1 of 1

SAFEGUARDS EQUIPMENT OF THE FUTURE
-
INTEGRATED MONITORING SYSTEMS AND REMOTE MONITORING

Cecil S. Sonnier
Charles S. Johnson
Sandia National Laboratories
Albuquerque, New Mexico, USA

ABSTRACT

Becoming aware of the significant events of the past four years and their effect on the expectations to international safeguards, it is necessary to reflect on which direction the development of nuclear safeguards in a new era needs to take and the implications. The time proven monitoring techniques, based on quantitative factors and demonstrated universal application, have shown their merit. However, the new expectations suggest a possibility that a future IAEA safeguards system could rely more heavily on the value of a comprehensive, transparent, and open implementation regime. Within such a regime, the associated measures need to be determined and technological support identified. This paper will identify the proven techniques which, with appropriate implementation support, could most quickly make available additional measures for a comprehensive, transparent and open implementation regime. In particular, it will examine the future of Integrated Monitoring Systems and Remote Monitoring in international safeguards, including technical and other related factors.

INTRODUCTION

From the beginning, equipment to support IAEA Safeguards could be characterized as that which is used to measure nuclear material, Destructive Assay (DA) and Non-Destructive Assay (NDA), and that which is used to provide continuity of knowledge between inspection intervals, Containment & Surveillance (C/S). In recent years, technology has advanced at an extremely rapid rate and continues to do so. Perhaps the most interesting aspect of this evolution, and that which indicates the wave of the future without much question, is the integration of video surveillance and electronic seals with a variety of monitors, as well as unattended NDA equipment. This is demonstrated by safeguards systems which are installed in several nuclear facilities in France, Germany, Japan, the UK, the USA, and elsewhere. The terminology of Integrated Monitoring Systems (IMS) has emerged with the employment of network technology capable of interconnecting all desired elements in a very flexible manner. Also, the technology for transmission of a wide variety of information to off-site locations, termed Remote Monitoring, is in widespread industrial use, requiring adaptation for safeguards use.

This paper will examine the future of Integrated Monitoring Systems and Remote Monitoring in International Safeguards, including technical and other related factors. These technologies are very important elements of the US Department of Energy's International Safeguards Program. A principal goal of this program is to enhance verification techniques and capabilities of international, regional, and bilateral regimes to support Non-Proliferation objectives. It promotes technology exchanges in a broad range of technologies to insure improvement in the effectiveness and efficiency of domestic and international safeguards, and international acceptance of new developments.

INTEGRATED MONITORING SYSTEMS

In the 1980's, under the US Program of Technical Assistance to IAEA Safeguards (POTAS) and the DOE International Safeguards Program, Sandia National Laboratories (SNL) developed and successfully tested an Integrated Monitoring System (IMS), which monitored the movement of spent-fuel shipping casks to/from light water

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.

reactors to reactor or away-from-reactor storage facilities. The system used a crane location monitor, and gamma radiation detectors recorded the information in a tamper-detecting, tamper-resistant enclosure for later inspection, and triggered a camera for photographic assessment of anamolies. An outgrowth of this system is the SNL/LANL-developed Channel Monitoring System in use by Euratom at the THORP facility in the UK.

A key element of state-of-the-art integrated systems is a modular nodal system which accepts information from sensors and provides information to both an on-site date storage unit as well as to a transmitter. The information from the sensors is processed within the nodal elements for authenticity as well as for sensor identification. Since the processing for authenticity occurs within the nodal elements, existing communication wiring (e.g. twisted pairs, coaxial cables) can be used. Intelligent nodes, nodes which can send command information to other nodes, allow information from one sensor to trigger another.

A number of "unattended monitoring systems" are currently in safeguards use or under development, some of which are the subject of other papers in this meeting. These include Candu Fuel Bundle Counters, the Portal/Penetration Monitoring System, CONSULHA, as well as the previously mentioned Channel Monitoring System.

