BNL-68711
IAEA-SM-367/7/03

Lessons Learned in Testing of Safeguards Equipment

Susan Pepper, Michael Farnitano, and Joseph Carelli
Brookhaven National Laboratory, Upton, New York

Joseph Hazeltine and David Bailey
Wyle Laboratories, Huntsville, Alabama

Abstract:

The International Atomic Energy Agency's (IAEA) Department of Safeguards uses complex instrumentation for the application of safeguards at nuclear facilities around the world. Often, this equipment is developed through cooperation with member state support programs because the Agency's requirements are unique and are not met by commercially available equipment. Before approving an instrument or system for routine inspection use, the IAEA subjects it to a series of tests designed to evaluate its reliability. In 2000, the IAEA began to observe operational failures in digital surveillance systems. In response to the observed failures, the IAEA worked with the equipment designer and manufacturer to determine the cause of failure. An action plan was developed to correct the performance issues and further test the systems to make sure that additional operational issues would not surface later. This paper addresses the steps taken to address operation issues related to digital image surveillance systems and the lessons learned during this process.

1. Introduction

The implementation of new equipment by the Department of Safeguards is costly. Expected costs associated with the implementation of equipment include capital costs, training and in some cases travel. Performance problems can dramatically raise the costs of implementing equipment by adding expenses related to studying the issues, modifying and upgrading the equipment and additional travel. It is expected that adequate testing prior to implementation will help the IAEA avoid expenses related to performance problems.

The U.S. Support Program (USSP) believes that the IAEA and its member states must strengthen equipment testing programs to ensure that the equipment approved for inspection use is reliable and will not place additional burden on the Department of Safeguards' maintenance and inspection staff. As a result of equipment reliability issues that arose during 2000, the USSP encouraged the IAEA to investigate additional testing that could be performed to ensure equipment reliability. Testing can improve reliability by identifying design deficiencies and vulnerabilities that can be mitigated through modifications or by ensuring compatibility with field environments. Under one task related to digital image surveillance (DIS), the USSP approved funding for system upgrades, design limit and accelerated lifetime testing, and a software review. While this paper will focus on experiences from this exercise involving DIS, the lessons learned apply to almost any safeguards instrumentation.

2. The History of Transition from Analog to Digital Surveillance Equipment

In the early 1990s the IAEA began a program to develop digital surveillance systems to replace analog ones. The replacement was required because spare parts and manufacturer support for analog systems were becoming hard to obtain. In addition, the transition to digital equipment was intended to facilitate compatibility between and integration of instruments, remote communication of data, improved data storage, and modernization. Many of the digital instruments are designed to operate on battery power during loss of facility power, and therefore, are designed to consume minimal power.

Testing of DIS systems began in 1996. Between 1996 and 1998, testing revealed a number of operational issues that were corrected. In 1997, an all-in -one-surveillance system (ALIS) camera failed, exhibiting symptoms of changed and corrupted data. The suspected cause was improper grounding between the camera and the server. This was the only failure in 170 unit-months of field-testing. DIS

was approved for use by the IAEA in July 1998 and installation began shortly thereafter. Failures occurred periodically over the next year; the failure symptoms were changed image dates and times and lost internal settings. The equipment designer suspected that an oscillator circuit was the cause. This cause was addressed in a new version of firmware released in December 1999. It was expected that when all units were upgraded, failures would cease. But in March through June 2000, additional failures with the same symptoms occurred in upgraded units.[1]

