SANITIZATION OF IRIG 106 CHAPTER 10 STORAGE MEDIA

Alfredo Berard, Catherine Cogan, Lorin Klein,
Heath Massey, and Rick Williams
846 TSS/TSI
Eglin Air Force Base, FL

ABSTRACT

For the last 30-years, magnetic tape systems have served as the primary means of recording data from airborne instrumentation systems. The IRIG 106 Chapter 10 Digital Recording standard [1] introduced and developed by the Range Commanders Council (RCC) Telemetry Group (TG) has served as a common ground for industry to develop technology for replacing those tape-based recording systems with digital systems and recording data onto Solid State Devices. Data assurance and validation has been paramount in the development. This paper examines the challenge of sanitizing and downgrading media that is Commercial off-the-shelf (COTS) and is utilized by test organization in the operational communities as well as the Major Range Test Facility Base (MRTFB) and other test ranges.

INTRODUCTION

Air Force policy is to safeguard sensitive data, no matter what the storage medium. Safeguarding sensitive information in storage media is particularly important during routine maintenance, product end of life, and reuse. Computer security personnel, operations personnel, and other responsible persons must be aware of all the risk factors before sanitizing and purging digital recorder storage media and releasing them from a controlled environment.

Sanitizing is the process of erasing or destroying media in a manner that eliminates the possibility of any threat agent having opportunity, motivation or capability to presume the value of the data is worth the time and cost to recover it. Downgrading is a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level. Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level, and can be properly protected at a lower level. Any official who is authorized to classify or declassify the information and has authority over the information may downgrade information. The downgrading process includes remarking the media with the new downgraded classification to denote the media still contains sensitive data.

Reuse of Removable Memory Modules (RMM's) utilized for storage of data from airborne IRIG-106 Chapter 10 digital recorders poses a significant challenge as Commercial Off The Shelf (COTS) Solid State Drives (SSD) are utilized as the storage media inside RMMs. This paper addresses the technical issues related to the sanitization of IRIG 106 Chapter 10 digital recorder RMMs and provides a guideline for implementation as it relates to security requirements.

BACKGROUND

When semiconductors were first invented, the United States Government was the majority customer of the U.S. electronics industry. During the 1980's there was a transition toward consumer electronics dominating the marketplace. By the 1990's with the end of the Cold War and the beginning of the "dot-com" boom the military went from being the driving market force in the electronics technology industry to less than one percent of the total U.S. market. With the modern day global economy manufacturing has been driven offshore and the DoD has been forced to meet system requirements by using commercially available parts. Although military requirements can be met technically, other requirements for non-obsolescence and security cannot be guaranteed. As it applies to digital recorders, one critical issue is how well the existing ever-changing, globally-distributed commercial supply chain, and its processes, meet the needs of the military consumer market. One key issue for data security is illustrated in Figure 1. The issue is that the COTS supply-chain provides little or no second-tier supplier configuration control of the product.

