LEGIBILITY NOTICE

A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although portions of this report are not reproducible, it is being made available in microfiche to facilitate the availability of those parts of the document which are legible.

3

LA-UR -87-3428 CONF-871007--31

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

LA-UR--87-3428

DE88 001833

TITLE SYSTEM SUPPORT SOFTWARE FOR TSTA

AUTHOR(S): Garnett W. Claborn, CTR-10
Lawry W. Mann, CTR-10
Clair W. Nielson, CTR-10

SUBMITTED TO: 12th Symposium on Fusion Engineering (IEEE)

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes.

The Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy.

MASTER

Los Alamos
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FORM NO. 836 R4
ST. NO. 2629 5/81

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

SYSTEM SUPPORT SOFTWARE FOR TSTA

Garnett W. Claborn, Lawry W. Mann, and Clair W. Nielson
Los Alamos National Laboratory
Los Alamos, NM 87545

Abstract: The software at the Tritium Systems Test Assembly (TSTA) is logically broken into two parts, the system support software and the subsystem software. The purpose of the system support software is to isolate the subsystem software from the physical hardware. In this sense the system support software forms the kernel of the software at TSTA. The kernel software performs several functions. It gathers data from CAMAC modules and makes that data available for subsystem processes. It services requests to send commands to CAMAC modules. It provides a system of logging functions and provides for a system-wide global program state that allows highly structured interaction between subsystem processes. The kernel's most visible function is to provide the Man-Machine Interface (MMI). The MMI allows the operators a window into the physical hardware and subsystem process state. Finally the kernel provides a data archiving and compression function that allows archival data to be accessed and plotted. Such kernel software as developed and implemented at TSTA is described.

The Tritium Systems Test Assembly (TSTA) is dedicated to the development, demonstration, and interfacing of technologies related to the deuterium tritium fuel cycle for large-scale fusion reactor systems. The control software must support the major objectives of TSTA, which are to provide a demonstration of the fuel cycle for fusion power reactors, to develop and test environmental and personnel protective systems, and to demonstrate the long-term reliability of components involved in the safe handling of tritium. At TSTA the primary concern is to prevent the exposure of personnel and of the environment to radioactive substances. The control software for TSTA is implemented in such a way as to provide safety interlocks for personnel and for the environment. The control system for TSTA must execute control algorithms to insure the safe handling of significant amounts (100 grams) of tritium in an experimental environment. Many of the components in use are novel and change as different experiments are performed; thus the control algorithms are subject to modification as more information is gained from actually running the facility.

The fact that TSTA is an experimental facility makes it impossible and undesirable to try to forecast the exact software requirements. Thus the software had to be written in a manner that would allow modifications without compromising the safety requirements imposed by the handling of tritium. This suggested a multi-level approach to the software. In this approach (much like the ISO network model) each level is isolated from the level below and above by cleanly defined interfaces. For example, the subsystem support level interfaces with the subsystem hardware through the software support level. Routines in the software support level provide operations like "OPEN VALVE" and "CLOSE VALVE" to the subsystem level. This isolates the subsystem level from the actual hardware. This is advantageous because changes can occur in any level without the need for propagating the change to any other level.

The TSTA control system consists of the hardware level, the data conversion level, the operator interface level, and the subsystem process level. These levels are now described.

The Hardware Level

The Hardware level is divided into three sublevels: the signal conditioning, the Front End Controllers (FECs), and the process computers. (See diagram at end of paper.) A signal wire is brought into the control room through a patch panel and into a signal conditioning unit. The patch panel provides a means of changing which signal conditioning unit and which CAMAC module a signal is routed to. If such a change were required by a faulty wire or CAMAC module, the change could be made without affecting the higher levels. The signal conditioning units take signals of varying ranges of voltages and maps the signals into a -5.12 volt to 5.12 volt range. The modified signal is then taken to the appropriate CAMAC module.

CAMAC modules are grouped together under the control of a front end controller (Digital LSI 11/23). Typically an FEC handles 3-4 CAMAC crates each capable of holding 24 CAMAC modules. Individual crates can be powered off for module replacement without affecting the FEC operation. The FEC gathers data from the CAMAC modules and formats the data for transmission to the process computer. An Ethernet link is used as the transmission media for FEC/process computer communication. The high bandwidth and wide availability of the Ethernet make it attractive as this communication channel. The Ethernet also provides "hot" connect and disconnect making it easy to switch to the standby net if problems are detected. Furthermore, the Ethernet provides total flexibility of interconnection and facilitates redundant implementation.

The data is received by the two process computers (Data General MV/4000's). One is considered to be running the process while the other is in standby mode, ready for "warm" switchover. The standby computer is also used for software development. A third class of computer also resides on the Ethernet, a dedicated shutdown computer. In case both process computers fail, the shutdown computer provides the ability to control individual hardware components and to safely shutdown subsystems by the use of predefined macros.

