Construction of the TPS Network System

Y. S. Cheng*, Y. T. Chang, C. H. Huang, C. H. Kuo, Jenny Chen, K. T. Hsu

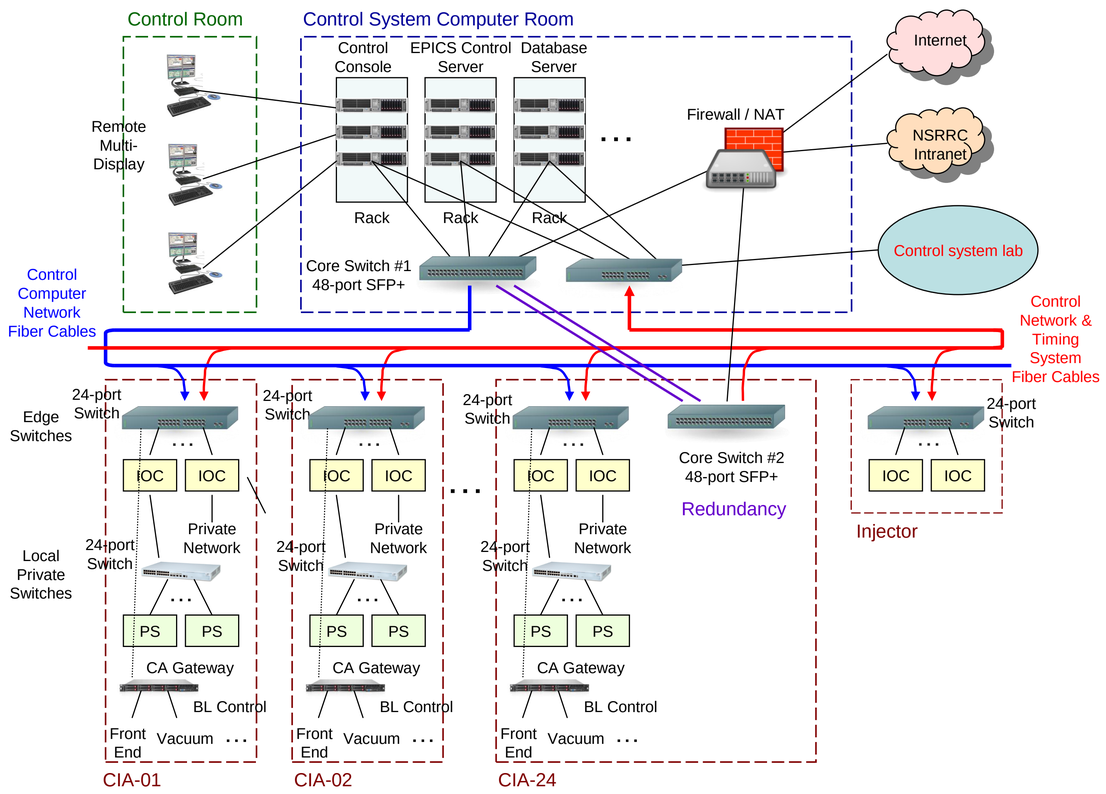
NSRRC, Hsinchu 30076, Taiwan

Abstract

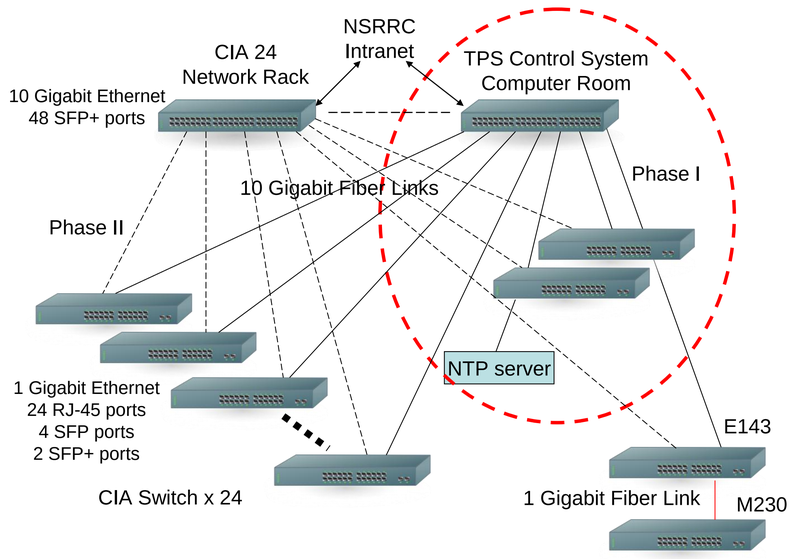
Project of 3 GeV Taiwan Photon Source (TPS) need a reliable, secure and high throughput network to ensure facility operate routinely and to provide better service for various purposes. The network system includes the office network, the beamline network and the accelerator control network for the TPS and the TLS (Taiwan Light Source) sites at NSRRC. Combining cyber security technologies such as firewall, NAT and VLAN will be adopted to define the tree network topology for isolating the accelerator control network, beamline network and subsystem components. Various network management tools are used for maintenance and troubleshooting. The TPS network system architecture, cabling topology, redundancy and maintainability are described in this report.

