

A Dictionary for Mayak Transparency

Richard Kouzes

November 16, 2001

Prepared for
The U. S. Defense Threat Reduction Agency

Pacific Northwest National Laboratory
Richland, Washington 99352

A Dictionary for Mayak Transparency

Richard Kouzes

Pacific Northwest National Laboratory

November 16, 2001

Introduction

There are many terms that are used in association with the DTRA Transparency Project associated with the Mayak Fissile Material Storage Facility. This is a collection of proposed definitions of some of these terms. There is a MPC&A glossary with Russian translations (PNNL-11762) with a small overlap of information. The IAEA also has a safeguards glossary of terms that is out of print, and has no overlapping terms (IAEA/SG/INF/1 1987).

A

Anonymous purchase is a process whereby the true purchaser and the intended purpose are hidden from the supplier as a means of obtaining a trustworthy and uncorrupted component. This procedure may be used by the Host to procure uncorrupted components for use and by the Monitor to procure a baseline copy for future comparisons during authentication activities. An Anonymous purchase assumes a mass market for the items, and is not possible when the market is less than many hundreds of items/year.

Applications Software is defined as software used to implement data analysis and equipment control. Equipment control software includes all the software used to support the basic functioning of the equipment used for measurements, as well as data collection from that equipment. For example, the Canberra Inspectors use drivers (from a support library), software to collect the data, and software to analyze the data. This is all applications software and subject to full disclosure of source code.

The **Applications Specialist** for an instrument is the most knowledgeable person about that particular instrument available for consulting with Monitors. Normally he/she will have been the task officer for the development or authentication of the equipment.

Attribute is a specific physics related quantity derived from measurement and analysis. The four currently proposed attributes for material stored at Mayak are: presence of special nuclear material, weapons grade material, mass above a threshold, and presence of metal. The range of acceptable attribute values, as well as the algorithms for extracting attribute values from potentially classified data, can be discussed openly. An attribute-based measurement system contains some physics-based analysis to extract pre-agreed parameter values from the measurement data and generally uses statistical analysis for error propagation and result evaluation.

Attribute Measurement System is measurement instrumentation (e.g., radiation, weight) that makes a measurement and analyzes the data to produce an attribute value. This term was applied to the first specific system proposed for use in the FMSF absolute control room.

Authentication is the process through which the Monitoring Party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item. (*Authentication Task Force definition*)

Authentication (IAEA) is the process of assuring that genuine information is obtained for safeguards purposes using equipment for which the IAEA lacks sufficient control or knowledge. (*IAEA definition draft May 2001*)

Authentication Assurance Level (AAL) is a package consisting of assurance components from document ISO/IEC 15408-3 that represents a point on the common criteria assurance scale that must be met to attain a given level of authentication assurance. Each AAL represents a band of confidence obtained by requiring passage of selected documentation completeness levels and authentication measures. The AALs are most useful in balancing authentication requirements to avoid leaving a major credibility gap.

An **Authentication Test Plan** is defined as the detailed plan for the steps necessary to achieve authentication of the equipment. It is used to ensure that the actual equipment system conforms to the provided documentation, functions only as specified (i.e., free of covert features), and meets the user requirements and the technical specifications.

B

Baseline is a set of critical observations or data used for comparison or control. Baseline implies a known, well-documented state. For example, baseline observations could be obtained from items either independently procured or obtained by random selection for extensive private examination. Authentication efforts in the field rely on comparisons to a set of baseline data. For example, installed software is compared to previously examined code.

C

Certification is the process by which a Host Party assures itself that an inspection system integrated with an information barrier will not divulge any classified information about an inspected sensitive item to a Monitoring Party. Certification also includes all processes required for the Host to allow operation of the system within its facility.

Commercial off the Shelf (COTS) is a commercial product that is available for anonymous purchase in a mass market.

Common Criteria are international standards that provide a common set of requirements for the security functions of information technology products and systems and for assurance measures applied to them during a security evaluation.

Common (Evaluation) Methodology is the methodology for authentication measurements evaluation; it describes the minimum actions to be performed by an evaluator to conduct a common-criteria evaluation.