The IAEA's investigation team continued to gather data on the failures through June and July 2000 and to conduct extreme tests on units (including magnetic pulse, communication, and electrical tests). In August, the designer and manufacturer were called in to help. No test was able to reproduce the same symptoms as the change of date and time and the corruption of data until the Fraunhofer Institute conducted neutron bombardment testing of a DCM-14 camera system in August 2000. In that test, the full range of symptoms was reproduced. Through these and subsequent Agency testing at the Seibersdorf Laboratories, there was strong evidence that the cause of the date/time and data corruption was due to single event upsets (SEUs). An SEU occurs when induced errors in microelectronic circuits are caused by charged particles losing energy by ionizing the media through which they pass, leaving behind a wake of electron-hole pairs. One specific example is the effect of neutron radiation interacting with micro-processors and digital memory chips and resulting in interruption of operating systems, erratic performance or corrupted data. Because the IAEA's original specifications and environmental test criteria did not address radiation, the developer did not design the DIS systems to operate in a radiation environment. During 2000, the IAEA installed systems in locations with high neutron dose rates.[1]

The discovery of the SEU failure mode demonstrates three weaknesses in the system for equipment development. The first is inadequate characterization of technical requirements. Second, there is an inadequate system for testing safeguards equipment before it reaches the field. Third, there is a failure to consult equipment specifications to ensure compatibility when installing equipment in new field environments.

3. Description of Equipment and Installation Environments

To date, the IAEA has installed over 200 digital surveillance units. The DIS systems selected by the IAEA are based on the DCM-14 model developed by the German Support Program. A number of variations of the camera system are used by the IAEA to address different safeguards requirements. The DIS systems employed by the Department of Safeguards include:

ALIS - All-in-One-Surveillance System - includes camera, electronics, and data storage. It replaces the Minolta Photo System and the COSMOS analog video system

SDIS - Server-based Digital Image Surveillance System - Communications server with remote monitoring capability - The IAEA can connect up to four DCM-14 cameras to an SDIS.

VDIS - Video Digital Image Surveillance System - VDIS consists of a DCM 14 module, CCD camera, and Li-Ion battery sealed in a blue standard camera housing.

DMOS - Digital Multi-camera Optical System - includes up to 16 cameras and has remote monitoring capability. It replaces the analog multi-camera system. The IAEA has not yet completed its acceptance testing of the system.

DSOS - Distributed Surveillance Optical System - The camera head is located separately from the electronics module. This is the digital replacement for the analog distributed video system known as MIVS.

The IAEA uses both portable equipment that is used by inspectors to monitor short-term activities and installed equipment that is left in the field to operate unattended for long periods of time. The equipment must be rugged to survive shipping and to withstand months of storage or unattended operation.

Surveillance equipment is used by the IAEA in all types of nuclear facilities, but predominantly in reactors. The environments in which the instruments are used can be harsh. The equipment can be subjected to temperature and humidity extremes, poor quality power, and radiation. The specifications developed by the IAEA prior to the development of the equipment attempted to comprehensively describe the environmental conditions to which the DIS systems would be subjected.

4. Current IAEA Requirements Aimed at Ensuring Equipment Quality

Equipment cannot be used by the Department of Safeguards for inspection until it has been approved for use. Approval for use is based on the results of testing as well as issues such as standardization and need. The *IAEA Common Qualification Test Criteria for New Safeguards Equipment* [2] is a solid foundation for safeguards equipment testing. The document outlines four standard series of tests that each newly acquired instrument is subjected to before being considered acceptable for safeguards use. The test categories addressed in this document are operational, thermal and humidity, mechanical, and electromagnetic tests. The document was developed and used jointly with Euratom and builds on the experience and lessons learned from earlier development efforts.

Additional IAEA testing activities that lead to an approval for use include acceptance testing, field-testing, and usability testing. Acceptance testing ensures that the product meets the requirements as defined by the IAEA. Field testing allows the IAEA to observe the instrument in operation in realistic field conditions, rather than more favorable laboratory conditions. Usability testing studies the reaction of users to the instrument to see where difficulties or user error might arise.

In an attempt to force a more standardized approach to equipment development, the IAEA encouraged their equipment manufacturers to pursue certification under ISO 9000 standards. The standard provides a rigorous approach to equipment development, including testing and documentation of the process in significant detail. Through the detailed documentation process, test results can be duplicated with a high level of confidence. We note that while certification is encouraged, many designers of safeguards equipment are not certified under ISO 9000 criteria.

