LA-UR-99-6053 (Rev.)
February 2000

Proposed Attribute Measurement System (AMS) with Information Barrier Fissile Material Transparency Technology Demonstration: The Security Watchdog

Duncan MacArthur
Geoffrey Dransfield
Chip Johnson
Richard Ortiz
Larry Sprouse

BACKGROUND

The objectives of the Fissile Material Transparency Technology Demonstration (FMTTD) demonstration are:

1) to demonstrate to the Russian delegation that an attribute measurement system (AMS) can be built with sufficient protection to allow measurement of classified components without revealing classified information, and
2) to construct this AMS in such a manner as to convince the Russian delegation that it would be possible for an inspecting party to fully authenticate operation of the system.

The AMS illustrated in Fig. 1 was designed to meet both of these goals. More details of this design are included in Ref. 1; Ref. 2 is a description of the entire system.

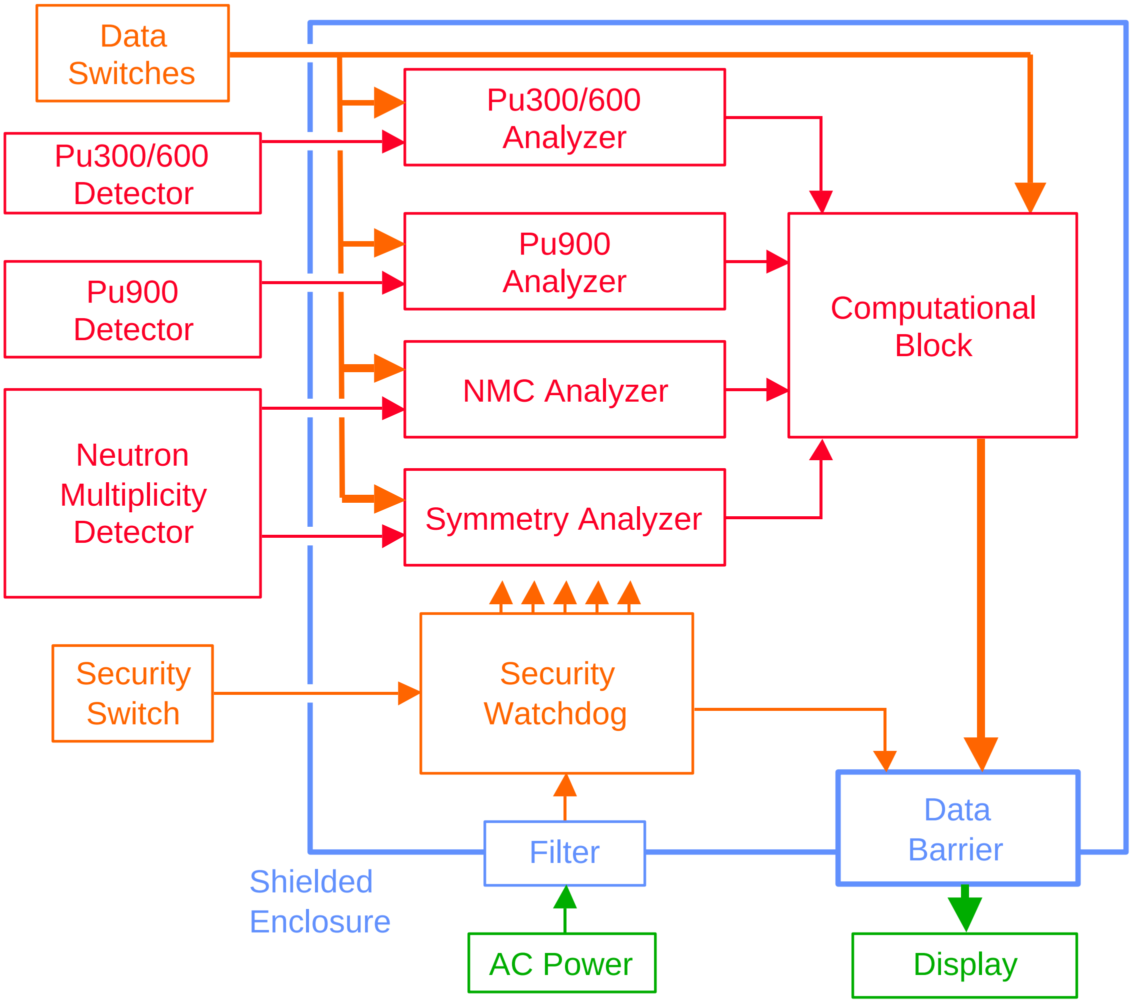

Fig. 1. Block diagram of attribute measurement system (AMS) for FMTTD. All of the other elements of the AMS receive their power through the security watchdog. This power connection is the only connection between the security system and the data analysis systems (detectors, analyzers, and computational block).

