ASCE STANDARD

ASCE/EWRI

78-24

Guidelines for the Physical Security of Water and Wastewater/ Stormwater Utilities

ASCE
AMERICAN SOCIETY OF CIVIL ENGINEERS

EWRI
ENVIRONMENTAL & WATER RESOURCES INSTITUTE

ASCE STANDARD

ASCE/EWRI

78-24

Guidelines for the Physical Security of Water and Wastewater/ Stormwater Utilities

PUBLISHED BY THE AMERICAN SOCIETY OF CIVIL ENGINEERS

Cataloging-in-Publication Data on file with the Library of Congress

Published by American Society of Civil Engineers
1801 Alexander Bell Drive
Reston, Virginia, 20191-4382
www.asce.org/bookstore | ascelibrary.org

This standard was developed by a consensus standards development process that has been accredited by the American National Standards Institute (ANSI). Accreditation by ANSI, a voluntary accreditation body representing public and private sector standards development organizations in the United States and abroad, signifies that the standards development process used by ASCE has met the ANSI requirements for openness, balance, consensus, and due process.

While ASCE's process is designed to promote standards that reflect a fair and reasoned consensus among all interested participants, while preserving the public health, safety, and welfare that is paramount to its mission, it has not made an independent assessment of and does not warrant the accuracy, completeness, suitability, or utility of any information, apparatus, product, or process discussed herein. ASCE does not intend, nor should anyone interpret, ASCE's standards to replace the sound judgment of a competent professional, having knowledge and experience in the appropriate field(s) of practice, nor to substitute for the standard of care required of such professionals in interpreting and applying the contents of this standard.

ASCE has no authority to enforce compliance with its standards and does not undertake to certify products for compliance or to render any professional services to any person or entity.

ASCE disclaims any and all liability for any personal injury, property damage, financial loss, or other damages of any nature whatsoever, including without limitation any direct, indirect, special, exemplary, or consequential damages, resulting from any person's use of, or reliance on, this standard. Any individual who relies on this standard assumes full responsibility for such use.

ASCE and American Society of Civil Engineers—Registered in US Patent and Trademark Office.

Photocopies and permissions. Permission to photocopy or reproduce material from ASCE publications can be requested by sending an email to permissions@asce.org or by locating a title in ASCE's Civil Engineering Database (https://cedb.asce.org) or ASCE Library (https://ascelibrary.org) and using the "Permissions" link.

Errata: **Errata, if any, can be found at http://dx.doi.org/10.1061/9780784485071.**

Copyright © 2024 by the American Society of Civil Engineers.

All Rights Reserved.
ISBN 978-0-7844-1615-0 (soft cover)
ISBN 978-0-7844-8507-1 (PDF)

Manufactured in the United States of America.

29 28 27 26 25 24 1 3 2 4 5

ASCE STANDARDS

The Board of Direction approved revisions to the ASCE Rules for Standards Committees to govern the writing and maintenance of standards developed by ASCE. All such standards are developed by a consensus standards process managed by the ASCE Codes and Standards Committee (CSC). The consensus process includes balloting by a balanced standards committee and reviewing during a public comment period. All standards are updated or reaffirmed by the same process at intervals between five and ten years. Requests for formal interpretations shall be processed in accordance with Section 7 of ASCE Rules for Standards Committees, which are available at https://www.asce.org/-/media/asce-images-and-files/publications-and-news/publications/documents/asce-rules-standards-committees.pdf.

Errata, addenda, supplements, and interpretations, if any, for this standard can also be found at https://ascelibrary.org/.

The provisions of this standard are written in permissive language and as such offer the user a series of options or instructions but do not prescribe a specific course of action. Significant judgment is left to the user.

This standard has been prepared in accordance with recognized engineering principles and should not be used without the user's competent knowledge for a given application. The publication of this standard by ASCE is not intended to warrant that the information contained therein is suitable for any general or specific use, and ASCE takes no position respecting the validity of patent rights. Be advised that the determination of patent rights or risk of infringement is entirely the user's own responsibility.

