USING A CONTROL SYSTEM ETHERNET NETWORK AS A FIELD BUS*

W. DeVan, S. Hicks, G. Lawson, W. Wagner, D. Wantland, E. Williams, ORNL, Oak Ridge, TN

Abstract

A major component of a typical accelerator distributed control system (DCS) is a dedicated, large-scale local area communications network (LAN). The SNS EPICS-based control system uses a LAN based on the popular IEEE-802.3 set of standards (Ethernet). Since the control system network infrastructure is available throughout the facility, and since Ethernet-based controllers are readily available, it is tempting to use the control system LAN for "fieldbus" communications to low-level control devices. These devices may or may not be compatible with the communications protocols, traffic levels, etc. This paper presents some of the benefits and risks of combining high-level DCS communications with low-level "field bus" communications on the same network, and describes measures taken at SNS to promote compatibility between devices connected to the control system network.

INTRODUCTION

A major component of a typical accelerator distributed control system (DCS) is a dedicated, large-scale local area communications network (LAN). The SNS EPICS-based control system uses a LAN based on the popular IEEE-802.3 set of standards (Ethernet). Since the control system network infrastructure is available throughout the facility, and since Ethernet-based controllers are readily available, it is tempting to use the control system Ethernet LAN for "field bus" communications to low-level control devices (e.g. programmable logic controllers (PLCs), vacuum controllers, and remote I/O). In the recent past such devices communicated over dedicated, proprietary communications networks. More recently the option of using industry-standard “field bus” communications networks has arisen (e.g. Fieldbus and Profibus). SNS elected to integrate their control system communications onto one large-scale Ethernet network rather than to use dedicated field bus networks. The consequences of this decision will be discussed in this paper.

BENEFITS/RISKS OF USING CONTROL NETWORK FOR FIELD BUS TRAFFIC

The primary benefit of using a single, integrated control system network (e.g. for both distributed control system communications and field-bus communications) is reduced cost. Adding a second network roughly doubles the cost of network hardware everywhere that the networks overlap. There are also maintenance and availability benefits since there are fewer network devices in the final system.

Another consideration is product availability. At present there are several field bus standards being used, and most control equipment vendors have picked one standard to base their products’ communications on. Once one picks a field bus standard, there is a relatively-limited set of vendors that have products that interface with that bus. This contrasts with Ethernet, which many vendors are adopting as an interface to their products.

Risks of using a single control system network for all control-related functions include the following:

- Low-level control devices (e.g. vacuum controllers, PID controllers, and remote I/O stations) typically have small processors that may not be able to handle high levels of network traffic. In particular, high rates of broadcast traffic can render such devices inoperable.
- Ethernet and TCP/IP communications are not deterministic, so communications response time between control devices is variable. Mixing DCS and field bus communications complicates performance expectations since the level of network traffic can be extremely variable and the number of devices (and associated traffic) on the network continues to increase with time. This can result in timing problems when implementing equipment interlocks over the LAN (as is commonly done over a field bus).
- Low-level devices may have special communications requirements that might otherwise not be necessary for the DCS. (For example, at SNS PLC-to-PLC communications requires use of “multicasting” services which are not required by our DCS).
- Placing field bus devices on the control system LAN can introduce network security issues. Policies that are reasonable to implement for high-level DCS devices may be impossible to implement for low-level field bus devices. For example, there may be low-level devices that do not have password protection against configuration changes.
- There is some risk that different communications protocols may not be compatible. (Fortunately we have not had this problem at SNS).
- It complicates trouble-shooting. Since all manner of devices share the network, they must all be suspect when problems arise.

SNS EXPERIENCE

SNS ICS Network

SNS made the decision to integrate the control system communications infrastructure as much as possible. A single, dedicated, Ethenet-based control system network

* Work supported by SNS through UT-Battelle, LLC, under contract DE-AC05-00OR22725 for the U.S. DOE. The SNS is a partnership of six national laboratories: Argonne, Brookhaven, Jefferson, Lawrence Berkeley, and Oak Ridge.

0-7803-8859-3/05/$20.00 ©2005 IEEE

(dubbed the Integrated Control System (ICS) Network) handles most control system communications. The ICS network handles network communications for the EPICS (Experimental Physics and Industrial Control System) DCS, PLCs, remote I/O, "on/off" controllers, etc. Exceptions include a few programmable logic controller (PLC) systems that use an industry-standard communications network for their remote I/O. Figure 1 shows the basic hardware architecture of the ICS Network.

