National Ignition Facility
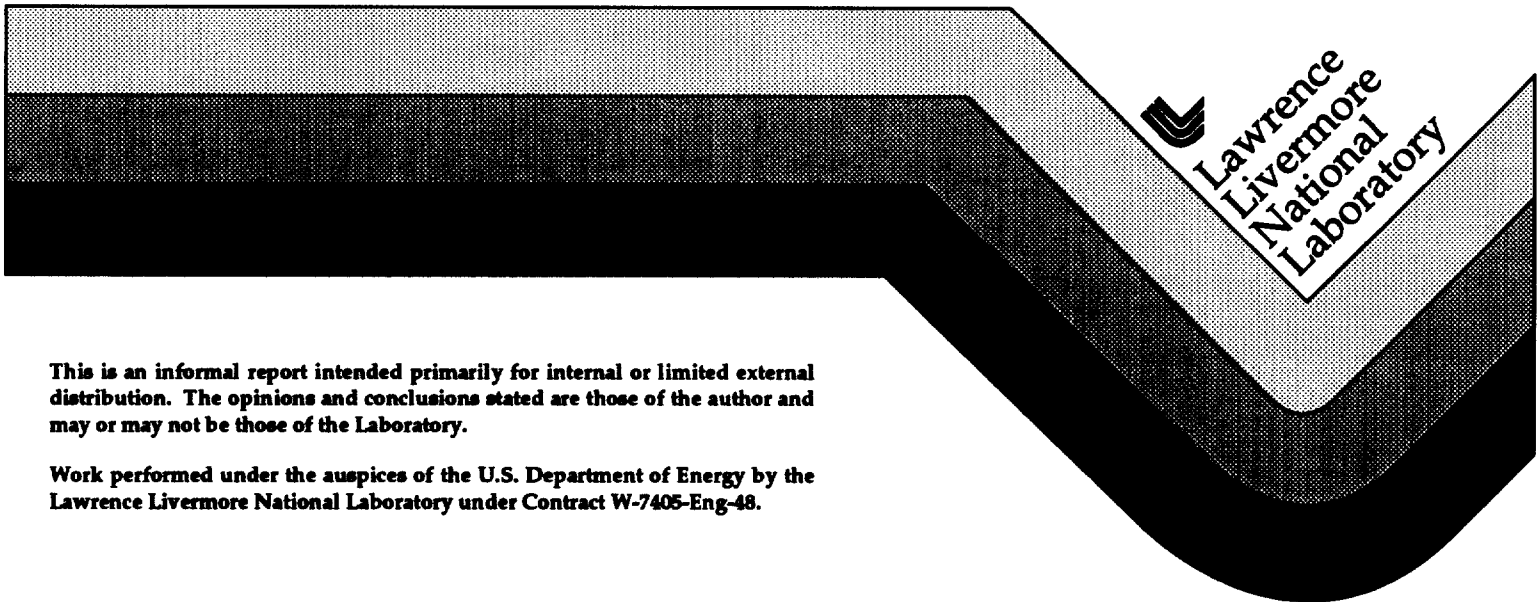# Sub-System Design Requirements
Computer System
SSDR 1.5.1

J. Spann
P. VanArsdall
E. Bliss

September 5, 1996

Lawrence Livermore National Laboratory

National Ignition Facility

Sub-System Design Requirements

Computer System

SSDR 1.5.1

Revision 2
5 September 1996

Prepared by:

J. Spann, Computer System Team Leader

Date

P. VanArsdall, Integrated Computer Controls
Lead Engineer

Date

E. Bliss, System Controls System Engineer

Date

Special Equipment Engineering Approval:

R. Sawicki, NIF Associate Project Engineer

Date

Engineering Review Board Approval:

S. Kumpan, NIF Project Engineer

Approval Date

1

Table of Contents

1.0   Scope
This System Design Requirement document establishes the performance, design, development, and test requirements for the Computer System, WBS 1.5.1 which is part of the NIF Integrated Computer Control System (ICCS). This document responds directly to the requirements detailed in ICCS (WBS 1.5) which is the document directly above.

2.0   Applicable Documents
This section lists DOE orders, codes, and standards which are applicable to the NIF Integrated Computer Control System. The applicable portions of these documents apply. Applicable LLNL standards are being considered contingent upon the decision of final site selection.

2.1   Applicable NIF Project Documents
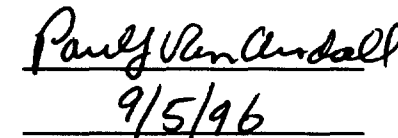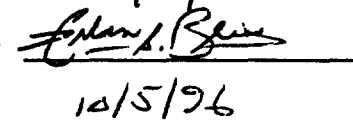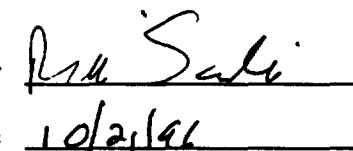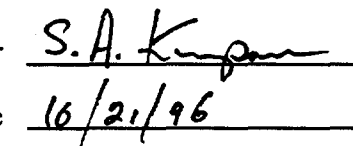National Ignition Facility Functional Requirements and Primary Criteria, Revision 1.4, Mar 1996. (FRPC)

2.2   Applicable US Government Orders and Standards
(flowdown from SDR004=fd, no-flowdown=nfd)

US. Government DOE General Orders:
   DOE 5700.6C—Quality Assurance (fd)