5. Corrective Action Plan

As a result of the identification of performance issues with DIS equipment, the IAEA, the equipment designer and the equipment manufacturer held a series of meetings between August 2000 and April 2001 and undertook a corrective action program to address the issues. In addition to taking steps to strengthen the system to combat the effects of neutron radiation, the corrective actions included steps to increase confidence in the systems and to better understand the environments into which equipment is placed. Under funding from the USSP, the IAEA participated in independent design limit and lifetime determination testing of the DCM-14 camera and the SDIS by Wyle Laboratories and endorsed a software audit by the equipment manufacturer.

In addition, the USSP provided access to instrumentation that could be used by the IAEA to characterize the environments in which equipment is installed. By characterizing the environment in advance, the IAEA can make an informed decision as to whether equipment can be expected to perform reliably.

6. Testing of DIS Systems at Wyle Laboratories

Two SDIS systems and six VDIS systems were subjected to a test program that consisted of environmental extremes, vibration, electromagnetic interference/power quality, and radiation effects. The testing program was designed to determine the operating environmental extremes under which the systems can properly perform its intended mission. The system had been designed without adequate knowledge of the intended installation environments and thus testing to determine the operating extremes was warranted. The operating environment's extremes had been evaluated post deployment and were reported to Wyle as follows:

Table I: Initial Environmental Data

Environment	Outside Containment	Inside Containment
Peak Temperature	55°C (35°C nominal)	50°C (35°C nominal)
Relative Humidity	95% (20% nominal)	65%
Radiation (gamma)	Background	0.154 gy/hr (15.4 rads/hr)
Radiation (neutron)	Background	30 msieverts/hr (3 REM/hr)
Voltage Fluctuations	26 ± 0.3 Vdc	24 ± 0.2 Vdc
Refueling Cycle	1 month outage every 18 months	

Wyle Laboratories was involved in all aspects of the test planning including the preparation of the test procedure and the testing sequence. The IAEA provided the acceptance criteria and the operating environment data. Wyle was responsible for defining the test method to be utilized and the selection of fixturing when required. The SDIS was placed in a normal operating mode for all energized tests.

7. Test Results

A formal test procedure was developed for the Design Limit and Life Determination testing on the SDIS system.[3] This procedure was submitted for approval to the IAEA prior to commencement of testing activities. The SDIS system testing revealed that the system is adequately designed for its intended environment in all but a few areas. The following aspects of the intended environment pose no significant technical risk: humidity, altitude, high and low temperature extremes, vibration, electromagnetic compatibility, shock, and design life. However, there are three areas of concern where testing has repeatedly shown the SDIS system, and in particular the DCM-14, to be susceptible to environmental conditions where it is installed. These are fast neutron flux, thermal neutron flux and gamma radiation. A summary of selected testing activities is provided in Table II. A full testing report is available in Reference [4].

The radiation sensitivity can be corrected in four ways, none of which are optimal. The DCM-14 electronics can be relocated to an outside containment location, the DCM-14 circuitry can be radiation hardened, the VDIS can be shielded, or the software/hardware system can be redesigned to withstand the occurrence of numerous SEUs.

Table II: Selected Test Procedures and Test Results[4]

SDIS Design Limit Test	Test Technique	Operating Environment	Results
Humidity	Starting at ambient, increase temperature and humidity to a maximum of 65°C and 95% RH. Then conduct three cycles where maximum humidity and temperature are evaluated	55°C and 95% RH maximum	System was found to be fully operational in a 100% condensing humidity environment.
Temperature	Starting at 25°C, temperature decreased and increased in 10°C increments until failure	Lower bound not specified, Upper bound 55°C	System tested from -40°C to 55°C, VDIS did not lose data
Electrostatic Discharge (ESD)	Starting at 4 kV, increase the ESD in 1 kV increments until failure occurs or until 8 kV is reached	Not specified	System was able to withstand 8 kV contact and 16 kV air discharges
Voltage Dips & Interruptions	Starting at interruptions of 20 milliseconds, increase the interruptions in 100-millisecond increments until failure occurs or until a dropout of 1 second has been reached.	Not specified	System was able to withstand voltage dips of 1 second

