LA-UR 97-1063

CONF-970625--3

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

TITLE: **"Human Factors Aspects of the Major Upgrade to the Control Systems at the Los Alamos National Laboratory Plutonium Facility"**

AUTHOR(S): Noah G. Pope, NMT-2, LANL
J. Higgins, Brookhaven National Laboratory

SUBMITTED TO: Global Perspective of Human Factors in Power Generation, The Power Engineering Society of IEEE, 1997 IEEE 6th Conference on Objectives June 8-12, 1997, Orlando, FL

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

"Human Factors Aspects of the Major Upgrade to the Control systems at the LANL Plutonium Facility"

by J. Higgins, BNL and N. Pope, LANL

Abstract

The Plutonium Facility (TA-55) at Los Alamos National Laboratory (LANL) has been in operation for over 15 years. The Operations Center of TA-55 is the nerve center of the facility where operators are on duty around the clock and monitor several thousand data points using the Facility Control System (FCS). The FCS monitors, displays, alarms, and provides some limited control of the following systems: HVAC, fire detection and suppression, radiation detection, electrical, and other miscellaneous systems.

The FCS was originally based on late 1970s digital technology, which is no longer supported by the vendors. Additionally, the equipment failure rates increased notably in the 1990s. Thus, plans were put into place to upgrade and replace the FCS hardware, software, and display components with modernized equipment. The process was complicated by the facts that: the facility was operational and could not be totally closed for the modifications; complete documentation was not available for the existing system; the Safety Analyses for the facility were in the process of being upgraded at the same time; and of course limited time and budgets. This paper will discuss the human factors aspects of the design, installation, and testing of the new FCS within the above noted constraints. Particular items to be discussed include the functional requirements definition, operating experience review, screen designs, test program, operator training, and phased activation of the new circuits in an operational facility.

1. Introduction

The Plutonium Facility at Los Alamos National Laboratory (LANL) is called Technical Area 55 (TA-55). It has been operated by LANL for the US Department of Energy (DOE) since the late 1970s. Its current mission is to reduce nuclear dangers by solving national and global plutonium problems. It handles projects such as: stockpile maintenance, surveillance, and dismantlement; pit rebuild; plutonium power source fabrication for long duration spacecraft missions (e.g., Cassini); nuclear materials technology research; nuclear materials storage; and remediation of nuclear waste. The bulk of the nuclear-related work is performed in Building PF-4.

The Operations Center (Ops Center) of TA-55 is located in PF-4. From the Ops Center, operators coordinate scheduling and approval of work in PF-4, monitor the safety of other systems at TA-55, and direct personnel actions during unusual or emergency events. Using the Facility Control System (FCS) operators can monitor approximately 2200 input and output data points and can also exert some small measure of control over selected facility systems.

DISCLAIMER

The FCS monitors the following systems for the TA-55 facility and Building PF-4: heating, ventilation & air-conditioning (HVAC); electrical power; continuous air monitors (CAMs); criticality alarm system; fire detection, suppression, and alarm system; and miscellaneous systems. The FCS also provides a small amount of control for the HVAC system and provides alarm processing for site safety notifications.

2. Description of Problems with Old System

The original FCS was installed in 1978. It consisted of field-run wiring from detectors to 23 Uniplex Field Multiplex Units (FMUs). The signals from the FMUs were then sent to two redundant Data General computers in the Ops Center. They had 256K RAM, about as much as a hand calculator of today, and a hard drive with 85 MB of memory. These computers drove the screen generators for the human system interface (HSI) of the FCS used by the operators in the Ops Center. They also: controlled data acquisition, output of control signals, and developed the necessary system logic associated with the FCS. The Data General computers were programmed only in machine level assembly language, which made it quite difficult to maintain or change.

Besides being outdated by today's standards for computers and digital control systems, some of the FCS equipment vendors went out of business in the mid-1980s. When Uniplex went out of business in 1984, TA-55 obtained as many extra spares as possible. Later in the 1980s, additional spares were obtained from other users of Uniplex equipment around the country. This process included scavenging spare parts from replaced or failed units. During this time frame, there were a couple of aborted attempts at redesigning and installing a new upgraded FCS at TA-55. However, due to the overall complexity of the project, these attempts were not successful and the system continued to be maintained by maintenance efforts.