US. Government DOE Orders relating to Safeguards and Security:
   DOE Order 1360.2B, Unclassified Computer Security Program (fd)
   DOE Order 5300.4D, Telecommunications: Protected Distribution Systems (fd)
   DOE Order 5639.6, Classified Computer Security Program (fd)

2.3   Applicable National Consensus Codes and Standards
Safety Standards:
   National Fire Protection Association (NFPA)-70 National Electrical Code (fd)
   ANSI C2-1990, National Electric Safety Code (fd)

Software and Electronic Standards:
Ethernet	IEEE-802.3 Local Area Network for Data Communications
FDDI	Fiber Distributed Data Interface, ANSI Standard X3.139-1987
RS-232C	EIA Serial interface standard
RS-485	EIA Multi-drop serial interface standard
IEEE-488	Standard Digital Interface for Programmable Instrumentation, ANSI/IEEE Std 488.1-1987 and ANSI/IEEE Std 488.2-1987
VMEbus	IEEE-1014
RS-170	EIA Video interface standard
Ada 83	ANSI/MIL-STD-1815A-1983, programming language
Ada 95	International Standard ANSI/ISO/IEC-8652:1995, January 1995
X11	X Window System, Version 11, windows graphics standard, MIT X Consortium
OSF/Motif	Motif graphical user interface, Open Systems Foundation
Postscript	Text and graphics printing language, Adobe Systems Inc.
POSIX	IEEE-1003 portable application programming environment
TCP/IP	Protocol stack for network communications
OSI/ISO	Open Systems Interconnect protocol stack for network communications
OSF/DCE	Distributed Computing Environment, Open Systems Foundation
OSF/DME	Distributed Management Environment, Open Systems Foundation

2.4   Applicable LLNL Standards
LLNL NIF Grounding Plan, L-17346-1

2.5   Supporting Documentation Standards

Instrument Society of America, ISA-S5.1, Instrumentation Symbols and Identification
Instrument Society of America, ISA-S5.2, Binary Logic Diagrams for Process Operations
Instrument Society of America, ISA-S5.3, Graphics Symbols for Distributed Control/Shared Display
Instrumentation, Logic and Computer Systems
Instrument Society of America, ISA-S5.4, Instrument Loop Diagrams
Instrument Society of America, ISA-S5.5, Graphics Symbols for Process Displays
ANSI/IEEE Std 730.1-1989, IEEE Standard for Software Quality Assurance Plans
Software Guidelines Standards, Practices, and Conventions (Final DRAFT), Applications Development
        Department, Lawrence Livermore National Laboratory, August 10, 1992
ANSI/IEEE Std 830-1984, IEEE Guide for Software Requirements Specification
ANSI/IEEE Std 1016-1987, IEEE Recommended Practice for Software Design Descriptions
ANSI/IEEE Std 828-1983, IEEE Standard for Software Configuration Management Plans
ANSI/IEEE Std 982.1-1988, IEEE Standard Dictionary for Measures to Produce Reliable Software
ANSI/IEEE Std 982.2-1988, IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce
        Reliable Software
The Software Productivity Consortium, Ada Quality and Style Guidelines for Professional Programmers
ANSI/IEEE Std 1063-1987, IEEE Standard for Software User Documentation

2.6   References

NIF-LLNL-95-044/L-15958-2, National Ignition Facility Quality Assurance Program Plan, September 1995
NIF-LLNL-94-017/L-15958-5, NIF Ancillary Software Quality Assurance Plan, January 12, 1994

3.0   Requirements and Verification

3.1   System Definition

3.1.1   System Description

The computer system and network architecture, shown in paragraph 3.1.2.2 provides control functions and
graphical user interfaces wherever needed in the facility to meet the dual requirements of centralized controls for
experiments and remote controls for construction and maintenance. The upper-level computer system is shown
attached to the Fiber Distributed Data Interchange (FDDI) high performance network whereas the lower-level
system is shown attached to less expensive local Ethernets. (Choice of actual network hardware are a design
decision and shall be made based on network traffic analysis.) Processors located anywhere on the network can
access any other using standard communication protocols. Computers on the network access data files from a
central operations file server. The server is a dual-host configuration that shares the work load and converts to a
single server (with somewhat reduced performance) in the event of breakdown. A separate software file server
and set of developer workstations segregates software engineering activities from on-line operations until new
updates are released.

Graphical User Interface (GUI) operator controls are implemented with graphics workstations adhering to the X-
Windows and Motif graphics standards. Four consoles are provided, one for each of the major subsystems.
Consoles in the control room offer four display screens and two keyboards with the capability of TV image
display. A two screen console serves the shot director. An auxiliary console supplies extra maintenance and
calibration support for all subsystems.

The lower-level network attaches to several types of FEP. Local control of FEP systems is achieved by displaying
GUI software on X terminals placed in the same equipment racks as the processors.

