

Issues of Control Networks When Introducing IP *

Nobuo Okabe

Ubiquitous Lab, Yokogawa Electric Corporation

Nobuo.Okabe@jp.yokogawa.com

Abstract

There are many kinds of control networks which have been used in various non-IP network areas, such as BA (Building Automation), FA (Factory Automation) and PA (Process Automation). Recently, many control network technologies have been introducing IP (Internet Protocol) and Ethernet for cost/capabilities benefits. IPv6, in particular, can be a driving force for the movement. However, it can influence entire architectures of control network technologies because it can invalidate implicit premises, i.e. closed networks, which have contributed to the dependability of the systems. This paper review the issues of control networks when introducing IP, and shows that IPv6 is crucial.

1. Introduction

Control networks are different from IP (Internet Protocol) with regard to their history, purposes and technologies. There are numerous technologies of control networks, e.g. FOUNDATION fieldbus [6], PROFIBUS [19], MODBUS [13], BACnet [1] and LonWorks [5], which have been used in various non-IP network areas, such as in BA (Building Automation), FA (Factory Automation) and PA (Process Automation), which have different requirements (see Fig. 1). Multiple technologies also coexist within a single system usually because the system's requirements are diverse. Their networks have been closed ones which have contributed to system's dependability.

Many control network technologies have been introducing IP (Internet Protocol) and Ethernet recently e.g. FOUNDATION fieldbus HSE, PROFINet, MODBUS/IP and BACnet/IP, which improves their cost and capabilities. IPv6, in particular, can be a driving force for the movement especially. However, it can also potentially influence their entire architecture. For example, if the prerequisite condition of

BA	- Controlling devices in buildings: lights, security, air conditioning, elevators, etc. - Assured response time: 100 msec - 1sec
FA	- Controlling manufacturing tools in factories: NCs, robots, assembling machines/lines, etc. - Cost > Reliability - Assured response time: 1 msec - 10 m sec
PA	- Controlling process plants: oil, chemical, medical, iron, paper, etc. - Need highly reliability, explosion-protection - Assured response time: 100 msec - 1 sec

Figure 1. Applications

a closed network is invalidated, unexpected traffic will appear in the control network which influences QoS (Quality of Service) of the network. If unexpected traffic includes malicious packets, it will influence the security of the network. In the next section, we summarize issues of control networks when introducing IP and Ethernet.

2. Issues of Control Networks

2.1. Protocol Architecture

Several control network technologies, e.g. BACnet/IP and MODBUS/IP, introduced IP not to the network layer but to the link layer (see Fig. 2), which cannot use the network layer capability of IP, e.g. IP routing. In other words, those technologies are not fully inter-operable with IP. Users who need inter-operability among control network technologies, e.g. [14], have to depend upon gateways which always have drawbacks, e.g. cost, protocol intransparency and potential points of failure. Therefore, a control network technology should fulfill the following requirements when introducing IP: 1) being inter-operable with other control network technologies, 2) inheriting user data of the control network technology, 3) being fully inter-operable with IP and 4) sharing important capabilities among other control network technologies.

*This research is supported/funded by the Ministry of Internal Affairs and Communications of Japan.

Application	BACnet Application Layer					
Network	BACnet Network Layer					
Link	IEEE802.3 Type-1	MS/TP	PTP	LonTalk	Virtual Link Layer	
					UDP	IP
Physical	IEEE802.3	ARCNET	EIA-485	EIA-232		IEEE802.3

Figure 2. Network architecture of BACnet

The following are proposals to enable the above requirements. First, control network technologies should introduce IP, especially IPv6 (see in Section 2.2), as the network layer. Second, functionalities of the control network technologies should be considered as the application layer. Third, capabilities which should be common among control network technologies are implemented below the application layer. The capabilities discussed in this paper are also addressed there.

