JEFFERSON LAB PERSONNEL SAFETY ELECTRONIC LOG RMA*

K. Mahoney, I. Carlino, K. Kindrew, T. Larrieu, T. McGuckin, N. Okay,
JLAB, Newport News, VA 23606, U.S.A.

Abstract

This paper describes a new electronic record management application (RMA) developed at the Thomas Jefferson National Accelerator Facility (Jefferson Lab) At Jefferson Lab and many other accelerator facilities, there is a permanent record of personnel entering and exiting a secure accelerator beam enclosure during Controlled or other special access conditions. These legal records – records that may be entered as evidence in a court of law - may also contain entries related to radiological controls, tests, and certification of access control interlock systems. Until recently, the stringent requirements for electronic legal records required by the U.S. government made it impractical to create an electronic version of the Personnel Safety System (PSS) paper log book. The staff at Jefferson Lab have now designed and implemented a PSS e-log book application and records management program that meets the requirements for electronic records. In order to successfully implement this system, the development included significant effort in database design, user interface, software quality assurance, and records management.

INTRODUCTION

By 2001, almost all Jefferson Lab accelerator operations logbooks were fully electronic; however, the Personnel Safety Systems (PSS) logs were an exception. Unlike the routine operations logs, the PSS logbook is considered a legal record of radiation protection system status, personnel access to radiologically controlled areas, and information related to PSS operations. PSS logbook information must be able to be maintained up to 25 years after the lab closed. Records must be created using accepted good practice for log keeping and a chain of custody maintained in case the records are subpoenaed in a court of law. This is normally accomplished by having the host institution maintain the records during its active life and transferring the information to the National Archives once the facility is closed.

Accepted good practice for logbooks is normally based on permanent ink entries in a paper log, with bound and sequentially numbered pages. In addition, there are requirements for entry validation, time and date, and limited corrections [1].

Additionally, the PSS logbook is used as an integral part of administrative procedures to process personnel in and out of a beam enclosure. Routine procedures such as "Sweep" and "Controlled Access" use an ink stamp form to ensure the Safety System Operator (SSO) follows the process and captures all of the necessary information each time. A separate section of the paper log book is used to account for each individual entering and exiting the beam enclosure during a Controlled Access. Errors, including those in human factors, in the implementation of a new log book could contribute to leaving unaccounted personnel in an active beam enclosure.

After the introduction of electronic operations logs (e-logs), the Jefferson Lab accelerator operations staff strongly desired an electronic version of the PSS log, integrated with the other electronic log book systems. To meet this demand, a team was formed to look in to the feasibility of creating an electronic PSS log book while maintaining the necessary traceability and continuity of information.

SYSTEM REQUIREMENTS

The initial phase of the project was dedicated to identifying statutory, regulatory, and accepted good practice for electronic records. Over 50 documents were identified. Many of these are captured in the U.S. DoD standard 5015.2, "Design Criteria Standard for Electronic Records Management Software Applications" [2]. This standard would later become the basis for the requirements of the U.S. National Archives and U.S. Department of Energy standards for electronic records [3], and ultimately, the Jefferson Lab electronic log RMA requirements document [4]. Secondly, a systems engineering approach was used in order to ensure the diverse demands on the application were identified and addressed from the beginning. These demands included security, human factors, data integrity, usability, testability, and records retention.

A software lifecycle was defined for the new application and requirements solicited from multiple potential customers, developers, and administrators. Paramount to the application was identifying the requirements for determinism, usability, traceability, security, and disposition. The initial version of the requirements was over 50 pages and was based on the DoD Standard 5015.2.

In 2002, a feasibility study by the Jefferson Lab Controls Software Group determined the existing e-log database structure would not support the determinism and security requirements for a PSS electronic log and RMA application. However, the new requirements were folded in to an existing project to redesign the operations e-log database and the PSS e-log project was shelved while these changes were implemented.

In 2007, after sufficient time for the new e-log applications to mature and stabilize, the PSS e-log project was restarted. The requirements document was revised

and re-issued by a team consisting of representatives from Jefferson Lab operations, controls software, records management, and safety systems groups. Each representative ensured that the final application was integrated in to their process and procedures. Testability was a key element designed in from the beginning.

