Use of a Computer-Assisted Administrative Control to Enhance Criticality Safety in LLNL for Fissile Material Disposition Operations

S.T. Huang  
D.A. Lappa  
T. Chiao

This paper was prepared for submittal to the  
Nuclear Criticality Technology Safety Project Annual Workshop  
Gaithersburg, MD  
May 5-9, 1997

April 1997

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.
DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California 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 the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.
Use of a Computer-Assisted Administrative Control to Enhance Criticality Safety in LLNL for Fissile Material Disposition Operations

Song T. Huang, David A. Lappa, and Tang Chiao

Lawrence Livermore National Laboratory
P. O. Box 808; Mailstop L-128
Livermore, CA 94551

1.0 INTRODUCTION--

All operations at LLNL involving significant quantity of fissionable material conform to the double contingency principle for criticality safety. The typical order of preference for criticality safety control is (1) passive engineered controls such as favorable geometry in equipment and spacing; (2) active engineered control; and (3) administrative control. In many instances, administrative controls are used due to practicality and cost considerations.

Protection against an inadvertent criticality incident is either through the control of two independent process parameters as the preferred approach or through a system of multiple controls on a single parameter. Administrative control generally relies on written procedures and human operators. For example, the two-person rule on the control of fissionable material mass limits has been used in various facilities as a means of meeting the double contingency principle.

It is important to recognize that not all operations which meet the double contingency principle have same safety margin. The term “safety margin” used in this paper refers to the likelihood of failure of a criticality safety contingency and degree of the subcriticality lost due to the failure of such a contingency. The ways to improve safety margin of a particular operation may be achieved through selecting a contingency with a lower probability of failure and/or using operational parameters with a larger subcriticality margin. In the area of administrative control, the assessment of safety margin is generally hampered by the lack of a validated model and an applicable failure rate data base to analyze relevant operator actions or lack of such behavior. Thus, the use of administrative control is a recognized week link in overall criticality safety control measures. To circumvent to some degree the difficulty associated with the issue of human reliability, many organizations opt to take a defense-in-depth approach if administrative control is used.

This paper deals primarily with the use of a two-person rule on the mass limit control. Main emphasis is placed on the appropriate use of a computer program to assist operators in carrying out mass control. An attempt will be exercised to compare the use of a mass control card system under a two-person rule with a computer-assist two-person system. The interface points relevant to criticality safety between computer and human operators will be identified. Features that will make a computer program useful in a
multiple workstation application environment will be discussed along with the merits of using the computer program. How such a computer-assist administrative control may be incorporated in the overall infrastructure for criticality safety will be analyzed. Suggestion of future development of using a computer program to enhance safety margin will also be made to stimulate further discussion on the application of computer technology for real-time criticality safety control.

2.0 DESCRIPTION OF THE COMPUTER SOFTWARE FOR MASS LIMIT CONTROL

At LLNL, a computer system has been used for tracking the nuclear material for accountability. The system can track the movement of items and provide the current inventory at each workstation. During last few years, this program has been used to assist operators in meeting the mass limit for each workstation for criticality safety control.

The computer program requires independent entries by two operators for all transfers. It is also required that both operators independently visually verify the fissile material inventory before and after transaction. Therefore, two operators will validate the mass limit for that transfer. This provides two independent controls on the same parameter (mass). The loss of one control on mass would not allow the mass limits to be exceeded and therefore double contingency is met.

The LLNL compute program was originally designed for the use of material tracking and material accountability. In order to fully use the computer system for criticality safety controls, additional improvements of certain aspects of the system are needed.

The new improved computer program should consists of three parts: 1). a mass module to track mass inventory, 2). a module to store critical mass limits for each workstation, 3). a module to provide the interface between the mass modules and the critical mass limit modules as well as the interface with the operator.

The first module should be able to update the material inventory data base as an item is transferred from one location to another. It shall also provide at any time the current mass inventories at a given location upon request.

