Table of Contents

11.1 Project X Network Overview

The Network shall be designed to support four distinct networks including separate networks for the commissioning and operation of the accelerator. The design should consist of a Controls network, DMZ network, Development network and General network. The design shall supply secure network access for specific individuals via authenticated gateways in the DMZ network to the Controls network. The Development network shall allow for testing an implementation of new devices, architecture, etc without interfering with either the Controls or site network. The General network shall accommodate desktops and laptops with authentication and authorization as prescribed by site policy. Each of these networks shall allow for necessary bandwidth, network protocols, VLANs and subnets, secure authentication and authorization, ACLs, firewalls, redundancy, cable plant, QoS, and future technology changes.

No.	Requirement	Source	Priority
CXR-N1-010	The Network shall provide and support a separate dedicated Controls network for accelerator controls	D. Stenman 1-2008	Critical
CXR-N1-020	The Network shall provide a DMZ network for authenticated gateway access to Controls Network	D. Stenman 1-2008	Expected
CXR-N1-030	The Network shall provide a Development network that isolates development activities but allows access to site and internet services, subject to network policies	D. Stenman 1-2008	Expected
CXR-N1-040	The Network shall support a General network for desktop, laptop and domain services	D. Stenman 1-2008	Expected

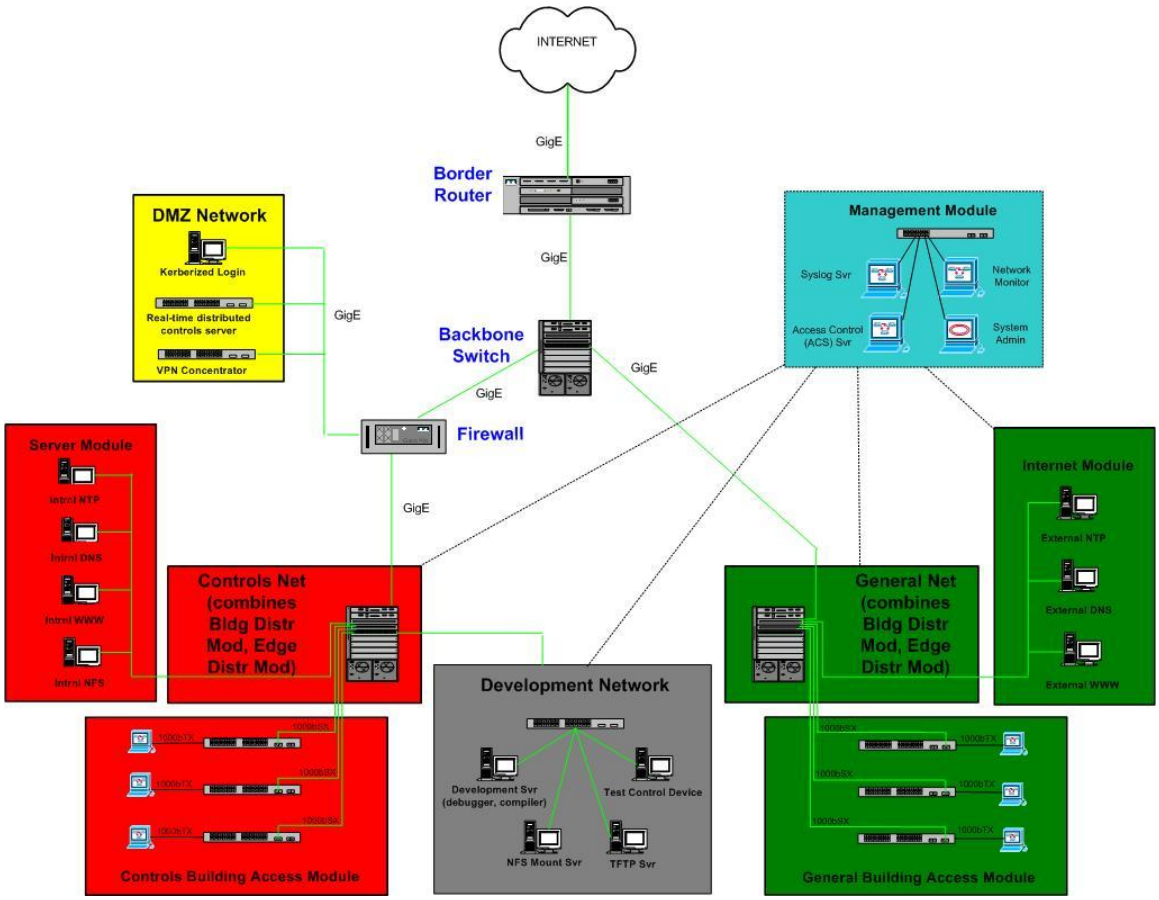

Figure 1. The Four network modules

11.1.1 The Controls network

The Controls network shall be physically separate from the DMZ, Developmental and General networks via dedicated infrastructure using both fiber and copper cable plant along with separate distribution and access network switches.

- The Controls network shall have a Firewall for select traffic with default deny inbound and outbound except for selected services.
- Authenticated access to the Controls network will be possible via gateway devices in the DMZ, including VPN (network based) and bastion hosts (login based).
- Critical network services, such as NTP, DNS, KDC and W2k Domain controllers shall have instances located in the Controls network to maintain usability when isolated from the other networks.
- A single point of disconnection shall be provided to enable total isolation of the Controls network from external network disturbances.

The Controls network shall be populated by network devices assigned static IP addresses in the Class B space of 131.225.x.x