CONTENTS

PREFACE ix

ACKNOWLEDGMENTS xi

1 OVERVIEW OF GUIDELINES 1
- 1.1 Scope 1
- 1.2 Purpose of the Guidelines 1
- 1.3 Background of the Initial Development 1
- 1.4 Use of These Guidelines 2
- 1.5 Glossary and Abbreviations 2

2 APPLICATION OF GUIDELINES 7
- 2.1 Introduction 7
- 2.2 Cumulative Defense Strategy 7
- 2.3 Critical Asset Identification 7
- 2.4 Consequence Identification: Critical Asset Breach 7
- 2.5 Scenario Identification: Attack Vectors 7
  - 2.5.1 Adversary on Foot 7
  - 2.5.2 Vehicle Ramming Breach 8
  - 2.5.3 Vehicle-Borne Improvised Explosive Device 9
  - 2.5.4 Adversarial Use of Maritime Vehicles 9
  - 2.5.5 Adversarial Use of Unmanned (Uncrewed) Aircraft Systems 9
- 2.6 Path Analysis 9
- 2.7 Difficulty Identification 9
  - 2.7.1 Defense Layer 9
  - 2.7.2 Defense Layer Elements 9
  - 2.7.3 Characteristics of Countermeasures 10
  - 2.7.4 Importance of the Mathematical Analysis of Defense Strategy and Countermeasures Methodology 11
- 2.8 Vulnerability Determination 11
- 2.9 Response Evaluation 11
- 2.10 Cost–Benefit Analysis 11
- 2.11 Risk Management 11
  - 2.11.1 Risk Mitigation 11
  - 2.11.2 Transferring the Risk 11
  - 2.11.3 Risk Acceptance 11

3 DETERMINING DIFFICULTY OF PHYSICAL SECURITY COUNTERMEASURES 13
- 3.1 Introduction 13
- 3.2 Probability of Success of a Given Threat ($P_{S/T}$) 13
- 3.3 Mathematical Analysis of Defense Strategy and Countermeasures Methodology 13
- 3.4 Minimum Difficulty Threshold 14
- 3.5 Site-Specific Model Calibration 17
- 3.6 Calculating Degree of Difficulty to Compromise Countermeasures 17
- 3.7 Expanded Cost–Benefit Analysis Discussion 17

APPENDIX A PHYSICAL SECURITY COUNTERMEASURES 21
- A.1 Fencing and Perimeter Walls 21
  - A.1.1 Chain-Link Fencing 21
  - A.1.2 Anti-Climb/Anti-Cut Fencing 21
  - A.1.3 Ornamental Fencing 21
  - A.1.4 Perimeter Wall 21
  - A.1.5 Fence Topping 21

A.1.6 Perimeter Line . . . 21
A.1.7 Fence Foundation Enhancements . . . 21
A.2 Gates . . . 21
A.2.1 Chain-Link Gates . . . 22
A.2.2 Electronic Gate Opening . . . 22
A.2.3 Electronic Gate Control System . . . 22
A.2.4 K-rated Gates . . . 22
A.3 Signage . . . 22
A.3.1 Fence Signage . . . 22
A.3.2 Primary Site Entrance Signage . . . 22
A.3.3 Water Intake Delineation . . . 22
A.4 Outdoor Security Lighting . . . 22
A.5 Bollards and other Vehicle Barriers . . . 23
A.5.1 Speed Reduction Techniques . . . 23
A.5.2 Entry and Exit Vehicle Flow Control . . . 23
A.5.3 Full Perimeter Vehicle Barrier . . . 24
A.5.4 Facility Barrier Protection . . . 24
A.6 Open Space (Observation Zone) . . . 24
A.6.1 Open Space between Detection Line and the Facility . . . 24
A.7 Electronic Security Systems . . . 24
A.7.1 Intrusion Detection Sensors: General . . . 24
A.7.2 Exterior Intrusion Detection . . . 24
A.7.3 Interior Intrusion Detection . . . 25
A.7.4 Door and Hatch Contact Alarm Switches . . . 25
A.7.5 Pipeline Vibration Detection . . . 25
A.8 Physical Access Control Systems . . . 26
A.8.1 Access Control Systems: General . . . 26
A.8.2 Locks and Padlocks . . . 26
A.8.3 Numeric Keypad Locks . . . 26
A.8.4 Card Reader Systems . . . 26
A.8.5 Dual-Factor Authentication . . . 26
A.8.6 Multifactor Authentication . . . 26
A.9 Surveillance Cameras . . . 26
A.9.1 General Considerations . . . 26
A.9.2 Field of View . . . 26
A.9.3 Housing and Mounts . . . 27
A.9.4 Video Network Servers . . . 27
A.9.5 Digital Video Recorders . . . 27
A.9.6 Unified Video Management System . . . 27
A.9.7 Video Analytics . . . 27
A.9.8 Restricted Surveillance Equipment Vendors . . . 27
A.10 Facility Hardening . . . 27
A.10.1 General . . . 27
A.10.2 Exterior Hardening . . . 27
A.10.3 Interior Hardening . . . 28
A.11 Intrusion Notification Systems . . . 28
A.11.1 Mass Notification Systems . . . 28
A.11.2 Alarms, Sirens, Signal Lighting, and Strobes . . . 29
A.12 Tactical Deterrence . . . 29
A.12.1 Human Capital . . . 29
A.12.2 Trained Animals . . . 29
A.12.3 Long-Range Acoustic Device . . . 29
A.12.4 Targeted Illumination . . . 29
A.13 Security, Controls, and SCADA Wiring . . . 29
A.13.1 SCADA and Electrical Control Panel Enclosures . . . 29
A.13.2 IT Equipment Enclosures . . . 29
A.14 Online Water Quality Monitoring . . . 29
A.15 Chemical Fill-Line Locking Devices . . . 29
A.16 Hydrants . . . 29
A.17 Manholes . . . 30
A.18 Site Utilities . . . 30