Over the last few years, all spares have been exhausted and the FMUs have been maintained by component level repair. For example, when data acquisition cards failed, they were removed and individually repaired. However, they could not be tested without reinstalling them and testing them in place. This type of procedure made troubleshooting quite time-consuming and difficult. A complicating factor through the 1990s was that the failure rate continued to trend upward.

During this time frame, failures of the Data General computers also increased. For example, in 1990 the HSI screen compiler failed and was not able to be replaced or repaired. Thus, no further changes to the screens were possible. The amount of support available from the computer vendor was decreased over the years. By January, 1997 support was to be only on a "parts available" basis, meaning that if they did not have the part, they would not repair the computer at all. Not all parts of the unique assembly language programming were understood onsite and only one LANL person was able to program in that language.

Documentation associated with the old original FCS was sketchy and in a poorly accessible format. Documentation of changes made to the system over the years was not maintained.

Thus, in many cases, actual wiring and terminations did not match the available drawings. For example, there were extra wires, removed wires, and relocated terminations.

3. Constraints and Complications Surrounding the Project

In order to properly understand the methods chosen and other aspects of the project, it is important to appreciate several constraints and complications that surrounded the FCS upgrade. The main ones were: the urgency of the work, the desire to accomplish the upgrade without any significant FCS or facility downtime, the design status of the FCS, and the required reviews and oversight of the design modification. These areas are expanded upon below.

As the failure rates of FCS components increased, the mean time between failures decreased. There was a growing concern among facility management and operators that failures would soon become more serious and the system may not be able to be promptly repaired, thus potentially jeopardizing facility safety. Thus, the need was established for completing the upgrade as soon as possible.

There were two general reasons for completing the project without incurring any significant facility downtime: one was operational and the other related to safety. Both the Department of Energy (DOE) and LANL had strong interest in the ongoing projects at the TA-55 facility. These projects would essentially all be stopped if the FCS were shutdown. Some projects, such as the development of power sources for the Cassini spacecraft, were time critical and could not be slipped. Regarding safety, Building PF-4 stores significant a amount of radioactive material, including Plutonium, that requires the continued operation of the HVAC and the alarm systems. The FCS is the normal method of monitoring the HVAC system and provides some automatic control functions. Shutdown of the HVAC system results in the gradual loss of the normal vacuum that is maintained on the building to prevent the escape of radioactive material. Manual control of the HVAC, without the FCS is possible but is difficult. The FCS is also the primary processor for all facility alarms and for monitoring other important systems, such as fire protection, and radiation detection. Thus stoppage of the FCS for more than a short time was not acceptable. The approach, of replacing the FCS without shutting down the facility, was initially characterized (albeit a bit overstated) as being similar to replacing the engine in a car while driving down the highway. Nonetheless a very workable and successful method was devised, as described below.

The design status of the system also created some problems. As noted in Section 2, as-built drawings of the FCS did not exist and had to be created as part of the upgrade project. This made design work and detailed planning more difficult at the outset. Also, the Safety Analysis Report (SAR) for the facility was being upgraded at about the same time, thus updating and revising somewhat the design basis for the facility systems, including the FCS.

Lastly, the required reviews and oversight had a notable impact on the project planning and implementation. The more significant a system and the more major the changes involved in a

modification, the more in depth are the required reviews by DOE. These are performed to ensure that all design, installation, and testing are all done properly and to allow restart or continued operation of the facility upon completion of the upgrade. This process influenced some of the early design decisions. For example, rather than provide new features in the upgraded FCS, the decision was to essentially duplicate the current FCS functionality. A more extensive modification would have provided improved operational capability, but would have required more time and effort for design, testing, procedure revision, operator training, and for regulatory oversight and review.

4. Overview of Project

The upgrade project contained two concurrent portions: the Facility Data Acquisition Interface System (FDAIS) and the System Integration. The FDAIS consists of programmable logic controllers (PLCs) and a data communications network that replace the field multiplex units and related wiring. The FDAIS equipment was fully installed but initially not connected to the field sensors and equipment. The system integration portion consists of: PLC programming, new computers, human system interface (HSI) software, and system testing. The new system has significant redundancy built into it, is configured for easy expendability, has much improved diagnostics, exhibits noticeably higher reliability, and has an improved HSI.

