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

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

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.

This page intentionally left blank

CONTENTS

This page intentionally left blank

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,