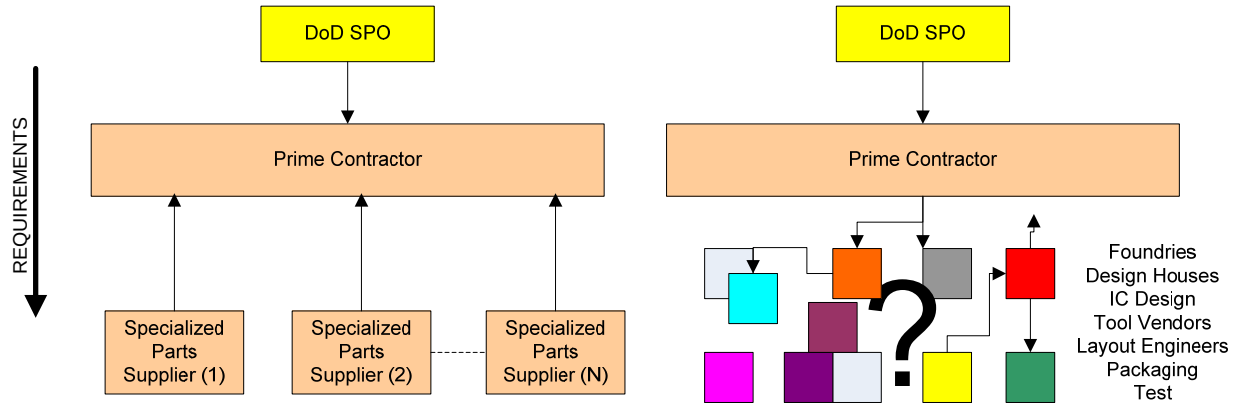

Figure 1: Configuration Control of Suppliers in COTS Products

The point is, there is no assurance that malicious code does not exist or cannot be introduced in the supply chain of solid state devices for an environment where security is required. Without that assurance, special precautions and safeguarding procedures must be taken.

WHAT IS SO DIFFERENT ABOUT A SSD?

SSDs have no moving parts, in fact some drives can withstand up to 1500 G's of shock force because of the lack of mechanical parts. An SSD basically consists of a printed circuit board, NAND flash memory chips, SDRAM cache, memory and interface controller. The method of erasing and writing data as well as interfacing to the airborne recorder and computing is a large factor determining how SSD's are controlled in a secure environment. The initial release of the IRIG 106 Chapter 10 standard required RMM's to be able to initiate a downgrading (sanitize) process whereby memory was overwritten and verified. This initial release required that RMM's have the capability to isolate and identify to the user those memory areas which could not be overwritten. However, this initial release did not provide standardized commands to the RMM until the 2007 release of Chapter 10. The 2007 release added new commands which provided mechanisms for the user to read those areas of the media which could not be verified and remove them from the logical address map.

The incorrect assumption by the authors of the standard from its inception was that supply chain management was prevalent throughout the acquisition process. This has been proven not to be the case as IRIG 106 Chapter 10 manufacturers are primarily integrating commercial SSD's inside the RMM's. This has led DoD organizations including the 46 Test Wing, at Eglin Air Force Base, to only allow security downgrade of RMM's to the SECRET level and mandate that no RMM's may ever be declassified to the unclassified level.

WHAT ARE THE SECURITY CONCERNS WITH ERASING SSD'S?

SSD's utilize floating gate transistors as part of their nonvolatile storage components. The transistors have a control gate and a floating gate. The floating gate is electrically isolated by SiO^2 insulating which helps create the non-volatile functionality of the memory, Figure 2. Electrical charge can be injected on the floating gate to manipulate the threshold voltage of the gate. With a higher threshold voltage the charge applied to the control gate must be greater to "activate" the transistor. The electrical charge is injected into the floating gate via Fowler-Nordheim tunneling when the transistor is "switched" on by applying voltage to the control gate. The electrical charge on the floating gate can be held for extended periods of time without having any voltage sources connected to the circuit (non-volatile) because of its electrical isolation from the rest of the circuit. If there is electrical charge present on the floating gate the threshold voltage is increased and the bit of memory is considered "programmed" and has a value 0. The process of clearing or erasing the memory involves removing the charge from the floating gate so that the threshold voltage is lowered. By applying voltages to the control, drain, and source terminals the floating gate charge and therefore the logical value stored in the "bit" can be manipulated. To read the values from memory a much smaller voltage is applied to the control gate than when writing to memory. Depending upon how much charge the floating gate has and thus how high the threshold voltage of the transistor is the current flow from source to drain of the transistor will vary; this is the methodology for distinguishing logic levels "0" and "1".

