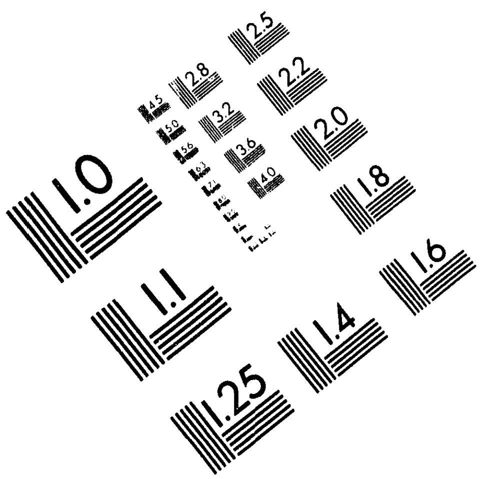
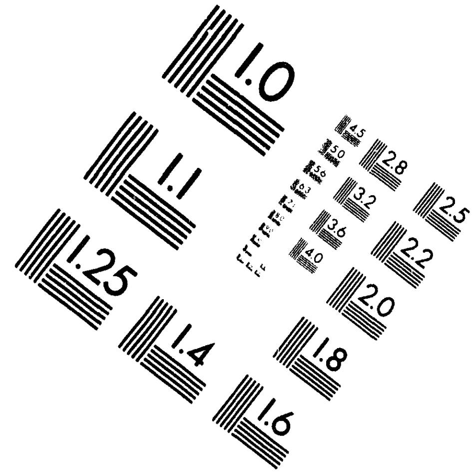
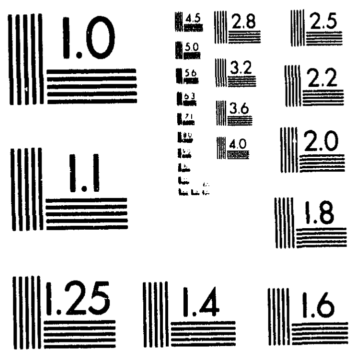


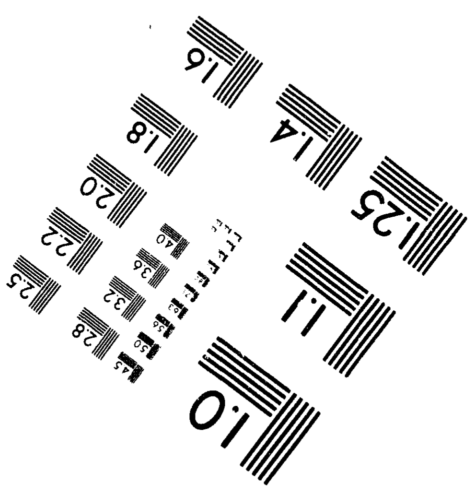
AIIM

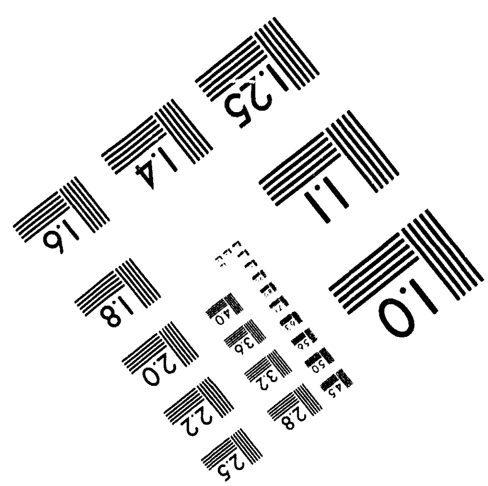
Association for Information and Image Management

1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910
301/587-8202









MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

1 of 1

Conf-940748--93
SAN094-0702C

Safeguards and Security Considerations for Automated and Robotic Systems

Sabina E. Jordan
Security and Survivability Department 5822
Sandia National Laboratories
Albuquerque, NM 87185-0761
(505)845-9077

