U.S. DEPARTMENT OF
ENERGY

PNNL-20531

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

Comparison of Routable Control System Security Approaches

TW Edgar
MD Hadley
TE Carroll
DO Manz
JD Winn

June 2011

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-20531

Comparison of Routable Control System Security Approaches

TW Edgar
MD Hadley
TE Carroll
DO Manz
JD Winn

June 2011

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

Pacific Northwest National Laboratory
Richland, Washington 99352

Table of Contents

Table of Figures

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.

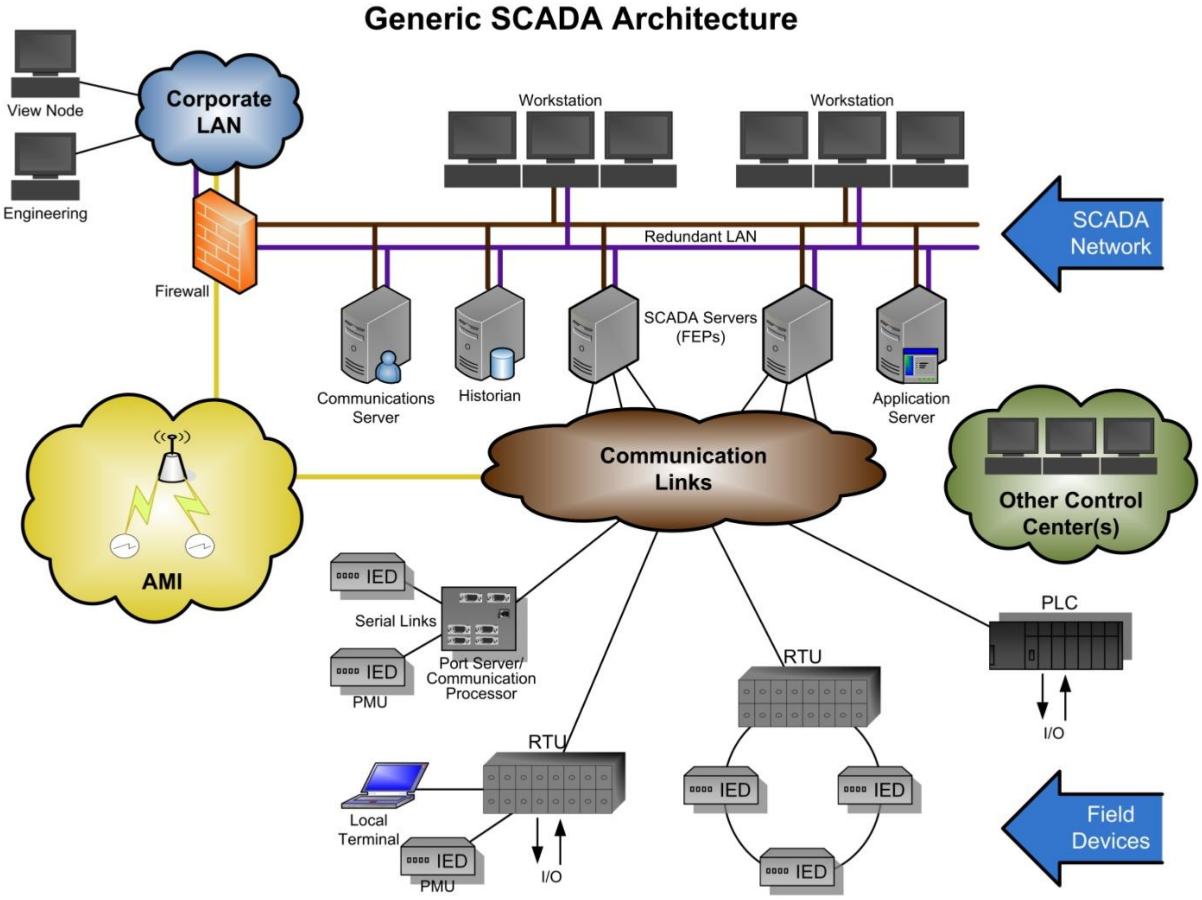

Figure 1: Generic Control System Architecture

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 Commission [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. This document will focus on routable IP communication.

Current routable control system communication over IP is often unsecured. For example, a utility using DNP/IP over utility-owned fiber may not implement Secure DNP or use TLS to increase the level of assurance. 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. International Electrotechnical Commission (IEC) IEC-62351 is an example of a control-system specific security effort currently being developed.

1.2 Purpose

The purpose of this document is to compare the security requirements identified in PNNL’s forward looking protocol design to available technologies and standards. The technologies under consideration were identified using a survey of vendor offerings and IP security technologies. Section 3 describes these technologies in more detail. Please reference the Secure and Efficient Routable Control Systems document for the complete vision, roadmap, functional technology comparison, and derived requirements.

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. A multidisciplinary team of researchers at PNNL was used to evaluate the various technologies using the requirements and vision identified in the SSCP Specification for Routable Control System Communication Document and the security objectives of these systems. Popular security solutions, protocols and applications were evaluated in light of the derived requirements in the companion document. See the next section for the results of the comparison.

3.0 Comparison

The following table contains a review of the available security technologies and their ability to natively support the derived requirements of the future control system vision.

Native Support for Routable Control System Object Protocol

Derived Requirement	SCTP	UDP/DTLS	TCP/TLS (IEC-62351)	IP/IPSec
Telemetry data must be only authenticated	Yes	Yes	Yes	Yes
Telemetry data may optionally be encrypted	Yes	Yes	Yes	Yes
Telemetry data must be a best-effort transport	Yes	Yes	No	Yes
Telemetry data must be ordered	Yes	No	Yes	No
Control data must be reliable transport	Yes	No	Yes	Yes
Control data must be authenticated	Yes	Yes	Yes	Yes
Control data must be encrypted	Yes	Yes	Yes	Yes
Control data must be in-order delivery	Yes	No	Yes	No
Control data must be highest-priority data with best available quality of service	Yes	No	No	No
Event data must be authenticated	Yes	Yes	Yes	Yes
Event data must be encrypted	Yes	Yes	Yes	Yes
Event data must be reliable transport	Yes	No	Yes	No
Transport layer must provide congestion control mechanism	Yes	No	Yes	N/A
Protocol stack must provide dual-homing and multi-path capabilities	Yes	No	No	Yes
Transport layer must provide management of priority of service	Yes	No	No	N/A
Transport layer management of distinct streams	Yes	No	No	N/A

As is evident, existing protocol do not fully addresses all requirements. Therefore, SCTP was created to satisfy all of the necessary derived requirements. No protocol or solution, in isolation, fully provides the confidentiality, integrity and availability required in control system applications.