3.1.2   System Diagrams

3.1.2.1 Layered Controls Architecture

Shot Director Coordination

Subsystem Operator Controls

Integration and Automation

Upper Level Computers

Local Area Network

Lower Level Computers

Front End Processors (FEP)

Embedded Controllers

Safety Interlocks

Sensors   Control Point Layer   Actuators
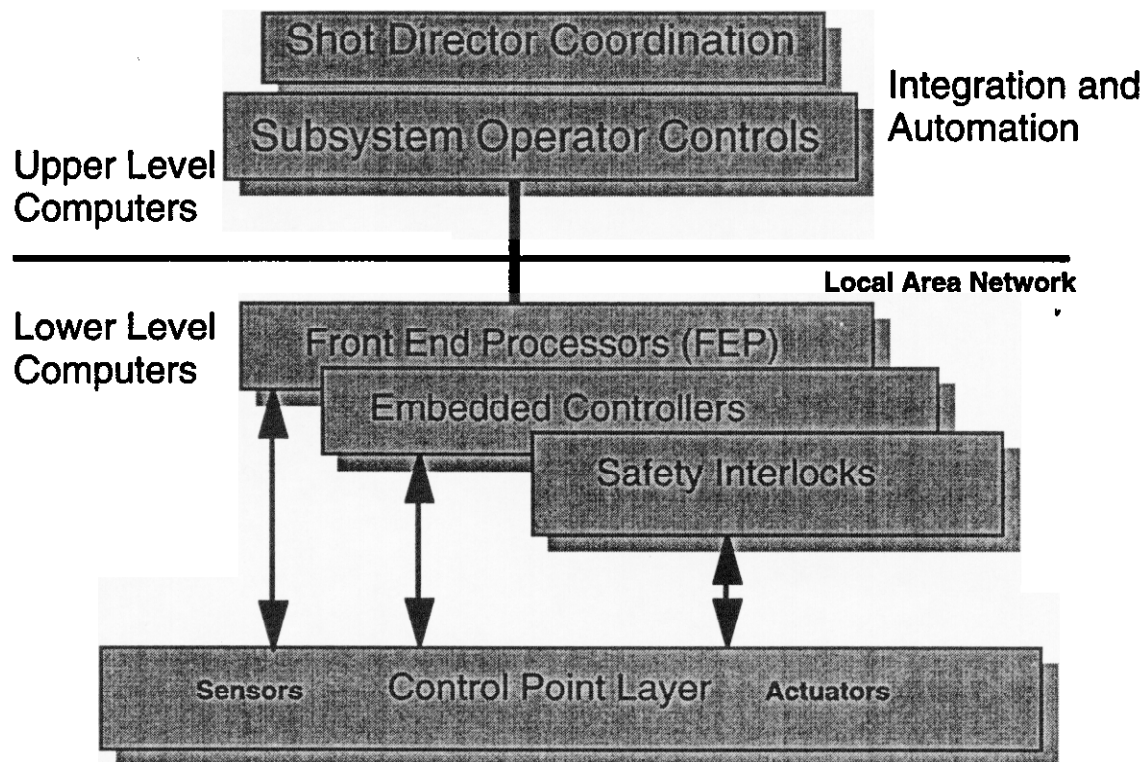
3.1.2.2 Computer System Network
(Figure is conceptual and quantities are subject to change in Title 2 design.)
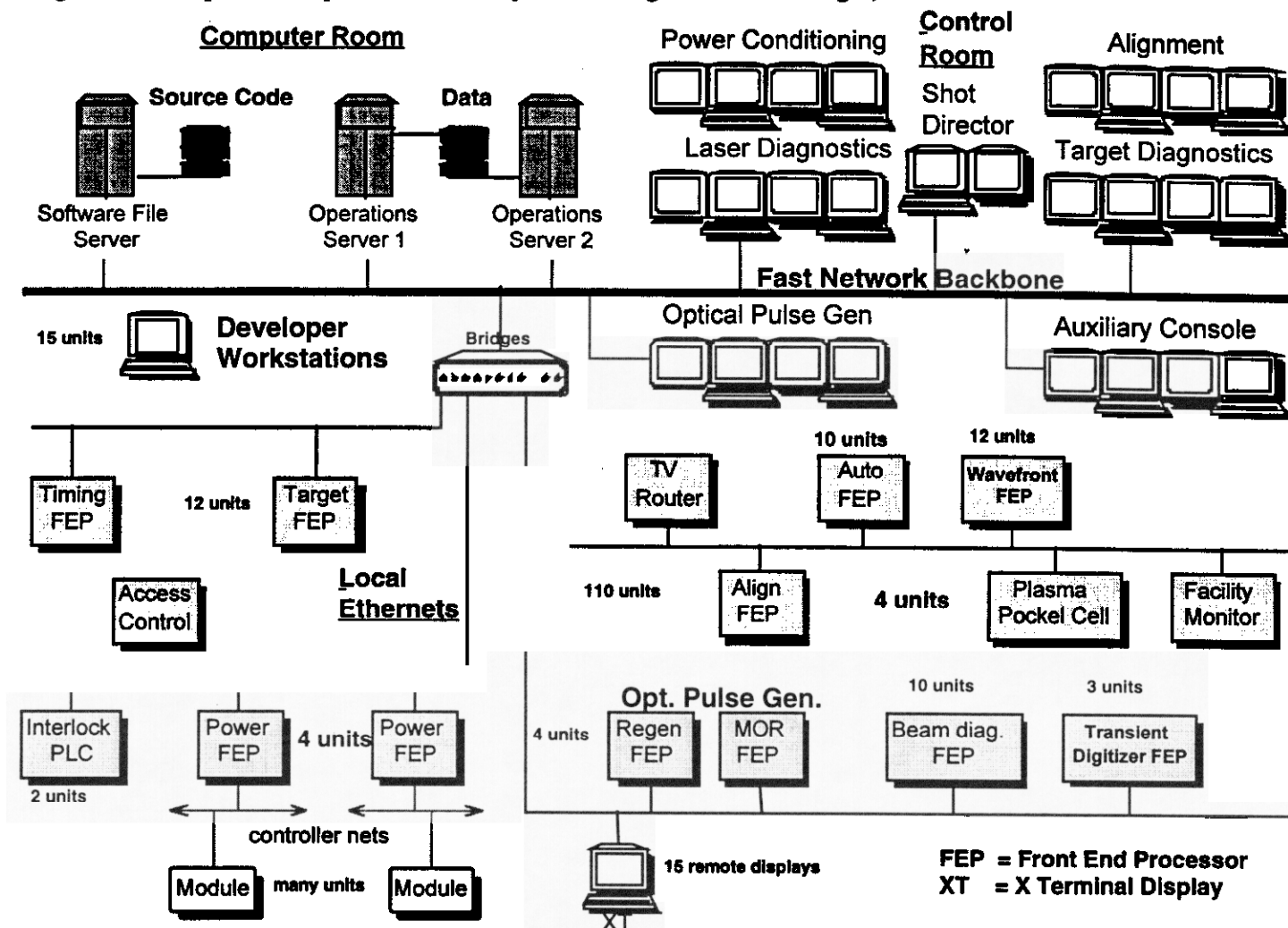
3.1.2.3 Control Room Layout
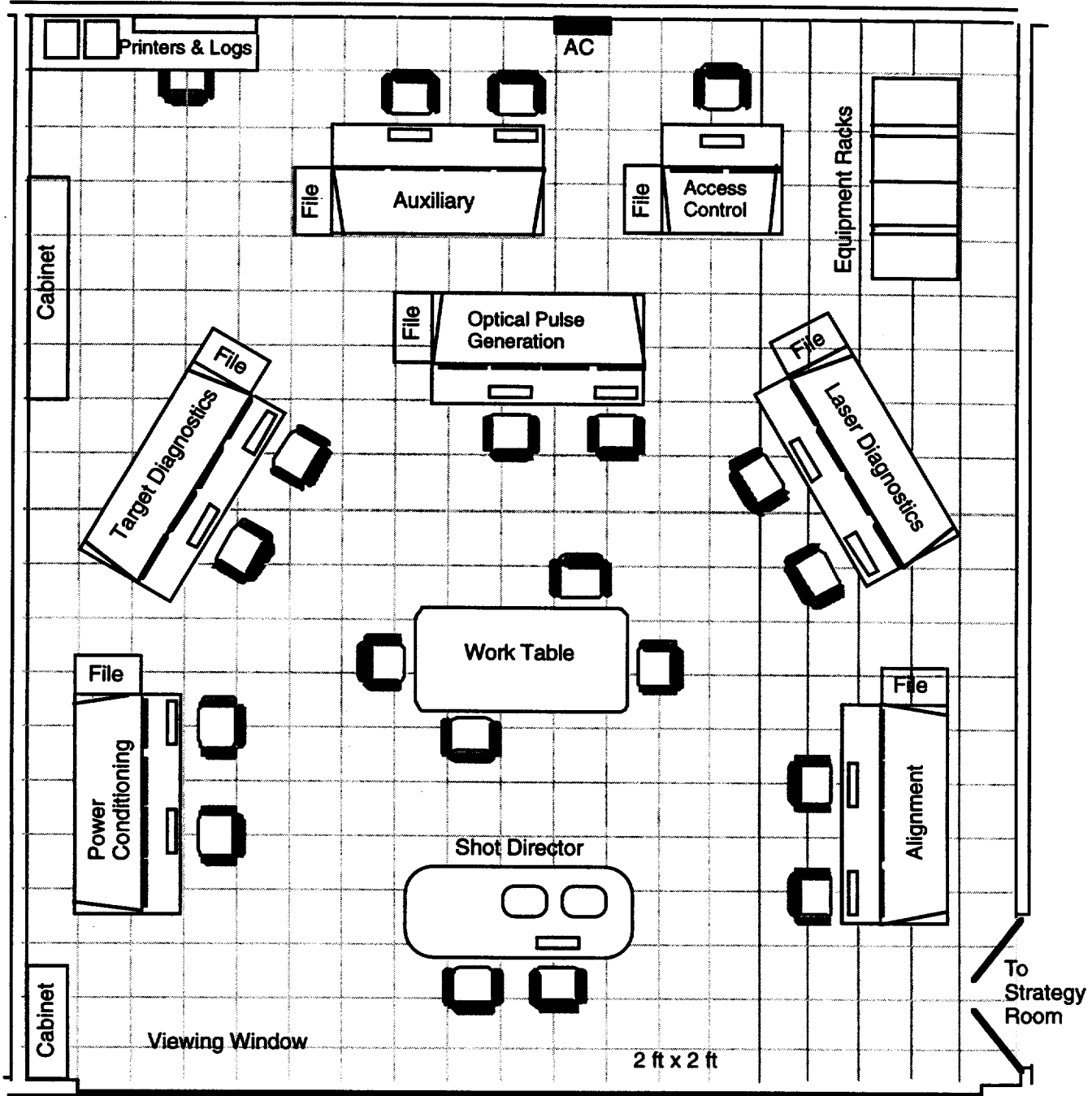
3.1.2.4 Computer Room Layout

