SANDIA REPORT

SAND 2004-0527
Unlimited Release
Printed February 2004

Architectures & Requirements for Advanced Weapon Controllers

Paul Klarer, Brian McMurtrey and Jon Bryan

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2004-0527
Unlimited Release
Printed February 2004

Architectures & Requirements for Advanced Weapon Controllers

Paul Klarer
Navigation, Pointing & Control

Brian McMurtrey and Jon Bryan
Weapons Controllers Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0501

Abstract

This report describes work done in FY2003 under Advanced and Exploratory Studies funding for Advanced Weapons Controllers. The contemporary requirements and envisioned missions for nuclear weapons are changing from the class of missions originally envisioned during development of the current stockpile. Technology available today in electronics, computing, and software provides capabilities not practical or even possible 20 years ago. This exploratory work looks at how Weapon Electrical Systems can be improved to accommodate new missions and new technologies while maintaining or improving existing standards in nuclear safety and reliability.

Contents

List of figures

Introduction

As part of Advanced and Exploratory Studies (A&ES) efforts funded in FY2003, Electronics Systems Center 2300 has been considering the topic of advanced weapons controllers to perform the surety function and the Arming, Fuzing, and Firing (AF&F) function for the next generation of nuclear weapons. Although no "new" next-generation systems are currently being funded for development, Life Extension Programs (LEP's) and feasibility studies for systems with extended or advanced capabilities not currently available in the stockpile are underway (B61 Phase 6.1 and Robust Nuclear Earth Penetrator – RNEP Phase 6.2). This A&ES effort directly addresses the perceived "needs" statement below:

> ***The current generation of nuclear weapons is based on 20 year old (or older) technology. They are not getting any younger, and the missions envisioned for them are changing. Both of these factors are driving system engineers to contemplate how they might accommodate new technologies and new mission needs in the future while retaining or improving surety (safety, security, and reliability)***

The goal of this initial A&ES effort was to explore the fundamental issues of subsystem architectures and weapon enablement approaches, with an eye towards identifying configurations with high potential for use in next-generation weapons. An important aspect of this was to identify approaches that would allow current weapon systems to be upgraded with the new architecture so as to allow future LEP's to take advantage of changes in technology, as well as to allow wholly new systems (if/when they are developed) to be easily modified or upgraded throughout their lifetimes. As a way of leveraging the A&ES effort in support of ongoing LEP's and feasibility studies, this effort was primarily limited in scope to addressing architectures in terms of the known requirements imposed by that ongoing work. We are working with the Robust Nuclear Earth Penetrator (RNEP) program, which is currently in the Phase 6.2 feasibility assessment stage. Regardless of any specific program's currently perceived needs, the team also tried to keep a forward-looking view with regard to weapon systems so that some anticipation of as-yet-unknown future requirements could be incorporated as well.

Requirements

The Robust Nuclear Earth Penetrator (RNEP) Phase 6.2 feasibility study provided a fairly specific scenario that although currently only notional, acted as a direction for this A&ES effort. The RNEP mission scenario illustrated in Figure 1 shows how the system would be deployed. The most obvious new or different requirements that can be inferred from Figure 1 include the trajectory environment, the use of a guidance package, the impact loads, and the need for a post-impact Detonate/Destruct logic function.