An important concept, devised to limit facility downtime, was a two step testing process. In the first step the new system, consisting of both FDAIS and System Integration equipment, was tested after installation, but before final connection to field sensors. During this step, the facility continued to operate using the old FCS. Then after initial testing, a "crossover" was performed one subsystem at a time, whereby the sensors were disconnected from the FMUs and reconnected to the PLCs. Further testing was then conducted. This will be described in more detail in Section 5.

A somewhat standard project management approach was initially planned. For the FDAIS this consisted of: an initial engineering study, detailed engineering design, procurement and construction, installation, inspection, and testing. For the system integration portion the approach consisted of: evaluate possible HSI packages, develop the HSI requirements specification, purchase HSI, programming and installation, testing.

5. Major Steps Viewed through HFE Lens

The Human Factors Engineering Program Review Model (PRM) was used to provide guidance and a structure to the design and test portions of the project. This model's purpose was to provide guidance on evaluating a control room design and implementation process that includes the HFE program elements required to develop an acceptable detailed design and to ensure that the final design reflects good HFE principles and that operator performance is appropriately supported. The PRM contains ten steps or elements. The elements of particular importance to the FCS upgrade project were: Operating Experience Review (OER), Functional Analysis/

Requirements Definition, Human Systems Interface (HSI) design, Verification & Validation (V & V), and Training.

Although one main intent of the project was to essentially duplicate the existing functionality and displays of the old FCS, it was important not to lose an opportunity to correct existing deficiencies. Thus an OER was performed whereby the performance of the FCS was examined and input was obtained from operators experienced in the use of the FCS. Past facility events over the last six years were also examined to determine any features of the FCS that contributed negatively to performance in events. Some potential improvements were identified in the areas of terminology, informaton requirements, annunciation, training, and situation awareness. The process of obtaining operator feedback was continued as the new interface screens were being developed and tested. As a result of these efforts the following improvements were implemented: changes in labels and colors, relocation of some equipment between screens, improved navigation features, corrected some building and room layouts that were inaccurate, standardized and improved wording on alarm messages, and added load lists to power system screens.

For the Functional Analysis phase, a clear and detailed definition of the Functional Requirements for the FCS had to be developed, since one did not exist at the outset. This was necessary to ensure that all functions were properly addressed in the new design and to have a basis for the test program acceptance criteria. This was done in parallel with the development of the new Safety Analysis Report for the facility.

The design of the HSI used the general techniques and guidelines of the vendor-supplied software. This was amplified by designer experience, operator input, and reference to NUREG-0700, Rev. 1. As noted in Section 3, there was a need to limit any changes to the overall layout of the screens (approximately 100 total screens). However, within this constraint, some additional improvements were added: standardization of screens both in color, format, and layout; muting of background information such as wall lines and improvement of visibility of process lines; improved labeling of equipment; conversion of navigation technique from arrows to mouse; added navigation hot points and button bars; changed some indication from demand-driven to results-driven; and added a help and definitions screen.

In order to provide for a thorough test program and to limit the facility down time a detailed V & V or test program was developed. The overall purpose of the program was to ensure that the FCS met the functional and operational requirements of the system. Figure 1 provides an overview of the program. The discussion below amplifies the various blocks on the Figure.

FIGURE 1

Checkout & Initial Operations (C&IO) consists of preliminary testing to verify that individual components, such as wiring, fiber optics, PLCs, and computer processors are properly installed and functioning at the component level. Verification consists of checks of the Human System Interface (HSI) software and hardware to verify that it is properly programmed per the functional requirements, conforms to good human factors practice, and appropriately supports operator tasks.

The general objective of validation is to ensure that the software and hardware functionality meets all requirements and supports safe and reliable operation. To be effective, validation needs to be performed with the actual completed system or with a reasonably high fidelity, dynamic simulator. Thus, a simulator was developed that could input signals as the real sensors would and that would also simulate all of the appropriate timing and system response. Due to the nature of the upgrade project and the fact that the facility needed to maintain its operational capability as much as possible during the phase-in of the new systems, a two step validation process was used.