Calvin D. Jaeger
Surety/Dismantlement Department 5821
Sandia National Laboratories
Albuquerque, NM 87185-0765
(505)844-4986

Abstract

Within the reconfigured Nuclear Weapons Complex there will be a large number of automated and robotic (A&R) systems because of the many benefits derived from their use. To meet the overall security requirements of a facility, consideration must be given to those systems that handle and process nuclear material. Since automation and robotics is a relatively new technology, not widely applied to the Nuclear Weapons Complex, safeguards and security (S&S) issues related to these systems have not been extensively explored, and no guidance presently exists.

The goal of this effort is to help integrate S&S into the design of future A&R systems. Towards this, we first examined existing A&R systems from a security perspective to identify areas of concern and possible solutions to these problems. We then were able to develop generalized S&S guidance and design considerations for automation and robotics.

Background

This project was sponsored by the Department of Energy (DOE) Office of Weapons Complex Reconfiguration. The project goal is to help integrate S&S into the design of future A&R systems that will be part of the reconfigured Nuclear Weapons Complex.

There are many benefits which could be gained from the application of A&R systems to the Nuclear Weapons Complex. An important benefit is the reduction in exposure of workers to hazardous environments. The use of automation and robotics helps support the as-low-as-reasonably-achievable (ALARA) criteria for minimizing worker radiation exposure. This will be especially important for the Complex in the future because of the likelihood of lower radiation exposure limits. Another important benefit is the reduction of hands-on access to nuclear material, which enhances security. Other benefits include high process repeatability, capturing of process knowledge, enforcement of procedures, automated audit trails, and

possibly lower life cycle and operational costs.

Systems Presently Being Developed

The Intelligent Systems and Robotics Center at Sandia National Laboratories (SNL) is the DOE/Defense Programs (DP) Center of Excellence for Automation and Robotics. To support the Weapons Complex Reconfiguration Program, a consortium of DOE automation resources, led by the Intelligent Systems and Robotics Center, was formed to provide automation guidance. They are working together with the Nuclear Security Systems Center at SNL to identify and develop appropriate S&S for A&R systems. Most of the Automation and Robotics work for Reconfiguration is in the baseline automation plan and conceptual design phase. There are, however, several projects for other DP programs further along in their development, which can yield insights into where S&S may be needed for future A&R systems.

Automated Weapon Disassembly: This system robotically performs several disassembly operations in a weapon disassembly process. The robotic system will do the portions of the disassembly process which involve the most radiation exposure.

Automated Pit Packaging: Packaging of the radioactive plutonium pit for long-term storage is a necessary part of the disassembly of a retired weapon. This system will automate the hands-on steps of pit packaging, significantly reducing worker exposure to radiation during the operation.

Weight and Leak Check System (WALS): The WALS project is the development of an automated system for performing remote weighing and leak checking of radioactive pits. WALS will remove operators from the contact handling operations which contribute most to radiation exposure. The WALS hardware appears in Figure 1.

Figure 1. Weight and Leak Check System

Automated Pit Radiography: A robotic system for automating handling of pits during radiography and the handling of radiographic media is being developed. This system will reduce operator radiation exposure obtained during manual pit handling operations.

Automated Glovebox Bagout System: When material must be removed from a glovebox, a procedure called bagout is used whereby material is removed from the glovebox through a bag-covered port. Manual bagout is considered potentially hazardous due to radiation exposure. Automation of the bagout process reduces radiation exposure of the operators, enhances security by removing the operators from the work area, and reduces the quantity of contaminated waste generated by the bagout process.

Automated Pit Handling (Stage Right): A solution to increase the staging capacity for pits at Pantex is to stack pallets of pit containers in the magazines, thereby increasing the capacity of each magazine. This, however, will preclude personnel from working for extended periods in the magazines due to increased radiation levels. The Stage Right concept involves stacking pallets of pit containers into the magazines using an automated guided vehicle (AGV). The AGV will perform the pallet storage/retrieval operations. The AGV that will be used for Stage Right is an automated forklift, and is pictured below in Figure 2.