Safety Interlock Rack   Network Equ. Racks

Test FEP

Test Console

Dev FS

FS A

FS B

System Operator

Manuals

Manuals

Cabinet

Cabinet

Cabinet

Cabinet

0   1   4   8   12   16

Scale -- Feet
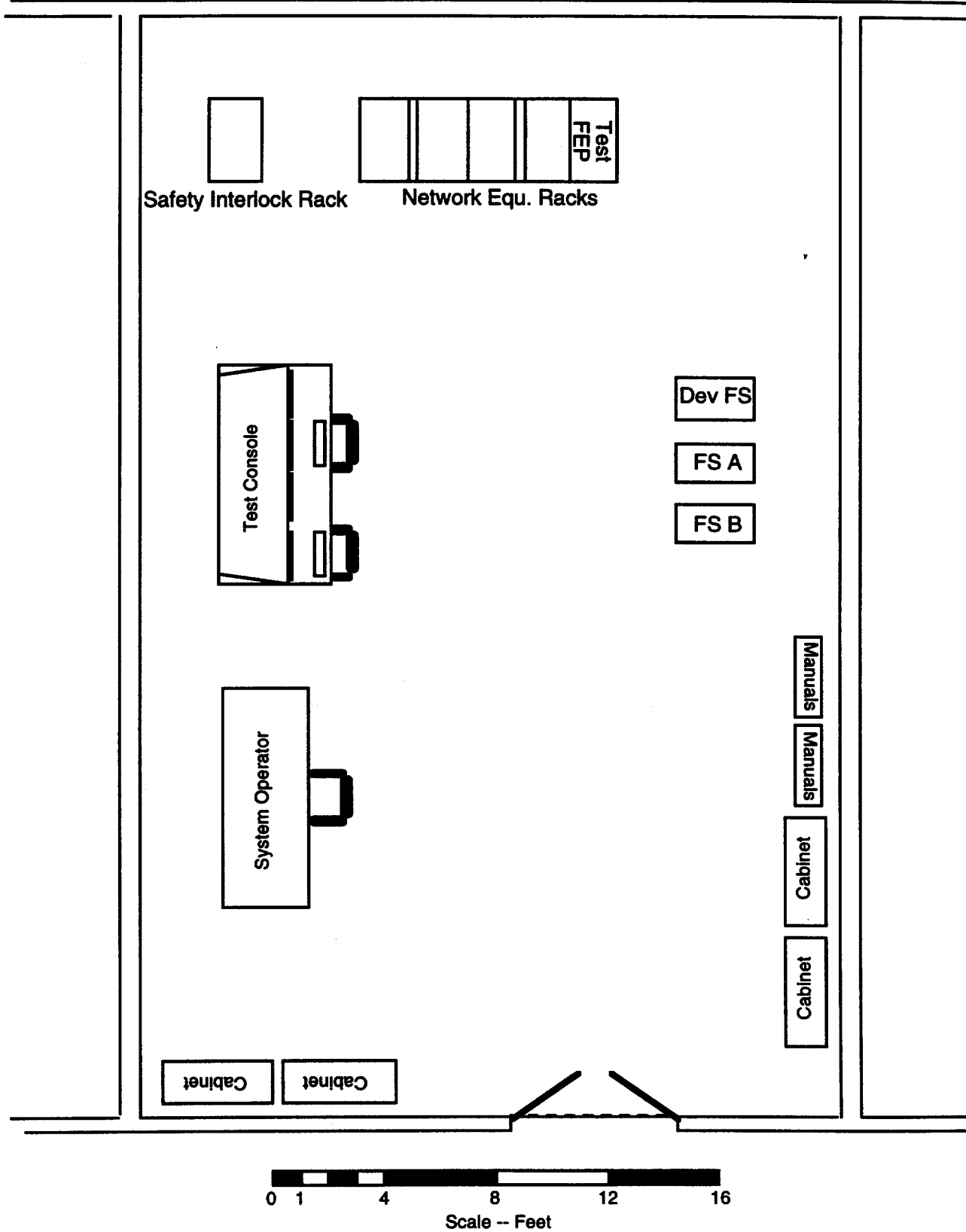
3.1.2.5 Operator Console Layout

