1993

Integrated computer controlled sensor monitor

Tariq Hafeez Malik
Edith Cowan University

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

Integrated Computer Controlled Sensor Monitor

by

Tariq Hafeez Malik

A Thesis

Submitted in Partial Fulfilment of the Requirements for the Award of

Bachelor of Applied Science (Information Science) Honours

at the Faculty of Science & Technology
Edith Cowan University
Perth, Western Australia, Australia

Supervisor: A/Prof Anthony Craig Watson

Submission date: 25th of November, 1993.

ABSTRACT

This research has developed an **Integrated Computer Controlled Sensor Monitor (ICCSM)** environment, to monitor and analyse alarm events associated with sensors, including an interface between a PC and a number of detectors. Such an environment will help the security industry analyse the factors causing false alarms at particular locations. The ICCSM environment monitors, and records, alarm data. Knowing exactly which sensor has been activated, and its location, is of paramount importance to the effective deployment of response forces and making the identification of causes of spurious alarms easier.

The ICCSM environment is a combination of software and general purpose hardware, including a PC, an interface between a PC and a range of sensors, a Video Cassette Recorder (VCR), and a video camera. The software can process information from 64 different sensors, and output control information to a VCR. A database has been developed to record information from sensors such as detector location, date, and time of alarm. The ICCSM also generates written reports, allowing the user to fully examine the performance of a detection system. An intrusion, or the event triggering the sensor, is also captured on VCR for future verification.

The ICCSM is a GUI based environment running under Microsoft Windows with menus and help facilities. It allows the user to simulate a range of conditions to adjust

sensor sensitivity levels, providing the means to test the integrity of a detection system. A database is designed to add and delete the sensor information. The database is automatically updated as an intrusion is detected.

The software operates in two modes, simulation and production. Simulation mode allows a security administrator to simulate possible alarm conditions to thoroughly test and fine tune a detection system. The production mode is for use in an operational environment and will operate autonomously for a maximum of 480 hours, thus previously unknown causes of false alarms may be determined.

Declaration

I certify that this thesis does not incorporate, without acknowledgment, any material previously submitted for a degree or diploma in any institution of higher education and that, to the best of my knowledge and belief, it does not contain any material previously published or written by another person except where due reference is made in the text.

ACKNOWLEDGMENTS

I would like to express my gratitude to my supervisor, Associate Professor Anthony Watson, for his support advises and numerous considerations of my documentation. I would also like to thank Jeremy Laidman, Mohammed Sarfraz, and Vincent Phillips - of the Edith Cowan University, Western Australia, for their guidance and positive comments.

DEFINITION OF KEY TERMS IN THE STUDY

The terms defined below are extracted from the Australian Standards (1986) unless stated otherwise.

- Alarm condition — State realised in any part of an intruder alarm system resulting from any of the following:
    - Operation of a detection device.
    - Operation of a tamper detection device.
    - Fault in the system
    - Intrusion or attempted intrusion.

- Alarmed area — That part of an area to which detection is afforded by an intruder alarm system.

- Alarmed sector — That part of an alarmed area or alarmed zone to which at least one detection device is allotted and for which individual indication is provided.

- Client — Person or organisation utilising the services of an alarm company.

- CCTV — Close Circuit Television.
- External alarm — Equipment consisting of either a sound-producing or light-producing device located on the exterior of alarmed premises and situated to attract attention.
- False alarm — Any alarm condition other than a genuine alarm.
- Fault alarm — Alarm condition caused by malfunctions of the equipment.
- Genuine alarm — Alarm condition caused by the intended operation of the alarm system.
- GUI — Graphical User Interface (not from the Australian Standards).
- Intruder alarm system — Any system designed to detect and signal the presence, entry, or attempted entry of an intruder into an alarmed area.
- Nuisance alarm — A false alarm; an alarm caused by equipment

		failure or a fault not related to an actual security violation (Fay, 1987).
•	Perimeter	Property boundary or alarmed area boundary.
•	PC	An IBM or IBM compatible Personal Computer (not from the Australian Standards).
•	Sensor	A device designed to produce a signal or other indication in response to an event or stimulus within its detection area, also known as a detector (Fay, 1987).
•	VCR	Video Cassette Recorder (not from the standards).

TABLE OF CONTENTS

List of Tables

List of Figures

1 INTRODUCTION

1.1 Background

The Department of Computer Science, Edith Cowan University, along with the Institute of Security and Applied Technologies, Edith Cowan University, has undertaken research into the use of computers for security applications and, in particular, the rate of false alarms for sensor technologies. This research is aimed at improving the quality of security systems by using alarm monitoring facilities to quality check the accuracy of any attached sensors. Significant reduction in false alarm rates can be achieved through better designed systems, producing more efficient and effective outcomes ("Challenges facing the alarm industry", 1988). The research environment, described in this thesis, may result in a better understanding of the problem of false alarms through the development of a computer based alarm monitoring system.

The developed research environment records both visual images and intrusion details into a database. The recorded intrusions then can be manually cross referenced against the situations captured on the VCR, thus identifying the cause of a specific alarm and also the environments causing the greatest number of false readings.

This study developed an Integrated Computer Controlled Sensor Monitor (ICCSM), that enables a security administrator to monitor security systems and

manually adjust motion detection sensors to minimise false alarm readings.

1.2 Rationale

There is extensive data indicating that security systems making use of detection sensors perform poorly. The result of this poor performance, usually in the form of an overwhelming number of false alarms, has increased cost for the users, security companies, and, by extension, society in general (Russell, 1991).

It has been suggested that it is not the detection systems that are at fault but the standard of sensor calibration and control. One possible solution is to provide users and administrators with the means to monitor and experiment with the sensor devices (Bernard, 1988).

It has been further suggested that current detection technology is rapidly advancing towards its saturation point, and that the false alarm problem cannot be resolved by improving existing detection technologies ("False Alarms: It's the user who holds the key," 1988). According to Richard Corey (cited in Russell, 1991, 43), head of American National False Alarm Prevention Committee, "false alarms cannot continue to go unaddressed. It will be a matter of time before the problem is overwhelming". Despite technical advances in alarm technology there is still an unacceptable rate of error.

1.2.1 False Alarm Statistics

The false alarm rate is high all around the world. Data gathered within the United States of America (USA) indicates that around seven million signalling systems are installed in USA, with police receiving some 14 million activation reports per year, an average of two per system. Only 280,000 (2%) alarms are genuine and, by implication 98%, are classified as false alarms (Carter, 1991).

For the rest of the world, including Australia, the false alarm rate is in excess of 96% (Galloway, 1992; Carter, 1991; Blundell, 1990; Oliver & Wilson, 1988).

A survey conducted in 1990 by Security magazine in the USA suggests that users experience more than one reason for a false alarm: 70% of the surveyed users indicated unit malfunction and of those 70%, 50% accused weather conditions as the cause of unit malfunction, and 48% blamed environmental changes in the alarmed area, for unit malfunction (Moss, 1990).

An independent study conducted by Bloom, Cross and McDougall (1991), which studied the monitored alarms in the Perth metropolitan area that were attended by the Western Australian police in the months of May and

September 1989, confirmed the high false alarm rates. Thus, it can be perceived that false alarm rates are reasonably consistent around the world.

1.2.2 Side Effects of False Alarms

Once an alarm has been detected the normal procedure is for a security company to inform the police and, possibly, dispatch an operative to the protected area (Hughes & Bowler, 1982). If the detected intrusion is a false alarm, at least two agencies are immediately mobilised, namely the security agency and the police. False alarms cause the subscriber, alarm company personnel and police to quickly lose confidence in a detection system (Weber, 1985).

New York police are not required to respond to sites that have more than three false alarms in a three-month period. In Woodstock, USA, the police charge $150 for a second false alarm call within a six month period (Russell, 1991). In England, false alarms cost the police $850 million (US) per year, and the police now refuse to attend premises that report excessive false alarms (Galloway, 1992).

It has been alleged that often physical layout of the security system and of security devices is improperly designed and users cannot reduce or recover from the false alarm problems (Russell, 1991). It has been further suggested that the Guardian Alarm Company of USA will not use some products because of their improper design. They found it difficult to switch some devices off once an alarm has been triggered.

In summary it can be stated that false alarms are costly to the user, to the police and to the public in general. The problem, which ICCSM addresses, is to reduce the number of false alarms by creating an environment which will formulate sensor adjustment to a given environment.

1.3 Objectives

The ICCSM has been designed with an objective to reduce the false alarm problems by providing the following facilities:-

1.3.0.1 Automatic Data Gathering

Occasionally passing traffic, vibration, employee error, weather changes and unit malfunction cause false alarms. For security firms, the difficulty is in determining the cause of an alarm (Galloway, 1992). The ICCSM environment is designed to isolate the environmental

factors causing the problems through the use of automatic data capture facilities. Such facilities would help security agencies to determine the weaknesses in individual detection technologies, and thus "fine tune" the performance of a security system.

1.3.0.2 Physical Design of a Security System

Owen (1986) stresses the need for PC's in security systems, and the requirement for effective software for future security applications. He suggests that personal computer applications may lead to better designed security devices and systems. Warnock (1992) states that physical design of the security system is far more complex than many people realise.

The ICCSM environment can assist the security administrator to validate and verify the physical design of the security system. Thus creating a better designed sensing environment with less false alarms.

1.3.0.3 Post Installation Maintenance

Warnock (1992) stresses the need for post-installation maintenance. He further suggests that if the system is not properly maintained, problems may arise in getting the alarm system to operate correctly. With an effective computer monitoring system a trend of degrading performance will become obvious long before the security system is compromised (Jonckheere & Weeden, 1985).

The ICCSM is designed to provide a mechanism to monitor sensors and gather data about the performance of sensors. The performance data then can be utilised by the security administrator to analyse the past and present performance of a detection system. The analyses of the past performance data can reduce the false alarm rate because the security administrator has better understanding of the causes of false alarms.

1.4 Problem Questions

The problem questions of the research were to:

- specify an integrated computer controlled sensor monitoring environment on the basis of past problems determined by research literature.

- design and build a computer controlled sensor monitoring environment for sensor devices (ICCSM).

- investigate how a computer controlled environment can reduce the false alarm rates of motion detection systems.

1.5 Limitations

The research software has no control over the time required to read the sensor status board, thus, there is a short delay of two seconds to get information from the sensor status board to the PC, process the data and store it. However to overcome this problem, a VCR control module mounted onto a "vero board", was developed to immediately shift the VCR from slow recording mode (14~480 hours mode) to normal (three hour) recording mode. The events leading to an alarm are also recorded by the

VCR but at a slower speed under ICCSM environment. The operational speed of the VCR is decided by the Security Administrator.

Limited real tests were conducted due to the difficulty in simulating the environmental conditions in a university. Extensive field testing and use of the system for the various conditions would form part of additional research.

1.6 Outline of the Study

Chapter Two examines literature describing the frequency of false alarms and explains the false alarm problem and possible advantages of ICCSM in greater detail. Chapter Three describes the motion detection technologies, providing a better understanding of their operational characteristics, to assist in understanding the false alarms. Chapter Four outlines the methodology followed in the development of ICCSM and details the hardware utilised. The software design of the ICCSM, including database design, is also detailed in chapter four. Chapter Five summarises the research.

The suggested experiment forms are attached in Appendix A. The reports structure, produced by the ICCSM, is included in Appendix B. Appendix C is a copy of the user manual of the ICCSM environment. Appendix D contains trade mark acknowledgments.

2 LITERATURE REVIEW

2.1 What is a False Alarm?

A false alarm can be caused by a variety of factors, including equipment malfunctions, small animals, man made disturbances and user error. Environmental conditions, such as rain, snow, wind and lightning can also interfere with a detection system and initiate an alarm (Bernard, 1988). For this research a false alarm was defined as:

- an intrusion that was not detected, and
- an alarm that should not have been triggered.

2.2 Why False Alarms are a Problem

False alarms are costly to users, security agencies and police both in time and resources. Legislation recently brought into force in NSW fines the owner of the security system $200 for excessive false alarms. Around 600,000 signalling systems were installed in England and Wales by the end of 1990 (Carter, 1991). There were about 1.25 million alarm activation and of those 4% were genuine alarms, and 96% of alarm activation were false alarms. This means that the probability of each sensor triggering false alarm is over 2.4 (1.25 million / 600,000) illustrating the enormity of the problem. The security systems with excessive false alarms have gained the disdain of security and police departments and are proving to be extremely costly to

end users (Russell, 1991).

The decline in sensor detection quality may be a direct result of physical deterioration of a sensor. The sensitivity level of sensors need to be adjusted regularly. The sensors deteriorate and post installation maintenance is required (Weber, 1985). A highly sensitive sensor may over react to a non-intrusion situation. The sensor reaction depends on the type of the sensor installed. For instance, a microwave sensor will trigger an alarm for a passing car. A passive infrared sensor may trigger an alarm for spot lights of a car, provided that the sensitivity level of the sensor is high.

False alarms are a nuisance to the user, security agency and the police. They waste their time and resources. The exact number of security devices, installed worldwide, and the false alarm cost associated with them is unknown. However, the sensors installed in USA and England, with a false alarm rate of over 90%, indicate the extent of problem. In monetary terms this high false alarm rate represents millions of wasted dollars.

2.3 Previous Solutions

Researchers have shown interest in different aspects of computing to improve the capabilities of detection technologies. Researchers, like Ellis, Rosin, and Golton (1990) describe the development of a knowledge-based visual recognition system,

automating the interpretation of alarm events resulting from a perimeter intrusion detection system. They have applied the system to real time situations and according to their analyses the system works according to its specification. Their research utilised a central repository to record information based on visual recognition. This research exhibited the use of a central repository or database to verify spurious alarms, proving the advantage of data gathering for analyses purposes.