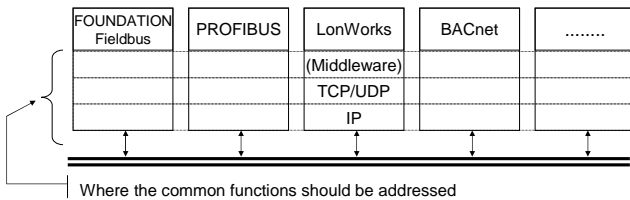


Figure 3. Proposed network architecture

2.2. Network Topology

Network topology of control networks is simple because of their requirement of high availability and the limited capability of their network technologies. In the former case, dual ring topology based upon a token passing mechanism, e.g. FDDI (Fiber Distributed Data Interface), is common if high availability is required. They can use non-ring topology when introducing Ethernet. However, the protocol of redundancy is dependent upon their topology, e.g. RPR (Resilient Packet Ring, IEEE802.17) for ring topology and RSTP (Rapid Spanning Tree Protocol, IEEE802.1w) for non-ring. Therefore, the network topology must be chosen according to the requirements of the system and the limitations of the technologies used. The history that many LANs (Local Area Network) have been changed from FDDI to Ethernet may be useful for cases of control networks.

In the latter case, IP makes control networks scalable. Multiple technologies can be interconnected in LAN and multiple sites separated geographically can be connected with WAN (Wide Area Network), e.g. the Internet. Those important requirements have been raised, but not been fulfilled yet. At this moment, IPv4 and private addresses are used for the partial solution which requires NAT (Network Address Translation). NAT harms the scalability, the sim-

plicity and the operational cost of the systems as considering long-term solutions. Therefore, IPv6 is essential for introducing IP because of its huge address space.

2.3. Network Security

Security of control networks have not been considered sufficiently. For example, current specifications of FOUNDATION fieldbus and MODBUS do not mention security. BACnet has the capability of network security, however, which is insufficient [9, 22]. Improvement is on-going [20]. Security of LonWorks supports only server authentication using challenge and response before starting a session. The security of LonWorks is weaker than BACnet because mutual authentication and packet based security, i.e. authentication, integrity and confidentiality, are not provided.

Control networks must be concerned with security as much as IP networks do because security incidents have occurred on control networks, and there are concerns for safety of social infrastructure [3, 7, 17]. This section describes security about unicast/multicast and against DoS (Denial of Service) attacks.

2.3.1 Unicast

Security is being reconsidered in many control network technologies recently [18, 20]. The common idea is to rely on the firewall model which assumes specific network topology. However, recent incidents of computer virus show that the firewall model is not always a complete solution. It is challengeable to manage security of normative devices with firewalls. Wireless technologies can expose network traffic behind firewalls easily. Therefore, end-to-end security mechanisms which do not need to assume any specific network topology are necessary. However, the small embedded devices commonly used in control networks have limited computational performance because of their restricted requirements of cost, physical size and power consumption. Therefore, the security mechanism for control networks should not overload small devices.

The authors are proposing a security architecture [15] which can meet the above requirements. That is based upon IPsec [11] and KINK [21] which can enforce security independent of applications and can be suited to limited computational performance as it does not use the public key cryptography.

2.3.2 Multicast

Multicast is necessary because several control network technologies have already used the capability with their own network layers, e.g. discovering nodes or services, controlling a set of devices at once. However, multicast security is challengeable [12]. Most difficulty is caused by dynamism

of multicast group, allowing nodes to enter/leave the multicast session without the permission or knowledge of other nodes. Many issues resulting from the difficulty can be abstracted into the issues of key distribution and management. There is no unified solution which can suit a variety of multicast applications. Therefore, multicast applications used by control network technologies should first be studied before discussing a multicast security mechanism.

2.3.3 Denial of Service Attacks

In the case of control networks, the damage caused by DoS can be serious. For example, it would take about a week to restart a huge process plant if it were stopped accidentally, and cause a huge financial loss while the plant is stopped. DoS against plants are becoming real, but closed networks and firewalls, which are the common countermeasures, are far from a complete solution. Desired countermeasures against DoS should fulfill the following requirements: 1) It protects the bandwidth of the network and CPU power of end nodes, i.e. servers and devices, in control networks. 2) Protecting mechanism should not be run in the devices because their performance and resources are limited. The devices may have ACL (Access Control List), however, which is far from the counter measure. Their limited CPU resources will be consumed with ACL processing when facing DoS. 3) In critical systems, programs/data of devices are updated infrequently, e.g. once every few years. It is not allowed for devices to update their programs/data autonomously. It means that devices can not get up-to-date signatures of malicious packets or something timely.