Video Printers
Access Control
Telephone
Video Switch Box
Crash Buttons
Key Enable Switches
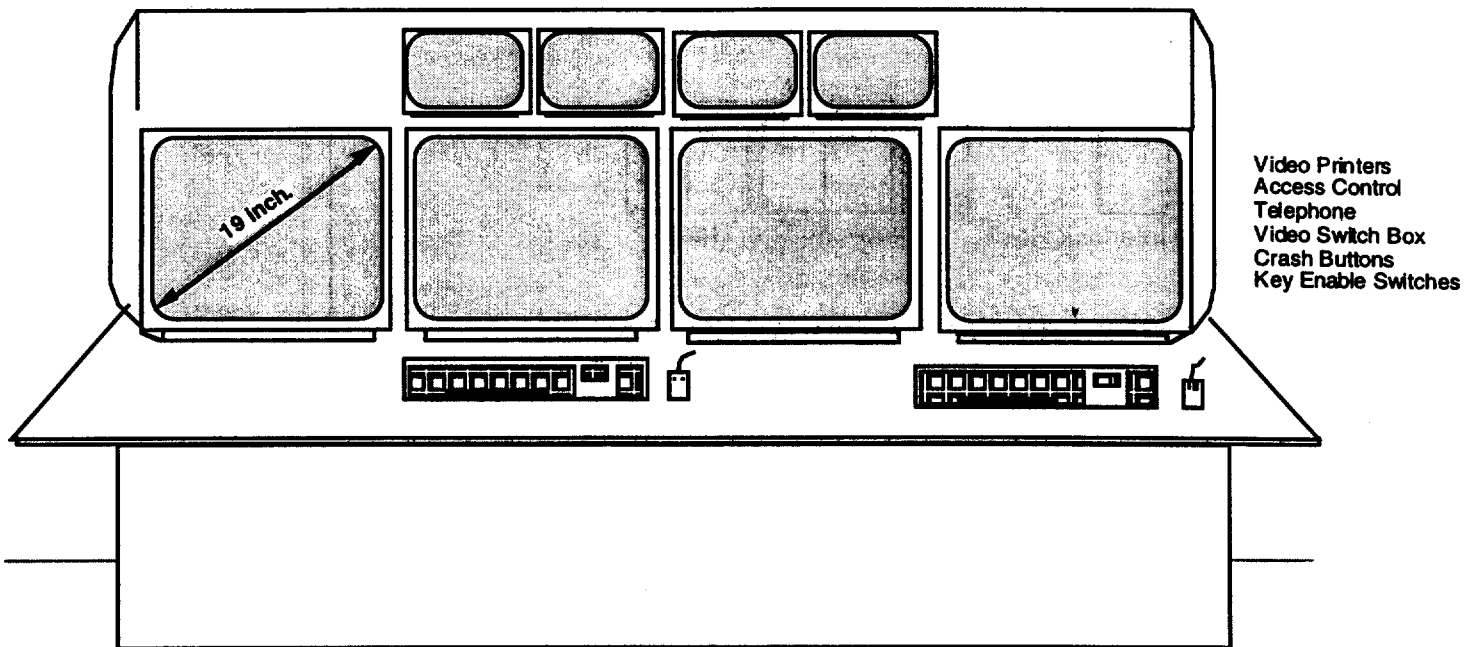
3.1.3   System Interfaces

The ICCS Computer System has interfaces to the following WBS systems:

WBS 1.5.2	Supervisory Software (computer hardware)
WBS 1.5.3	Integrated Timing System (network)
WBS 1.5.4.1	Integrated Safety System(network)
WBS 1.5.5	Automatic Alignment (network)
WBS 1.5.6.1	Video Distribution (network)
WBS 1.5.6.3	Environmental Monitor (network)
WBS 1.8.3.11	Target Diagnostics Control Room(network)
WBS 1.7.3	Wavefront Control (network)
WBS 1.7.2	Beam Diagnostics (network)
WBS 1.7.1	Alignment Systems (network)
WBS 1.3.4	Power Conditioning (network)
WBS 1.3.3	Pockels Cell System (network)
WBS 1.3.1	OPG (network)
WBS 1.3.1	OPG Modulator (network)
WBS 1.3.1.1	OPG in MOR (network)
WBS 1.3.1.5	OPG/Preamp (network)

3.1.4   Major Subsystems

Consists of WBS 1.5.1.1 (Software Engineering Computer) system used for software development, and WBS 1.5.1.2 (Operations Computer System).

3.2.00   Functional Requirements
The Computer System shall provide:
- upper-level computers: file servers, disk storage, workstations
- software development environment to include: .
  - operating system
  - languages and software engineering tools
  - graphical user interface (GUI) design and other tools
  - database tools
  - software configuration management
- software archival storage
- provide graphical operator consoles for rapid assessment of system status and input of controlcommands
- temporary shot data storage
- control room operator consoles and remote stations located near laser- and target-area subsystems
- local area network to connect all upper- and lower-level computers and FEPs, distribution system, filtering bridges
- provide computational capability for routine data reduction and quick-look analysis

3.2.01   Console Ergonomics
Control and monitoring consoles located in the control room shall be ergonomically designed to maximize the efficiency of the operators and minimize strain associated with computer workstations.

3.2.02   Computer System, Operating System
The Computer System shall provide UNIX as the standard operating system platform for Supervisory and Front End Processor software.

3.2.03   Computer Networks

3.2.03.1 Facility Wide Computer Network
A facility-wide data network shall be provided as the backbone for data communications in NIF. Connecting to this backbone system are several or local area networks. Subsystems with related control and data dependence shall be closely coupled on separately bridged and isolated segments to achieve the desired performance and information transfer rates.

The Computer System shall provide a capacity planning analysis during Title 1, to plan and determine the network configuration.

3.2.03.2 Computer Network, Safety Systems
No Safety System related controls shall be operated over the facility wide computer network. Safety related systems shall operate over a network dedicated to safety related functions.

3.2.04   Optical Communications Safety
Where the Computer System uses lasers for optical communications, it shall conform to the applicable eye-hazard safety requirements to mitigate the possibility of eye exposure to an uncapped laser diode or unterminated active fiber source. Applicable standards include ANSI Z-136.1 (1993) and ANSI Z-136.2 (1988).

3.2.05   Computer System and Network Reliability
The computer system, with its integrated data communication network, shall meet the reliability standards for industrial grade control systems. Redundancy in the control system is not considered essential to achieve adequate reliability. Main computer system failures shall be repaired by the computer equipment vendor or equivalent repair service. These factors shall be controlled by the RAM allocation in paragraph 3.2.28 of this SSDR.

