Multiple Processors vs. A Single Processor In Attribute Measurement Systems

Robert Landry, Luca Gratton, and Duncan MacArthur
Los Alamos National Laboratory

Los Alamos, NM 87545 USA

Multiple Processors vs. A Single Processor In Attribute Measurement Systems

Robert Landry, Luca Gratton, and Duncan MacArthur
Los Alamos National Laboratory
Los Alamos, NM 87545 USA

SUMMARY
Competing design proposals for data acquisition and analysis components in an attribute measurement system (AMS) differ in the processor (CPU) specifications, and in the distribution and tasking of the processors. Primary design considerations include the number of CPU's, their locations within the system, and their processing assignments. Because the processor system must communicate with multiple measurement collection units, viable design options include the use of one multitasking CPU or multiple single-tasking CPU's.

After a comprehensive comparison, the authors advocate the use of multiple, single-tasking CPU's rather than a single, multitasking unit (Tables 1.a and 1.b). This comparison is made on the basis of anticipated attributes for generic systems. Detailed comparisons in each of the categories require formal system descriptions, which are beyond the current scope of this effort.

The multiple processor design provides distinct advantages for AMS hardware and software simplicity, certification, authentication, repair times and failure modes, processing capabilities, and information security. The single processor design has advantages for apparent hardware simplicity (i.e., the visual perception of simplicity), integration, system size, and communication network security. Ties are recorded for physical security, the cost of processor acquisition, and processing system reliability.

Table 1.a. A Categorical Comparison of Processor Design Solutions.

Category	Advantage To		
	Multiple Processor	*Single Processor*	*Tie*
Hardware/Software Functional Simplicity	●		
Hardware Apparent Simplicity		●	
Hardware Integration		●	
Physical Size of the Processing System		●	
Processor Certification	●		
Processor Authentication	●		
Duration of Processor System Unavailability and Repair Time	●		

Table 1.b. A Categorical Comparison of Processor Design Solutions (Continued).

Category	Advantage To		
	Multiple Processor	*Single Processor*	*Tie*
Restriction of Processor Failure Modes and Criteria	●		
Processing Mode Capabilities	●		
On-Processor Information Security	●		
On-Network Information Security		●	
Physical Security			●
Reduced Cost of Acquisition			●
Processor System Reliability			●

INTRODUCTION

An AMS allows qualitative assessments to confirm declarations for nuclear material properties without divulging classified information. Differences among competing design proposals for an attribute measurement system include the specifications for computer processor (CPU) control of the measurement subsystems, and for the distribution and task-devotion of the processors. Primary design considerations include the number of CPU's in the system, and their processing assignments among many possible system control distribution plans.

A proposed design solution uses several small microprocessors in the data gathering system to implement different functions. An alternative proposal is to use only one processor to perform all the functions in multitasking operations. In this paper, we present advantages and disadvantages of each approach.   Because advantages for the multiple processor implementation are disadvantages for the single processor configuration and visa-versa, both advantages and disadvantages are presented in the context of the multiple processor implementation. The disadvantages of the multiple processor implementation are understood to be advantages of the single processor configuration.

ADVANTAGES OF A MULTIPLE PROCESSOR DESIGN

The use of a multiple processor design for the attribute measurement system confers advantages in the categories of simplicity of function, certifiability, authenticatability, modularity, length of system recovery and repair time, system development time, failure criteria and modes, processing modes, and information security. There is no significant advantage for either solution in the category of physical security of communication and power lines.

2

Simplification

Simplicity is a desirable system design characteristic that may enhance system reliability. Simplicity additionally accelerates maintenance and repair operations, and eases certification and authentication activities. A multiple processor solution is preferable for achieving a high degree of system simplicity.

A multiple CPU design employs a basic single-tasking operating system and limited instruction set on each processor. A simple processor running a basic operating system is easier to inspect than a single processor running a more complex multitasking operating system. This observation is consistent with the findings of a working group formed to review information barrier system concepts, which has recommended that extraneous code and complex operating systems be avoided.[1] A simple design facilitates visual inspection of the physical layout of the CPU's, cables, interconnections and interfaces to other hardware. An advantage of a multiple processor solution is that the physical architecture better mimics the functional architecture. It is therefore easier to visually inspect a multiple processor design with a smaller number of traces and connections at each of the dedicated CPU's, and a limited distribution of interfaces among CPU's, because the required function of each CPU is simpler than for the single processor design. Additionally, the multiple CPU solution better facilitates the removal and replacement of individual processors because fewer interconnections exist at each processing node and because simple single-tasking software requires only a limited suite of diagnostic checks following installation. Finally, the hierarchical software structure that is inherent to the multiple CPU solution better compliments the hierarchical physical architecture.[2]