Confidence is a faith, belief, or assurance that parties to an agreement will act in a right, proper, or effective way. In statistics, confidence is usually expressed as a probability that a statement is true and quantifies the reliance that can be placed in a statement about a parameter.

Continuity of Knowledge (CoK): For purposes of the FMS, CoK of material is defined as “knowing the identification and location of every AT-400R container at all times following declaration.”

D

Defect means a condition of an item that does not meet the expected characteristics. For Mayak, this is the failure of a container to meet at least one required material attribute, or a missing container.

Defective Item is defined as a container that fails to meet one or more of the prescribed attribute criteria.

E

Evaluation Assurance Level is a package consisting of assurance components from document ISO/IEC 15408-3 that represents a point on the common criteria assurance scale that must be met to attain a given level of security assurance.

F

Fissile Material Storage Facility (FMSF) is the storage building complex at Mayak that is being built with US funds by DTRA to store weapon-origin material.

Functional Testing is testing of systems and components to insure that they function as designed and disclosed. Functional testing of radiation monitoring equipment includes, but is not limited to, testing with a set of physical and/or electronic sources. Only exhaustive functional testing, which considers all possible input states and sequences, can insure that covert features are not included.

G

H

Hash Function: A hash function uses an algorithm to mix a multi-byte seed value with a data block to produce a multi-byte digest value, usually of the same length as the seed. Whenever the number of digest bytes is much smaller than the data block, it is impossible to reconstruct the original data from the digest value. A hash-function-based comparison compares the digest values of two data blocks when hashed with the same seed value. The large number of possible input seed values makes the comparison robust against intentional modifications. In contrast, a simple checksum comparison intended to detect rare accidental errors is easily defeated by an intentional modification. A hash-function scheme is commonly used with computer security and digital signatures.

Host Party refers to the Russian Federation or its representatives for the Mayak FMSF regime.

Host Supply of equipment implies that the Host Party will provide all measurement and surveillance systems. At a minimum, Host-supply means that the Host has last private access to all the equipment to perform certification. Under Host-supply, the Host may obtain portions of the hardware and/or software from vendors associated with the Monitoring Party.

I

An **Information Barrier** consists of technology and procedures that prevent the release of Host-Country classified information to a Monitoring Party during a joint inspection of a sensitive item, while promoting assurance of an accurate assessment of Host Country declarations regarding the item.

Integration is the process of combining sub-systems of detectors, hardware, and software into operational systems with all the documentation, functional testing, and procedures necessary for the regime.

J

Joint Executive Committee is a US-RF group that manages the implementation of the monitoring regime at FMSF Mayak.

K

L

M

Monitoring Party generally refers to the United States or its representatives when related to a bilateral FMSF regime. It is also recognized that the International Atomic Energy Agency could act independently as the Monitoring Party under another regime.

N

O

P

Procedures are written descriptions of the steps involved in performing specific operations, which could include design practices, manufacturing processes, authentication activities, or inspection protocols.

Q

R

Random Selection refers to the process by which the Monitoring Party selects among two duplicate Host-supplied items that have been fully tested and certified.

Reliability is the continued ability of a component to complete its intended function with independent confirmation of that ability.

Remote Monitoring System is an unattended monitoring system that electronically communicates monitoring data to monitors at another site.

S

Sampling Plan is a statistical means used to select a portion of items for measurement or other special attention.

System Effectiveness is the measure of the ability of a system to detect a defect.

T

Tamper-Indicating Device (TID) is a device or seal that provides permanent evidence of any attempt to gain access to the sealed item. Each TID must be uniquely identifiable to preclude replacement with a counterfeit duplicate.

Tamper-Indicating Enclosure (TIE) is an enclosure with tamper indicating features that provides permanent evidence of any attempt to gain entry to the interior. The enclosure can either be self-sealing or sealed with an external Tamper-Indicating Device.

Template Measurement System is a term applied to a measurement system that makes a comparison of measurements, such as parts of gamma ray spectra, between an unknown item and a known item. A template-based system may just state that the two items are similar or different using statistical comparison techniques without necessarily using any physics-based data analysis to extract fundamental attribute values.