3.2.06   GUI Support
The Graphical User Interface (GUI) shall support a mouse or trackball input device and shall include a color and black/white hardcopy capability.

3.2.07 Network Performance, Average Latency
Computer network performance shall provide a two-way (round-trip) average response time of less than 50 milliseconds.

3.2.08 Network Performance, Maximum Response Time
Computer network performance should provide a two-way (round-trip) maximum response time of less than 500 milliseconds under maximum network loading.

3.2.09 Network Performance, Sustained Data Rate
The computer network shall be capable of sustained throughput of greater than 100 Kbytes per second to any single end point. This is to ensure good overall network throughput. The use of subnets, filtering bridges and/or switches is suggested to maintain these rates.

3.2.10 Ethernet Loading
Where Shared Ethernet is utilized in the computer network, the Ethernet average load shall be no greater than 15% of maximum over a shot cycle.

3.2.11 GUI Computing Capacity, Interactive Device Update Performance
The GUI (Graphical User Interface) shall support an average minimum of 10 status updates per second for one GUI window per operator display location.

3.2.12 GUI Computing Capacity, Alarm and Exception Report Performance
ICCS shall present an alarm and report update to the console operator in less than one second when used in an event driven mode. These alarms and reports shall be logged.

3.2.13 GUI Computing Capacity, Broad View Update Performance
When the operator console is being used to display status of the control system, typically acquired in a polling mode, the update response shall be less than 10 seconds. This response time is deemed to be a reasonable compromise between timely screen updates and excessive network traffic.

3.2.14 Configuration
There shall be two distinct computer systems, one for software development and one for operations. All software development shall be done on the development system. The only exception to this rule is development and testing of final operations scripts and system interaction testing shall be done on the operational computers but in a manner to not interfere with shot operations.

Installation of new software products shall follow a Configuration Management Plan and be coordinated with the operations staff.

3.2.15 Shot Data Disk Storage Capacity
On-line disk storage capacity shall be sufficient to store two weeks of shot data. The two week capacity provides a reasonable amount for on-line use (comparisons, setups, short term trends). This two week storage shall be rolled out to an archival storage facility or media on a weekly basis. This allows reasonable backup overlaps. One shot is expected to produce 60 megabytes of data.

3.2.16 Shot Data On-line and Archived
Two weeks after a shot, most experiment data will be rolled off to an archival storage media (where data integrity is guaranteed) and deleted from the laser computer system disks. However, laser performance and configuration data will be permanently kept on-line (in disk or other rapid access media) to allow quick performance comparisons of previously used laser configurations. Estimated configuration data quantity is 2.5 megabytes per shot.

3.2.18 Control Room Console Configuration
The main control room console configuration shall consist of 5 main consoles: Alignment, Laser Diagnostics, Target Diagnostics, Power Conditioning, Optical Pulse Generation, one shot director console, an Access Control Console, and one auxiliary console. There also shall be a remote console in the Classified Control Room.

This accommodates a total of 10 operators plus a shot director with the Auxiliary Console as a spare.

3.2.19 Console Graphics Standard
The console graphics standard shall be "X11-R5" or later.

3.2.20 ˙ Console System Flexibility
Any console subsystem shall be capable of displaying and operating any control subsystem. In a distributed computing environment, flexible operations is required.

3.2.21 Network Backbone
A low latency, high data rate network shall make up the digital communication system backbone. The data rate of this backbone shall be at least 100 megabits/sec. Present candidates are FDDI, ATM and 100Mbit/sec Ethernet. Other candidates are also possible. A survey and technical evaluation shall be made during Title 1 to determine this choice. Regardless of the choice, the physical cabling shall be configured in a hub-and-spoke (radial) fashion, to allow easier upgrades at a later date.

3.2.22 LAN Subnets (Ethernet)
The Computer System shall provide LAN subnets using 10 megabit/sec Ethernet, if latency and throughput is adequate. That is, FEP designers can expect to connect to a 10 megabit/sec Ethernet as the lowest common denominator network interface.

3.2.23 Lower-Level Computer Attachment to LAN
All computer equipment shall utilize network hardware and protocols compatible with the NIF network and bandwidth appropriate to the equipment requirements.

3.2.24 Ethernet Protocol
At a minimum, the network shall support TCP/IP as the network transport protocol.

3.2.25 Graphics Software
The graphic standard software shall be X-windows, X-toolkit and Motif. This means that the low-level (non-supervisory) systems shall use the same standard as the console system.

3.2.26 Computer Availability
Mean time to repair (MTTR) for an individual computer shall be less than 4 hours, unless further restricted by RAM analysis and allocation. This time allows the use of standard, cost-effective, maintenance contracts.

3.2.27 Computer System QA Level Requirements
The Computer System shall adhere to the following Quality Level specifications:
  Reference for QA Level is the NIF QA Plan as stated in paragraph 2.6 of this document.

WBS 1.5.1.1 Software Engineering Computer System   Q-Level 3
WBS 1.5.1.2 Operations Computer System   Q-Level 3

3.2.28 Computer Availability, cold start
Restarting all computers from a power-down condition shall take less than 30 minutes.
This allows quick recovery from a power failure.

3.2.29   Computer System and Network, Lifetime, Replaceability and RAM

3.2.29.1 Computer System and Network, Lifetime
Lifetime: The Computer System shall operate for 30 years.

3.2.29.2 Computer System and Network, Replaceability
Replaceability: Any portion of the Computer System which cannot reasonably be designed for 30 year lifetime shall be designed to be replaced or repaired at reasonable cost in a timely manner consistent with the overall availability of the System.