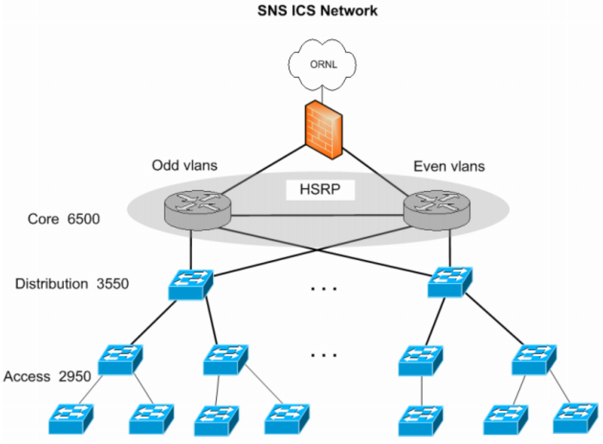


Figure 1: Diagram of ICS network hierarchy.

Table 1 lists the approximate quantities of nodes connected to the ICS network. Quantities are given for equipment on the network now (the "2005" columns) and for when the construction project will be complete (the "2006" columns). Quantities of nodes on the Accelerator Virtual Local Area Network (VLAN) are provided since that is by far our most heavily populated VLAN (and by extension our biggest broadcast domain).

Table 1: ICS Network Node Quantities

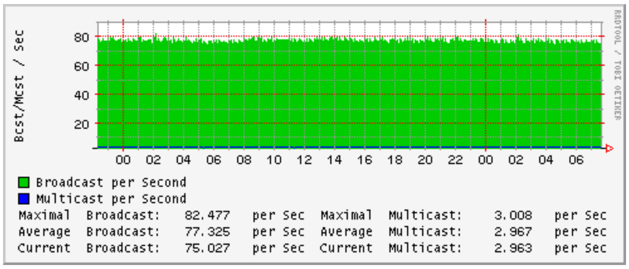
Network Nodes	Accel VLAN		Other VLANs		ICS Network Total	
	2005	2006	2005	2006	2005	2006
EPICS, VME IOCs	110	142	22	26	132	168
EPICS, Diagnostic IOCs	180	302	0	0	180	302
EPICS, Other	77	86	52	60	129	146
Fieldbus Devices	149	164	36	48	185	212
Comm. Services	0	0	113	146	113	146
Other Misc.	12	21	2	2	14	23
Total	516	694	223	280	739	974

Broadcast Rates

SNS is presently using the traditional implementation of EPICS, i.e. there is no central name server. Clients (e.g. the archiver) broadcast requests to prospective servers (e.g. I/O Controllers (IOCs)) for the locations of process variables (PVs) that aren't known to that client. This can at times result in high levels of broadcast traffic, e.g. after a power outage. Another detriment is that incorrect or obsolete PV names result in continued broadcasts as clients continue to search for the bad PV names. The field bus devices on the network must process these broadcasts even though they aren't meant for them. This introduces the risk that at some level of broadcast traffic, field bus devices with minimal processing power won't be able to keep up with the network traffic and may even be unable to operate.

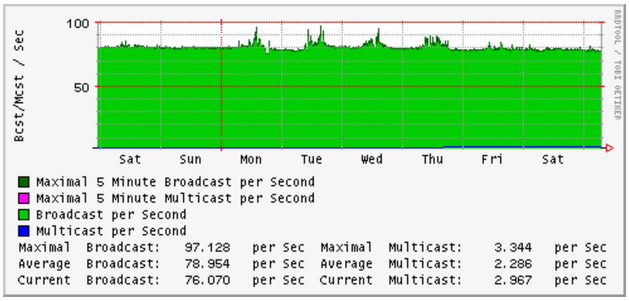
SNS uses VLANs to logically divide ICS network traffic into isolated broadcast domains. The division at this time is by major subsystem (e.g. Accelerator, Cryogenics, Target, Conventional Facilities, etc.). This approach is generally working for us, but there have been some surprises along the way.

