INFRASTRUCTURE OF TAIWAN PHOTON SOURCE CONTROL NETWORK

Y. T. Chang, C. H. Kuo, Y. S. Cheng, Jenny Chen, S. Y. Hsu, C. Y. Wu, K. H. Hu, K. T. Hsu
National Synchrotron Radiation Research Center, Hsinchu 30076, Taiwan

Abstract

A reliable, flexible and secure network is essential for the Taiwan Photon Source control system which is based upon the EPICS toolkit framework. Subsystem subnets will connect to control system via EPICS based CA gateways for forwarding data and reducing network traffic. Combining cyber security technologies such as firewall, NAT and VLAN, control network is isolated to protect IOCs and accelerator components. Network management tools are used to improve network performance. Remote access mechanism will be constructed for maintenance and troubleshooting. The Ethernet is also used as fieldbus for instruments such as power supplies. This paper will describe the system architecture for the TPS control network. Cabling topology, redundancy and maintainability are also discussed.

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. The construction began in February 2010, and the commissioning is scheduled in 2014.

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 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. [3]

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. 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.

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.

Connection to TLS control network is required for remote operations of the TLS facility. Control system laboratories for software development and hardware maintenance are also connected with the control network. The TPS control network infrastrcture is shown in Figure 1.

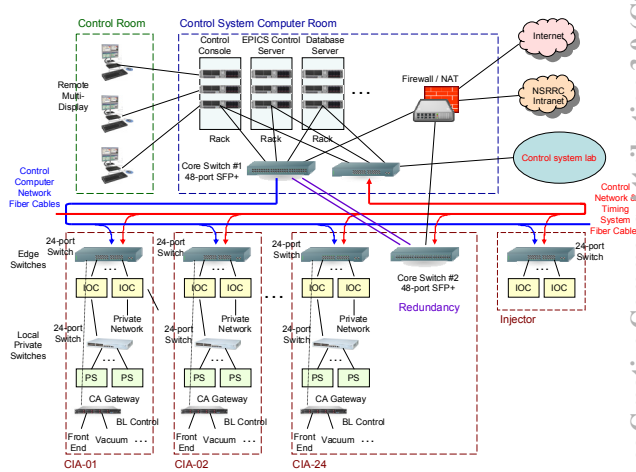

Figure 1: TPS control network infrastrcture.

A high performance switch with 48 10-Gbps fiber ports will be defined as the core switch. Two core switches will be used for redundancy, one is located inside the Control System Computer Room and the other is located inside CIA #24. Optical fiber links between core and edge switches are matched up with redundant cabling structure.

There are two types of switches be used in every CIA. The first type is defined as the edge switch which is used to connect IOC nodes and uplink to the high-speed backbone through 10-Gbps fiber uplinks. A 24-port 100/1000BASE-T switch with 2 10-Gbps fiber uplink ports wil be selected as the edge switch.

The second type is defined as the local private switch which is used for local private network to connect control devices such as power supplies and uplink to the IOC nodes. Depending on the needs, a variety of low cost Ethernet switches will be used as the local private switch.

Considering the budget, only one core switch will be used in Phase I. The redundancy structure will be implemented later in Phase II. But the fiber cabling for redundancy will be ready in Phase I. Figure 2 shows the baseline plan of the TPS control network.

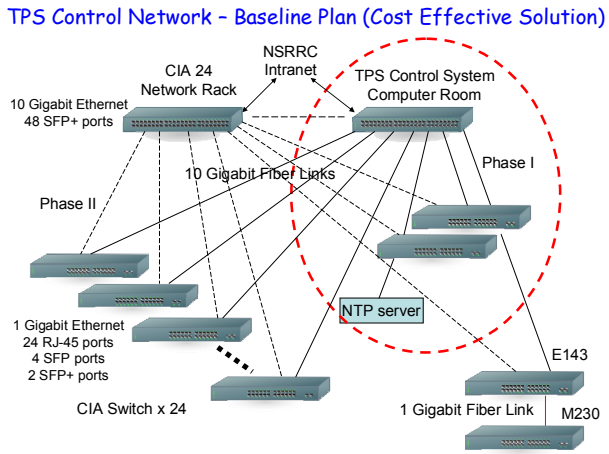

Figure 2: TPS control network – baseline plan.

SUBSYSTEM SUBNET

One Class B private network will be used for IOC network. Because there is a huge number of netwroked devices which scatter over a vast area (e.g. 24 CIAs), the IP addressing schema will be easy to identify the locations of IOCs and devices. This will be helpful to speed up finding the devices for maintenance and troubleshooting. This Class B private network will use IP range 172.20.xx.yy which xx represents locations (e.g. number of CIA) and yy is for functional groups.

