Pipeline Control Systems Cybersecurity

API STANDARD 1164
THIRD EDITION, AUGUST 2021



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. The use of API publications is voluntary. In some cases, third parties or authorities having jurisdiction may choose to incorporate API standards by reference and may mandate compliance.

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.

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.

All rights reserved. No part of this work may be reproduced, translated, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001-5571.

Copyright © 2021 American Petroleum Institute

Foreword

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.

The verbal forms used to express the provisions in this document are as follows.

Shall: As used in a standard, “shall” denotes a minimum requirement in order to conform to the standard.

Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the standard.

May: As used in a standard, “may” denotes a course of action permissible within the limits of a standard.

Can: As used in a standard, “can” denotes a statement of possibility or capability.

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, 200 Massachusetts Avenue, Suite 1100, Washington, DC 20001. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

The American Petroleum Institute maintains this standard under continuous maintenance procedures. These procedures establish a documented program for regular publication of addenda or revisions, including timely and documented consensus action on requests for revisions to any part of the standard. 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, 200 Massachusetts Avenue, Suite 1100, Washington, DC 20001.

Suggested revisions are invited and should be submitted at any time to the Standards Department, API, 200 Massachusetts Avenue, Suite 1100, Washington, DC 20001, standards@api.org.

Contents

Page

1 Scope 1
1.1 Purpose 1
1.2 Intended Audience 2
1.3 How to Read This Standard 2

2 Normative References 4

3 Terms, Definitions, Acronyms, and Abbreviations 4
3.1 Terms and Definitions 4
3.2 Acronyms 9

4 ONG Pipeline IAC Cybersecurity Profiles 10
4.1 IAC Cybersecurity Profile-Introduction 10
4.2 IAC Cybersecurity Profile-Common Constraints 10
4.3 IAC Cybersecurity Profile-Threat Protection Objectives 11
4.4 IAC Cybersecurity Profile-Business and Mission Objectives 12
4.5 IAC Cybersecurity Profile-Objectives Impact to Threat Protection Mapping 13

5 ONG IAC Cybersecurity Policy, Plan, and Program 13
5.1 IAC Cybersecurity Plan-Development 15
5.2 IAC Cybersecurity Plan-Risk Management Foundation 15
5.3 IAC Cybersecurity Plan-Operationalizing an IAC Cybersecurity Program 17
5.4 IAC Cybersecurity Plan-Selecting Cybersecurity Profiles 18
5.5 IAC Cybersecurity Plan-Customizing Selected Profile Requirements 27

6 ONG IAC Cybersecurity Profile Requirements-Identify (ID) 28
6.1 Governance (ID.GV) 28
6.2 Risk Management Strategy (ID.RM) 32
6.3 Business Environment (ID.BE) 35
6.4 Supply Chain Risk Management (ID.SC) 39
6.5 IAC Risk Assessment (ID.RA) 42
6.6 Asset Management (ID.AM) 49

7 ONG IAC Cybersecurity Profile Requirements-Protect (PR) 55
7.1 Access Control (PR.AC) 56
7.2 IAC Cybersecurity Awareness and Training (PR.AT) 63
7.3 Data Security (PR.DS) 67
7.4 Information Protection Processes and Procedures (PR.IP) 75
7.5 Maintenance (PR.MA) 89
7.6 Protective Technology (PR.PT) 92

8 ONG IAC Cybersecurity Profile Requirements-Detect (DE) 97
8.1 Anomalies and Events (DE.AE) 97
8.2 Security Continuous Monitoring (DE.CM) 100
8.3 Detection Processes (DE.DP) 106

9 ONG IAC Cybersecurity Profile Requirements-Respond (RS) 110
9.1 Response Planning (RS.RP) 110
9.2 Communications (RS.CO) 111
9.3 Analysis (RS.AN) 114
9.4 Mitigation (RS.MI) 118
9.5 Improvements (RS.IM) 120

Contents

Page

10 ONG IAC Cybersecurity Profile Requirements-Recover (RC) 122
10.1 Recovery Planning (RC.RP): 122
10.2 Improvements (RC.IM) 122
10.3 Communications (RC.CO) 124