SDIS Design Limit Test	Test Technique	Operating Environment	Results
Lightning Surge	Starting at a surge of 1 kV increase the surge voltage in 500-volt increments until failure occurs or until a level of 2 kV has been reached.	Not specified	System was found to be fully operational after 2kV surges had been applied.
Electric Fast transient (EFT)	Starting at a pulse of 1 kV, increase the pulse voltage in 500-volt increments until failure occurs or until a level of 2 kV has been reached.	Not specified	System was found to be functional with 750 Volt EFT pulses, but was not functional at 900 Volts.
Radiated Immunity (Electric Field)	Starting at radiated field level of 3 V/m, increase the voltage in 3-V/m increments until failure occurs or until a level of 10 V/m has been reached.	Not specified	System was found to be fully operational in a 10 V/m radiated field
Radiated Immunity (Magnetic Field)	Starting at radiated field level of 1 A/m, increase the field strength in 1-A/m increments until failure occurs or until a level of 3 A/m been reached.	Not specified	System was found to be fully operational in a 2 A/m magnetic field
Indirect ESD	Starting at 6 kV, increase the ESD in 1-kV increments until failure occurs or until 12 kV is reached	Not specified	System was found to be fully operational with 8 kV ESD pulses delivered to the horizontal and vertical coupling planes.
Gamma Radiation Exposure	Radiate the camera only with a field of 1×10^5 rads/hr until either the camera fails to operate or a total integrated dose of 1.6×10^6 rad has been achieved	15.4 rads/hr	Camera was found to operate at low dose rates 5.0E+03 rads/hr. As the dose rate was increased from this point, the system suffered non-recoverable errors.
Fast Neutron Radiation Exposure	Radiate the camera only with a field of 6.16×10^3 rads/hr until either the camera fails to operate or a total integrated dose of 1.31×10^4 rad has been acheived	3 rem/hr	SEUs occurred with reactor flux level at 3.3E+06 n/cm^2, (criticality) but the system was functional. As flux level increased to 3.3E+07 n/cm^2 the system failed to operate
Drop Shock	Bench Handling drops from 6 inches	Not specified	System survived
Inclined Impact Shock	Simulate actual transportation of the SDIS	Not specified	System survived.

8. Lessons Learned and Issues Raised

Many valuable lessons have resulted from the yearlong investigation into issues related to the performance and reliability of DIS systems. While this paper focuses on DIS systems as an illustration of the challenges facing the Department of Safeguards, the lessons learned during this investigation apply to all sophisticated electronic systems currently in use or under development.

8.1. System Simplicity

The IAEA and its Member State Support Program (MSSP) developers should strive to keep systems as simple as possible. The more complex a system is, the harder it will be for the designer, manufacturer, users, and maintainers to work with and understand it. The concept is crucial when a system is designed by one contractor and manufactured by another, as is sometimes the case with MSSP activities in support of the IAEA. Systems must be designed in such a way that allows for another party to thoroughly understand them. This means that detailed design documents for both hardware and software must be prepared and the designer must be willing to share them.

The concept is also important when performance problems arise. Correcting performance issues often requires modifications to the equipment. Modifications to a system should be made such that the resulting system is as simple as possible. Additional complexity may result in components that interfere with one another. The casual introduction of additional components may result in a system that is more difficult to use, maintain or understand.

8.2. Understanding the Impacts of the Modification

If proper reviews are not performed and the parties effecting a system redesign do not adequately understand the system, a modification to correct one performance problem may result in the creation of another problem. Even if care is taken to simplify the design of a system, electronics are composed of hardware and software components that can be disrupted by the addition or subtraction of other components meant to correct performance problems. Whenever a modification is made to a system, a new design review should be undertaken to ensure that that the modification will not interfere with system operation and that every component is understood and will work as expected.