It is important to note the classic difference between the concept of simple triggering of optical surveillance devices and systems which log all information (apart from the optical device) as well as trigger these devices. This latter dual function was in fact incorporated in the IMS of the 1980's previously described. From an engineering point of view, information from detectors, absent any optical surveillance data, could lead to identification of an anamoly which could form the basis for investigation by an inspector.

Technical Factors - In the past several years, under the US Department of Energy's International Safeguards Program, SNL has developed a network-based Integrated Monitoring System. A new flexible technology is now available to design sensor and control networks based on a protocol embedded in an intelligent communications processor. The flexibility allows a system designer and/or system installation personnel to make appropriate tradeoffs between simplicity, function, and cost in the design of network nodes and their installation. This is especially important in designing the installation scenario for a safeguards network. The network technology permits several choices of installations with the same basic node hardware, providing the ability to interconnect a number of different types of sensors and control devices into a simple network which can communicate over a single cable at a relatively low cost. Network technology exists to meet these features by providing each node of the IMS with distributed intelligence capable of handling both the communication protocol and the data processing requirements of the individual sensors. Most sensors for safeguards and security systems seldom need to transmit messages, since the sensors are not activated very frequently. The messages sent by the sensors are generally very small amounts of data consisting of a very few bits indicating things like "alarm", "tamper", or "status ok". Infrequent messages with low- data content can easily be handled by the IMS, which can communicate over a number of different physical media making it possible to configure different network configurations with interconnecting bridges. The same basic nodes can be configured to provide data collection in any number of different types of facilities and from networks varying in size from a very few sensors to a large number, including unattended NDA equipment, as well as a variety of detectors from the physical protection area. A network can be installed using network management software and a computer, referred to as a Network Management Tool, which offers full flexibility to change the network during installation. Such tools can provide different degrees of complexity depending upon the safeguards applications and the amount of changes that need to be made during installation.

The low cost integrated communications processor upon which the Integrated Monitoring System (IMS) is based contains all the software for communications protocol and additional applications processing power to accommodate a large number of the safeguards sensor and control requirements. Another microprocessor can also be added if still more processing power is required. An important feature of the IMS is the capability to authenticate all of the data transfers over the network.

From this description, it is clear that much care must be taken in the configuration of an IMS, and numerous adjustments will have to be made before full safeguards implementation in a particular facility will be possible. This is quite sensitive to facility configurations and environments. This task is not likely to be one that the IAEA should be expected to perform alone - rather, significant support will be required by the system developers, facility operators, and the state.

Other Related Factors - The transition from conventional C/S and unattended NDA to Integrated Monitoring Systems raises issues of cost and facility/state

acceptance. Important features of the IMS described above are both low cost and the capability to install the same basic types of sensor nodes in many different facilities. The simple interconnection of all the sensors through one cable is very important to minimize installation costs.

Acceptance will clearly depend on what benefits will be achieved by the IAEA and the state/facility operators. There will always be the question of "why additional measures". The answer that is apt to be found to be most acceptable is that the additional measure(s) will mean less inspector effort/presence. That in turn may require another look at the current safeguards procedures and criteria.

REMOTE MONITORING

Remote monitoring of nuclear facilities is not a new concept. We need only to recall the images presented on a daily basis on the television networks throughout the world. Also, as stated in the introduction, there are many examples of everyday applications of remote monitoring: security sensors monitor homes and businesses; data from seismic stations are remotely transmitted; land-mobile satellite communication systems send and receive test messages to and from mobile vehicles as well as determine the location of the vehicles.

In 1978, the US Arms Control and Disarmament Agency (ACDA) developed and tested a secure system for remote verification of the status of containment and surveillance instruments employed at nuclear facilities by the IAEA; it was called RECOVER (Remote Continual Verification). As many will remember, this was at a time when the failure rate of the Minolta Camera Systems was quite high; it was, perhaps more importantly, at a time when many in the international community were simply not willing to accept the concept of transmitting safeguards data across national borders.

Shortly after the RECOVER program, the Japanese developed the TRANSEAVER (Transportation by Sea Verification) System as a potential safeguards measure.