Arlowe and Coleman (1990) describe MIDAS - a Mobile Intrusion Detection and Assessment System. It is a system that can be quickly deployed to provide coverage for mobile assets. This system uses two passive infrared imaging sensors, one for intruder detection and one for assessment. Targets are tracked while assessment cameras are directed to view the intruder for operator observation and assessment. The dual sensor design allows simultaneous detection, assessment and tracking. Control and status information is provided to an operator using a colour terminal, touch panel driven menus and a joystick for control of the assessment sensor. The MIDAS research is directed towards military applications of passive infrared technology. The system is not completely automated as an operator must make decisions regarding an alarm. The observed detection and tracking were better under cloudy conditions, or with live grass, low brush or water background. Where sun heating and random thermal cooling events become significant, detection performance was degraded. Rain and high humidity also led to poor performance. The physical positioning of the detectors also affected the alarm outcome. The research outlines the significance of detector locations and that a dual detection

system can be more effective than a single technology. The ICCSM environment can be utilised as a workbench to examine the operational characteristics of an individual or dual technology detector to determine which technology will be best suited for particular locations and also to verify the physical location of the installed sensor.

Custance (1988) suggests that the false alarm rate will be affected by the environment in which a detector is operating. He implies that the correlation between false alarm rates and the environment offers the opportunity for sensors to be improved. The objective of his research, was to examine methods for processing the data to identify those key factors in the environment which correlate with causing a false alarm. The alarms due to non-weather causes were extracted from the data before analyses. The particular objectives of the analyses were to explore the usefulness of statistical and rule induction techniques for predicting the likelihood of a false alarm occurring under given weather conditions. The study concluded that, wind speed and direction were the most significant causes of false alarms. ICCSM, can be utilised to monitor the effects of those environmental factors and improve their performance according to local weather and environmental conditions.

Patten & Folea (1989, p. 21) have studied the use of infrared technology for detecting intruders in tactical and strategic applications. Signal input to a simulated sensor system came from either an infrared video camera or from video tapes of intrusions recorded previously. This permitted extensive laboratory testing of sensor performance under various weather conditions. Their research proved the viability of

an infrared imaging sensor system for tactical and physical security applications. The research also demonstrated the importance of a computer to monitor sensor performance for intrusion verification. ICCSM does not verify the difference between a false alarm and a real intrusion but does provide video images for later verification of spurious and real alarms.

2.4 Similar Approaches

Morton (1984, p. 29) introduced a product offered by the Senstar Corporation of Canada, called SENTRAX II. The system utilises distributed microprocessor technology. The system is equipped with CCTV cameras, lights and these devices can be activated once an alarm is sensed. This product allows the user to monitor and control security sub systems from a control console. The user can inspect the status of sensors and other security equipment. They can switch security equipment on or off, such as turning the lights on in a troubled area or start recording an intrusion.The user controls their security network from a console (Morton, 1984).

The video images are later used for intruder verification. The system is good for indoor environments, such as hotel security. A dedicated person is required to monitor the console and decide which equipment needs to be switched on or off (Morton, 1984). Unlike the SENTRAX II system, the ICCSM environment is also equipped with a database facility to monitor and store detection information for future reference. The ICCSM environment can monitor an environment for a

maximum of 480 hours without human intervention.

2.5 Significance of the Study

The previous research and expert opinions have demonstrated the importance of the following aspects of a security system for the reduction of false alarms.

- Automatic Data Gathering,
- Physical Design of the Security System (Warnock, 1992) and
- Post-Installation Maintenance of the Sensors (Warnock, 1992).

2.5.1 ICCSM and Data Gathering

The data gathering of alarm events is considered by experts as an important aspect for the future deployment of false alarms. Experts such as Martin Bone (1990) envisages a greater degree of integration between a control environment and the detectors. Jackson (1990) confirms the ability to extract a system log and to analyse the past performance of the detectors can be a major step towards reducing the false alarms.

Jonckheere & Weeden (1985) declare that a data gathering and analyses process can be effective in analysing the operational use of the security sensors. Oliver & Wilson (1988) suggest that information such as

alarm date, alarm time, what happened and physical location should be recorded. The ICCSM environment automatically records the intrusion data and also records video images of the intrusion. The user can analyse the recorded data to identify the cause of an alarm.

2.5.2 ICCSM and the Physical Placement of the Sensors

The Security Gazette magazine in an article "Matching the system" (1988) explains the possibility of significant reductions in false alarms in motion detection systems by improving the physical placement of security devices.

The physical design of a building or premise may vary from building to building. In turn the false alarm causes differ from premise to premise due to the different physical layouts. Warnock (1992) mentions security installations where the security devices were incorrectly wired or the physical layout of the detectors was questionable. Before a sensor is installed a thorough survey is necessary to decide upon the best suited detector type for that location.

The potential sources of indirect reflected energy may cause false alarms. Heat generated outside the protected area that is radiated into the field

of detection through glass or reflected into the field of detection by mirrors or metal surfaces located outside or within the protected premise may cause false alarms. Once a sensor is installed a guideline is utilised by the security agencies to test and verify the sensor location. The guideline is a set of instructions carried out following a detector installation (P. Knight, personal communication, n.d. 1992). They may not cover the various layouts and side effects of the material used for the construction of a building. The guidelines, most certainly, don't cover the effects of various electrical devices in operation on a premise. The detection technologies may then, behave differently on a premise than another. These alarms are mostly triggered due to physical placement differences or due to interference from other electrical devices. The detection technologies may pass through the walls or be reflected by an uneven surface resulting in unpredictable conditions. Their detection capability might be interfered by harmonic distortion and electronic fields from other electronic devices resulting in spurious alarms (Warnock, 1992).

The ICCSM, functioning as a workbench, can be used to simulate known false alarm conditions or to leave the performance monitoring system switched on to test the sensor and sensor layout. Warnock (1992) considers that half the battle is won by installing a sensor at the right location. The ICCSM reports can be utilised to determine any other causes of false alarms not included in the guideline.

If two or more detectors are installed closely to each other then a crevice between two detectors will weaken the detection capability of the security system. The user needs to experiment and document all the possible entrances to eliminate a crevice. The ICCSM environment can be utilised to find out and log any discrepancies in the physical placement of the security system. A crevice will be identified after experimenting on all the possible entrances and then can be eliminated.

2.5.3 ICCSM and Post-Installation Maintenance of Sensors

Clive Hayton, marketing director, Shorrock Security Systems (cited in "False Alarms", 1988) explains the importance of continuous monitoring and post-installation maintenance of a sensor. The sensor performance can be affected by the environmental conditions. Weber (1985) regards humidity as a cause of degradation in sensor performance. The detection range of sensors may reduce in time and post-installation maintenance could be required to upgrade it (Warnock, 1992).

Some passive infrared detectors tend to suffer from reductions in range and sensitivity when ambient temperatures are 35°C or higher. This problem is of greater concern in environments where, during closed periods when air

conditioning and ventilators are closed down, the ambient temperature may rise slowly to levels in the 37.7-54.4°C range. If such temperature occur, particularly in warehouse and factory environments in warmer climates, intrusion may go undetected (Weber, 1985). Weber (1985) suggests that tests need to be performed on the sensors to attain the right sensitivity levels to detect possible intrusions.

Jonckheere & Weeden (1985), emphasise the need for a diagnostic tool for equipment maintenance. The decline in sensor performance can be identified by comparing the current test results with the recorded results.

The ICCSM is an environment to test the sensors and record the test results. Continuous monitoring of sensors is required for some installations to maintain the high quality of their detection and at the same time not have false alarms due to environmental conditions. The continuous monitoring of sensors may well determine that the sensor type is incorrect for that alarmed area. The sensor may need replacement to achieve a high quality of detection and at the same time reduce false alarms.

2.6 Conclusion

The data presented by the researchers has shown that the rates of false alarms are in the vicinity of more than 90% (Russell, 1991) world wide and most of the reasons for these false alarms are known and reasonably well understood. Experts also emphasised the importance of past performance data, physical design of the security system and the post installation maintenance. This research has developed a workbench to validate the security system installation design, fine tune the devices, and log detected intrusions for future reference.

3 MOTION DETECTION TECHNOLOGIES

The previous chapter has demonstrated that environmental factors are a significant cause of false alarms. This chapter presents an overview of the two sensing technologies which are widely used for intrusion detection by security agencies (Knight, personal communication, n.d, 1993). It is important to identify their advantages, disadvantages and operational characteristics to discover their vulnerabilities to environmental factors.

3.1 Passive Infrared Technology (PIR)

Passive infrared (PIR) is the most popular intrusion-detection sensor technology presently available (Weber, 1985). Paul Knight of Direct Alarm Supplies (personal communication, n.d, 1993), Western Australia, Australia, consider PIR movement detectors as "industry" standard for movement detection. PIR detectors are passive devices and unlike other technologies do not transmit any energy but simply detect changes in heat energy emitted by the background of an alarmed area.

All objects with a temperature greater than absolute zero radiate energy in proportion to their temperature. For instance, an intruder with a body temperature of 37°C radiates more energy than a wall at 20°C. Thus, when an intruder passes through a protected area the difference in thermal energy is detected between the

intruder and background (Alexander, 1988).

A passive infrared intrusion sensing device consists of a pyroelectric heat sensing element, an optical lens system, a low-current power supply and a logic circuit or analyser. The device can accomplish the following (Weber, 1985, p.57): "

- Measure temperature (infrared energy) changes.
- Relate temperature change to changes in time.
- Compare the change in temperature within a period with the ambient temperature.
- Transmit an alarm signal if the coefficient of temperature change exceeds temperature-time change."

3.1.1 Advantages of Passive Infrared Technology

PIR detectors are not effected by noise. Similarly, vibrations caused by low flying planes, railroad cars, or ground tremors, may vibrate the passive infrared sensor through its mounting structure, but its operation is not affected. This is in contrast to ultrasonic, microwave, or photoelectric beam devices (Bernard, 1988).

PIR detectors are not affected by wind, rain, or air turbulence. The greatest advantage is that PIR detectors have the best sensitivity when an intruder moves across the detection field, and the lowest sensitivity for motion towards or away from the detector. Whereas, the microwave technology detects an intruder while moving towards or away from the detector. Thus, the combination of these two technologies should detect all possible movement directions (Steiner & Wagli, 1983).

3.1.2 Disadvantages of Passive Infrared Technology

Sharp changes in temperature may cause a false alarm. Sharp changes in temperature resulting from mechanical failure of heating and air-conditioning units, and drafts created by broken windows can also cause false alarms. Energy created by sunlight and mechanical energy resulting from vehicle headlights, spotlights, or heavy flashlights shining directly or reflected into an optical detection zone may also cause an alarm signal (Weber, 1985).

When an intruder passes through the security system in an environment where background temperature is the same as his or her body temperature then passive infrared detectors will not detect the intrusion (Walker, 1988).

As PIR detectors do not radiate energy, they will not protect areas shielded by building materials, such as stacked cartons and newly added walls (Trimmer, 1981).

3.2 Microwave Technology

In the late 60's, many electronic manufacturing companies, research, and development companies sought commercial security applications for the electronic devices and systems they had developed for US space program and the Vietnam war. The application of microwave technology for the detection of the movement of intruders was one of the earliest and most successful applications of existing technologies (Weber, 1985).

The microwave signal source is typically a Gunn oscillator diode. This diode produces microwave energy when supplied with a DC voltage at low-current. As the transmitted signal strikes the intended target some microwave energy will be reflected back to the sensor. The amount of reflected signal is dependent upon the composition and shape of the object, and the distance from the sensor. The reflected signal is received within the sensor by a detector diode. The detector diode is essentially the inverse of the Gunn diode as it transforms the microwave energy into a voltage signal that is then amplified and interrogated for information regarding the target. The signal strength increases in the presence of an intruder. This is the result of the

Doppler shift and, obviously, is affected by the movement of an object (Saucier, 1991).

3.2.1 *Advantages of Microwave Technology*

Microwave sensors operate without touching the object of interest and are unaffected by airborne contamination and extremes of temperature and noise. In addition, temperature gradients, drafts, or even pressurised air, do not affect performance. Microwave energy can penetrate many non metallic materials, allowing sensor electronics to be physically separated from target environments (Saucier, 1991). Thus, the microwave detectors, can be used in an office environment where obstacles are blocking the way for passive infrared detectors or for any other technology detector.

3.2.2 *Disadvantages of Microwave Technology*

As microwave energy can penetrate many non metallic materials, it creates a unique false alarm problem. Any object moving outside the protection zone can trigger a false alarm (Weber, 1985). Masonry walls (brick, concrete, or stone) will not be penetrated easily, thus, the sensitivity of the microwave detector needs to be adjusted according to the detection zone (Trimmer, 1981).

3.3 Dual-detectors

Walker (1988) concedes that no sensor designed for intruder detection is complete in itself. Alexander (1988) states that each type of sensor has its individual advantages and disadvantages, and thus a combination of different technologies is required. The two motion detection technologies, microwave and passive infrared, are sensitive to some environmental changes and less sensitive to others.

A new technology has emerged known as *Dual Detection*. These sensors combine two sensing technologies to reduce the incidence of false alarms. The most popular of dual detectors use PIR and microwave technologies (Knight, personal communication, n.d, 1993). With dual detectors the first pulse from either of the technologies will open a time window and if the other technology triggers within that time window the detector will signal an alarm condition.

Weber (1985) suggests that this concept, which provides for identical patterns of detection coverage, is superior to the redundancy achieved by the installation of two separately operated intruder-detection sensors and it is certainly a more efficient way of achieving the primary objective of fewer false alarms (Moss, 1990).

The combination of PIR and microwave technologies is regarded as a possible winner by Weber (1985). PIR prefers motion across its field of view, thus missing, or rejecting, a potential source of false alarm. Where as microwave is at its best with

motion towards or away from it.

The advantage of dual technology detectors can also be a disadvantage. As both technologies need to detect the intrusion before raising an alarm. If one fails to detect the real intrusion, even though the second technology has detected the intrusion, no alarm will be raised. Walker (1988) questions the use of dual detectors. He asks what is more important, the certainty of detection or freedom from false alarms. He further suggests that dual detectors raise risks of an intrusion and the user should lean towards making certainty of detection their priority.

3.4 Environmental Factors Influencing the Sensors

According to the literature the following environmental conditions are those hypothesised to affect the accuracy of sensors.

- Rain, Dampness — Rain and Damp can affect both PIR and microwave technologies. Friedl (1989) includes rain and dampness among other factors, contributing towards higher false alarm rates. Humidity is also an important factor in sensor performance (Weber, 1985).