- The third number in the dotted decimal notation shall be provided by Computing Division as requested by the AD Network Group, such as 131.225.146.0 to 131.225.146.255)
- The third and fourth set of numbers in the dotted decimal notation shall then be assigned by the AD Controls group. The third set of addresses shall refer to subnets having related functionality or geography.
- AD Controls shall have an option to specify strategic address allocation for network diagnostic equipment, routers and switches
- All Controls network addresses shall be in one CIDR block (able to be fully specified in the format 131.225.x.y/z where 0<=x<=255, 0<=y<=255 and 16<z<32.).

No.	Requirement	Source	Priority
CXR-N1-110	The Controls network shall be physical separate with a dedicated cable plant and network devices	D. Stenman 1-2008	Critical
CXR-N1-120	The Controls network shall have a firewall with default deny inbound and outbound except for select services	D. Stenman 1-2008	Critical
CXR-N1-130	Authenticated access to the Controls network shall be via gateway devices in the DMZ network, including both a VPN and kerberized bastion hosts.	D. Stenman 1-2008	Critical
CXR-N1-140	The Controls network shall be physically isolated by way of a single point of disconnect.	D. Stenman 1-2008	Critical
CXR-N1-150	Static IP addresses shall be assigned to devices in subnets related to geography and functionality.	D. Stenman 1-2008	Expected
CRX-N1-160	Critical network services such as NTP, DNS, KDC and W2K Domain controllers shall have instances located in the Controls network	T. Zingelman 1-2008	Expected
CRX-N1-170	All devices connected to the Controls network will have a registered system administrator responsible for them	D. Stenman 1-2008	Expected
CRX-N1-180	All Controls network addresses shall be in one CIDR block (able to be fully specified in the format 131.225.x.y/z)	T. Zingelman 1-2008	Desired

11.1.2 The DMZ network

The DMZ network shall provide the method to access the Controls network.

- There shall be a Kerberized bastion host and a VPN server in the DMZ that provide account authentication and allow login or network access for individuals according to Lab strong authentication policy.
- There shall be a real-time distributed controls system gateway server in the DMZ network that will provide software running outside the Controls subnets with access to specific control and monitor points within the Controls network.
- The real-time distributed controls system server shall recognize a subset of Lab User IDs from specific hosts and authorize them remote program access to the Controls network.

11.1.3 The Development network

The Network shall support a Development network to allow for engineering and testing of components to be used in the Controls network.

