Preliminary Planning of Taiwan Photon Source Control Network

Y. T. Chang*, C. H. Kuo, Y. S. Cheng, Jenny Chen, S. Y. Hsu, K. H. Hu, Y. K. Chen, K. T. Hsu
NSRRC, Hsinchu 30076, Taiwan

Abstract

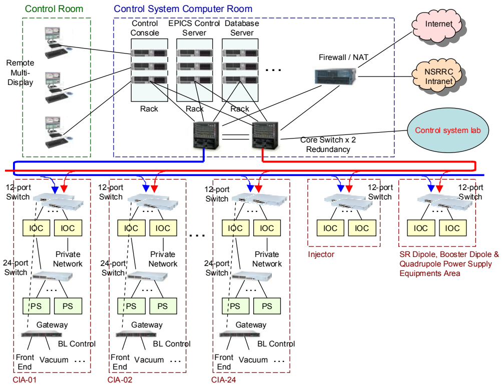
The Taiwan Photon Source (TPS) control network is one of the most important infrastructures for the control system which is based upon the EPICS toolkit framework. The TPS network is built to be a modern, reliable, flexible and secure environment between public and private Ethernet with various network control and monitor techniques including firewall, SNMP, QOS, VPN, etc. Network tunneling technique will be applied in the remote access, out of TPS especially. The Ethernet will be intensively used as fieldbus also, topology of the fieldbus is also considered. This paper will describe the preliminary planning and conceptual design for the TPS control system network. We also discuss the system architecture in this conference that consists of cabling topology, redundancy and maintainability.

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).
- The control network will be a 1-Gbps switched Ethernet network with a backbone at 10-Gbps.

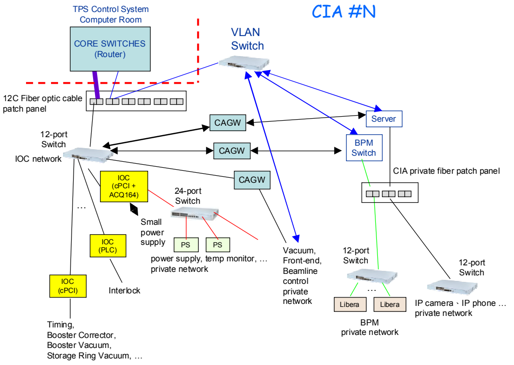
Infrastructure

- To build a reliable, agile, flexible, scalable and secure network for TPS control system.
- Network services will be available at the control room, control system computer room, 24 Control Instrumentation Areas (CIA), linear accelerator equipment area, transport lines, and main power supply equipment room which are distributed along the inner zone just outside of the machine tunnel.
- Control consoles with remote multi-display will be used to manipulate and monitor the accelerator through network.
- Control system computer room contains EPICS control servers, database servers, control consoles, and network equipments.
- Dual high-performance core switches configured with Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) will be used to implement redundancy.
- Each CIA serves for one cell of the machine control and beamline interface. Major devices and subsystems connected to the control system are installed inside CIAs.
- 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.
- Control network connects to NSRRC campus network through a firewall with Network Address Translation (NAT) function. Segregating the network will strengthen the security for those devices that need additional protection and high availability.



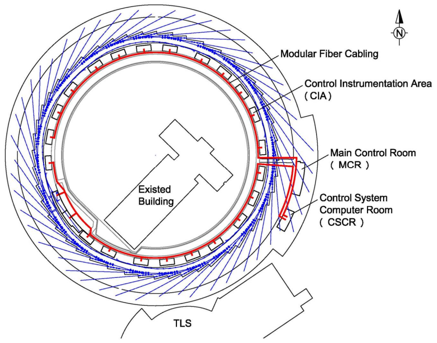
Subsystem Subnet

- One Class B private network will be used for IOC network.
- Multiple Class C private networks for respective subsystems, such as BMP IOCs, motion controllers, global machine protection, GigE Vision, front-end, vacuum, beamline control, etc.
- CA gateways will connect these Class C private networks to TPS control network.
- VLAN routing mechanism will be implemented for providing access from the TPS control network or outside network.


TPS Control System Computer Room
CORE SWITCHES (Router)
CIA #N
VLAN Switch
12C Fiber optic cable patch panel
12-port Switch
IOC network
CAGW
CAGW
CAGW
Server
BPM Switch
CIA private fiber patch panel
IOC (cPCI + ACQ164)
24-port Switch
Small power supply
PS
PS
power supply, temp monitor, … private network
IOC (PLC)
Interlock
IOC (cPCI)
Timing, Booster Corrector, Booster Vacuum, Storage Ring Vacuum, …
Vacuum, Front-end, Beamline control private network
12-port Switch
Libera
Libera
BPM private network
12-port Switch
IP camera、IP phone … private network

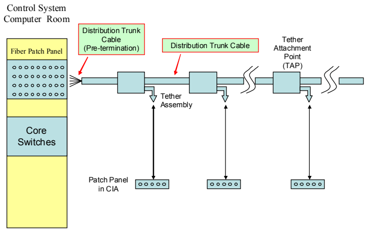
Cabling

- Optical fiber cables are distributed from the Control System Computer Room (CSCR) to every CIA.
- Copper STP/UTP or fiber cables are used to connect CIA network switches to various IOCs and network attached devices within the same CIA.


N
Modular Fiber Cabling
Control Instrumentation Area (CIA)
Main Control Room (MCR)
Control System Computer Room (CSCR)
Existed Building
TLS

Cabling Topology

- Modular fiber cabling system is under consideration. It replaces traditional point-to-point links with a single distribution trunk cable and multiple tether attachment points.
- Tradeoff between cost and installation time of the modular fiber cabling system versus tradition fiber system is under serious study.


Control System Computer Room
Fiber Patch Panel
Core Switches
Distribution Trunk Cable (Pre-termination)
Distribution Trunk Cable
Tether Attachment Point (TAP)
Tether Assembly
Patch Panel in CIA

Network Management

- Implementing Simple Network Management Protocol (SNMP), management tools can monitor the network-attached devices for administrative attention.
- Network monitoring software (e.g. MRTG, PRTG, …) 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.
- Some applications may need guaranteed throughput to ensure that a minimum level of quality is maintained. QoS can optimize bandwidth resources to improve network performance.
- 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.
- Network tunneling tools, such as Virtual Private Network (VPN), can be used to penetrate the firewall system of the protected network. It can establish an encrypted and compressed tunnel for TCP or UDP data transfer between control network and public networks inside or outside the TPS.
- Reliable authentication mechanism is also essential to remote access the control network.
- 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.
- The Precision Time Protocol (PTP) with 100 ns ~ 100 ms timing precision might deploy in the TPS control network after its hardware and software mature in the future.
- NAT network balance technology will be required to scatter the communication load.

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.

Summary

- An adaptive, secure and fault-tolerant control network are essential for the stable operation of the TPS.
- Control network will be separated from the NSRRC campus general purpose network.
- Subsystem subnets will connect to control system via CA gateways for forwarding data and reducing network traffic.
- VLAN routing mechanism will provide access to subsystem subnets.
- Network management tools will be used to enhance productivity.
- Remote access mechanism with proper authentication will be implemented for system maintenance or troubleshooting.
- The latest development of network technologies will be adopted for the future planning.

*E-mail: ytchang@nsrrc.org.tw