The entire hardware system is protected by an uninterruptible power supply (UPS), with both battery and diesel powered generator power backup. The control room is cooled by two air-conditioners and a third, standby air-conditioner is housed in the control room. All this redundancy is provided to insure the safe handling of the tritium in the system.

The Data Communications Level

Data is being continuously collected from the CAMAC modules by the FEC's. This data is periodically placed on the Ethernet. Once on the Ethernet it is available to all processes that have a need for it. On the process computer the Data Communications level receives the Ethernet packets and places the data into the appropriate place in a read only shared database. This level provides a clean interface to the Data Conversion level for accessing the raw data. The data is stored in the 12 bit CAMAC form. This reduces the size of the database and makes archiving and compression easier.

Archiving of data is an important task of the Data Communications level. Snapshots of the database are taken once a minute and stored on disk. This archiving is done on both the controlling and standby process computers creating a disk file of about 12 megabytes of information per day. This data is available for access by subsystem designers, operators and TSTA management and is used for system analysis. At shortly after midnight the previous day's data is compressed. The compression algorithm notes a variable's starting value and then stores the changes from that value in as few bits as possible. Currently a 15 to 1 compression ratio is obtained. At TSTA 3 months of archives are kept on the disk with older data available on tape. (Purchase of a disk to allow 2 years of data online is planned.)

The other task of the Data Communication Level is to provide communication between various software processes. This communication is provided through logical "mailboxes". A process is said to "own" a mailbox if that process is authorized to write to the mailbox. (Only one process is allowed to write in any mailbox.) The mailbox data, like the FEC data, is stored in a read only database. The Data Communications Level also places this data on the Ethernet periodically. The standby process computer reads in this mailbox data so that its database is kept current. This greatly facilitates warm (operator initiated) switchover between the two process computers. Processes at the upper levels are unaware of the switchover because of the presence of logical variables with current values. A system designed in this manner would be easily adaptable to a multi or distributed processor environment. This database is also archived the same as the FEC data.

The last task of the Data Communications level is to provide an interface between upper levels and the FEC's. Commands for FEC execution are collected here and routed to the appropriate FEC with the necessary error detection and correction. This frees the upper levels from the details of how commands are executed and how errors are handled.

The Data Conversion Level

The Data Conversion level provides the conversion between the 12 bit data stored in the database to engineering units used by the upper levels. The conversions go both ways. As commands for execution are received, the set value is in engineering units or is a digital value like OPEN or CLOSED. These values are converted to 12 bit integers understood by the Data Communications level. When data is read by the upper levels, the Data Conversion level converts the 12 bit data into analog engineering units or to the appropriate digital value. The conversions are done on an "as needed" basis to reduce computer overhead.

This level also provides limit checking by periodically checking variables with predefined limits for being in range. If a variable is found to be out of range then a bit is set in the database. An interface to this limit data is provided for the upper levels which will provide various sorts of alarms. Another function of this level is to combine several raw data points into one logical measurement. For example the tritium room monitors provide a digital range information signal and an analog level signal. These two signals are combined to give the physically meaningful value of radiation level. The composite value is stored in the database as a logical mailbox measurement.

The Operator Interface Level

This level provides the human user with an access to the database. This level is subdivided into two levels, the dialog level and the database access level. The dialog level provides the subsystem level and the lower levels with a mechanism to get information to and from the human operator. The dialog level collects messsages called alarms from the upper and lower levels. The dialog level maintains a separate read-only database of outstanding requests for information. The database access level through the Man Machine Interface (MMI) accesses this request database for questions to pose to the human operator.

The MMI runs on 5 Aydin color, character graphic terminals. Through the MMI the operator is able to display predefined piping diagrams, system status displays, and alarm lists. The MMI provides the interface between the upper levels and the human operator. Upper levels can ask the operator pertinent questions and receive replies across the level boundary in a clean fashion. The MMI screen is divided into 4 parts. The top 3 lines are reserved for alarms. These prioritized alarms are messages from all levels reporting errors, conditions that need immediate attention, and general information. The bottom 2 lines of the screen provide the operator command line and response line.

