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
National Synchrotron Radiation Research Center, 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.

INTRODUCTION

Taiwan Photon Source (TPS) [1] will be the new 3 GeV synchrotron radiation facility to be built at National Synchrotron Radiation Research Center, featuring ultra-high photon brightness with extremely low emittance. It is planned to begin construction in late 2009, and the commissioning is scheduled in 2013.

The control network is used for the operations of accelerators and beamlines. TPS control system will be implemented using the Experimental Physics and Industrial Control System (EPICS) [2] 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

The main goal of this preliminary planning is to build a reliable, agile and secure network for TPS control system. The design will provide enough flexibility and scalability for future expansion.

Accelerator operators are the principal users of the control system. Control consoles with remote multi-display will be used to manipulate and monitor the accelerator through network. For remote monitoring and control Taiwan Light Source (TLS) facility, dedicated control consoles are planned to be installed in TPS control room.

Control system computer room contains EPICS control servers, database servers, control console computers, and network equipments (e.g. core swiches and firewalls). Dual high-performance core switches are planned to be used for reliability. Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) will be configured to implement redundancy. Links between core and node switches are matched up with redundant cabling structure.

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. 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.

Node switches are distributed in every CIA. Each IOC node will be directly connected to a 1-Gbps switch. Then the switches are connected to the high-speed backbone through 10-Gbps uplinks.

EPICS based CA gateways will provide necessary connectivity and isolation. It will be used to connect to subsystems such as Beam Position Monitor (BPM) system, beamline control, GigE Vision cameras, etc. The functionality of the 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. Network traffic burden will also be lowered by isolating from general purpose network. Remote access mechanism will be constructed for maintenance and troubleshooting. The TPS control network infrastrcture is shown in Fig. 1.

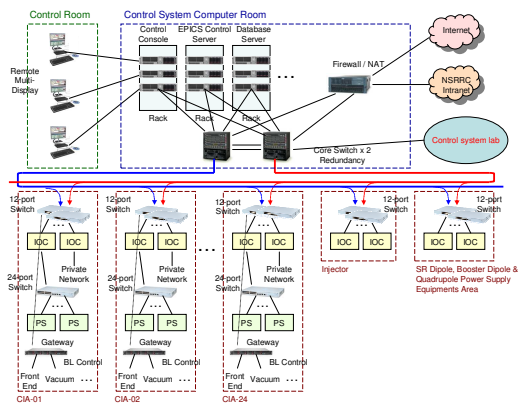

Figure 1: TPS control network infrastrcture.

Control system laboratories for software development and hardware maintenance are also connected with the

control network. Connection to TLS control network is required for remote operations of the TLS facility.

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.

There are multiple Class C private networks for respective subsystems, such as BPM IOCs, motion controllers, global machine protection, GigE Vision, etc. Access of these Class C private networks might connect to the the VLAN router to provide access possibility.

Subsystem Subnet

Highly reliable Ethernet will be heavily used as fieldbus in the TPS control system. Power supplies for dipole, quadrupole and sextupole are planned to connect to the EPICS IOCs by private Ethernet. Miscellaneous instruments will connect to the control system IOC located at each CIA via Ethernet also, such as LXI instruments, temperature/voltage monitors, etc. All of these devices might comply with LXI standard or not.

Orbit data is the most important operation information and should be captured in 10 Hz rate without interruption. In order to provide better service for this, a dedicated Class C subnet is planned for BPM IOCs. A CA gateway will connect with the BPM network to the TPS control network. VLAN routing mechanism will be implemented for providing access the BPM IOCs from the TPS control network or outside network.

It is expected that every beamline will have a Class C private network for their control system, data acquisition, and endstation applications. This network can connect to the NSRRC campus intranet via VLAN routing mechanism. The beamline EPICS control environment will connect to the machine control system via CA gateway at each CIA. This design will provide necessary connnectivity between the machine control system and beamline control system. It can also restrict unnecessary network traffic across different network segments. Firewall switch might be used to provide further security service.

Timing of the TPS will adopt the event system. It is a separate system from the control network and not included in the scope of this report.

IP technology will be heavily used in the TPS control system. For providing more convenient environment for system maintenance, IP based cameras for area monitoring, phones, pagers are planned to attach to a Class C private network. This network will connect to the control network via a CA gateway and/or VLAN mechanism to the NSRRC intranet for saving network bandwidth.

GigE Vision for diagnostics is based on the Internet Protocol standard and can be adapted to EPICS environment. Also, the images can be easily accessed through network for machine studies. The GigE Vision cameras can connect to control system through Ethernet with the data transfer rate up to 1000 Mbits/s. For decreasing traffic loading, one Class C private network and one CA gateway will also be used for the GigE Vision cameras to connect with the control system.

For miscellaneous devices, the same principle will be adopted. The cabling scale will be downsized by using CA gateways and VLAN routing mechanism. Fig. 2 shows the layout of CIA networking.

