PNNL-19474

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Secure and Efficient Routable Control Systems

TW Edgar
MD Hadley
DO Manz
JD Winn

May 2010

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm**

This document was printed on recycled paper.
(9/2003)

PNNL-19474

Secure and Efficient Routable Control Systems

TW Edgar
MD Hadley
DO Manz
JD Winn

May 2009

Prepared for the U.S. Department of Energy's Office of Biological and Environmental Research under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Table of Contents

1.0 Introduction 1
1.1 Current Environment..2
1.2 Document Purpose 3
1.3 Scope 3
2.0 Approach 4
3.0 Control System of the Future...6
3.1 Characteristics 6
3.2 Architecture..9
4.0 Derived Requirements 11
5.0 Survey..12
5.1 Application Layer Options 13
5.2 Transport Layer Options 14
5.3 Network Layer Options...15
6.0 Solution...17
6.1 Network Layer...17
6.2 Transport Layer 18
6.3 Application Layer..19
6.4 Requirements Mapping 19
7.0 Roadmap..22
7.1 Step 1 – Enable Existing Security 22
7.2 Step 2 – Aggregation Point Security 24
7.3 Step 3 – End Device Protection...28
7.4 Step 4 – Optimized Security..30
7.5 Requirements Mapping 33
8.0 Summary..35
Appendix A – OSI Model 36
Appendix B – Routable Transport Survey 38

Table of Figures

Figure 1: Generic Control System Architecture 1
Figure 2: Current vs. Future Communication Sequence Diagram..8
Figure 3: Future Control System Architecture...10
Figure 4: Protocol Stack Diagram of Survey 13
Figure 5: Proposed Protocol Stack...17
Figure 6: Existing Security Methods 24
Figure 7: Aggregation Point Security 27
Figure 8: End Device Protection...30
Figure 9: Protocol Stack Streaming to Packet Format 31
Figure 10: Optimized Security..32
Figure 11: OSI Model 36

Acronyms and Abbreviations

ATM	Asynchronous Transfer Mode
COTS	Commercial-off-the-Shelf
CROP	Control system Routable Object Protocol
CSTP	Control system Secure Transport Protocol
DCCP	Datagram Congestion Control Protocol
DCS	Distribution Control System
DiffServ	Differentiated Services
DNP	Distributed Network Protocol
DSCP	Differentiated Services Code Point
DTLS	Datagram Transport Layer Security
FIPS	Federal Information Processing Standard
GRE	Generic Route Encapsulation
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
I/O	Input/Output
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
MBAP	Modbus Application Protocol
MPLS	Multi Protocol Label Switching
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OC	Optical Carrier
OPC	OLE (Object Linking and Embedding) for Process Control
OSI	Open System Interconnection
PMU	Phasor Measurement Unit
QoS	Quality of Service
RTP	Real-time Transport Protocol
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCTP	Stream Control Transmission Protocol
SEM/SIEM	Security Information and Event Manager

SSCP	Secure SCADA Communications Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
SYN	Synchronize flag in TCP
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network

1.0 Introduction

The control system environment that monitors and manages the power grid historically has utilized serial communication mechanisms. Leased-line serial communication environments operating at 1200 to 9600 baud rates are common. However, recent trends show that communication media such as fiber, optical carrier 3 (OC-3) speeds, mesh-based high-speed wireless, and the Internet are becoming the media of choice. In addition, a dichotomy has developed between the electrical transmission and distribution environments, with more modern communication infrastructures deployed by transmission utilities.

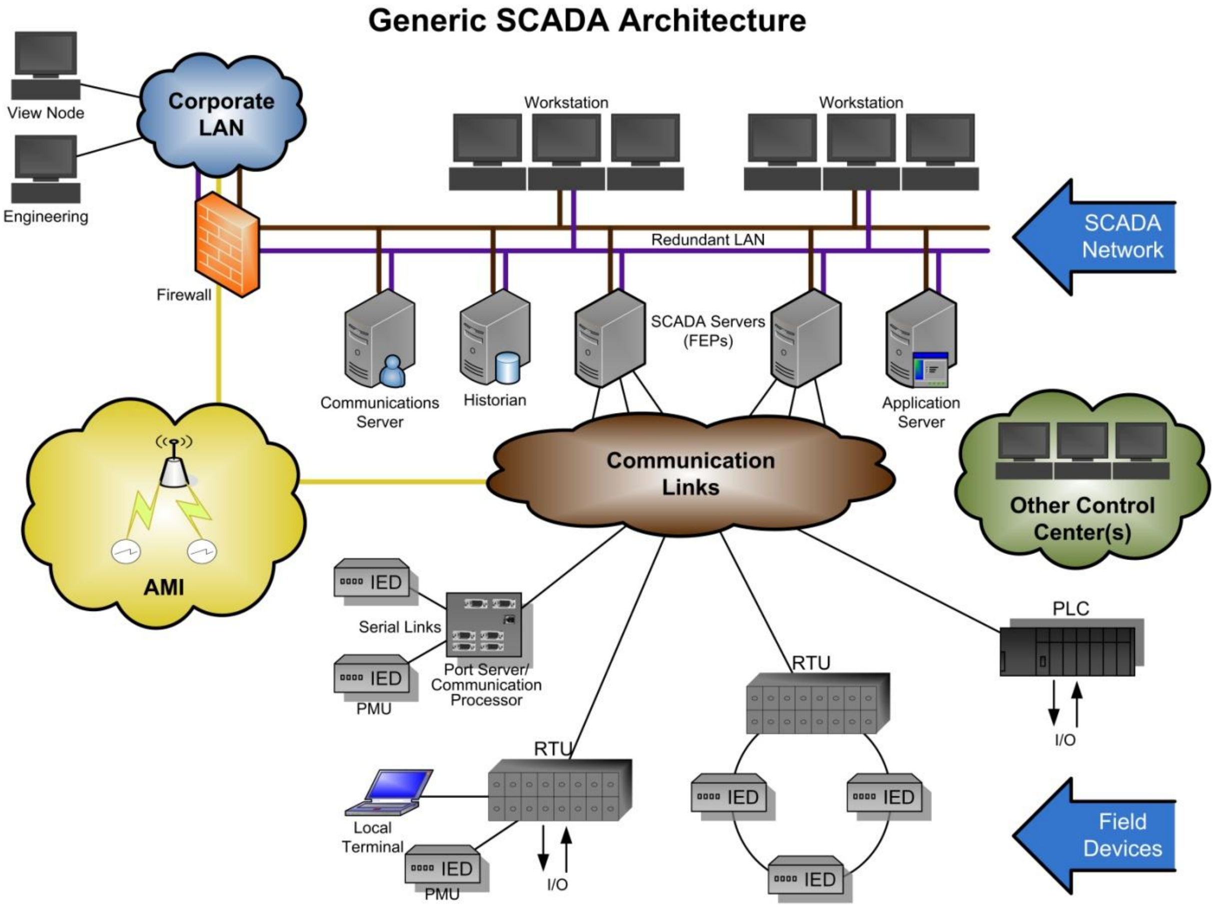

Figure 1: Generic Control System Architecture

The preceding diagram represents a typical control system. The Communication Links cloud supports all of the communication mechanisms a utility might deploy between the control center and devices in the field. Current methodologies used for security implementations are primarily led by single vendors or standards bodies. However, these entities tend to focus on individual protocols. The result is an environment that contains a mixture of security solutions that may only address some communication protocols at an increasing operational burden for the utility. A single approach is needed that meets operational requirements, is simple to operate, and provides the necessary level of security for all control system communication. The solution should be application independent (e.g., Distributed Network Protocol/Internet Protocol [DNP/IP], International Electrotechnical Commision [IEC] C37.118, Object Linking and Embedding for Process Control [OPC], etc.) and focus on the transport layer. In an ideal setting, a well-designed suite of standards for control system communication will be used for vendor implementation and compliance testing. An expected outcome of this effort is an international standard.

1.1 Current Environment

Control system environments are designed to provide centralized control of dispersed physical processes. The data communicated across control systems is used to monitor the state of the physical processes in operation as well as to provide the remote control capability to physically alter the state of the system. The physical processes often have staff and public safety concerns in addition to monetary considerations. Therefore, the data transmitted across the control system has high security requirements for data integrity.

Current control system environments are a mix of legacy serial communication and routable IP communication. Serial communication is slowly being replaced with IP communication as equipment is updated. While serial is not within the scope of this document, the original Secure SCADA Communications Protocol (SSCP) project provides the necessary security to protect serial communication.

Current routable control system communication over IP is often unsecured; for example, a utility using DNP/IP over utility-owned fiber. Of the protocols that can provide security, the constraints and requirements of control system traffic are ignored in favor of a one-size-fits-all security solution. Consider the use of Internet Protocol Security (IPsec) to establish a virtual private network (VPN) connection over which all communication between a control center and a substation flows. Control and telemetry traffic require very different security policies but are treated the same in VPN tunnels. Internet security solutions are being applied to routable control system traffic without consideration for their requirements. The fundamental limitation of current control system protocols that operate over IP is their assumption that all traffic is equal and should be treated identically. This means that control traffic, data telemetry traffic, physical security data, and engineering maintenance are all secured, tagged, and transported in an identical manner, regardless of how the security objectives for the traffic might differ.

As control system traffic continues to integrate with corporate and public networks, the attack surface increases proportionally. Devices that were disconnected from the Internet are now directly or indirectly accessible worldwide. While this interconnectivity reduces costs and increases productivity, the security risks must be addressed before widespread adoption. The advantage of using commercial-off-the-shelf (COTS) applications, protocols, and devices is that it makes deployment and integration with corporate and public networks much easier. Using popular and well know protocols means that security can often be leveraged from the information technology (IT) world and applied to the control system implementations. However, while this solution unarguably provides security, it will not consider the constraints and requirements of communication traffic in control system networks.

While Internet traffic employs a variety of technologies, the vast majority of all user communication relies upon two popular protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Both of these protocols operate on top of the ubiquitous and foundational IP. As online movie and TV watching, Voice over IP (VOIP) communication, online gaming, and other intensive forms of traffic have increased, the limitations of TCP and UDP have become apparent. TCP provides reliable, ordered communication, while UDP provides no quality of service guarantees. They are the two extremes of data transport service. However, these new forms of communication are unsuited for TCP communication and require more assurance than UDP can provide. Numerous new protocols have been or are being developed to suit the streaming, data-intensive nature of the new network traffic. Similarly, control system network traffic should not rely on a one-size-fits-all approach of using the well proven but inflexible TCP or the bare-bones UDP.

1.2 Document Purpose

Simply stated, the purpose of this document is to describe the methods to secure routable control system communication in the electric sector. The solution described is applicable to generation, transmission, and distribution environments. These diverse implementations utilize different protocols and communication media and have different performance expectations. The challenge is to define an approach to extend and implement the security objectives of the SSCP into the routable communication infrastructure in a manner that applies to all of these environments.

This document takes a long-term view of the future control system rather than focusing on immediate needs. The intent is to creatively determine how a control system could function in the future. Consider an environment where real-time awareness is measured, versus today’s norm of estimating state based upon a sample of available data points. An important question to answer is how the type of data and collection methods will change in the future. Once that vision and associated characteristics are established, existing technology can be examined for applicable use and gaps can be identified.

The objectives of this document are presenting a vision for a future control system, identifying characteristics and requirements that govern communication, and presenting a four-step implementation roadmap for the identified goals. The final step also includes the specification of a new protocol for future routable control system communication that incorporates the security objectives of the SSCP in addition to concepts such as priority and quality of service. This future vision can be used to direct the implementation of secure, routable control system communications for future electric sector systems.

1.3 Scope

The scope of this project covers routable traffic within control system networks. This traffic includes telemetry, control, and event data. The primary goal is to introduce a future secure routable control system environment. To encourage awareness and adoption, a roadmap is also provided as a means of transitioning from today’s insecure state to the more secure future.