Certification

Certification and attestation of the AMS are performed by the party hosting the measurements (i.e., usually the steward of the nuclear materials). Certification and attestation ensure that the AMS adequately protects sensitive information while operating in a secure acquisition mode. It is more efficient for the hosts to certify a simple processor running a basic operating system than a single processor solution running a more complex multitasking operating system. From the certification standpoint, a network of simple processors, each running a basic operating system and instruction set, can be evaluated on a node-by-node basis to ensure operational integrity. Compared to a single processor design, the multiple CPU design is better distinguishable in terms of component functionality and dedication of purpose. The functional dedication facilitates systematic inspection processes consisting of a series of simple checks that are specific to a given processing node. Because individual CPU tasks are dedicated, and reduced compared to the single multi-tasking CPU design, it is easier to identify execution errors, aberrant and unauthorized operations at a given node. Smaller CPU stacks and layers of boards can be used for each processor, thereby reducing the likelihood that undetected programmable logic or persistent memory is present, or that extraneous functionality exists. With simpler instruction sets, smaller sizes for executable single-tasking programs on each CPU, and dedicated function, the multiple CPU design allows minimization or elimination of unused sections of memory so that they are not exploited for covert data storage or code execution. Memory optimization for the intended processing operation also provides impediments to the execution of self-modifying code. Similarly, with the functional dedication and reduced number of interconnections at a single processor in the multiple CPU solution, the certification of inputs and output connections at processing nodes is simpler than for the single CPU option.

Authentication
Authentication is performed by the party monitoring the measurements. Authentication activities provide assurance that the AMS implementation provides genuine and accurate output. Accurate output is demonstrated by the evaluation of reference materials in an open (non-secure) measurement mode. The benefits of a multiple CPU design to the authentication procedures are analogous to those for certification procedures. The multiple CPU design facilitates the authentication process in three major categories: abilities to conduct (1) detailed examination of equipment, (2) functional and (3) system performance testing.

Multiple processor implementations may include standardized hardware components to allow for module exchange. For a modular CPU design, a single processor is considered to be an interchangeable module. Replacements for the CPU hardware components of multiple subsystems can be stored in a reduced (compared to a single CPU solution involving multiple expansions) spare parts inventory that consists of a single type and model of processor board, perhaps with the exception of the software PROM. The use of standard modular hardware allows random component selection from a larger pool of replacement parts. Because the same part may be used for components in multiple subsystems in a modular, interchangeable component design, it is less likely that a defect or engineered vulnerability in the replacement can be successfully exploited for installations in all eligible subsystems. The use of a random hardware selection procedure in situations where the host supplies the hardware, therefore, provides authentication process advantages that are amplified where modular CPU designs are employed. Moreover, these modules are inexpensive. Additionally, if all of the modules (processor systems) are identical with the exception of the software PROM, replacement of a failed module is faster. Two existing attribute measurement system designs with specifications for multiple processors use single board computers conforming to a PC-104 architecture to achieve a degree of modularity.[1,3]

Recovery and Repair Times
For identical types of CPU failure, the time to system repair and the duration of system unavailability can be reduced with a multiple processor design, relative to a single processor design. System state-of-health software can identify a failure in a single module, and notify the operator of the problematic module. Prior attribute measurement system designs conduct operator notification by use of an unclassified output error signal that crosses the data barrier.[4] More detailed error messages would probably require operator access to diagnostic messages that reside within the information barrier security enclosure, and may need to be preceded by an active purge of sensitive information. The distribution of control and processing tasks among dedicated CPU's makes problem isolation and identification simpler; the characteristic of the failed function indicates the problematic node and operation in a multiple processor design. Finally, the replacement of the failed processor requires installation and manipulation of a limited number of connections for the multiple processor design (e.g., see Reference 4, p. 10, Fig. 8). Processor replacement would be a standard and rapid operation where modular components are concerned.

The scope of diagnostic and operational integrity checks for a replacement module in a multiple processor design can be limited to tests for the proper operation of the affected subsystem. The

ability to limit scope reduces the time required to develop, troubleshoot and debug simple hardware and software configurations in a multiple CPU design. Additionally, the diagnostics software for the individual single-tasking processors can be relatively simple in the multiple processor design. Because the multiple CPU's are controllers for respective subsystems, troubleshooting and debugging may proceed for the subsystems individually. For a single processor design, all system functions would require testing following replacement of the failed processor component and system software. Each diagnostic check in a series of tests would involve evaluation for the proper operation of relevant subsystems in a multitasking mode for the single processor solution. The additional checks required for the multitasking system would correspond to an increased expenditure of time in performing diagnostics. Additionally, a relatively complex diagnostics and control program is required to take advantage of the multi-tasking operating system in the single CPU solution.