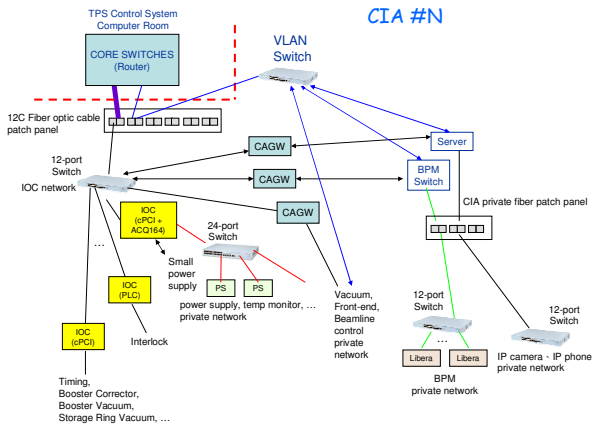

Figure 2: CIA networking layout.

Cabling

Optical fiber cables are distributed from the server & network equipment room 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.

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 (e.g. CORNING Plug & Play AnyLAN System). The modular cabling structure is shown in Fig. 3. Tradeoff between cost and installation time of the modular fiber cabling system versus tradition fiber system is under serious study.

The integrated global orbit feedback system combined with slow and fast correctors will adopt dedicated fiber links to transport beam position data and correctors setting at 10 kHz rate (e.g. serial RocketIO links). These fibers will accompany with the network fibers.

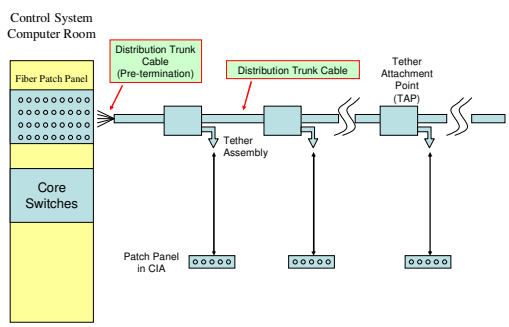

Figure 3: Modular cabling system.

NETWORK MANAGEMENT

Implementing Simple Network Management Protocol (SNMP), management tools can monitor the network-attached devices for administrative attention. SNMP exposes management data of the managed systems as variables. Then these variables can be queried or set by managing applications. For example, management tools can show the port status of the switch and enable/disable the switch ports.

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.

Quality of Service (QoS) can apply different priority to different data flows, users, or applications, and guarantee a certain level of performance to a data flow. 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. There are many ways to configure the network to enable remote access. 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. Providing a 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. For the system required by the picosecond timing, event system will deal this. The Precision Time Protocol (PTP) is another time-transfer protocol with 100 ns ~ 100 μs timing precision which might deploy in the TPS control network after its hardware and software mature in the future.

Because there are many subnets that will need to go out to Internet, more than one NAT router might be used. NAT network balance technology will be required to scatter the communication load.

CYBER SECURITY

Today's accelerator control systems are commonly based on modern Information Techonolgy (IT) hardware and software, such as Windows/Linux PCs, PLCs, data acquisition systems, networked control devices, etc. Control systems are correspondingly exposed to the inherent vulnerabilities of the commerial IT products. Worms, viruses and malicious software have caused severe cyber security issues to emerge [3].

Security policy for control network is needed. Regulations should be defined for the accelerator scientists and engineers to access the control system.

It is necessary to use network segregation to protect vulnerable devices. Combining firewall, NAT, VLAN… technologies, control network is isolated to protect IOCs and accelerator components that require insecure access services (e.g. telnet).

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. Worms are not only designed to self-replicate and spread but also consume the network bandwidth. Thus security gateway or IPS (Intrusion Prevention System) is needed to block worm attacks and quarantine suspicious hosts. IPS can detect and stop network threats such as worms, viruses, intrusion attempts and malicious behaviors.

Remote access mechanism needs network tunneling applications to bypass the firewall. It will provide a private tunnel through the public network for remote access to the control network. The remote access mechanism also requires appropriate types of protection and control. It must be enhanced with a reliable user authentication mechanism for full security.

Security will always put at the highest priority for the TPS control system. However, balance between security and convenience will be addressed also.

SUMMARY

This report describes the conceptual design of the TPS control network. An adaptive, secure and fault-tolerant control network are essential for the stable operation of the TPS. To impose cyber security, the 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. Some issues, such as cabling topology, are still under intensive study. The latest development of network technologies will be adopted for the future planning.

REFERENCES

[1] TPS Design Book, v16, September 30, 2009.
[2] Experimental Physics and Industrial Control System, http://www.aps.anl.gov/epics/.
[3] S. Lüders, "Summary of the Control System Cyber-Security (CS)2/HEP Workshop", Proceedings of ICALEPCS07, Knoxville, Tennessee, USA. 18 (2007).