SANDIA REPORT
SAND2007-0383P
Unlimited Release
September 2007

Impacts of IPv6 on Infrastructure Control Systems

Brian Van Leeuwen

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2007-0383P
Unlimited Release
September 2007

Impacts of IPv6 on Infrastructure Control Systems

Brian Van Leeuwen
Critical Infrastructure Systems
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0672

Abstract

This document presents information on the impacts of adopting Internet Protocol version 6 (IPv6) into infrastructure control systems. The investigation was performed by members of Sandia National Laboratories and funded by the Department of Energy's (DOE) National SCADA Test Bed (NSTB) Program. Specifically, the document presents a brief background and description of the features of IPv6, details on how IPv6 may be implemented in a control system, and potential issues that may surface related to reliability and security.

IPv6 networking is being adopted and brings additional functionality when compared to IPv4 that will be useful to control system applications. Thus, control system operators should begin their planning by developing an IPv6 transition strategy that will enable the planned introduction of IPv6 compatible components into their control system infrastructures. In the near term the adoption process should proceed with education and control system architecture planning for the introduction of IPv6.

Acknowledgements

The author would like to acknowledge that the work that produced the results presented in this paper was funded by the U.S. Department of Energy/Office of Electricity Delivery and Energy Reliability (DOE/OE) as part of the National SCADA Test Bed (NSTB) Program. In addition, the author would like to acknowledge the various industry participants who provided valuable input concerning their knowledge and views with respect to IPv6.

Executive Summary

This document presents information on the impacts of adopting Internet Protocol version 6 (IPv6) into infrastructure control systems. The investigation was performed by members of Sandia National Laboratories and funded by the Department of Energy's (DOE) National SCADA Test Bed (NSTB) Program. Specifically, the document presents a brief background and description of the features of IPv6, details on how IPv6 may be implemented in a control system, and potential issues that may surface related to reliability and security.

The research approach used by the investigation team included identifying the general requirements of IP networks that support critical infrastructure control systems. A typical electric utility control system architecture was selected as an example infrastructure and examined at varies operational levels. Control system device and network equipment used in the various levels were identified and examined to determine the implications of transitioning to IPv6. Specific protocols used in control systems were investigated to assess their readiness levels for IPv6 support. In addition, a number of equipment vendors and utilities were contacted to obtain their views on industry's adoption of IPv6.

At the time of this report release no vendor of control system equipment or devices had yet developed a product that requires IPv6. The vendors express concern over the lack of a broadly accepted transition strategy that supports a secure IPv4/IPv6 transition that could drive the demand for IPv6 devices. Security and reliability are also a major concern impeding the adoption of an IPv4/IPv6 transition. However, a factor that will encourage the adoption of IPv6 is a requirement by the U.S. Office of Management and Budget (OMB) that specifies that all federal agencies must support IPv6 on their networks by June 2008.

Support of IPv6 is more common for equipment and applications used at the organization's operation centers. Many applications used in an infrastructure operation centers operate on common workstation operating system. Common operating systems such as Linux and Microsoft products support both IPv6 and dual stack IPv4/IPv6 requirements. However, no application or equipment was found to require IPv6.

It is clear that the adoption of IPv6 will occur over time and there will be a significant period of IPv4/IPv6 coexistence. Thus, organizations with significant Internet utilization should develop a transition strategy for adopting IPv6. Key aspects of a transition strategy include education, equipment upgrades, architecture planning and development, IPv4/IPv6 transition mechanism selection, and testing. Some organizations that have begun the transition process are publishing their experiences, which can provide infrastructure organizations a wealth of valuable information. However, at this time no organization has described transitioning a control system to IPv6. Since infrastructure control systems have increased reliability and security requirements the transition to IPv6 must be done very carefully so as to not introduce near-term reliability and security risks.

The *Roadmap to Secure Control Systems in the Energy Sector*[1] established as Goal 2 (Develop and Integrate Protective Measures) the following as a key challenge: Security upgrades are hard to retrofit to legacy systems, may be costly, and may degrade system performance. Thus organizations transitioning their infrastructure control systems to IPv6 should diligently address the potential security implications of both an IPv4/IPv6 transition network and an IPv6-only network. Note that an important feature of IPv6 that can enhance security is the requirement that implementations support IP Security (IPsec). However, realizing this potential security improvement will continue to depend on well-coded applications, effective key management, and a strong device identity structure. In addition, threats have already been identified with the deployment of IPv6. Some threats are similar in nature to those that impacted IPv4 networks; however, new threats have also been identified that are specific to IPv6 deployments.

The U.S. Office of Management and Budget (OMB) requires all federal agencies to support IPv6 on their networks by June 2008. According to OMB congressional testimony[2], the studies by the U.S. Government Accountability Office[3] and the U.S Department of Commerce[4] that led to this requirement both indicate that significant technical and economic risks can be associated with failure to adequately plan for and appropriately schedule IPv6 adoption.

IPv6 networking is being adopted and brings additional functionality when compared to IPv4 that will be useful to control system applications. Thus, control system operators should begin their planning by developing an IPv6 transition strategy that will enable the planned introduction of IPv6 compatible components into their control system infrastructures. In the near term the adoption process should proceed with education and control system architecture planning for the introduction of IPv6.

[1] *Roadmap to Secure Control Systems in the Energy Sector*, U.S. DOE and U.S. DHS, prepared by Energetics Incorporated, January, 2006, http://www.controlsystemsroadmap.net/

[2] *Mandate for IPv6*, Office of Management and Budget. http://www.whitehouse.gov/omb/legislative/testimony/evans/evans052905.html; June 2006.

[3] *Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks*; U.S. Government Accountability Office Report to Congressional Requesters; May, 2005. http://www.gao.gov/new.items/d05471.pdf

[4] *The Evolving Internet: A Technical and Economic Assessment of Internet Protocol, Version 6 (IPv6),* U.S. Department of Commerce, January 2006.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

The research presented in this report is intended to help infrastructure organizations to begin the transition process to IPv6 (Internet Protocol version 6). Key to a successful transition process of adopting IPv6 is structuring a vision and strategy and, if necessary, revising the strategy as new experiences become available. The report is structured to provide an overview of the benefits and potential issues of adopting IPv6. Also included are descriptions of transition approaches and how to proceed with adopting IPv6.

The remainder of this introductory section consists of a description of why IPv6 was developed, a description of the U.S. Government's strategy on IPv6 adoption, and an overview of industry views concerning IPv6.

In Section 3.2 the new features of IPv6 are introduced. Brief descriptions indicate the potential benefits of adopting IPv6 in an infrastructure organization's control system. Section 3.3 includes, for example, discussion of an electric utility's control system architecture, an overview of the network communication to move data and control signals between system layers, and an overview of the current state of IPv6 support by various software and device/equipment products.

Section 3.4 describes how an organization would transition to an IPv6 communication network. Included is a description of where to obtain IPv6 addresses. Since the transition to IPv6 will occur over many years there will be a period of IPv4/IPv6 coexistence. This section includes descriptions of transition methods. Since network security is critical to the operation of an infrastructure system, Section 3.5 is included to describe security and vulnerability issues of IPv6 that can impact operations.

Section 4 states the primary conclusions of the work described here about the nature and state of the process of transition to IPv6. Section 5 recommends cybersecurity policy and strategy for reducing risk during the transition from IPv4 to IPv6.

1.1 Background

The U.S. Office of Management and Budget (OMB) requires all federal agencies to support IPv6 on their networks by June 2008 [1]. The studies by the U.S. Government Accountability Office [2] and the U.S Department of Commerce [3] that led to this requirement both indicate that significant technical and economic risks can be associated with failure to adequately plan for and appropriately schedule IPv6 adoption.

1.1.1 Description

IPv6 is a network layer or Layer 3 protocol standard that is used by electronic devices to exchange data across a packet-switched network. IPv6, as a network layer protocol, is tasked to handle the routing of data between points in a network, be it a data network or a control system network. Network layer protocols are *best effort* protocols, in that they don't guarantee delivery or the correctness of the received data. Network protocols, including IPv6, depend on upper layer protocols such as TCP to provide important functions not provided by the network layer such as reliable delivery and congestion control.

IPv6 supports a much larger address space than IPv4. The increased address space is the primary driver for IPv6; however, other new features such as auto address configuration, security enhancements, and prioritization through quality of service (QoS) are expected to be the real drivers for industrial adoption.

IPv6, its various new features, and its implementations are described in various Internet Engineering Task Force (IETF) Request for Comments (RFC) documents. The overall IPv6 protocol is described in [RFC-2460].

1.1.2 Historical Information

IPv6 was developed as a replacement for the current dominant network layer protocol on the Internet: IPv4. IPv6 was primarily developed to address the problem of the IPv4 address depletion. The IPv4 address depletion issue is impacting the international community more significantly than it is impacting the U.S. since the U.S. received a much larger portion of IPv4 addresses than other parts of the world with rapidly expanding economies. For example, China is large supporter of IPv6 since they will benefit greatly from the additional address space. Their interest lies not only in the opportunity for additional workstations but also the interest of increasing numbers of IP-enabled devices that monitor information flows and other monitoring and control devices. Thus the IPv6 adoption rate is expected to be much more pronounced in the international community than in the U.S., however, the U.S. Federal Government has established requirements for adopting IPv6 in its organizations.

1.1.3 Significance

The transition to IPv6 will impact the entire group of Internet users at some time. IPv6 will impact these users at different times and in different ways since the Internet consists of millions of smaller domestic, academic, business, and government users. The users depend on different applications, which include various information services, such as email, file transfers, monitoring and control, VoIP, online chat, and web pages.

The U.S. Office of Management and Budget (OMB) has specified that all federal agencies must support IPv6 on their networks by June 2008 [1]. This specification applies only to network infrastructure equipment, such as backbone routers, switches, and hardware firewalls. The specification does not mandate that an agency must enable IPv6 on every component of its extended network. However, the OMB clearly desires to get the U.S. on a path to adoption of IPv6.

The U.S. Department of Defense (DoD) already requires IPv6 support for many of its hardware bidding specifications. Many DoD requirements include remote data acquisition or mobile IP and thus receive IPv6 attention because of the IPv6 features that enable these capabilities.

1.1.4 Literature Review

Citations to key IPv6 documentation and descriptive material from U.S. government agencies, industry associations, technology providers, standards groups, and knowledgeable individuals appear throughout this report.

In particular, the *Request for Comment* (RFC) collection is a series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies. The serialized RFCs comprise a continuous historical record of the evolution of Internet standards and are cited extensively in this report. For more details about RFCs and the RFC process, see [RFC 2026], *The Internet Standards Process, Revision 3*.

RFC citations in this report are of the form "[RFC-xxxx]", where xxxx represents the serial number assigned to the RFC by the Internet Society's RFC Editor. References to the individual RFCs do not appear explicitly in this report's reference section, *Appendix A: References*. The RFCs themselves can be accessed at http://www.faqs.org/rfcs/.

1.2 Purpose

The objective of the study described in this report is to identify the impacts of IPv6 and IPv4-to-IPv6 transition on infrastructure information and process control systems.

1.2.1 Reason for Investigation

Since an organization's information system is key to its operations, a vision and strategy must be developed to guide the organization's migration to IPv6. In general, the migration to IPv6 will impact many aspects of an organization's information systems. The migration will impact information system applications and platforms, network services and devices, organization communication system architectures, and policies related to information system operations and security.

In particular, infrastructure organizations such as electric, natural gas, oil, water, sewage, and railroads depend on a multi-layer information system. The information system components range from business operation systems to process control systems (PCS) that include distributed control systems (DCS), automated control systems, and supervisory control and data acquisition (SCADA) systems. These systems support the organization's process functions such as electric generation and transmission functions. The control systems are comprised of various applications, data acquisition equipment, control equipment, and communication links. Infrastructure organizations must consider how to transition these various information system network layers to IPv6 in a safe, reliable, and secure manner and when to begin the transition.

1.2.2 Roadmap Challenges

The *Roadmap to Secure Control Systems in the Energy Sector* [4] established as Goal 2 (Develop and Integrate Protective Measures) the following as a key challenge: Security upgrades are hard to retrofit to legacy systems, may be costly, and may degrade system performance. Thus organizations transitioning their infrastructure control systems to IPv6 should diligently address the potential security implications of both an IPv4/IPv6 transition network and an IPv6-only network. Note that an important feature of IPv6 that can enhance security is the requirement that implementations support IP Security (IPsec). However, the improved security features still depends on well-coded applications, effective key management, and a strong device identity structure. In addition, threats have already been identified with the deployment of IPv6. Some threats are similar in nature to those that impacted IPv4 networks; however, new threats have also been identified that are specific to IPv6 deployments.

1.2.3 Audience

The intended audience of this report includes PCS device/equipment vendors, asset owners, and other industry participants. The recommendations provided in Section 5 are intended to provide this audience guidance on selecting IPv6 for their systems.

1.2.4 Desired Response

This report is intended to help device/equipment vendors and asset owners understand the benefits and potential consequences of implementing IPv6 in PCS. It also will help the audience avoid potential pitfalls with adopting IPv6 in their PCSs and help with selecting a secure IPv4/IPv6 transition approach.

1.3 Scope

The objective of the investigation described in this report is to provide the necessary background information on IPv6 from a technology standpoint as well as its adoption into information systems and methods to transition IPv4 to IPv6. IPv6 impacts on security are also presented in the report.

1.3.1 Extent and Limits of Investigation

Infrastructure control systems employ devices that interface objects in the physical world to the control system. These devices include remote terminal units (RTUs), programmable logic controllers (PLCs), and intelligent electronic devices (IEDs). Since the IP communication interfaces on these devices are independent of their specific function and name, the content of this report is applicable to all the devices. In this report RTUs, PLCs, and IEDs are referred to as *field hardware* unless referenced to a specific industry.

1.3.2 Goals

The investigation described in this report has a goal of establishing secure infrastructure control systems. This goal aligns with the *Roadmap to Secure Control Systems in the Energy Sector* [4] Goal 2 (Develop and Integrate Protective Measures). More specifically the goal of the investigation is to have organizations securely transition their infrastructure control systems to IPv6. Included in the goal is to have organizations select a secure IPv4/IPv6 transition network and an IPv6-only network.