For the above reasons, it is better to protect DoS by network, i.e. routers and switches, than by end nodes. In critical systems, network traffic is predictable because the entire system includes networks have been designed carefully (see Section 2.5). Therefore, it can not be difficult to detect/drop the flow of DoS (see Figure 4). sFlow [16], SNMP [4], Diff-serv [8], IEEE802.1p and packet filtering can be candidates for the solution.

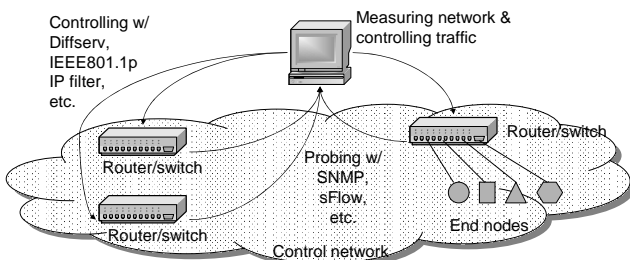


Figure 4. A counter measure against DoS attacks

2.4. Redundancy

The redundancy of a system is composed of 1) networks, 2) points of contact between networks and end nodes, 3) end nodes. Critical systems have often used redundant ring topologies and applications which are aware of specific technologies of redundancy (see Figure 5). In other words, 1), 2) and 3) have been coupled tightly.

The systems should use redundancy technologies which are common among switches and routers when introducing IP. The technologies of layer 2 are more suitable to 1) than the ones of layer 3 when considering assured response time described in Table 1. For example, Port Aggregation(IEEE802.3ad), RSTP(Rapid Spanning Tree Protocol, IEEE802.1w) and RPR(Resilient Packet Ring, IEEE802.17) can be the candidates for the solution. For 2), network interfaces which are aware of 1) are necessary. 3) should also be aware of 1) and 2).

2.5. Quality of Service

The management of network bandwidth is important for highly reliable systems. To achieve this goal, for example, applications have been designed not to exceed their given bandwidth (see Figure 5). Other example is that communications are scheduled by arbiters with a token of application layer (see Figure 6). The common presupposition, i.e. every device should keep its role and there should be no unknown device, will be broken if the networks are not closed. It can be a counter measure to enforce QoS policy on the network, i.e. routers and switches, with Diffserv or IEEE802.1p if the traffic of the system is predictable. The granularity of identifiable flow can be coarse resulting from IPsec which hides information above the IP layer, i.e. port numbers, upper layer protocol and data. However, it can be solved if the end nodes specify DSCP (DiffServ Code Point) in their outgoing packets, described in [2].

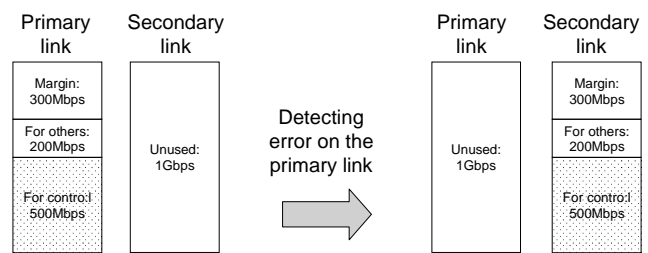


Figure 5. An example of QoS

2.6. Hard Real-time

Hard real-time of a system has two kind of factors, i.e. one is end node and the other is network. The former, real-time OS or hardware architecture, is beyond the scope of

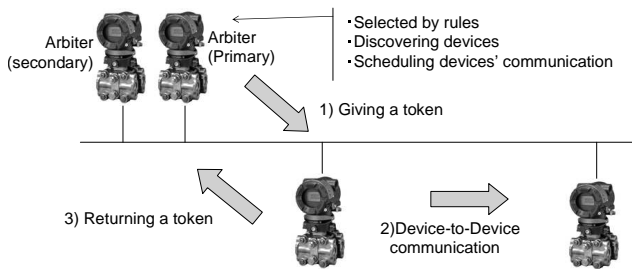


Figure 6. Other example of QoS

this paper. It is inevitable to define the scalability of the system, i.e. within LAN or multiple LANs connected with WAN when discussing the latter. At this moment, LAN seems reasonable for control networks. However, WAN will have to be considered in the future because the performance of WAN is being improved rapidly.