More recently, the US and Japan jointly developed the prototype Containment and Surveillance Data Authenticated Communication (CASDAC) System. This was a feasibility test of remote monitoring of unattended sensors conducted by SNL and the Japan Atomic Energy Research Institute (JAERI) under a bilateral agreement between the ACDA and JAERI. The system's purpose was to perform remote monitoring of sensor status through the international telephone network; it was a prototype developed by JAERI for nuclear safeguards and physical protection. The design was based on experience gained from RECOVER and TRANSEAVER.

Currently, the US Department of Energy's International Safeguards Division, SNL and other DOE National Laboratories, and a number of international partners are engaged in an active project termed "International Remote Monitoring Project". The objectives of this project are to:

- examine and, through field trials, define the technical parameters related to communications protocol, digital standards, sensor and sub-system interfaces, data display and management, overall reliability, and others as deemed necessary,

- demonstrate the technical feasibility and political acceptability of remote monitoring in today's safeguards environment, and

- gain international acceptance of the remote monitoring concept

Remote monitoring systems will be deployed in an incremental manner. The first trial began in Australia in February 1994; the results of this field trial to date have been most encouraging. Additional field trials are planned in Sweden in August 1994; in Argentina in September 1994, and in Japan in October 1994. Other planned installations include Germany and JRC Ispra in late 1994 or early 1995. Several other installations are currently under consideration. In addition, a fully operational Integrated Monitoring System will be installed at SNL. To the extent practical, this system will contain one of all types of detectors and video systems used in the various installations of the International Remote Monitoring Project (IRMP). The IMS will be connected to the IRMP network and will be used as a test bed for all detectors provided by the DOE Laboratories and the DOE international partners.

Technical Factors - Technology exists to enable the IMS to be interrogated via various communication links such as telephone, satellites, or radio frequency tranceivers. The data can be collected from storage devices on the network, or the individual sensors can be polled to determine their status. Data management, including presentation, will present a technical challenge when a large number of facilities are to be monitored.

The block diagram in Figure 1 shows an example of the equipment that could be installed at facilities for

remote monitoring systems. A network of nodes would collect data from a number of different sensors and security devices. Detection devices would be installed to complement each other for C/S applications. In addition, unattended NDA equipment, as well as simple gross attribute, yes/no, radiation detectors could be used.

Referring again to Figure 1, the Authenticated Item Monitoring System (AIMS) could be used to monitor drums or other storage containers. AIMS Sensor Transmitters (ASTX) could be attached to the items with Velcro. The number of AIMS transmitters used would be determined by the items being monitored. Several infrared motion detectors (IRMD) with AIMS transmitters could be installed to detect motion in selected areas. Single ASTX's could be installed on other items of safeguards interest to detect their movements. The data from the AIMS devices can be collected in two different ways. A Receiver Processor Unit (RPU) could operate independently to collect AIMS information. An AIMS receiver node could also collect the same information for storage in the data logger and for remote interrogation.

Microwave motion detectors connected to the network could be used to determine if any activity is occurring in the area. Detection of any activity could trigger video recordings to be made on the video recording module. The number of microwave motion detectors would be determined by the requirement of the selected area.

Ultra-wide band Radar Motion Sensors could also be installed to detect activity. The pulses emitted from these sensors are well below one microwatt and are spread over several Giga Hertz (GHz). Their coverage consists of a spherical shell around the sensors that has an adjustable radius.

Other types of sensors such as photoelectric sensors could be used on the network depending on the area to be monitored. Door switches, temperature sensors, radiation detectors, etc. could be connected to the nodes. Computer data interface devices with RS-232 data outputs or inputs can also be connected through the network.

Dual video systems could be utilized to collect video images. An analog recording system, like the Portable Surveillance Unit (PSU), could be connected to the network. It could be programmed to record when certain sensors or combinations of sensors detect activity in the area under safeguards. A second video system using digital compression technology and connected to data logger/system controller could collect digital images and store the images on removable data discs or accessed for remote transmission. The "Digital Video Recorder" should also contain an internal hard drive for storing images. Data and images from the area under safeguards can be remotely accessed via telephone lines from a distant monitoring center. Similarly, this information could be accessed via satellites where such a media is required. Periodically it would be necessary to remove data discs from the data logger and video tapes from the video recording modules.