•	Temperature Change	Temperature change is a potential source of false alarms for PIR technology. Most heaters warm up slowly enough that they will not be detected by PIR, but a sharp change in temperature will trigger an alarm. Microwave technology does not get affected by sudden change in the temperature, thus eliminating the possibility of a false alarm due to temperature change.
•	Slow Movement	Slow moving objects may not be detected in the microwave detection area.
•	Small Animals	Small animals such as dogs and cats can cause problems, depending on their size and distance from the detector. Mice and birds are unlikely to cause problems unless they pass within metres of the detector ("Matching the system with the environment", 1988).

4 THEORETICAL FRAMEWORK

4.1 Introduction

4.1.1 Objectives

The problem definition and the literature review, explains the existence of the false alarm problem in the intrusion detection area. Experts such as Paul Parr, Richard Corey (cited in Russell, 1991), Owen (1986), Roy Carters (1991) have emphasised the importance of false alarm problems and the need for a solution which can drastically reduce the proportion of false alarms.

The rationale of the ICCSM environment is to design and build a computer controlled sensor monitoring environment to investigate the possible reduction of false alarm rates of detection systems by a computer controlled sensor monitoring environment. This is to achieved by:-

- monitoring the environment in which a sensor is operating. This is required to analyse the causes of false alarms due to a change in the physical environment in which a detector is operating. The change of environment may include a change in the weather, such as rain or change in the physical space in which a detector is operating, such as creating or removing a partition in the office space and

- by analysing the performance of the security detectors for regular maintenance and fine tuning the detectors before the security of the detection system is compromised.

4.1.2 Scope of the Requirements

The ICCSM environment will isolate one of several triggered alarms, capturing details such as which alarm was activated, the date, the time and location of the detector. The cause of an alarm is captured on video recorder to enable manual verification of the alarm outcome. As a result the security administrator can modify and fine tune the security devices.

The system specification has been grouped into four categories.

- Database Specification;
- Functional Specification;
- Hardware Specification and
- Software Specification.

4.1.2.1 Database Specification

The ICCSM environment required a database to automatically record detected alarm events. SQLBase database was preferred over other products because:

- SQLWindows can send and receive data from high-level computer languages, such as "C". The interaction between the "C" programming language, and the SQLWindows was required to perform sensor status monitoring by the "C" programs and to record the intrusion information into the database.

4.1.2.2 Functional Specification

The ICCSM software adheres to the following specifications:

- the ICCSM functions as a workbench to evaluate the quality of the security system,
- the sensitivity level of a sensor can be adjusted manually by the security administrator. The ICCSM environment, functioning as a workbench, can be utilised to perform continuous experiments on the sensor until such time when the sensitivity level of the sensor is appropriate,

- the attached video cassette recorder captures continuous video images, and thus, captures the real intrusion,
- the ICCSM database keeps a log of detected intrusions,
- the motion detector types are recorded in the database, and new detectors can be added and deleted from the database,
- an easy to follow help facility and
- the system provides various informative reports:-
    - all the intrusions for a particular detector type,
    - a list of intrusions from a particular date and
    - all the intrusions for a particular experiment type.

4.1.2.3 Hardware Specification

The following hardware specifications were met by the ICCSM environment:

- with the exception of the video cassette recorder, general purpose hardware was utilised to lower the ICCSM development cost,
- a special VCR which operates at a slower speed and switches to normal recording mode when an intrusion is detected,
- external to the computer, special input/output boards, PC-IO-NR boards, are utilised for sensor status monitoring,
- installed inside the computer is a special input/output card, PC-BD-IO

card, to connect a maximum of fifteen PC-IO-NR boards to the computer,

- the PC-IO-NR boards have an acceptable signal to noise ratio and
- the hardware can be easily moved to a different location without major hardware adjustments.

4.1.2.4 Software Specification

The ICCSM software meets the following specifications:

- an easy to use graphical user interface,
- an easy to follow help facility,
- real time alarm situations should be captured by the VCR and also recorded into a database,
- extensive data and user input validation has been performed and
- user input is kept to minimum to reduce the possibility of human typographical errors.

4.1.3 Description of the Requirements

The objective of this research is to build a computer environment where motion detector data can be gathered and later evaluated for fine tuning the motion detectors to reduce the false alarm rate of the security detectors.

A database is required to effectively store intrusion data. A normal "C" file system could have been created but was rejected, because, as the intrusion data file size increases the input output from the file takes longer and can be inefficient. A database also reduces the possibility of data redundancy and data duplication.

The video images of intrusions verify the causes of spurious alarms. A user can manually adjust the sensitivity level of a sensor after analysing the visual data for that sensor.

The hardware cost of the ICCSM system were kept to a minimum thus a clone system can be manufactured by any security agency without enormous hardware costs. The ICCSM environment can easily be ported to an another location.

An application's user interface determines its appearance and behaviour. When the user interface makes use of graphical objects such as windows and menus, it is called a Graphical User Interface (GUI). GUIs have become an industry standard in the majority of professional software packages. The ICCSM environment makes full use of GUI, because users generally prefer to interact with a GUI application (Barkakati, 15).

4.1.4 Data Flows

4.1.4.1 Database Structure

- The ICCSM environment is also equipped with a database. The Entity-Relationship Diagram of the database is as follows:

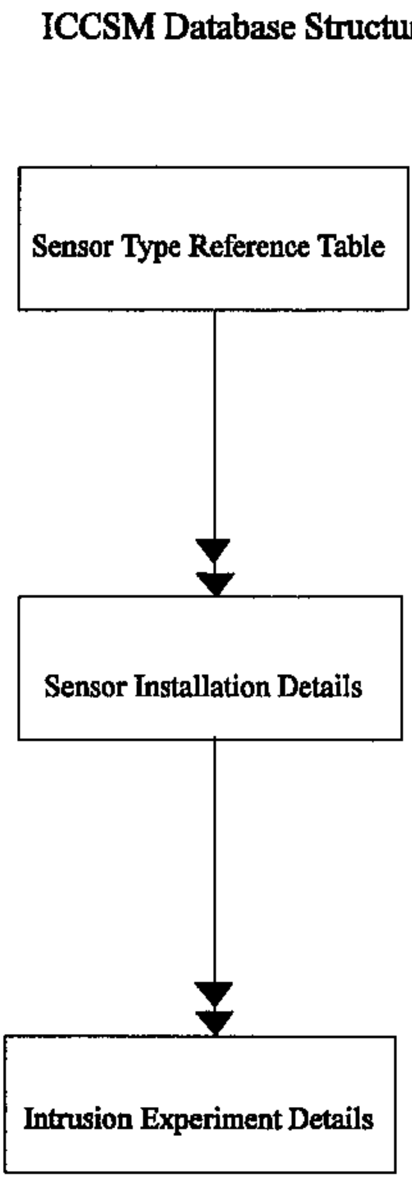

Figure 1: ICCSM Database Structure

4.1.4.2 Database Design

Three database tables were created and their attributes are:

Table Name : Intrusion Experiment Details

Attribute	**Attribute Type**	**Field Length**	**Primary Key**	**Foreign Key**
Alarm_No	Integer	4	Yes	No
Board_Num	Integer	4	Yes	Yes
Current_Temp	Integer	4	No	No
Experiment_Ty	Char	25	No	No
Fog_Level	Char	15	No	No
Max_Temp	Integer	4	No	No
Min_Temp	Integer	4	No	No
Object_Color	Char	20	No	No
Object_Size	Char	15	No	No
Sensor_Num	Integer	4	Yes	Yes
Sim_Date	Date	4	No	No
Sim_Time	Time	3	No	No

Figure 2: Intrusion Experiment Details

Table Name : Sensor Installation Details

Attribute	**Attribute Type**	**Field Length**	**Primary Key**	**Foreign Key**
Board_Num	Integer	4	Yes	Yes
Sensor_Num	Integer	4	Yes	Yes
Sensor_Type	Char	40	No	Yes
Installed	Char	15	No	No

Figure 3: Sensor Installation Details

Table Name : Sensor Type Reference Table

Attribute	**Attribute Type**	**Field Length**	**Primary Key**	**Foreign Key**
Sensor_Type	Char	40	Yes	Yes
Sensor_Name	Char	40	Yes	No

Figure 4: Sensor Type Reference Table

4.1.4.3 Reports Structure

The report layout, produced by the ICCSM, is attached as Appendix A of this document.

4.2 Environment

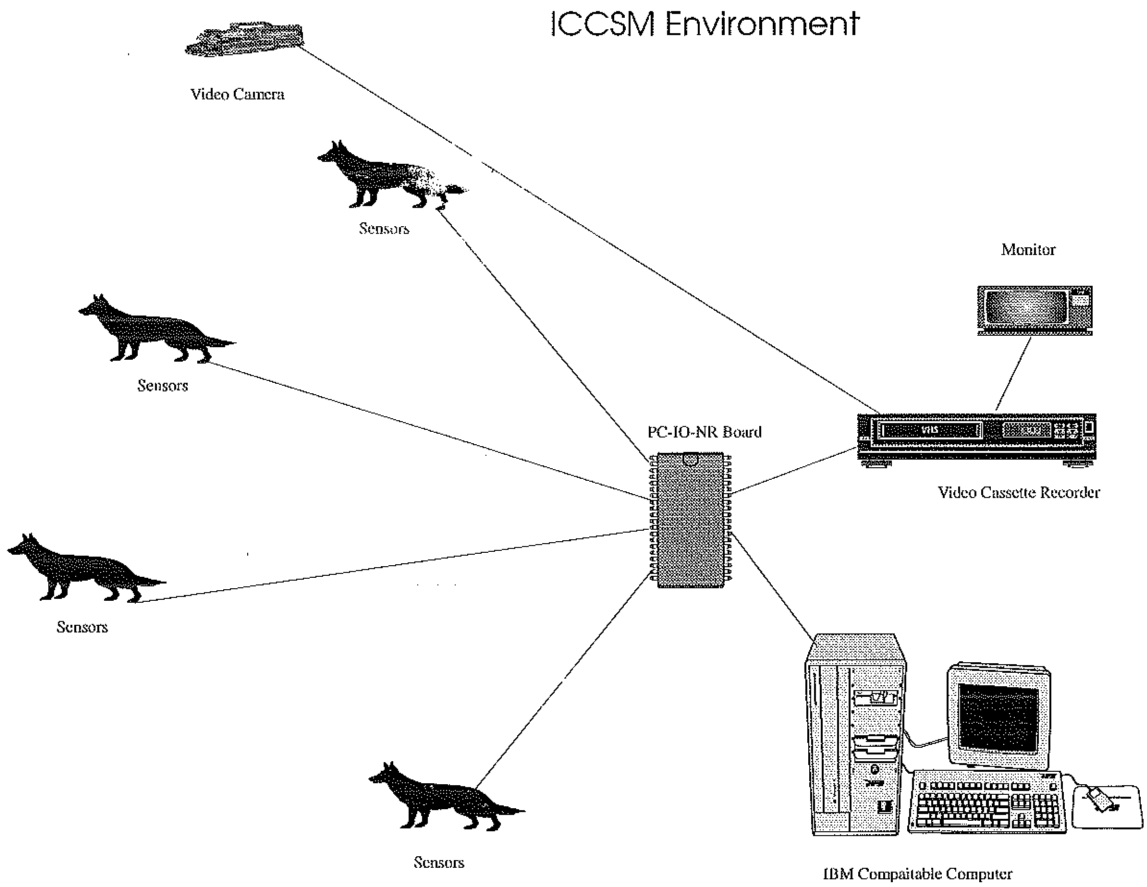

Figure 5: Hardware Setup of the ICCSM Environment

4.2.1 Equipment

4.2.1.1 Hardware Utilised

The ICCSM environment utilises general purpose hardware and a special VCR. An external board, PC-IO-NR, formulates the link between the sensors and an IBM compatible computer under Microsoft Windows environment.

4.2.1.2 The Hardware Setup

IBM or IBM Compatible Personal Computer (PC)

An IBM or IBM compatible PC with at least 4 megabytes of Random Access Memory (RAM) is necessary to execute the ICCSM software and to manipulate the hardware. It is strongly recommended to use a 486-DX or 486-DX:2 machine with a clock speed of 33 MHZ or higher to cope with the extensive processing required by the ICCSM environment.

PC-IO-NR IO Board

The PC-IO-NR board provides the means of controlling electrical devices from a computer using a relay ladder logic style of programming and

is required to connect motion detectors with a PC. The PC can monitor inputs from the detectors and can set the output conditions, such as switching the VCR and lights on or off.

The PC-IO-NR board requires an IBM PC or compatible machine with a DOS version 2.1 or higher. The board is mounted externally to the PC and connects to any suitable bi-directional printer port. In this project Procon's PC-BD-IO bi-directional interface card was utilised for increased reliability. As the board was mounted externally, it was easier to mount or unmount the motion detectors.

Each I/O board provides eight isolated inputs and eight isolated outputs. However additional boards can be connected to one PC-BD-IO card for expansion up to 120 inputs and 120 outputs. Four DIP switches select each board address setting on the PA-BUS, allowing up to 15 boards to be connected to a single interface card. The research environment catered for eight PC-IO-NR boards limiting the inputs and outputs to 64. All I/O has LED status indication showing the current status of Input or Output.

The input/output options include: 5 or 12 Volt input/output, a definite advantage if a sensor requires 5 Volt input (a normal sensor requires 12 Volt input). The board also provides input filtering resulting in complete electrical isolation. This allows the input devices to be situated up to thousands of

metres from the I/O board and protects the computer against noise and voltage spikes. The I/O board can be controlled directly from any high-level language that provides direct serial input/output port control.

PC-BD-IO Card

The PC-IO-NR board can damage a PC if input indication remains on whilst connected to a standard parallel port. The PC-BD-IO card is designed to prevent any harm to the PC and is a bi-directional parallel port. This card is necessary to connect a PC and the PC-IO-NR board and is a reliable link between the two of them.

Video Cassette Recorder (VCR)

The video recorder for the research environment is Panasonic's AG-6720A. Besides the standard 3-hour recording mode in VHS and S-VHS, the VCR also supports intermittent recording (for 14-, 24-, 72-, 120-, 180-, 240-, 480- hours, or 1 shot modes). All the various mode settings, including the recording times of the internal timer, the alarm recording mode and the sensor recording mode, can be programmed.