Figure 2. Stage Right Automated Forklift

Threat Definition for A&R Systems

Most of the A&R systems will likely be located in the Material Access Area (MAA) of facilities. While location within the MAA already provides a great deal of security, location alone should not necessarily be relied upon to meet all of the S&S needs for the A&R systems.

The physical protection system of a facility provides several layers of protection that an Outsider adversary would have to defeat before being able to reach the MAA. For the A&R systems located within the MAA, the major threat to be concerned with is the Insider who has access to the MAA. Potential adversary actions are sabotage (industrial/radiological/toxicological), theft of special nuclear material (SNM), or diversion of SNM (e.g., unauthorized placement within the MAA).

Some sites have a Human Reliability Program (HRP) in place for workers given access to the MAA, which helps mitigate the threat from the Active Insider. However, for the Insider to be considered exclusively Passive requires both an HRP and other basic elements of Insider security, some of which could be provided by the security features of A&R systems. Additionally, DOE Order 5632.2A on the physical protection of SNM, leads us to consider S&S features for A&R systems.

S&S for A&R systems is of course very important when considering the Active Insider. It may be necessary to consider the Active Insider for A&R systems of the future. It is not difficult to imagine that the Insider threat for the 21st century will escalate, especially with the Complex scaling down, possibly yielding an increased number of disgruntled employees.

Another reason to consider the Active Insider is that the use of A&R systems introduces new elements to the security equation. For example, using A&R systems to perform remote handling could allow the adversary to achieve radiological sabotage without having to contaminate himself or herself, which may be more attractive. Or, colluding Insiders may no longer be needed to perform a physically challenging adversarial goal; the A&R system could help a single adversary perform it. Also, with "complicated" A&R systems, adversarial action could be claimed to be an innocent

mistake or an A&R malfunction, making adversarial intent harder to prove.

Generalized S&S Guidance for Future A&R Systems

The security suggestions and observations in this section should be considered for future A&R systems' designs since they are important in addressing the Insider threat. For the most part, the suggestions presented here would not be difficult to implement, and also could be retrofitted into existing A&R systems if needed.

Use Control

Enforcement of the two-person rule is required by the DOE order on the physical protection of SNM. The A&R systems must therefore have two-person login to impose the requirement of two authorized users needed to operate the equipment. The use of passwords are an option for personnel identity verification at login, but the application of a biometrics device (e.g., hand geometry or retinal scan) would provide a much greater degree of security since passwords can be compromised, unlike unique physical characteristics. The user workstation should also prohibit unauthorized re-booting, which would prevent access to the system by resetting of the hardware. When the user program which operates the A&R system terminates, the workstation should always return to the login prompt.

The implementation of various user privilege classes, such as separate levels of privilege for a technician, a supervisor, and a system administrator, is a good idea. This would limit unnecessary access to sensitive parts of the system not required by a person to perform his or her job. This compartmentalization would prevent both intentional and non-intentional adverse events from occurring.

Another very useful security feature to include would be audit logs, such as a user command log and a sensitive file access log. The logs would include the identified user, along with the operations performed by the system. The audit information would act as a deterrent to misuse of the system (providing employees were aware they were being audited), and would be useful for resolving incidents after the fact.

Trusted Operation

Extensive and rigorous testing of the software and hardware during development is critical to ensure trusted operation. As part of maintenance, it is also important to perform some testing on a periodic basis after the system has been installed.

Another important practice is the implementation of warnings or better yet, prevention mechanisms, when changes are made to the software that are inconsistent with safety. For example, if path points in a data file were changed incorrectly, the robot could smash a pit into a work surface.

Checksums are a mathematical function calculated over all the bytes in a file or program. Performing checksums on the software is a good practice. It should be done at installation to verify that the software delivered is the same software that was tested, and also periodically to ensure the software's integrity.