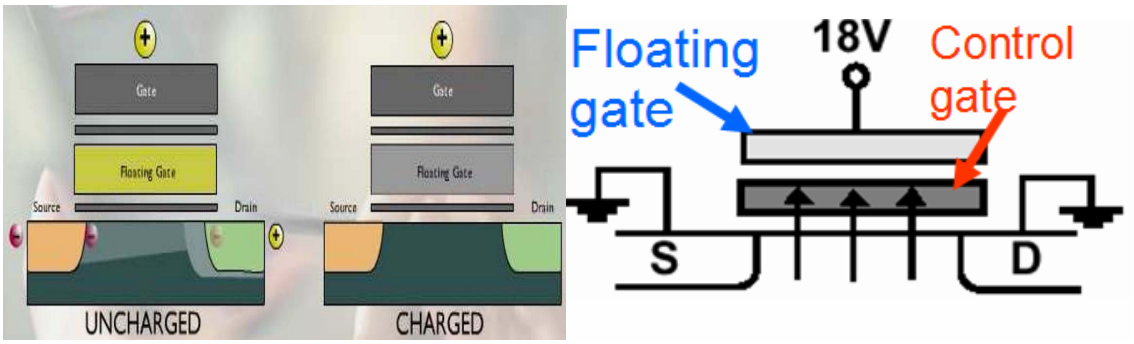

Figure 2: Floating gate

The question of whether or not the previous stored value could be determined by residual charge arises, Figure 3. If all cells had completely uniform program and erase times, then one might conclude that cells with higher threshold voltages were previously 0 (programmed) and cells with lower threshold voltages were previously 1 (already erased) before the block erase occurred. By writing an arbitrary pseudo random pattern after the memory has been cleared any possible residual charge is over-written.

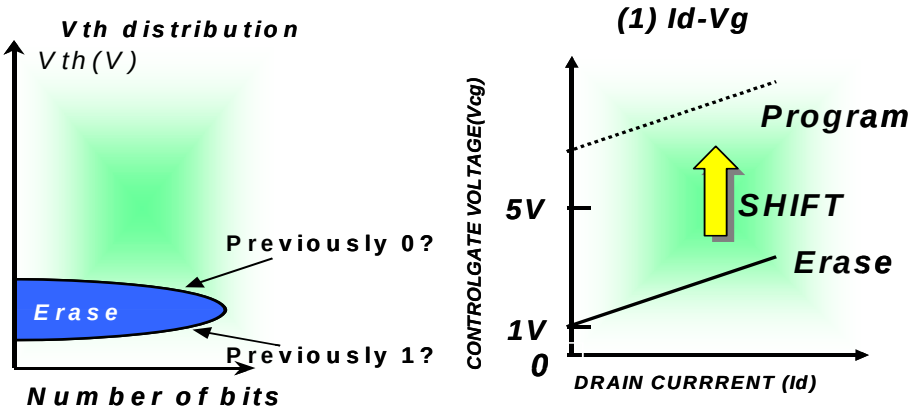

Figure 3: Program and erased states

The 846th Test Support Squadron mandates and verifies that SSD's provided by RMM manufacturers with flash technology incorporate an erase capability (changing of cell from 0 to 1) within the flash cell chips. The 2009 release of the IRIG 106 Chapter 10 Digital Recording Standard will provide specific commands that allow a host application to initiate an erase of the SSD and determine if any memory blocks cannot be overwritten. Any blocks that are found to fail the erase and verify cycle are written into a *bad block* table. In operation, all SSD user locations are erased (0xFF) except for locations where the invalid block information is written prior to shipment by the memory chip manufacturer. By specification it is required that a user be able to map out bad blocks so they are no longer addressable. Figure 4 illustrates the Bad Block

Mapping process. Once an address has been mapped out it will no longer be identified in the *bad block table*.