Built-in timer recording times, recording time modes, alarm recording modes, sensor recording modes and other data can be retained in the video

memory semi-permanently. In a power failure situation the VCR retains the contents of its memory for a month.

In long time recording mode when an intrusion is detected by the detectors, the VCR is automatically shifted from slower recording mode to normal recording mode to record the state of abnormality in detail. Switching from slow recording mode to normal recording mode by the VCR is shown in Figure 6 below.

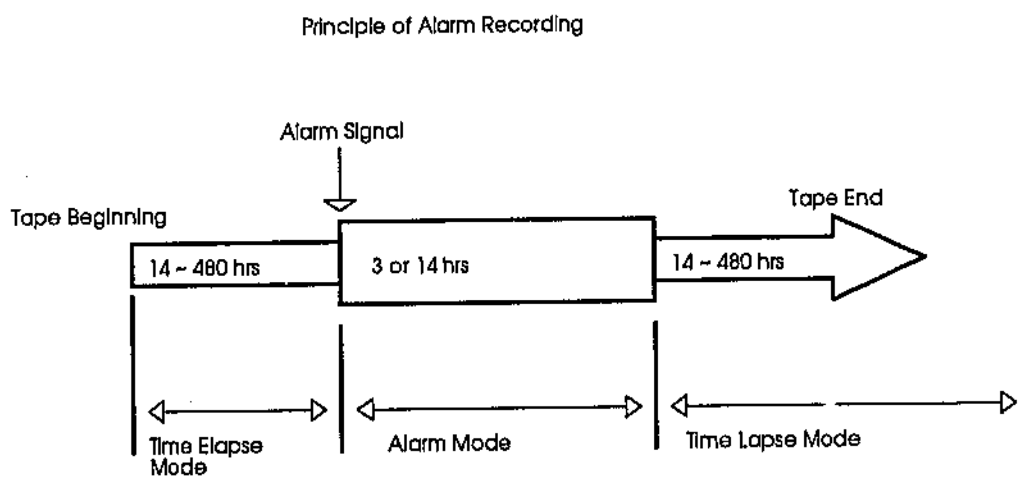

Figure 6: Principle of Alarm Recording

Monitor

The computer controlled monitoring system requires a separate display screen to view the intrusions captured by the video recorder. The monitor utilised by the ICCSM is Panasonic's BT-M1420PY. The monitor can be switched between line A and B inputs, RGB input, or VCR input - which is switchable between Super VHS and conventional video.

Video Camera

Panasonic's WV-CL350 video camera captures the live images for the ICCSM environment. The camera has signal-to-noise ratio of 46db, which is important when the ICCSM system is in operation in a factory or warehouse.

VCR Control Module

During the research it was observed that there was a delay of four seconds between detecting an intrusion and switching the VCR into normal recording mode. A special module was developed to speed up the process. Figure 7 is the diagram of the VCR Control Module.

The input to 74 LS 244 are held high by the pull up resistor on the input lines.When an alarm occur this cause one of the input line to go low.

The 74 HC 373 is wired in parallel with the connection to the input of the 74 LS 244 this causes the low input to be presented to the input on the HC 373. The enable line is tied to ground, when the chip is enable, as latch enable is tied to ground through the inverter, causes a high at the input to latch enable, this enables the latch output of the HC 373. So when a low or high is presented to the inputs of the HC 373 then it is passed through to the input of the 74 LS 30

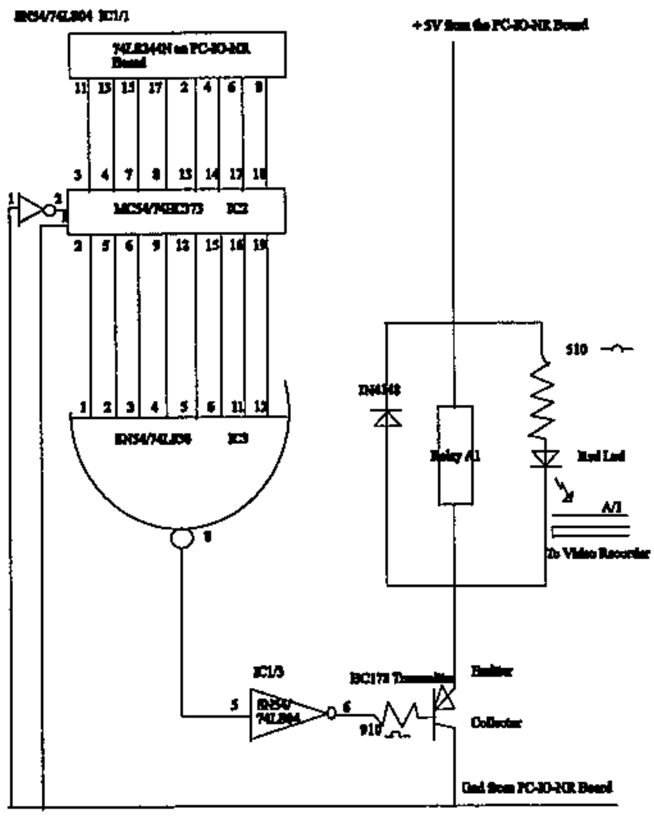

Figure 7: VCR Control Module

The 74 LS 30 is an 8-Input Nand Gate. The output from the 74 LS 30 is low if all the inputs are high, and high if one or more inputs are low. The output from the 74 LS 30 Nand Gate is passed onto 74 LS 04 Hex Inverter.

The output from the 74 LS 04 Hex Inverter is passed on to BC 178 transistor The transistor is acting as a switch. The output from the 74 HC 373 will be low, then the output from the 74 LS 30 chip will be high. The 74 LS 04 Hex Inverter will invert the signal from high to low.

When output from the Hex Inverter is high the transistor will turn off causing the Relay to be turned off. When output from the Hex Inverter is low the transistor turns on the current flow through the Relay Coil, through the Emitter of the transistor to the Collector to ground and the Relay contacts are open. The high is passed on to the VCR, which switches from slower recording mode to normal recording mode immediately.

4.2.2 Software

4.2.2.1 Software Developed

The Integrated Computer Controlled Sensor Monitor is developed to sense input signals from the detectors and respond accordingly. It records the information into a database and shifts the VCR to normal recording mode. Software routines are written in assembler, C, SQLWindows and also includes utilities from Microsoft and Procon Software. The ICCSM is a real time monitoring environment. The developed software and the components required to run the ICCSM are:

- Integrated Computer Controlled Sensor Monitor's executable (ICCSM.EXE), SQLWindows dynamic link libraries, Simulation environment (SIMULATE.EXE), production environment (PRODUCT.EXE), Adjust boards (ADJBOARD.EXE) and help (HELP.HLP) executable files (the software is written and compiled by Microsoft Assembler, Borland C++ and SQLWindows),
- Microsoft Window's System Diagnostics Utility (MSD),
- Microsoft Windows 3.1 or over,
- Windows Help (WinHelp) utility and
- SQLBase Database.

The research specifications were used to construct the ICCSM environment. The developed software executes under Microsoft Windows only. The user input from the keyboard is kept to a minimum to reduce the possibility of human typographical errors.

4.2.3 System Functions

Upon initial loading of the ICCSM software, the user will see the Main Screen as shown in figure 8 below, which acts as the control centre for the ICCSM environment. This screen consists of a title bar and pull down menus. Mouse users can move the pointer to the title of the menu and click the desired option to pull the menu down.

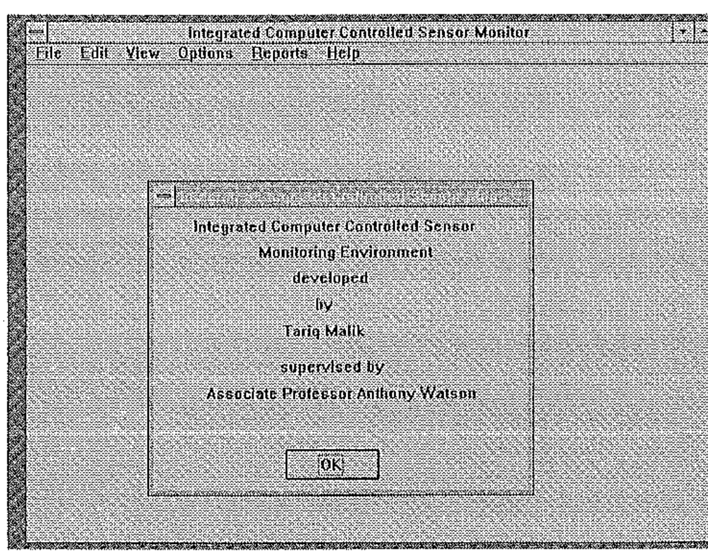

Figure 8: The ICCSM Environment - Main Screen

Figure 9 is an example of a pull down menu. By selecting an item from the pull down menu corresponding functions can be invoked.

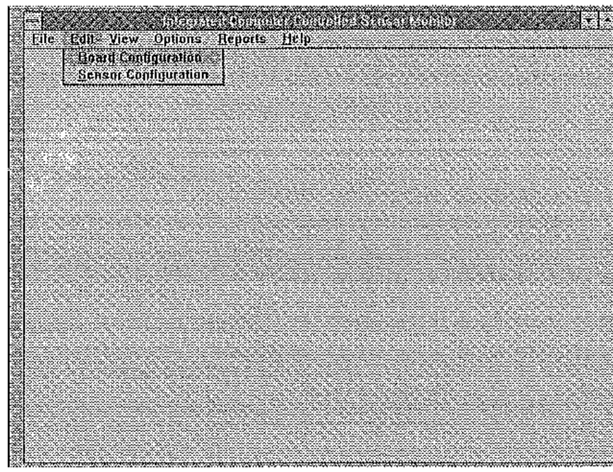

Figure **9**: Pull Down Menu Screen

4.2.3.1 Edit Sensor Configuration

After selecting 'Edit' from the Main Screen and then selecting "Sensor Configuration", a screen such as shown in figure 10 will be displayed.

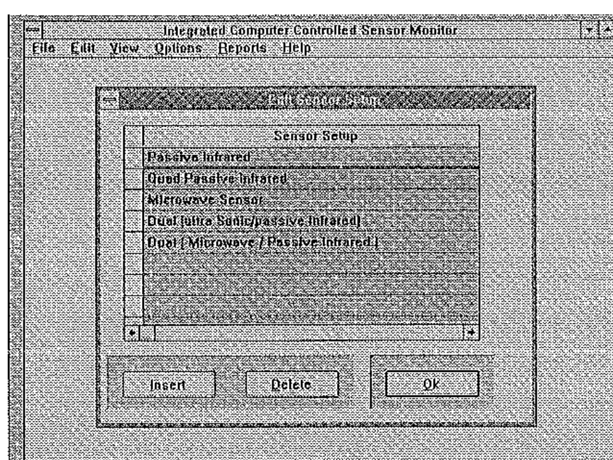

Figure **10**: Edit Sensor Setup

Edit Sensor Setup (see figure 10) is a data entry screen which the user must complete for each new sensor connected to the ICCSM environment. The ICCSM database can be expanded to any length

and new sensors can be added or deleted from it. Thus, a user can have many different types and brands of sensors for a single technology type.

4.2.3.2 Edit Board Configuration

The sensors monitored by the ICCSM environment have to be connected to special boards, called PC-IO-NR boards (see section 4.2.1.2). At a site, any type of sensors may be installed. The Edit Board Configuration window is to record the sensor details into the database. It requires information such as name of a sensor, sensor type and its location. This information is vital for the ICCSM functions.

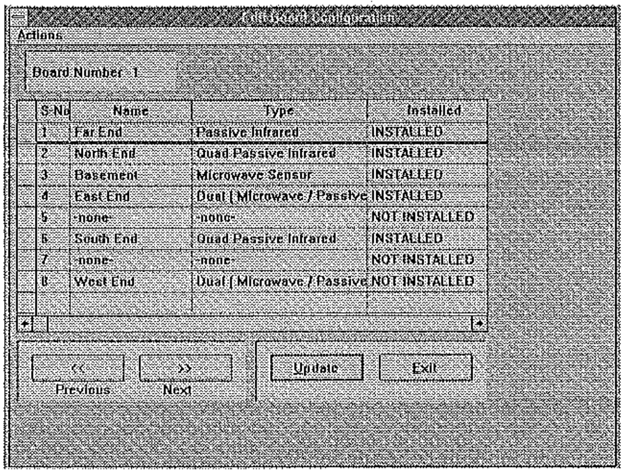

Figure 11: Edit Board Configuration

The "Update" push button (see figure 11) updates the database. The

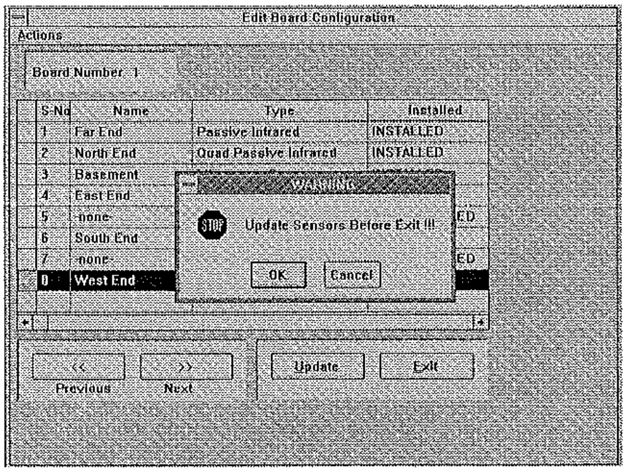

Figure 12: Error Message

"Exit" push button exits without updating the database. If a change has been made and the "Exit" push button is pressed then a window with an error message, *Error Message* screen (see figure 12) will be displayed. The user can either cancel the update or accept the exit thus abandoning the changes.

4.2.3.3 View board Configuration

After selecting the "View" pull down menu from the Main Screen and then selecting "Board Configuration", the *View Board Configuration* screen (see figure 13) will be displayed. This screen does not allow the user to update the database. The "Previous" and "Next" push buttons flick through eight boards. The displayed information is retrieved from the ICCSM database and can be updated through the "Edit Board Configuration" option.