- The Development network shall isolate development activities from the other subnets, therefore not interfere with normal activities on the Controls network or AD and site-wide Fermi networks.
- Network devices in the Development network shall be assigned static IP addresses and the Mac address, System Administrator, Primary User and location registered accord to Lab policy.
- The Development network shall be accessible through secure channels to network devices, desktop and laptop computers used by the AD Controls Group, while also allowing for access to resources on the Fermi network and the internet.
- The AD Controls Group shall be able to add a reasonable number of net devices to the Development network, which will not be accessible from the internet except through secure channel or have access to any service outside the Fermi network.
- The Development network shall contain a development server, accessible from all devices on the development subnet.
- The Development server shall provide TFTP service (not visible outside the development network), NFS mount service, development tools (debuggers, compilers, etc), and any other software necessary for the Controls Group.

No.	Requirement	Source	Priority
CXR-N1-310	The Development network shall isolate activities from other subnets	D. Stenman 1-2008	Expected
CXR-N1-320	All Development network nodes shall have static assigned IP addresses, and be registered according to Lab policy	D. Stenman 1-2008	Expected
CXR-N1-330	The Development network shall be accessible through secure channel from Controls Group computers.	D. Stenman 1-2008	Expected
CXR-N1-340	The Development network shall have a development server, accessible via secure channel by Controls Group and offering	D. Stenman 1-2008	Expected

	development services.		

11.1.4 The General network

The General network shall offer secure access for development, commissioning and general computing services, following Lab strong authentication policy. The General network includes Static and DHCP network addresses, WiFi access, Printing services, domain login, personal home directory storage, WWW access and email. VoIP and Video data streaming should also be included using QoS to insure network priority.

- General network shall have access to Fermi network and internet.
- Static IP addresses shall be assigned desktops, printers and servers.
- DHCP addressing shall be available for laptops.
- The General network shall have support for QoS.
- ID list.

No.	Requirement	Source	Priority
CXR-N1-410	Fermilab strong authentication policy shall apply to all network attached devices in the General network	D. Stenman 1-2008	Critical
CXR-N1-420	Static IP addresses shall be assigned to desktops, printers and servers in the General network	D. Stenman 1-2008	Expected
CXR-N1-430	DHCP addressing shall be available for laptops in the General network.	D. Stenman 1-2008	Expected
CXR-N1-440	The General network shall have support for QoS.	D. Stenman 1-2008	Desired

11.2. Acceptable failure rate and impact

Redundancy or immediate failover of key core and backbone network resources shall be present in The Network, such as central router, firewall, DNS, NTP, Kerberos. On-site spares shall be present which involves manual replacement of access network equipment. Maintain of these live spares shall consist of all network devices, including backbone, distributed and access switches/routers.

No.	Requirement	Source	Priority
CXR-N2-010	Redundant firewall, border router, DNS server, NTP server, Kerberos server and W2K Domain server shall be provided.	D. Stenman 1-2008	Critical
CXR-N2-020	7/24 hardware/software maintenance shall be provided for critical core routers and backbone switches	D. Stenman 1-2008	Critical
CXR-N2-030	On-site hot spares shall be available to replace distribution and access network devices.	D. Stenman 1-2008	Critical

11.3. Monitoring and response

All network devices and services shall be monitored via a central management station. A Management VLAN shall be configured for The Network to enable secure login, software upgrade, traffic monitoring and logging of network appliances. Allow for automated notification of network degradation. Network problems shall be coordinated with the MCR and a designated call list shall be provided for off-hour response.

No.	Requirement	Source	Priority
CXR-N3-010	Network devices shall be managed from a central server through a dedicated VLAN	D. Stenman 1-2008	Critical
CXR-N3-020	There shall be an automated notification of network degradation	D. Stenman 1-2008	Expected
CXR-N3-030	Network problems shall be coordinated with the MCR and a designated call list for off-hour response	D. Stenman 1-2008	Expected

11.4 Physical Layout and Network Model

The Controls network shall be completely self-contained. Specifically, it shall be able to perform all control system functions and provide all services without a physical connection to any other network.