Figures 2 and 3 show recent snapshots of the broadcast rates experienced on the Accelerator VLAN, our largest VLAN. As can be seen, the average rate for that period was approximately 80 broadcasts/second with peaks of up to 100 per second. While ideally the rate should be lower, our field bus devices appear to be able to handle rates of this order. We do have some concern that we will start having problems as the broadcast rate scales up, and so contingency plans are being considered (see more below).



```
Maximal  Broadcast:   82.477   per Sec  Maximal  Multicast:    3.008   per Sec
Average  Broadcast:   77.325   per Sec  Average  Multicast:    2.967   per Sec
Current  Broadcast:   75.027   per Sec  Current  Multicast:    2.963   per Sec
```

Figure 2: Recent daily report of broadcast rate for ICS Network Accelerator VLAN.



```
Maximal  Broadcast:   97.128   per Sec  Maximal  Multicast:    3.344   per Sec
Average  Broadcast:   78.954   per Sec  Average  Multicast:    2.286   per Sec
Current  Broadcast:   76.070   per Sec  Current  Multicast:    2.967   per Sec
```

Figure 3: Recent weekly report of broadcast rate for ICS Network Accelerator VLAN.

Last year we had some EPICS configuration problems that caused an unusually large number of broadcasts. Before the problems were corrected we experienced broadcast storms with rates of more than 1,000 broadcasts/second. This huge level of network traffic caused some temperature controllers and even some EPICS I/O Controllers to lock up.

SNS is considering options for reducing EPICS channel access broadcast traffic. One option would be to move field bus devices to their own VLAN. This would set them in their own broadcast domain, isolated from EPICS channel access broadcast traffic. A disadvantage of this approach is that communications between EPICS IOCs and field bus devices would have to be routed between VLANs.

Another option for reducing EPICS broadcast traffic would be to use a central PV name server to provide clients with PV location information. This would eliminate the need for clients to broadcast requests for this information, and should reduce broadcast traffic accordingly.

Multicast Communications

SNS uses PLCs to handle many of our process control tasks. Much of our PLC-to-PLC communications is implemented via Ethernet. For our standard model of PLC, the PLC-to-PLC communications are implemented as IP multicast utilizing the Internet Group Management Protocol (IGMP), with no alternative method available. IGMP snooping is used to constrain multicast traffic within the VLAN. Otherwise, multicast traffic is flooded throughout the VLAN in a manner similar to broadcasts.

SNS has a limited number of PLC-to-PLC interlocks implemented over Ethernet. A watchdog timer is used to force the interlock to "fail safe" should communications be delayed. Recently there was an incident where the watchdog timer for an interlock was frequently timing out. After an intense network sniffing campaign, it was discovered that a network switch was inexplicably pruning one the "multicast-receiving" PLCs from the multicast group. Both PLC and network switch vendors were contacted. One of the solutions we tried was to update our switches' software to a version containing a more complete implementation of IGMP, and that appears to be what cured the problem. We could only conclude that IGMP snooping is new enough that the switch vendor was still getting the bugs out.

Network Security

The SNS ICS network is a "private" network and is isolated from the ORNL network by a firewall. This goes a long way to protect the network from intrusion from the outside. However some of our field bus devices have limited network security features that violate "best practice" guidelines.

The SNS standard model of PLC supports network management via a Simple Network Management Protocol (SNMP) agent which runs on its Ethernet interface module. Per the SNMP standard, requests to a PLC for communications-related data must include a password (a "community string") known by the PLC. Unfortunately, for this model of PLC the password is fixed and the same for every Ethernet module sold. The vendor has indicated that there will soon be an upgrade to fix this problem.

A more general problem is that field bus devices are often not password protected against configuration or programming changes. When such devices are connected to a widely-available network, the chances of accidental or deliberate changes to the devices' configuration increase.

CONCLUSION

SNS has successfully integrated field bus devices and distributed control system equipment on the same network, but has experienced some problems and concerns as the network has grown. Having a single network has proved to be cost-effective and manageable from a construction point of view. However VLANs must be configured and managed to keep network traffic at an acceptable level. The network has to be configured to handle multicasting properly. Network support personnel must exercise a continuous improvement process as network security features mature for field bus devices. Ultimately new initiatives may have to be launched to keep network traffic down to acceptable levels as the network grows in size (e.g. add new VLANS and/or an EPICS name server).

0-7803-8859-3/05/$20.00 ©2005 IEEE