perimeter assessment system is to display as much as possible of the clear zone including fences. For accomplishing the requirement, the spacing between the fences which are uniform, a minimum width for the clear zone, grading or removal of vegetation from the clear zone and adequate area for illumination should be required [4]. For example, The resolution limited by field of view of CCTV camera is based on experimental data from Sandia report[6] to classify a 30cm target(crawler intruder) and located where the horizontal field-of-view is 30cm wide

3. Characteristics of Performance test for IDS

3.1 Performance Characteristics

Performance of Intrusion sensors for the test bed can be described by 1) Probability of detection(P_D), 2)Nuisance alarm rate(NAR) and 3)Vulnerability to defeat.

P_D of an intrusion is one if the sensor is ideal; that is, it detects 100% of attempted intrusion. However no sensor is ideal and the P_D is always less than 1.0.

Not all alarms are caused by intrusion. Any alarm that is not caused by an intrusion is a nuisance alarm. If the IDS is ideal, NAR would be zero. In the real world, all sensors interact with environment and they cannot discriminate between intrusions and other events in detection zone.

Intruders can defeat the IDS through means such as bypassing and spoofing. All existing sensors are vulnerable to defeat because they are not ideal. Bypassing means is to go around sensor's detection limits for defeating the system because all intrusion sensors have a finite detection zone. Spoofing means is the technique that allows a intruder to pass through the sensor's normal detection zone without generating an alarm.

3.2 Method for performance test

We should conduct the performance test of the walking, running and crawling while monitoring the output relay for the presence of an alarm condition.

Walk test is consisted of initial walk test, shuffle walk test and normal walk test. Initial walk test assures proper spacing from the fence to the sensor. If someone walks along the entire length of the zone parallel to the fence, no alarm should occur. Shuffle test is performed by someone walking very slowly across the beam with no swinging of arms. Step size taken should be less than 2 in. The shuffle speed of the walk should be approximately 2.4 in/s. The test identifies the slow speed response of the sensor. A number of walk test perpendicular to the sensor beam centerline should be performed. When an alarm occurs, a colored block may be dropped. Upon completion of the test, the colored blocks should represent the detection envelope. The detection envelope should be smooth pattern.

A run test identifies whether the receiver response is fast enough. The test should be performed approximately 20ft from the transmitter and the receiver, where the microwave beam is narrow. The test should be performed at a velocity of approximately 26 ft/s perpendicular to the beam. There have been instances where a circuit board was stuffed with the wrong value components and the sensors failed this test.

Ideally, the sensitivity of a IDS should be adjusted to the lowest level that will adequately detect the parallel stomach-crawl intruder. The sensitivity assures that the NAR is reduced to the lowest level. To eliminate the need for actual human crawl test and to obtain more repeatable results, the crawl test can be performed by dragging an aluminum sphere with a diameter of 12in across the detection zone. A metal sphere can be used to simulate the various modes of human locomotion because movement along any given path causes rather sinusoidal phase variations that are independent of the target shape.

4. Further consideration

After the establishment of a test bed, we are going to test IDS in consideration of the environmental factors in domestic nuclear sites including all the performance tests as mentioned above. We could make the recommendations for installing and evaluating physical protection components. The test bed would be used to provide the countermeasures against threats if a national design basis threat is developed. Also, Data base establishment would be expected through this study in order to provide the criteria for performance-based physical protection inspection

REFERENCES

[1] IAEA-TECDOC-967(Rev.1) Guidance and considerations for the implementation of INFCIRC/225/Rev.4, The Physical Protection of nuclear material and nuclear facilities. May 2000.

[2] NNCA/TS-001/2006 '핵물질과 원자력시설의 물리적 방호' 의 이행을 위한 지침서. 2006 년 3 월

[3] IAEA-TECDOC-1276, Handbook on the physical protection of nuclear and facilities. Mar. 2002.

[4] Workshop on Physical Protection System of research reactor. Australia, 2004.

[5] SAND94-1145, Interior intrusion detection systems, SNL, 1994.

[6] SAND99-2391, Exterior Intrusion Detection systems, SNL, 1999.