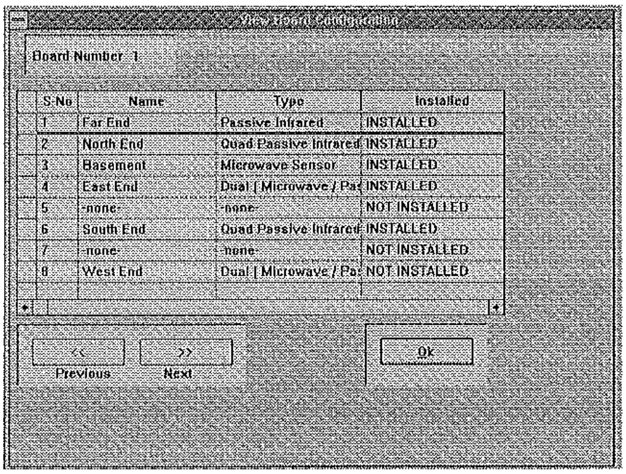

Figure 13: View Board Configuration

4.2.3.4 PC's Diagnostics Utility

After selecting "View" pull down menu from the Main Screen and then selecting "System Configuration", the *System Diagnostics Utility* screen (see figure 14) will be displayed. This screen examines the hardware and installed resident programs in the PC's memory. The user can take advantage of this information to correct any interrupt or base address conflicts in the Random Access Memory (RAM). It also displays number of Input/Output ports, computer type, RAM size etcetera. Microsoft's MSD is executed by the ICCSM as the diagnostic option.

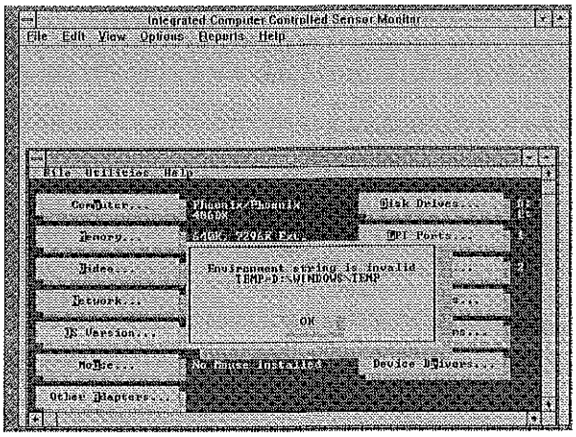

Figure 14: System Diagnostics Utility

4.2.3.5 Performing Experiments

The ICCSM environment operates in two modes, Simulation and Production. While operating in simulation mode the ICCSM can be utilised as a workbench.

Simulate Experiments

Five environmental experiments can be simulated for the ICCSM environment. The "Simulation" option pulls down another pull down menu (see figure 15). The next menu lists the possible environmental experiment types. The user is required to select an experiment type to continue. Mouse users can simply click the desired option.

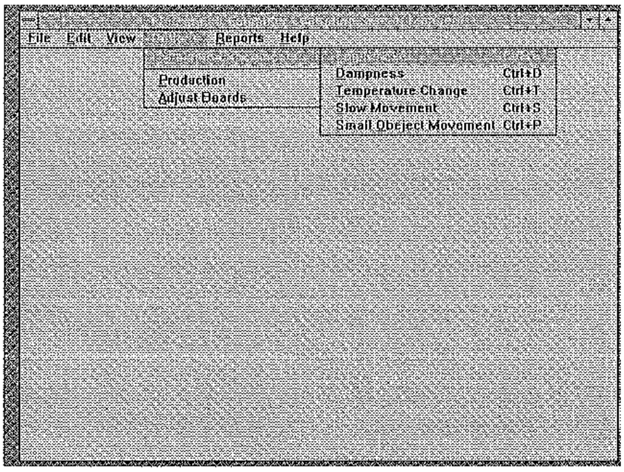

Figure 15: Simulation Experiment Types

After selecting an experiment type the *Experiment Criteria* window (as shown in figure 16) will be displayed. Every simulated experiment performed by the ICCSM environment requires a scale to measure its performance. Thus, user is requested to enter experiment criteria. For example, the user has to enter the current, minimum and maximum temperatures expected for the temperature change experiment (see figure 16).

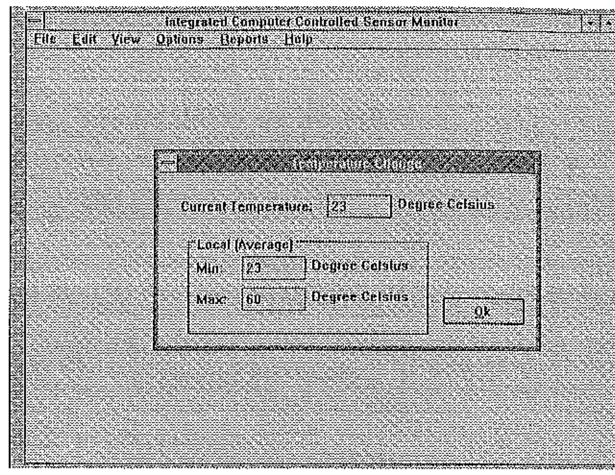

Figure **16**: Experiment Criteria

After entering the experiment criteria (see figure 16), simulation of the experiments can start. The sensor details must have been recorded through the "Edit Board Configuration" option. If the entry for the

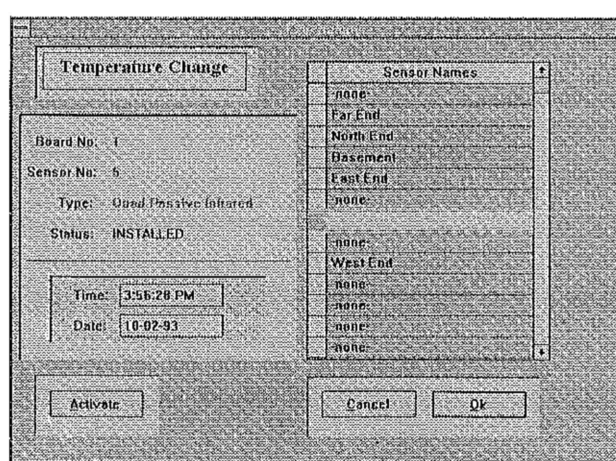

Figure **17**: Sensor Selection

sensor states "Not Installed" then the push button to activate an experiment will stay in the background mode and the user cannot accidentally start an experiment. If the sensor is physically not connected, the ICCSM software will detect that and will not start the simulation. Thus, no false alarms will be triggered.

Once an installed sensor is selected from the sensor list, the "Activate" push button on the bottom left of the menu is highlighted. Pressing of the "Activate" push button will commence simulation of experiments. The simulation results are recorded into the database for the effective use by the ICCSM environment. Simulation Experiment screen (see figure 18) displays intrusion details such as, Alarm Number, Sensor Location, Detector Type, Intrusion Date and Intrusion Time. Pressing "Alt F4" or clicking the top left corner of the simulation window at any time will stop the simulation.

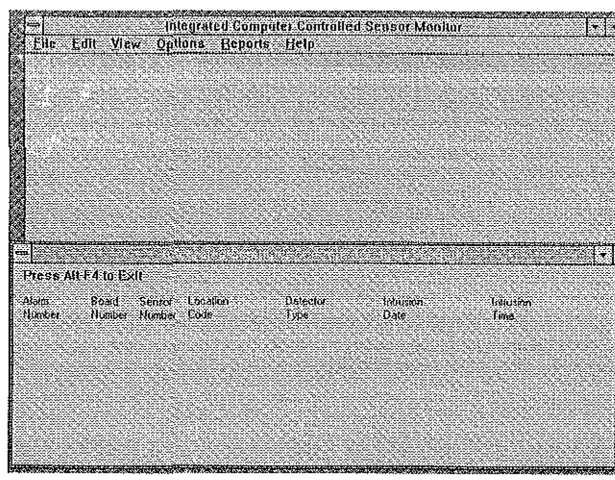

Figure **18**: Simulation Experiment

Production Environment

The production environment is to monitor the entire detection system without human intervention. The system can be left in operation for a maximum of one week.

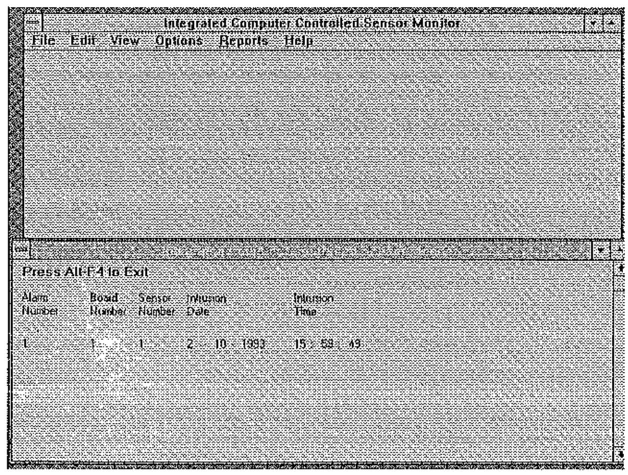

Figure **19**: Continuous Monitoring (Production Environment)

The production environment activates immediately after the user selects the production option from the options pull down menu. The ICCSM is an automatic log system when operating in production mode. The automatic log produced by the system can be utilised to help determine the causes of false alarms at a site. Continuous Monitoring screen (see figure 19) displays an intrusion detected by the ICCSM environment. Pressing "Alt F4" or clicking the top left corner of the production window at any time will stop the continuous monitoring.

4.2.3.6 Adjust Boards

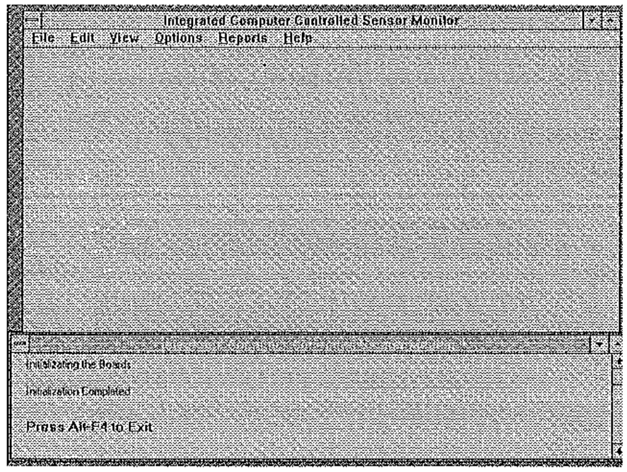

Figure **20**: Initialise Boards

If the security administrator fumbles and presses a wrong key while sensor monitoring is in progress or a power failure has occurred, the PC-IO-NR board configuration can change incorrectly. The 'Adjust Boards' option re-initialises all the devices connected to PC-IO-NR boards to their original status, including sensors and video cassette recorder. Initialise Boards screen (see figure 20) displays the initialisation of Input/Output devices. Pressing "Alt F4" or clicking the top left corner of the *Initialise Boards* window will pass the control back to Main Screen.

4.2.3.7 Help Index

The ICCSM software is GUI (Graphical User Interface) based and is easy to use. After selecting "Help" pull down menu from the Main Screen and then selecting "Index", *Help Index* (see figure 21) will be displayed. The *Help Index* screen explains the ICCSM environment and available ICCSM options. The help program has been written and compiled using Microsoft's help compiler, with hyper links to jump from one help topic to another.

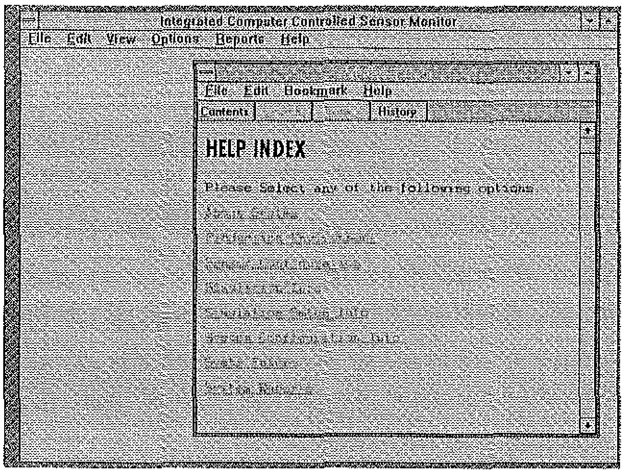

Figure **21**: Help Index

4.2.3.8 About Help

The *About Help* screen (see figure 22) explains how to use the ICCSM help.

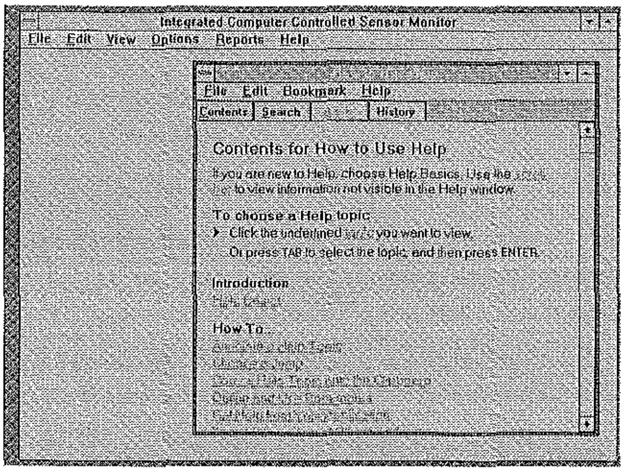

Figure **22**: About Help

4.2.3.9 Reports

The ICCSM environment produces three different types of reports. After selecting "Reports" pull down menu from the Main Screen, the *Report Types* screen (see figure 23) will be displayed. The *Report Types* screen displays the pull down menus listing different types of reports available.

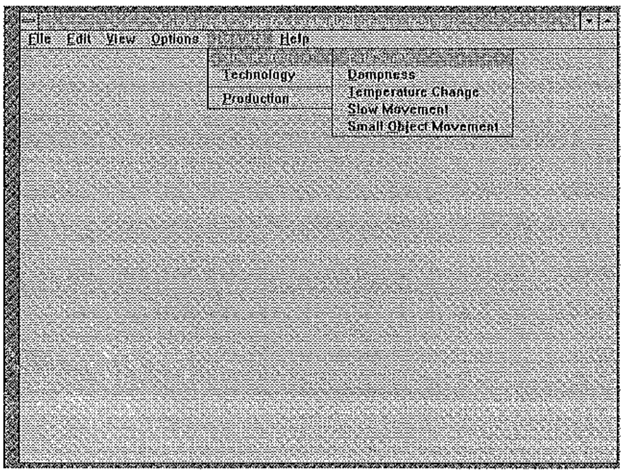

Figure 23: Report Types

Report by Sensor Type

After selecting "Report" pull down menu from the Main Screen and then "Sensor Type", the *Report by Sensor Type* (see figure 24) will be displayed. The user is required to select the desired sensor type. The report contents will include all the detected intrusions for that particular sensor. The information will include date, time, location and nature of the experiment.