APPENDIX B PHYSICAL SECURITY COUNTERMEASURE REFERENCE TABLES WITH TYPICAL APPLICATION DRAWINGS . . . 31
B.1 Introduction . . . 31
B.2 Countermeasure Reference Table Matrix . . . 31
B.3 Countermeasure Reference Tables Overview . . . 31

APPENDIX C SYSTEM FACILITIES SCOPE AND MISSION . . . 51
C.1 Introduction . . . 51
C.2 Water Treatment Plants . . . 51
C.2.1 Scope . . . 51
C.2.2 Mission . . . 51
C.3 Raw Water Facilities . . . 51
C.3.1 Scope . . . 51
C.3.2 Mission . . . 51
C.4 Wells and Pumping Stations . . . 52
C.4.1 Scope . . . 52
C.4.2 Mission . . . 52
C.5 Water System Support Facilities . . . 52
C.5.1 Scope . . . 52
C.5.2 Mission . . . 52
C.6 Finished Water Storage Facilities . . . 52
C.6.1 Scope . . . 52
C.6.2 Mission . . . 52
C.7 Water Distribution Systems . . . 53
C.7.1 Scope . . . 53
C.7.2 Mission . . . 53
C.8 Wastewater/Stormwater Treatment Plants . . . 53
C.8.1 Scope . . . 53
C.8.2 Mission . . . 53
C.9 Collection Systems . . . 53
C.9.1 Scope . . . 53
C.9.2 Mission . . . 53
C.10 Pumping Stations . . . 54
C.10.1 Scope . . . 54
C.10.2 Mission . . . 54
C.11 Wastewater/Stormwater System Support Facilities . . . 54
C.11.1 Scope . . . 54
C.11.2 Mission . . . 54

REFERENCES . . . 55

INDEX . . . 59

PREFACE

Historically, malevolent acts have largely been categorized as threats alongside of natural hazards as part of an "All-Hazards" approach, and most vulnerability assessments score physical security as a low priority due to a lack of frequentist probability data when compared to natural weather phenomena. This has caused reduced confidence among owners and operators in the assessments and the subsequent mitigation steps for malevolent acts. Instinctively sensing something awry, key stakeholders have been likely to overspend on physical security countermeasures by trying to ensure the protection of everything, or conversely, by trusting that the assessment accurately revealed that security spending should be minimized, they grossly underspend. In this context, the ANSI/ASCE/EWRI 56-10/57-10 *Guidelines for Physical Security for Water and Wastewater/Stormwater Facilities* became little more than a checklist of optional security countermeasures without providing a means of cost–benefit analysis.

The suggested new direction was to update *Guidelines for the Physical Security of Water Utilities and Wastewater and Stormwater Utilities*, accepted in 2010 by ASCE. This new direction recognizes that the original intent of these guidelines was to serve as a "centralized starting point for water and wastewater/stormwater utilities to integrate modern security practices into the management, operation, construction, or retrofit of water, wastewater and stormwater systems."

Key Findings of 2021 ASCE/EWRI WISE SC Ad Hoc Group In 2021, the ASCE/EWRI WISE SC Ad Hoc Group indicated that previous versions of water sector security guidelines were limited, using a common risk model to protect against malevolent attacks. The original risk model was assessed in terms of threat likelihood, vulnerability, and consequence ($R = T \times V \times C$), which has led to a reaction of chasing threats, real or otherwise, and over- or under-hardening of critical assets as a reaction to the data produced. The reason is that defining a malevolent threat is dependent on the identification of the "who," "capability," and "likelihood" of malevolent actors, all of which were unknowns.