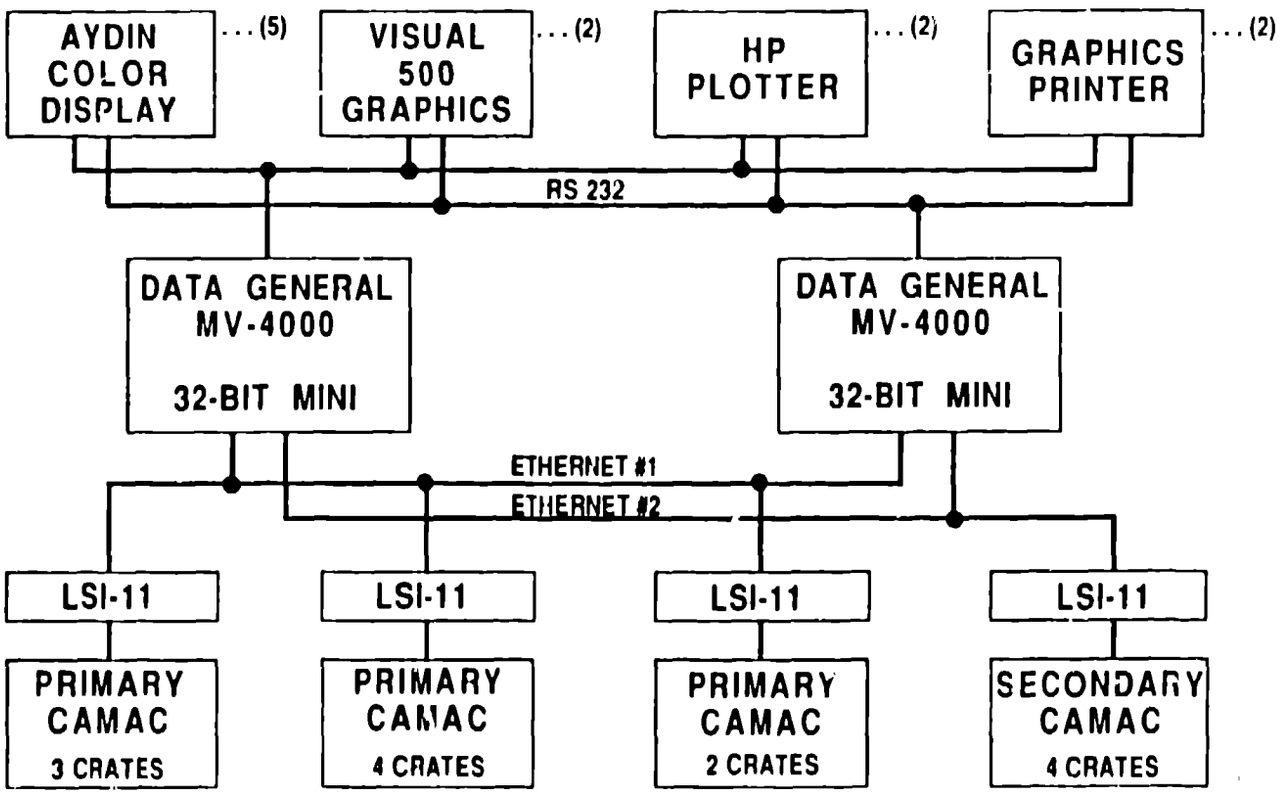
From the command line the operator can control individual subsystem components with commands like "OPEN TWT_CD_LPR1" which means "open the value to the first low pressure receiver in the Tritium Waste Treatment subsystem". Some parameters are designated as more hazardous to operate. These are protected by a second layer which requires confirmation prior to being operated. The confirmation can be one way, such as on OPEN only, or both ways, such as for OPEN and for CLOSE. The operator can also communicate with the subsystem level by setting logical mode mailboxes such as "SET TWT.OPRMODE RUN" which means "Set the operator choice for the Tritium Waste Treatment subsystem to RUN mode". All operator commands are logged on a hardcopy device and in a daily disk file. The daily disk files are searched weekly for unusual happenings and such are reported to management in a weekly report.

The MMI provides a menu driven trackball interface and a keyboard driven interface. Four displays are stored in local memory and are available instantly through the use of function keys, other displays are available after a 3-4 second delay for downloading into local memory. There are currently over 300 displays defined. Also an extensive macro language allows for the execution of predefined sequences of commands such as "STARTETC" which means "start the Emergency Tritium Cleanup Subsystem".

Another part of this level provides graphical information on system parameters. The archive can be accessed and the data presented in tabular or graphical format. Seven graphics terminals are available for graphical output. Two of these have HP 6-pen color plotters attached for hardcopy output. Any terminal can send graphical data to a laser printer for black and white output. Real time trending information can be obtained both in graphical and tabular form. The scan rate can be as fast as 6 seconds between updates. The data so captured is also available for hardcopy output.

The last level is the Subsystem Process Level. It is further described in the following paper in these proceedings.

Conclusions

There are many advantages to a system implemented in levels such as the one at TSTA. It is possible to upgrade individual levels without propagating any errors introduced to other levels. It facilitates software testing, as each level can be easily tested without the upper levels, and with a minimum of coding, can be tested independent of the lower levels. The presence of the levels and of the Ethernet adds flexibility to the software and hardware design. For example, the MMI could be upgraded to stand alone graphical work stations that are connected on the Ethernet. The control software has been in place at TSTA for four years. During that time the computer hardware has undergone a major upgrade and the software staff has been reduced from three to one. That such an upgrade could occur with no disruption of operations and the fact that one person now maintains and enhances the software is an indication of the effectiveness of the TSTA software design.

TSTA CONTROL SYSTEM