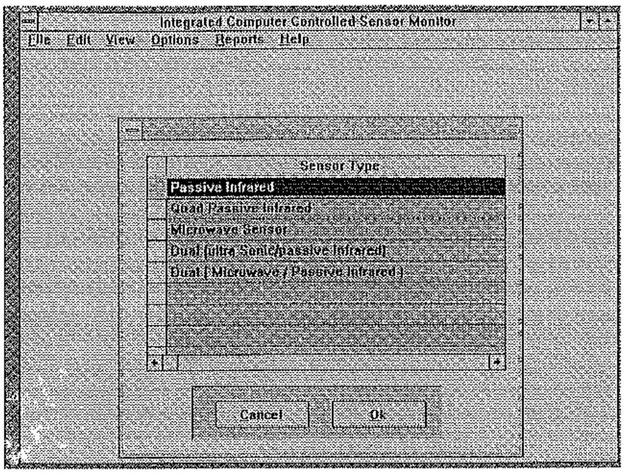

Figure 24: Report by Sensor Type

The *Report by Sensor Type* screen (see figure 25) displays a sample report for the Passive Infrared Detectors. The output of the report can be sent to a printer by selecting "Print" pull down menu from *Report by Sensor Type* screen.

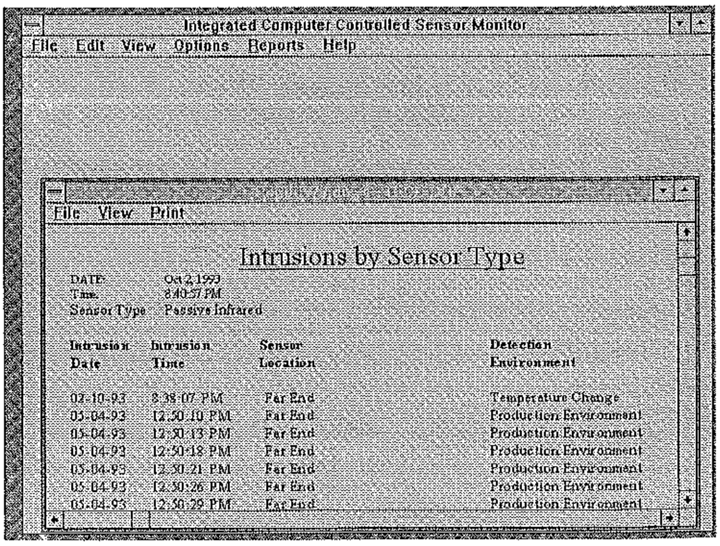

Figure 25: Report by Sensor Type

Report by Experiment Type

After selecting "Report" from the Main Screen and then "Simulation Experiments", another layer of menu will be displayed (see figure 22). Select the desired experiment type. The simulation experiment report details the sensor location, experiment criteria, sensor type, intrusion date and intrusion time.

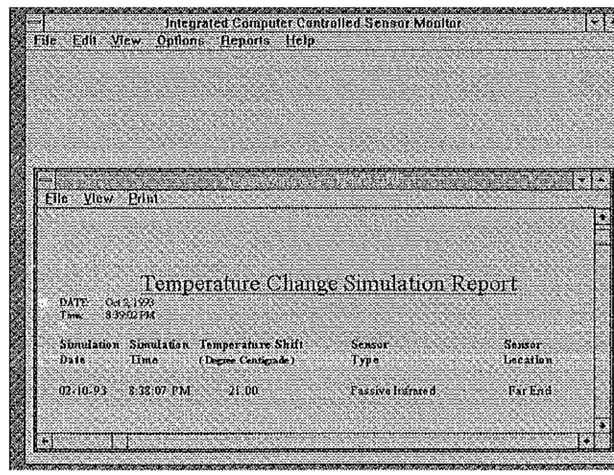

Figure 26: Simulation Report

The *Simulation Report* screen (see figure 26) is displaying a sample report for the temperature change experiments. The output of the report can be sent to a printer by selecting "Print" pull down menu from the *Simulation Report* screen and then selecting "Print" again.

Report by Date

After selecting "Report" pull down menu from the Main Screen and then "Date", the *Data Entry for Report by Date* screen (see figure 27) is displayed. The user is required to enter a date for which a report shall be provided in *Data Entry for Report by Date* screen.

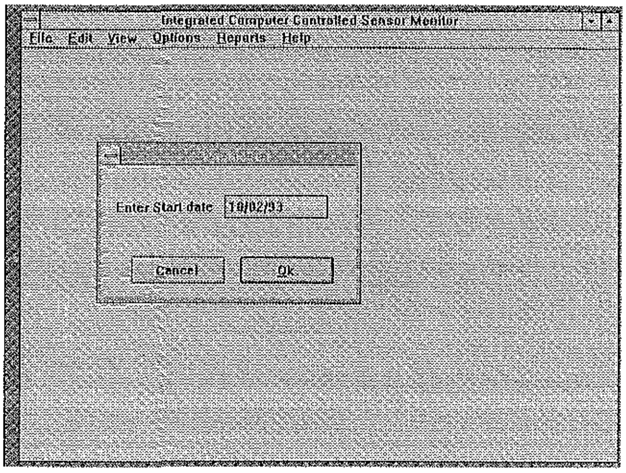

Figure 27: Data Entry for Report by Date

The *Report by Date* screen (see figure 28) is displaying a sample report. The output of the report can be sent to a printer by selecting "Print" from the pull down menu and then selecting "Print" again.

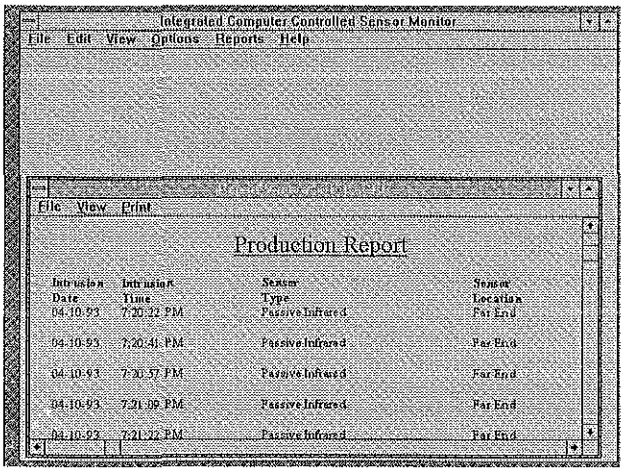

Figure 28: Report by Date

4.2.3.10 Printer Setup

A report can be directed to the PC monitor and to a printer. If the computer has access to a network printer, the output can be redirected to the network printer.

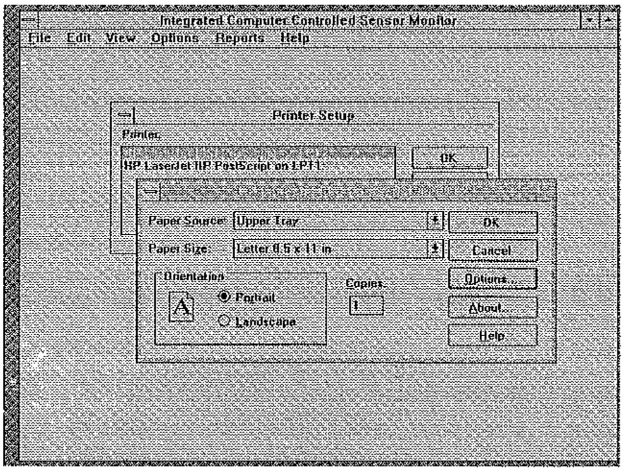

Figure **29**: Printer Setup

Select "File" from the pull down menu and then select "Printer Setup", the *Printer Setup* screen (see figure 29) will be displayed. The *Printer Setup* screen is displaying a sample setup for HP LaserJet IIIsi printer.

4.2.4 System Testing

The EXECOM methodology (1991-1993) breaks the testing process into five phases.

- Program or Module Testing - to test the system modules and programs,
- Function Testing - to assure that the system functions perform in accordance with the functional requirements,
- System Testing - various aspects of the system such as hardware and software interaction is tested to validate the system functionality,
- Acceptance Testing - confirm that the system satisfies the requirements specification and
- Installation Confirmation - confirm that the system has been installed correctly, the required hardware configuration is present, and files and libraries have been allocated and loaded.

4.2.4.1 Program or Module Testing

Individual unit testing was conducted on the modules written for the ICCSM environment. The name and the purpose of the modules are:

SQLWindows Interface

The front end interface is comprised of SQLWindows. The executable name is ICCSM.EXE and is the driving program of the ICCSM environment. The SQLWindows interface calls the other programs, for example Simulate.exe and Product.exe, and automatically updates the database.

Simulate.c

This module is written in "C" and executes library routines defined by pcioc.asm for sensor status monitoring and also handles the VCR. This module allows the user to simulate known false alarm conditions to fine tune a sensor.

Product.c

The name of the module stands for production environment and monitors the status of every installed sensor. This module switches the video recorder on or off if the sensor status changes. It is written in C and utilises the library routines defined by pcioc.asm.

AdjBoard.c

Another C module, initialises the sensors and video recorder to no intrusion status.

Pcioc.asm

Assembler routines to perform low level input and output from multiple PC-IO-NR boards.

Help.hlp

A help program written in rich text format with hyper links. It was compiled by Microsoft's Help Compiler.

4.2.4.2 Function Testing

Function testing is the next step up in the testing process where modules are put together to form the system and the system is compared against the functional specification.

The ICCSM environment was tested and validated against the functional specification of the ICCSM environment.

4.2.4.3 System Testing

Numerous tests were performed to ensure the software and hardware interaction. This phase is more concerned with finding errors which result from unanticipated interactions between different hardware software components.

4.2.4.4 Acceptance Testing

Acceptance testing is the process of testing the system with real data - the information which the system is intended to manipulate.

No real test with the sensors were conducted due to the difficulty in simulating the environmental conditions in a university environment. Such testing is outside the boundary of this project.

5 ICCSM SUMMARY

5.1 About ICCSM

Integrated Computer Controlled Sensor Monitor (ICCSM) is a GUI based sensor monitoring environment, consisting of an interface between a PC and a number of sensors. The alarm events are analysed to reduce the false alarm rate of motion detection sensors.

ICCSM allows the user to simulate a range of experimental conditions to adjust sensor sensitivity levels, perceiving the means to examine the integrity of a detection system. The ICCSM environment includes a database which was designed to add and delete the sensor information. The intrusion information is automatically updated after every detected intrusion. The ICCSM also provides the written reports to the user along with few other useful options.

The ICCSM environment is a combination of general purpose hardware, including a PC, an interface between a PC and a range of sensors, a VCR, and a video camera. The detected intrusions information is record into the database, such as detector location, date and time of an alarm. The intrusion or the event which triggers the sensor is also captured on VCR for future verification.

The ICCSM environment is aimed at improving the quality of security systems by using alarm monitoring facilities to quality check the accuracy of any attached sensors.

Limited tests were conducted using the ICCSM environment due to the difficulty in simulating the environmental conditions in a university. Comprehensive testing of the ICCSM is outside the boundary of this project. Detailed performance testing can be performed by security agencies or the vendors of the various sensors. Some sample forms have been designed to conduct the simulation experiments. It is intended that the security agencies may utilise this format to simulate environmental conditions to perform environmental tests on the sensors.

TEMPERATURE CHANGE EXPERIMENT

Table 1: Temperature Change Experiment Table

Experiment Type	:	Temperature Change Experiment;
Experiment Date	:	xx/xx/xx;
Detector Type	:	xxxxxxxxxxx;
Detector Location	:	xxxxxxx;

Alarm No	Detector Range (metres)	Heat Source Distance (metres)	Simulation Startup Time (hh:mm:ss)	Startup Temperature (celsius)	Maximum Temperature Reached (celsius)	Time acquired for Maximum Temperature (hh:mm:ss)	Temperature Shift (celsius)	Result
1	6	7	12:04:12	23	44	00:00:20	21	Alarm
2	6	8	12:20:32	23	44	00:00:20	21	Alarm
3	6	9	01:15:22	23	44	00:00:20	21	No Alarm
4	6	7	02:02:56	23	26	00:04.23	3	No Alarm

5.2 Outcome of the Limited Testing

Some analyses are presented for the temperature change experiment. For the temperature change experiment, table 1, the first alarm was triggered when the detector's detection range is 6 metres and a heat source is at 7 metres from the detector. When there was a temperature shift of 21 °C within 20 seconds an alarm was detected. The heat source is 8 metres away from the detector for the second test. The temperature shift was exactly the same and an alarm occurred. In the fourth test the heat source is at 9 metres and there was no alarm. Whereas in the fifth test the sensor range was 6 metres and the heat source at 7 metres with a temperature change of 3 °C in 4.23 seconds and there was no alarm. The conclusion from this test would be that either the sensitivity level of the sensor should be reduced from 6 metres or the sensor can be moved to a different location not facing the heat source. The second solution can be to move the heat source reasonably away from the detector range so that it cannot effect the detector or to adjust the temperature variation of the heat source to a uniform rate.

5.3 Conclusion

The literature indicates that an effective alarm monitoring system can improve the performance of individual motion detectors. The performance of a particular detector is dependent upon the environment in which it is operating. Motion detectors are affected by weather and everyday human activities causing nuisance alarms, false alarms, and degraded detection. Even a high grade detector will display poor

performance if it is not calibrated and maintained for the conditions it may encounter.