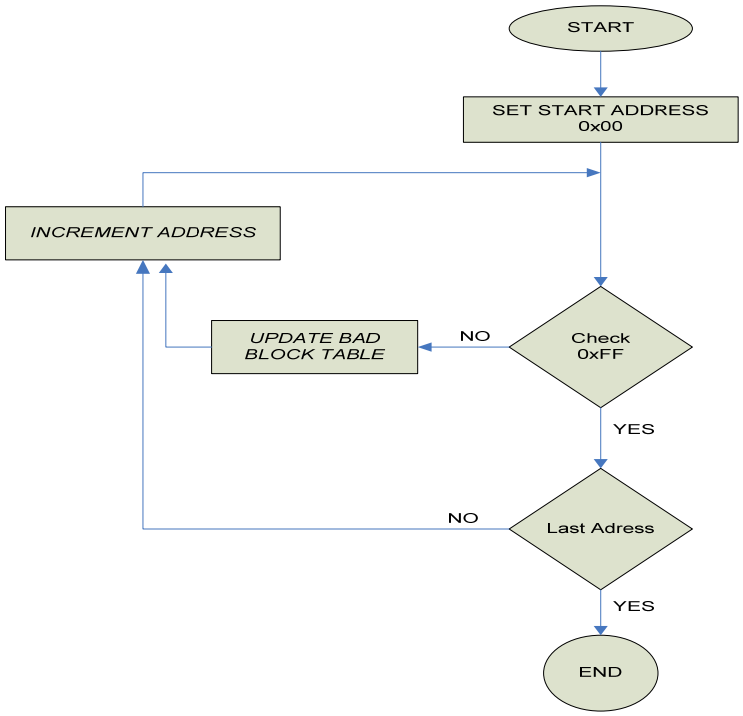

Figure 4: SSD "Bad Block" Detection Process

A major security concern relates to supply chain management. SSD memory components typically provide areas within the memory chips that are utilized for storage of control information such as bad block table, internal data base information and error correction. For example, data in an SSD is stored in 512 byte increments or sectors with an associated 16 byte control block, Figure 5. The control blocks store bad block information, error correction, and database or proprietary information required for reuse of the SSD drive. For the user to effectively accomplish a physical sanitization and reuse of the drive and downgrade to an unclassified level they would have to know the exact SSD memory chip geometry, drive configuration, and proprietary information required for reuse. For this reason the 846th Test Support Squadron has determined (as approved by NSA on 8 Jul 08) that RMM's can only be sanitized at the logical address level and can only be downgraded to SECRET level until destroyed.

Figure 5: Sector data and associated control bytes

There are numerous manufacturers of SSD's that provide methods for sanitizing and clearing; however, without a standardized process, and procedures, it would be doubtful that risk analysis would allow downgrading SSD's to any classification level. The existing 2007 release of the standard has undergone six revisions to facilitate sanitization by both the airborne recorder and RMM host Automated Information System (AIS).

The first revision of the standard provides two standardized IEEE-1394b commands that allow for configuration control of internal components of an RMM. The ".IDENTIFY" command has been added to the standard. This command allows the AIS application to gather firmware revision levels and drive manufacturer of the SSD. The second command is a ".MEDIA P" command, whereby the {P} attribute denotes physical configuration. This command provides the user AIS application with the necessary information to read the contents from physical addresses of the SSD.

The second revision of the standard is to execute a clear/verify command upon reception of existing IEEE-1394b ".DECLASSIFY command. This command will cause all SSD addressable memory locations (hereinafter referred to as "Beginning Of Media" -- BOM to "End Of Media" -- EOM) to be erased with a value of "FF". It is also required that for the clear command to be effective a verification of "FF" from BOM to EOM be accomplish by memory chip controllers of the SSD. The intent of this clear command is to remove information from storage media in a manner that renders it unrecoverable by normal system utilities or technical means.

The third revision to the standard is to modify the method by which bad blocks are reviewed. Two commands have been altered such that binary access of data instead of existing American Standard Code for Information Interchange (ASCII) Small Computer Systems Interface (SCSI) read commands can be executed. A ".BBREAD P" whereby the {P} denotes physical block has been added to allow for binary access of data. This binary access shall allow users to view the contents of any *block* that has not been verified (all values 0xFF).

The fourth revision to the standard is to provide the necessary IEEE1394b commands that allow for Sanitization of media residing in the RMM. Required Commands are as follows in table 1:

Table 1:

Command	Description
.IDENTIFY	This command queries the RMM for SSD identification and firmware version.
.VERSION	This command queries the RMM for its firmware version.
.MEDIA P	This command queries the RMM for information about the physical media of the SSD and the transfer limits for the required physical I/O commands.
.SANITIZE	This command initiates the .SANITIZE operation.
.INITIALIZE	This command initiates the .INITIALIZE operation.
.BBLIST	This command directs the RMM to retrieve the bad block list from the SSD.
.BBLIST R	This command retrieves the bad block list from the RMM.
.BBREAD P *blk_id*	This command directs the RMM to initiate a physical block read of the specified physical block identifier.
.BBREAD D	This command retrieves the data from the physical block. See the .MEDIA P command for information.
.STATUS	This command requests status from the RMM. Note that this is not a new command, but new response codes have been defined.
.IRIG106	This command provides revision number of the IRIG-106 Standard

The fifth revision of the standard modifies and adds standard command responses from the RMM regardless of SSD utilized, Table 2. A status response typically consists of a state code and four arguments. Typical Response and state codes are as follows:

```
*.STATUS
S   A   B   C   [D%]
*
```

Where …

A …. State Code of the RMM. Four new state codes have been defined. See the table below.
B …. State specific value.
C …. State specific value.
D …. Progress percentage (0..100), only present in certain states.