This document will focus on securing control system traffic. Securing engineering access and serial communication is not within the scope of this document. Existing solutions such as Transport Layer Security (TLS), Secure Socket Layer (SSL), Secure Shell (SSH), or SSCP provide the necessary security and functionality. Corporate IT network communication security (such as e-mail and VOIP) is also beyond the scope of this document and is extensively documented elsewhere.

2.0 Approach

The security objectives typically found in IT networks (confidentiality, integrity, and availability) differ in importance for control systems. The nature and purpose of the data in the control system network cause availability and integrity to be critically important. Confidentiality is therefore less important.

With these objectives in mind, a discussion of the approach to secure routable control system communication necessitates a brief history on the development of the SSCP. The SSCP was designed to secure serial control system communication with support for legacy, current, and future control system environments. The majority of this communication is point-to-point, and baud rates as low as 1200 are common. Serial control system communication is also typically highly predictable with data often being repeated in time cycles of less than one minute.

Standard cryptographic principles for authenticating and securing a communication session must be applied. Care must be taken to ensure that cryptographic protection of serial control system communication begins with strong session negotiation and that the authenticator is not predictable. To achieve a secure serial cryptographic solution, the SSCP enhanced and expanded existing technologies available in routable networks. For example, Diffie-Hellman was selected for session negotiation not only because it is proven but also because it allows for a secure session to be established over an untrusted communication media. The authentication algorithms selected by the SSCP are included in Federal Information Processing Standard 198 (FIPS-198), and key update recommendations come from National Institute of Standards and Technology (NIST) guidance. As an example, to provide a unique identifier for each predictable control system message, the SSCP uses the output of a NIST-approved hash algorithm to create a pseudo-random number specific to the control system message.

Migrating the control system specific security functions provided by the SSCP to routable control systems poses an interesting challenge. Unlike the serial communication environment, many solutions exist today to secure routable communication. As a prime example, consider TLS, which provides both encryption and authentication for data flowing over a communication link. Deploying the SSCP in this manner in essence duplicates TLS with the addition of configurable authentication lengths. While improving performance, this approach does not provide new security. A more thoughtful approach is required that identifies requirements and carefully considers all communication options.

The approach used to derive the solution described in this document was to first define the end goal. Working backward from that end goal, requirements were defined, technology research was performed, and a solution was developed. This section outlines each step of the approach used to arrive at the solution, which will be detailed in subsequent sections.

To define the end goal, a vision for an ideal control system of the future was characterized. All legacy restraints and concerns were disregarded during this process to allow for the creation of an elegant and efficient environment. The trends of today's cutting-edge control system applications as well as the capabilities of current IT technologies were leveraged.

From this future vision, control system environment requirements for communication were derived. These requirements distilled the environment into the core functional elements necessary to achieve its design. The requirements developed at this stage are the driving force behind the solution described in this document.

As stated above, current IT technologies were leveraged in the design of this solution. Numerous IT communication protocols have been developed to achieve many differing goals. The intent is not to recreate something that is already available in the community but to leverage as much work in the public domain as possible. IT transport layer protocols and a few network and application candidates were surveyed to determine if some or all of the derived requirements could be met. The benefits and drawbacks of each protocol were defined as they relate to the requirements of the end goal.

Leveraging the protocol survey, a communication stack for the future control system environment was defined. This stack is designed to cover the derived requirements of the future control system environment. It is unrealistic to expect vendors and asset owners to discard their current systems and start from scratch. Therefore, a technology roadmap was developed with multiple intermediary steps to chart a course from current control system environments to reach the future routable control system solution.

3.0 Control System of the Future

Control system data requirements should be the driving factor for designing transmission and security. Not all routable control system communication should be treated equally. A secure routable SCADA protocol that distinguishes differing control system traffic and secures, transports, labels, and provides appropriate quality of service will be better suited than extending existing routable (primarily IP and TCP) security protocols. A tailored solution will address the control system traffic more specifically than simply deploying a solution that ignores control system constraints. A targeted protocol stack will benefit the industry immediately by providing secure control system communication and, in the long run, benefit future maintainers by distinguishing the appropriate traits for all traffic while being modular and extensible.

Before routable control system communication becomes too entrenched with proprietary or piecemeal approaches, a step back is needed to determine what kind of routable communication is necessary for the application. To determine the vision, questions such as the following were asked:

- Will one existing protocol be able to satisfy all the requirements of the differing traffic types?
- Should legacy protocols be used, or should some measure of future proofing be incorporated to allow control system networks to adapt to future pressures and needs?
- Will a "push" architecture prevail over the current "pull" methodology?
- Will the security objectives of future control systems be the same as today?

In the end, while security must remain a priority, reliable availability must be guaranteed; a simple portage of Internet and commercial applications may not be up to the task.

The envisioned future control system will have separate communication channels for telemetry, control, and security event data. These channels are built around the security and operational requirements of the data. With routable communication, the old Master-Slave architecture is no longer a requirement for sensor telemetry, which can now be operated in a data-streaming model. By utilizing a streaming format, operators can improve situational awareness for their systems. Supervisory control traffic, on the other hand, should be reliable, fault tolerant, authenticated, and encrypted. Additional types of traffic can be formulated as needed, but a one-size-fits-all approach will not allow for the finer granularity that maximizes the limited resources available and respects the appropriate constraints for control system traffic.

Instead of continuing the porting of legacy control system solutions to the routable world, the proposed solution is creating a new communication stack from the ground up that uses the beneficial attributes of the environment while meeting the needs of the data. Now is the time to redress issues with current IP routable control system communication before too much traction and momentum is developed.

3.1 Characteristics

The control system environment of the future will continue to have many of the characteristics and constraints of today's environment, but additional reliability and security characteristics must be included to meet the needs and growth of the future.

Communication for control system networks can be identified based upon data type characteristics rather than other traditional forms of categorization. Broadly, communication can be separated into telemetry, control, and event data types. Telemetry traffic includes all control systems information traffic, such as

SCADA data acquisition and phasor measurement unit (PMU) data. Control traffic contains all management and operational communication for the control systems; examples include SCADA supervisory control and distribution control system (DCS) control traffic. The event data collected will then provide operators with information regarding physical security, the health of cyber security mechanisms, and anomalies in expected communication patterns. This data is crucial to reliable operation, but the order of messages may not be critical to analysis. For example, if two events are received out of order, their significance is not devalued. All events will contain a system-synchronized timestamp. Applications will use this timestamp to correlate significance to other events. The transport of events across the system cannot be expected to arrive to centralized processing applications in order; therefore, the analysis must be able to handle out-of-order events and all events should be processed.

Also, each traffic data type should have differentiated security mechanisms. Based on their unique communication requirements, differing confidentiality, integrity, and availability security policies will be placed upon the distinct traffic. For example, control system traffic should always be authenticated and must travel over reliable, fault-tolerant connections that provide high availability and possibly redundant means of communication. Telemetry traffic must also be authenticated, but it does not require the same order of availability as control messages. Depending on the nature of the telemetry data (e.g., customer data, financial data, corporate proprietarily data), the traffic might optionally be encrypted. This traffic can be considered best-effort communication. Often near real-time or real-time information, telemetry is required for the safe and secure operation of control systems and the telemetry traffic needs to be treated as such. Event traffic must be authenticated and optionally encrypted, similarly to telemetry, but the speed and reliability of this form of traffic should never supersede control and telemetry traffic. A minimal best-effort approach will allow the eventual delivery of the event traffic without interfering with higher availability information.

Control system communication will fall into three categories. Messages that require a connection will use a protocol that allows for session or connection establishment. Connection-oriented communication is defined as guaranteed delivery of data. Conversely, connectionless-oriented communication operates via best-effort delivery. Messages can be further divided into two categories based on order. Order does not denote if the application data has an ordering but instead refers to the requirements of data delivery and receipt. A connection with ordering channel buffers future packets until it receives the next packet in the order. A channel with a connection but without order does not buffer any packets and accepts them out of order, but ensures all packets are delivered. A connectionless with order channel drops any packets older than the last accepted packet. Finally, a connectionless without order channel accepts all packets as they come. Some control system traffic will not require connections or sessions but must arrive in order, while other traffic will require both sessions and order. Communication data types can be directly mapped to these communication categories.

The three varieties of communication are:

- connection with order (control data)
- connection without order (event data)
- connectionless with order (telemetry data).

In addition to the security policy delimitations that will be placed on control system traffic, prioritization and varying quality of service (QoS) will provide added functionality and security for future control system networks. The explicit labeling of the various traffic types with differing levels of service guarantees will allow vital traffic (such as control commands) to have the greatest right of way in times of resource scarcity. The next level of service can be provided to telemetry to verify that a viable common operating picture is established and maintained. The lowest level of service can be for batch and event data where the traffic can take a considerable amount of time and suffer multiple retransmissions of information without adversely affecting the operational safety and security.

A characteristic of current control systems that will continue into the future is a focus on data-centric as opposed to user-centric communication. The information security and reliability policies focus on end device communication. This differs from environments where user access to data is the focus. For example, traditional approaches of authenticating users to objects are not accurately reflected in the data-centric future control system environment.

As additional functionality and greater features are added to control system environments, increased opportunity for security and reliability can be realized. Multi-homing and multi-path communication are two such examples. Multi-homing provides increased reliability by allowing devices to connect to the network in multiple complementary ways. A single device might have multiple links to the control system network, the corporate IT network, or even the Internet. Multipath communication provides redundancy in communication exchanges. In addition to multiple means of connecting, devices will have multiple redundant paths on which communication can travel. This means of communication will provide automatic failover redundancy for control system communication traffic.

The control system communication of the future will be push-based rather than pull-based. With increased availability and security, the archaic method of requesting information will be supplanted by an automatic pushing of applicable information to the relevant consumers. Devices will no longer wait to be asked for information; rather, they will utilize all the preceding characteristics to provide safe and secure communications to the appropriate upper-level devices. The move to push-based communication will increase the quality of the operational common operating picture and will allow quicker responses to changes in the control system environment. See Figure 2 for a visual depiction of the sequence of communication between the current polling model and the future push model. As can be seen, the streaming nature of the push-based model increases the efficiencies by all devices simultaneously transmitting data at the same time during each time slice.

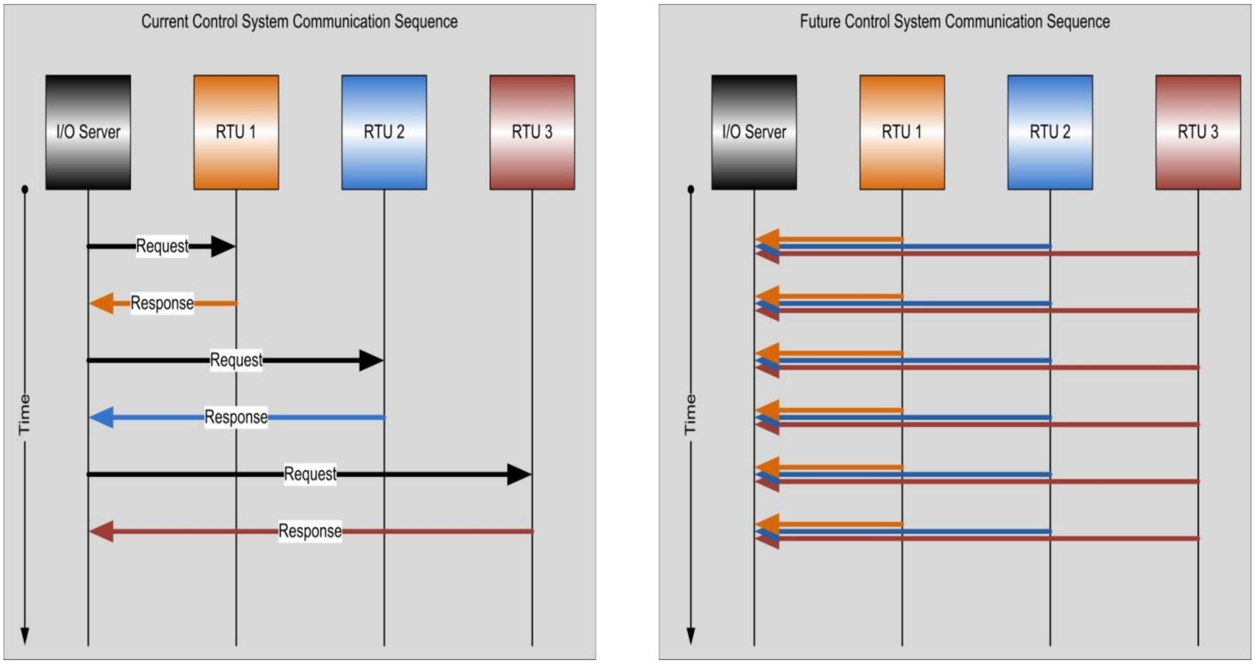

Figure 2: Current vs. Future Communication Sequence Diagram

In the future, a convergence between SCADA and synchrophasor environments will occur. Today, the same type of data is repeatedly requested by the SCADA system. Typically, analog values, digital values, and status information are requested on a predictable schedule. Synchrophasor data, on the other hand, is streamed from field devices over UDP communication. In both cases, the merging of these two will provide SCADA data to be received from the field in a timelier manner. The benefit will be improved situational awareness.