1.3.3 Objectives

In pursuit of the above listed goals the investigation included the following objectives:

1. Identify features of IPv6 and its benefit to infrastructure control systems.
2. Identify current state of IPv6 adoption in information systems.
3. Obtain views from industry concerning IPv6 adoption. Views from asset owners and views from device/equipment manufactures are included in the investigation.
4. Perform initial investigation of known security issues when using IPv6.
5. Identify IPv4/IPv6 transition approaches.
6. Provide recommendation to industry concerning adoption of IPv6 in their infrastructure control systems.

2 Approach

2.1 Methods

The investigation included reviewing the Internet Engineering Task Force (IETF) documents that describe IPv6. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture. The IETF provides descriptions of protocol standards, including IPv6, via Request for Comments (RFCs). Although many of the RFCs describe protocol standards, other RFCs provide information or application guidance to protocol users and implementers.

Additional literature searches were performed to obtain other research papers on issues surrounding both the IPv6 protocol and its implementation in information systems.

The expert opinions of a number of industry researchers, device/equipment vendors, and other infrastructure and industry participants have been incorporated as well. These were obtained either through direct contact or from recently published interviews discussing industrial control systems.

2.2 Assumptions

The material presented in this report assumes a process control system that uses networked communication based on IP. It is also assumed that a single-step adoption of IPv6 is not possible and that there will be a lengthy period of IPv4 and IPv6 coexistence.

2.3 Procedures

The research team performed the following activities in this research task.

1. Investigate current literature that described the IPv6 standard, its various supporting protocols, and its state of development.
2. Research concepts on how IPv6 will benefit to infrastructure control systems.
3. Communicate with asset owners and device/equipment manufactures concerning their knowledge of the IPv6 protocol suite and plans for IPv6 adoption.
4. Perform initial investigation of known security issues associated with IPv6. Investigation included consulting with networked system security analysts.
5. Investigate IPv4/IPv6 transition approaches.
6. Develop a recommendation to industry concerning adoption of IPv6 in their infrastructure control systems.

— This page intentionally left blank —

3 Results and Discussion

Following is a summary listing of the main issues that were identified in the industry outreach. Detailed information of the various participants and a more lengthy description of their opinions and feedback are included in Appendix B of this report.

1. For control systems, no current device/equipment, protocols, or software *require* IPv6. However, vendors are planning to support IPv6 and, in cases, have prototype environments in place.
2. Some field device vendors have introduced beta versions of IPv6 enabled devices; however, there is concern that it is still too risky to commercialize these devices.
3. Some device/equipment vendors believe IPv6 provides opportunity to implement improved security. However, others noted that the addition of IPv6 security mechanisms might be too much of a burden on embedded systems.
4. There is a concern related to IPv6 address allocation and how internet service providers (ISPs) are to assign these addresses.
5. It was noted that Network Address Translation (NAT) while dealing with the address exhaustion issue creates new limitations related to peer-to-peer communications, mobility, and ad hoc connectivity. Thus the need to transition to IPv6.
6. An additional driver for adoption of IPv6 is the potentially large increase in wireless devices providing data from system sensors.
7. An additional driver, that is not yet present, is the development of applications that depend on IPv6 features such as multicast, security, mobility support, and address auto-configuration.
8. It was cautioned that the transition to IPv6 brings potential new avenues of attack. These avenues are neither better nor worse than IPv4 but they do require new considerations.
9. The most significant challenge to adopting IPv6 is the development of a workable IPv4/IPv6 transition strategy and maintaining an IPv4/IPv6 infrastructure.
10. Implement dual stacks during the transition to support both IPv4 and IPv6 applications.
11. IPv6 has benefits over IPv4 but applications that require IPv6 need to be developed before we see an increased adoption rate.
12. The adoption rate of IPv6 at the international level will require that U.S. organizations adopt at an increasing rate. Thus vendors must support IPv6 to hold the interest of the international market.

3.1 State of IPv6 Deployment and Availability

Initial support and availability of IPv6 are expected to come from service providers from international companies. Service providers in Asia such as NTT and KDDI have started IPv6 testing and offering preliminary IPv6 hosting and gateway services [5]. In general, the two primary issues that are preventing the more rapid adoption of IPv6 by service providers are:

- No key applications require IPv6 as this is being written. Service providers are driven by profit and if there is no demand for IPv6 the upgrade to IPv6 is difficult to justify.
- The complexity and cost associated with the adoption of IPv6 and supporting the transition to IPv6 with IPv4/IPv6 dual mode support. As with the adoption of any new protocol, there are concerns with stability issues and security issues. These issues are further compounded by the lack of training, operational experience, and IPv6 network management tools.

The adoption of IPv6 will occur over time resulting in a long period where IPv4 and IPv6 will coexist. This fact has led to the development of techniques to manage IPv6 and IPv4 networks simultaneously via dual mode mechanisms. However, this approach is less than ideal because of the increased management load for network administrators. Additional details on mechanisms that support IPv4/IPv6 networks are included in Section 3.4.

However, IPv6 does have features that are expected to benefit applications. It is expected that once application begin to require IPv6 for their operation that service providers will accelerate their deployment. As service providers increase their deployment of IPv6, application developers are expected to increase their development of applications that require IPv6-only features.

3.2 Features of IPv6 and its Benefits to Infrastructure Control Systems

As indicated above IPv6 will support a much larger address space when compared to IPv4. The increased address space is the primary driver for IPv6, however, there are other new features such as auto address configuration, security enhancements, and prioritization through quality of service (QoS) that could be the real driver for industrial adoption. IPv6, its various new features, and its implementations are described in various Internet Engineering Task Force (IETF) Request for Comments (RFC) documents. The overall IPv6 protocol is described in [RFC-2460]. See [6] for the current status of IPv6.

Infrastructure information systems can benefit from the new or extended features of IPv6 if their system applications are developed or modified to use IPv6 features. In many cases, middleware is used between the application and the network interfaces. Examples of middleware solutions include CORBA, .NET, and Java RMI. Thus application or middleware must support the new or extended features of IPv6 for the most effective operation. Following are descriptions of features of IPv6 that should be attractive for infrastructure control systems.

3.2.1 Increased Address Space

IPv6 was primarily developed to eliminate the IPv4 address depletion problem. IPv6 increases the number of available Internet addresses from 2^{32} to 2^{128} (e.g. 4 bytes versus 16 bytes of addressing). Since the IPv4 address depletion problem has been an issue for some time, a method to deal with the problem prior to extensive adoption of IPv6 has been implemented. However, the address depletion work-around has introduced different problems.

An approach to tackle the address exhaustion problem uses a technique called Network Address Translation (NAT) to conserve public, globally routable IPv4 addresses. This is achieved by placing NAT devices at the boundary between private data networks and the public Internet so that multiple nodes within the private data network can share the same public IPv4 address when communicating over the public Internet.

Many types of information systems address the IPv4 address shortage with NAT. However, a NAT based approach imposes limitations on the end-to-end model of internet connectivity. Communication approaches using the standard client/server model works well in a NAT based network. NAT based solutions, however, do not work so well when other communication models such as peer-to-peer or publish-subscribe communication are used. Peer-to-peer and publish-subscribe communications are used by some protocols used in control systems [7]. An increasing number of IP communication-capable field devices provide status feedback and control functions for use in process control systems. Example electric utility applications that require more field devices (e.g., IEDs and PLCs) with bidirectional communication capability include Wide Area Measurement System (WAMS), Wide-Area Stability and Control System (WACS), and Advanced Distribution Automation (ADA) [7]. This bidirectional communication is beyond the abilities of NAT. Other undesirable side effects introduced by NAT include difficulty in network troubleshooting, network administration, and implementing security protocols such as IPsec.

3.2.2 Address Auto-configuration

IPv6 also enables the automatic allocation and changing of IP addresses. Since more nodes, whether they are workstations or simple IP addressable sensor or control devices, are expected to make up information systems there is a need for address auto-configuration. Address auto-configuration will help ease the need for administration of a dynamic host configuration protocol (DHCP) infrastructure and mitigate addressing issues associated with mobile computing. An IPv6 communication network can perform either stateless or stateful address auto-configuration.

Stateless auto-configuration by an IPv6 node occurs when the node is connected to the communication network. The node will send a link-local multicast request for its configuration parameters and a router will respond with a router advertisement packet that contains network-layer configuration parameters. The stateless auto-configuration is used if the network does not require the use of any specific addresses. Note that even if no IPv6 router is on the network, IPv6 nodes on the same link can communicate with each other because they have automatically generated link-local addresses. These link-local addresses are derived from the node's MAC address. The major beneficiaries of this capability are nodes that depend on ad hoc connections. Thus the capability could be useful for the creation of ad hoc wireless control systems [RFC-2462].

IPv6 also offers a stateful auto-configuration capability that employs a server to distribute addresses and configuration information. This approach can use DHCPv6 or can simply be manually configured.

3.2.3 Hierarchical addressing

IPv6 addresses are organized in a hierarchical manner to facilitate scaling, aggregation, and routing functions. The global routing prefix and subnet identifier of an IPv6 address represent the three basic levels at which addresses are hierarchically constructed; global, site-local, and link-local. This partitioning reflects the topography of the Internet as a whole and results in backbone routers have much smaller IPv6 routing tables. Smaller routing tables increase routing efficiency and provide faster routing, through faster route lookup and reduced latency. It is expected that the IPv6 hierarchal address structure can benefit in organizing network connectivity for infrastructure system management and control applications [8].

Link-local and site-local addresses are used within the organization. Link-local addresses are used to support auto-address configuration and neighbor-discovery functions. Routers should not forward link-local addresses to other links. Site-local addresses are limited to use within the organization and routers should not forward these addresses outside the organization.

3.2.4 Multicast and Anycast Addressing

IPv6 is required to support multicast, both on the local link and across routers, for specific senders to communicate with specific groups of receivers. Broadcast is supported in IPv6 as a specific single hop multicast. A number of predefined address prefixes are used in IPv6 to enable the multicast function. In contrast, IPv4 multicast was optional and rarely deployed across routers.

Additionally, IPv6 incorporates an anycast address capability. With anycast, a single sender can communicate with the nearest of several receivers in a group. In anycast communication, “nearest” means “the smallest number of hops”. An important use of nearness information is in efficiently updating routing tables. There is little operational experience with the anycast address type. Additional information on anycast addresses can be found in [RFC-3513].

Multicast can be used to efficiently send data simultaneously to a number of field devices. In contrast if unicast is used, the data must be sent to each device one at a time. Multicast supports the capability to make configuration at several selected field devices in a coordinated fashion to ensure proper functionality of that group.

3.2.5 Security Extensions

IPv6 provides a new security architecture that is based on IPsec. Both authentication and encryption can be used in IPv6 and are provided by IPsec. The security architecture defines authentication and encryption extension headers separately so that the can be used either separately or together. The applications using the security extension define which of the security protocols are necessary. IPv6 security features are implemented using extension headers and can be turned off if security features are not needed. Note that IPsec can be used in IPv4 as an option.

An advantage of IPsec, a network layer security protocol, supports providing security services to all applications on a device whether they use TCP or UDP at the transport layer. This is in contrast to application using transport layer security (TLS) which can secure applications only if they use TCP. An additional advantage when comparing an IPv6 IPsec implementation to an IPv4 IPsec implementation is that an end-to-end security approach

cannot be implemented in an IPv4 network that uses NAT. Note that the successful deployment of IPv6 with IPsec does not help mitigate security breaches that occur at the application level.

An implementation challenge that does not change with the introduction of IPv6 is that of key management. IPv6 does not provide any simplification for the required IPsec key management. Key management issues have proved to be challenging and until these issues are resolved, deployment of IPsec will be hampered, slowing its deployment and exposing unprotected traffic to unauthorized sniffing and data analysis. Also, security via IPsec and the necessary supporting protocols does introduce additional overhead, which may be too much of a burden on some embedded control system devices.

Several IPsec components are necessary when deploying IPv6 security extensions. The components include the supporting authentication header (AH) protocol, the encapsulation security payload (ESP) protocol, security associations (SAs), key management approach, and supporting algorithms for authentication and encryption. Following are brief descriptions of the IPsec components.

An advantage of employing IPv6 in an organization's control system is that the IPv6 implementation had security as a primary feature during its development and implementation. IPv6 benefits from continuous improvement in security from the research community [9].

3.2.6 Authentication Header

Authentication Header (AH) provides authentication for the IP header, message payload, and when used with some cryptography algorithms also provides for non-repudiation. Thus the AH will allow for the detection of any modification of the contents of the packet in-transit. In addition, the AH includes a sequence number to detect replay attacks on a data stream. Note that individual nodes that are not equipped to participate in authentication may ignore the authentication data and accept the data as is [RFC-1826].

3.2.7 Encapsulation Security Payload

Encapsulating Security Payload (ESP) provides data confidentiality, message payload integrity, and with some cryptography algorithms also provides for authentication. When ESP and AH are used together in tunnel mode with a security gateway they provide confidentiality and authentication of the IP header [RFC-2406].

3.2.8 Security Association

A Security Association (SA) is the set of security information that two entities share in order to support secure communication. An SA defines traffic flow from one node to another via a Security Parameter Index (SPI), a destination IP address, and either the AH or the ESP protocols. Two SPIs are required to define a two-way correspondence between two endpoints. Note that two separate SPIs are required if both AH and ESP are used resulting in four SPIs to secure duplex communication between two endpoints with AH and ESP.

3.2.9 Key Management

Key management includes all of the provisions made in a secure communication system design that are related to generation, exchange, storage, safeguarding, use, vetting, and replacement of cryptographic algorithm keys. Both automatic and manual key management implementations are available. SAs established with automatic key management are governed by the Internet Security Association and Key Management Protocol (ISAKMP), as defined in [RFC-2408], or Internet Key Exchange (IKE), defined in [RFC-2409].

3.2.10 Secure Addressing

IPv6 has the option of binding a public signature key to an IPv6 address when the Secure Neighbor Discovery (SEND) protocol is used as described in [RFC-3972]. Cryptographically Generated Addresses (CGAs) are IPv6 addresses whose rightmost 64 bits are generated by computing a cryptographic hash from a public key and auxiliary parameters. Thus, a binding between a public key and an IPv6 address is created and the protection works without a certification authority or public key infrastructure (PKI).