1. WHO: In an effort to define who the adversary might be, a prerequisite was placed on determining one of the predefined malevolent actor types of vandals, criminal, saboteur, or insider, also known as design basis threat (DBT) methodology. This resulted in a low probability of accuracy because of limited historical data. This approach also restricted the ability to guard against emerging threats such as foreign or domestically activated disenfranchised people groups through social media disinformation campaigns resulting in ground swell, organic attacks that do not fit in the DBT classifications. For these reasons, the use of DBT in these standards has been deprecated.
2. CAPABILITY: In addition, the effort was to define malevolent actor capability by presupposing their training, funding, ideology, preferred targets, tools, or ability to gain access to intelligence such as insider information, all without being caught by law enforcement. Again, limited historical data reduced this effort to guesswork, resulting in unfounded predictions about the preparation or skill a malevolent actor might have.
3. LIKELIHOOD: Likelihood of a malevolent threat event happening was calculated by using historical frequency. By following this method, the Environmental Protection Agency (USEPA) in February 2021 determined that out of 100,000 potential water utility targets, the likelihood of threat events such as adversaries jumping from helicopters into a water utility each year was 1:1,000,000 (or 10^{-6} power) (USEPA 2021). Using this approach for breach scenarios and data configurations has created wide error bands since the implied conclusion is to minimally invest in physical security countermeasures altogether.

The ASCE/EWRI WISE SC Ad Hoc Group indicated that the lack of an adequate data set from which to ascertain the aforementioned criteria put disqualifying limitations on the risk formula and created errors for making informed decisions. Furthermore, the attempt to derive meaningful data from what is not known has produced erroneous probability results that are hazardous to the physical security of water sector utility operations.

Cumulative Defense Strategy Overview Cumulative Defense Strategy is a process that is used to help secure critical assets against malevolent attacks. The process takes a wholistic approach to helping protect the facility under evaluation. Similar to methodologies used by other organizations, the approach considers the consequence of a particular critical asset being compromised and the approach used to carry out the attack. Using path analysis and the existing physical security countermeasure installed at the facility, the degree of difficulty to compromise the critical asset is mathematically calculated using the Foster–Wallace Formula (Wallace and Foster 2021). With this information, the facilities' vulnerability to different attack scenarios can be evaluated, response plans can be formulated, and subsequent risk management decisions can be made to further mitigate the current exposure in the event of an attack.

Mathematical Analysis of Defense Strategy and Countermeasures Methodology Overview The Mathematical Analysis of Defense Strategy and Countermeasures (MADSC) methodology is the process of evaluating the probability of success of a given threat based on a scenario identified, difficulty identified, and a consequence identified. It relies on cumulative defense strategy for the sequential increase in quantity and quality of physical security countermeasures across multiple defense layers to defend against specific attack vectors. Only attack vectors that are reasonable to defend against using security countermeasures available to the public sector are considered in these standards. The MADSC methodology as suggested by Wallace et al. (2024) provides a comprehensive plan to evaluate and enhance physical security countermeasures to defend against malevolent attacks.

Other Valuable ASCE Books Topics in *Structural Design for Physical Security*, MOP 142, could be a valuable resource to projects that have physical security concerns related to explosive, ballistic, forced entry, and hostile vehicle threats that include

- Threat determination and available assessment and criteria documents,
- Methods by which structural loadings are derived for the determined threats,

- Function and selection of structural systems,
- Design of structural components,
- Function and selection of window and facade components,
- Specific considerations for retrofitting structures,
- Testing methodologies, and
- Bridge security.

Additional topics in *Hazard-Resilient Infrastructure Analysis and Design*, MOP 144, provide a comprehensive description of facility resilience with respect to critical infrastructure. The process discussed in that MOP used in conjunction with the MADSC methodology could help provide a comprehensive hazard-resilient infrastructure plan for critical infrastructure.

ACKNOWLEDGMENTS

These voluntary guidelines were developed during the USEPA WISE Project, Phase 3, under the direction of the ASCE/EWRI WISE Standards Committee (ASCE/AWWA/WEF 2006a, b). The former committee consisted of the individuals first listed below through the end of the 2010 Committee balloting processes. The current ASCE/EWRI WISE standards committee consists of both groups of individuals listed.

Clyde R. Dugan
John H. Easton, Ph.D., *Vice Chair*
Conrad G. Keyes Jr., Sc.D., P.E., P.S., D.WRE (Ret.), Dist.M.ASCE, *Past Chair*
Jorge A. Garcia, Ph.D., P.E.
Neil S. Grigg, Ph.D., P.E., D.WRE (Ret.)
C. Dale Jacobson, P.E., BCEE, D.WRE
Charles R. Stack, MPH, BCES
C. Wesley Strickland, Esq.
James F. Wheeler, P.E.
Robert C. Williams, P.E., BCEE

The newest members listed per Fiscal Years 2020–2023 WISE SC balloting processes follow.