3.2 Architecture

The future system will support the logical and/or physical separation of communication mechanisms by data type or function. Today it is common to use a single network in the substation to handle all communication needs—engineering access, physical security, SCADA data, etc. Combining data types and networks in this manner increases the attack pathways available to an adversary and actually makes the adversary's job easier. Segmenting traffic by type and securing the interfaces between them reduces risk and helps to prevent an attack on one system from easily becoming an attack on all systems.

Separating traffic by type also allows for the elimination of the one-size-fits-all security mentality. Data types with different security requirements can be protected uniquely. Separating traffic by type also leads to the implementation of a new data acquisition scheme. Instead of polling for information as is done today, a push configuration for telemetry can be used. Not only is this more efficient but also the method is already used for synchrophasor measurements. In short, the future could see a convergence of synchrophasor and SCADA technologies and protocols.

Between the control room and remote stations will be a cloud of routing equipment. Depending on the size of the control system, this cloud could consist of one routing device or many. The routing devices in the future architecture will be configured to provide QoS custom fit to each data type. Therefore, if the network is saturated with a higher-priority packet, such as a control command, it will give priority to the control command. This capability provides the ability to maintain the low latency requirements in a routable network necessary for this environment.

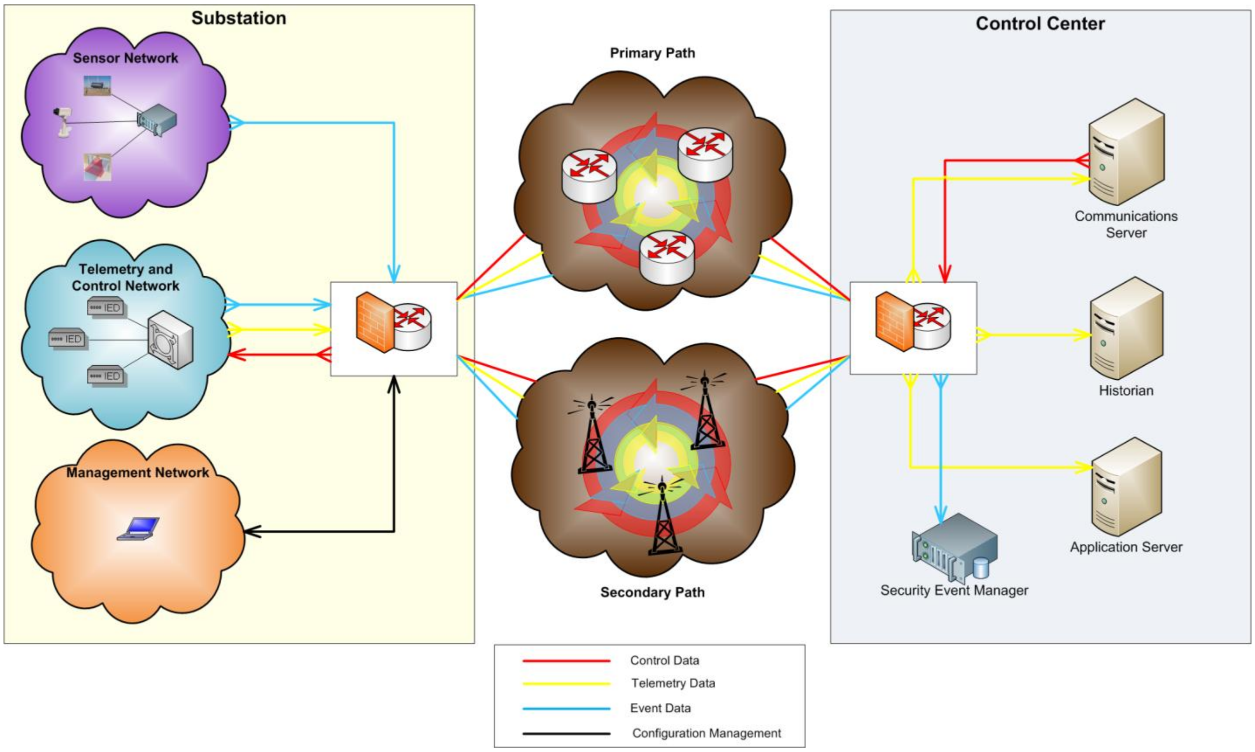

Figure 3: Future Control System Architecture

Because the reliability of the network is critical, the future architecture will have a secondary path that traffic can use when the first path is unavailable. The secondary path could be a logical path simply using a different route through the network, but generally the secondary path will use a completely separate communication infrastructure. The primary path could be the more reliable connection, such as a fiber backbone, and the secondary path could be less reliable, such as a microwave or cellular backhaul. The devices and network infrastructure will have the capability of automatically choosing the correct path.

Figure 3 depicts the future control system architecture defined in this section. At the substation, communicating devices are segregated into local area networks (LANs) based upon common functionality and data characteristics. If a communication problem arises on one LAN, due to malicious, inadvertent, or natural causes, the other LANs are protected and not impacted. The backhaul network between remote stations and the control center will provide redundancy. The primary path in the picture displays a more reliable path, such as a fiber network, with a secondary less reliable and more costly path such as microwave or cellular towers. Control system data will use multiple transmission streams to separate the data so that it can be operated more efficiently, routed with QoS, and delivered to the appropriate applications.

4.0 Derived Requirements

The definition of a future control system provides a good picture of the environment but it does not provide the necessary actionable requirements for developing a secure routable communication stack. Therefore, the future control system vision is distilled into derived requirements in this section.

- Transport channels must be configurable to meet the requirements of the following data types:
  - Telemetry
  - Control
  - Event.
- Telemetry data must be streamed in a push architecture.
- Telemetry data must be authenticated.
- Telemetry data may optionally be encrypted.
- Telemetry data must be a best-effort transport.
- Telemetry data must be ordered.
- Control data must be reliable transport.
- Control data must be authenticated.
- Control data must be encrypted.
- Control data must be in order delivery.
- Control data must be highest-priority data with best available quality of service.
- Event data must be authenticated.
- Event data must be encrypted.
- Event data must be reliable transport.
- Event data must be un-ordered delivery.
- There must be a transport layer mechanism to accommodate priority of service when more than one data channel is present on a device.
- Protocol stack must provide multi-homing and multi-path capabilities.
- Transport layer must provide management of priority of service.
- Transport layer must provide management of multiple distinct streams.

5.0 Survey

To make the required impact, a survey was conducted to determine the state of industry and to minimize any duplication of effort. The following are several potential protocols that operate at varying layers of the network communication stack. It is important to remember that any application message sent involves a protocol from each layer. This means that a selection of a protocol at one layer does not preclude selection of a protocol at another layer. First, the upper layer (predominantly application layer) protocols are described. Next, the transport layer provides the majority of options for security, reliability, and quality of service. Ultimately, the lower layer combines data link and network link or Internet link layers. The survey performed was not a complete protocol survey. Protocols were only included in the survey if they contained characteristics fulfilling some of the requirements set forth in Section 4.0, "Derived Requirements." The text provided in this section is a summary of the findings in the survey. See Appendix B – Routable Transport Survey for a more complete and extended survey of transport layer protocols.

Figure 4 displays the surveyed protocols arranged into a network stack. The colors of the boxes denote the different stack layers at which the protocols reside. Because transport layer security is not an independent layer, it is represented by thinner boxes. The terminal server and Multi Protocol Label Switching (MPLS) are also represented with thinner boxes because they are both tunneling protocols of a sort and do not fit directly into any one layer. An attempt was made to denote which protocols fit together via a vertical progression. However, all of the application layer protocols (except for the Terminal Server) can generally work on any of the transport layer protocols. The white space above SCTP represents its built-in security capabilities, which can operate independently of transport layer security protocols or with Datagram Transport Layer Security (DTLS) or TLS.

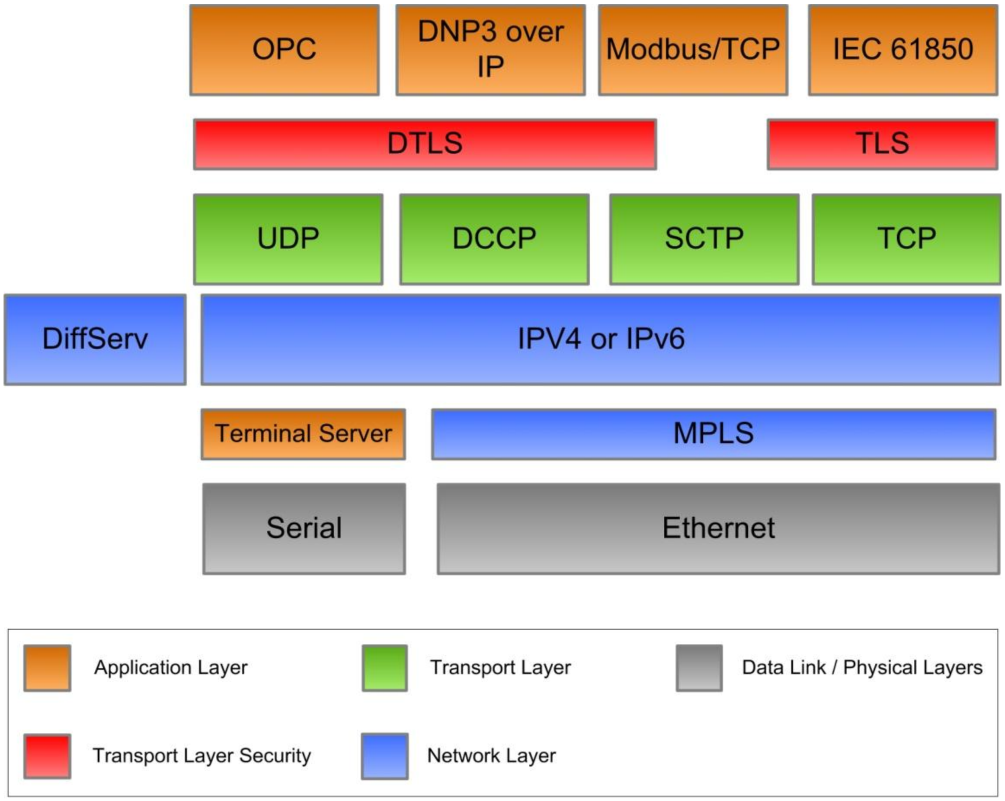

Figure 4: Protocol Stack Diagram of Survey

5.1 Application Layer Options

Terminal Server – A terminal server provides remote network access to a connected serial device. Cisco’s Generic Route Encapsulation (GRE) Tunneling and Dymec’s Port Server are examples of available terminal server technologies.
Benefits: A terminal server requires no changes to current legacy protocols.
Drawbacks: It is a solution for transitioning legacy equipment to routable communication; therefore, it is not a routable solution and carries with it all of the inappropriate characteristics of serial traffic.