The module for critical mass limits should include all current appropriate mass limits including limits for the various operating conditions, dispersible components and box loss, and isotopic compositions for a given location. The mass limits shall be defined by approved operation safety procedures(OSPs) only and entered/maintained independently from operators. The change of mass limit shall not be made before the formal change of an OSP is issued and the change shall not be entered by the operators. However, the operator should determine which operating condition is for each intended operation in a workstation and be able to verify the mass limit provided by the computer against the OSP. In addition, the module for critical mass limits should have potential of expansion to include other relevant control limits such as the amount and type of moderator allowed in each workstation, effective date of OSP, etc.
The module which provides the interfaces should be the only link between the mass inventory module and the critical mass limit module. Therefore, both inventory system and mass limit system can be updated and QA independently. The interface module should be able to obtain the current mass inventory information from the mass inventory module, add on the mass of the proposed transaction, and performs on-line comparison with the appropriate mass limit obtained from the mass limit module. If the proposed transaction violated the allowed limit, a real time warning signal should be sent out to the operator and proposed transaction should be prohibited by computer. The interface module will perform all mass calculations for workstations involved in the material transactions. Once the transaction is completed, the new mass inventories in workstations will be sent to the mass inventory module to update the inventory database.

The interface module should be user friendly. The interface between the operator and the computer system is mainly through the computer terminal, the monitor display, and the printer. The computer terminal is for receiving request from the operator. The required operator input should be as simple as possible. The monitor display is for computer's response to operator’s requests. The display should be clear to understand, simple, and no unnecessary information to confuse the operator. The computer printout provides hard copy record of the transaction. The printout should be self-explanatory. If necessary, the printout should provide several levels of details of the transaction information.

The interface system must provide capability for “two man” verification control and log all transactions for audit. The “two man” verification rule should not only require the second operator to log in his user and password to concur the transaction, but also enter some “key” requests for that transaction. The “key” requests may include the destination workstation number, series number of the transferred item, or a check mark to concur the mass inventory staying in the mass limit after the transfer, etc. The computer logging should include not only the successful transactions, but also transaction request rejected by the computer.

The interface system must be able to accommodate multiple transaction requests simultaneously. The computer will be used by the entire facility at various locations (or by all fissile facilities at LLNL). Multi-user is a necessary requirement. If conflicted transaction request arises, the interface system must be able to identify the conflicted requests, provide a real time warning to both users, and prohibit the involved transactions until issue is resolved.

3.0 Comparative Evaluation

3.1 Method of Evaluation

The comparison of manual versus computer-assisted mass control systems is significantly complicated by the human elements in each system. The wide variability in human performance, the complexity of analyzing human failure, and the dearth of significant relevant databases can make the quantitative reliability analysis of such systems difficult, if not impossible.
However, there are objective methods for evaluating the reliability of systems involving human action, and, more importantly, the uncertainty in performance data is more problematic to absolute assessments of reliability than it is to relative comparisons such as this one. There is a significant body of literature dealing with many aspects of reliability analysis, human performance, etc., and we do not attempt to summarize it here. Indeed, that literature makes clear there are continued needs to accumulate and gather validated databases on reliability for complex systems involved human operators.

In this comparative evaluation, we do not address the reliability of manual and computer-assisted mass control systems in detail. Instead, we describe such systems generally, and focus on those details most relevant to differences in reliability of the two systems.

3.2 Manual Mass Control System

3.2.1 General Description

As the name implies, this class of systems is highly or exclusively dependent on human action to control mass. A typical example of such a system is one employing log sheets or “blue cards” for each workstation, and on which material handlers and/or their supervisors make handwritten entries for such quantities as: the present inventory of a specific material type in that workstation, the amount of that material type being transferred into or out of a workstation, the resultant inventory, and administrative notations such as check book markings and signatures to indicate that the resultant inventory is within mass limits for the workstation and/or that there has been multi-person control of the operation.