Infrastructure shall follow the TIA/EIA-568 standard hierarchical cable system architecture using single mode fiber for backbone and distribution layer, and copper for access of most attached devices. Single mode fiber allows for 1 Gigabit (1000BASE-X) or 10 Gigabit uplinks (10GBASE) while copper accommodates common 1 Gigabit interface (1000BASE-T). Required is a comprehensive calculation of the number of network attached devices, bandwidth/timing needs, distances from service buildings, tunnels, Main Control Room, Data Center, and any specific protocol requirements or priorities. 1U switches shall be used for the access layer and network chassis for the distribution layer. Physical separation of the four networks dictates individual switches and fiber. Design shall resist the flat design model. Maintain a hierarchical design that allows for isolation of critical systems, network/computing security, distribution of higher or lower capacity sub-networks, independent subsystem commissioning and network protocol or traffic configuration.

The Controls network shall be centered in the AD Computer Room and connect all areas of the AD accelerator facility.

- All Controls network nodes shall have the ability to communicate with any other node in the Controls network.
- Each device shall have a primary Ethernet connection on a specific subnet.
- Some devices may desire a secondary Ethernet connection on a different subnet from their primary one
- Terminal service and power management shall also be available on dedicated subnets of the Controls network.

There shall be physical connection network taps located at specific points in the accelerator area and wireless access points temporarily available.

- Only roll-around computers and laptops registered and/or configured by the AD network group shall have access in the accelerator area.
- Wireless access points pre-configured by the AD network group shall be provided in the General net to allow restricted wireless access in the accelerator area.

There shall be uniform speed and duplex for connections within and between all networks.

- All network devices in the Controls and DMZ networks shall have the ability to communicate at speeds up to 1000 Mbps, full duplex, preferably on copper media except where distance or RF interference are an issue.
- All network devices in the Development network shall have the ability to communicate at speeds up to 1000 Mbps, preferably on copper media except where distance or RF interference are an issue.
- Connections to the Controls network from the DMZ shall have the ability to communicate at speeds up to 1000 Mbps.

Subnet Requirements; there shall be a set of VLANs (virtual networks or broadcast domains) available on the Controls network to provide an organized structure and isolate specific functions which have bandwidth or timing requirements.

- All subsystems shall have the ability to belong to a separate dedicated VLAN/subnet or broadcast domain.
- There shall be a Network Management VLANs for dedicated network services.

No.	Requirement	Source	Priority
CXR-N4-010	The Network cable system shall be of TIA/EIA-568 Hierarchical design using single mode fiber or better for the backbone and Category 6e or better for access attached nodes	D. Stenman 1-2008	Critical
CXR-N4-020	The cable plant shall have individual cable and network devices for the Controls network to ensure isolation from DMZ, Development and General networks	D. Stenman 1-2008	Critical
CXR-N4-030	The Network shall have physical connection network taps located at specific points in the accelerator area.	D. Stenman 1-2008	Expected
CXR-N4-040	The General Network shall have wireless access points temporarily available for the accelerator tunnels and areas in addition to the permanent access points	D. Stenman 1-2008	Expected
CXR-N4-050	All subsystems shall have the ability to belong to a separate dedicated VLAN/subnet or broadcast domain	D. Stenman 1-2008	Expected
CXR-N4-060	All Controls network nodes shall have the	D. Stenman	Expected

	ability to communicate with each other	1-2008	
CXR-N4-070	The only 'portable' devices which shall be connected to the Controls network are those that have been securely configured by the network group	D. Stenman 1-2008	Critical
CXR-N4-080	All network devices shall be capable of 1000 Mbps, full duplex communication on all ports	D. Stenman 1-2008	Critical
CXR-N4-090	All network devices shall be capable of IPv6 operation	T. Zingelman 1-2008	Expected
CXR-N4-100	All network edge connections shall be via copper	D. Stenman 1-2008	Expected
CXR-N4-110	All network distribution connections shall be via fiber	D. Stenman 1-2008	Expected
CXR-N4-120	There shall be Network Management VLANs	D. Stenman 1-2008	Expected

11.5 Network Security

The Controls network shall be firewalled with default deny inbound and outbound except for selected services.