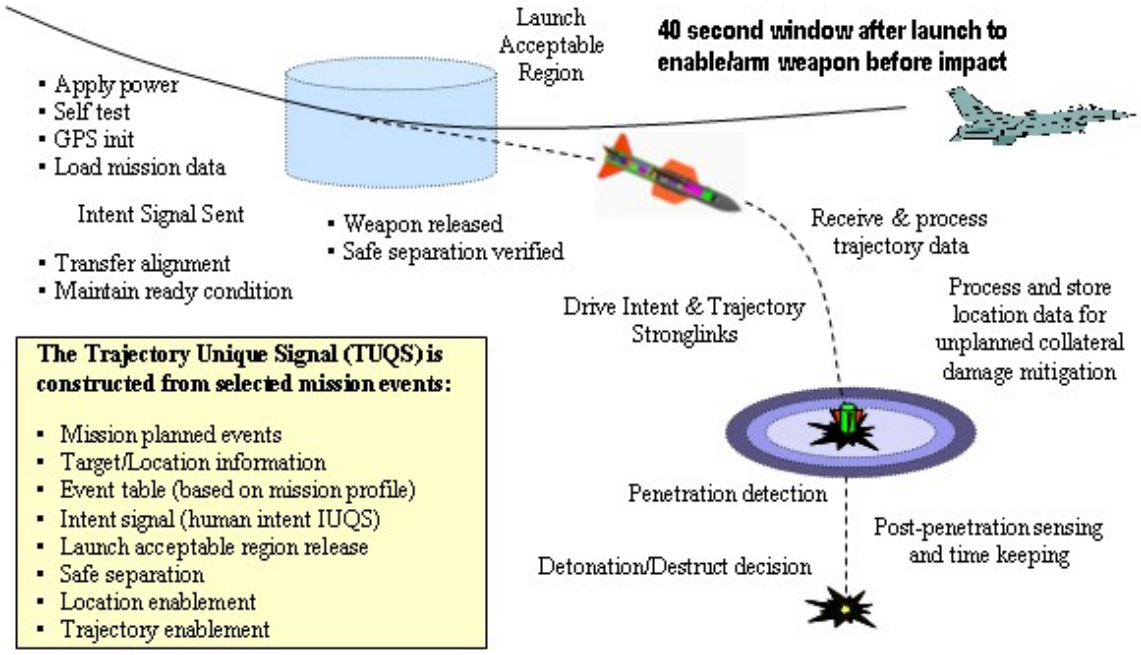

Figure 1 RNEP Deployment

The requirements inferred above indicate that the two current RNEP candidate baseline systems, namely the B83 and B61, will require some new capabilities and that implies the potential replacement and/or redesign of portions of the Weapon Electrical System (WES).

Weapon System Design Issues

The following issues become apparent when considering WES design/redesign tradeoffs and how any new/modified weapon system must still satisfy safety, security, and reliability requirements. Again note that although RNEP played a role in focusing the discussion, it should not be assumed that the following list is all-inclusive beyond the RNEP scenario's requirements.

- Component Redesign vs. Reuse: (which components can and will be changed to use an internal weapons bus vs. which components will be retained from existing system design).
    - Specific existing components affected include:
        - Preflight Controller
        - Stronglinks
        - Firing Set
        - Inter-Connect Unit (ICU)
        - Programmer/Sequencer
        - Trajectory Sensing Signal Generator (TSSG)
    - Potential new components include
        - Inertial Measurment Unit
        - Global Positioning System Receiver

- Bomb Damage Indicator
- Active Tail-Kit (Navigation, Guidance & Control)
- Dual-bus Interface
- Shock-Hardened Controller

Although not addressed in FY03, the issues outlined below will be addressed in follow-on A&ES work tentatively planned for FY04 and beyond. The issues that have yet to be addressed in any detail but appear to be crucial to resolve early in any new WES component design efforts include the following:

- Combining ICU/Programmer/TSSG functionality into a single unit
  - Security issues, if any
  - Electrical isolation (do stronglink signals and firing signals need to be isolated into separate components?)
  - Operational reliability (does this imply redundancy is needed?)
- Hardened Controller
  - How to receive communication when other components may be destroyed by severe but expected environment?
  - Surety issues
  - Mechanical survivability
- Implementing a completely new approach to weapon surety

Component Redesign vs. Reuse

Integrating new technologies and a new system architecture into an existing design is considerably more challenging than starting with a "clean slate", primarily because the customer wants to minimize reengineering costs and sees reusing existing components as a way to achieve that. It should be noted however, that reusing existing system components imposes constraints on the designer that may not exist at all in a new design and may in fact require more effort to accommodate than simply starting from scratch.

As illustrated in Figure 2, the notional reuse of existing B83 or B61 components in an RNEP system does not eliminate the need to reengineer some components in order to provide all functionality RNEP requires. Furthermore, keeping the existing point-to-point system architecture makes further enhancements or modifications to this system highly problematic. Adding new functionality (e.g., an optical seeker/sensor in the nose section) to the system illustrated in Figure 2 is not a straightforward matter and would likely require additional changes to components beyond simply adding the new device or subsystem. One of the RNEP top-level requirements is that the system must be compatible with military carrier aircraft that provide only an all-digital "System 2" interface. This begs the question of whether maintaining the older analog "System 1" internal architecture makes sense from either an engineering perspective or an economic one.