One of the most significant aspects of a purely manual control system is that all arithmetic involved with calculating transfer masses and resulting masses is carried out by humans, presumably with the aid of basic computing aids like hand calculators. (As defined here, such systems do not comprise computerized materials control and accountability (MC&A) or other such systems which routinely track, in a semi-automated way, the inventories of workstations, etc. for safeguards purposes.)

The specific process for mass control calculations can vary, depending on the degree of redundancy that system designers seek to establish. For example, a system could require that two handlers independently, using different techniques and without interaction, calculate the masses involved with a proposed operation and evaluate its appropriateness, communicating their findings with each other only when both of them have completed their assessment. By contrast, a system could have a primary handler carry out the assessment, and a supervisor “check” the completed assessment for validity; or, two handlers could together carry out the assessment, with the second handler monitoring, at each step, the accuracy of the primary handler’s calculations; or, etc.

3.2.2 Reliability Considerations
For this system, the large dependence on human action in conformance with administrative controls is a potential weakness. Depending on the specific design characteristics, irrespective of personnel quality and training, such manual systems will have greater or less reliability by virtue of the degree of true redundancy derived from human action. Specifically, consider an electronic system in which two identical components, in parallel, each perform a critical function, and either one of which is sufficient for successful system operation. The degree of reliability enhancement from these parallel redundant components is affected strongly by the degree of independence of the two components. For example, if the specific component has an inherent design weakness to vibration, then, if physically collocated, there will be little or no improvement in reliability with respect to vibration, as both components are likely to fail simultaneously, i.e., a common cause failure.

Likewise, the degree to which the employment of multiple personnel in manual mass control systems enhances reliability is highly dependent on the correlation of failure of those personnel. Among the systems described in section 3.2.1, we can see that some human actions may be more independent of other, redundant human actions, if opportunities for correlation are reduced or eliminated. Thus, having two handlers, employing different techniques, redundantly assess the viability of an operation is probably superior to having them work “cheek by jowl” to assess viability as a team.

One of the intrinsic weaknesses of a pure two-person mass control system is that the system is prone to common cause failures such as a supervisor’s influence towards conduct of operations, human susceptibility of circumventing procedures when under programmatic schedule pressure, and inability to recall details under multiple work-station working environments.

3.3 Computer-assisted Mass Control Systems

3.3.1 General Description

In these systems, designers have attempted to improve reliability, reduce costs, increase productivity, or etc. by employing computer technology to complete one or more functions carried out by humans in a manual mass control system. For example, the “pure” manual system described in section 3.1 is actually mildly computer-assisted by virtue of the hand calculator -- a computer -- being used to carry out simple arithmetic operations which otherwise would be done using pencil and paper. We nevertheless regard the system in 3.1 as “manual” because, over the past few decades, the use of hand calculators has been deemed, appropriately or not, to be greatly superior to longhand arithmetic for all but the most trivial calculations. (Indeed, not many people would readily identify their pocket calculator, wristwatch, etc. as an electronic computer because those objects have entered the realm of “tools”, i.e., low-tech and highly reliable; while computers are now deemed to be overly complicated and unreliable objects like PCs and programmable VCRs.)

For our discussion, “computer-assisted” refers to more than the employment of hand calculators and other simple devices. Specifically, it means the use of one or more CPUs, running compilable software, employing non-volatile databases, and accessed through a human-machine interface such as a keyboard, mouse, and monitor.
There are a variety of ways in which computers can be employed to assist with mass control. The most obvious and, probably, the most common way is to employ computers to carry out those functions to which computers are best suited. Computers tend to be far more reliable than humans at: storing and retrieving large quantities of numeric data; rapidly carrying out numerous, complex arithmetic calculations with great precision, including comparative operations; monitoring a data stream continuously for interesting characteristics; and ease of record keeping and management.