Transparency is a means of gaining confidence by examination and provision to obtain evidence that specified requirements have been fulfilled. When *Transparency* is applied to equipment, it means that the design and operations of a monitoring system are completely open and fully understood by all parties. (see Verification)

Transparency Regime refers to an agreement to perform some specified action in an open manner so that other parties to the agreement gain confidence that the specified action has occurred. A Transparency Regime requires less confidence by direct inspection/measurement than a Verification Regime where the national security stake is higher. (see Verification Regime)

Transparent System refers to a completely documented system where one has the ability to look into all the design and component details as a means of gaining a full understanding of all the processing occurring within the system. (see Verification)

U

Unattended Monitoring System: A monitoring system designed to take data on the operation of the facility being monitored while the U.S. monitors are not present.

V

Validation is confirmation by examination and provision to obtain objective evidence that the particular requirements for a specific intended use are fulfilled.

Validation (MC&A) is

- Confirmation, by testing, that an implemented, operational system or critical

- system element meets established requirements.
- Process used to verify the accuracy of data gathered during an inspection or survey.

Verification is confirmation by examination and provision to obtain objective evidence that specified requirements have been fulfilled. (see Transparency)

Verification Regime refers to an agreement to perform some specified action and allow the other parties to the agreement to insure that the specified action has occurred. A Verification Regime generally applies when national security is at risk if the action is not performed as agreed. A Verification Regime requires a higher degree of confidence regarding compliance than a Transparency Regime. Many of the methods of achieving sufficient confidence are similar, but they are pursued more vigorously and with more resources. (see Transparency Regime)

Verification (MPC&A): Process whereby information is evaluated relative to appropriate standards.

Vulnerability (PP): Exploitable weakness or deficiency in a system or at a facility.

Vulnerability assessment/analysis (PP): Systematic evaluation process in which qualitative and/or quantitative techniques are used to identify vulnerabilities and recommend upgrades to a MPC&A system.

Vulnerability Assessment (Host) is the set of procedures typically used by the Host Party to identify potential security threats to a system. It would establish that the procedures for, and the design of, an information-barrier-protected system adequately protect classified information over the entire lifecycle of use. The Host's assessment would include consideration of potential methods of covertly extracting information and the probability of discovering all such methods. (see Certification)

Vulnerability Assessment (Monitor) is the set of procedures typically used by the Monitoring Party to identify potential threats to a system relative to the credibility of an information-barrier-protected system (authentication) and to establish that authentication efforts are adequate relative to the regime. A Monitoring-party vulnerability assessment would consider the probability of the authentication team finding various example spoofs/hidden switches and the completeness of the authentication effort. Monitoring Party concerns regarding protection of classified information are limited to a desire that the system be certifiable in both countries (potential reciprocal agreements).

Vulnerability Assessment Level is a package consisting of assurance components from document ISO/IEC 15408-3 that represents a point on the common criteria assurance scale that must be met to attain a given level of authentication assurance. The VALs have been defined by the IAEA for their evaluation of monitoring equipment.

W

X

Y

Z

Acronyms

AAL	Authentication Assurance Level
AMS	Attribute Measurement System
CoK	Continuity of Knowledge
CoKALs	CoK Assurance Levels
COTS	Commercial off the shelf
CPU	Central Processing Unit
CTR	Cooperative Threat Reduction
DOE	U.S. Department of Energy
DTRA	U.S. Defense Threat Reduction Agency
EAL	Evaluation Assurance Level
FMCP	Fissile Material Control Program
FMS	Facility Monitoring System
FMSF	Fissile Material Storage Facility
HEU	Highly Enriched Uranium
HPGe	High-Purity Germanium Detector
HRGS	High-Resolution Gamma Spectrometry
IAEA	International Atomic Energy Agency
IB	Information Barrier
ISMS	Inventory Sampling Measurement System
IT	Information Technology
JEC	Joint Executive Committee
JTAG	Joint Technical Advisory Group
NMC	Neutron Multiplicity Counter
RAM	random access memory
RD	Recording Device
R.F.	Russian Federation
SNM	Special Nuclear Material (usually plutonium or HEU)
TID	Tamper-Indicating Devices
TIE	Tamper-Indicating Enclosure
TOE	Target of Evaluation