Modbus TCP – Modbus TCP is a specifically created protocol that writes a new message header and strips out the payload from Modbus[1] communication. The Modbus Application Protocol (MBAP) header is added to the message and the checksum is removed[2] and placed into an Ethernet Frame then into a TCP packet.
Benefits: Modbus TCP was developed for routable traffic, has moderate market penetration, and is well understood.
Drawbacks: It does not allow the separation of control and telemetry data into separate channels and is not flexible enough to handle all applications.

Modbus over TCP (or Modbus via TCP) – Modbus over TCP simply provides a total TCP encapsulation of the Modbus message. The payload is the original intact unmodified Modbus message. A discussion provides some justification for why Modbus chooses TCP over UDP for connection-oriented

[1] http://www.modbus.org/faq.php.

[2] http://www.modbus.org/faq.php

traffic. While DNP3 operates on layer 2 (data link), the encapsulated protocol message is able to take advantage of protocols and features much higher on the stack.
Benefits: Modbus over TCP is well understood and has extensive market penetration.
Drawbacks: It is not built for routable communication. It does not allow the separation of control and telemetry data into separate channels and is not flexible enough to handle all applications.

DNP3 (Distributed Network Protocol) over IP – DNP3 over IP is much like Modbus over TCP, in that the entire DNP3 message is encapsulated in an IP message[3]. Typically, both TCP and UDP protocols can be used on top of the IP layer.
Benefits: DNP3 is robust and has extensive market penetration.
Drawbacks: It is not built for routable communication and does not allow the separation of control and telemetry data into separate channels.

OPC (OLE [Object Linking and Embedding] for Process Control) – OPC is a series of protocol standards that specify a common interface to process control data.
Benefits: OPC has extensive market penetration and support.
Drawbacks: OPC has high overhead and does not allow the separation of control and telemetry data into separate channels.

IEC 61850 – IEC 61850 is a standard for the design of substation automation. It provides abstract data models to frame protocols and allow for interoperability. Its goal is to create a single substation protocol.
Benefits: It is designed for routable communication and is more flexible than DNP3.
Drawbacks: It has limited penetration in North America.

5.2 Transport Layer Options

TCP (Transmission Control Protocol) – TCP provides reliable, in order, flow control, congestion control, and error-free messages (checksums).
Benefits: TCP is well understood, used ubiquitously, and implemented on all major platforms.
Drawbacks: With TCP, reliable transport is too burdensome for some data. It does not support multiple channels with varying requirements. There is also no multi-homing or path discovery.

UDP (User Datagram Protocol) – UDP provides connectionless, unreliable, out of order, duplicated messages without error checking.
Benefits: UDP is well understood, used ubiquitously, and implemented on all major platforms.
Drawbacks: UDP lacks congestion control and reliable transport. It does not support multiple channels with varying requirements. There is also no multi-homing or path discovery.

DCCP (Datagram Congestion Control Protocol) – DCCP provides connection creation, congestion control, and connection negotiation. DCCP is connection flow-based (like TCP) but does not provide in order messages. It is designed for data with timing requirements that cannot accommodate the re-transmittal of reliable, in-order delivery, and designed to be a better network conserving protocol than UDP with congestion control
Benefits: DCCP provides congestion control and was developed for streaming data.
Drawbacks: DCCP lacks reliable transport. It does not support multiple channels with varying requirements. There is also no multi-homing or path discovery.

[3] http://controltoolbox.com/blog/2009/03/why_dnp_over_ip_is_smarter_tha.html

SCTP (Stream Control Transmission Protocol) – SCTP provides reliable, in order messages and congestion control. SCTP seems to combine TCP with UDP. It is message-oriented as opposed to connection-oriented. SCTP can create primary data transmission path and has greater support: UNIX, Linux, and Windows ports.
Benefits: SCTP is multi-homing and multi-path capable. It is able to handle multiple channels for data and provide reliable in-order transport as well as best-effort delivery. It can also provide congestion control.
Drawbacks: It cannot perform different levels of security for different channels.

5.2.1 Transport Layer Security Options

Most of the transport layers do not provide their own security mechanisms but instead rely upon the protocols defined in this subsection. Of all the surveyed transport protocols, only SCTP provides inherent security capabilities. However, SCTP also has the capability to utilize protocols in this section to provide additional security. No benefits or drawbacks are defined for these protocols because they are designed to secure either connection-oriented or connectionless transport protocols but are created from the same base concepts. Their definitions are included to provide a complete picture of the environment.

TLS (Transport Layer Security) – TLS is the successor to SSL. TLS continues to provide integrity and confidentiality, primarily for TCP communication (with extensions for UDP and DCCP).

DTLS (Datagram Transport Layer Security) – DTLS extends TLS to provide secure communication for connectionless communications. (OpenSSL supports DTLS.)

5.3 Network Layer Options

The lower layers provide a foundation upon which an application can directly run (e.g., traditional Modbus and DNP3) or upon which more sophisticated protocols provide enhanced service (e.g., DTLS, TCP).

IPv4 (Internet Protocol, version 4) – The Internet Protocol provides the critical backbone for the Internet. IP defines routable packet switched (as opposed to circuit switched) communication worldwide. IP provides an unreliable connectionless link over heterogeneous networks and a means to route and resolve global addresses.
Benefits: IPv4 is the de facto standard, is well understood, and has extensive market penetration.
Drawbacks: IPv4 must be extended to provide the capabilities of IPv6.

IPv6 (Internet Protocol, version 6) – IPv6 is an update to IPv4. Among other changes, it provides additional addressing space, simplified header construction, and inherent security.
Benefits: It is the enhanced version of IPv4 and will be the de facto standard of the future. It has built-in security.
Drawbacks: IPv6 currently lacks support and adoption.

DiffServ and MPLS are both designed to mitigate perceived limitations in IP. Specifically they strive to provide QoS.[4]

MPLS (Multi-Protocol Label Switching) – MPLS uses labels to create circuits or paths through which variable length messages flow. These labels can additionally provide message-handling instructions. It is a layer 2.5 protocol. MPLS can carry IP, Asynchronous Traffic Mode (ATM), and Ethernet traffic, among

[4] http://www.protocols.com/papers/diffserv.htm

others. It provides less overhead than ATM and a connection management like TCP. MPLS can provide path discovery services for IP to route around congestion problems.
Benefits: MPLS provides good QoS capabilities.
Drawbacks: It requires investment in hardware infrastructure.

DiffServ (Differentiated Services)/DSCP (Differentiated Services Code Point) – DSCP is an additional header in IP packets that allows labeling and message markup. DSCP could be used to identify and isolate supervisory access, engineering management, and data acquisition messages. DSCP is used in DiffServ which provides coarse-grained traffic management and QoS for IP.
Benefits: DiffServ is simple to enact.
Drawbacks: There is no classification for control systems. It does not guarantee QoS and instead provides the mechanism to enact it.

6.0 Solution

None of the surveyed protocols fully match the derived requirements in section 4.0. The proposed solution utilizes an unmodified network layer protocol, a modified transport layer protocol, and a nearly new application layer protocol derived from two protocols from the survey. Figure 5 displays the stack diagram for the solution. Ethernet is shown as the choice for the data link layer but it is only chosen because it is ubiquitous. However, other data link layers could be interchanged where appropriate as long as they support IP at the network layer. This section details the choices made at each layer of the communication stack for the proposed solution and finishes with a matrix with the coverage of the derived requirements.

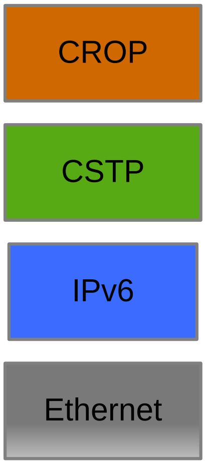

Figure 5: Proposed Protocol Stack

6.1 Network Layer

The first layer of the routable stack that must be defined is the network layer. This is the layer that provides routable capabilities. The most obvious choice for the network layer is IPv4, which is used ubiquitously. IPv4 could be used for all the higher layer choices discussed; however, the transition to IPv6 should be made now as it is the future of IP networking. IPv6, an upgrade to IPv4, increases the addressing space of routable devices. IPv6 also provides updates in two key areas that make it a better choice for an optimal routable SCADA architecture: security and quality of service.

IPsec is a protocol in the IP suite that was developed to provide end-to-end authentication and encryption capabilities. IPsec was implemented as a bolt-on solution to IPv4 after it was realized that security was necessary when routing through public networks. This bolt-on status has relegated IPsec to use almost exclusively in VPN tunneling applications. IPv6 has IPsec built in, which transitions its capability from being used as VPN tunnels to the possibility of secure tunnels between every device.

The other major benefit of IPv6 is the built-in QoS. IPv6 provides a mechanism to prioritize packets. One of the main concerns with control systems using routable networks is the potential latency that may cause strict communication timing constraints to be missed. With IPv6, QoS control packets could be set to the highest priority, jumping to the first in line at all routers, reducing the latency to as little as possible.

IP routing provides the means by which both multi-homing and path selection are provided. Multi-homing means that a device can have more than one address. Because IPv6 provides such a large addressing space, the network address translation (NAT) translation problems are no longer an issue.

With routing tables, these two addresses can be used to deliver a message over two different network paths. If one address is managed by a router that is attached to the primary fiber backbone path and the other address is managed by a router to a secondary cellular network, two network paths are created. The first address is used until a communication failure is discovered and then the second address is used to route around the problem through the secondary network. While IP provides the means to accomplish multi-homing and path selection, it is the responsibility of protocols higher in the stack to leverage them.

6.2 Transport Layer

An underlying requirement to this process is the separation of functionality so that it may be protected and processed with the appropriate levels of security and performance. Therefore, the three primary classes of data defined in this process are data acquisition or telemetry, supervisory control, and event data. Data acquisition is defined as real-time streaming data (PMU-like operation), which requires connectionless, best-effort, in-order delivery. Supervisory control requires a reliable connection with low latency. Lastly, event data is defined as audit logs or ancillary service event notifications, which require the least restrictive, best-effort, connectionless delivery. Each different data type could have different security controls depending on the risk management process of each implementer. However, at a high level all three require authentication, and only event data requires encryption (it is optional for the other two data types).

None of the surveyed protocols could meet this requirement. SCTP can potentially provide the capabilities to meet all three data transport requirements, but it isn’t as robust when it tries to perform connectionless, best effort transport. It also has the highest amount of overhead for the surveyed protocols, requiring chunks to be padded to a certain size. It also allows only one security connection for all streams, which would force the highest security for all streams.

The selected solution for the transport layer is to modify the SCTP to add the ability to create all of the variations of connection/connectionless and reliable/best-effort transport necessary. The extended version provides the capability to create multiple streams with the differing characteristics for telemetry, control, and event data. On top of the connection characteristics, the extended version also enables the ability to set up different security protections for each stream. For example, telemetry data can be authenticated only while control data can be authenticated and encrypted. These capabilities enable the protocol to fulfill the requirements of independently configuring streams appropriately for the data. The extended SCTP will be referred to as the Control system Secure Transport Protocol (CSTP) in the remaining sections of the document.

It is desirable to have multiple streams over one channel instead of three separate channels because it allows for congestion control within each stream as well as across the streams. Congestion control is altering the rate of transmission when communication loss and latency begin to rise. Not only does this reduce the communication failures on the channel of communication but it also relieves pressure on the network, making it better for all traffic involved. When congestion control is applied across multiple streams, it enables intelligent transmission shaping at the originating device. For instance, if congestion is seen on the control channel, the CSTP can choose to restrict the transmission of the telemetry stream instead of the control stream, thereby ensuring the higher priority packets are not delayed or dropped. With separate channels, the congestion could potentially be seen on both the control and telemetry channels, and both would perform congestion control, potentially holding back data and preventing the timely delivery of control data.

