SAND2009-7888C

Considerations for Joint Use of Equipment

K. Tolk
Sandia National Laboratories
M. Zendel
International Atomic Energy Agency

November 2009

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

What Drives the Joint Use of Equipment?

- The verification and monitoring of nuclear material at increasingly automated nuclear facilities require sophisticated, often expensive installed safeguards equipment within the various process areas.
- The sharing of such safeguards equipment between IAEA, national or regional SSACs and operators becomes the only viable solution to meet efficiency and effectiveness goals for IAEA safeguards implementation.
- Legal commitment (INFCIRC 153/(corrected) article 7 and 31) :…the Agency in carrying out its verification activities, shall make full use of the State's system of accounting for and control of all nuclear material….shall avoid unnecessary duplication….

Why JUE?

- Safeguards data may be more easily obtained by the Agency with equipment provided by the State or the operator than that the Agency could not obtain with strictly independent equipment;
- The Agency may save resources by sharing with operators or State authorities the costs of acquiring, maintaining and operating safeguards equipment;
- Facility operators may find Agency safeguards less burdensome if installed operator equipment is used for some safeguards measurements; and
- Inspector and technician radiation exposure may be reduced.

Why not JUE?

- The independence of the Agency's safeguards conclusions may come into doubt;
- The integrity and authenticity of data obtained from joint-use equipment may be difficult to ensure;
- Safeguards measures may be easier to defeat when operators or State authorities know the exact performance characteristics of safeguards equipment;
- Safeguards measures may be easier to defeat when operators or State authorities have direct access to the data from safeguards equipment; and
- The addition of the required IAEA authentication measures may result in unacceptable additional costs, when compared to a non joint-use of safeguards equipment.

The Joint Use Arrangement

- Each Joint Use Arrangement (JUA) must be approved by the Deputy Director General of Safeguards.
- The IAEA should be involved early in the facility design phase and the instrument development process to ensure that the Agency's needs for authentication, integrity are met and to minimize the impact on the partner in the JUA.
- A vulnerability analysis of the system as it will be used under the joint use arrangement is required. This is in addition to the similar analysis performed during the Instrument Authorization Procedures.
- If equipment is shared which does not meet all requirements for JUE as specified below, adequate additional measures on a case by case basis need to be agreed to compensate for the shortcoming

Impact on the Partner in the JUA

- The JUE will be kept under seal using either IAEA seals or common seals and will not be physically accessible to the other party in the JUA without IAEA presence. This may cause operational issues in the case of equipment failure.
- The other party may also not have immediate access to the data from the equipment. Some data might never be shared.
- Any upgrades and software patches must be approved and installed by the IAEA.
- The JUA should address how calibration and other routine maintenance will be performed.

The Need to Trust the Data

- The question is often asked, “Has anyone ever attempted to tamper with the IAEA’s data or equipment?” If adequate equipment authentication, tamper indication, and data authentication measures have **not** been implemented, the only valid answer is “I don’t know”.
- The IAEA must have adequate assurance that the data used to draw safeguards conclusions is valid. Otherwise, they cannot defend those conclusions.

Trust

- The partners in Joint Use Arrangements are often frustrated by the limitations placed on them with respect to equipment access and data sharing, leading them to ask, “Why don’t you trust us?”
- In many cases, the trust that they desire would allow them to alter the equipment or the data, which would bring the independence of the IAEA’s conclusion into question.
- This level of trust would require a directive from the Director General of the IAEA. Without that directive, the partner must be viewed as a potential adversary.

Trust (continued)

- The IAEA may use data generated from other “non-trusted” operator’s equipment as additional information for consistency purposes.
- In some cases, the IAEA might use data from operator’s equipment that cannot fully meet JUE requirements if the authenticity of the data can be ensured through additional measures.

The Assumed Adversary (1of 3)

The assumed adversary for equipment development and vulnerability assessment is referred to as the “National Level Threat”. The following are some of the characteristics of this threat level for this type of application:

- Knows everything about the system except the passwords and secret or private cryptographic keys.
- Can likely obtain a copy of the equipment on which to develop and test tampering scenarios.
- Can draw on the computing capabilities of a national entity.

The Assumed Adversary (2 of 3)

- Has experts with extensive knowledge of cryptography and system penetration techniques.
- May know operating system vulnerabilities that have not yet been made public and are not yet addressed in commercial security software.
- Can draw on extensive manufacturing capabilities – can produce exact counterfeits of enclosures and other equipment that might be damaged during a tampering attempt.
- Has complete physical access to all equipment outside the STIEs, including all communications/signal cables.

The Assumed Adversary (3 of 3)

- Has the ability to measure electromagnetic emissions to discover security related information, such as when a triggered measurement is being taken.
- Could alter the measurement configuration, for example, radiation sources or shielding can be introduced to influence the nondestructive assay of a sample.
- Can produce complex and sophisticated radiation sources for use in tampering scenarios.
- Has extensive time, resources and access to the equipment's location to assess its operation under a range of scenarios over which the adversary has control.

Equipment Authentication

- The equipment must be designed for authentication. Attempting to add authentication features after the design is complete has proven to be expensive and may even be impossible.
- The IAEA should be involved in the equipment design as early as possible to ensure that adequate authentication features are incorporated.
- The equipment, including the sensors and data cables must be encased in tamper indicating enclosures. However, the design of the equipment should minimize the amount of tamper indicating surface area that must be inspected.

Equipment Authentication (2)

- If possible, the equipment should monitor itself for tampering.
- The equipment must be sealed inside a tamper indicating enclosure at any time that an adversary might gain access to it.

Data Authentication

- Data authentication is a cryptographic process that is used to provide assurance that the data came from the designated sensor, was collected in the appropriate time window, and that it has not been modified after it was taken.
- Data authentication must be applied to data before it can be modified by an adversary.

Data Sharing

- The general policy of the IAEA is to avoid sharing data, but some level of data sharing is part of almost all joint use arrangements
- Since all measurements have unavoidable measurement errors, the data should not be shared until the operator has made his declaration. Otherwise, the declaration might be altered to take advantage of these measurement errors.
- All data that is transmitted outside of tamper indicating enclosures without encryption should be considered as having been shared.

Equipment Dependent Data Sharing Issues

- If data is being shared, the adversary knows when equipment fails and might take advantage of the situation. This is especially problematic with seals.
- When one system, such as a portal monitor or motion sensor, is being used to trigger another system, such as a camera, the trigger signal must be obfuscated to prevent the adversary from learning the sensitivity of the trigger.

Summary

Joint use equipment can potentially save money, effort, and radiation exposure to workers. However, the equipment and safeguards approach must be designed to accommodate the special considerations to make the sharing successful. All parties to the agreement should be aware of the possible drawbacks to sharing the equipment.