Consequently, one of the most prevalent uses of computers in mass control operations today is in the safeguards and security area. Such MC&A systems are employed to keep track of the type and amount of SNM in various locations in a safeguarded facility. If those locations are defined to be the same level of workstation at which criticality or other mass limits are imposed, then the potential utility an interface with such a MC&A system to obtain inventory to mass control is self-evident. If material handlers are being administratively required to employ a computer-based MC&A system to log all SNM transactions, then additional software and data can extend that MC&A system to one which also monitors workstations for the potential of exceeding any of various mass limits, whether criticality, fire safety, dispersability, etc.

3.3.2 Reliability Considerations

It is noted that the reliability of a computer-assist administrative control depends largely upon the design features of the system and its implementation within the framework of the overall criticality safety control infrastructure at a particular facility. Perhaps the single most important factor affecting the reliability of a computer-assisted mass control system is whether the computer-based functionality is added to supplement or replace human-based functionality. Borrowing from the systems described under section 3.1, consider two handlers who independently assess the viability of a transaction before comparing their results. If the system is modified so that, after this process, the handlers then are required to carry out the transaction via an MC&A system with a mass limit checking function, then the system reliability is likely improved by the additional computerized operation. However, if the employment of mass limit checking within a computerized MC&A system means that procedurally, or in practice, handlers no longer carry out their redundant and independent assessment of transaction viability, then system reliability may be degraded.

One of the clear advantage of a computer-assist mass control system is the ability of the program to provide a real time warning when a proposed mass transfer exceeds the allowable mass limit of a workstation. The benefit of such a real time warning function may be recognized in reliability evaluation as (1) providing an independent element from human errors, and (2) providing a marked reduction of the failure rate of a contingency. Thus, such a system is much less susceptible to human failures and will provide much needed enhancement to administrative control.

3.4 Comparison of Manual and Computer-assisted Reliability

Detailed, direct comparison of two such systems is possible only with fully developed systems descriptions. Here, we are dealing with more general aspects of
manual and computer-assisted mass control systems. Thus, our comparison is general in nature, though some specific points of comparison based on hypothetical details is offered.

**Double Contingency Principle**

A natural basis for weighing the advantages and disadvantages of computerization of mass control procedures relates to the double contingency principle as stated in DOE Order 420.1 “Process designs shall incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible. Protection shall be provided by either (i) the control of two independent process parameters (which is the preferred approach, when practical, to prevent common-mode failure), or (ii) a system of multiple controls on a single process parameter. The number of controls required upon a single controlled process parameter shall be based upon control reliability and any features that mitigate the consequences of control failure....”.

Independence- A key requirement here is “independence”; meaning among other things, to prevent common-cause failure. This basis alone argues for a robust criticality safety control employing diverse safety features. Thus, systems which are highly dependent on multiple handlers and/or supervisors, all subject to common modes of human failure and, therefore, common cause failure under similar or identical operating conditions, are likely to have less defense-in-depth than systems which depend on a combination of human and “mechanical” safety features. (Here, “mechanical” is used to mean features which are based in hardware, including electronic computers, etc., with little or no active human participation in the safety function of that feature.)

Unlikely- Another key requirement is “unlikely” which deals primarily with frequency of failure. By example, consider the system described in section 3.1, wherein two personnel simultaneously and independently assess the viability of a transaction before sharing their assessment. If both individuals are employing the same data, the same assessment method, and under the same conditions, the likelihood for common mode or common cause failure is greater than if the two employed different data and methods under different conditions. Consequently, replacing one of these fully manual checks with one that relies to strong degree on computerized databases, algorithms, and environments may greatly reduce the potential for simultaneous failure of multiple controls.

**Controls Reliability**

The number of controls required upon a single controlled process parameter is based upon control reliability. To strengthen a control reliability, one needs to examine all the key features contributing to the reliability of that control and seeks to strengthen each of those individual features. Thus, for a feature involving human action, factors like: education, training, and experience; performance monitoring and metrics; real-time performance feedback; environmental factors; morale; etc. are all enormously important to controlling the reliability of that feature. Humans are much more prone to make arithmetic errors than, say, a well-developed software application platform. Where operations involve the retrieval and manipulation of numerical databases, as with SNM masses in a
critical mass control process, there is likely to be significant benefit from the employment of a computerized safety feature in parallel with a human-based assessment of transaction viability.