The CSTP provides additional data prioritization and QoS capabilities. First, it provides the management and operation of the multi-homing and path selection capabilities. As was described in the network layer section, multi-homing and path selection provide redundancy and reliability to communication via backup communication routes. The CSTP protocol provides dual-homing and automatic fail-over to the second address when the first address becomes unreachable, thereby routing around the problem without the application's intervention. In addition to the multi-homing and path selection, the modified version is responsible for selecting the QoS prioritization of the IPv6 header. Control data is set with the highest priority, followed by telemetry, and, finally, event data.

6.3 Application Layer

Currently, serial control system protocols are essentially being encapsulated into the routable protocol stack. This is inefficient and keeps the differing applications tied together. Therefore, to improve the efficiencies of communication and enable the tailoring of management and security, a new control system application layer protocol is proposed. In this protocol, only the data objects will be extracted from the control system communication, which will then be encapsulated by the previously mentioned protocols.
DNP3 and IEC 61850 are sufficiently comprehensive to meet the needs of many applications. Therefore, they will be leveraged as a basis to develop this new routable-friendly protocol. The new application layer protocol will be referred to as the Control system Routable Object Protocol (CROP) in the remaining sections of the document.

6.4 Requirements Mapping

Derived Requirements	IPv6	CSTP	CROP
Transport Channels must be configurable to meet the requirements of the following data types: o Telemetry o Control o Event		Provides the capability to handle multiple streams of data, each with different security and operational characteristics.	Allows the separation of control system communication into functional data types.
Telemetry data must be streamed in a push architecture.			Removes the need to poll for data and allows telemetry and control to be separated in different channel streams. This separation allows for the streaming of telemetry data.
Telemetry data must be authenticated.	Provides the capability to authenticate packets.	Provides the capability to authenticate data in each stream.	

Derived Requirements	IPv6	CSTP	CROP
Telemetry data may optionally be encrypted.	Provides the capability to encrypt packets.	Provides the capability to encrypt data in each stream.	
Telemetry data must be a best effort transport.		Provides a best effort stream for telemetry data.	
Telemetry data must be ordered.		Provides mechanism to order telemetry data.	
Control data must be reliable transport.		Provides a reliable stream for control data.	
Control data must be authenticated.	Provides the capability to authenticate packets.	Provides the capability to authenticate data in each stream.	
Control data must be encrypted.	Provides the capability to encrypt packets.	Provides the capability to encrypt data in each stream.	
Control data must be in order delivery.		Provides mechanism to order control data.	
Control data must be highest-priority data with best available quality of service.	Provides QoS capabilities.	Selects highest QoS for control data streams.	
Event data must be authenticated.	Provides the capability to authenticate packets.	Provides the capability to authenticate data in each stream.	
Event data must be encrypted.	Provides the capability to encrypt packets.	Provides the capability to encrypt data in each stream.	
Event data must be reliable transport.		Provides a reliable stream for event data.	
Event data must be un-ordered delivery.			

Derived Requirements	IPv6	CSTP	CROP
Transport layer must provide a congestion control mechanism.		Provides congestion control for each stream and across all streams electing to restrict lower priority streams first.	
Protocol stack must provide dual-homing and multi-path capabilities.	Provides the capabilities to perform dual-homing and path selection.	Operates the functionality of address and path selection.	
Transport layer must provide management of priority of service.		Selects the priority of service based on the data type.	
Transport layer must provide management of multiple distinct streams.		Manages multiple data streams over one transport channel.	

7.0 Roadmap

Creating a roadmap to guide industry from the current to the future environment greatly enhances acceptance of the solution. For this purpose, a roadmap to achieve the future end-state is presented in this section. This roadmap was developed to be used by asset owners and vendors. It is designed for those entities to smoothly transition into a secure routable communications environment.

Multiple steps are defined in the roadmap to provide a graduated course of action. It is assumed and expected that asset owners will roll out the upgrades at differing rates, creating environments with subsystems at different steps in the roadmap. The following steps identify existing technologies and actions that can be implemented to improve security of routable control system communication links and the requirements to achieve the future environment with embedded security.

7.1 Step 1 – Enable Existing Security

The initial step to secure routable control system traffic is focused on the communication links. This approach allows partial security to be deployed in a reasonable time frame using existing products and security mechanisms; no new products need to be developed. The available cryptographic technologies address sender and message authentication and confidentiality. Example technologies include Transport Layer Security[5] (TLS), Secure Sockets Layer (SSL) at the transport layer, and Internet Protocol Security[6] (IPsec) at the network layer. These technologies are commonly used in other routable infrastructures to secure communication and in essence are the de facto standard.

7.1.1 Action

This step involves enabling commercial-off-the-shelf SSL/TLS or IPsec to secure all routable communication channels. IP-capable devices can immediately use IPsec to provide security. Also, TCP/UDP-capable devices should be able to use TLS with little or no changes in software.

7.1.2 Assumptions

It is assumed that Ethernet and IPv4 are used throughout the control system network infrastructure. Also, it is assumed TLS and IPsec are used to provide security.

7.1.3 Target Implementation

Security will be implemented on any IP-capable device (most likely network infrastructure but potentially control system components). Examples include routers, firewalls, and if supported, communication processors.

7.1.4 Advantages

This step will provide confidentiality and optional integrity for all network traffic including control system data that flows over the communication channel. No changes to control system protocols are required to implement this step. The SSCP characteristics of message integrity and confidentiality are provided for communication links.

[5] Dierks, T. and Rescorla, E. “The Transport Layer Security (TLS) Protocol, Version 1.1.” 2006. The Internet Society. <http://www.ietf.org/rfc/rfc4346.txt>.

[6] Kent, S. and Atkindson, R. “Security Architecture for the Internet Protocol.” 1998. The Internet Society. <http://www.ietf.org/rfc/rfc2401.txt>.

7.1.5 Limitations

These technologies do not provide data integrity of control system messages before they traverse the link. Security must also be initiated at the control system device. Additionally, all control traffic is now treated in the same manner with the same overall security policy.

7.1.6 Requirements Mapping

• Telemetry transport channel	
• Control transport channel	
• Event transport channel	
• Telemetry data must be streamed in a push architecture.	
• Telemetry data must be authenticated.	✓
• Telemetry data may optionally be encrypted.	
• Telemetry data must be a best-effort transport.	
• Telemetry data must be ordered.	✓
• Control data must be reliable transport.	✓
• Control data must be authenticated.	✓
• Control data must be encrypted.	✓
• Control data must be in-order delivery.	✓
• Control data must be highest-priority data with best available quality of service.	
• Event data must be authenticated.	✓
• Event data must be encrypted.	✓
• Event data must be reliable transport.	
• Transport layer must provide congestion control mechanism.	
• Protocol stack must provide dual-homing and multi-path capabilities.	
• Transport layer must provide management of priority of service.	
• Transport layer management of distinct streams.	

7.1.7 Diagram

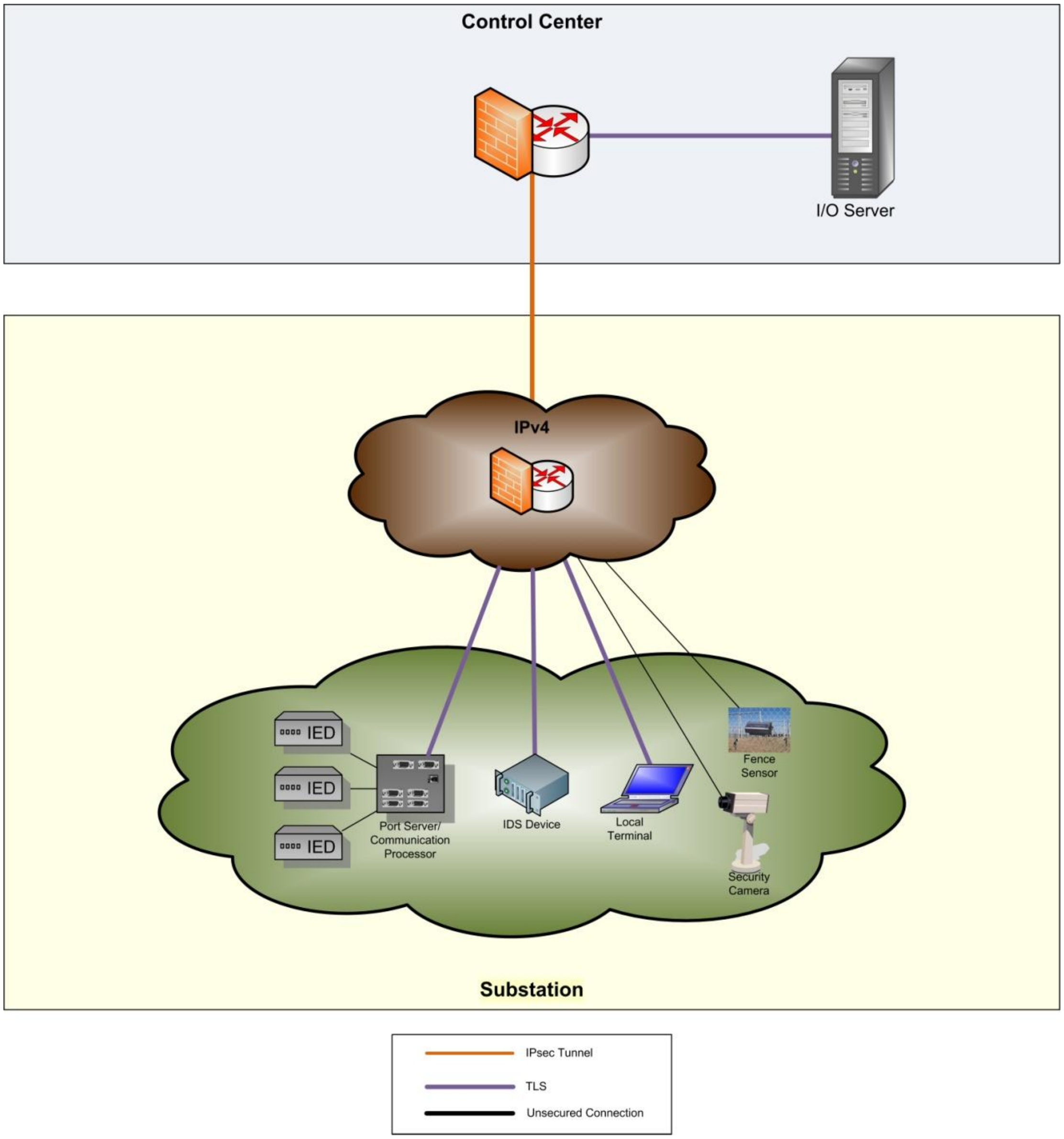

Figure 6: Existing Security Methods

Figure 6 depicts the protection of data during transmission by enabling existing secure communication technologies such as TLS and IPsec. At a minimum, the network infrastructure components should support these secure communication technologies. In addition, control system devices such as communication processors, terminal servers, and input/output (I/O) servers may also be capable of supporting secure communication. While a good first step, more must be done to accomplish the security goals of the future control system.

7.2 Step 2 – Aggregation Point Security

The next interim step in the roadmap is to begin enforcing tailored protection of control system communication. In the same manner that SSCP is a data-driven solution, this step differentiates among data types using the payload type field, which can be protected distinctly. By embedding cryptographic technology into control center servers (e.g., front-end processors) and substation equipment (e.g., remote terminal unit (RTU) or communications processor), the various data types can be protected uniquely. For example, telemetry data can use message authentication, while control signals use both message authentication and encryption. Although embedded onto devices, this approach is still a bolt-on solution.