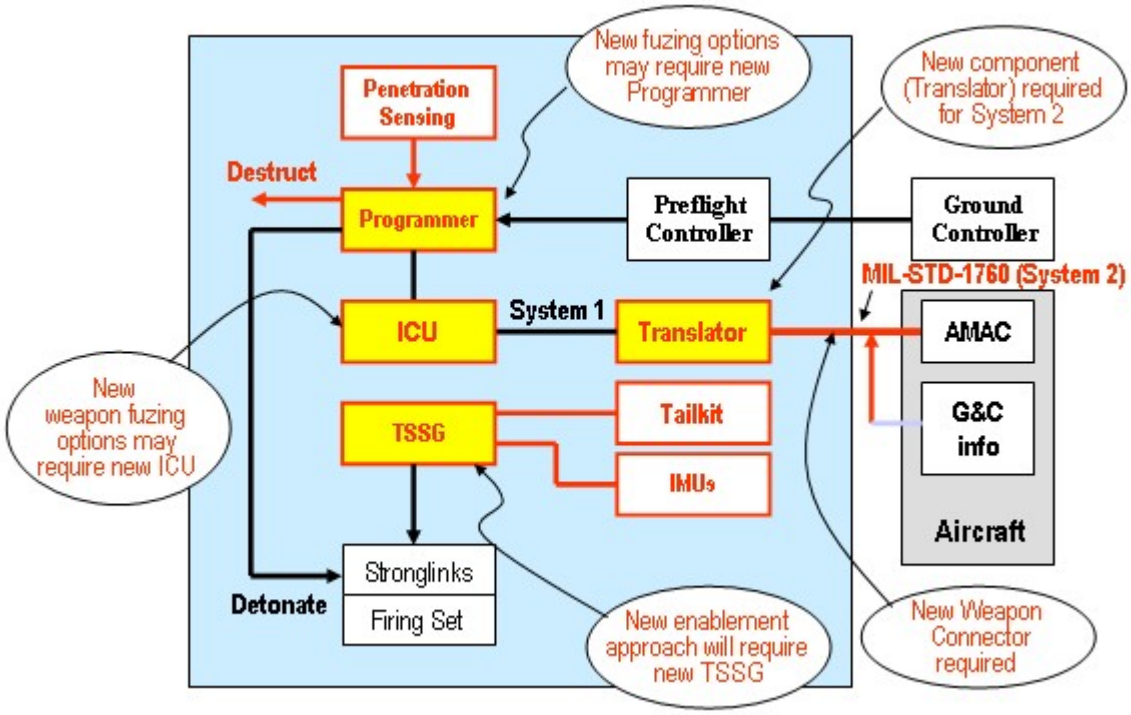

Figure 2 Reuse of Existing Components (yellow items require modification/replacement)

In order to achieve operational performance objectives with regard to pinpoint targeting, RNEP will likely require some active Navigation, Guidance and Control (NG&C) element onboard that can modify the weapon's trajectory in the terminal phase. Thus the need for a "tailkit" (the NG&C package) and potentially one or more additional Inertial Measurement Units (IMU's) as illustrated in Figure 2. The additional functionality requirements that drive the system designer to add new system components like NG&C or IMU's tend to make some level of redesign of the existing B83 or B61 WES inevitable. Reuse of some existing components in that context will result in a hybrid weapon system with older technologies grafted into a more modern and flexible system architecture, with a vision of future upgrades being facilitated by a system architecture that inherently provides for modularity.

Architecture Options

The options available to implement an Advanced Weapon Electrical System (AWES) architecture can be decomposed into three basic categories; discrete point-to-point, serial data-bus, and hybrid. The existing systems are point-to-point, discrete systems that are custom designed for one purpose only. These are simplest to implement but have virtually no flexibility to be modified or enhanced over the lifetime of the system. An alternative is a serial data-bus or -backbone configuration that relies on a network to communicate information between components connected to the backbone as illustrated in Figure 3 in notional form. Serial data-bus architectures are somewhat more complex to implement than discrete point-to-point systems primarily due to data communications and throughput implementation issues, yet they provide considerable flexibility due to the modular nature of such systems. Familiar examples of serial data-bus architectures

include (among others) Universal Serial Bus (USB), Controller Area Network (CAN), Ethernet, FireWire, and the MIL-STD-1553 military aircraft avionics bus. Data is communicated between components using multiple-byte digital messages addressed to specific recipient(s) on the bus and transmitted as a formatted byte stream.