The aim of this research is to design and develop a computer controlled monitoring environment to improve the quality of security systems for sensor devices. The ICCSM environment assists the security administrators by providing following facilities:

Automatic Data Gathering

Validating the Physical placement of Sensors

Assistance for Post-Installation Maintenance of Security Sensors

Automatic Data Gathering

The ICCSM environment is designed to isolate the environmental factors causing false alarms through the use of automatic data capture. It will help security agencies to determine the weaknesses in individual detection technologies and thus fine tune the performance of a security system. The ICCSM environment automatically records the intrusion data and also records the video images of the intrusion. The user can analyse the recorded data to identify the cause of an alarm.

Validating the Physical Placement of Sensors

The ICCSM, functioning as a workbench, can be utilised to simulate known false alarm conditions or to leave the performance monitoring system switched on for a test period. The ICCSM reports are there to assist the security administrator to validate the physical layout of the sensors.

Assistance for Post Installation Maintenance

ICCSM is designed to provide a mechanism to monitor and to gather data about the performance of sensors. The past and present performance data of sensing devices can be used to verify the quality of the sensor hardware and detection capability.

A computer controlled monitoring environment and improved sensing devices can reduce the false alarm rate by providing automated data gathering facilities. The user's interpretation of sensor data will determine the improvement in the quality of detection systems.

6 REFERENCES

Alexander, P. (1990). External intrusion detection systems for critical facilities. *Proceedings: 1990 Carnahan Conference on Security Technology* (pp. 139-140). Kentucky, USA: University of Kentucky.

Arlowe, H. D. & Coleman, D. E. (1990). The Mobile Intrusion Detection and Assessment System (MIDAS). *Proceedings: 1990 Carnahan Conference on Security Technology* (pp. 54-58). University of Kentucky, USA.

Barakati, N. (1991). *Unix Desktop Guide to X/Motif.* Indiana, USA: Hayden Books.

Bernard, R. L. (1988). *Intrusion Detection Systems.* Boston: Butterworths Publishers.

Bloom, L. M., Cross, J. M. & McDougall, D. (1991). *An Analysis of the monitored Electronic Alarm Activation in the Perth Metropolitan Area*, Perth, Western Australia: Edith Cowan University.

Blundell, L. (1990, February). Alarm Report : Goodbye to the good old days. *Security Australia*, pp. 32, 34.

Bone, M. (1990, June). The Finger on the Pulse. *Security Gazette*, pp. 24-25.

Carter, R. (1991, December). Wasting Police Time? *Security Gazette*, pp. 511-512.

Challenges facing the Alarm Industry (1988, June). *Security Gazette*, pp. 19, 28.

Custance, N. D. E. (1988). Perimeter detection systems: Correlation of false alarm cause with environmental factors. *Proceedings: 1988 Carnahan Conference on Security Technology* (pp. 89-97). Kentucky, USA: University of Kentucky.

Custance, N. D. E. & Leach, G. H. (1990). Image Surveillance Systems; Some novel design features. *Proceedings: 1990 Carnahan Conference on Security Technology* (pp. 93-97). Kentucky, USA: University of Kentucky.

Ellis, T. J., Rosin, P. L. & Golton, (1990). Model Based Vision for Automatic Alarm Interpretation. *Proceedings: 1990 Carnahan Conference on Security Technology* (pp. 62-67). Kentucky, USA: University of Kentucky.

EXECOM. (1991-1993). *Student APT by EXECOM.* Perth, Western Australia: EXECOM.

False Alarms : It's the user who holds the key (1988, June). *Security Gazette*, pp. 25-27.

Fay, J. J. (1987). *Butterworths Security Dictionary: Terms and Concepts.* Boston: Butterworths Publishers.

Friedl, W. J. (1989). Is it possible to reduce false alarms. *Proceedings: 1989 Carnahan Conference on Security Technology* (pp. 37-40). Kentucky, USA: University of Kentucky.

Galloway, D. (Producer). (1992). *Beyond 2000* [Film]. Sydney: Beyond International Group, Sydney.

Hughes, D. & Bowler, P. (1982). *The Security Survey.* England: Gower Publishing.

Jackson, I. (1990, June). A Dial-Up Solution for the Alarm Controllers. *Security Gazette*, pp. 27-28.

Jonckheere, M. T. A. & Weeden, M. R. (1985). Automated Performance Monitoring of Electronic Security Systems. *Proceedings: 1988 Carnahan Conference on Security Technology* (pp. 81-87). University of Kentucky, USA.

Lynn, J. K. (1988). Smart Sensor Systems for Outdoor Intrusion Detection. *Proceedings: 1988 Carnahan Conference on Security Technology* (pp. 45-49). University of Kentucky, USA.

Matching the system with the environment (1988, June). *Security Gazette*, pp. 22-23, 28.

Morton, E. H. (1984). *An Integrated Security Display and Control System. Proceedings: 1984 Carnahan Conference on Security Technology* (pp. 29-33). University of Kentucky, USA.

Moss, B. (1990, May). Dual Technology Sensors Reduce False Alarms Ease Detection Challenges. *Security*, pp. 54-58.

Newman, M. (1992, February). Breaking out of the false alarm jungle. *Security Gazette*, pp. 35-36.

Oliver, E. & Wilson, J. (1988). *Practical Security in Commerce and Industry.* USA: Gower Publishing Company.

Owen, J. W. (1986). Physical security applications of personal computers. *Proceedings: 1989 Carnahan Conference on Security Technology* (pp. 65-69). University of Kentucky, USA.

Patten, W. A. & Folea, R. V. (1989). An Infrared Imaging Sensor for Detecting and Classifying Intruders in Tactical and Strategic Applications. *Proceedings: 1989 Carnahan Conference on Security Technology* (pp. 19-22). University of Kentucky, USA.

Russell, R. D. (1991, May). Industry Strive to reduce False Alarms. *Security*, pp. 43-44.

Sanders, A. H. (1987). Final testing of a multi-sensor perimeter intrusion detection system. *Proceedings: 1987 Carnahan Conference on Security Technology* (pp. 11-13). University of Kentucky, USA.

Saucier, M. R. (1991). Microwave based sensors, technology and applications. *Electro International Conference Record* (pp. 655-660). Electron Conventions Manage, USA.

Standards Association of Australia (1986). *Intruder Alarm Systems Part 1 - Systems Installed in Client's Premises* (Australian Standards 2201.1). North Sydney: Standards Association of Australia.

Steiner, P. & Wagli, P. (1983). *New developments in Ultrasonic and Infrared motion detectors*. Proceedings: 1983 Carnahan Conference on Security Technology (pp. 101107). University of Kentucky, USA.

Trimmer, H. W. (1981). *Understanding and Servicing Alarm Systems*. Boston: Butterworths Publishers.

Walker, P. (1988). *Electronic Security Systems*. London: Butterworths Publishers.

Warnock, W. J. (1992, September). Silencing False Alarms. *Security*, pp. 116-117.

Weber, T. L. (2nd ed). (1985). *Alarm Systems and Theft Prevention*. Boston: Butterworths Publishers.

APPENDIX A - EXPERIMENT FORMS

FOG/SMOKE EXPERIMENT

Table 2: Fog/Smoke Experiment Table

Experiment Type : Fog/Smoke;
Experiment Date : xx/xx/xx;
Detector Type : xxxxxxxxxxx;
Detector Location : xxxxxxx;

Alarm No	Detector Range (metres)	Object Distance when detected (metres)	Fog/Smoke Level (High/Moderate/Low)	Temperature at Object Detection (celsius)	Intrusion Startup Time (hh:mm:ss)	Intrusion Detection Time (hh:mm:ss)	Detection Time Difference (hh:mm:ss)
1	2	1.5	High	23	23:04:56	23:05:44	00:01:12

RAIN/DAMPNESS EXPERIMENT

Table 3: Rain/Dampness Experiment Table

Experiment Type : Dampness Experiment;
Experiment Date : xx/xx/xx;
Detector Type : xxxxxxxxxxx;
Detector Location : xxxxxxx;

Alarm No	Detector Range (metres)	Object Distance when detected (metres)	Dampness Level (SlightlyMoist/Moist/Wet)	Temperature at Object Detection (celsius)	Intrusion Startup Time (hh:mm:ss)	Intrusion Detection Time (hh:mm:ss)	Detection Time Difference (hh:mm:ss)
1	6	1.5	Wet	23	23:04:56	23:05:44	00:01:12
2	12	9	Slightly Moist	23	00:25:42	00:26:03	00:00:21

SLOW MOVEMENT EXPERIMENT

Table 4: Slow Movement Experiment Table

Experiment Type	:	Slow Movement;
Experiment Date	:	xx/xx/xx;
Detector Type	:	xxxxxxxxxxx;
Detector Location	:	xxxxxxx;

Alarm No	Detector Range (metres)	Object Distance when detected (metres)	Object Speed (metre/min; feet/min; inches/min)	Object Colour	Simulation Startup Time (hh:mm:ss)	Simulation Detection Time (hh:mm:ss)	Detection Time Difference (hh:mm:ss)	Sensitivity Level (High; Medium; Low)	Result
1	3	-	inches/min	Black	05:30:45	-	-	Medium	No Alarm
2	3	2.5	feet/min	White	06:04:23	06:06:24	00:02:01	High	Yes
3	5	3	feet/min	White	06:20:00	06:26:00	00:06:00	Medium	Yes

SMALL ANIMALS MOVEMENT EXPERIMENT

Table 5: Small Animals Movement Experiment Table

Experiment Type	:	Small Animals;
Experiment Date	:	xx/xx/xx;
Detector Type	:	xxxxxxxxxxx;
Detector Location	:	xxxxxxx;

Alarm No	Detector Range (metres)	Object Distance when detected (metres)	Small Animal Size in centimetres (length/ height/ width)	Current Temperature (celsius)	Simulation Startup Time (hh:mm:ss)	Simulation Detection Time (hh:mm:ss)	Detection Time Difference (hh:mm:ss)	Result
1	18	-	54/18/12	19	00:14:24	-	-	No Alarm

APPENDIX B - REPORTS STRUCTURE

Fog/Smoke Report

Report Date : 99/99/99
Report Time : 99:99:99

Simulation Date	Simulation Time	Fog/Smoke Level	Detector Type	Detector Location
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA

2: Fog/Smoke Report

Rain/Dampness Report

Report Date : 99/99/99
Report Time : 99:99:99

Simulation Date	Simulation Time	Dampness Level	Detector Type	Detector Location
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA

3: Rain/Dampness Report

Temperature Change Report

Report Date : 99/99/99
Report Time : 99:99:99

Simulation Date	Simulation Time	Start Temperature	Finish Temperature	Temperature Shift	Detector Type	Detector Location
99/99/99	99:99:99	99.99	99.99	99.99	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	99.99	99.99	99.99	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	99.99	99.99	99.99	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	99.99	99.99	99.99	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	99.99	99.99	99.99	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	99.99	99.99	99.99	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	99.99	99.99	99.99	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	99.99	99.99	99.99	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAA

4: Temperature Change Report

Slow Movement Report

Report Date : 99/99/99
Report Time : 99:99:99

Simulation Date	Simulation Time	Movement Speed	Detector Type	Detector Location
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA

5: Slow Movement Report

Small Animals Movement Report

Report Date : 99/99/99
Report Time : 99:99:99

Simulation Date	Simulation Time	Experiment Criteria	Detector Type	Detector Location
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAA	AAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAA

6: Small Animals Movement Report

Report by Date

Report Date : 99/99/99
Report Time : 99:99:99

Intrusion Date	Intrusion Time	Detector Type	Detector Location	Environment Type
99/99/99	99:99:99	AAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAAA

7: Report by Date

The Sensor Type Report

Report Date	:	99/99/99
Report Time	:	99:99:99
Detector Type	:	AAAAAAAAAAAAAAAAAAAAAA

Intrusion Date	Intrusion Time	Detector Location
99/99/99	99:99:99	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
99/99/99	99:99:99	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

8: Report by Sensor Type

APPENDIX C - HELP MANUAL

ICCSM (Integrated Computer Controlled Sensor Monitor) is a windows application with a graphical user interface that monitors and gathers alarm data from security sensors. The two main features of ICCSM are:

- the ICCSM is capable of monitoring and gathering alarm data automatically from 64 security sensors, regardless of the sensor or technology type and
- secondly ICCSM allows the simulation of environmental conditions to adjust the sensor sensitivity level in order to examine the integrity of a security system.

A database (SQLBase Database) has been developed to record information on the sensors. ICCSM interfaces with the database making possible the addition, updating and deletion of sensor information.

Every time an intrusion is detected by a sensor, the sensor location data and time are stored in the database. This information can be obtained later in the form of reports generated by ICCSM.

C.1 The ICCSM Environment

The ICCSM environment is a combination of special hardware. Therefore your system may need special hardware to handle the ICCSM environment (To use this product, please check to be sure you have all you need).

ICCSM consists of the following components:

- a personal computer,
- an interface between a PC and a range of sensors (PC-IO-NR card),
- a VCR control Module,
- a VCR and
- a video camera.

C.2 ICCSM Operation Modes

ICCSM operates in two modes: simulation and production mode. The simulation mode is to test a security system with experimental conditions and observe their affects on the sensor performance. The production mode is to monitor and capture data from sensors without human intervention to find out the events that triggered an alarm.

C.2.1 Simulation Mode

As mentioned above, the simulation mode is to simulate known alarm conditions to thoroughly test a detection system and fine tune the detectors to desired sensitivity.

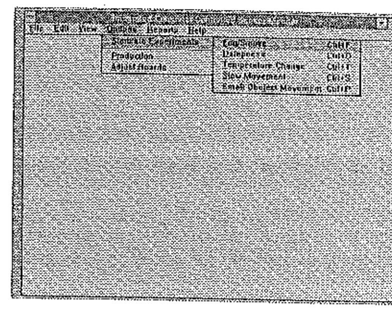

Figure **30**: Simulation Experiments

The environmental conditions with which to experiment in simulation mode are Fog/Smoke, Dampness, Temperature Change, Slow Movement and Small Animal Movement (see figure 30).