Table 2:

State Code	Description	Other response data values (x,y,z)
11	.SANITIZE command completed and new UNSECURED bad blocks were found.	B – Not used. C – Specifies the number of new UNSECURED bad blocks found. D – Not present.
12	.SANITIZE command completed and no new UNSECURED bad blocks were found.	B – Not used. C – Not used. D – Not present.
13	.INITIALIZE in progress	B – Not used. C – Not used. D – Provides progress for the current initialization (0..100%)
14	.INITIALIZE complete. After the RMM has reported this state to the host one time, the RMM will reinitialize	B – Not used. C – Specifies the number of seconds required for the RMM to reset. The host application should not send any commands to the RMM for the period specified by this value. This mechanism allows time for the RMM and SSD to reset if required. If no reset or delay is required, an RMM may report 0 in this field. D – Not present.

The sixth revision to the standard provides a standardized method of generating a non-repeating pseudo random pattern from BOM to EOM once the clearing process has been completed. Generation of numbered passes with a pseudo random pattern can be executed on the AIS or Digital Recorder as required by the Designated Approval Authority (DAA). In Accordance With (IAW) AFSSI-5020 a single overwrite with an arbitrary pseudo pattern is sufficient for effective sanitization of flash memory.

Other than writing 0xFF from BOM to EOM the sanitizing process for the RMMs involves writing two sequences once again from BOM to EOM. The first of the two sequences is a 16-bit pseudo-random value generated from 16 separate Fibonacci Linear Feedback Shift Registers (LFSR) in parallel. Seeding of the LFSRs is accomplished by either the IRIG-106 Chapter 10, 10MHZ Relative Time Counter (RTC), when the RMM resides in a Digital Recorder or is derived from Central Processing Unit (CPU) clock cycles of the host AIS when the RMM is sanitized outside of a Digital Recorder.

The Fibonacci LFSR's are numbered 0-15 and provide the corresponding bit for the 16-bit random values written to the SSD. The LFSR's increase in length starting with 16 bits for lane 0 and reaching 31 bits for lane 15. Each LFSR has specified taps. The taps are the bits for a specific LFSR that have an Exclusive-or (XOR) logical operation applied to produce a feedback bit for the LFSR. Each LFSR has 4 tap bits; the feedback is inserted into the least significant bit (lsb) of each LFSR after the LFSR is left shifted. Therefore, the LFSR's are shifted from lsb to most significant bit (msb), the feedback produced by the XOR of the taps is placed into the lsb and the bit shifted out of the msb of each LFSR is used as the corresponding bit of the 16-bit random value written from BOM to EOM.

The diagram below demonstrates the functionality of LFSR_0 (the 16 bit LFSR) including the specified tap bits. In this example the value 0xC8AC is initially in the LFSR. The next bit shifted out and used as part of the random value will be the msb which is 1. The next bit placed into the lsb, the result of the XOR taps, is 1. The value of the LFSR will become 0x9159 after one iteration.

A maximal LFSR produces an n-sequence pattern (i.e. cycles through all possible $2^n - 1$ states within the shift register except the state where all bits are zero), that will not repeat for the specified number of iterations. By incorporating multiple LFSRs with varying length the random values generated are within an even longer n-sequence pattern. In this particular example of using 16-31 bit LFSRs, the least common multiple (LCM) of all 16 of the LFSR's $2^n - 1$ length sequences gives the sequence length before the pattern begins repeating. The sequence will not repeat for millions of terabytes.