Infrastructure

- The control network will be a 1-Gbps switched Ethernet network with a backbone at 10-Gbps.
- Two high-performance core switches will be used for redundancy.
- There are 24 Control Instrumentation Areas (CIA). Each CIA serves for one cell of the machine control and beamline interface.
- Edge switches are used to connect IOC nodes and uplink to the high-speed backbone through 10-Gbps fiber uplinks.
- Local private switches are used for local private network to connect control devices and uplink to the IOC nodes.



TPS Control Network – Baseline Plan (Cost Effective Solution)



Subsystem Subnet

- One Class B private network will be used for IOC network. The IP addressing schema will be easy to identify the locations of IOCs and devices.
- Multiple Class C private networks for respective subsystems, such as BMP IOCs, power supplies, motion controllers, GigE Vision, front-end, vacuum, beamline control, etc.
- Subsystems can access process variables of accelerator control system via CA gateways.
- The functionality of the EPICS based CA gateway is to forward channel access to different network segments. It can also reduce network traffic and provide additional access security.

Cyber Security

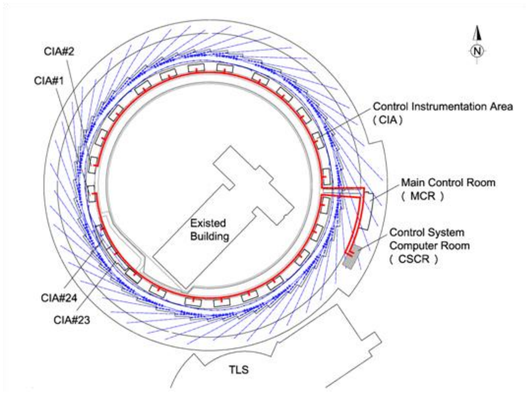
- Control systems are correspondingly exposed to the inherent vulnerabilities of the commercial IT products.
- Combining firewall, NAT, VLAN… technologies, control network is isolated to protect IOCs and accelerator components that require insecure access services.
- Firewall only passes the packets from authorized hosts with pre-defined IP addresses outside control network and opens specific service ports for communications. But firewall is not able to resist the spread of worms.
- Security gateway or IPS (Intrusion Prevention System) is needed to block worm attacks and quarantine suspicious hosts.
- Remote access mechanism needs network tunneling applications to bypass the firewall. It also requires a reliable user authentication mechanism for protection.
- Security will always put at the highest priority for the TPS control system.

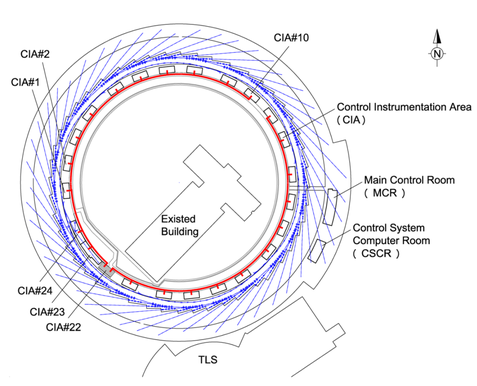
TPS Project

- Taiwan Photon Source (TPS) will be the new 3 GeV synchrotron radiation facility with ultra-high photon brightness and extremely low emittance.
- TPS control system will be implemented using the Experimental Physics and Industrial Control System (EPICS) software toolkit.
- Control devices are connected by the control network and integrated with EPICS based Input Output Controller (IOC).