Whether this argues for the employment of two, redundant, computer-assisted assessments as superior to one human and one computer-assisted assessment is doubtful. As with human actions, computer-based actions are also prone to failure from common modes or causes, such as software quality assurance errors, data entry errors, hardware malfunction, human-machine interface failure, etc. However, this type of weaknesses can generally be minimized by proper system design and quality assurance implementation. In real world applications, human operators are generally needed except in a totally remote and totally automation robotics environment. It is therefore advantageous to employ computer-assist administrative control to capture the merits of such a system over a pure administrative control measure.

Additional Considerations

The employment of a computer-assisted mass control safety feature may provide additional improvements to overall system reliability than those discussed above. One of such improvements is the ability to provide real time warning when the proposed material transfer request exceeds the mass limit of a workstation. As mentioned earlier, such a warning feature enhances the “independence” aspect of the controls and provides a marked improvement of the “unlikely” aspect of the controls as well. Furthermore, given the facility with which transactional data can be captured, stored, and processed -- even in real-time -- by modern computer systems, there is enormous potential for a computer-assisted system to be employed to monitor materials transactions, including the temporal frequency and type of transaction, material quantity and type distributions, handler calculation error, handler duty factors, etc. The list is long, and that fact points to the high potential utility of computer-assisted mass control system safety features to improve overall system reliability and reduce the risk of inadvertent criticality.

4.0 CONCLUSION

Using computer system to track the nuclear material for material accountability as well as nuclear material safeguard is not a new concept. DOE facilities and other government installations have adopted the computer systems for this purpose for a number of years. Perhaps using the real time computer system for criticality safety control is the next-step development for all DOE facilities. At LLNL, not only it is necessary to use computer system to track material transaction for material accountability, but also the computer system is used for criticality safety control: increasing the criticality safety margin by enhancing the two man controls on the mass.

Computer system will reduce math errors in tally up material quantity. LLNL performs research work for the government. By the nature of research work which is different from task performed at the production facility, the material in each workstation may be different from day to day, different from task to task. The inventory of material in the workstation can not be tallied by the number of batches. It must be tallied each time
during material transaction. In addition, many times, it is necessary to transfer material from one workstation though several other workstations which may have different mass limits. Material, therefore, must be divided or combined. Adding, subtracting and recording the material is not difficult, but is tedious. Repeated tedious work will increase the probability of error. One of the error of special criticality safety concern is mass violation. But computer system will reduce math errors in tally up material quantity to zero.

Computer provides an automatic comparison of the mass limit and the inventory for each workstation. If any transaction will result in violation of the mass limit, the computer will provide a real time warning. The automatic comparison and real time warning are desirable features to prevent violation before its happening.

The computer may still provide erroneous mass inventory in the workstation if the researcher input erroneous material quantity or item identification. With two persons to verify the computer inputs, especially, if some “key” requests for each transaction are to be input by both persons, the computer assisted “two man” rule can be indeed considered to meet the double contingency with high safety margin as committed by defense-in-depth criticality safety program at LLNL.

Finally, the computer will log all transaction records. These records can be used as accumulation of valuable real time failure data base. These data not only can identify operations which may lead to higher probability of mass violation and consequently the operation procedures can be revised and improved, but also provide basis for other studies such as probability and fault tree analysis, trend analysis for operations.

Furthermore, if so desired, the interface system could provide capability for “Training”; using the real time information in each workstation to perform the computer assisted transaction training to new operators, independent of other transaction activities. Once the computer terminal is logged in the “training mode”, all data from mass inventory module and critical mass limit module should be available to the training, but all transactions performed under the “training mode” can not be used to update the data in the mass inventory module. The use of the “training mode” should be approved and controlled by the training department only.

This work was performed under the auspices of the U.S. Dept. of Energy at LLNL under contract no. W-7405-Eng-48.