Due to the non-existence of a one-protocol solution, the best and only practical approach is to use separate channels and protocols for each data type to meet their needs. Data acquisition needs the least amount of overhead because it is streaming data. Therefore, the two best choices from the survey are UDP or DCCP. UDP is lighter than DCCP, but the goal of DCCP is to add congestion control to UDP. As mentioned previously, latency is a concern for control system traffic; therefore, congestion control is a very highly valued attribute. Because of the required congestion control, DCCP is the recommended transport protocol for data acquisition. DCCP works with DTLS to provide the security controls for the data.

Supervisory control data needs a low latency and reliable connection. The low latency problem can be solved by making these higher-priority packets in the network layer. The two potential protocols for providing the reliable transmission of data are TCP and SCTP. While TCP provides slightly less overhead, SCTP provides functionality that greatly outweighs it. TCP was developed to create a connection to stream data. SCTP sends message blocks, which fit better with the control command messages being sent. However, the greatest benefit of SCTP over TCP is built-in multi-homing and path management. A network architecture can be established with a primary path such as a fiber line with a backup microwave connection. If the fiber line has problems, the built-in capabilities of SCTP can be leveraged to automatically reroute the command through the microwave connection. One other additional benefit is that SCTP uses a four-way handshake to eliminate the SYN-flood problems with TCP.

7.2.1 Action

This step involves enabling SCADA applications to use different channels for each function (telemetry, control, events, etc.). Each channel can have unique security constraints and policies.

Encapsulated SCADA traffic remains unaltered.

7.2.2 Assumptions

It is assumed that:

- DCCP and DTLS, in conjunction with Real-time Transport Protocol (RTP), are used for telemetry.
- SCTP and DTLS are used for control traffic.
- IPv4 is still widely deployed.

7.2.3 Target Implementation

Aggregation Point Security will be implemented between control center front-end processors and substation communications processors. A software shim/library can be used on the front-end processors to encapsulate traffic and provide necessary functionality. The communications processors will require a firmware update to support both secure communications and the differentiation and streaming of control system connections. Each communication path between end devices can have specific security criteria based upon explicit policies.

7.2.4 Advantages

This step will add differential service to control communications and move the desired behavior one step closer to the end device. This step supports the SSCP characteristic of securing various types of payloads differently. Also, the protocol independent nature of the SSCP is available in this step.

DCCP and DTLS provide appropriate support for telemetry communication requirements. DCCP provides congestion control for connectionless data, while DTLS provides message security. RTP provides a time stamping mechanism for communication.

SCTP offers a framework for SCADA control communication with QoS and independent channels.

7.2.5 Limitations

This approach is still an add-on solution. Desired behavior such as priority of service and push-based communication is not available.

7.2.6 Requirements Mapping

• Telemetry transport channel	
• Control transport channel	
• Event transport channel	
• Telemetry data must be streamed in a push architecture.	
• Telemetry data must be authenticated.	✓
• Telemetry data may optionally be encrypted.	✓
• Telemetry data must be a best-effort transport.	✓
• Telemetry data must be ordered.	✓
• Control data must be reliable transport.	✓
• Control data must be authenticated.	✓
• Control data must be encrypted.	✓
• Control data must be in-order delivery.	✓
• Control data must be highest-priority data with best available quality of service.	
• Event data must be authenticated.	✓
• Event data must be encrypted.	✓
• Event data must be reliable transport.	✓
• Transport layer must provide a congestion control mechanism.	
• Protocol stack must provide dual-homing and multi-path capabilities.	
• Transport layer must provide management of priority of service.	
• Transport layer management of distinct streams.	

7.2.7 Diagram

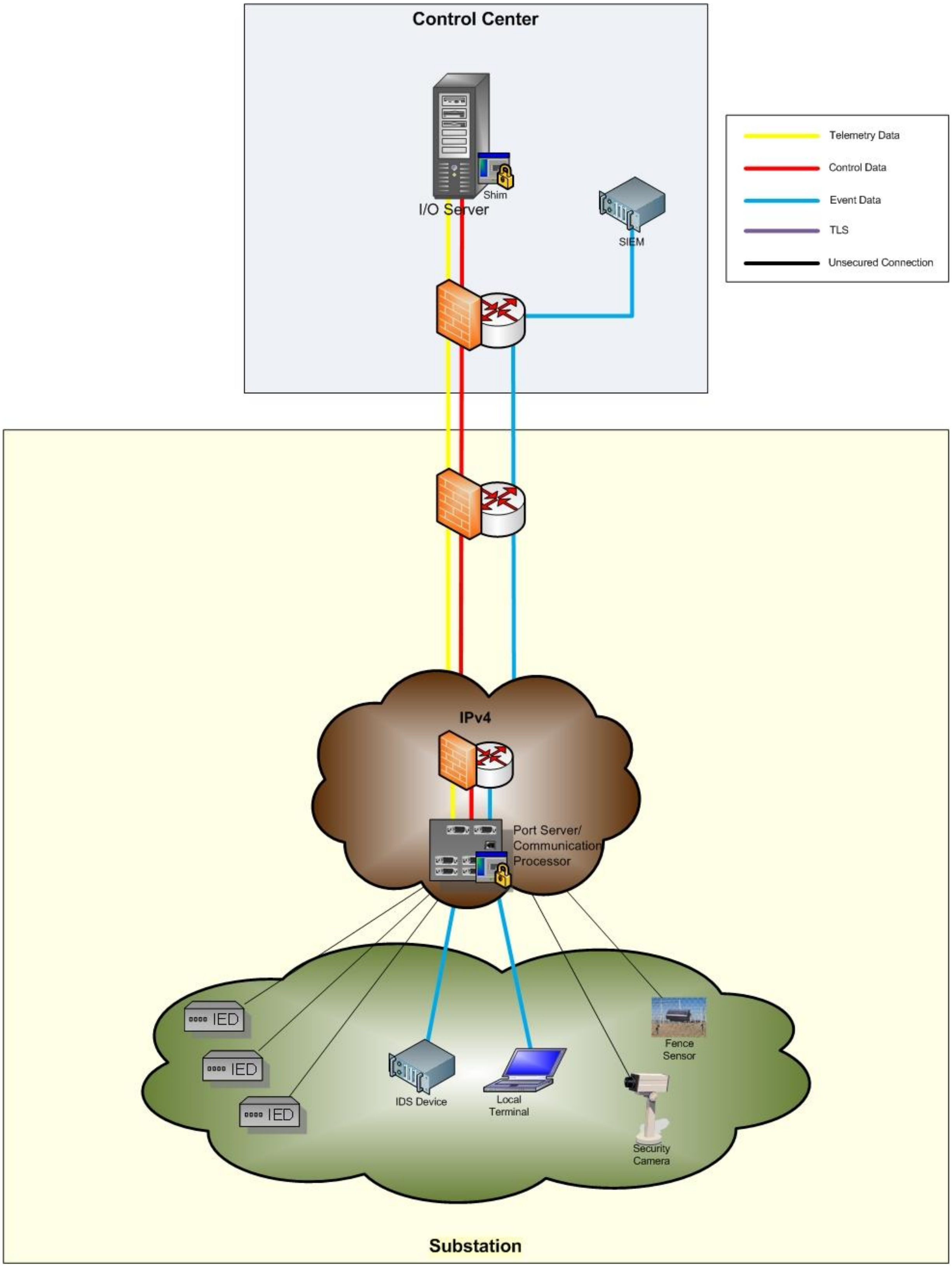

Figure 7: Aggregation Point Security

Figure 7 depicts several changes to control system communication related to the future vision. First, telemetry and control messages are transmitted over distinct communication channels using existing protocols such as SCTP and DCCP. Second, differing protection mechanisms can be applied to these separate channels. It is important to note that a software shim is used to provide the required functionality on select control system components. At this stage in the roadmap, control system protocols have not been altered; the next step in the process addresses this need.

7.3 Step 3 – End Device Protection

The last interim step in the roadmap is to extend the cryptographic protection of communication closer to the end points. This step moves SSCP functionality to the application layer of the Open System Interconnection (OSI) model. An optimized SCADA protocol utilized on end devices will be able to secure traffic by type, prioritize communication, and stream telemetry data to control centers. Prioritization of traffic guarantees control commands are given precedence over telemetry and event data. This step supports the streaming capability, which is a merging of today’s synchrophasor and SCADA communication characteristics. The ability to implement distinct channels on end devices removes the one-size-fits-all mentality of IT-based link protection schemes.

7.3.1 Action

This step involves creating a new SCADA protocol (CROP) to protect communication over appropriately separated channels. Existing network-compatible devices will receive a firmware update providing a means of streaming, securing, and prioritizing control system traffic. Also, traditional end devices will be network enabled, communicate via Ethernet and IP, and include the same firmware functionality.

7.3.2 Assumptions

It is assumed that IPv6 and TLS will be commonly used. SCTP and DCCP continue to be used as separate transport channels as in step 2.

7.3.3 Target Implementation

All the devices from step 2 and devices behind the aggregation points (RTU, intelligent electronic device [IED], and programmable logic controller [PLC]) will support the new protocol.

7.3.4 Advantages

The four primary advantages of End Device Protection are:

- The ability to stream SCADA data
- The ability to prioritize communication
- SSCP functionality for routable traffic
- The ability to match security mechanisms to specific data channels based upon policy.

7.3.5 Limitations

Modification of the application level is required to converse between end devices. CROP does not provide security capabilities; therefore, TLS and DTLS are still required.

7.3.6 Requirements Mapping

• Telemetry transport channel	✓

• Control transport channel	✓
• Event transport channel	✓
• Telemetry data must be streamed in a push architecture.	✓
• Telemetry data must be authenticated.	✓
• Telemetry data may optionally be encrypted.	✓
• Telemetry data must be a best-effort transport.	✓
• Telemetry data must be ordered.	✓
• Control data must be reliable transport.	✓
• Control data must be authenticated.	✓
• Control data must be encrypted.	✓
• Control data must be in-order delivery.	✓
• Control data must be highest-priority data with best available quality of service.	✓
• Event data must be authenticated.	✓
• Event data must be encrypted.	✓
• Event data must be reliable transport.	✓
• Transport layer must provide congestion control mechanism.	
• Protocol stack must provide dual-homing and multi-path capabilities.	
• Transport layer management of priority of service.	
• Transport layer management of distinct streams.	