Networking Concerns

A subject which introduces some security concerns involves networking the

A&R systems to other computers at a facility. The problem in doing so is that it opens up the possibility of break-ins via the network. Connecting to a closed, classified network within the MAA would be fine, but where break-ins become a concern is in considering the possibility of future multi-level security computer networks which might be part of the modernized Complex. Some prevention measures and alternatives that still allow information to be shared with other computers include:

- Use of a "sneaker-net" where data is exchanged between computers via a person walking over with the data stored on electronic media

If networking is implemented,

- Have network fire walls in place which enforce limited accessing capability
- Boot off of removable hard disks, for example, to prevent the A&R software from being changed via the network
- Perform verification of file integrity before each session by the use of checksums
- Use more robust authentication techniques for network login than passwords, e.g., smart cards (which make passwords a "moving target" with time and are therefore difficult to "sniff" off the network), or even better, biometric login

Protection of Hardware

The critical hardware involved in controlling the A&R system, (e.g., a robot controller, or an on-board computer for an AGV) should have tamper detection or protection. Items such as teach pendants, which are used to "train" the robot and can control it, and robot keys should be secured from unauthorized access.

Maintenance

Maintenance personnel, both hardware and software, are always one of the most significant Insiders to consider. The threat from a maintenance person could be reduced by:

- Requiring two-person teams for the maintenance of critical systems (each person must be technically qualified to detect tampering by the other)
- Performing effective testing after maintenance operations are completed

Special Concerns for AGVs

There are some additional security concerns that come up when considering AGVs. Examples of undesirable events involving AGVs include the possibilities of diversion of SNM, switching "full" with "empty" or "waste" containers, causing criticalities or SNM item damage, and bringing unauthorized items into storage areas (e.g., explosives or flammables). Some suggested security features for AGVs include:

- Separate flows for personnel and AGVs as much as possible, separated by physical barriers
- No hands-on access to the AGVs or its cargo, except under very special conditions (maintenance, etc.)
- Secure wireless communications link to AGVs using encryption or some other means to prevent unauthorized interception or substitution of data
- Intrusion detection over the AGV tracks and tamper detection on the control lines
- Multiple system safeguards to prevent vehicle crashes, criticalities, etc.

– Technology for the continuous monitoring of SNM while in transit

Interface to Other Systems

It is important that the S&S for the A&R systems integrate well with the overall facility security system, for example, the alarm communications system. Also, integration of automated processing and handling of SNM with Material Control and Accountability, would significantly streamline inventory procedures.

Summary

A&R systems presently under development were examined to identify S&S guidance for future A&R designs. Here we presented a list of generalized security considerations for A&R systems, but each different A&R application must be thought through individually, and the appropriate safeguards then applied. Any S&S implemented for an A&R system should be done in the context of the overall facility security system, and of course, should be commensurate with the threat and consequences involved. Cost-benefit analysis should be performed and the level of acceptable risk considered. Although the project goal is to be able to design security in up-front for A&R systems, since that is most efficient and least expensive, the S&S guidance presented here could also be used for retrofitting existing systems.

Acknowledgments

The authors wish to gratefully acknowledge the support and contributions of Bill Drotning, Jill Fahrenholtz, Al Jones, J. F. (Red) Jones, Howard Kimberly, Larry Shipers, and Bob Watson of the Intelligent Systems and Robotics Center at SNL, and also, Mark Snell of the Nuclear Security Systems Center at SNL.

This work was supported by US Department of Energy under contract DE-AC04-94AL85000 and by the Department of Energy Office of Weapons Complex Reconfiguration, DP-40.

Bibliography

1. Quintana, G.R., Thunborg, S., and Morimoto, A.K., *Secure Automated Canning and Identification Task (SACIT)* 32nd Annual INMM Meeting Proceedings July 1991

DATE
FILMED
10/20/94

END