APPLICATION DEVELOPMENT

The implementation phase was divided in to four major efforts: user application design, database design, records disposition design, and V&V. The application design is the user interface to the electronic log book. In order to minimize operator confusion and retraining, the application was designed to mimic the major functions of the existing paper and ink log book.

The user application serves four functions:

1. State Change, where an SSO records the status of each PSS operational segment.
2. An eStamp application for recording Sweep and Controlled Access procedures.
3. Controlled Access log to record specific information for each entrant
4. Information entries for general notes on PSS operations.

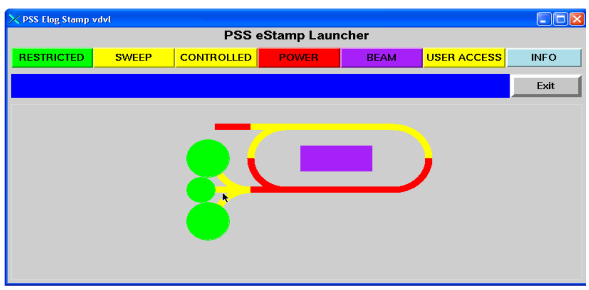

Figure 1: PSS eStamp Launcher Application. The color codes are keyed to the PSS status and are the same as seen on PSS operations screens.

The SSO selects an operation through the Launcher dialog (see Fig. 1.) A comparison of the paper log ink stamp and the corresponding PSS e-log (eStamp) form is shown in figure 2a and 2b. An example of a Controlled Access log entry is shown in Fig. 3.

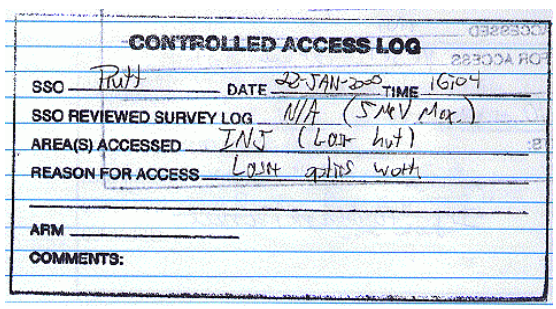

Figure 2a: Paper log stamp entry for Controlled Access.

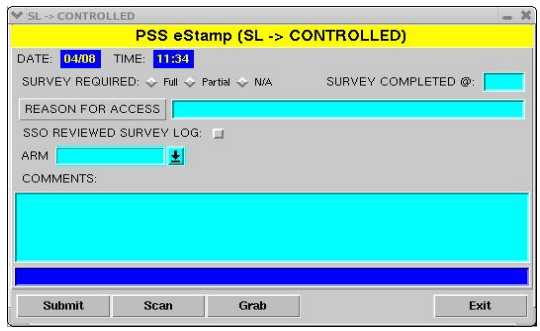

Figure 2b: Electronic log Controlled Access eStamp user interface.

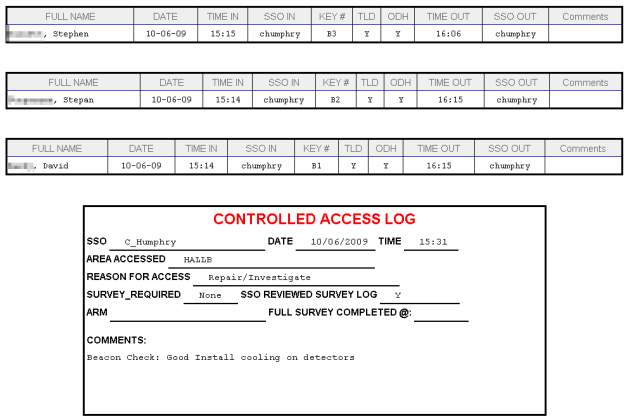

Figure 3: Controlled Access record showing both the completed stamp and entry log.

User Authentication

There are two unique issues related to creating an electronic logbook record. The first is how to verify the "signature" of the person making each entry without making the process onerous. The second is how to support multiple operators making concurrent entries relating to different machine segments; a typical operations shift may see dozens of logbook entries by two or more authorized Safety System Operators (SSOs). The application development team tried several verification methods, including biometrics, before settling on an RF ID badge reader. The device reads information from the Safety System Operator's (SSO) existing employee ID badge.