Cabling

- For control computer network, optical fiber cables will distribute from the Control System Computer Room (CSCR) to every CIA.
- Copper STP/UTP cables are used to connect CIA network switches to various IOCs and network attached devices within the same CIA.
- For control network and timing system, optical fiber cables will distribute from the CIA#22 to every CIA and Control System Computer Room (CSCR) .
- The length of fiber cables will be equal for receiving timing signals synchronously.





Network Management

- Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) will be configured to implement redundancy. .
- Network monitoring software (e.g. MRTG) will be used to show traffic and usage information of the network devices. By collecting and analyzing the packets, it can measure the traffic and usage to avoid bandwidth bottlenecks.
- It is necessary to access the control system from outside in case of machine problems. Remote maintenance or troubleshooting has the advantages of convenience and time-saving.
- The Network Time Protocol (NTP) servers are needed for timekeeping. NTP is used for synchronizing the clocks of computer systems over the TPS control network within 10 ~ 100 millisecond performance.
- Using Simple Network Management Protocol (SNMP), the behaviour of network-attached devices can be monitored for administrative attentions. A dedicated EPICS IOC with SNMP support will be used to monitor the status of control system components such as CompactPCI (cPCI) IOC crates, network switches, servers, UPSs, etc.

Current Status

- All backbone fiber network are in installation and will be finished in October, 2013.
- Electricity are available at installation site now. Air conditioning will be available in early 2014. Installation areas for network devices will available in the last quarter of 2013.
- Only limited network access is scheduled at TPS site will be available in October, 2013 due to infrastructure is still not fully available.
- Full access of the network will be available in the first quarter of 2014. All network equipments are ready for installation.
- Figure 5 shown all network devices for control system, accelerator system, Phase I beamlines (7 beamlines) are in testing and configuration. It is expected when the installation site and utility available, the network service can be started immediately without further delay.

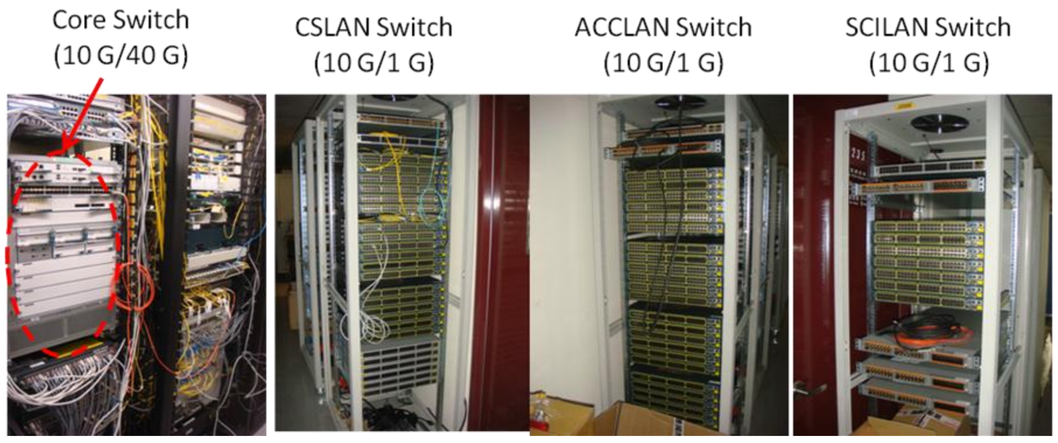


Figure 5: Network switches are ready for installation, and configuration is in proceed.

Summary

- An adaptive, secure and fault-tolerant control network are essential for the stable operation of the TPS.
- The control network will be separated from the NSRRC campus general purpose network for imposing security. Subsystem subnets will connect to control system via EPICS CA gateways for forwarding data and reducing network traffic. Two fiber cabling distributions are described.
- Network management tools will be used to enhance productivity. Remote access mechanism with proper authentication will be implemented for system maintenance or troubleshooting.
- An infrastructure monitoring system is planned to adopt the EPICS and SNMP. Cyber security will be the most concern.

*E-mail: cheng.ys@nsrrc.org.tw