Other Related Factors - One of the most important aspects of remote monitoring is the potential constraints related to the transmission of data out of a facility or beyond national borders. If used, must the data be encrypted? In what form must it be encrypted? Will the facility or state require all information transmitted, etc.? In addition to the transmission of data from an IMS beyond national borders, there will be uses for remote monitoring in large facility complexes and from facilities within a state. This latter application was, in fact, the principal objective of the German Local Verification (LOVER) project of the 1980's. Another important factor which must be considered is the overall cost effectiveness of remote monitoring. Here, very important issues must be addressed; e.g. can acceptable safeguards assurances be achieved through acquisition of data from remote monitoring and reduced inspection effort ?

SUMMARY

This paper, as well as other papers in this and other sessions, clearly demonstrates the abundance of technology that supports the configuration of Integrated Monitoring Systems and Remote Monitoring Systems. The technology presents a rather minimal challenge, except in the areas of authentication, encryption, and standardization. The situation with Remote Monitoring Systems is further complicated by policy issues related to state rights, transparency, safeguards criteria, and other issues.

It is quite clear that much care must be taken in the configuration of an IMS, and numerous adjustments will have to be made before full safeguards implementation in a particular facility will be possible. This is quite sensitive to facility configurations and environments. The authors feel that this task is not likely to be one that the IAEA should be expected to perform alone - rather, significant support will be required by the system developers, facility operators, and the state.

As the IAEA and the International Safeguards Community address the current safeguards procedures

and criteria and all that it means in todays world, it is necessary to realize that technology offers the potential of making significant contributions to the goals of safeguards. However, it is doubtful that these contributions can be realized to their maximum benefit unless much more importance is placed on the qualitative parameters that could contribute to safeguards.

Becoming aware of the significant events of the past four years and their effect on the expectations to international safeguards, it is necessary to reflect on which direction the development of nuclear safeguards in a new era needs to take and the implications. The time-proven monitoring techniques, based on quantitative factors and demonstrated universal application, have shown their merit. However, the new expectations suggest a possibility that a future IAEA safeguards system could rely more heavily on the value of a comprehensive, transparent, and open implementation regime. Within such a regime, the associated measures need to be determined and technological support identified. Clearly one important element of the new regime will be remote monitoring using integrated monitoring systems.

REFERENCES:

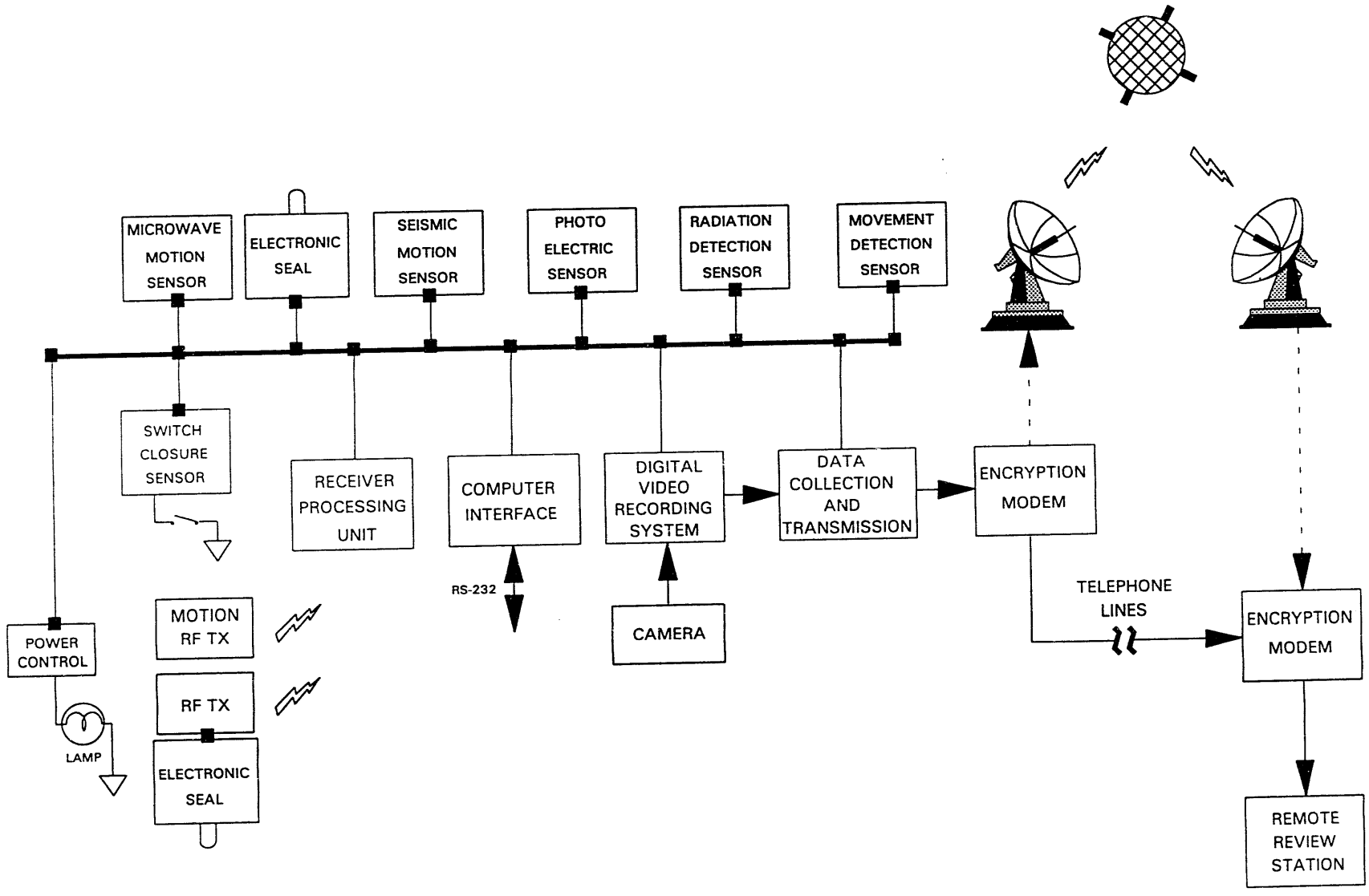
1. "International Safeguards Program - Strategic Plan - Fiscal Year 1994", October 1993, US Department of Energy, Office of Arms Control and Nonproliferation, International Safeguards Division, Washington , DC 20585.

2. "Integrated Monitoring System (IMS) Development and Demonstration Activities: Summary of POTAS Task E.45", SAND84-1439, April 1986.

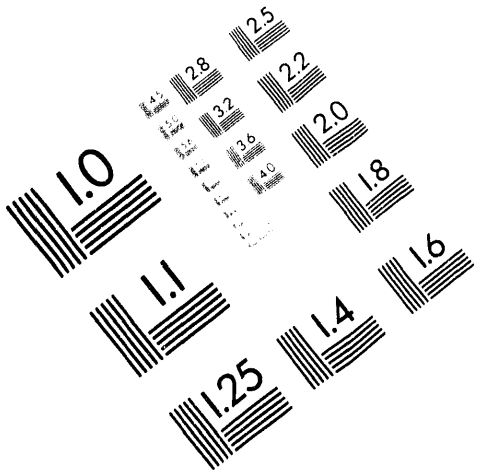
3. "RECOVER: Results of Independent IAEA Test Program, 3 November to 24 November 1980", prepared for the US Arms Control and Disarmament Agency, January 23, 1981 (Draft).

4. K. Ystesund, R. LeGalley, K. Koyama, Y. Yamamoto, "Containment and Surveillance Data Authenticated Communication (CASDAC) Project Final Report", prepared for the Defense Nuclear Agency, November 1993.