Validation #1 tested the new hardware and software using selected scenarios and procedures, while the facility continued to operate using the old FCS. In the case of the TA-55 FCS upgrade, the design process lent itself very well to using the actual equipment (prior to crossover) for this validation. Thus, this validation was performed with the new, integrated system, including field programmable logic controllers (PLCs), all system wiring, control PLCs, and the operations center HSI computer hardware and software. The only portions not included were the sensors and the termination panels. This validation was performed with simulation programming on a separate computer attached to the system architecture.

A major side benefit to using the described platform to perform the validation testing was that it provided effective operator training on the new integrated system before it was fully operational. It is also available for operator training and system engineering use now that the facility is up and running on the new FCS.

For Validation #1 each subsystem of the FCS (e.g. Criticality, HVAC, Fire Protection, etc.) was separately and thoroughly tested to confirm proper operation of all functional requirements of the subsystem, as defined during the functional analysis phase . These tests included the simulation of the performance of Operational Safety Requirements test procedures. After successful validation of each subsystem, an integrated validation test was performed. The integrated test consisted of a loss of all AC power test. This challenged the FCS system by providing essentially the largest number of alarms and signals possible.

After Validation #1 was successfully completed then system crossover began. Crossover is when the wiring from the actual field sensors is disconnected from the old FCS and connected to the new system. Each subsystem (except HVAC) was transferred during a four day shutdown. The facility was then restarted and operated for about a week, until time for the next shutdown

and system crossover. A number of these shutdowns was needed to transfer all the subsystems. The HVAC was a special case requiring more time (about two weeks) due to its complexity. Thus, the HVAC was the last system crossed-over.

For Validation #2 each subsystem was validated after it has been crossed-over and before facility start-up from the four day shutdown. This subsystem validation was performed by operation of the actual components in the plant. This testing also included the performance of an OSR test for the subsystem in question. Validation #2 thus:

1. Tested the portions of the FCS that were not tested in Validation #1 (sensors and termination panels); and

2. Confirmed that the crossover did not create any unforeseen problems.

Validation #2 was more limited in scope when compared with Validation #1. This saved important plant operation time, since Validation #1 was done with the plant operating while Validation #2 was done with the plant shutdown.

A final integrated validation was needed after all subsystems had been successfully crossed-over and tested. This test confirmed the integrated operation of the entire new FCS. An actual loss of all offsite electrical power was imposed and the integrated response of the FCS and the operators was observed.

The V & V program was very successful. A few issues of the following types were identified and corrected as a result of the program: test procedure errors, a small number of minor software problems, and a timing problem under very high signal loading that caused the FCS to switch from the primary to the secondary computer.

Operators were trained during the installation of the new components. This consisted of classroom training bothonsite and at the equipment vendor, required reading, and review of the new procedures. Also, the new FCS video display units (VDUs) were installed in the Ops Center, prior to crossover, linked to the simulator. Thus, the operators had the opportunity to use and learn them during their spare time, while the facility was still being operated using the old FCS and VDUs.

6. **Summary**

The new Facility Control System was successfully installed and tested several months ahead of the original schedule. The new system is more reliable with fewer failures. It has self-diagnostic features and is simpler to repair. Their is significantly improved documentation for the system and correspondingly better understanding by all facility personnel. The number of VDUs in the Ops Center was increased from four to eight, providing greater flexibility.

The system allows for much simpler upgrades as changes and improvements are identified. Also the simulator is available for testing of and training on any new upgrades. As a result of all the above, safety has been increased by improved operator performance with the FCS and by reduced FCS failures. Further, future facility downtime due to FCS failure and necessary repairs has been decreased.

7. References

J. C. Higgins & J.M. O'Hara, Guidance for the Development of a Test Program for the TA-55 FCS and Control Room Upgrade Project, BNL Technical Report 4193/4-96, April, 1996

J. M. O'Hara, J. C. Higgins, and W. F. Stubler, NUREG-0711, Human Factors Engineering Program Review Model

J. M. O'Hara, et al., Human-System Interface Design Review Guidance, NUREG-0700, Rev. 1

Noah Pope, et al., Upgrade of the Los Alamos Plutonium Facility Control System, presented to the ANS Conference on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, May 6-9, 1996

TA-55 docs (Noah - any here to include???)