CGA reduces spoofing of IPv6 addresses and can eliminate attacks against a control system network that include spoofing the origination address. An attacker cannot take a CGA created by one node and send signed messages that appear to come from another node address.

Since control systems must act in real-time and since many of these devices have limited computation power the additional computations of using CGA can impact communication latency. Additional computation for CGA includes operations such as calculating the cryptographic hash and calculating the parameters for the verification process. These cryptographic calculations include verifying the association between the public key and the IPv6 address.

Other methods of providing address protection are with VPNs or tunnel extensions. Current methods of implementing VPNs and tunnels are applicable to IPv6 as described in [RFC-1826, RFC-1827]. Specific support for an IPv6 tunnels broker is described in [RFC-3053].

3.2.11 Quality of Service (QoS)

A critical requirement of communications in infrastructure control systems is the delivery of messages in timely and predictable manner. This requirement is addressed with adequate communication network bandwidth and reliability. Bandwidth resources of networks can be managed with quality of service (QoS) management. QoS management allocates resources and ensures that conflicts are resolved according to policies governing the control system. IPv6 introduces new features to manage network QoS requirements. Unlike the QoS support in IPv4, IPv6 QoS can be achieved even when the payload is encrypted with IPsec since the QoS extension lies in the packet header. Two primary methods to implement QoS are Integrated Services (IntServ) and Differentiated Services [RFC-1633, RFC-2205, RFC-2475].

In infrastructure or industry control system applications, prioritization of time sensitive data streams and efficient packet handling may be key to IP networks supporting critical operations. QoS can provide the means to allocate various priorities and network resources to meet the needs of time-sensitive data streams. Control system applications will benefit from

the ability to define priorities for control messages, exception reporting, file transfers, and other system functions. In addition, prioritization with QoS improves the ability to carry voice and video packets alongside data. As with incorporating other IPv6 features in a control system network, QoS requires modifying the applications that will use QoS.

3.2.12 Extension Headers

IPv6 provides for optional header extensions as a means to support specific functionality. The header extensions provide both flexibility and efficiency in the creation of IPv6 packets. Only fields needed for the specific packet are added to the extension header resulting in packets being smaller than if the header were always present. The header extensions provide support for security, fragmentation, source routing, network management, and other functions.

In IPv6 the number of required header fields has been reduced to 8 from IPv4's required 14 header fields. If the minimum number of IPv6 header fields is used, processing efficiencies can be gained. This can be important in low power control system applications. In some systems, including control system, bandwidth may be severely limited and any additional header length may increase packet delays. A method to mitigate the effects of the increased IPv6 header size is to employ *header compression*, which uses redundancy and, in some cases, predictability of various headers to reduce the overall header size. Several approaches are documented in [RFC-2507, RFC-3095, RFC-3150, RFC-3241]

3.2.13 Routing

Routing in IPv6 networks benefit from the hierarchical addressing discussed above. As stated above this addressing approach results in routers have much smaller IPv6 routing tables. Smaller routing tables increase routing efficiency and provide faster routing, through faster route lookup and reduced latency. In addition, existing routing protocols have been extended to work with the larger IPv6 addresses. Border Gateway Protocol (BGP) IPv6 extensions are described in [RFC-2545]. Open Shortest Path First protocol (OSPFv6) IPv6 extensions are described in [RFC-2740].

To support IPv6 auto-address configuration, routers provide router advertisements so that nodes can compute their own address, thus providing the option to eliminate the need for the Dynamic Host Configuration Protocol (DHCP).

IPv6 also includes an election protocol that supports the automatic reassignment of router duties in the case of primary router failure. The Virtual Router Redundancy Protocol (VRRP) provides for dynamic router selection on a LAN and can be configured to provide automated router switch over. However, the development of this protocol is somewhat lagging the development of the main IPv6 protocol.

3.3 IPv6 and Infrastructure Control Systems

The control system architectures used by organizations to support their operations employ a distributed hierarchical structure to meet the objectives of fault-tolerance and scalability for their overall system. The distributed hierarchical structure is compromised of multiple sub-networks that perform their specific operation functions. The various sub-networks are inter-

connected to support overall system operation. As an example, in an electric utility the top layers of the information architecture shown in Figure 1 from [10] include the Independent System Operator (ISO) operating center and energy trading system that supports the operational and planning aspects of the organization's systems. These networked systems are considered part of the business operation systems and employ Information Technology (IT).

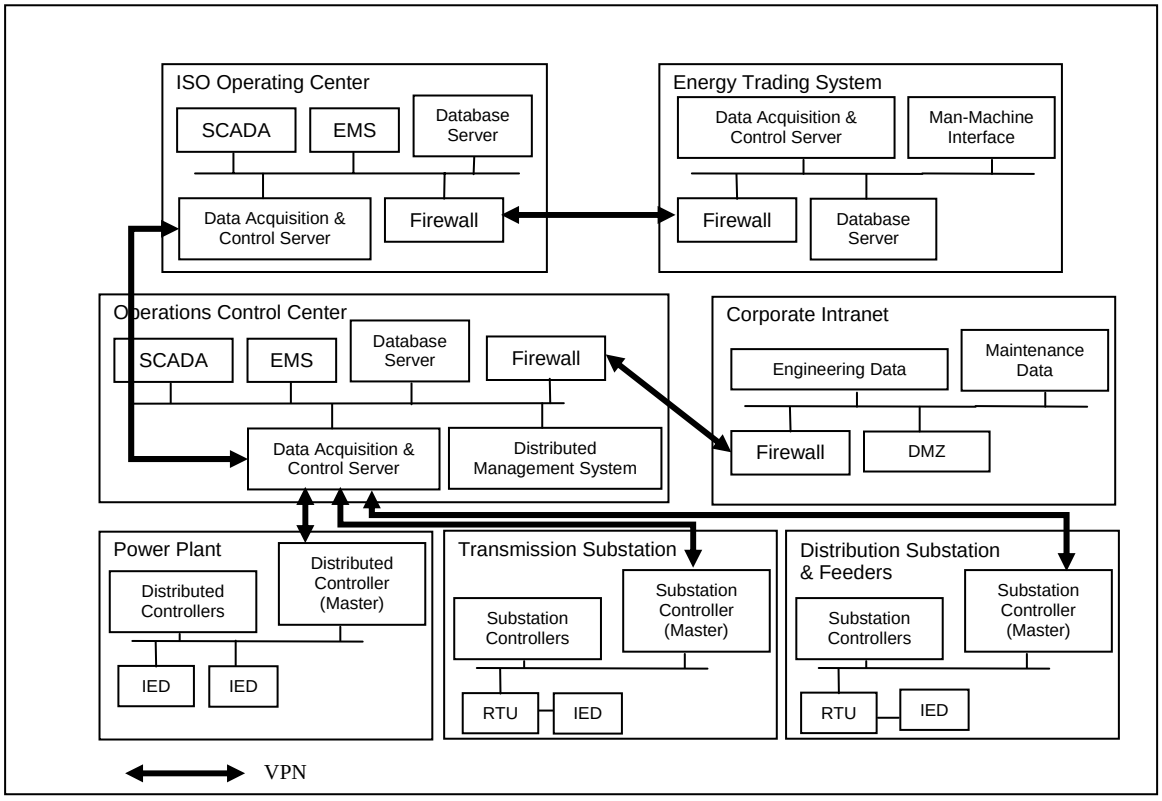

Figure 1: Levels of a Control System Architecture

Table 1 from [11] contrasts the attributes of the business systems and control systems. The lower layers, or control system networks, address the detailed operation of the process, such as power plants, transmission substations, and distribution substations for electric utilities. The control networks support control systems where sensors, actuators, control units, and human machine interfaces depend on data flows between themselves [10].

Table 1: Attributes of Business System Networks and Control System Networks

Attribute	Business Operation System	Control System
Reliability	• Occasional failures tolerated • Beta test in field acceptable	• Outages intolerable • Thorough QA testing expected
Risk Impact	• Loss of data	• Loss of device/equipment or reduced device/equipment life
Performance	• High data throughput required • High delay and jitter tolerated	• Modest throughput acceptable • High delay a serious problem
Risk Management	• Recover by reboot • Safety is typically a non-issue	• Fault tolerance essential • Explicit hazard analysis expected
Security	• Focus is central server security	• Tight physical security • Isolate control system network from business network where possible • Focus is control system stability

3.3.1 Control System Architecture

The impact to system operation of introducing IPv6 in each of the various sub-networks in Figure 1 and the impacts of having an IPv6 connectivity between the sub-networks vary based on the equipment and devices that comprise each sub-network. The major difference between the upper-layer networks and lower-layer networks that support control system operation is *reliability*. The following sections provide an overview of the various equipment and device that comprise each sub-network.

3.3.1.1 Operating Center, Energy Trading Center, Operations Control Center, and Corporate Intranet

The ISO Operating Center, Energy Trading Center, Operations Control Center, and Corporate Intranet are comprised of sophisticated management applications and database applications that, to a large extent, operate on commercial operating systems such as Linux or Windows. At this time these applications do not require any specific IPv6 functionality. If the operating system supports IPv6 then these applications should function on IPv6 based systems. Additional IPv6 details concerning the control system equipments that make up these organization assets are included in the following sections.

Host Applications

Applications that require IPv6 are expected to be the major driver of IPv6 adoption by organizations. A June 2006 report by the U.S. Government Accountability Office [12] indicates that applications that use a number of IPv6 features are being developed or in planning stages. A number of IPv6 applications are under development to support government activities such as emergency response, operations planning, and warfighting. IPv6 activities outside the federal government include applications being planned or developed by broadband cable providers and telecommunications industry participants. However, the report indicates these applications are few in number since the transition to IPv6 is still in early stages, thus leaving little incentive at this time.

It is expected that application developers will recognize IPv6-only features that can be used to enhance the capability of their products and will make their products IPv6 capable. Features such as multicast and IPsec security are expected to be the primary drivers for IPv6 adoption. Initial steps for application developer's adoption of IPv6 are to include IPv6 libraries and APIs in their development environments. As an example, applications developer Wonderware has identified IPv6's use of IPsec as a driver to adopt IPv6.

Databases provide important functions at various points in an organization's control system. A specific example of IPv6 support in a database application is with Microsoft SQLServer. SQL Server 2005 and later versions support IPv6 through the Windows IPv6 stack and can also support IPv4/IPv6 dual-stack configurations.

Host Middleware

Middleware software and libraries support the exchange of data between the application and other software components. Specific types of middleware that supports calls to procedures on remote nodes are remote procedure call (RPC), remote method invocation (RMI), and object request brokers (ORBs). Middleware, including CORBA, .NET, and Java RMI, are based on these procedures and usually does not require modification to the application. The procedure itself must support IPv6 and it appears these common procedures are available in IPv6 based environments.

Host Operating Systems

Operating system (OS) vendors have incorporated IPv6 support in their OS products over the last few years. OS vendors such as Microsoft, Sun, and Redhat are providing OS products that support IPv6. In cases, the performance of the IPv6 stack can impact the performance of applications they support. A recent research activity, described in [13], provides experimental results for Windows, Linux, and FreeBSD operating systems. A brief overview of the level of IPv6 support is included in Table 2.

Table 2: Overview of IPv6 Support

Operating System	IPv6 Support
Microsoft Windows	Microsoft will offer default support for IPv6 in the Vista operating system. Windows XP and Windows 2003 Server will support IPv6; however the user must enable the support. These Window versions also support various IPv4/IPv6 tunneling approaches.
Linux	Many Linux distributions are IPv6 ready and the capability is available after activation and configuration. Linux also supports various IPv4/IPv6 tunneling approaches.
UNIX	Solaris versions 8 and higher provide IPv6 support. Recent versions of BSD distributions, HP/UX, and AIX also provide IPv6 support.
Mac OS X	Apple platforms beginning with OS X are IPv6-ready.

Host Firewalls

Host or personal firewalls with support for IPv6 are not yet widely available.

3.3.1.2 Power Plant, Transmission Substation, and Distribution Substation & Feeders

In the layered architecture example shown in Figure 1, the amount of data processing involved increases with each layer from bottom to top. The separation of the computation requirements results in field devices located in the Power Plant, Transmission Substation, and Distribution Substation & Feeders layers having reduced computation requirements and capabilities. If the field devices support IP communications, it is currently, limited to the IPv4 standard. In this example, field devices include RTUs, IEDs, and PLCs.

Control System Devices

Control systems devices in many cases are reduced form factor device that have limited computing and network communication capability. Some implementations are embedded systems developed without an operating system or with a custom proprietary operating system since the product has very specific and simple functional tasks to perform. Field devices depend on software upgrades from their manufacture thus any transition from an IPv4 compatible device to an IPv6 device must come from the manufacture via updateable firmware [14]. Support of IPv6 in IP-capable field devices appears to be non-existent at the time of this report. Indications are that vendors are developing plans to move forward with IPv6 support and in some cases prototypes may be in the test phase. See Appendix C for additional details.

In some cases, the control system device utilizes a real-time operating system (RTOS) and thus can support applications developed via modularized code. Many third party RTOSs are available that may be used in devices that support control systems. Two examples of RTOS that support IPv6 are the Green Hills RTOS and the IXXAT Automation RTOS. Field device applications that depend on an IPv6-compatible RTOS appear to be non-existent at the time of this report.

The limited functionality inherent in some control system devices may limit the level of IPv6 support in these devices. In control systems there is potential for a large number of sensor and control devices on a system. The desire is to have each of these devices to have their own IP address. In some cases these devices may have reduced functionality because of low computing power and other scarce resources. IPv6 has a number of mandatory security functions that are required for conforming nodes as described in [RFC-4294]. These mandatory requirements may limit the level of reduced functionality a device manufacture can pursue in order to minimize the device functionality. Additionally the IPv6 end-to-end security model may not be applicable to the reduced functionality node since they may not have enough resources to protect themselves and will be dependent on perimeter security.

3.3.2 Supporting Communication Network Architectures

The communication networks that support the system operator's control system architecture are also built in a hierarchical structure. The communication network can be comprised of simple sensor and actuator wires at the lowest level to LANs and WANs at the higher levels. The various levels are interconnected via gateways, firewalls, and servers.