5. J. L. Schoeneman, C. D. Jenkins, R. D. Tooley, "Universal Authenticated Item Monitoring system", 31st Annual Meeting Proceedings of the Institute of Nuclear Materials Management, July 1990.



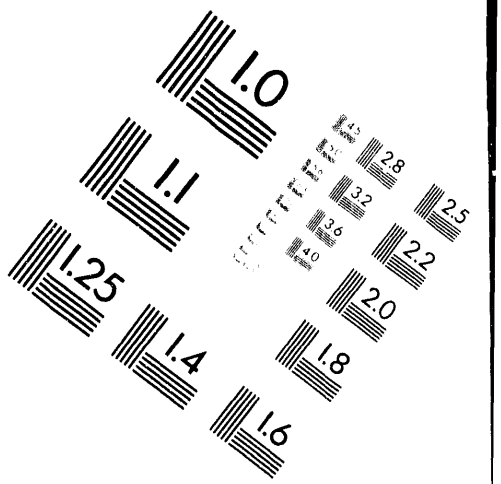
REMOTE MONITORING SYSTEM

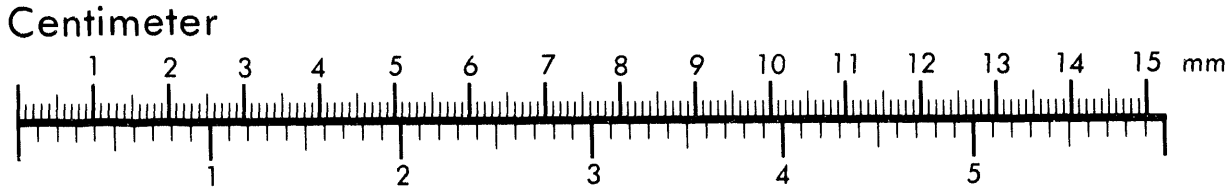


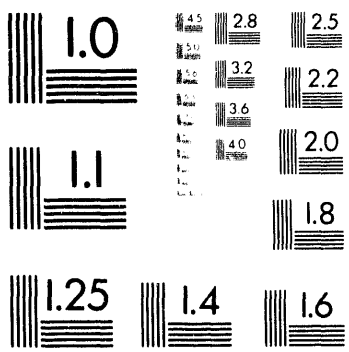
Association for Information and Image Management

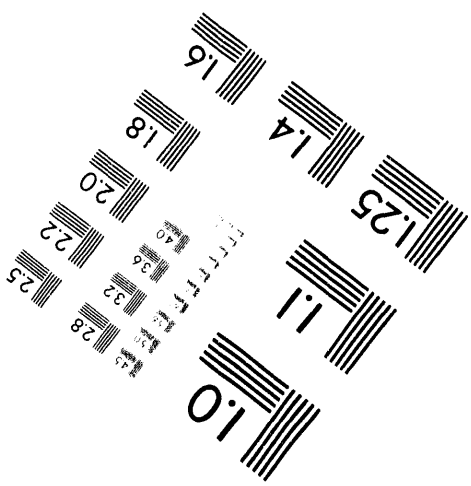
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

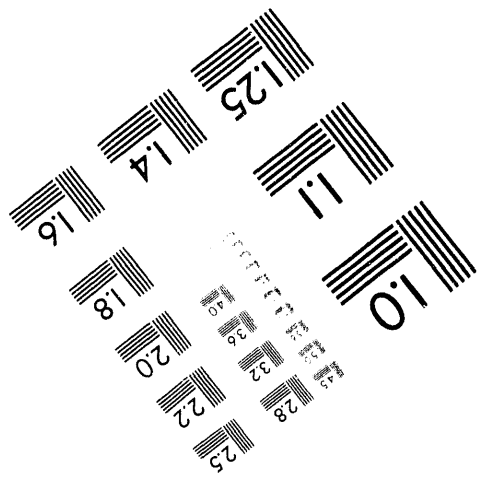
301/587-8202











MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

DATE
FILMED
12/6/94
END