There are multiple Class C private networks for respective subsystems, such as BPM IOCs, power supplies, motion controllers, GigE Vision, etc. These Class C private networks will use IP range 172.21.xx.yy which schema is also the same as above. Access of these Class C private networks might connect to the the VLAN router to provide access possibility.

Highly reliable Ethernet will be heavily used as fieldbus in the TPS control system. Power supplies for dipole, quadrupole and sextupole are connected to the EPICS IOCs by Class C private Ethernet within the CIAs.

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.

EPICS based CA gateway will provide necessary connectivity and isolation. Its functionality is to forward channel access to different network segments. It can also reduce network traffic and provide additional access security.

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.

Subsystems such as vacuum, front-end, beamline control, and utility can access process variables of accelerator control system via CA gateways. It is expected that every beamline will have a Class C private network for their control system, data acquisition, and endstation applications. 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 and also restrict unnecessary network traffic across different network segments. The relations between the machine control system and beamline control do not clearly defined at current stage.

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.

For miscellaneous devices, the same principle will be adopted. The cabling scale will be downsized by using CA gateways and VLAN routing mechanism.

CABLING

For the long distance (> 100 m) networking, single-mode fiber (SMM) in the category G652.D will be used for cost consideration. There are two SMM cabling distribution links. One of the links is for control computer network only, the other is for control network and timing network dual function fiber pairs in one fiber cable.

The fiber cables for the control computer network will distribute from the Control System Computer Room and surround half of the ring clockwise and counterclockwise to every CIA. Then Copper STP/UTP cables are used to connect CIA edge switches to various IOCs and network attached devices within the same CIA. The fiber cabling for control computer network is shown in Figure 3.

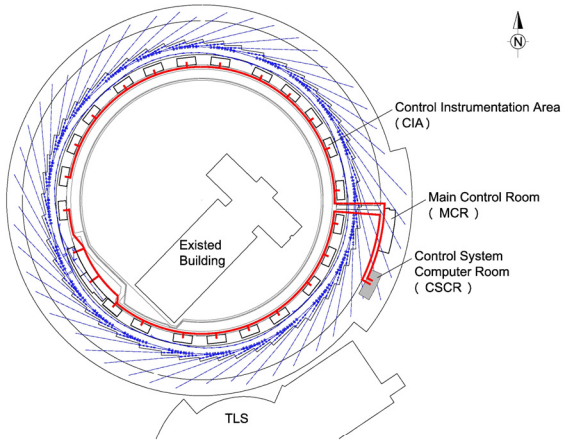

Figure 3: Fiber distribution for control computer network.

Since the timing master is located inside CIA #24, the fiber cables for control network and timing system will distribute from the CIA #24 to every CIA and Control System Computer Room. For receiving timing signals synchronously, the length of fiber cables will be equal. Besides, one fiber pair will be used as the redundancy for the control computer network. The fiber cabling for control network and timing system is shown in Figure 4.

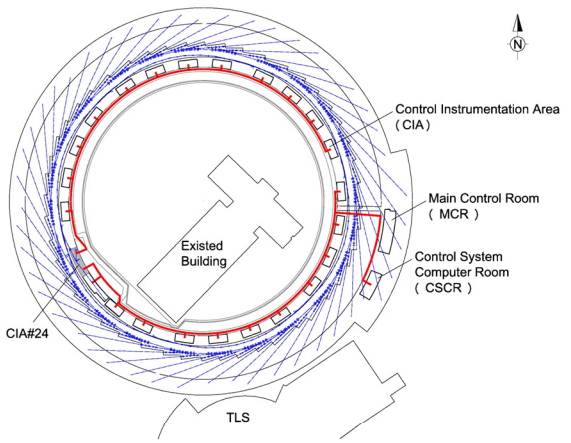

Figure 4: Fiber distribution for control network and timing system which strated form CIA #24.

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. 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.

Using Simple Network Management Protocol (SNMP), the behaviour of network-attached devices can be monitored for administrative attentions. Since the TPS control system is based upon the EPICS framework, 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, Uninterruptible Power Supplies (UPSs), etc. The equipment room environment such as temperature and electric power will also need to be watched. [4]

CYBER SECURITY

Current 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.

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. Security policy for control network is essential. Regulations should be defined for the accelerator scientists and engineers to access the control system. It's everyone's responsibility to protect the

infrastructure. However, balance between security and convenience will be addressed also.

SUMMARY

This report describes the infrastructure of the TPS control network. 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 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.

REFERENCES

[1]. TPS Design Book, v16, September 30, 2009.
[2]. Experimental Physics and Industrial Control System, http://www.aps.anl.gov/epics/
[3]. Y.T. Chang, "Preliminary Planning of Taiwan Photon Source Control Network", ICALEPCS 2009
[4]. Y.T. Chang, "Plans for Monitoring TPS Control System Infrastructure Using SNMP and EPICS", PCaPAC 2010.