Figure 2, taken from [10], illustrates the possible protocols associated with the example control system shown in Figure 1. As described in the figure the primary communication

network employs the TCP/IP protocol suite for the upper layers of the control system architecture. The lowest control system level supports control system field devices such as sensors and actuators. In general, the lower layers generate larger amounts of data that is filtered and aggregated at the servers and gateways located between the layers.

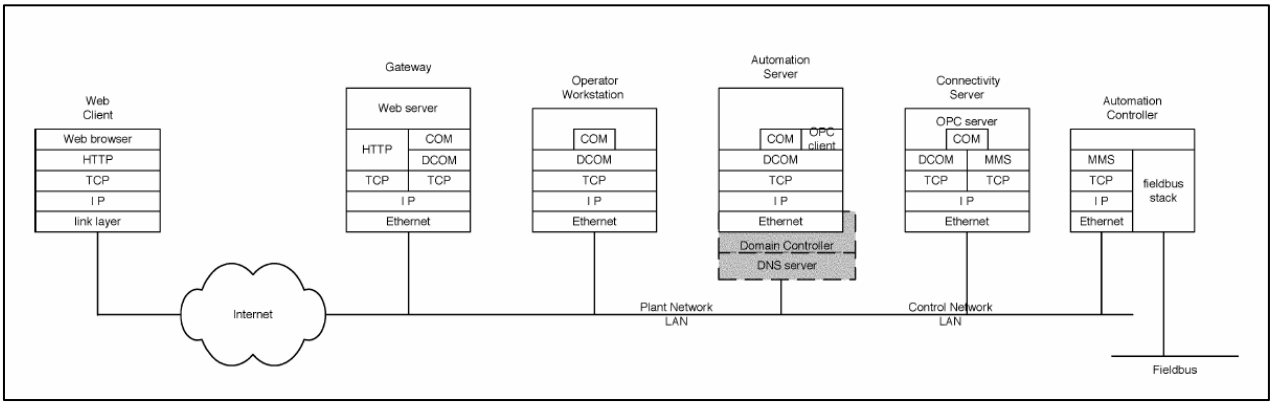

Figure 2: Electric Utility Control System Network Communications

Continuing with the electric utility example, there are several organizations that provide security standards. Security standards specifically directed at data and communication security over IP networks are provided by International Electrotechnical Commission (IEC) in their IEC 62351 Standard, *Data and Communication Security*, as described in [15]. The IP security required by the standard primarily comes from Transport Layer Security (TLS) [RFC-2246]. A listing and brief descriptions of a number of the key sections of the IEC 62351 are included in Appendix C.

3.3.2.1 Field Bus and Device Level Communications

In typical installations field buses or dedicated wiring provide field devices, such as sensors and actuators, communications with the master controller and in many cases have their own specific protocols. In cases where devices use their own specific protocols, gateways must be introduced for protocol conversion and to provide a common interface to the higher levels. In other cases these devices employ standard communication protocols and typically communicate over serial ports or Ethernet [16]. If IP is used, specific support protocols include Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) to communicate over serial links. SLIP is not IPv6 capable; however, PPP supports IPv6 packets as described in [RFC-2472].

In IP-based control systems, the simple network management protocol (SNMP) can be used to monitor and control system-attached devices such as field devices [RFC-1157] as described in [17]. SNMP is an application layer protocol that uses management information bases (MIBs) to specify the management data of the device. Additional details on SNMP in IPv6 are provided in Section 3.3.2.2.

Electric utility substations employ several protocols to support field device communications, including Digital Network Protocol (DNP) and Fieldbus Message Specification (FMS) [18].

In the electric utility industry, DNP was designed primarily for communications between a master controller and field devices such as RTUs or IEDs. The protocol also supports communications in a master-slave operation between RTUs and subordinate IEDs. DNP3 performs multiplexing, data fragmentation, error checking, link control, prioritization, and addressing services for user data. It uses typical RTU network communication architectures such as point-to-point or multi-drop and is not well-suited to peer-to-peer communications or networked based communications. However many recent applications now communicate DNP3 messages over TCP/IP.

When operating over TCP/IP, Transport Layer Security (TLS) is to provide measures for confidentiality and integrity thus providing protection against eavesdropping and replay attacks when using DNP3. TLS is implemented at the transport layer with TCP and is independent of whether IPv6 or IPv4 is used at the network layer.

Fieldbus uses the FMS at the application layer. Electric utilities use fieldbus to link PLCs to the various devices such as sensors and actuators. A wide variety of fieldbus standards exist, such as Modbus, CAN, LonWorks, PROFIBUS, and Industrial Ethernet. Industrial Ethernet has allowed the migration of this level of communication to Ethernet in that Ethernet is used at the link layer and one of the other fieldbuses is used at the application layer. Several examples of fieldbus that use IP for their transport medium are FOUNDATION fieldbus HSE, PROFInet, and Modbus/IP. Most Industrial Ethernet implementations simply encapsulate fieldbus protocol over either TCP or UDP at the transport layer and are independent of whether IPv6 or IPv4 is used.

In general, the control system networks at the fieldbus and device communication level benefit from being in isolated network environments and in most cases do not have connectivity to the broader Internet. However, if these control system networks are connected to the broader Internet great caution must be exercised in the area of security.

Another protocol used in the electric utility is the Generic Object Oriented Substation Event (GOOSE), which is included in the IEC-61850 definition. GOOSE has the objective of getting messages to peer devices quickly and uses a publish/subscribe-based communications. This publish/subscribe approach employs a reduced communication protocol stack and directly accesses the Ethernet link layer. The access is obtained with standardized EtherTypes; more specifically GOOSE has three specific EtherTypes to support its operation [16], [19]. Since GOOSE employs its own EtherType it is independent of the IPv6 protocol, which has its own EtherType identifier.

A report describing future needs for substation control has identified the need to extend GOOSE to permit its use in local and wide-area networks using multicast IP addresses [5].

3.3.2.2 Local Area Networks (LANs)

The field devices communicate their time-critical data to the substation controllers. The substation controllers perform gateway function to perform any protocol conversion and provide a common interface to the higher levels. More specifically the substation controllers must communicate with the data acquisition and control server located in the Operations Control Center. Two commonly used interface standards are the Manufacturing Message

Specification (MMS) and the OLE for Process Control (OPC) [20]. Most common implementations of MMS and OPC are built on TCP/IP and can operate over either IPv4 or IPv6.

MMS is an application layer standard for communications between devices and PLCs. MMS uses TCP/IP in the transport/network layer, and Ethernet and/or RS-232C as physical media. The interfacing of MMS to TCP/IP is defined by [RFC-1006] and specifies data formats, frame assembly, and port numbers. In general, all communication handling in MMS is the same regardless of network type and connected devices. MMS is also a basis for the IEC 61850 standard [20].

OPC is also an application layer standard for control systems and is designed to bridge Microsoft Windows based applications and process control hardware and software applications. OPC is based on the Object Linking and Embedding (OLE) Component Object Model (COM) and Distributed COM (DCOM) technologies developed by Microsoft for the Microsoft Windows operating system family. DCOM employs TCP or UDP when invoking a Remote Procedure Call (RPC) over the network.

Most LANs used in control systems use TCP/IP and are based on switched IEEE 802.3 Ethernet at the physical layer. IP based LANs depend on protocols to support addressing and routing of network data. Each node on a LAN must have an IP address that may be static or dynamic. Dynamic addresses are assigned by Dynamic Host Configuration Protocol (DHCP). Network nodes can find IP addresses of nodes with whom they desire to communicate via the Domain Name Server (DNS). Also associated with each node is a Layer 2 address called the Media Access Control (MAC) address, which is a unique identifier, attached to most forms of networking equipment. The DNS translates node names to IP addresses. The mapping of IP addresses to MAC addresses is performed by the Address Resolution Protocol (ARP). Switches are used to forward data packets within the LAN to their destinations. Routers are used to forward data packets across multiple subnets. Routers and switches support network management functions over the network via the Simple Network Management Protocol (SNMP). Simple Network Time Distribution Protocol (SNTP) is used to manage time needs. Following are brief overviews of the various LAN components and functions that can be impacted by the adoption of IPv6.

DHCP and DNS

If DHCP and a DNS are in an IPv6 network their operation is similar to that of an IPv4 network; however, they must be modified to accommodate the increased IPv6 address size of 128 bits.

Routers

The router is a major network device that will require upgrade for IPv6 . It is expected that router upgrades will consist of primarily of software upgrades. The router operating system must support IPv6 or must be upgraded. In cases, the router’s memory may need to be increased to support an upgraded operating system.

A security issue that has been noted in IPv6 routers is the inconsistent implementation of IPsec when securing routing protocols such as OSPFv3 and RIPng. The implementations are

inconsistent across internetworking vendors resulting in potential security implications [21]. In addition, from a security viewpoint care must be taken to make sure that the IPv6 equipment supports Access Control Lists (ACLs) since some IPv6 equipment does not yet support this important security feature [2].

Switches

Since switches are intended to operate at high speeds, much of their capability comes from chipsets and application-specific integrated circuits (ASICs). Thus, if a switch doesn't support IPv6, either the switch chipset or the entire switch will need to be replaced.

Firewalls

Enterprise firewalls are available that currently have support for IPv6, however, they are at an early stage of development and may be limited in their ability to implement IPv6 filtering rules. Some IPv6 firewalls are not able to deal with the current full set of IPv6 extension headers and thus drop traffic that includes headers that are not equipped to decipher. Firewall vendors are increasing their support for IPv6.

Firewalls do pose a challenge in dual IP4/IPv6 networks since, in some cases, configurations are not adequate to address tunneling approaches such as Teredo. These configurations increase risk by allowing outbound UDP traffic without taking into account IPv6 over UDP as used in Teredo.

Intrusion Detection Systems (IDS)

IDS are now beginning to become more available for IPv6 networks, however, there are concerns with respect to performing full analysis because of issues with parsing the IPv6 headers correctly. In addition, since IPv6 offers the opportunity to employ end-to-end security with IPsec, the security protection must be provided by the end node since the IDS will only have access to encrypted traffic and cannot perform its detection duties without accessing the data.

In IPv4/IPv6 dual configurations the IDS must be able to decode both IPv4 and IPv6 to detect exploits. Thus IDSs must examine packets at increased levels due to the encapsulation of IPv6 in IPv4. This should be required for all IPv4/IPv6 tunneling methods.

A number of IDSs support the IPv6 protocol, including NFR Sentivist 4.0, ISS RealSecure 7.0, and Proventia [22].

Virtual LANs (VLANs)

In addition to LAN functionality many control systems employ Virtual LANs (VLANs). VLANs are a method to create independent logical networks within a physical network. A network node on a VLAN may be physically connected to multiple segments of a LAN but behaves as if it is only connected to those nodes on the same VLAN. Several VLANs can co-exist within the same physical network. Some field devices, in electrical substations for example, connect back to their control center via VPNs.

There are a number of methods to construct VLANs, one of which could be impacted by the transition to IPv6. Methods to construct a VLAN include port based, MAC address based,

authentication based, and protocol based. Protocol-based VLAN approaches separate different protocol traffic based on EtherType. Example protocol-based VLANs include IP machines operating on an IPv4 VLAN and AppleTalk machines operating on an AppleTalk VLAN. Thus if an IP VLAN has an EtherType specification that carries IPv4 traffic it must be changed to an EtherType specification that carries IPv6 traffic to continue operation.

Wireless Connectivity

Wireless connectivity is also widely used for access to field devices, which increases the potential threat of data interception. In general wireless connectivity describes a physical layer attribute and in most cases does not impact the network layer protocol. For example, an IEEE 802.11 wireless network using a Cisco wireless access point will forward IPv6 traffic without interruption. It is expected that in the future wireless device vendors will utilize native IPv6 features on their wireless devices.

Network Management in IPv6

Network management consists of a set of functions to perform tasks such as inventory, topology, security, monitoring, and reporting. The functions are typically performed via simple network management protocol (SNMP). Here the SNMP server usually queries SNMP agents for status information. SNMP relies upon a Management Information Base (MIB) in the query process and thus in an IPv6 implementation the MIBs must contain IPv6 information [RFC-2452, RFC-2454]. A number of industry specific MIB standards are being developed and described in IEC 62351-7 [15].

The majority of router vendors have some level of SNMP support for IPv6. More specifically, Cisco, Juniper, Hitachi, and 6WIND have various levels of IPv6 support. These vendors have plans for full SNMP over IPv6 support in future releases.

A number of IPv6 MIBs have been implemented, however, others, considered important by some users, are still not readily available. These MIBs include counters for IPv6 traffic and an updated BGP MIB for IPv6 traffic [23]. Specific vendors such as Cisco, Juniper, Hitachi, and 6WIND have implemented IPv6 MIB support based on a number of RFCs.

In support of network management activities routers may employ Cisco's NetFlow Version 9. NetFlows features generate netflow records that can be exported from the router and collected using a netflow collector. NetFlow Version 9 can be enabled for IPv6 [RFC-3954].

Currently a number of vendors support IPv6 in their network management platforms and monitoring tools. Support for IPv6 continues to increase in these products and the current level of support should be requested of specific vendors. A list of tools that support IPv6 can found in [24].

As another example, Nmap, a commonly used network management tool, has only limited support for IPv6 networks [22].

3.3.2.3 Wide Area Networks (WANs)

Since many infrastructure control systems may be geographically separated these systems require wide area networks to support communications. To support these necessary links

most utilities lease communication capacity from telecommunication providers or maintain their own physical communication links. WANs provide communications between infrastructure control centers, regional control centers, individual utilities, and non-utility generators.

WANs can be physically supported by many types of communication link, including radio links, the Public Switched Telecommunications Network (PSTN), and the Internet. In general, the leased telecommunications capacity is more secure than public telecommunications lines. Asynchronous Transfer Mode (ATM) networks and Frame-Relay Permanent Virtual Circuits (PVCs) are the most popular mode for leased line network communications. ATM and Frame Relay have reliability and quality of service that can provide the necessary support for critical applications.