Six attributes will be measured in the demonstration AMS. These are:

1) Presence of plutonium,
2) plutonium isotopic ratio,
3) plutonium mass,
4) plutonium age,
5) presence of oxide, and
6) symmetry of plutonium.

Measurement of any of these attributes requires use of a detection system that generates classified data. Thus, an information barrier hides all of the “raw” data and only unclassified yes/no threshold evaluations are shown on the unclassified display.

As shown in Fig. 1, the raw data generated in the detection systems passes into the shielded enclosure to the specific data acquisition systems and analyzers. Both the raw data from the detectors and the analyzed data from the analyzers will be classified if a classified item is being measured. The analyzed results pass into the computational block where the threshold values are stored and threshold comparisons are performed. The outputs from the computational block, in the form of yes/no data are passed through the data barrier and finally to the unclassified display.

Several additional important elements of the AMS are also illustrated in Fig.1. All power for the AMS enters the security watchdog through an ac line filter. The only function of the security watchdog is to monitor the security status of the entire system and to remove all power from all other AMS elements if the access doors are opened or if classified material is introduced into the system incorrectly. The security mode of the security watchdog (and hence the entire AMS) is set by the security switches. In addition, several data switches are used to start a background run, start calibration runs, and start measurement runs.

INTRODUCTION

The demonstration AMS can operate with the access doors open or closed. When the access door is closed, a red and green LED display is the only output from the system. In this configuration, either classified items or unclassified reference materials can be measured, but only the simple unclassified display is possible. When the access door is opened, all power is immediately removed from the system. Since no data is stored in non-volatile memory, this power removal, in combination with an active purge procedure, will ensure that no classified information can remain in the AMS after the door is opened. If, and only if, a known unclassified container is present in the AMS, the security watchdog will restore power to the AMS following a delay of approximately 20 seconds. This will allow authentication measurements to take place using unclassified reference materials only. If the unclassified object is removed from the system while the door is open, all power to the system will be immediately cut off and will remain off until the unclassified item is replaced or the shielded enclosure access door is closed.

All power for the AMS enters the security watchdog through an AC line filter. The only function of the security watchdog is to monitor the security status of the entire system and to remove all power from all other AMS elements if the access doors are opened or if classified material is introduced into the system incorrectly. The security mode of the security watchdog (and hence the entire AMS) is set by the security switches that are controlled by the security container itself without human intervention.

An important feature of the demonstration AMS is the separation between the security and data processing functions. The security switches control the security watchdog directly. The security watchdog, in turn, controls the power to all of the other elements of the AMS, **but** there is no other connection from the security watchdog to the CPUs. Thus, the CPUs do not know the position of the security switches and have no way of knowing whether they are processing classified or unclassified data. This adds some assurance that the analyzers are operating identically whether or not a classified item is being measured.

Since the only function of the security watchdog is to control the AC power to the rest of the AMS, the security watchdog can utilize simple relay logic with no silicon components or software. There are two power relays in the watchdog. The first, or main, relay turns on AC power to the remainder of the AMS if, and only if, the doors to the shielded enclosure and any auxiliary enclosures are closed. In this case power is applied to the AMS regardless of whether or not classified objects are present. If a door is opened, the main relay contacts open, and all power is removed from the remainder of the AMS. Following a delay of approximately 20 seconds, a second relay (K2) will close (re-energizing the AMS) **only if** a known unclassified container is present (as determined by the security switches).

In addition, the security watchdog incorporates a SCRAM switch that, if pressed, will remove all power from the AMS regardless of whether classified material is present or not.