2.7. System Operation

Network operation, i.e. operation of routers and switches, is inevitable when introducing IP. However, operators of control systems should not be expected to network operators. Therefore, network management tools should abstract network operation to help them.

Other operational issue is the installation cost if there are a huge number of devices. Current control systems, which did not introduce IP, have already faced this issue. The auto-configuration mechanism of IPv6 is necessary for this issue. However, it is not enough. The authors are studying an autonomous bootstrap mechanism [10] which is based upon IPv6 and [15].

2.8. Network Emulation and Simulation

If a system uses network capabilities described in Section 2.3, 2.4, 2.5 or 2.6, it is necessary to evaluate and verify the capabilities. Part of the activity should be done without actual systems or networks because actual systems/networks are not readily available for those purposes. Therefore, network simulation and emulation is important.

3. Summary

It brings the benefit of cost and capabilities to introduce IP to control systems. However, it can invalidate implicit premises which have contributed to the dependability of the systems. This paper review the issues of control networks when introducing IP, and shows that IPv6 is crucial. The issues are network topology, security, QoS, redundancy, network measurement, traffic control, hard real-time, system operation and network simulation/emulation.

References

- [1] ASHRAE. *ANSI/ASHRAE Standard 135-1995, BACnet A Data Communication Protocol for Building Automation and Control Networks*, 1995.
- [2] R. Atarashi, S. Miyake, et al. QoS Policy Control by Application on the Next Generation Internet Technology. *IEICE transactions on Information and Systems*, Aug. 2002.
- [3] E. Byres. Plant network security: Can't happen at your site? inTech, ISA, Feb. 2002. http://www.isa.org/Content/ContentGroups/InTech2/Features/20023/February6/Cant_happen_at_your_site_.htm.
- [4] J. Case, M. Fedor, et al. A Simple Network Management Protocol (SNMP). RFC1157, 1990.
- [5] EIA. *EIA/CEA-709.1-B, Control Network Protocol Specification*, 2002.
- [6] Fieldbus Foundation. *FF-581-1.3, FOUNDATION Specification: System Architecture*, 2003.
- [7] J. Gerston. Water and Wastewater Utilities Enhance System Security. In *Texas Water Resources*, volume 27. Texas Water Resources Institute, Dec. 2002.
- [8] D. Grossman. New Terminology and Clarifications for Diff-serv. RFC3260, 2002.
- [9] D. G. Holmberg. BACnet Wide Area Network Security Threat Assessment. NISTIR 7009, NIST, Jul. 2003.
- [10] A. Inoue, M. Ishiyama, et al. A Secured Autonomous Bootstrap Mechanism for Control Networks. Annual Review of Communications, Volume 57, International Engineering Consortium, Nov. 2004.
- [11] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. RFC2401, 1998.
- [12] P. Kruus. A survey of multicast security issues and architectures. In *Proc. 21st National Information Systems Security Conference*, 1998.
- [13] MODBUS.ORG. *Modbus Application protocol V1.0*, 2002.
- [14] OBIX. Open Building Information eXchange. <http://www.builtalk.com/index.html>.
- [15] N. Okabe, S. Sakane, et al. Security Architecture for Control Networks using IPsec and KINK. In *SAINT2005, The 2005 International Symposium on Applications and the Internet*, Jan. 2005.
- [16] P. Phaal, S. Panchen, et al. InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks. RFC3176, 2001.
- [17] K. Poulsen. Slammer worm crashed Ohio nuke plant network. SecurityFocus, Aug. 2003. <http://www.securityfocus.com/news/6767>.
- [18] Process Control Security Requirements Forum. NIST. <http://www.isd.mel.nist.gov/projects/processcontrol/>.
- [19] PROFIBUS International. *IEC 61158, Digital Data Communication for Measurement and Control - Fieldbus for Use in Industrial Control Systems*, 1999.
- [20] D. Robin. IBACnet Security Messages. SPPC 135 WG Document DR-029-6, BACnet committee, Mar. 2004.
- [21] M. Thomas and J. Vilhuber. Kerberized Internet Negotiation of Keys (KINK). draft-ietf-kink-kink-05.txt, 2003.
- [22] J. Zachary, R. Brooks, et al. Secure Integration of Building Network into the Global Internet. NIST GCR 02-837, NIST, Oct. 2002.