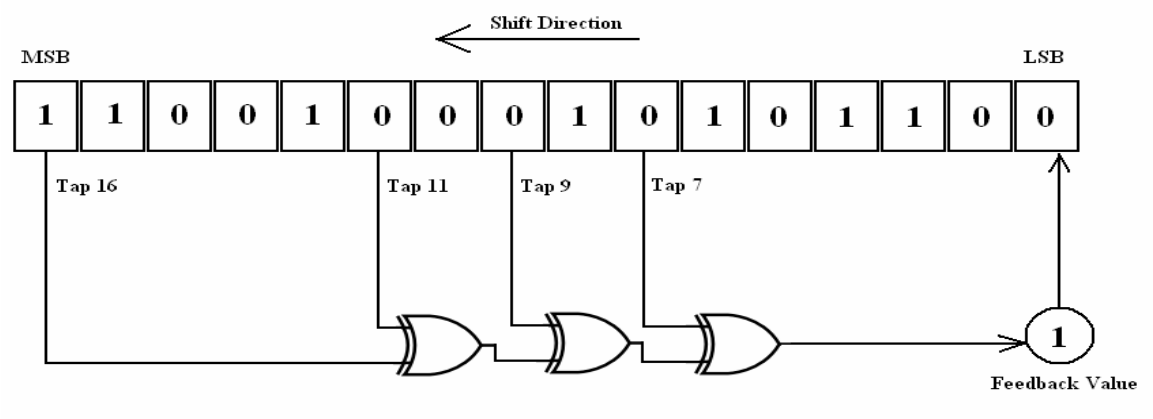

Figure 6: Linear Feedback Shift Register

The second sequence consists of writing the word "SECURE" at 512 byte intervals from BOM to EOM . The first location "SECURE" is written between the word 32 and word 253 of the media and is never at the same starting offset from word 32. The purpose of this pattern is to allow the AIS application to quickly determine if the media has been sanitized. Additionally every logical address can be verified from the SSD by implementing the same Fibonacci LFSRs and seed value (first 31 words) and validating the data.

APPLICABILITY OF IRIG 106 CHAPTER 10 SANITIZATION TO NATO AND AIR FORCE AFSSI-5020 DECLASSIFICATION GUIDANCE

NATO AEDP-3 Edition 1, Advanced Memory System Declassification and Sanization Guidance [2] and AFSSI 5020, Remanence Security [3], describe declassifing media. Neither of these documents are applicable to the IRIG 106 Chapter 10 storage media sanitization process due to the media being downgraded to a SECRET level. The media will never be downgraded to the unclassified level.

RMM'S AND SPECIFICATIONS

Flight Test applications by default require a small form factor, ruggedness and significant greater reliability and performance when compared to Non-Flight Test requirements. Until now acquisitions of RMM's have not considered tailoring specifications to allow different SSD's to be utilized within the same RMM. Given the falling cost per Giga-Byte of SSD and commercial independent research and development (IRAD) dollars being invested, acquisition of RMM's should mandate the ability to replace SSD's allowing reuse of the RMM with different SSD's.

CONCLUSION

We have shown that current COTS processes are not robust enough to allow declassification of solid state memory to an unclassified level. The best that we can currently attain is downgrading media to the secret level, if, and only if, standards are used. We have demonstrated that with adherence to the IRIG 106 standard, we can reuse the costly memory modules in a multi-level security environment at the secret level. Even downgrading to this level, and still limited in reuse, the cost savings are significant. In transitioning from tape to solid state devices, it was recognized from the outset that the reusable media costs were significant, but the extent that the compounding effect of multi-level security would have on media canister availability, and the resulting cost in the operational environment was never fully appreciated. Standardization and close attention to supply chain management offers a means of downgrading previously used canisters for reuse and results in significant cost avoidance but only if the memory has a mapping capability. And, that capability requires the RMM manufacturer to ensure it is a feature in their product. Since life cycle media costs can far exceed the initial recorder investment cost, RMM reuse is a major consideration in a multi-level security environment. And, for future consideration, the only current means for declassifying RMMs to the unclassified level is to remove and destroy the SSDs and reuse the RMM electronics with new SSDs. Therefore, provisions for replacing SSDs within RMMs should be a major consideration in the life-cycle suitability decision of the acquisition of recording systems.

REFERENCES

[1] IRIG 106-07, Telemetry Standards (Part 1), Chapter 10, Digital On-board Recorder Standard, September 2007 https://wsmrc2vger.wsmr.army.mil/rcc/index.htm

[2] NATO AEDP-3 Edition 1, Advanced Memory System Declassification and Sanization Guidance

[3] AFSSI 5020, Remanence Security