DETAILED DESCRIPTION

The functionality of the security watchdog circuit is illustrated in Fig. 2. This figure does not document several fuses, circuit breakers and power switches that are required for safe operation of the watchdog and AMS, but are not part of the security function. The assembled security watchdog chassis is pictured in Fig. 3. The entire detailed schematic of the security watchdog is included as Fig. 4. The following description references Fig. 2.

The DC power supply for the watchdog supplies power to the coils of both of the relays. The SCRAM switch can interrupt power to both relays. If all of the door switches are closed (i.e. all of the doors are closed), then relay K2 is energized, supplying AC power to the remainder of the AMS. If the doors are closed, K2 will be energized regardless of the position of the security switches. Thus, either classified or unclassified material can be measured with the door closed.

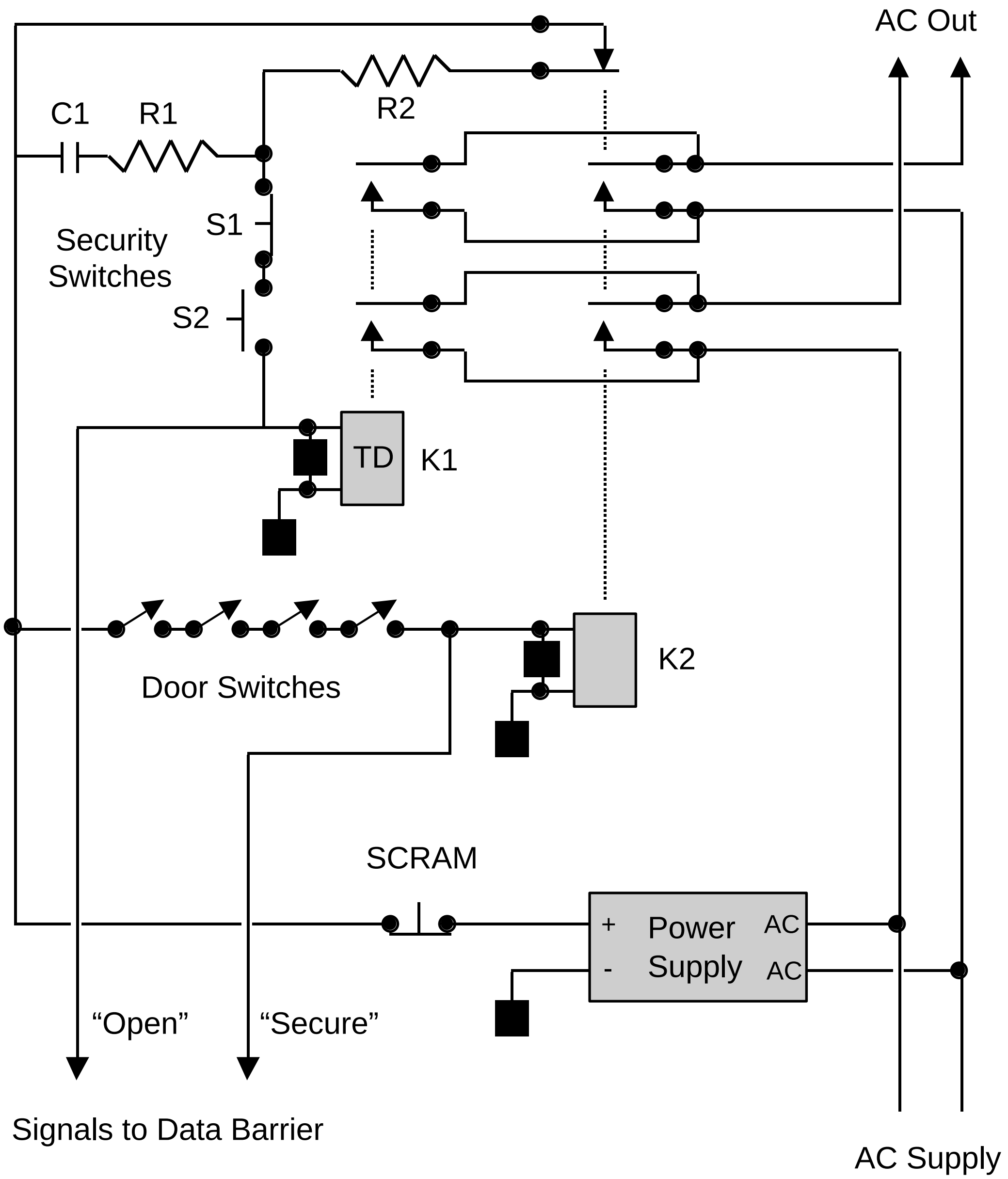

Fig. 2. Functional schematic showing security related components of the security watchdog. All components shown in this figure, other than the switches, are mounted within to the security watchdog chassis that is inside the shielded enclosure.