8.3. Configuration Management

As systems that are already in use are modified to add additional capability or to correct performance problems, it is impossible to reconfigure all owned systems to the same design and it is often not desirable to do so. The result is an inventory of systems that are configured in different ways to address different applications. Configuration management is an essential management tool that ensures an organization can identify each unit's configuration when necessary. The lack of a strong configuration management system can lead to performance issues when one or more units is installed in an environment for which it is not appropriate.

8.4. *Costs and Benefits of Testing*

The USSP endorses the concept of independent testing of equipment as a means to maximize the IAEA's knowledge of the performance level and limitations of equipment. The testing performed by Wyle Laboratories was designed to evaluate the operating envelope of the SDIS System to determine design limits and potential failure modes for evaluation of lifetime expectancy. Testing was designed to minimize the impact on the IAEA's installation schedule.

Professional, independent testing of equipment can be costly. At first glance it might seem that the cost of testing is not justifiable. However, the costs of testing should be compared to the costs associated with system bugs that remain undetected at the time of installation. If a performance problem is identified after equipment has been installed in the field, there are significant costs to modify, retrofit, and reinstall equipment. There are costs related to identifying the cause of failure, problem resolution, engineering the solution, modifying systems, and replacing the unreliable units. Failures also introduce delays in the installation and operation schedules. These delays as well as the loss of safeguards have non-quantifiable costs. These total costs associated with correcting performance problems are significant. As an example, the USSP contributed over US$500,000 in addition to the funding approved for independent testing to meet only the quantifiable costs associated with identifying the problems of the modified DCM-14-based system and correcting them.

The cost per DIS unit is sufficiently high to justify the expense of testing. The IAEA spent approximately US$2.5 million in each of 1999, 2000, and 2001 on DIS equipment needed to replace outdated analog counterparts. In addition to these capital expenses, the IAEA incurred expenses associated with the travel of staff installing the units in facilities. The testing undertaken by Wyle Laboratories amounted to less than 10% of the overall expense.

When addressing issues of safeguards implementation, traditional cost/benefit analysis may not be appropriate. Many of the costs and benefits related to safeguards are non-quantifiable. One cannot put a value on the credible conclusion of the nondiversion of nuclear material, but such a conclusion is very important in non-monetary terms. Likewise, the cost associated with the inability to draw that conclusion is non-quantifiable yet has a large impact on the IAEA's credibility and the member states' satisfaction with the organization. Therefore, while cost/benefit analyses are important in understanding the financial

costs of an activity, an activity such as testing of equipment should not be discounted because the quantifiable costs outweigh the quantifiable benefits.

8.5. Assessment of Environmental Conditions

A weakness encountered in the testing of DIS systems was the lack of formality in the assessment of the environmental conditions under which the SDIS system is utilized. The environmental conditions upon which testing was based were obtained via telephone communication. At the time, no written document was available to Wyle. These conditions must be well known, formally documented, and shared with designers and testing organizations to ensure that future testing activities are consistent with field conditions.

8.6. Avoid Testing "In the Dark"

Testing should not be the last step in equipment development. The qualities of reliability and security must be built in right from the start. A testing organization should participate in planning the development of such a system in order to ensure that the system requirements can be verified through testing. Moreover, testing should take place as soon as possible and at various points in the development process. Specifically, preliminary prototypes should undergo testing and all testing should be completed before implementation begins. Testing efforts undertaken after implementation may identify how the technology fails to meet its requirements, but the information can only be used to "fix" the product within the constraints of the existing design rather than fixing the design to ensure that it meets the intended requirements. Testing that is performed after products have been fielded can result in expensive analysis, modifications, and testing to prove the device is acceptable for the intended application.