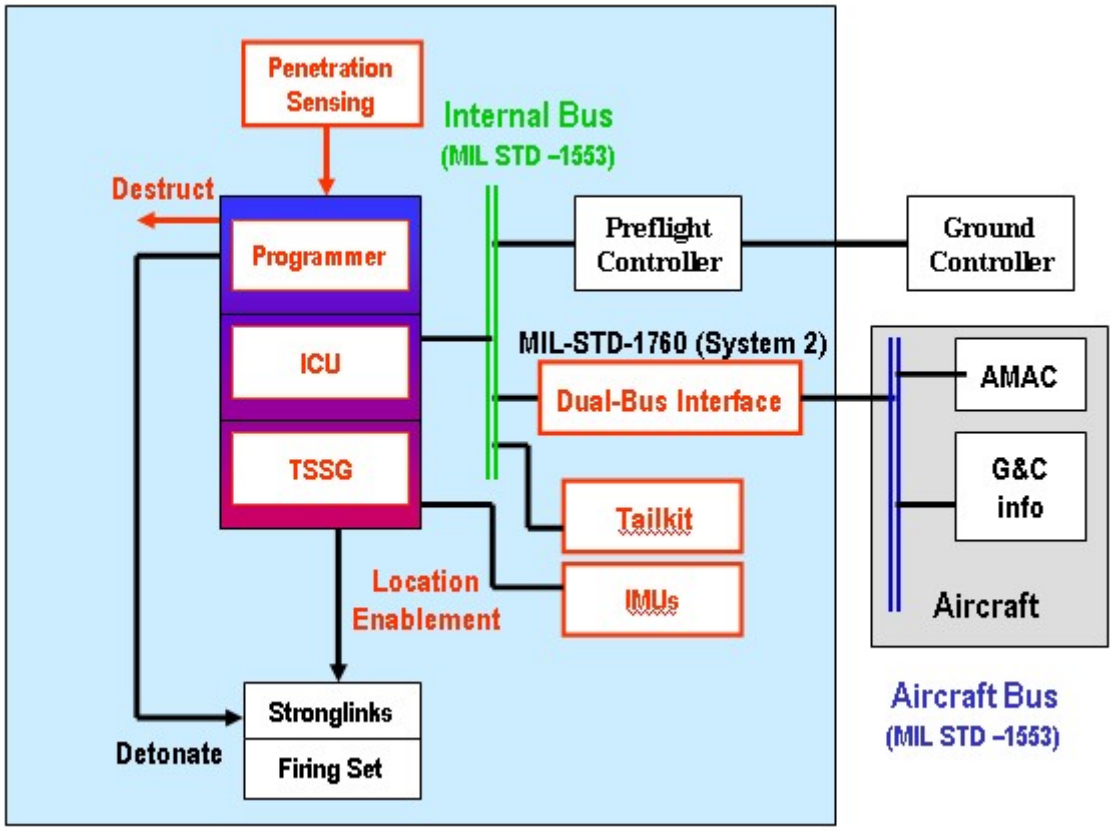

Figure 3 Notional data-bus type architecture

Because System 2 is essentially a data communication protocol that relies on the MIL-STD-1553 communications bus hardware architecture common in all modern military aircraft, it made sense to consider how a new or modified weapon's internal architecture might be configured to best make use of that. Advantages afforded by the MIL-STD-1553 communications data-bus that are relevant to weapon systems include:

- Electrical isolation between nodes
- Manchester data encoding
- Data integrity (parity) checking
- Command/response messaging
- Megabit/sec throughput
- Wide acceptance and use in military aircraft
- High degree of modularity & flexibility

Figure 4 shows a notional advanced WES that employs a modular approach via a MIL-STD-1553 communications bus and is configured for the RNEP mission scenario. The external interface to the carrier aircraft is System 2, and the data communications among

the weapon's internal components is accomplished via a separate MIL-STD-1553 bus local to the weapon. A dual-bus interface allows the two MIL-STD busses (one in the aircraft and one in the weapon) to operate together while the weapon is attached to the aircraft. This is necessary because a MIL-STD-1553 bus must have one and only one (master) Bus Controller unit connected, and all of the other units present on the bus must be configured as (slave) Remote Terminals. The dual-bus interface isolates the two busses when connected together so that they can still communicate in accordance with the MIL-STD-1553 standard, and allows them to remain independent so that they can both continue to operate as required after separation.