If any of the door switches are opened, power is removed from relay K2, disconnecting AC power from the rest of the AMS. When this happens, the normally closed contact of K2 closes, supplying power to the coil of time delay relay K1 through resistor R2 if both security switches are closed. The time delay is set to approximately 20 seconds. If either of the security switches is opened at any time, then power is removed from K1 and the AMS is de-energized.

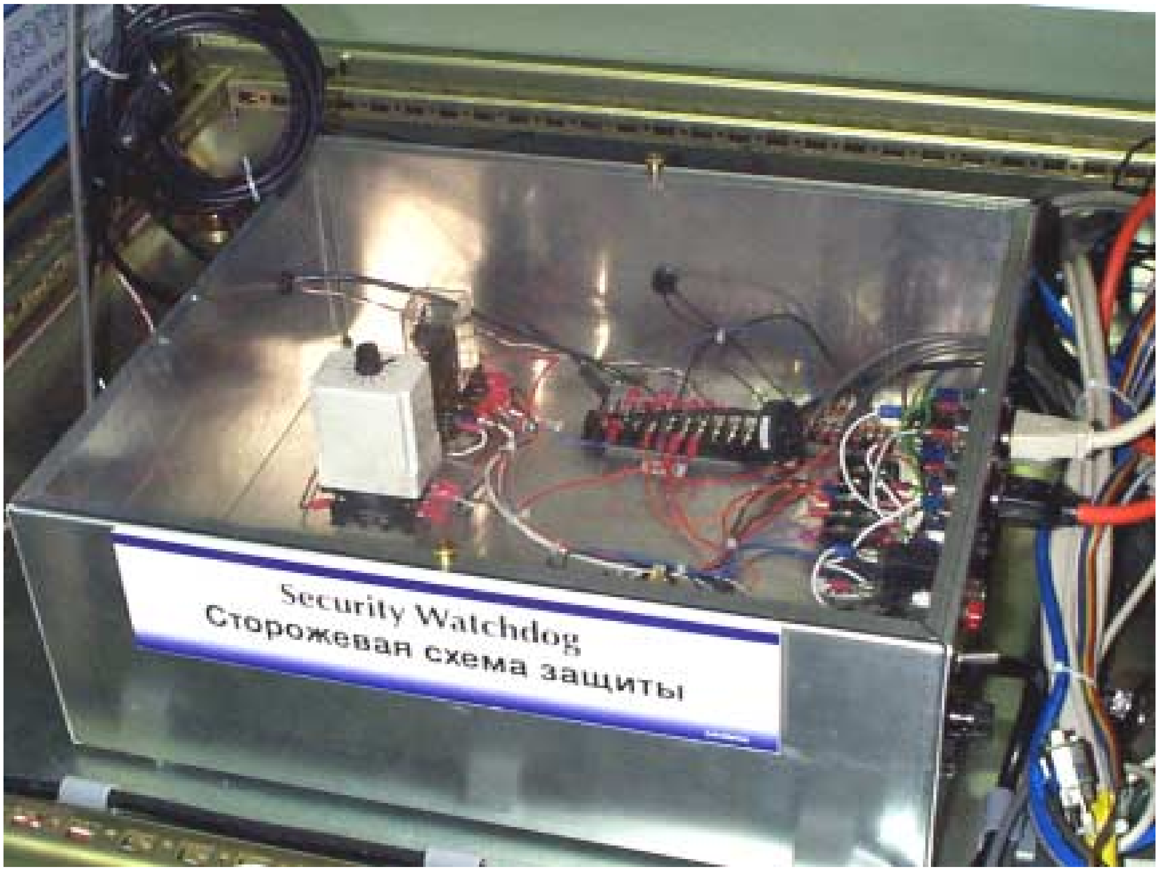

Fig 3. The assembled security watchdog chassis.