For WANs, IPv6 can provide network layer services over WAN links that use, for example, ATM, Ethernet, Token Ring, ISDN, Frame Relay, and T1. These WAN links are transparent to IP version, however if IPv4 is used by one entity and another uses IPv6 there will be interoperability problems unless IPv6/IPv4 tunnels are used.

For the case of electric utilities open standards have been established; two examples are the Inter-control Center Communications Protocol (ICCP) [25] and IEC 60870-6 for data exchange over WANs based on IP. ICCP and IEC 60870-6 are supported by most major EMS and SCADA systems to move real-time data into and out of SCADA/EMS. ICCP interfaces to the various applications it supports, such as SCADA databases, data acquisition and control, energy management systems, operator consoles, RDBMSs, and network management. ICCP is to communicate data between control centers that operate SCADA systems and between control centers and power generation facilities. The protocol is also used in power pools, regional control centers, and regional transmission organizations. Based on client/server concepts, ICCP runs over MMS, which utilizes TCP/IP and can operate on either IPv6 or IPv4 networks. Security measures are obtained with TLS for ICCP.

To support the exchange of information amongst multiple electrical utilities will require IPv6 compatibility amongst these organizations. Much of this network traffic flows via ICCP and links corporate information and control systems with partners. Linking multiple corporate control systems can increase the threat to the sensitive and proprietary information contained in those systems. IPv6 end-to-end security approaches can be employed to help manage these threats to control systems.

3.4 Transitioning an IPv4 Network to IPv6 Network

The transition from IPv4 to IPv6 has begun and is expected to take many years to complete. Since the community has been aware that this transition period will be quite lengthy, much thought has gone into how IPv4 networks will be transitioned into IPv6 networks. To maintain, at minimum, current levels of network service, organizations need to support both IPv4 and IPv6 in parallel for a significant amount of time. All transition approaches have security and other operational implications that must be considered prior to implementation.

Transitioning is expected to include both software/firmware upgrades along with hardware upgrades. For example, it is likely that IP end-nodes will only require software upgrades of

their operating system in order to become IPv6-capable while hardware changes may be required for specific networking equipment such as high-speed routers. Most equipment associated with the communication network that supports the organization's control system will require at a minimum configuration changes.

Transitioning the organization's control system places additional burdens since software upgrades are slow to be deployed since great caution is exercised to maintain system reliability. In many cases, control systems go quite some time before being upgraded or even rebooted. In cases this time can be years [26].

3.4.1 Obtaining IPv6 Address Blocks

One of the steps in deploying IPv6 in any information or control system is to obtain IPv6 addresses. An organization will request and obtain their IPv6 addresses from their service provider. The service provider usually provides a /48 address block. Service providers obtain their IPv6 addresses from Internet address authorities. In the U.S. IPv6 addresses are obtained from the American Registry for Internet Numbers (ARIN) [2].

As an organization develops plans for the transition to IPv6 the general consensus is that organization should consider a 50-year time horizon for requesting an IPv6 address allocation. An organization should consider that individual nodes might require multiple addresses due to, for example, classification level, redundancy, community of interest, and geospatial coding [27].

From a security standpoint the companies obtaining IP addresses from ARIN must recognize that the registration information, including address assignment is publicly available. This information could be used by a malicious entity for identifying exploitable company assets that are accessible via the Internet [28].

3.4.2 Basic Steps Involved in Transitioning to IPv6

The following list identifies, at a high level, the steps involved for an organization to transition their supporting networks to IPv6. In general the transition will occur over time but incorporating IPv6 into current network procurement, training, planning, and budget is critical to a cost effective transition [29].

1. Begin IPv6 education and training now. Add funds in training budget to educate designers and operators about IPv6 protocols and implementation.
2. Assess your inventory of existing IP infrastructure including routers, applications, servers, and nodes.
   - Identify IPv6 compatible equipment, and deployed dual-stack equipment including routers, applications, servers, and nodes.
   - Identify current IPv4 equipment that may be upgradeable to IPv6.
   - Identify current equipment that is limited for use with IPv4. This equipment will require replacement.
3. Assess your existing IP infrastructure hardware for upgradeability. The equipment identified in the previous step that is limited for use with IPv4 should be on this list. In many cases, firewalls, routers with acceleration hardware, and devices with encryption accelerators are often IP version specific.

4. Include detailed IPv6 specifications where possible on new device/equipment purchases, including licensing agreements for hardware, operating systems, and software upgrades.
5. Develop a clear security policy for the organization's information system. The policy must address the difference between the business operation system and control system.
6. Begin internal system architecture planning and address areas of concern with detailed analysis via simulation and/or lab testing. Address compliance issues with organizational policies.
7. Acquire IPv6 prefixes/addresses from the American Registry for Internet Numbers (ARIN).
8. Identify a procedure to renumber your network without causing unplanned outages. See [RFC-4192].
9. Select an IPv4/IPv6 transition mechanism that operates with both IPv4 and IPv6 network traffic.
10. Broaden testing with a limited launch (e.g. tunnels, trial peering) of IPv6 to gain experience in implementation. Upgrading in stages allows for learning along the way.
11. Provide feedback to vendors to help improve device/equipment and refine requirements.

A number of organizations have documented their experience with transitioning their information systems to IPv6. Their approaches, experience, and best-practice guidelines can be found in [21] and [30]. However, at the time of this report no organization has reported on transitioning a control system to IPv6.

3.4.3 IPv4/IPv6 Co-Existence

IPv6 and IPv4 must co-exist for some time as organizations transition their networked systems while maintaining operations. A suitable transition method must be selected and securely deployed to initiate the transition to IPv6. .

3.4.3.1 Transitioning Mechanisms

Several approaches exist to transition to an IPv4 network to IPv6 over time. The approaches are dual stack, tunneling, and translation [21], [31].

Dual Stack

A dual stack transition approach will maintain network nodes that include both an IPv4 stack and an IPv6 stack. Dual stack nodes must reside on networks that can carry IPv4 and IPv6 traffic simultaneously thus routers and switches must be able to process both protocols. Dual stack nodes may be impacted not only from threats from the IPv4 stack and IPv6 stack but also threats that come from the dual stack implementation. Any node controls, such as firewalls, VPN clients, intrusion detection systems (IDSs), and intrusion protection systems (IPSs) should be configured to perform their functions on both IPv4 traffic and IPv6 traffic. The threats from the IPv6 stack are summarized in Section 3.5 of this report.

As with many networked system technologies the more complicated the technology the more opportunity for security issues. From this standpoint, it is best to keep the transition mechanism as simple as possible. Use dual stacks if possible since the security issues are

better understood [RFC-3964]. Note that additional configuration for IPv4/IPv6 dual stack network device increase opportunity for misconfiguration.

Tunneling

Tunneling can be used if an isolated IPv6 node or network must use the existing IPv4 infrastructure to reach another IPv6 entity. Tunneling consists of encapsulating IPv6 packets within IPv4 packets and transmitting them over an IPv4 network. Two approaches to tunneling are automatic tunneling and static or configuration tunneling.

Endpoints are determined by the routing infrastructure when automatic tunneling is used. Automatic tunneling includes embedding IPv4 address information within IPv6 addresses on the local network. In contrast to automatic tunneling, configuration tunneling requires either human operators or tunnel brokers to explicitly configure the tunnel endpoints.

Static tunnels used in configuration tunneling increases the complexity for both IPv6 endpoint sites and the IPv4 networks providing the tunneling service. The complexity occurs in the creating, managing, and operation of manually configured tunnels.

A specific tunneling approach to reduce the complexity of configuration tunneling is the *6to4* transition mechanism. The *6to4* transition mechanism enables IPv6 domains to transmit their IPv6 packets over an IPv4 network without the need to configure explicit tunnels. Additionally, *6to4* tunnels are used to provide connectivity into a larger IPv6 routing infrastructure that has connectivity to an organization's IPv6 end-user site networks. Discussions on how *6to4* eliminates complex tunnel management, sending and receiving rules for *6to4* routers, return path and source address selection, and various complex *6to4* usage scenarios are presented in [31].

Another specific form of tunneling is Teredo [RFC-4380]. Teredo is a short-term solution to the problem of providing IPv6 service to nodes located behind IPv4 NAT. This tunneling approach tunnels packets via UDP to bypass NAT. With this approach security issues may surface from allowing UDP packets to pass through the firewall.

Networks that support Multi-Protocol Label Switching (MPLS) can be used to perform IPv6 tunneling. MPLS networks provide ease of implementation in tunneling IPv6 traffic since the tunneling router in general becomes an MPLS label edge router (LER) [RFC-2547].

Following is a listing of security considerations when a tunneling IPv4/IPv6 approach is used to ultimately transition the organization to IPv6. This high-level list of areas is not complete and each individual system may have issues that warrant special attention.

- If possible, use static or configured tunnels rather than automatic tunnels.
- If automatic tunneling is used, implement outbound filtering on firewall devices to allow only authorized tunneling endpoints.
- Network architectures should provide separate IPv4 and IPv6 firewalls. IPv6 traffic arriving encapsulated in IPv4 packets should first be directed through an IPv4 firewall, decapsulated, then directed through an IPv6 firewall.

- If 6to4 tunnels are used, review [RFC-3964] to help identify threats. All 6to4 relay routers must accept traffic from any native IPv6 node and thus enable a number security threats such as denial of service and for the spoofing of IPv6 addresses.
- Care must be taken in configuring firewalls to account for IPv6 tunnels to prevent unauthorized traffic from traversing the firewall. Great caution must be used when allowing for automatic tunneling mechanisms and their susceptibility to packet forgery and DoS attacks.
- Note that tunneling mechanisms also offer the ability for an adversary to send traffic and mask the source address.

Translation

Translation is necessary if an IPv6 node requires access to an IPv4 service such as an IPv4 web server. Dual-stack application layer proxies can support both IPv4 and IPv6 and are used to support translation. In translation the dual stack node will transfer the request IPv6 packet from IPv6-only into an IPv4 packet. The node will also take the IPv4 response packet and transfer it into an IPv6 packet. An IPv6-to-IPv4 translation technique is the NAT – Protocol Translation (NAT-PT) described in [RFC-2767].

A number of limitations of the translation approach exist. This high-level list of areas is not complete and each individual system may have issues that warrant special attention.

- Security compromises can occur with address translation in mapping IPv4 addresses to IPv6 addresses. A representation of an IPv4 address as an IPv6 address is accomplished by inserting the IPv4 address into specific fields of the IPv6 address. This mapping makes it difficult for a receiving node to discern whether an IPv4 mapped address or an IPv6 address has been received. Potential security issues can arise with attacker attempts to bypass access control with this encapsulation method.
- Cannot implement end-to-end security since the translation node must be placed in the communication path.
- The translation node is a single point of failure if no redundant translation node is available.

3.4.3.2 Issues with IPv4/IPv6 Network Transitioning

The transitioning from an IPv4 network to a network where both IPv4 and IPv6 coexist brings additional issues that should be considered. The issues arise from either the IPv6 protocol itself, the transition mechanism, or the transition deployment.

Domain Name Service (DNS) in IPv4/IPv6 Networks

During the period when both IPv4 and IPv6 nodes are used and must communicate with one another the DNS provides its normal role of mapping node names to node IP addresses but also provides information on the node's ability to support IPv6 connectivity. Each name in the DNS is associated with an IPv4 address and/or an IPv6 address. Thus the DNS provides signaling to other nodes if the node supports IPv6 connectivity. [RFC-1886] provides details on IPv6 extensions to DNS.

Fragmentation in an IPv4/IPv6 Networks

IPv6 mandates that all supporting networks and links carry a minimal MTU of 1280 bytes. IPv6 networks also do not support fragmentation of the IPv6 packet at intermediate system devices. All IPv6 fragmentation is done at the source. This fragmentation limitation in IPv6 enables minimal implementations, such as that can be used in control systems, to avoid implementing an MTU discovery and simply send packets smaller than 1280 bytes. However, IPv4 supports fragmentation anywhere in the packet's path. Thus in tunneling IPv6 over IPv4 networks mechanisms must be in place to deal with IPv4 networks attempting to fragment packets. Consideration must be given to translating IPv4 ICMP "packet too big" errors to IPv6 ICMPv6 "packet too big" errors [RFC-2893][32].

Security Aspects

The transition to IPv6 will bring other security considerations that must be addressed. To date there has not yet been a thorough treatment of the threats a dual mode IPv4/IPv6 network will face. An IETF document is in draft stage that discusses the transition considerations [33].

In general, an organization should maintain node and application security since the introduction of IPv6 in a network can result in some nodes not being completely secured. Other nodes on the network will have less chance of being used by a compromised node if they properly are secured [21]. Also note that IPv4/IPv6 transition attack tools currently exist that that can spoof, redirect, and launch DoS attacks in a transition network. One attack tool directed at specific IPv6 weaknesses associated with ICMPv6 is described at [32].

3.4.4 IPv6 Network Equipment Acquisition

An organization transitioning to IPv6 must have deployed network equipment that supports IPv6. This includes IPv6 capable routers, switches, various information assurance equipment, and servers. In general, most routing infrastructure and servers purchased in recent years may support IPv6 or can be upgraded.

Since the DoD is very active in their adoption of IPv6 they have established developed certification processes and various test plans to validate IPv6 support in network equipment. The DoD has a website that provides a list of IPv6-capable equipment [34]. Note that at the time this report was being written, the list was short.

An issue to consider with IPv6 networking equipment is the level of support for various IPv6 functionality. Support for IPv6 data plane functions and control plane functions such as DNS for IPv6, DHCPv6, Neighbor Discovery, SNMPv6, OSPF, and BGP.

It is expected that equipment manufactures will adopt IPv6 at various levels over time. It is further expected that equipment manufactures will advertise IPv6 capabilities with varying degrees of support of IPv6 features. To provide the equipment purchaser some indication of the degree of IPv6 support that the equipment may have, the IPv6 Forum [36] has initiated an *IPv6-Ready Logo* Program [37]. Since interoperability will be a critical aspect to the IPv6 adopters and a large number of implementations will exist, it is important to give to the market a strong signal proving the interoperability degree of various products. In order for equipment to earn the "IPv6-Ready" logo it must pass IPv6 conformance testing.