Note that the system illustrated in Figure 4 shows one possible configuration, but not the only configuration possible or desirable. The use of data-bus standards other than the MIL-STD-1553 for the internal WES bus is certainly feasible and should be examined in depth in the future. The configuration of hybrid systems that make use of some bus-connected components and some legacy (System 1) components is also a possibility that could lend itself to a phased approach in upgrading existing discrete point-to-point weapon systems to a serial data-bus architecture. An exploratory System 2 hardware demonstration effort was conducted as a part of this A&ES work in FY03.[1] Preliminary results from that work indicate that less than 0.3% of transmitted messages require retransmission due to errors, and that 8-bit microprocessors used in existing WES components (e.g., Intel 8031) were capable of handling the throughput, although switching to a 16-bit (or more) microprocessor would likely result in significantly reduced work-loading of the processor for the communications task.

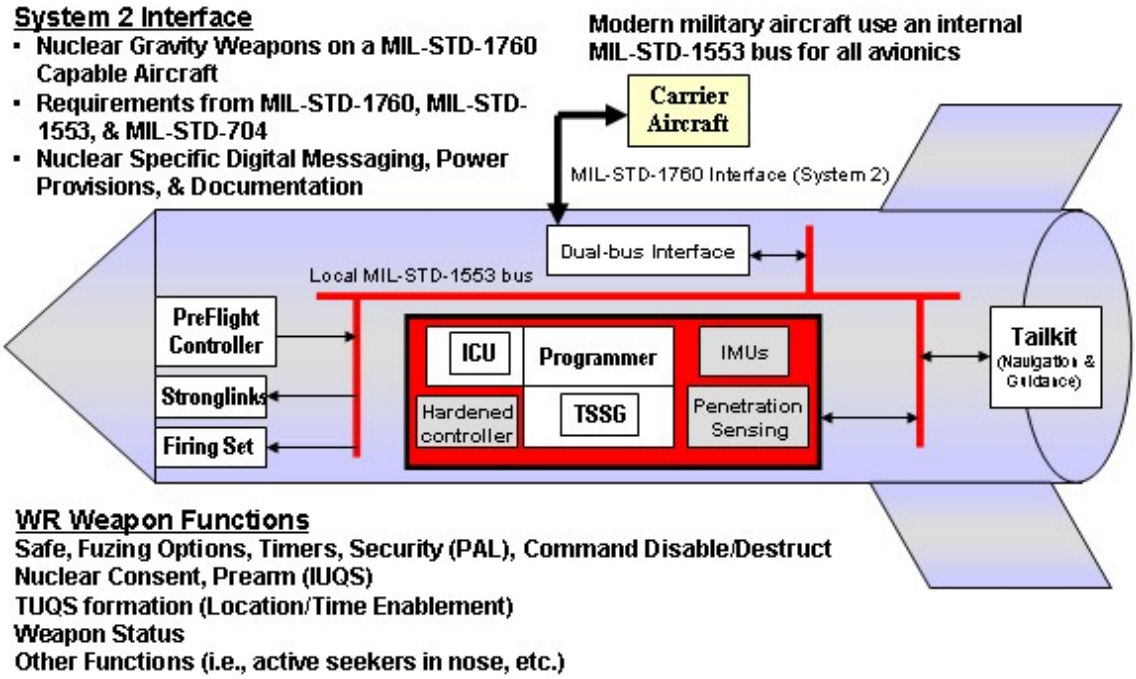

Figure 4 Notional modular WES architecture for RNEP

A major consideration in choosing a particular data-bus standard for implementation is bandwidth. The data-bus must provide sufficient bandwidth to support the "worst-case" communications throughput anticipated for the system. Normal operations for a nuclear weapon as they are currently configured for System 1 require very little bandwidth, since the number of information data "bits" is quite small (less than 1000) and the time available to transmit them is several seconds. A weapon system with additional capabilities (e.g., an active guidance package or a seeker sensor-head) could conceivably require considerable bandwidth, on the order of megabits per second for imaging sensors like Laser Detection and Ranging (LADAR) units. For the RNEP system, the NG&C system will generate position and velocity estimates and will make that data available over the data-bus to the weapon surety controller. Estimating the bandwidth requirement for an NG&C unit is fairly straightforward and proceeds as follows:

1. Estimate data stream configuration
2. Estimate data update rate
3. Calculate the data bit-rate or bandwidth

The data stream should at a minimum include position information in 3 axes (latitude, longitude, elevation); orientation information provides little additional utility and is not required for surety purposes. In order to obtain position resolution of at least 3 meters in latitude and longitude and 1 meter in elevation (over a maximum range of 30,000 meters), the data packets must be 25 bits, 26 bits, and 15 bits long respectively. This is a total of 66 bits of data. Although velocity information is available from the NG&C system, high resolution velocity data is not required for the surety function. If velocity information is required for some reason, it can be calculated from differences in successive positions over a measured time period by the surety controller and so is not required to be transmitted over the data-bus. The data stream will require a certain amount of overhead to accommodate packetization of the data. Assuming a "worst-case" packetization efficiency of 50% then the total data message must be (2*66) or 132 bits long including all data content, header, and trailer information.