C.2.1.1 Setting the Simulation Mode

- from the "Option" pull down menu, choose "Simulate Experiments",
- select the experiment type from the menu,
- enter the test scale for the environmental condition (see figure 31),
- press "Enter" or click "OK" button to continue,
- the *Simulation* screen (see figure 32) will appear. Select the

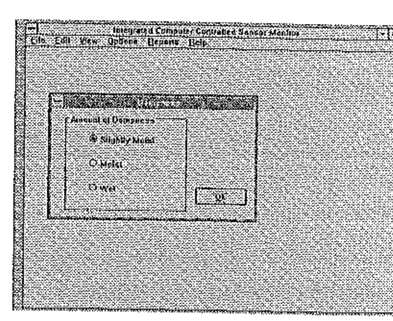

Figure **31**: Simulation Criteria

sensor to be tested from the sensor list. The sensor information is displayed on the side of the screen,

- click "Activate" button to activate simulation,
- the sensor status must be "Installed" before starting the simulation. If the sensor status is "Not Installed" the "Activate" button will stay in background and

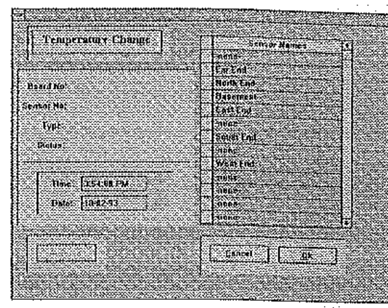

Figure 32: Simulation

- press "Alt-F4" or click the top left corner of the experiment window to de-activate simulation mode.

C.2.1.2 Dialogue Box Options in Simulation Mode

Dampness Dialogue Box

The dampness scales are Slightly Moist, Moist and Wet (see figure 31). The dampness scale can be selected by clicking the desired dampness level. Press "Enter" or click "OK" push button to continue.

Temperature Change

The current, minimum and maximum temperatures must be entered to simulate an experiment under the Temperature Change option (see figure 33). Enter current and expected temperatures and press "Enter" or click "OK" push button to continue.

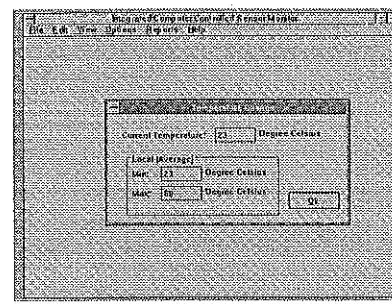

Figure 33: Temperature Change Experiment Criteria

Slow Movement

Three scales are defined for slow movement experiment. They are inches/min, feet/min and metre/min (see figure 34). Select desired movement scale and press "Enter" or click "OK" push button to continue.

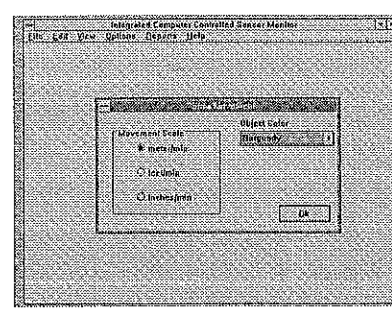

Figure 34: Slow Movement Experiment Criteria

Small Object Movement

Three different sizes can be selected for Small Objects: Small, Medium and Large (see figure 35). Select desired animal size and press "Enter" or click "OK" push button to continue.

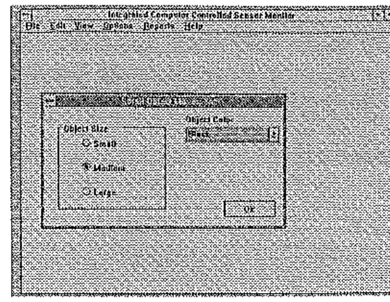

Figure 35: Small Object Movement Criteria

C.2.2 *Production Mode*

Production mode is for use in a real sensor controlled environment and can be left in operation for a maximum of 480 hours to determine the unknown causes of false alarms at a premise.

Under this mode ICCSM can monitor up to 64 sensor at the same time without human intervention. The intrusion data is automatically updated in a database when an intrusion is detected. A video recorder records the visual images of the intrusion for later analyses. The VCR control module speeds up the whole process.

If the sensors are not physically connected to the ICCSM environment or they are physically connected but are defined as "Not Installed" in the database then the production mode cannot be activated. Which means that one

or more sensors must be installed before activating production mode. Please refer to "How To Set Up The Sensors" for more information.

C.2.2.1 Setting the Production Mode

- from the "Option" pull down menu choose "Production",
- the production mode window is displayed. Once an alarm is detected the alarm details such as alarm number, board number, sensor number, intrusion date and intrusion time are displayed. The production mode also updates the ICCSM database,

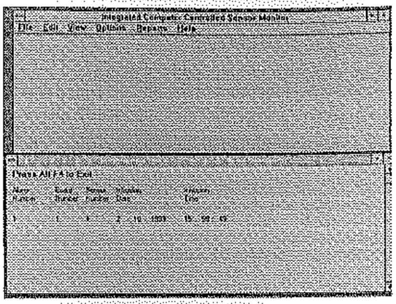

Figure 36: Production Mode

- press "Alt-F4" to de-activate the production mode and
- remember to set up the sensors before using this option.

C.2.2.2 Edit Sensor Configuration

Inserting A new Sensor Type

- from the "Edit" pull down menu select "Sensor Configuration". A windows lists the installed sensors in the database,
- place the cursor where the new sensor will be inserted,

- click "Insert" button,
- enter the sensor type in the dialogue box.
- press "Enter" or click "OK" push button to record the sensor type into the database. Click "Cancel" to quit.

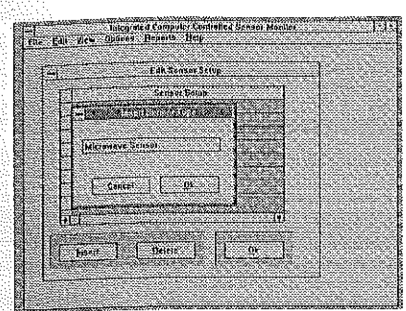

Figure 37: Inserting a Sensor

Deleting A Sensor Type

- from the "Edit" pull down menu select "Sensor Configuration". A windows lists the installed sensor in the database,
- click "Delete" button.
- enter the name of the sensor type to be deleted in the dialogue box (see figure 38) and
- press "Enter" or click "OK" button to remove the sensor name from the database. Click "Cancel" to quit.

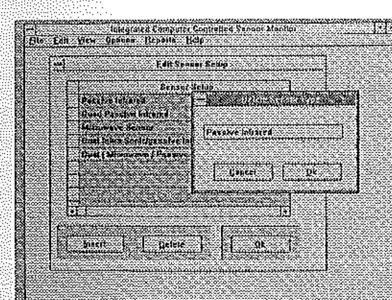

Figure 38: Deleting a Sensor

C.2.2.3 Edit Board Configuration

The production and simulation modes of ICCSM environments can not be activated unless the sensors are properly configured in the database. The sensor setup is accomplished by entering the sensor details into the database through "Edit Board Configuration" option. A maximum of 64 sensor can be connected to eight input boards.

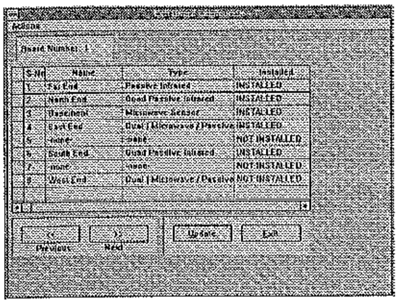

Figure 39: Edit Board Configuration

To configure the boards

- select "Board Configuration" option from the "Edit" pull down menu,
- click a row to enter sensor description (figure 40). The sensor data can be entered in the following order :
    - sensor name : a string of character or numbers. It must start with a character,
    - sensor type : this field refers to the type of sensor technology. Select one from the list that appears on the screen. The sensor types have to be defined previously in the database. To get more information, please refer to "Edit Sensor Type"

- sensor status : select one of the two options : "Installed" or "Not Installed".
- to navigate around the different boards, click "Previous" and "Next" buttons and
- press "Enter" or click "Update" button to update the database.

Click "Exit" to quit.

C.3 ICCSM Options

C.3.1 Obtaining Reports

The ICCSM system also provides written reports which can be generated for experiment type (eg: Rain/Dampness, Temperature Change) by sensor type (eg: Dual, Passive Infra-Red) and by date (see figure 40).

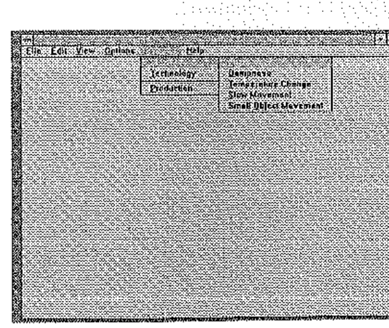

Figure **40**: Report Types

C.3.1.1 Getting reports by simulation

- select "Simulations" from the Report menu,
- select the experiment type from the sub-menu,
- press "Enter" or click "OK"

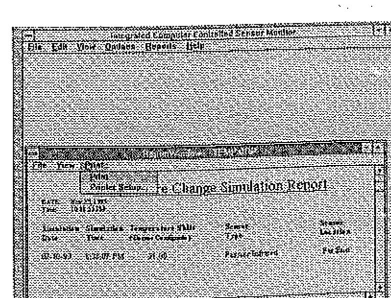

Figure **41**: Simulation Report

button to get a report,

- select "Print" pull down menu from the report,
- choose "Printer Setup" to nominate a printer and
- select "Print" from the menu to print the report.

C.3.1.2 Getting reports by sensor type

- select "Technology" from the Report menu,
- select the sensor type from the sensor list,
- press Enter or click "OK" push button to obtain a report,
- select "Print" from the report title bar,
- choose "Printer Setup" to nominate a printer and
- select "Print" from the menu to print the report.

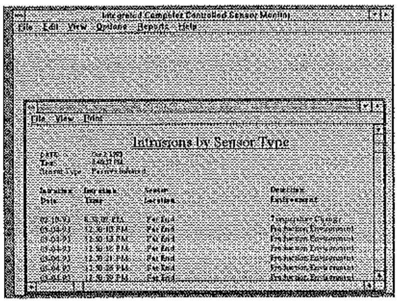

figure 42: Report by Sensor Type

C.3.1.3 Getting reports by date

- choose "Production" from the Reports menu,
- enter the start date in the dialogue box,
- press "Enter" or click "OK"

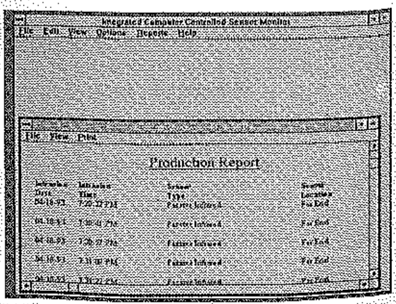

Figure 43: Production Report

button to get a report,

- select "Print" from pull down menu of the production report,
- choose "Printer Setup" to nominate a printer and
- select "Print" from the menu to print the report.

C.3.2 View Board Configuration

Information about the sensor configuration can be viewed without risking the integrity of the database.

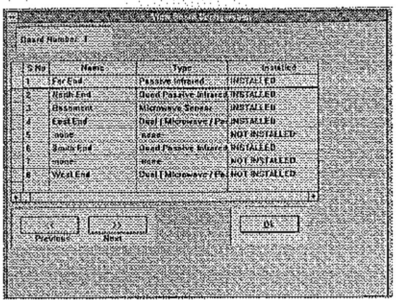

Figure 44: View Board Configuration

C.3.2.1 To view Board configuration

- select "Board Configuration" from the "View" pull down menu,
- to navigate from one board to another, click "Previous" and "Next" buttons and
- press "Enter" or click "Exit" to exit.

C.3.3 *File Option*

C.3.3.1 About System

Briefly describes the ICCSM system.

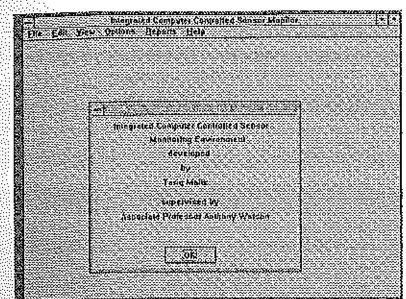

Figure 45: About ICCSM

C.3.3.2 Printer Setup

- select "Printer Setup" from the File menu,
- select the printer to print the report.
- make sure the paper size is correct.
- a report can be printed by generating the desired report, follow the instructions in "Obtain Reports", and then printing it from the report title bar and
- press "Enter" or click "OK" to select the printer and press "Cancel" to cancel the printer.

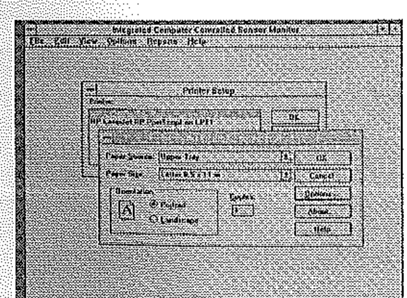

Figure 46: Printer Setup

C.3.3.3 Exit

To exit from the system.

C.3.4 Help Option

C.3.4.1 Help Index

Help Index briefly details the ICCSM environment and functions provided by it.

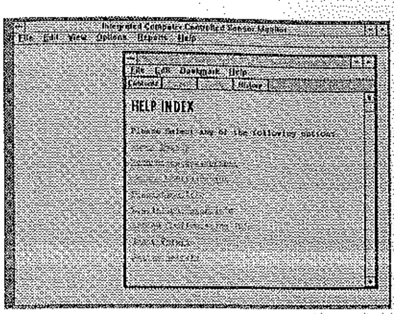

Figure **47**: Help Index

C.3.4.2 About Help

Provides general information about how to use help in Microsoft Windows environment.

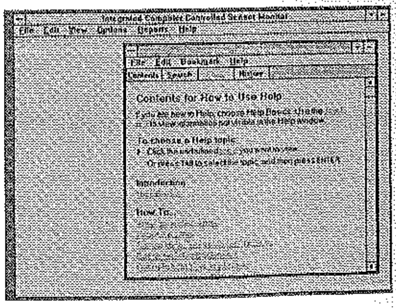

Figure **48**: About Help

APPENDIX D - TRADEMARK ACKNOWLEDGMENTS

- Borland C ++ is a product of Borland Corporation.
- SQLWindows is a product by Gupta Corporation.
- IBM stands for International Business Machine Corporation.
- MASM Assembler is a product by Microsoft Corporation.
- PC-BD-IO and PC-IO-NR Board are products of Procon Software.
- Windows 3.1, MSD and WinHelp are products of Microsoft Corporation.