- VPN, real-time distributed controls system gateway and Bastion Hosts shall be in the DMZ network to allow authenticated inbound traffic through the firewall.
- Controls VPN shall have authentication time limited network access.
- Bastion Hosts shall have Kerberized login as per Fermi strong authentication policy.
- Bastion Hosts shall have time limited logins.
- Bastion Hosts shall have SSH port forwarding allowed.
- Bastion Hosts shall have NFS mounts of selected inside disk to allow kerberized FTP access (FTP shall be blocked at Firewall).

There shall be ACLs on particular subnets and/or VLANs to further limit access for sensitive devices and ones that cannot conform to all provisions of strong authentication.

Network devices shall reside on secure Network Management VLANs and require either authentication login using Kerberos or individual Radius user accounts.

There shall be an emergency disconnect at division border to ensure Accelerator operation regardless of site or internet traffic storms.

Cyber protections shall provide security without disruption to accelerator operations.

- Patching and anti-virus services shall be available for OSs and Applications of all network attached devices, including network routers, switches and access points.
- Scanning of The Network for standard network services/ports, adherence to critical system patches and anti-virus shall be tolerated by all network attached nodes.

An inventory of all systems on the network shall be maintained, to include OS, hardware, MAC address, IP address, sysadmin and primary user

- Any changes in registered IP and MAC address shall have automated notification.

No.	Requirement	Source	Priority
CXR-N5-010	There shall be Access Control Lists on subnets and VLANs as required to provide isolation in addition to the firewall.	D. Stenman T. Zingelman 1-2008	Expected
CXR-N5-020	VPN, a real-time distributed controls system gateway and Bastion host shall have time limited login.	D. Stenman T. Zingelman 1-2008	Expected
CXR-N5-030	There shall be an emergency disconnect at division border.	D. Stenman T. Zingelman 1-2008	Expected
CXR-N5-040	Cyber protections shall provide security scanning and patching without disruption to accelerator operations.	D. Stenman T. Zingelman 1-2008	Expected
CXR-N5-050	An inventory of all systems on The Network shall be maintained, to include OS, hardware, MAC address, IP address, sysadmin and primary user.	D. Stenman T. Zingelman 1-2008	Critical
CXR-N5-060	Any changes in registered IP and MAC address shall have automated notification.	D. Stenman T. Zingelman 1-2008	Critical
CXR-N5-070	Network devices shall reside within Management VLANs with secure authentication.	D. Stenman T. Zingelman 1-2008	Critical

11.6 Remote Network Monitoring

Network devices shall implement RMON, a flow-based monitoring and analyzing client/server model. The RMON2 agents will include MIB legacy groups of RMON1 (such as host statistics, top users, alarms, SNMP traps, etc) and the extended groups of RMON2.

- Network Statistics
- Alarms
- Hosts Statistics and top Hosts
- Network-Layer Host
- Network-Layer Matrix
- Application-Layer Host
- Application-Layer Matrix

- Probe configuration
- Protocol Directory and Distribution

No.	Requirement	Source	Priority
CXR-N6-010	RMON shall be implemented to monitor and analyze Ethernet packets	D. Stenman 1-2008	Desired
CXR-N6-020	RMON2 shall be included with its extended MIB groups to add support for network and application layer	D. Stenman 1-2008	Desired

11.7 Data Center

The AD Computer room, XGC-108, shall expand to include additional network equipment, Controls servers, Front Ends, Database servers, and file servers.

Available conventional power shall be expanded to include additional Java engines, Controls database servers, Front Ends, etc. Amount of expansion depends on watts per unit device.

Available UPS power shall be expanded to include additional Java engines, Controls database servers, Front Ends, etc. Amount of expansion depends on watts per unit device.

Air flow and temperature and humidity control shall be increased according to level of heat load per square foot within Computer Room.

No.	Requirement	Source	Priority
CXR-N7-010	Conventional power in the computer room shall be expanded according to increase of watts per unit device	D. Stenman 1-2008	Critical
CXR-N7-020	UPS power in the computer room shall be expanded according to increase of watts per unit device	D. Stenman 1-2008	Critical
CXR-N7-030	Air flow and temperature/humidity controls in the computer room shall be expanded to accommodate increase of heat load per square foot within Computer Room.	D. Stenman 1-2008	Critical