Information Security And System Reliability
The level of physical security of the power and data communications lines and CPUs is dependent mostly on the security enclosure, and is independent of the number of processors used in the system. Either design requires the same number and types of barrier penetrations through a shielded security enclosure for power delivery and communications. The use of multiple processors requires a greater number of communication buses between CPU's, but all added buses are located within the security enclosure.

In an efficient multiple processor design, sensitive information is distributed among multiple, secure processors. Applications for other attribute measurement systems with information barriers have used multiple CPU's, with operational relegation to either dedicated classified processors and other unclassified processors in a distributed processing mode.[1] Ideally, the entire ensemble of sensitive information is not simultaneously resident on a single processor for the duration of a measurement, as is the case in a single processor solution. Therefore, unauthorized access to an entire ensemble of sensitive information on a multiple processor system requires more work and the defeat of more subsystems than with a single processor. These considerations conform to functional requirements that mandate a minimization of the amount of classified data residing at each stage of the system.[5]

Additional security benefits of a multiple processor design are that fewer memory operations are required and that memory capacities can be sized for the subsystem operations. Fewer manipulations of information in core memory are required for a network of single-tasking processors than for a multitasking single processor. Consequently, sensitive information vulnerabilities are lowered by the less frequent storage and retrieval that occurs with the multiple single-tasking processor design. Finally, sizing the memory in hardware such that it is just sufficient to accommodate the executable and any runtime overhead requirements is a security measure that provides assurances that unauthorized code execution is not occurring on any of the processors. This resident memory tailoring is more difficult to do with a single, multitasking processor because runtime dynamic memory allocation demands are generally greater.

A multiple processor design is less sensitive to a single failure, and is easily designed for the system to fail gracefully while providing diagnostic warnings. This design thereby allows the retention of important system functions, the active archival or erasure of information as

appropriate, the broadcast of diagnostic information, and the recovery of crucial system capacities (e.g., information security functions) following the loss of a CPU. A single processor solution is prone to catastrophic failure with the loss of a CPU. For a single processor design, loss of the CPU has the consequences that core system functions are disabled, that information is irretrievably lost, and most importantly, that the system is unable to transmit diagnostic information to the operator.

Processing
The parallel processing capabilities of a multiple processor system can be used to shorten data collection cycle times. This may only be a discernable advantage where the measurement count rates are high, because no processor system supervisory deadtime from the multitasking operation in a single processor configuration would be encountered with multiple processors. However, this may only be a modest benefit that further shortens already-brief collection cycles.

ADVANTAGES OF A SINGLE PROCESSOR DESIGN
The use of a single, multitasking processor design for the attribute measurement system offers advantages in the areas of hardware integration, size, apparent simplicity and network security.

Integration, Size and Apparent Complexity
An advantage of the use of a single multitasking processor is the integration of all system control and analysis functions in a single piece of hardware. This alleviates some of the interface and communications issues present for the multiple processor design, but places added burdens on the software, particularly with respect to security, reliability and programming error issues in multitasking operations. Because of the hardware integration, the volume of a single processor is generally accepted to be less than the combined displacement of multiple processors and communications lines. Therefore, it is expected that less internal space is required for electronics. The apparent complexity (i.e., the observer's visual perception of system complexity) of a single processor solution is lower than for a multiple processor system. While the validity of this perception does not stand up to a detailed consideration of the functional simplicity of the entire (hardware and software) system, the perception may confer advantages for host and/or inspector acceptance of a single processor design.

Hardware Acquisition and Operation Costs
The relative cost of acquisition for a single multitasking processor system, compared to that for multiple single-tasking processors, is dependent on the specific design proposals. If the CPU's considered for the single and multiple processor implementations are equivalent, it is reasonable to expect that the acquisition cost for the single processor would be lower. Processor prices are currently low, and the processors are among the least expensive components in the attribute measurement system for either the single or multiple processor solutions. For these later reasons, the processor acquisition cost is considered to be indifferent to a single or multiple processor solution.

The integrated costs of acquisition, installation, maintenance, and repair are also dependent on a comparison of specific design proposals. However, the computational expense is lower, and the utilization factor is much greater, for one complex computer system running a multi-tasking operating system than for the distribution of load over many CPU's. Finally, the operational

costs (e.g., power requirements) are lower for a single multitasking CPU. Though it is unlikely that computational and power costs are significant economic factors in the operation of an attribute measurement system, operational cost issues may have added significance in applications involving frequent or continuous measurement system use in remote locations.