Naturally, the IAEA would prefer not to be in the test-in-the-dark situation at all. However, if an organization is forced into a test-in-the-dark situation, the following approach is recommended to determine what testing should be undertaken:

- Determine the system requirements to know what testing needs to be done;
- Define the importance of quality to the project to decide how much time and effort can be devoted to testing;
- Define a test plan, including acceptance criteria, to build a consensus of the important elements of the system, and to know when purchase and installation are warranted

8.7. Need for Testing Standard Components

There is a need for an on-going, independent testing and certification program to identify robust, reliable and serviceable components for safeguards systems that require high reliability. The components may consist of uninterruptible power supplies, batteries, DC power supplies, industrial computers, data storage units and modems. Challenges facing the Agency include the rapid change in availability of critical components, the production of safeguards systems by third parties, and the Agency's lack of resources. An on-going, independent testing and certification program is the only way to identify robust and reliable components that can become the Agency standard. Such a testing and certification program can reduce costs by reducing maintenance of unreliable components, reducing nuclear material safeguards re-verifications required by equipment failures, and reducing the effort associated with technical support and training on a reduced number of components.

8.8. How Much and What Kind of Testing

As a part of the initial testing effort, Wyle Laboratories contracted with Quanterion Solutions Incorporated to develop the *IAEA Reliability and Maintainability Guidance Template.*[5] This document provides an overview of the reliability process in the development of critical systems such as the SDIS. Of particular note is the section on Reliability and Maintainability (R&M) Testing where different testing techniques are addressed. The testing techniques include reliability demonstrations, reliability growth testing, accelerated reliability testing, environmental stress screening, Bayesian reliability testing, maintainability demonstrations, and HALT/HASS[1] testing.

---

[1] The acronyms HALT and HASS stand for highly accelerated limit testing and highly accelerated stress screening.

Quanterion concluded that the reliability demonstrations, Bayesian reliability testing and the maintainability demonstrations are either very costly or difficult to implement. All of the other techniques were involved in the design limit and life determination testing on the SDIS that was completed by Wyle Laboratories. It is concluded that each of these techniques has a role in finding the right solution for a more reliable digital surveillance system.

The selection of testing methods must consider all aspects of the project including the following areas of technical and programmatic concern:

- Cost of the product
- Cost of testing
- Cost of product modification
- Time to complete testing
- Product deployment schedule
- Testing capabilities available
- New technology needed for testing
- Possibility of over-testing the product
- Ability to analyze the test results

Once these parameters have been considered and the available R&M Testing techniques are reviewed, the right solutions on the product design and testing can be made.

8.9. Acceptable Failure Rates

Despite efforts to design and manufacture reliable safeguards systems, the equipment will always fail in the field at some rate, albeit low. It is not realistic to expect safeguards systems to operate for year after year without any failures. The IAEA must develop a contingency plan for the instances when equipment will fail.

Conclusion

This paper addresses the steps taken to address operational issues related to digital image surveillance systems and the lessons learned during this process. The test methods, test results, conclusions and program recommendations from the Design Limit, Reliability and Life Determination Testing conducted on the SDIS by Wyle Laboratories personnel during testing completed in 2001 were provided. During this testing it was determined that the design of the SDIS system is mostly compatible with the environment in which it is used. The one major exception is the system's susceptibility to gamma and neutron radiation. Further testing at lower dose rates and total accumulated doses are currently planned or in progress at other facilities.

The lessons learned during testing of the SDIS are relevant to all sophisticated electronic equipment in use or under development by the IAEA.

REFERENCES

[1] WHICHELLO, J., "DCM14 Based Surveillance Systems Test Report on Improved HW, SW, and Firmware," March 2001.
[2] KORN, C., "Common Qualification Test Criteria for New Safeguards Equipment (K, Gaertner, P. Meylemans, and R. Mackowiak, Eds.), Joint Research Center, European Commission, 1999.
[3] WYLE LABORATORIES, Test Procedure 45449-10.
[4] WYLE LABORATORIES, Test Reports Number 45449-01, 45449-02, and 45449-03.
[5] QUANTERION SOLUTIONS, INC., "IAEA Reliability and Maintenance Guidance Template," May 2001.