If power is supplied to the AMS through K2, then the doors must be closed and the system is secure. The output display indicating “system secure” is derived directly from the coil of K2. Similarly, if the system is operating with the door open then the AMS power is being supplied through K1. The output display indicating “system open” is derived directly from the coil of K1.

Capacitor C1 was included to ensure that the AMS remained powered as the door was being closed. Without C1, relay K2 would be energized and relay K1 is de-energized at exactly the same time. If K1 operated more quickly than K2, then power would be briefly lost to the AMS. This loss of power would require re-calibration of the entire system. In particular, any value of authentication with the doors open would be lost. Capacitor C1 will delay the de-energizing of K2 by a few tenths of a second to ensure that either K1 or K2 is energized at all times during the door closing transition.

Resistors R1 and R2 are included to limit current flow through the relay contacts during transitions. Similarly, the two diodes will “snub” the reverse EMF generated in the relay coils when de-energizing.

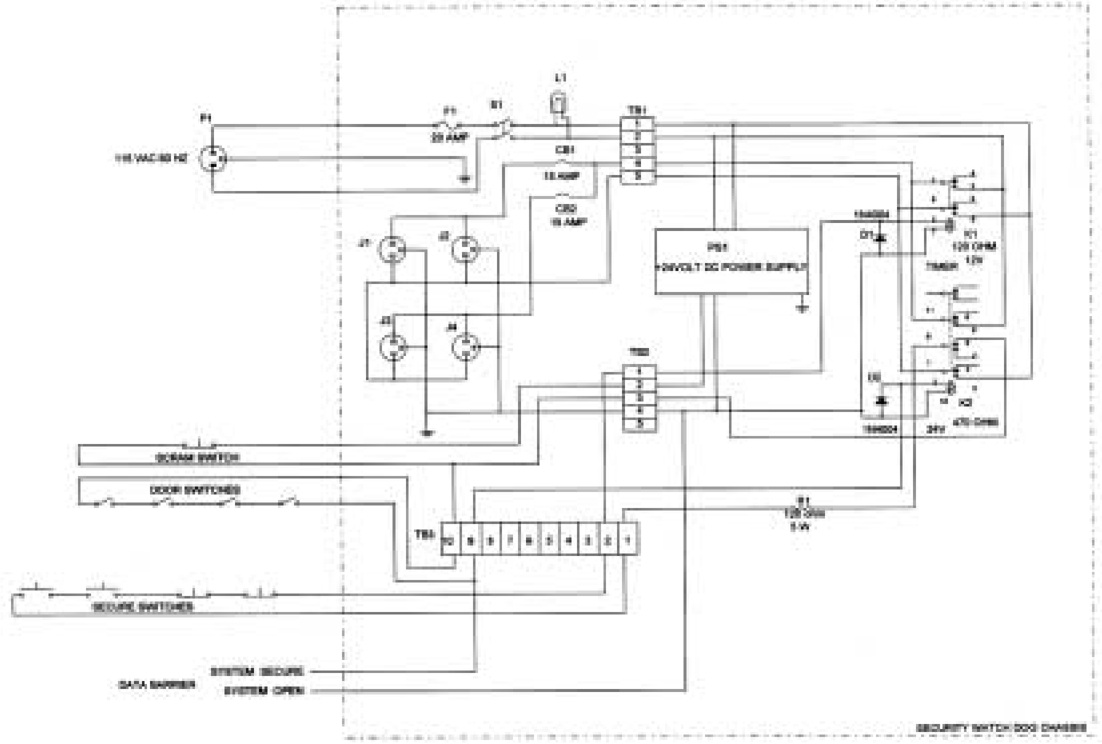

Fig 4. The entire detailed schematic of the security watchdog.

SWITCHES

A detailed description of the switches themselves is outside the scope of this report. However, the functional operation of these switches is important to a full understanding of the security watchdog circuit.

When the system is in a secure configuration, all door switches will be closed. Opening a door in the shielded enclosure or one of the auxiliary enclosures (only the gamma detector enclosures are interlocked in the demonstration system) will open one or more of the door switches and remove power from the main relay.