Information Security And System Reliability
The single multitasking processor solution is slightly superior on the issues of network vulnerabilities and reliability issues. The multiple processor design requires interprocessor interfaces via communication lines and ports (i.e., a network). Possible network security measures include the enforcement of one-way data transfers, the disconnection of network connections during periods of inactivity, checksum-based block protection schemes, encryption, and key management and authentication.[6,7] Few elaborate network security schemes should be necessary because of the physical protection inherent to the location of the system within an information barrier enclosure. However, network security must be considered with a multiple processor solution. The advantage of a single multitasking CPU design is that no interprocessor communication security considerations exist.

Although the single processor implementation has a quantitative advantage for system reliability if all CPU's have equivalent component failure probabilities, the quantitative difference in system reliability between single and multiple processor designs is negligible and demonstrates an indifference to design solution for likely implementations (i.e., comparisons to multiple processor systems with far fewer than 10 CPU's). Differences in system failure probability scale linearly with the number of processors. Parametric comparisons demonstrate the scalings for the examples of a 1 and a 3 CPU system over an arbitrary service lifetime. For small independent and constant component failure probabilities, the parametric comparisons show that the system failure probability is an intuitive factor of 3 greater than that for a single processor system. Only at high uniform component failure probabilities (> 0.1) do the system failure probabilities for the 1 and 3 CPU systems converge. Because a reliable design implementation would lead to the choice of processor components with failure probabilities less than $1 \cdot 10^{-3}$ over a standard service life (i.e., prior to routine processor replacement), the difference in the values of system failure probability by a factor of 3 between solutions is of negligible consequence for overall system reliability.

The computational loads on each of multiple processors would be smaller than for the CPU in a single processor design. Therefore, it is likely that smaller and simpler CPU's can be used in a multiple processor design. Each of the simple (i.e., smaller number of traces and lower circuit density) CPU's would have a higher component reliability than the CPU in the single processor configuration. This results in a sub linear scaling of the system failure probability, relative to the failure probability for a 1 CPU system. The reliability differences of the 1 and 3 CPU systems may, therefore, may be much less than a factor of 3 under actual implementation.

CONCLUSIONS
A comprehensive consideration of the advantages and disadvantages for single or multiple processor design options results in a general endorsement for the multiple processor design by the authors. The multiple processor solution provides distinct advantages in the categories of functional simplicity for hardware and software; processor certification; processor

authentication; the brevity of processor system unavailability and repair time; the restriction of failures to a tolerable field of failure modes and associated criteria; processing mode capabilities (e.g., parallel); and processor-resident-information security. The single processor solution has advantages in the categories of apparent hardware simplicity; the integration of processing hardware; the processing system size; and information security over any inter-processor communication network (the single processor does not have this network vulnerability). Though the single processor solution nominally enjoys a modest quantitative advantage over the multiple processor design in the category of processor system reliability, a tie is recorded for the competing solutions in this category. The tie is assigned because the system reliability is largely indifferent to the solution (provided the number of processors in the multiple processor system does not approach or exceed 10) in the anticipated individual component reliability regime. A tie also occurs in the physical security category, because there are no significant differences between the barrier enclosures, or the number and types of enclosure penetrations, for the competing solutions. Finally, the processor acquisition cost category is indifferent to the type of solution. Processors are currently of low expense, and are among the least costly of components in an attribute measurement system with either single or multiple CPU's.

REFERENCES

[1]Bruce Geelhood, Richard Comerford, David Lee, James Mullens, and James Wolford, "Review of Two US Information Barrier Implementations," Report PNNL-SA-34973, Pacific Northwest National Laboratory, June 26, 2001.

[2]Sally Bahowick, George Staehle, Daniel Decman, Randy Logsdon, Greg White, Thomas Gosnell and Thomas Moore, "Functional Specification Inventory Sampling Measurement System (ISMS), Version 1.04," Lawrence Livermore National Laboratory, June, 2002.

[3]Duncan W. Mac Arthur, "Proposed Attribute Measurement System (AMS) with Information Barrier for the Mayak/PPIA Demonstration: System Overview," Report LA-UR-99-5611, Los Alamos National Laboratory, 1999.

[4]Rena Whiteson, Duncan W. Mac Arthur, and Robert P. Landry, "Functional Specifications for a Prototype Inspection System with Information Barrier," Report LA-UR-99-1174, Los Alamos National Laboratory, 1999.

[5]Rena Whiteson and Duncan W. Mac Arthur, "Functional Requirements for a Prototype Inspection System and Information Barrier," Report LA-UR-98-5982, Los Alamos National Laboratory, 1998.

[6]Bruce D. Geelhood, "Information Barriers to Protect Sensitive Information During Nuclear Weapons and Materials Inspections," Report PNNL-11982, Pacific Northwest National Laboratory, September 2, 1998.

[7]Matthew J. Moyer, Josyula R. Rao, and Pankaj Rohatgi, "A Survey of Security Issues in Multicast Communications," *IEEE Network* 13(6), pp. 12-23, November 1999.