3.2.29.3 Computer System and Network, Reliability
The Computer System shall have an overall reliability of 99.94%. Reliability is defined as the probability of meeting the minimum requirements of the experiment per no-yield shot.

3.2.29.4 Computer System and Network, Availability
The Computer System shall have a shot availability of at least 99.62%. The ITS is unavailable when it is undergoing unplanned maintenance. Unplanned maintenance includes failure detection and active repair as well as logistic and administrative downtimes.

3.2.29.5 Computer System and Network, Maintainability
The Computer System shall have a scheduled maintenance plan that fits within an overall annual plant goal of 69 days. The unplanned maintenance goal is 1.0 days per year. Opportunistic maintenance activities are performed between shots and during other system downtimes.

3.2.30   Environmental Requirements/EMI

3.2.30.1 Environmental Requirements, Temperature and Humidity
The Computer System components shall be capable of operating in a standard commercial temperature and humidity of 5C to 40C (41 to 104F) and 20% to 80 % RH non-condensing when installed in their appropriate enclosures.

3.2.30.2 Environmental Requirements, Plenum Approved/CL2 Cables
All Computer System cabling installed in air plenums shall use plenum approved cabling. Otherwise controls cabling shall conform to CL2 specifications.

3.2.30.3 Environmental Requirements, EMI Fields
All Computer System electronic equipment shall be designed or purchased to tolerate, where warranted, an operating environment of 50 V/m external electrical field and 0.1 A/m external magnetic field without adverse effects. (ref ANSI C95.1-1991)

3.2.30.4 Environmental Requirements, Ionizing Radiation
Ionizing Radiation effects are an issue only inside the target room. Inside the target room careful consideration shall be given to the radiation and EMI effects as described in "Radiation and EMI Effects in the NIF Environment", UCRL-ID-118202.

3.2.31   Human Factors
The Computer System shall be designed in an ergonometric fashion to ensure that human reliability during operation and maintenance is sustained at a level consistent with meeting overall availability and reliability objectives. Consistency in displays, warnings, and human interfaces should be maintained throughout the Computer System and, if possible, throughout the NIF facility (i.e. GUI displays, access ports, tooling)

14

3.2.32   Recovery From Abnormal Event
The time required for the Computer System to recover from any abnormal event shall be less than the maximum times cited below, as a function of the expected yearly frequency of occurrence of the event.

Expected Frequency of Occurrence Per Year, F	Maximum Recovery Time
$F \geq 1$	24 hours
$1 > F > 1e-2$	1 week
$1e-2 > F \geq 5e-4$	3 months

Probabilities listed in DOE-STD-1020-94 shall be used for natural phenomena.

For frequent events, the maximum allowed recovery time may be restricted by availability requirements to be less than that shown in the table above.

3.2.33   Documentation and Records
The Computer System shall provide sufficient documentation to comply with the NIF Quality Assurance Plan, and DOE Order 5700.6C, Quality Assurance, Criterion-4 Documents and Records, which states: "Documents shall be prepared, reviewed, approved, issued, used and revised to proscribe processes, specify requirements or establish design. Records shall be specified, prepared, reviewed approved and maintained."

Examples of documents that should be controlled include drawings, data files, calculations, specifications, computer codes, purchase orders, vendor supplied documents, procedures, work records and data sheets and test records. Revisions should be reviewed by the organizations that originally prepared and approved the documents. Controlled documents should be distributed to those doing the work.

3.2.34   Computer Security
The Computer System shall provide and operate under a LLNL/DOE approved unclassified computer security plan.

3.4   Logistics

3.4.1   Maintenance
As a part of the design/construction project, the Computer System shall provide all equipment required to inspect, service, and maintain all subsystems within the Computer System to meet the maintainability and availability requirements. Maintenance equipment shall include all handling fixtures, lifting equipment, and other special tools not otherwise available within the NIF, that are necessary to perform any planned (scheduled or unscheduled) maintenance activity.

3.4.2   Spares
As a part of the design/construction project, the Computer System shall provide an initial compliment of spare parts as required to activate the system.

6.0   Revision Record

Rev Letter	Rev Date	Change by	Description
A	12Mar96	Severyn	Convert to FileMaker, update.
A	30May96	Severyn	Post Mid Title-1 update.
2	06Aug96	Severyn	para 3.2.34,Add Computer Security. para 3.4.1, fix typo in 3.4.1 (Computer System was called Timing System). para 3.2.27, updated Q-levels. para 2.6, new ver QA reference.
2	20Aug96	Severyn	para 2.2, was empty, updated to DOE orders, flowdown from SDR004. para 2.3, Added ref to NFPA/NEC (flowdown from SDR4). para 2.4, was empty, added ref to NIF Grounding Plan (SDR4). para 2.6, Deleted ref to Functional Requirements because para 2.1 ref to FRPC is sufficient.
2	23Aug96	Christensen/ Clasen	Convert to Word 6.0.1
2	27Aug96	Severyn	Scale figures, update header, call this version 2 to match Sherpa. Minor indentations fixed (no text change).
2	05Sep96	Severyn	para 3.1.2.2 added "(Figure is conceptual and quantities are subject to change in Title 2 design.) per PVA.

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551