Pipeline SCADA Security

API STANDARD 1164
SECOND EDITION, JUNE 2009

REAFFIRMED, OCTOBER 2016

energy API
AMERICAN PETROLEUM INSTITUTE

Pipeline SCADA Security

Pipeline Segment

API STANDARD 1164
SECOND EDITION, JUNE 2009

REAFFIRMED, OCTOBER 2016

energy API
AMERICAN PETROLEUM INSTITUTE

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

Classified areas may vary depending on the location, conditions, equipment, and substances involved in any given situation. Users of this standard should consult with the appropriate authorities having jurisdiction.

Users of this standard should not rely exclusively on the information contained in this document. Sound business, scientific, engineering, and safety judgment should be used in employing the information contained herein.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Foreword

This standard on SCADA security provides guidance to the operators of oil and gas liquids pipeline systems for managing SCADA system integrity and security. The use of this document is not limited to pipelines regulated under Title 49 *CFR* 195.1, but should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA system. This document embodies the API's *Security Guidelines for the Petroleum Industry*. This guideline is specifically designed to provide the operators with a description of industry practices in SCADA security, and to provide the framework needed to develop sound security practices within the operator individual companies. It is important that operators understand system vulnerability and risks when reviewing the SCADA system for possible system improvements.

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Shall: The term "shall" is used in this standard to indicate those practices that are mandatory.

Should: The term "should" is used in this standard to indicate:

— those practices for which engineering judgment is required;

— those practices which are preferred, but for which operators may determine that alternative practices are equally or more effective.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 1220 L Street, NW, Washington, DC 20005. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 1220 L Street, NW, Washington, DC 20005.

Suggested revisions are invited and should be submitted to the Standards Department, API, 1220 L Street, NW, Washington, DC 20005, standards@api.org.

Contents

Page

1 Scope . . . 1
1.1 Purpose and Objectives . . . 1
1.2 Roles and Responsibilities . . . 1

2 Definitions and Acronyms . . . 1
2.1 Definitions . . . 1
2.2 Acronyms . . . 10

3 Management System . . . 11
3.1 Personnel . . . 11
3.2 Security Policies . . . 12
3.3 Risk and Vulnerability Assessment . . . 12
3.4 Business Continuity Plan (BCP) . . . 12
3.5 Incident Response Plan (IRP) . . . 13
3.6 Change Management . . . 13
3.7 Operating System and Application Updates . . . 14
3.8 Application and Software Restrictions . . . 14

4 Physical Security . . . 14

5 System Access Control . . . 15
5.1 Restricted Access . . . 15
5.2 User Accounts . . . 15
5.3 Operating System Accounts . . . 15
5.4 SCADA Accounts . . . 16
5.5 Password Controls . . . 16
5.6 Biometrics . . . 17
5.7 Disabled Non-required Services . . . 17
5.8 Operating System Tools . . . 18
5.9 Device Access . . . 18
5.10 Personnel Administration . . . 18

6 Information Distribution . . . 18
6.1 Confidential . . . 19
6.2 Restricted . . . 19
6.3 Public . . . 20

7 Network Design and Data Interchange . . . 20
7.1 Network Design . . . 20
7.2 Network Management . . . 21
7.3 Data Interchange . . . 24

8 Field Communication . . . 26
8.1 Field Device Technology . . . 26
8.2 System Access . . . 27

Page

Annex A (informative) **28**

Annex B (Example) **SCADA/Control System Security Plan** **7**

Additional Resources. **64**

Figures

1 General SCADA Systems Layout **9**
2 Typical Non-isolated Implementation—Not Recommended. **20**
3 Typical Firewall Isolation Implementation—Minimal Isolation **21**
4 Typical DMZ Implementation—Recommended **22**
5 Typical Dual-homed Computer Bridge Implementation—Not Recommended. **22**

Pipeline SCADA Security

1 Scope

This document is structured so that the main body provides the high-level view of holistic security practices. The annexes provide further details and technical guidance. Reviewing the main body of this document and following the guidance set forth in the annexes assists in creating inherently secure operations. Implementation of this standard, to advance supervisory control and data acquisition (SCADA) cyber security, is not a simple process or one time event, but a continuous process. The overall process could take years to implement correctly depending on the complexity of the SCADA system. Additionally, the process would optimally be started as part of a SCADA upgrade project and use this standard to “design in” security as a element of the new system.

1.1 Purpose and Objectives

The goal of an operator is to control the pipeline in such a way that there are no adverse effects on employees, the environment, the public, or the customers as a result of actions by the operator, or by other parties. This SCADA security program provides a means to improve the security of the pipeline SCADA operation by:

— analyzing vulnerabilities of the SCADA system that can be exploited by unauthorized entities,

— listing the processes used to identify and analyze the SCADA system vulnerabilities to unauthorized attacks,

— providing a comprehensive list of practices to harden the core architecture,

— providing examples of industry best practices.

1.2 Roles and Responsibilities

The operator’s senior management shall implement a program of SCADA security for their organization to identify accountability for all aspects of SCADA security at every organizational level. The SCADA security program scope should include the operator’s organization, business partners, vendors, and external suppliers of SCADA products and services for the SCADA system. The SCADA security program should document the SCADA security plan, identify the roles and responsibilities of security professionals and practitioners who will implement policies and procedures, and provide for the coordination of security efforts in the SCADA domain with the cyber security activities of the entire organization. The SCADA security program shall be designed and communicated so that all personnel who have actual or potential impact on the security of the SCADA system are fully informed of their security roles and responsibilities, and receive adequate training to complete their tasks securely. The SCADA security program should be designed to ensure the organization’s ongoing implementation of industry best practices in cyber security and compliance with all relevant standards.

2 Definitions and Acronyms

2.1 Definitions

For the purposes of this standard the following definitions apply.

2.1.1
access control list
ACL
A list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.