The security switches are pushbuttons located within the AMS detector region. One of these switches (S1) is normally closed and the other (S2) is normally open. Both switches must be closed in order for the AMS to be energized with the door(s) open. Thus a specially modified source container that presses switch S2 (closing it) but not switch S1 (leaving it closed) **must** be in place in order to make any measurements with the door open. If a container containing a classified object (or any other non-modified container) is placed within the detector, security switch S1 is also depressed and the second power relay cannot be activated.

The security switch S2 is used to check whether a container is in the system. If no container is the system, then S2 is open and relay K2 cannot be energized. Similarly, if an unmodified container is in the system, both S1 and S2 are pressed, again allowing measurements in the classified mode. Thus, the **only** time that open measurement s are permitted is when the modified container is present in the system. Any attempt to remove this container with the enclosure doors open will remove power from the AMS.

The SCRAM switch is a large button accessible from the outside of the shielded enclosure. If the SCRAM switch is pressed, all power is removed from both relays in the security watchdog. Thus, all AC power is removed from all other components of the AMS until the SCRAM switch is reset manually. The SCRAM switch will not reset itself.

FAILURE MODES

Due to the key position of the security watchdog in the AMS, it is important to consider failure modes of this circuit. In particular, the security watchdog should fail in the “safe” configuration (no power supplied to the remainder of the AMS) if common component failures occur.

- If the power supply or related wiring fails, then neither K1 nor K2 can be energized and no AC power can be supplied to the remainder of the AMS.
- Both relays are connected in a “fail safe” configuration. An active connection to the coil is required in order for the watchdog to supply AC power to the rest of the AMS.
- Both sides of the AC line are switched by relays K1 and K2. Thus, the failure of one contact will not prevent the watchdog from interrupting power.
- If the wiring to the SCRAM switch fails or becomes disconnected, then neither K1 nor K2 can be energized and no AC power can be supplied to the remainder of the AMS.
- Each or the doors on the shielded enclosure has 2 interlock switches, either one of which is sufficient to de-energize K2 if the door is opened.
- The door switches are all normally closed. Therefore, if one of the cables connecting the auxiliary door switches to the main cabinet is not connected correctly, then the watchdog acts as if one of the doors was open.
- If the coil of either relay becomes open, that relay cannot supply AC power to the AMS.
- The security switches, S1 and S2, will each be a pair of mechanical switches in the final implementation. Failure of any one of these four switches **cannot** cause the security watchdog to malfunction.
- The security switch circuit requires closure for the system to make open measurements. Therefore, if one of the cables connecting the security switches to the main cabinet is not connected correctly; the security watchdog will not allow open measurements.
- Both the “door open” and “system secure” displays are driven directly from the relay coils in the watchdog. This is the best indication that the relays are actually in the configuration displayed.

In general, the failure of any wire or connection within the watchdog will result in AC power being interrupted more often (or continuously) rather than less often. As desired, failures of the watchdog will generally default to a more secure, as opposed to less secure, configuration.

ACTIVE PURGE

Any time the doors are opened, all power is removed from the system. Since no data is written into non-volatile memory during AMS operation, this operation should remove all classified information. (This power-down method is termed a “passive purge”.) However, in cases where a passive purge is not sufficient, the volatile memory must be overwritten before the purge is considered complete. (This overwriting method is termed an “active purge”.)

An active purge of the memory in the demonstration AMS is performed procedurally rather than electronically. The SCRAM button is pressed and manually released prior to opening the access door. The computers are allowed to restart (which overwrites their entire RAM) **before** the door is opened. This procedure can be repeated as many times as required to achieve appropriate sanitation of the system.

REFERENCES

[1] Duncan MacArthur and Geoffrey Dransfield, “PPIA System Wiring Diagram,” Los Alamos Publication LAUR-99-5295, September 1999.

[2] Duncan MacArthur, Rena Whiteson, Diana Langner, James K. Wolford Jr.; “Attribute Measurement System with Information Barrier for the Fissile Material Transparency Technology Demonstration: System Overview,” Los Alamos Report LA-UR-99-5611, October 1999.