Annex A (informative) API Standard 1164 Construction and Mapping 126

Annex B (informative) Plan-Do-Check-Act Model 129

Annex C (informative) Recurring Actions 131

Bibliography 132

Figures
1 API 1164 Security Level Threat Protection Objectives 12
2 API 1164 Business Objective Impact Mapping to Threat Protection Profiles 13
3 API 1164 CSF Sources for IAC Cybersecurity Policy and Plan 14
4 IAC Cybersecurity Plan Development Participation 15
A.1 TSA Cybersecurity Measures to CSF Core Mapping 126
A.2 CSF Core Mapping to Pipeline Target Profile Requirements 127
A.3 NIST CSF Informative References 128
A.4 API 1164 Content Creation Mapping 128
B.1 Plan–Do–Check–Act (PDCA) Cycle 130

Tables
C.1 Recurring Action Requirements 131

Background

This standard was developed using U.S. Transportation Security Administration's (TSA) *Pipeline Security* Guidelines (March 2018), especially Section 7, "Pipeline Cyber Asset Security Measures." This standard is based on the U.S. National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, *Version 1.1* (CSF) (April 16, 2018), addressing all functions, categories, and subcategories. Activities were selected from the CSF core, with a focus and scoping of industrial automation and control (IAC) environments for the oil and natural gas (ONG) pipeline industry. Special attention was given to common risk management considerations, legal and regulatory requirements (e.g., TSA, FERC, DOT, PHMSA, etc.), and shared business/mission objectives.

This document is specifically written to provide an industry targeted IAC cybersecurity standard for the owner/operators of pipelines regulated under *Code of Federal Regulations (CFR) Title 49 for Transportation, Volume 2, Chapter I, Pipeline and Hazardous Materials Safety Administration (PHMSA), Department of Transportation, Part 192 – Transportation of Natural and Other Gas by Pipeline: Minimum Federal Safety Standards or Part 195 - Transportation of Hazardous Liquids by Pipeline*. This targeted standard specifies the framework, practices, and requirements needed to develop, implement, maintain, test, and constantly improve a robust IAC security program as part of the TSA's required Corporate Security Program. References to these regulations were incorporated at the time of this document's publication. Users are responsible for conforming to current and applicable regulations.

Pipeline Control Systems Cybersecurity

1 Scope

1.1 Purpose

This standard provides requirements and guidance for managing cyber risk associated with industrial automation and control (IAC) environments to achieve security, integrity, and resiliency objectives. Within this standard, this is accomplished through proper isolation of IAC environments from non-IAC environments to help IAC operational continuity.

Even with proper isolation of IAC environments from IT environments, both play a part in overall business continuity. IAC operational continuity and IT system continuity are often developed and implemented jointly as part of the overall business continuity plan.

The scope of this standard is limited to only the IAC cybersecurity aspects that can influence overall business continuity.

This standard is tailored for the oil and natural gas (ONG) pipeline industry, which includes, but is not limited to, natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems, liquefied natural gas (LNG) facilities, propane air facilities, and others involved in these industries.

This standard was developed to provide an actionable approach to protect IAC essential functions by managing cybersecurity risk to IAC environments. IAC environments can include, but are not limited to, supervisory control and data acquisition (SCADA), local control, and industrial internet of things (IIoT) solutions. This standard should be used in the context of developing, implementing, maintaining, and improving an IAC cybersecurity program, which includes the policies, processes, and procedural and technical controls for IAC cyber environments.

This standard is a set of requirements that should be customized prior to implementation using the company's risk management processes. The outcome is a customized, company-specific set of requirements for an IAC cybersecurity program to help manage the cybersecurity posture and any resulting residual risk to its IAC environments in alignment with the company's mission, objectives, and risk strategy, and in accordance with its policies and procedures.

While identification of threats and impacts is critical to the development of the IAC cybersecurity program, a risk-based evaluation of each will ensure the program is appropriately implemented, executed, and sustained consistent with an organization's desired risk posture. This standard focuses on desired cybersecurity outcomes by defining requirements for specific business objective impact protection levels.

Although the principles defined in this standard could be applied to safety instrumented systems (SIS), they are out of scope of this document. The security requirements specified within this standard do not attempt to address potential impacts to SIS safety integrity level (SIL) selection or determination. Any use of this standard in SIS environments is at the implementer's discretion and risk.

For companies that already have an IAC cybersecurity program, including one or more approved program policies and a documented IAC cybersecurity plan or plans implemented or being implemented, this standard should be considered an augmentation to their existing cybersecurity program elements. In these situations, a process of mapping this standard to current IAC cybersecurity program elements will determine any API 1164 requirements not currently in the existing program. The implementation of any missing elements should be tailored and prioritized using the company's risk management processes. The tailoring process for API 1164 cybersecurity requirements is described in 5.5.