7.3.7 Diagram

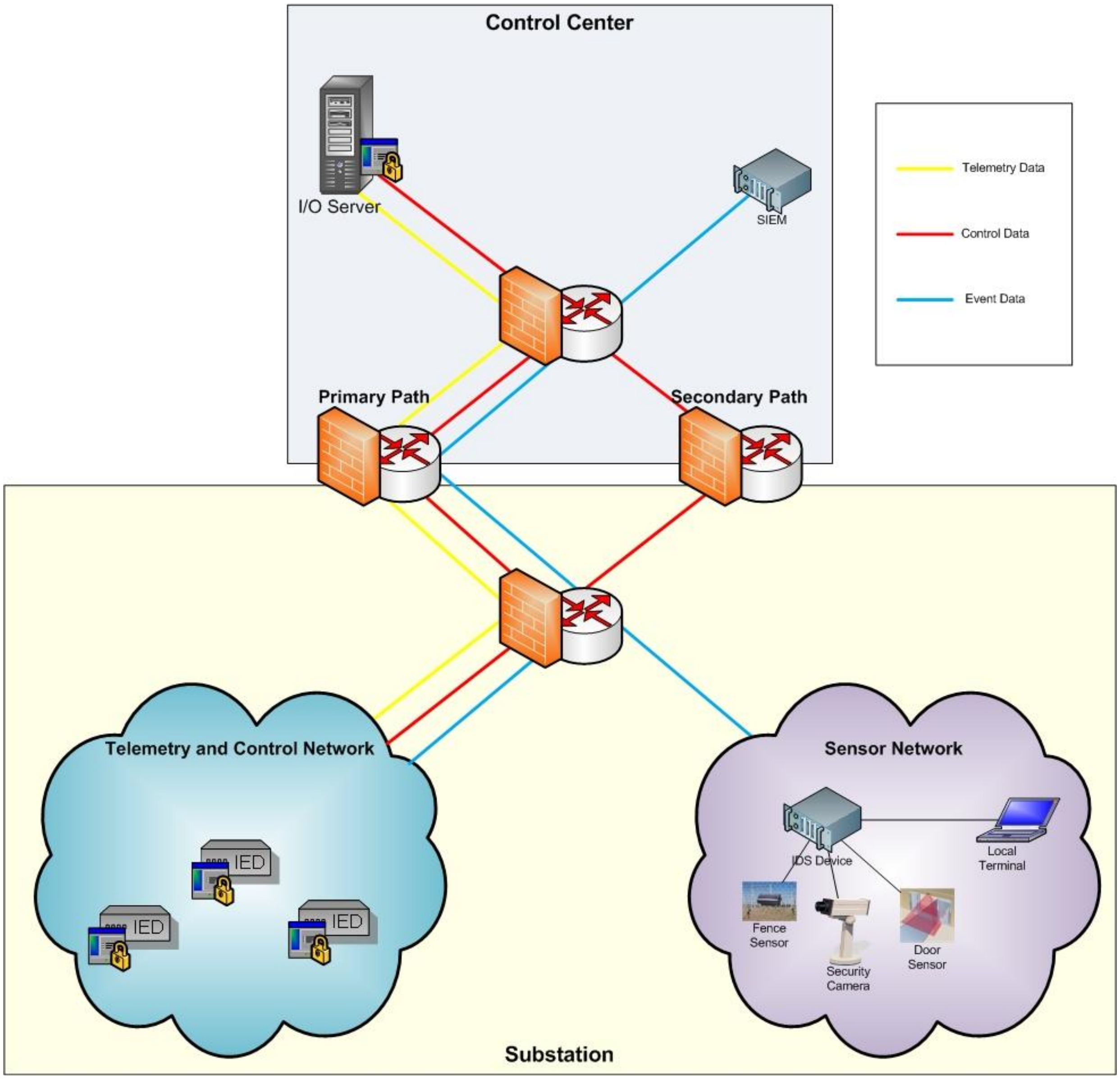

Figure 8: End Device Protection

Figure 8 depicts the deployment of the CROP that natively separates and protects data uniquely by data type. The functionality updates used in the previous step have been incorporated into end devices. This near optimal step uses separate but application-managed communication channels, leading to the need for step four.

7.4 Step 4 – Optimized Security

During this final step, an optimized transport layer—the CSTP—is implemented on all end devices. This method secures all CSTP data chunks. Each chunk is a different data object from the CROP, which can be secured independently.

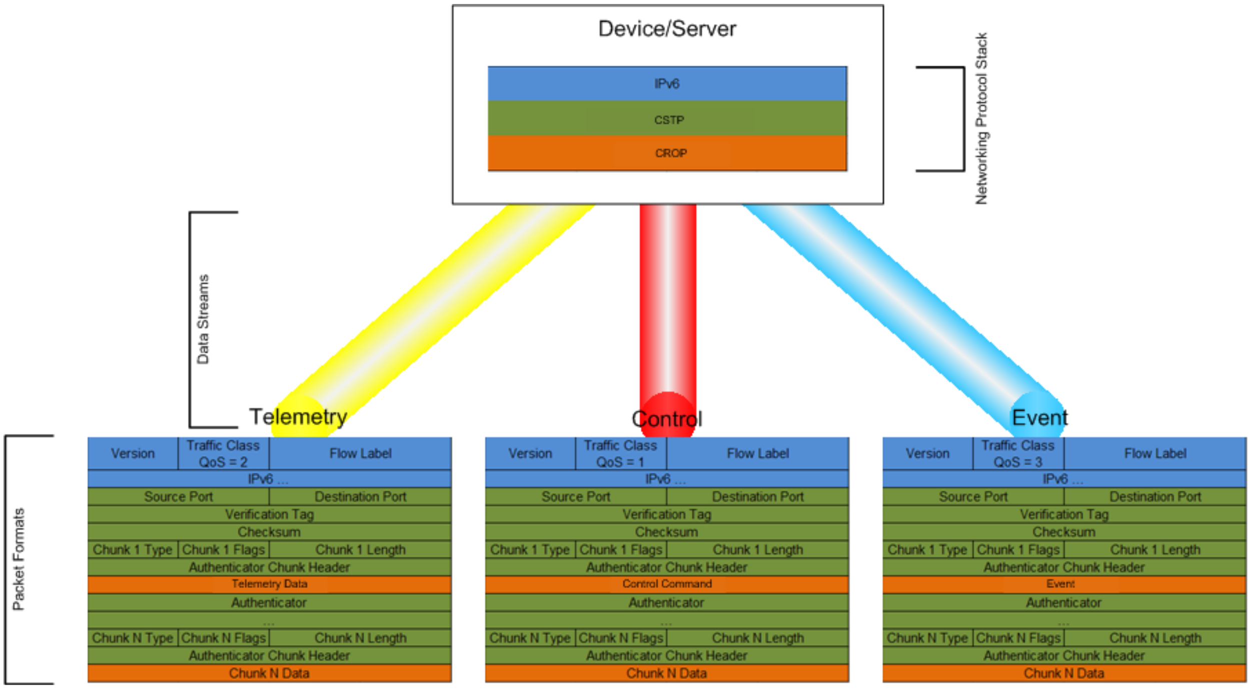

Figure 9: Protocol Stack Streaming to Packet Format

Figure 9 depicts the multiple managed streams and their respective packet formats. The first stream is telemetry data protected using message authentication. Stream two adds encryption to secure a control command to protect the details of the control action from an adversary. In the final step, the last stream encrypts and authenticates individual event messages per chunk. As depicted in the blue sections, the IPv6 headers provide QoS. The values are set for each stream with lower values equaling higher QoS.

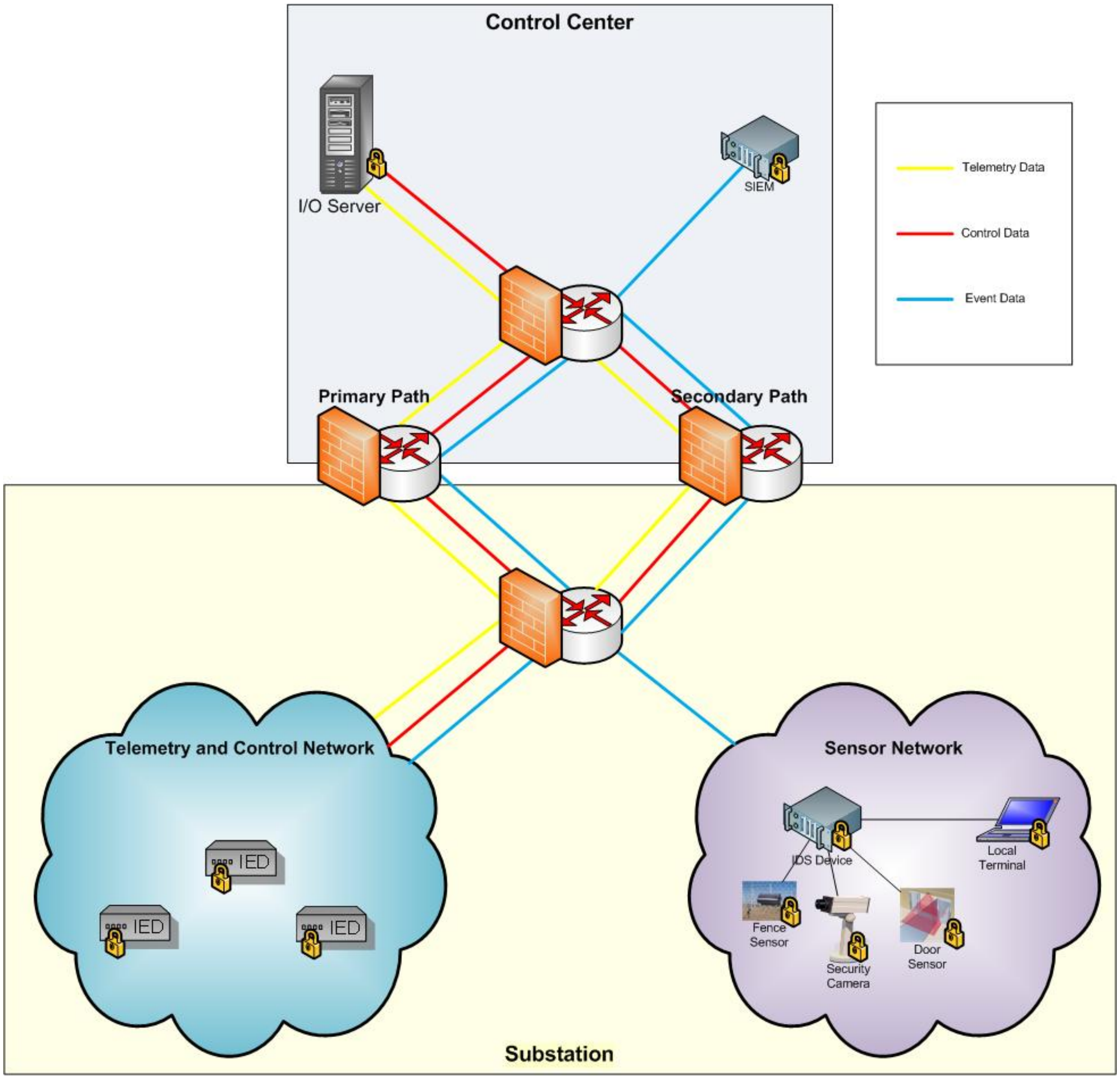

Figure 10: Optimized Security

Figure 10 depicts CSTP, which provides both priority and quality of service for each unique type of control system traffic. For example, not only are control messages given priority over telemetry but also control system traffic is given priority over other types of communication such as E-mail and Internet traffic.

7.4.1 Action

In addition to the new application layer protocol from Step 3 (CROP), another new protocol, CSTP, is created. CSTP is an optimized and tailored extension of SCTP. See the Solution Section 6.0 for further details. All end devices now use both CROP and CSTP.

7.4.2 Assumptions

CROP must be supported and available. All networking devices support IPv6.

7.4.3 Target Implementation

This step implements the CSTP on all devices and software solutions used in Step 3.

7.4.4 Advantages

This is the last step in the roadmap where all of the capabilities in the vision are implemented natively. This step produces a new future protocol that provides necessary functionality—protocol convergence.

7.4.5 Requirements Mapping

• Telemetry transport channel	✓
• Control transport channel	✓
• Event transport channel	✓
• Telemetry data must be streamed in a push architecture.	✓
• Telemetry data must be authenticated.	✓
• Telemetry data may optionally be encrypted.	✓
• Telemetry data must be a best-effort transport.	✓
• Telemetry data must be ordered.	✓
• Control data must be reliable transport.	✓
• Control data must be authenticated.	✓
• Control data must be encrypted.	✓
• Control data must be in-order delivery.	✓
• Control data must be highest-priority data with best available quality of service.	✓
• Event data must be authenticated.	✓
• Event data must be encrypted.	✓
• Event data must be reliable transport.	✓
• Transport layer must provide congestion control mechanism.	✓
• Protocol stack must provide dual-homing and multi-path capabilities.	✓
• Transport layer management of priority of service.	✓
• Transport layer management of distinct streams.	✓

7.5 Requirements Mapping

The approaches outlined in this specification identify what must be done to secure control system communication in routable environments. The following table maps the requirements identified in section 4.0 to the implementation step where they are addressed:

Requirements	Step 1	Step 2	Step 3	Step 4

• Telemetry transport channel			✓	✓
• Control transport channel			✓	✓
• Event transport channel			✓	✓
• Telemetry data must be streamed in a push architecture.			✓	✓
• Telemetry data must be authenticated.	✓	✓	✓	✓
• Telemetry data may optionally be encrypted.		✓	✓	✓
• Telemetry data must be a best-effort transport.		✓	✓	✓
• Telemetry data must be ordered.	✓	✓	✓	✓
• Control data must be reliable transport.	✓	✓	✓	✓
• Control data must be authenticated.	✓	✓	✓	✓
• Control data must be encrypted.	✓	✓	✓	✓
• Control data must be in-order delivery.	✓	✓	✓	✓
• Control data must be highest-priority data with best available quality of service.			✓	✓
• Event data must be authenticated.	✓	✓	✓	✓
• Event data must be encrypted.	✓	✓	✓	✓
• Event data must be reliable transport.		✓	✓	✓
• Transport layer congestion control mechanism.				✓
• Protocol stack must provide dual-homing and multi-path capabilities.				✓
• Transport layer management of priority of service.				✓
• Transport layer management of distinct streams.				✓

8.0 Summary

While a large percentage of current control systems still communicate over serial data links, the inevitable trend is toward Ethernet and IP communications. Foresight in developing reliable and secure routable communication for control systems will alleviate the considerable anguish and cost that comes with piecemeal and one-size-fits-all solutions that are slapped onto the routable control systems networks.