The data update rate occurs in two different contexts; internal to the NG&C unit for closed loop control, and external to the NG&C unit via the data bus for weapon surety purposes. The internal rate will be much higher than the external rate, and it is only the external rate that is relevant to the question of data-bus bandwidth. Assuming the surety controller needs to receive 256 successive position estimates to perform the surety function and the weapon is in flight for 20 seconds then the update rate would necessarily be 12.8 Hz. This is not an unreasonable number and assumes a large number of data points and a short flight time to obtain a "worst-case" estimate.

The resultant data throughput estimate for the data-bus is simply the number of bits per message times the number of messages per second, that is: (132 * 12.8) or approximately 1690 bits per second. The bit rate is directly related to the bandwidth in Hz since it typically takes a single bus voltage level "cycle" (rise and fall) to describe a single bit of information. Therefore a bus bandwidth of 1.69 kHz is required to get all of the NG&C data transmitted at the required rate. However, this is not sufficient because data bit-

errors occur and if multiple transmitters are connected to the bus (as they usually are) data message collisions can occur that necessitate re-transmission of some messages. A simple rule of thumb to accommodate bit errors and retransmission requirements is to avoid loading the data bus more than 50% of capacity. This means that the true minimum bandwidth for the NG&C function is (2*1690) or 3.38 kHz, a value well below the 1 MHz capacity of the MIL-STD-1553 bus. Although additional data messages will necessarily be communicated between the weapon surety controller and other WES components, those data rates will be similar to that currently employed in System 1 type weapons and will not significantly impact data-bus bandwidth.

Summary

In response to a perceived need for advancing the capabilities of nuclear weapon controllers to perform the surety and AF&F functions for the next generation of nuclear weapons, Electronics Systems Center 2300 has been conducting activities under A&ES funding. Although specific requirements for particular future weapon systems do not currently exist, requirements for systems currently under study for feasibility (such as RNEP) provide a point of departure for identifying weapon system design issues such as "reuse vs. redesign" of major WES components. Other important issues identified for future exploration include how functionality might be combined into a smaller number of major components to improve reliability, and how special/extreme environmental conditions can be expected to drive component design. A notional architecture has been proposed to provide flexibility and modularity, both seen as being needed to facilitate future weapons systems designs and upgrades over their operational lifetimes. Some limited experimental hardware work has been done that investigates implementation-specific issues regarding the proposed architecture; the details of that work are contained elsewhere but referenced here.

Further work in this area is recommended, including:

- expand on notional architecture, flesh out details
- investigate more powerful computation platforms, including the Sandia Secure Processor (SSP) system currently under development in Org 2100.
- assess bus throughput/bandwidth requirements in greater detail
- assess implications of new architecture on Nuclear Surety issues
- investigate implications of extreme environmental conditions on hardware design
- investigate redundancy vs. reliability issues

References

[1] "Report on System 2 Communication Work: A/E Project", McMurtrey, B., et.al.; Sandia National Laboratories internal report, September 2003

SAND REPORT DISTRIBUTION

MS 0447	(2111)	James D. Mangum (1)
MS 0482	(2131)	Kent D. Meeks (1)
MS 0482	(2131)	Grant J. Bloom (1)
MS 0503	(2330)	David W. Plummer (1)
MS 0537	(2331)	Perry A. Molley (5)
MS 0537	(2331)	Jon R. Bryan (1)
MS 0537	(2331)	Brian J. McMurtrey (1)
MS 0501	(2338)	Paul R. Klarer (2)
MS 0319	(2610)	John R. Fellerhoff (1)
MS 9034	(8221)	Alfredo McDonald (1)
MS 9034	(8221)	Michael E. DeVay (1)
MS 9036	(8222)	Edward B. Talbot (1)
MS 9005	(8240)	Brian K. Damkroger (1)
MS 0899	(9616)	Technical Library (2)
MS 0501	(2334)	Jennifer D. Brechiesen (1)
MS 0835	(2830)	J. Michael McGlaun (1)
MS 9018	(8945-1)	Central Technical Files (1)