3.4.5 IPv4/IPv6 Transitioning System Testbed

Since any control system disruptions can create large problems for infrastructure organizations, experts suggest establishing testbeds to evaluate the coexistence of IPv6 with IPv4. In cases, a dedicated research network has been used to examine how well critical applications perform with an IPv6 network [30]. The benefit of a test bed is the opportunity to test IPv6 operation without disrupting the operation network.

In cases, network operators may choose to establish a pilot deployment on part of their operation network to gain experience of deploying IPv6. If this is done, a great deal of caution must be directed at not allowing the pilot deployment to have less security than the operation network.

3.4.6 Testing of IPv6 Network Design and Implementation

There are benefits and challenges to migrating from an IPv4 network infrastructure to an IPv6 network infrastructure. The migration may impact system operations in multiple ways including network disruption resulting from configuration issues and network performance issues resulting from additional protocol overhead. In most cases infrastructure control system must be highly reliable and any system disruptions can lead to large overall system disruptions such as blackouts. Thus methods are necessary to test new protocols and their interoperability with existing protocols.

Since in some cases a testbed of the infrastructure's control system to test new devices, protocols, and applications is not available another means to test system operation must be identified. One approach is to use a testbed built with real components, emulated components, and modeled components to represent the actual control system. A testbed using this approach provides a cost-effective means of examining new protocols under specific scenarios that an analyst has identified as potentially being suspect.

Sandia National Laboratories is developing the Virtual Control System Environment (VCSE), which is a hybrid testbed to perform experiments that can help assess the impacts of new protocols such as IPv6. The VCSE is a modular testbed that can merge real hardware with emulated software and various modeling and simulation tools. Key to the analysis of the implications of IPv6 protocols on a control system is the inclusion of a network modeling and simulation tool that models IPv6 protocols. The current implementation of the VCSE employs the OPNET Modeler network modeling and simulation tool, which includes an extensive library of IPv6 protocols.

As indicated by several industry experts (see Appendix B) there is concern of overall system disruption that may result from the IPv4/IPv6 transition mechanisms currently available to industry. The VCSE can also be used to perform analysis via experimentation of any potential transition mechanisms and assessing the targeted configuration of the transition mechanism. The IPv4/IPv6 transition mechanisms are described in Section 3.4.

The VCSE with the OPNET Modeler module [38] can be used to assess a number of key IPv6 features including: expanded addressing, dual stack implementations, RIPng, OSPFv3, IPv6 static routing, IPv6 tunnels, ICMPv6, and neighbor discovery. With these IPv6 protocol models, an analyst can perform studies of IPv6 migration plans using different transition

approaches and examine the operation with various IPv6 protocol enhancements. Assessing tunneling methods such as 6to4 tunnels and configuration of the supporting routers and their static routing table attribute can be done with this tool.

The authors of this report participated in an assessment of the impacts on incorporating IPv6 in a military system [39]. This assessment included a number of detailed simulation experiments that compared several system scenarios using IPv4 and then repeating the experiment using IPv6. The simulation results were then compared. A key finding was the potential system performance degradation that occurs on networks with high (near 100%) bandwidth utilization. Following are several noteworthy points that may have applicability to automated control system networks that are comprised of any bandwidth constrained links.

- As network bandwidth utilization approaches 100% in an IPv4 network the transition to IPv6 will result in a performance degradation resulting from increased packet collisions. In addition, the network system response by intermediate routers is to buffer the message traffic. The result is increasing message delivery delays (latency) and an increased variation in the latency (jitter). Message delivery latency can negatively impact real-time application performance. The increased size of the IPv6 header over an IPv4 header results in additional bandwidth usage, which results in network performance degradation.
- Networks that carry mostly packets with small data payloads will suffer a larger impact in bandwidth usage when transitioned from IPv4 to IPv6. This is because larger IPv6 addresses increase the size of IP headers resulting in increased bandwidth utilization. As noted in Section 3.2, *header compression* can be used to reduce the effects of the increased header size of IPv6 packets.

3.5 IPv6 Security Implications on Process Control System

This section identifies and briefly describes threats that can impact IPv6 networks differently than IPv4 networks. Threats whose impacts on IPv6 networks and IPv4 networks are similar, such as man-in-the-middle attacks or flooding, are not listed. This section summarizes many of the threats described in [21] and [33].

The transition to IPv6 introduces opportunities to improve security with new security mechanisms. A major aspect of IPv6 is the requirement that all implementations support IP Security (IPsec). However, the improved security offered by IPv6 depends on well-coded applications, effective key management, and a strong node identity structure. It is entirely possible for implementers with inadequate knowledge to deploy IPv6 in a non-secure fashion without cryptographic protection of any kind.

A concern noted by the authors of [21] is that some organizations such as the U.S. Department of Defense are planning a full migration to IPv6 by 2008 in support of their security goals. The authors note, “This goal is admirable; but IPv6 is not a panacea for all security problems.”

A number of threats exist with the deployment of IPv6. Some of these threats are similar in nature to the threats that can impact IPv4 networks. In addition, new threats have been identified that are specific to IPv6 deployments (see [21] and [33] for a description). Many of

the threats identified with IPv6 affect network services used by infrastructure systems as discussed in Section 3.2, *Features of IPv6 and its Benefits to Infrastructure Control Systems*. The threats also impact system security enforcement points in the supporting networks. More specifically, firewall and edge router and security applications that run on these devices, such as Intrusion Detection Systems (IDS), Intrusion Protection Systems (IPS), and application proxies can be affected

3.5.1 Reconnaissance

Reconnaissance is an important part of any attempt to breach or attack a network. Approaches to perform reconnaissance include both active scanning and passive data mining. Active scanning in an IPv6 based network is more difficult because of the substantial increase in size of the IPv6 address space. However, this is somewhat migrated since in cases the MAC address is part of the IPv6 address thus knowledge of the NIC manufacture could help reduce the search space.

When nodes use IPv6 stateless address autoconfiguration to generate addresses information about the node can be derived from the address [RFC-3041]. With IPv6 address privacy extensions, the stateless address changes over time and makes it more difficult for eavesdroppers to collect information about the node and its transactions. However, implementing IPv6 address privacy extensions should be done carefully since there is a tradeoff between privacy regarding network scans and an ability to trace problems on a network.

IPv6 introduces new multicast addresses that have site-specific domain, node, or link uses that can help an adversary identify the site-specific address of routers or DHCP servers. Reconnaissance techniques that attempt to exploit these addresses can be mitigated by performing filtering at the network borders [21]. Also consider using non-obvious static addresses that can be used to make guessing an address of a critical node more difficult.

Some IPv4 reconnaissance techniques depended on using ICMP messages and aggressive filtering of these messages mitigated the reconnaissance effectiveness. However, IPv6 networks depend much more on ICMPv6 messages for their normal operations so filtering of these messages must be done with more caution [32].

IPv6 uses a neighbor discovery mechanism to perform duties equivalent to IPv4's ARP function. Routers on IPv6 networks store neighbor discovery information in a local cache that, if exploited, could reveal network address information.

In general, forms of reconnaissance such as network discovery functions are necessary for normal network operation thus all reconnaissance activities cannot be blocked.

3.5.2 Unauthorized Access

Unauthorized access in IPv4 networks has been primarily been mitigated with access control technologies on gateways and end systems with access control lists (ACLs), firewalls, and IPsec implementations. IPv6 can use theses same approach, however, the IPv6 address header will change how these technologies are deployed.

The addressing approach of IPv6 introduces the ability of a single adapter in an IPv6 node to support multiple IPv6 addresses. A single node may have separate IPv6 addresses for communicating on the local subnet, within an organization, or on the Internet [21]. Thus strategies can be developed to limit access via IPv6 addressing and routing approaches.

IPsec support in IPv6 allows more flexibility in its implementation to allow firewall technology to inspect upper layer protocol information that may not be accessible in the IPv4 IPsec implementation. This is accomplished by only using the authentication-header encapsulation offered in the IPv6 implementation. It is expected that the requirement for IPsec in IPv6 may enable easier end-to-end access control. However, an end-to-end security implementation limits the effectiveness of perimeter security with firewalls since the firewalls are unable to inspect the encrypted contents of the packet. Additional security is obtained by configuring firewalls to only allow IPv6 extension headers that provide necessary options.

As discussed in the reconnaissance section above, IPv6 depends on ICMP messages and aggressive filtering of these messages is not possible. In IPv6 networks the firewall must support a number of ICMPv6 messages to be received by, generated by, or pass through firewall devices. [21] provides an overview of the critical ICMPv6 messages and their functions in an IPv6 network.

Firewall capabilities and configurations must also be considered for IPv6 multicast and anycast message inspection. Issues may arise when servers are responding to anycast or multicast service with its real address through a stateful device [33].

3.5.3 Packet Fragmentation

Adversaries have used packet fragmentation as a means to bypass Intrusion Detection Systems (IDS) and stateful firewalls. Both IPv4- and IPv6-capable firewalls and IDSs attempt to assemble fragmented network traffic so that it can be examined for attack signatures and access control rules applied.

IPv6 may mitigate some fragmentation based attempts to bypass security devices since [RFC-2400] prohibits intermediary devices from fragmenting IPv6 packets. Thus even if these overlapping fragments bypass security devices many but not all operating systems that support IPv6 will not accept these packets. In addition IPv6 defines a minimum MTU size of 1280 octets thus any fragment that is not the last packet and smaller than 1280 octets should be dropped by security devices. In general, drop IPv6 fragments that are not consistent with the IPv6 fragmentation rules.

3.5.4 Address Spoofing

IPv6 may offer a slight benefit in reducing Layer 3 address spoofing in that IPv6 addresses are globally aggregated and can be summarized at points in the overall network. This allows filtering of network traffic based on portions of the IPv6 address. However this benefit is very slight since even portions of an IPv6 address can be very large.

3.5.5 ARP and DHCP Attacks

ARP and DHCP are critical parts of the process of initializing network communications. IPv6 employs stateless autoconfiguration provided by ICMPv6 to perform the functionality of IPv4 DHCP. However, IPv6 stateless autoconfiguration messages can be spoofed resulting in denying access to the targeted device. IPv6 employs services provided by DHCPv6 servers to configure network equipment, e.g., DNS servers and time servers. Some protection mechanism must be used to prevent spoofing of the DHCP6 servers.

In IPv4, ARP is used to establish bindings between IPv4 addresses and link-layer MAC addresses. An IPv4-based network attack may manipulate the bindings between the two addresses and redirect SCADA traffic through a malicious node. In IPv6, IPv4's ARP functionality is replaced with a neighbor discovery mechanism that uses ICMPv6. As with ICMPv6 messages for stateful autoconfiguration, ICMPv6 messages for neighbor discovery can also be spoofed, resulting in spoofed router cache information. In general, it is wise to employ static neighbor entries for critical systems to prevent disruption by spoofing attacks on the IPv6 neighbor discovery mechanism.

3.5.6 Routing Disruption

Routing disruptions attempt to disrupt mechanisms that direct traffic in networks. IPv6 employs a similar technique as that used in IPv4 networks. In IPv4 the primary technique to protect routing announcements between peers is the Message Digest 5 (MD5) algorithm authentication. The Border Gateway Protocol (BGP) supports IPv6 in a similar fashion as it supported IPv4 with MD5 authentication. The Intermediate System-to-Intermediate System (IS-IS) also supports IPv6 but with no change to its authentication approach.

Both Open Shortest Path First – version 3 (OSPFv3) and Routing Information Protocol – Next Generation (RIPng) are modified to remove the authentication fields and are required to depend on IPsec to provide protection of the information.

An additional limitation with IPv6 routers is that the information provided to aid in anomaly detection is not as extensive in IPv6 at this time.

3.5.7 Blended Threats

Blended threats may attempt to elude detection by a single type of security solution by exploiting protocols different from the underlying IP protocols. These threats attack weaknesses in, for example, electrical utility system protocols, such as ICCP, Modbus, DNP 3 and others. Exploits in these higher-layer protocols make a firewall-only security approach ineffective. Placing a standard firewall between the control system network and the corporate operation network is not adequate to detect blended threats. Nor does a transition to IPv6 help mitigate these threats other than the added opportunities to employ IPsec.

3.5.8 Virus and Worm Infections

Viruses and worms attempt to disrupt node operation through infections and furthermore impact overall network operation by increasing loads on network routers and switches and application servers. ICCP servers or other devices that are not protected with antivirus software are susceptible to infection. In general, a virus's ability to infect an IPv6 based node

has not changed. However, it is expected that the larger IPv6 address space affects the way some viruses and worms propagate through networks. If viruses or worms depend on some form of random or hierarchical address selection, IPv6 could negatively affect their selection of addresses. This could result in viruses or worms having difficulty selecting useful addresses and thus propagating.

3.5.9 Rogue Devices

In general IPv6 does not provide any additional protection when compared to IPv4 from rogue devices attempting to spoof DHCP or DNS functionality. Additionally, no new protection is obtained from rogue routers or switches being inserted into a network ([21], [RFC-4074]). However, IPv6 does provide opportunity to implement IPsec in a more comprehensive way that protects information during node initialization.

3.5.10 Denial of Service

Denial-of-service (DoS) in an infrastructure control system network can have very serious consequences and is considered to be a more important issue than if DoS occurs in other types of communications. Thus attention must be directed at assuring IPv6 protocols do not introduce new avenues for DoS.

The use of ICMPv6 messages to perform DoS attacks by sending large numbers of erroneous IP packets is substantially limited in IPv6. Implementing ICMPv6 as described in the [RFC-2463] specification limits the number of ICMP messages with an error-rate limiting mechanism.

Additionally, IPv6 does not limit the number of hop-by-hop options in the option header of an IPv6 packet. Any option can appear any number of times. Any forwarding node of a packet with many hop-by-hop options set must process each of the options and thus potentially consuming large amounts of network resources leading to DoS [33].

3.5.11 Special Protocol Threats

This category of threats has to do with specific protocols that support higher-level control system functions. Examples protocols for the electric utilities include DNP3, ICCP, and Modbus. When operating DNP3 over TCP/IP, its security is provided by Transport Layer Security (TLS) encryption. In general, DNP3 will suffer from any vulnerability in the implementation of TLS. DNP3 implementations are not robust against receiving improperly formatted frames thus if the TLS is compromised and improperly formatted frames are received system disruptions may occur.