Secure control system deployment should occur in a deliberate and extensively tested and reviewed manner to ensure that all stakeholders are satisfied and that all issues—from security to reliability—are addressed. The solution described throughout this document provides meaningful progress toward securing routable control system communication for the present and the future. The roadmap described previously presents a path from the current routable control systems of today to the idealized but achievable secure control systems of the future.

This document provides the methods to secure routable control system communication in the electric sector. The approach of this document yields a long-term vision for a future of secure communication, while also providing near-term steps and a roadmap. The requirements for the future secure control system environment were spelled out to provide a final target. Additionally, a survey and evaluation of current protocols were used to determine if any existing technology could achieve this goal. In the end, a four-step path was described that brought about increasing requirement completion and culminates in the realization of the long-term vision.

Future work will detail the specifications for CROP and CSTP and discuss preliminary implementation concerns. Subsequent to the creation of a specification, prototype development will create trial implementations of each protocol. After a working prototype is developed, local small-scale testing will be conducted to evaluate the performance and compare it to the requirements. Lastly, large-scale testing and evaluation with outside participation will achieve vendor and end user input and utilization.

This document should be used as a starting point to solicit stakeholder input from industry, additional researchers, end users, vendors, and the government. The ongoing dialogue is not only critical to the successful adoption of a secure routable control systems network but also crucial in the very development and formulation of the needs and possibilities of such a secure environment.

Appendix A – Open System Interconnection Model

Open System Interconnection Model[7,8]

The communication protocol described in this specification will use the Open System Interconnection (OSI) model as a guide. The OSI model is a description for layered communications and network protocol design. It divides network architecture into seven layers, where control is passed from one layer to the next. A layer is a collection of conceptually similar functions that provide services to the layer above it and receives services from the layer below it. From bottom up, the layers are Physical, Data Link, Network, Transport, Session, Presentation, and Application.

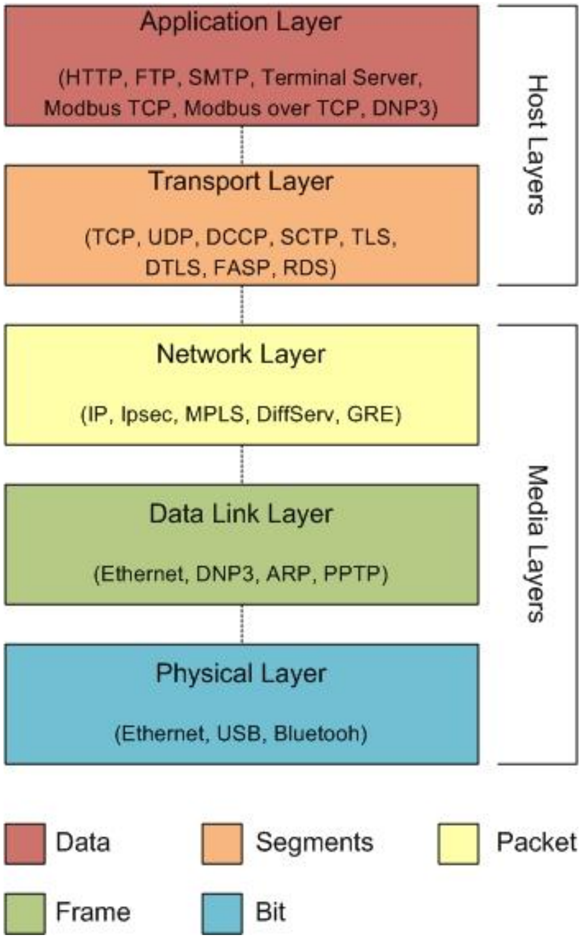
Application Layer
(HTTP, FTP, SMTP, Terminal Server, Modbus TCP, Modbus over TCP, DNP3)
Transport Layer
(TCP, UDP, DCCP, SCTP, TLS, DTLS, FASP, RDS)
Network Layer
(IP, Ipsec, MPLS, DiffServ, GRE)
Data Link Layer
(Ethernet, DNP3, ARP, PPTP)
Physical Layer
(Ethernet, USB, Bluetooh)
Host Layers
Media Layers
Data
Segments
Packet
Frame
Bit

Figure 11: OSI Model

Physical Layer

The Physical Layer defines the electrical and physical specifications for devices and defines the relationship between a device and a physical medium. The major functions and services performed by the

[7] International Telecommunication Union. "Architecture Framework for the Development of Signaling and OA&M Protocols Using OSI Concepts." 1994. ITU-T. <http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Q.1400-199303-I!!PDF-E&type=items>.

[8] "The 7 Layers of the OSI Model." 2008. 20 May 2010 <http://www.webopedia.com/quic_ref/osi_layers.asp>.

Physical Layer are: establishment and termination of a connection to a communications medium; participation in the process whereby the communication resources are effectively shared among multiple users; and modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel.

Data Link Layer

While the Physical Layer is primarily concerned with the interaction of a single device with a medium, the Data Link Layer is concerned more with the interactions of multiple devices with a shared medium. At this layer, data packets are encoded and decoded into bits. The Data Link Layer furnishes transmission protocol knowledge and management and handles errors in the physical layer.

Network Layer

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the QoS requested by the Transport Layer. The Network Layer performs network routing functions and may also perform fragmentation and reassembly and report delivery errors.

Transport Layer

The Transport Layer is responsible for encapsulating application data blocks into data units (datagrams or TCP segments) suitable for transfer to the Network Layer for transmission to the destination host, or managing the reverse transaction by abstracting network datagrams and delivering their payload to an application. The protocols of the Transport Layer establish a direct, virtual host-to-host communications transport medium for applications.

Application Layer

The Application Layer is the OSI layer closest to the end user, which means that both the Application Layer and the user interact directly with the software application. Application Layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication to satisfy the user’s needs.

Appendix B – Routable Transport Survey

Desired Functionality	SSCP	DCCP/DTLS	TCP/TLS	SCTP (with PR-SCTP extension)	Heterogeneous Packet Flows	Structured Stream Transport	IPv6	SRTP/RTCP	RUDP
Push Telemetry	Designed around legacy architecture with a master communicating with many slaves. Nothing stops it from working like this but it was not designed for this.	Streams data well.	Connection-oriented with reliable in-order delivery so will retransmit any dropped packets. Will add latency trying to get every packet to destination.	Can operate similarly to DCCP but has higher overhead and complexity	Provides mechanism to stream data	Provides streams for delivery real-time data	Allows use of UDP	Built for delivery of media.	
Secure DA & SC & Events	A separate channel would need to be established for each different type of data.	A separate channel would need to be established for each different type of data.	A separate channel would need to be established for each different type of data.	Comes closest to meeting needs of all three over one channel. However, I think this would force one security profile across all three.	No discussion of security	Comes closest to meeting needs of all three over one channel. However, I think this would force one security profile across all three.	Same security for all/ per IP connection (IPsec)	A separate channel would need to be established for each different type of data.	
DA - Connectionless but ordered	Would work but would rely on an underlying protocol	Completely unreliable. Order would have to be provided by application.	Cannot do connectionless.	Can do connectionless and ordered with PR-SCTP extension	Provides both reliable and best-effort	Provides both reliable and best-effort	Allows use of any transport protocol	Provides facilities for jitter compensation and detection of out-of-order sequence arrival on top of UDP or DCCP.	

Desired Functionality	SSCP	DCCP/DTLS	TCP/TLS	SCTP (with PR-SCTP extension)	Heterogeneous Packet Flows	Structured Stream Transport	IPv6	SRTP/RTCP	RUDP
SC – Connection-oriented; reliable	Would work, but would rely on an underlying protocol	Completely unreliable.	Fits but is designed for streams of data and not one off commands.	Provides reliability per stream, so one stream does not hold up another (DA not held up by Events)	Provides both reliable and best-effort	Provides both reliable and best-effort	Allows use of any transport protocol	No	
Events - Connectionless without order	Would not work for out-of-order packets. Does not allow previous sequence numbers.	This fits this model.	Diametrically opposed	RFC says, "SCTP provides a mechanism for bypassing the sequenced delivery service. User messages sent using this mechanism are delivered to the SCTP user as soon as they are received." However, I did not see how this mechanism worked.	Provides both reliable and best-effort	Provides both reliable and best-effort	Allows use of any transport protocol	Designed to provide ordering	
Priority of communication, configurable QoS	Would rely solely on underlying protocols.	Does not provide priority or QoS but provides congestion control.	No QoS		Provides mechanisms to define priority of data for network QoS purposes	Can prioritize streams	Best option for true QoS	Provides side channel to transmit communications statistics for QoS adjustments	

Desired Functionality	SSCP	DCCP/DTLS	TCP/TLS	SCTP (with PR-SCTP extension)	Heterogeneous Packet Flows	Structured Stream Transport	IPv6	SRTP/RTCP	RUDP
Logically &/or physically separated com. channels	A separate channel would need to be established for each different type of data.	A separate channel would need to be established for each different type of data.	A separate channel would need to be established for each different type of data.		Pseudo logically separated streams via differing levels of QOS per frame	Logically separated streams can be set up for each com.		A separate channel would need to be established for each different type of data.	
Device to Device comm.	Would need to be integrated with routable control system protocols.	Fits	Fits	Fits	Fits	Fits		Fits	
Cryptographic sessions required	Met	Met	Met	Met		Met	Met	Met	
Other Benefits	Low latency. Provides a migration path from legacy.	DCCP implementation in Linux.	Most widely used and understood	Multi-homing		Software library available but has not yet reached a stable release	Multi-homing		Lighter than TCP
		Very little overhead from stack.		Path management; provides built in capabilities to route around problems.		One connection to set up other lightweight streams of data.	Does not preclude any others and can be used with all others		
		Provides for different congestion control algorithms.		SCTP implemented in many OSs including Linux and IOS					
		DCCP helps UDP traverse NAT and firewalls.		Open source library available that works on all major OSs					

Desired Functionality	SSCP	DCCP/DTLS	TCP/TLS	SCTP (with PR-SCTP extension)	Heterogeneous Packet Flows	Structured Stream Transport	IPv6	SRTP/RTCP	RUDP
				4-way handshake (prevent SYN flood)					
Other Drawbacks	Small address space in light of possible AMI size.	DCCP not widely used.	Forces most reliable connection.	Most complex	A research paper	A research project and not standard effort		Requires an additional protocol and channel for connection maintenance	Seems dead
	Does not currently integrate with any routable/transport layer protocols.	Any form of reliability or ordering must be done at the application layer.	Stream-oriented forcing record framing in application	Most overhead (I think); chunks have to fit into a multiple of 32bits so require padding	No updates in a decade			Designed around video delivery	
				Unseasoned security mechanism (does not use TLS variant); there is an RFC for using TLS with SCTP but doesn't seem to fit that well.				Application layer protocol	