David Wallace, M.ASCE, *Chair*
Kris Schartau, B.S.E.E, A.M.ASCE, *Secretary*
Joseph Crisologo, P.E.
Thomas DeFelice, Ph.D., M.ASCE
Robert Janke
Kathlie S. Jeng-Bulloch, Ph.D., P.E., D.WRE, CFM
Leonard J. Kusek
David Lewin

CHAPTER 1
OVERVIEW OF GUIDELINES

1.1 SCOPE

The first physical security of water and/or wastewater/stormwater guidelines were developed as a joint effort between ASCE and the American Water Works Association (AWWA) with technical input from the Water Environment Federation (WEF), in accordance with ASCE Rules for Standards Committees, and were published initially as the proposed drafts, *Guidelines for the Physical Security of Water Utilities* (ASCE/AWWA/WEF 2006a) and *Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2006b). That consensus process included balloting by a balanced ASCE/Environmental & Water Resources Institute (EWRI) Water Infrastructure Security Enhancement (WISE) Standards Committee (SC) and reviewing during a public comment period. In 2014, Supplement No. 1 for the two ANSI/ASCE/EWRI physical security standards 56 and 57 were taken through the same process. From 2018 to 2021, another balloting process of combining the two documents (called Com 56-57 by the WISE SC) was taken through the last ASCE balloting process in 2021 and both 56 and 57 (ASCE 2010b, c) were withdrawn as ANSI/ASCE/EWRI standards; but the material was saved by the WISE SC and has become a part of these current guidelines. The provisions of this document have been written in permissive language and, as such, offer the user a series of options or instructions but do not prescribe a specific course of action. Significant judgment is left to the user of these documents.

These guidelines use customary units, with the International System of Units (SI) in parentheses. This approach was in the best interest of ASCE, AWWA, and WEF at the time of development of the initial drafts of the previous guidelines.

1.2 PURPOSE OF THE GUIDELINES

These guidelines apply to the evaluation and enhancement of physical security for facilities used in potable water sources (raw water), treatment, and distribution systems, as well as for wastewater and stormwater facilities.

1.3 BACKGROUND OF THE INITIAL DEVELOPMENT

Highlights related to the creation of all the WISE guidance documents and/or standards in the early years of the twenty-first century are summarized as follows (ASCE 2010b, c; Wallace et al. 2024):

1. Under the US Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL 107–188), drinking water utilities serving more than 3,300 customers were required to conduct vulnerability assessments of their water systems. The vulnerability assessments often recommended security improvements to reduce the risk of malevolent acts (such improvements may also reduce the risk associated with natural events). Similar requirements for wastewater utilities have yet to be promulgated, but the protection of wastewater utility facilities using similar approaches has been promoted by the Environmental Protection Agency (USEPA) and various industry organizations. In addition, ASCE, AWWA, and WEF agreed to work together to develop materials to assist in the implementation of security recommendations and the overall improvement of water and wastewater infrastructure security. The project was funded by USEPA under a cooperative agreement to foster public/private partnership in water and wastewater security. This project was known as the USEPA Water Infrastructure Security Enhancements (WISE) Project.
2. Phase 1 of the USEPA WISE project focused on the creation of Interim Voluntary Security Guidance documents (ASCE/AWWA/WEF 2004a, b, c). The purpose of these documents was to provide a centralized starting point for utilities as they integrate modern security practices into the management, operation, construction, or retrofit of their water, wastewater, and stormwater systems. Training materials were developed in Phase 2 to disseminate the information contained in the Phase 1 guidance documents.
3. Under the direction of the EPA, Phase 3 focused solely on the development of physical security guidelines for water, wastewater, and stormwater facilities. These voluntary consensus guidelines were first developed as the Draft and were published initially as *Guidelines for Physical Security for Water Utilities* (ASCE/AWWA/WEF 2006a) and *Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (ASCE/AWWA/WEF 2006b).
4. The USEPA Water Security Working Group presented its report *Recommendations of the National Drinking Water Advisory Council to the U.S. Environmental Protection Agency on Water Security Practices, Incentives, and Measures* to the National Drinking Water Advisory Council (NDWAC) on May 18, 2005 (WSWG 2005). Those findings included 18 features of an "active and effective" security program. The ANSI/ASCE/EWRI 56 and 57 guidelines addressed the following NDWAC recommendations, which discussed physical security:
   (a) Establish physical and procedural controls to restrict access to utility infrastructure to only those conducting authorized official business and to detect unauthorized physical intrusions.
   (b) Incorporate security considerations into decisions about acquisition, repair, major maintenance, and