With the adoption of IPv6, the security will be located at the network layer while with TLS the security is implemented at transport layer. Thus IPv6 security is applied to all data packets above the network layer while a TLS implementation provides only authentication and confidentiality to data packets that use transport layer protocols.

4 Conclusions

Driven by advances in information system technologies used around the world, the transition to Internet Protocol version 6 (IPv6) has begun and will continue for years to come. Organizations have migrated much of their information system communications to Internet Protocol (IP) technologies over the years and the transition to IPv6 is another step in the process. IPv6 offers improvements over IPv4 and these improvements are drivers for adoption of IPv6. However, it is expected that recognition of the benefits of IPv6 will occur over time and thus the transition will be phased and multi-year in nature.

Infrastructure control systems are transitioning toward increasing interconnection between the various subsystems, from the business operation systems to the control systems. The interconnection of the various infrastructure systems is becoming more established via open standard networking using IP. The initial implementations of IP networking are based on IPv4 protocols and now a transition is taking place to move the IPv4 networks to IPv6. Thus control systems that operate over IP will be transitioned to IPv6 at some point in the future.

Some organizations, in particular a large number of organizations within the U.S. Federal Government, have begun the adoption to IPv6. Other organizations have recognized the drivers to adopt IPv6 but have not yet even begun planning a transition. As with any major decision that can have organization-wide impact, a cost-benefit analysis can be done to help drive the decision.

This report outlines many of the potential benefits and concerns related to adopting the IPv6 protocol for an organization's various systems. In general, many of the potential benefits coming from IPv6 features have been implemented in IPv4 in some way. For instance, security based on IPsec is commonly used in IPv4 networked system. However, these implementations do have limitations in cases that are not present in IPv6 networks.

IPv6 standards are immature and in some cases still in progress. In most cases, device and equipment vendors for control system components have not yet made products that depend on IPv6. However, network equipment vendors have products that are IPv6 compliant. It is expected that interoperability of different vendor equipment may be an issue as IPv6 compliant equipment is deployed. Additionally, based on their immaturity, IPv6-specific protocols are expected to have software bugs. Security is also a concern for both IPv4/IPv6 transition approaches and IPv6-only implementations. IPv4/IPv6 transition attack tools currently exist that that can spoof, redirect, and launch DoS attacks in a transition network.

Within the infrastructure control systems the more immediate advantage of moving to an IPv6 networking protocol is associated with addressing the potentially large increase in the number sensors collecting data from the infrastructure system. Sensors will use wireless network communications and power line communications (PLC) to communicate data to control systems. However, these near-term advantages are currently outweighed by the need to provide a transition and test plan. Early adopters have the disadvantage of being in the

vanguard of deploying a protocol that has not been extensively integrated in any other large public communications systems.

IPv6 brings useful functionality that will benefit control system applications and it appears that control system vendors are beginning to consider how best to implement IPv6 features in their products. It is expected that infrastructure organizations will first transition their control system networks to dual IPv4/IPv6 networks as a first step. Thus it is expected that device vendors will offer products that are compatible with both protocols.

5 Recommendations

Full adoption of IPv6 will certainly take several years, so there will be a significant period of IPv4/IPv6 coexistence. Thus, organizations with significant Internet utilization should develop a transition strategy for adopting IPv6. Key aspects of a transition strategy include education, equipment upgrades, architecture planning and development, IPv4/IPv6 transition mechanism selection, and testing.

Since infrastructure control systems have significant reliability and security requirements, the transition to IPv6 must be done very carefully so as to not introduce near-term reliability and security risks. Compared to IPv4, IPv6 networking brings additional functionality that will be useful in control system applications. Thus, control system operators should begin their planning by developing an IPv6 transition strategy that will enable the planned introduction of IPv6-compatible components into their control system infrastructures. In the near term the IPv6 adoption process should proceed with education and control system architecture planning to accommodate and take advantage of IPv6.

Organizations that foresee a transition to IPv6 should begin the following activities:

- Begin IPv6 education and training now. Add funds in training budget to educate designers and operators about IPv6 protocols and implementation.
- Assess your inventory of existing IP networking infrastructure including routers, applications, servers, and nodes.
  - Identify deployed IPv6-compatible equipment and dual-stack equipment, including routers, applications, servers, and nodes.
  - Identify current IPv4 equipment that may be upgradeable to IPv6.
  - Identify current equipment that is limited to use with IPv4. This equipment should be replaced with IPv6-compatible equipment on its regular replacement schedule.
- Include detailed IPv6 specifications where possible on new device/equipment purchases, including licensing agreements for hardware, operating systems, and software upgrades.

One approach that organizations may follow to meet the OMB mandate [1] is to employ IPv6-in-IPv4 tunnels. This approach allows for an entity to meet its obligation of IPv6 support without fully upgrading every network device on its network infrastructure. Approaches to implement IPv6-to-IPv4 tunnels and other transition mechanisms are described in Section 3.4 of this report.

Some organizations that have begun the transition process are publishing their experiences, which can provide infrastructure organizations a wealth of valuable information. However, at this time no organization has described transitioning a control system to IPv6.

Finally, doing nothing to prepare for IPv6 is unwise since IPv6 networking is being adopted around the world and has distinct benefits. Vendor products will become available that implement IPv6 features. Since there are different requirements between business operation systems and control systems, organizations should adopt IPv6 first in the business operation

systems, where short outages will have significantly fewer consequences than outages in critical control systems.

— This page intentionally left blank —

Appendix A: References

[1] *Mandate for IPv6*, Office of Management and Budget. http://www.whitehouse.gov/omb/legislative/testimony/evans/evans052905.html

[2] *Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks*; U.S. Government Accountability Office Report to Congressional Requesters; May 2005. http://www.gao.gov/new.items/d05471.pdf

[3] *The Evolving Internet: A Technical and Economic Assessment of Internet Protocol, Version 6 (IPv6),* U.S. Department of Commerce, January 2006.

[4] *Roadmap to Secure Control Systems in the Energy Sector*, U.S. DOE and U.S. DHS, prepared by Energetics Incorporated, January 2006. http://www.controlsystemsroadmap.net/

[5] *IPV6: The Road Ahead*, Lucent Technologies Whitepaper, 2006.

[6] The IETF Portal website; http://www.ipv6tf.org/news/newsroom.php

[7] *IntelliGrid Architecture – Communications Infrastructure Technologies*, Electric Power Research Institute (EPRI). http://intelligrid.info/IntelliGrid_Architecture/Technology_Analysis/Anl_Comm_Recomm.htm

[8] The Industrial Ethernet Book website. http://ethernet.industrial-networking.com/articles/articles.asp

[9] Julian L. Rrushi, "Employing IPv6 to Improve Layer 3 defence in SCADA Systems", *European CIIP Newsletter (ECN)*, Volume 2, Number 1, January / February 2006.

[10] Zhaoxia Xie, et al.; *An Information Architecture for Future Power Systems and Its Reliability Analysis.* IEEE Transactions on Power Systems, Vol. 17, No. 3, August 2002.

[11] Eric Byres, et al., *Worlds in Collision – Ethernet and the Factory Floor*, BCIT Research Paper.

[12] *Internet Protocol Version 6 - Federal Government in Early Stages of Transition and Key Challenges Remain*, United States Government Accountability Office (GAO), Report to the Chairman, Committee on Government Reform, House of Representatives, June 2006.

[13] S.S. Mohamed, M.S. Buhari, and H. Saleem; "Performance comparison of packet transmission over IPv6 network on different platforms", *IEE Proceedings: Communications*, Vol. 153, No. 3, June 2006.

[14] Connect One Webpage, http://www.connectone.com/ichips.asp

[15] Rolf Carlson, et al., *National SCADA Test Bed: A Summary of Control System Security Standards Activities in the Energy Sector*, October 2005.

[16] *Draft Recommended Practice for Network Communications in Electrical Power Substations*, C3TFI Working Group, IEEE Standards Activity, January 2006.

[17] "Draft Standard for Substation Integrated Protection, Control and Data Acquisition Communications"; *IEEE Power Engineering*; September 1999.

[18] Lennart Swartz, "Interoperability of Intelligent Electronic Devices in a Substation", *Power System Control and Management*, 16-18 April 1996, Conference Publication No. 421, 1996.

[19] *IEEE List of EtherType Values*; http://standards.ieee.org/regauth/ethertype/eth.txt

[20] Dacfey Dzung, et al, "Security for Industrial Communication Systems", *Proceedings of the IEEE*, Vol. 93, no. 6, June 2005.

[21] Sean Convery and Darrin Miller, *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)*, Cisco Whitepaper. http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf

[22] Drago Žagar and Saša Vidakovi, "IPv6 Security: Improvements and Implementation Aspects", *Proc. 8th International Conference on Telecommunications - ConTEL 2005*.

[23] *IPv6 Network Management*, Taipei, August 23, 2005 Presentation.

[24] Jérôme Durand, editor; *Final report on IPv6 management and monitoring architecture design, tools, and operational procedures*; technical report, 6Net project, October 2004. http://www.6net.org/publications/deliverables/D6.3.3.pdf

[25] *Inter-control Center Communications Protocol (ICCP)*, IEC Standard 60870-6 TASE.2, 1997.

[26] Gary Sevounts, "Cybersecurity Threats and the Power Grid", *World Energy Magazine*, Vol. 8 No. 1 – 2005.

[27] *Guide to Federal Agencies Transitioning to IPv6: IPv6 Best Practices World Report, Volumes 1 & 2*, Juniper Systems.

[28] Paul Oman, et al., *Attack and Defend Tools for Remotely Accessible Control and Protection Equipment in Electric Power Systems*, Schweitzer Engineering Laboratories, Inc.

[29] *ATIS IPv6 Report & Recommendation*, May 2006

[30] Alan Joch, *Stops along the IPv6 road: After drawing the map comes the hands-on work*, FCW.com, July 2006.

[31] Brian Carpenter, *Connecting IPv6 Routing Domains Over the IPv4 Internet*, http://www.cisco.com/web/about/ac123/ac147/ac174/ac197/about_cisco_ipj_archive_article09186a00800c830a.html

[32] *Effects of ICMPv6 on IKE and IPsec Policies*, Internet Engineering Task Force (IETF), http://www2.rad.com/networks/h2003/icmpv6/Effects%20of%20ICMPv6.html

[33] Davies, E.; Krishnan, S.; and Savola, P.; *IPv6 Transition/Co-existence Security Considerations*, IETF Draft, October 2006.

[34] Jordi Palet, *Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communications*, ISOC Member Briefing #13, May 2003.

[35] *DoD IPv6-Capable Approved Products List (APL)*, Joint Interoperability Test Command, http://jitc.fhu.disa.mil/adv_ip/register/register.html#router

[36] The IPv6 Forum website; http://www.ipv6forum.com/

[37] The IPv6 Ready Logo Program website; http://www.ipv6ready.org/frames.html

[38] The OPNET website; http://www.opnet.com/

[39] *The Impact of IP Version 6 on the Future Combat System*, Future Combat Systems Integrated Support Team, January 2004.

[40] Darrin Miller; “IPv6: The views from industry”; *The Industrial Ethernet Book*; Issue 27, July 2005.
http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=800

[41] Brian Batke and Paul Brooks; “IPv6: The views from industry”; *The Industrial Ethernet Book*; Issue 27; July 2005.
http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=802

[42] Lynn A. Linse; “IPv6: The views from industry”; *The Industrial Ethernet Book*; Issue 27; July 2005.
http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=801

[43] Andreas Pfeiffer; “IPv6: The views from industry”; *The Industrial Ethernet Book*; Issue 27; July 2005.
http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=803

— This page intentionally left blank —

Appendix B: Acronyms

ACS	Access Control List
ADA	Advanced Distribution Automation
AH	Authentication Header
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ASIC	Application Specific Integrated Circuit
BGA	Border Gateway Protocol
CGA	Cryptographically Generated Address
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DNP	Digital Network Protocol
DNS	Domain Name Server
ESP	Encapsulating Security Payload
FMS	Fieldbus Message Specification
GOOSE	Generic Object Oriented Substation Event (protocol)
ICCP	Inter-control Center Communications Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
IPv6	Internet Protocol Version 6
ISO	Independent System Operator
ISAKMP	Internet Security Association and Key Management Protocol
LAN	Local Area Network
MAC	Media Access Control (address type)
MIB	Management Information Base
MMS	Manufacturing Message Specification
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OSPF	Open Shortest Path First (protocol)
PCS	Process Control System

PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PPP	Point-to-Point Protocol
PSTN	Public Switched Telecommunications Network
RDBMS	Relational DataBase Management System
RPC	Remote Procedure Call
RIPng	Routing Information Protocol – Next Generation
QoS	Quality of Service
RFC	Request for Comments
RTOS	Real-Time Operating System
RTU	remote terminal units
SA	Security Association
SCADA	Supervisory Control and Data Acquisition
SLIP	Serial Line Internet Protocol
SNMP	Simple Network Management Protocol
SNMT	Simple Network Time Distribution Protocol
SPI	Security Parameter Index
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VCSE	Virtual Control System Environment
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WACS	Wide-Area Stability and Control System
WAMS	Wide Area Measurement System

Appendix C: Views from Industry

Following are the expert opinions of industry researchers, device/equipment vendors, and other industry participants. These opinions were obtained either through direct contact or from recently published interviews on industrial automation.

Security Entity - 10/27/06 discussion
Provider of tools to support security assessment of devices and implementations. Indicated that they have been working with device vendors that are currently interested in identifying vulnerabilities in their current products and implementation of existing protocol standards. Believed that IPv6 is something vendors are thinking about, but does not believe much development is occurring at this time. These companies are much more interested in implementing wireless systems with protocols; Bluetooth. They're getting request to identify vulnerabilities in supporting wireless protocols. Also working with network equipment vendors in assessing their IPv6 implementations. Believes that even these implementations of IPv6 are immature and that vulnerabilities are being identified.