The SSO must authenticate their identity once per eight hour shift by entering their username and password. The authentication process also validates the operator is an authorized Safety System Operator. Once authenticated, the action of simply swiping the badge automatically submits subsequent log entries. Multiple SSOs may be authenticated simultaneously as long as each entry is uniquely tied to one SSO. Access control procedures that cross multiple shifts are supported by separately recording the SSO processing a person IN and OUT of the enclosure.

User Application Features

With the basic functions of the paper log replicated, the user application capitalizes on information available to a computer that make the overall process more robust than possible with a paper logbook. For example, the application enforces policies such as 'at least one person sweeping the enclosure must be authorized to sweep the area.' Another significant utility added is the ability to 'look-up' names of personnel requesting access. Correctly identifying and spelling names of an internationally diverse user group was a difficult and time consuming process with the paper log book. All entries are screened for completeness before a record is submitted. Error trapping and message feedback is used extensively throughout the application. For example, all user entries are also screened for compatibility with the ASCII character set.

DB DESIGN

With the redesign of the underlying database structure for the operations e-log complete, the major effort in the PSS e-log database design concentrated on utilities for secure and deterministic records creation and management. One major challenge was the requirement to capture linked information that may span multiple shifts and operators. For example, a Controlled Access record is considered all of the information relating to a specific Controlled Access period during accelerator operations. The record includes the Controlled Access stamp information as well as the information for each person entering and exiting the tunnel.

This is accomplished by creation of a temporary record which may be updated as the process is completed. All actions during the process are recorded in an audit log. The SSO is allowed to make limited corrections to an open entry, however all information is captured sequentially in the audit log. The temporary data is stored redundantly. If the e-log application is halted for any reason, all of the data for an access is recovered from the temporary record. Once the Controlled Access or Sweep is completed, the record is automatically closed and stored for permanent archival. The database is fully searchable through a standard e-log web interface.

RECORDS DISPOSITION

A PSS e-log records management policy was developed with the collaboration of the Jefferson Lab Records Manager. National Archives requirements stipulate that electronic records must be stored in a flat ASCII format. Graphical information must be linked to the record but stored separately. In order to accomplish this while retaining the capability of retrieval and display of archive data, the records are recorded in Oracle database, xml, and text formats. The data is backed up daily and stored on-site and redundantly off-site.

TESTING AND V&V

Testability was designed in to the PSS e-log system from the beginning. For example, the overall systems validation tests were based directly on the systems requirements document. Off-line simulation tools were developed as part of the application development process. The simulators allowed incremental validation of modules as they were developed. The simulation capability was also very useful for identification of implementation errors. The database system has extensive audit and tracing capability in order to follow a record throughout its lifecycle.

The initial beta version of the application was introduced to the control room in the summer of 2008. Operators were trained on how to use the new system. A user's guide was also introduced at the same time. During the test phase, operators would make entries in both the paper and electronic logs, with the paper log still remaining the official record. During this phase operators provided feedback on the utility and ease of use. Bugs were reported to the application development team and usually corrected within a few days. After the final release a more rigorous test configuration control structure was implemented.

Two test documents were created: The validation document assessed the system's performance against the original requirements. A separate, simplified, verification document is used to routinely test the application when minor bug fixes are implemented. The final system was commissioned in the spring of 2009. At that time the paper log book was officially retired, although there is a procedure for using the paper log in an emergency.

CONCLUSIONS

An electronic log and records management application was developed at Jefferson Lab that meets the requirements for electronic records. The system not only duplicates the functionality of the paper log but also enhances the quality of the access control process and information recorded. Experience with the e-log to date is very favourable. By using a systems engineering approach to the design, testability, maintainability, and security were designed in from the start.

REFERENCES

[1] DOE Standard DOE-STD-1035-93, "Guide to Good Practices for Logkeeping" Change 1, December 1998.

[2] DoD5015.2-STD, "Design Criteria Standard for Electronic Records Management Software Applications" November 24, 1997.

[3] DOE Technical Standard DOE-STD-4001-2000, "Design Criteria Standard for Electronic Records Management Software, March 2000.

[4] "Requirements for the Electronic Logbook for Jefferson Lab", rev. 2.0, August, 2008.