Utility – August 4, 2006 email
In control systems, none of the current device/equipment or protocols specifies IPv6. Who allocates/controls the IPv6 address space? Current IPv4/IPv6 networks use a firewall/gateway to perform the address translation. The IPv6 specification does not describe a mechanism for IPv4 to know (e.g. error response) about IPv6 without address translation/gateway. Are there issues with this approach and what are all the other many issues in getting a combined IPv4/IPv6 infrastructure working? What are the security issues in a combined IPv4/IPv6 infrastructure? The combined infrastructure poses many challenges even before the industry can tackle the issues with the migration/re-specification of the entire utility SCADA infrastructure/protocols.

Device Vendor – 9/13/06
IPv6 is planned for all their products with IP connections. However, short terms needs of customers and maintaining existing releases are priority. Many products will support IPv6 to the degree that the third party operating system supports IPv6. In general, plans to move in that direction are out across all the product lines. It is likely still to be several years before all the products are released with IPv6 support promoted. IPv6 will provide opportunity for increasing security and any additional burden of computation will be accommodated with increasing processor performance.

Utility – 8/15/06
Expressed concern about cost of transitioning to IPv6 and where the funds will be obtained. IPv4 equipment is represents a substantial sunk cost. Agrees that the IPv4 address exhaustion is a real problem.

Electric Power Research Institute (EPRI) -
http://intelligrid.info/IntelliGrid_Architecture/New_Technologies/H3_Networking_Technologies.htm
Advantages/Strengths: IPv6 has increased address space and other advantages over IPv4. *Disadvantages/Weaknesses:* Because of the enormous investment in IPv4, and the limited additional benefits of IPv6, IPv6 has not yet been implemented widely, and not much progress has been made in convincing vendors of the need to convert from V4 to V6.

Senior Network Advisor **– *Rich Terzigni [Network World][OPNETWORKS-2006]***
Social Security Administration
We use all the add-ons for IPv4 that are also in IPv6. We have not yet identified any benefits of IPv6' that will help SSA in its mission. On address space, we manage our resources very well, so right now we don't need extra addresses. But if the desktop requires multiple addresses, that will dictate moving to IPv6. If we need more than one IP address per user, we'll have problems without IPv6. On auto-configuration of devices; SSA manages its IPv4 addresses centrally and plans to continue doing so with IPv6. SSA has no plans to use auto-configuration and instead will continue running Dynamic Host Configuration Protocol (DHCP) like it does with IPv4. We know by the IP address where the physical address is of that system. We have had that capability with our private class A block of IPv4 address space. We're going to do the same thing with IPv6. We have to be able to audit everything we do on our network, and that has to go down to the IP address. We won't use any ad hoc networking or auto configuration. We'll use DHCP." Concerning QoS, SSA already runs QOS on its IPv4 network. SSA takes advantage of its MPLS backbone network, and it has converged its voice, video and data traffic onto a single network platform. Concerning IPv6's end-to-end security model, SSA uses IPsec and has firewalls and other security mechanisms on its IPv4 network. SSA officials believe IPv6 will add vulnerabilities to its network rather than improve its security posture because of IPv6 features such as neighbor discovery and auto configuration bring with them a wide range of additional security vulnerabilities that are not an issue with IPv4. Although SSA has not identified a concrete benefit of IPv6, SSA needs to support the technology because it will be in use globally across the Internet. If IPv6 is widely deployed it could provide enhanced network management. For the transition, suggestions include supporting IPv6 in dual stack mode. SSA has chosen a dual stack approach to IPv6 deployment, which allows the agency to support both IPv4 and IPv6 applications for the foreseeable future. This approach requires the agency to have routers with a powerful enough engine and sufficient memory to support running IPv4 and IPv6 concurrently. Dual stacking is the best way to deal with the fact that many commercial software applications don't support IPv6 yet. All new equipment is IPv6 compatible but IPv6 is not turned on yet.

Information Security Researcher – ***Darrin Miller***, see [40] for interview transcript
Specialist in SCADA, embedded device and process control architecture and security analysis.
Industrial automation and process control has little direct interest in IPv6 at present and no impending applications absolutely dependent upon it because of a variety of reasons, most significantly that the adoption rate in process control of new platforms/ applications that can support IPv6 is a medium-long term issue. No vendor I am dealing with has expressed anything other than a prototype development environment in terms of platforms, much less the applications. Network Address Translation (NAT) is limited to the current computing paradigm of client to server. However, most IPv6 proponents quote three factors: mobility, ad hoc networks and peer-to-peer applications that are enough to invalidate NAT as a feasible option. I'll leave it up to you to make your determination, but I believe the mobility and ad hoc aspects will also be valid in process control networks. One could argue that a proliferation of IP-enabled devices will turn the traditional server/client relationship on its head. The standard network has few servers and many clients. Field device servers are many and the control stations - clients - are few. With this change network management could get out of control with simply too many servers to handle sensibly. This is a risk and why IPv6 is viewed as evolutionary as opposed to revolutionary in an effort to caution operators about the possible side effects of the explosion of devices. In addition this all adds new avenues of attack. These avenues are neither better nor worse than IPv4, they are just new considerations. In terms of network addressable field devices such as valves, sensors, pneumatics, or anything which could possibly 'benefit' from a degree of web services feedback monitoring as well as feed forward action commands over the network will affect the operator's ability to manage the process network both in terms of the network devices themselves as well as the information overload that may occur with the increased data flows. However, to start the data flows will be very similar to what is already in existence. Over time new applications will develop that leverage the mobility and open aspect of the IPv6 network will drive new application adoption that will change this data flow and management model, but I think that is a longer term proposition. This is very analogous to the use of IP for voice. The collection of networks widely called the Internet existed for over 15 years before the idea of putting voice on that network gained mindshare. In those 15 years lots of thought was put into managing this new flow of data and has continued to evolve as VoIP has grown in popularity. My personal opinion is that new applications using the mobile, ad hoc and open nature of the current IPv4 and IPv6 networks are going to be the drivers, not IPv6 unto itself. IPv6 does have benefits over IPv4, but the application that ONLY works on IPv6 needs to be developed before we see IPv6 take hold. Outside of process networks I see one of those applications being the mobility requirements for 4G (my term for the use of native voice encapsulation on a handset) that will drive the requirement for IPv6. Concerning industrial network providers see the in-built security layers of IPv6 as a source of encouragement to adopt the protocol. I am suspect of equipment vendors adopting IPv6 for any security reasons, since they are having a hard enough time implementing robust IPv4 stacks on their embedded devices. Eric Byres is making a nice living on showing how

vulnerable these devices are on being moved to Ethernet. Many operator tools (like network scans) have been demonstrated to cause security and reliability issues with these embedded devices. For this reason and also the very heavy computational load that IPv6 security mechanisms (public/private key cryptography, etc.) puts on an embedded system, I don't see IPv6 as a more secure transport being enough motivation to make the vendors move. They might move to IPv6 without security (similar to their move to IPv4 without security) if a new application paradigm is introduced that requires IPv6.

Open DeviceNet Vendors Association (ODVA) **– *Brian Batke and Paul Brooks*** [41]
ODVA is an organization that supports computing network technologies based upon the Common Industrial Protocol (CIP) and includes representatives of leading automation companies.
Today most organizations minimize their use of public IP addresses and operate their internal networks using that rests upon IPv4. Moving from IPv4 to IPv6 will require thoughtful planning in addition to effort to retool products and applications to ensure maximum interoperability. As automation product suppliers this gives us an obligation not just to implement what is best for our own individual components, but also to work with all parts of our customers' businesses, with other automation vendors, and with the major intranet and Internet infrastructure suppliers to ensure that implementations do not get in the way of information flow.

Digi International – ***Lynn Linse, Principal Engineer*** [42]
Digi International develops products and technologies to connect and securely manage local or remote electronic devices over the network.
IPv6 will eventually be the norm in protocol standard. The primary driving forces for adoption are, one, IPv6 support for mobility with its roaming IP capability, and, two, the political landscape associated with the uneven dispersion of IPv4 addresses. Note that large USA universities have more legal IPv4 addresses than whole countries like China have. So more than anything, companies selling internationally (outside the USA) will increasingly find IPv6 mentioned as a 'check-mark' on the Request-for-Quotation. It may not be required for operation, but will be useful for marketing. I would not be surprised if in the next few years China places import restrictions on products NOT supporting IPv6. I know of some Asian automation companies adding IPv6 to products expressly because their large North American competitors are not. Modern trends in Network-Address-Translation (NAT) and the widespread use of the Internet-community sanctioned 'Private Address' ranges like 10.x.x.x and 192.168.x.x have largely made IPv6 a non-issue for industry. Since most SCADA and automation users are on private networks anyway, using a 10.x.x.x address scheme offers for example over 65 thousand subnets with 250+ nodes each. Few automation systems would use even 1% of this address space. Even if industry starts making wider use of wireless "Public" IP nodes, the addresses used will be provided by the service provider.

Bernecker + Rainer Industrie-Elektronik **– *Andreas Pfeiffer*** [43]
B&R develops products and technologies for industrial process control systems.
As it is with every new technology there are a few early adopters starting immediately with implementations and a majority looking at the real value first. Thus, many are waiting for others to make the first step. Providers are hesitant since they cannot evaluate what difficulties they may face when migrating to IPv6, and there is no real demand from the end-user for just another protocol. Frankly, end-users don't really care what protocol transports their data from end to end. They expect the providers to take care about the detail. Some component vendors have introduced some IPv6 enabled beta versions of their products. However, it is still too much of a risk for them to fully commercialize these products. Perhaps carriers may even fear the risk that regular connection-based services may be replaced by the improved packet-oriented services enabled by IPv6. Migrating from IPv4 to IPv6 does not only affect routers and network devices; it also impacts both software and hardware. Literally every occurrence of an IP-number in data structures of operating systems, data bases and applications need to be changed. Thus many systems cannot be changed in short time - or will ever be touched at all. There are also comments that the new protocol is over-featured. Some experts predict that only a down-sized version will be able to make it. In addition, techniques like network address translation has taken some pressure off the potential address space limitations of IPv4. Now, what does this all mean for Industrial Ethernet? There is simply no need to implement IPv6 immediately. However, the industrial market needs to be prepared when the IT market begins adopting IPv6 on a broad basis. The present uncertainty pervading the world of office automation underlines the importance of implementing only international standards-based Industrial Ethernet technology.

— This page intentionally left blank —

Appendix D: Interoperability and Test Activities

Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture. The IETF provides descriptions of protocol standards via Request for Comments (RFCs). Although many of the RFCs describe protocol standards other RFCs provide information or application guidance to protocol users and implementers.

IETF RFC #	Name and Description
4057	IPv6 Enterprise Network Scenarios: This document presents three base scenarios to be used as models by enterprises defining specific scenarios.
3750	Unmanaged Networks IPv6 Transition Scenarios:
4038	Application Aspects of IPv6 Transition:
3756	IPv6 Neighbor Discovery (ND) Trust Models and Threats: This document defines the types of networks in which the Secure IPv6 Neighbor Discovery mechanisms are expected to work and the threats that the security protocol(s) must address.
2874	DNS Extensions to Support IPv6 Address Aggregation and Renumbering

Internet Engineering Task Force (IETF) IPv6 Operations (v6ops)

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture. A subgroup in the IETF's operations and management area is the IPv6 Operations working group (v6ops) [v6ops]. The v6ops working group develops guidelines for the operation of a shared IPv4/IPv6 Internet and provides operational guidance on how to deploy IPv6 into existing IPv4-only networks. The group's guidelines also address new IPv6 network installations. A key role of the group is to publish informational Request for Comments (RFCs) that identify potential security risks in shared IPv4/IPv6 networks and document mitigation strategies. Additional value provided by this group includes guides to network operators and users on which approaches of deploying IPv6 work and which approaches do not work. An excellent listing of RFCs applicable to IPv6 and brief summaries of each can found in [JuniperVolumn2]. http://ops.ietf.org/lists/v6ops/

Issues related to specific IPv6 protocols or applications and their operation and deployment are addressed by other IETF groups. These other groups address issues with IPv6 applications such as Transport Protocols, Routing Protocols, DNS or Sub-IP Protocols. IETF FAQ Webpage – http://www.ipv6.org/

Moonv6 Project

The Moonv6 test project is led by the North American IPv6 Task Force and was primarily prompted by the U.S. Department of Defense (DoD)-mandated transition to IPv6 by 2008 for all inter- and intra-networking. The project is operated by the University of New Hampshire InterOperability Laboratory (UNH-IOL) and is designed to promote adoption of the new IPv6 protocol throughout the industry. A major function is to provide a peering network for the testing of IPv6 implementations for interoperability and verification of functions within the IPv6 protocol and architecture [moonv6web]. The peering network is intended to support testing configurations that could result in problems when deployed if the device under test does not operate properly with other devices connected to it.

IPv6 Portal

This organization creates technical documents and white papers describing technical aspects of IPv6. Included are reports describing IPv6 related vulnerabilities and potential issues. www.ipv6tf.org

IPv6 Forum

IPv6 is promoted worldwide by this group. The group provides reports and other documentation on IPv6 implementations and best practices. www.ipv6forum.com

International Electrotechnical Commission

IEC 62351 Data and Communication Security

- IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP (these security standards cover those profiles used by ICCP, IEC 60870-5 Part 104, DNP 3.0 over TCP/IP, and IEC 61850 over TCP/IP)
- IEC 62351-4: Data and Communication Security – Profiles Including MMS (these security standards cover those profiles used by ICCP and IEC 61850)
- IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0) (these security standards cover both serial and networked profiles used by IEC 60870-5 and DNP)
- IEC 62351-6: Data and Communication Security – Security for IEC 61850 Peer-to-Peer Profiles (these security standards cover those profiles in IEC 61850 that are not based on TCP/IP – GOOSE, GSSE, and SMV)

6NET Project

6NET project built a native IPv6-based network connecting sixteen countries in order to gain experience of IPv6 deployment and migration from existing IPv4-based networks. 6Net project webpage – http://www.6net.org/

Appendix E: For More Information

Author	Brian Van Leeuwen (bpvanle@sandia.gov) Critical Infrastructure Systems Department Sandia National Laboratories P.O. Box 5800 Albuquerque, New Mexico 87185
National SCADA Testbed (NSTB) Project	Jennifer DePoy, Manager (jdepoy@sandia.gov) Critical Infrastructure Systems Department Sandia National Laboratories P.O. Box 5800 Albuquerque, New Mexico 87185