ANSI/AWWA J100-21

(Revision of ANSI/AWWA J100-10[R13])

AWWA Standard

Risk and Resilience Management of Water and Wastewater Systems

Effective date: May 1, 2021.

First edition approved by Board of Directors January 17, 2010.

This edition approved Jan. 25, 2021.

Approved by American National Standards Institute Dec. 3, 2020.

American Water Works Association

Approved American National Standard

ANSI

STANDARD Since 1881

AWWA Management Standard

This document is an American Water Works Association (AWWA) management standard. It is not a specification. AWWA management standards describe consensus requirements for utility management practices. The use of AWWA management standards is entirely voluntary. This standard does not supersede or take precedence over or displace any applicable law, regulation, or codes of any governmental authority. AWWA management standards are intended to represent a consensus of the water industry of requirements and practices that utilities should strive to achieve. When AWWA revises or withdraws this standard, an official notice of action will be placed in the Official Notice section of *Journal AWWA.* The action becomes effective on the first day of the month following the month of *Journal AWWA* publication of the official notice.

American National Standard

An American National Standard implies a consensus of those substantially concerned with its scope and provisions. An American National Standard is intended as a guide to aid the manufacturer, the consumer, and the general public. The existence of an American National Standard does not in any respect preclude anyone, whether that person has approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard. American National Standards are subject to periodic review, and users are cautioned to obtain the latest editions. Producers of goods made in conformity with an American National Standard are encouraged to state on their own responsibility in advertising and promotional materials or on tags or labels that the goods are produced in conformity with particular American National Standards.

Caution Notice: The American National Standards Institute (ANSI) approval date on the front cover of this standard indicates completion of the ANSI approval process. This American National Standard may be revised or withdrawn at any time. ANSI procedures require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of ANSI approval. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute, 25 West 43rd Street, Fourth Floor, New York, NY 10036; (212) 642-4900, or e-mailing info@ansi.org.

ISBN-13, print: 978-1-64717-04[illegible]-8 ISBN-13, electronic: 978-1-61300-583-5

DOI: 10.12999/AWWA.J100.21

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including scanning, recording, or any information or retrieval system. Reproduction and commercial use of this material is prohibited, except with written permission from the publisher. Please send any requests or questions to permissions@awwa.org.

Committee Personnel

The AWWA Standards Committee on Risk and Resilience Management, which reviewed and approved this standard, had the following personnel at the time of approval:

John McLaughlin, Chair

Service Provider/Consulting Services

D.B. Ballantyne, Ballantyne Consulting, LLC, Tacoma, Wash.
J.P. Brashear, Consultant, Ashland, Ore.
B.O. Elwell, Elwell Consulting Group PLLC, Taylorsville, Utah
J. Graves, AEM Corporation, Herndon, Va.
C. Jaeger, Consultant, Albuquerque, N.Mex.
J.W. McLaughlin, Merrick & Company, Charlotte, N.C.
D.C. Rees, Tynwdd Consulting Group LLC, Seattle, Wash.

Management Interest

L.W. Casson, University of Pittsburgh Engineering, Pittsburgh, Pa.
S.W. Clark, USEPA, Washington, D.C.
K. Morley, American Water Works Association, Washington, D.C.
E.S. Ralph (*liaison, nonvoting*), Standards Engineer Liaison, American Water Works Association, Denver, Colo.

Utility/User

G.V. Burchfield, Columbus Water Works, Columbus, Ga.
X.J. Irias (*liaison, nonvoting*), East Bay Municipal Utility District, Standards Council Liaison, Oakland, Calif.
N.W. Santillo, Jr., New Jersey American Water, Cherry Hill, N.J.
S.D. Spencer, Prince William County Service Authority, Norwalk, Conn.
S. Stephens, Witt O'Briens, LLC., Kyle, Tex.
M. Stuhr, Portland Water Bureau, Portland, Ore.
C.T. Walczyk, SUEZ, Paramus, N.J.

This page intentionally blank.

Contents

All AWWA standards follow the general format indicated subsequently. Some variations from this format may be found in a particular standard.

SEC. PAGE

Tables

Foreword

This foreword is for information only and is not a part of ANSI/AWWA J100.

I. Introduction.

I.A. *Background.* The AWWA Management Standards Program is designed to serve water, wastewater, and reuse utilities* and their customers, owners, service providers, and government regulators. The standards developed under the program are intended to improve a utility's overall operation and service. Among these standards is this effort to establish formal management and operational guidelines. These guidelines identify appropriate practices, procedures, and behaviors whose implementation will provide effective, efficient, secure, and resilient utility operations, and contribute to the protection of public health, public safety, the environment, and the regional economy.

AWWA's standards process has been used for more than ninety years to produce water sector standards for materials and processes that are accepted by the American National Standards Institute (ANSI). These standards are recognized worldwide and have been adopted by many utilities and organizations. This management standard is developed using the same ANSI-recognized formal process. Volunteer standards committees establish standard practices in a uniform and appropriate format.

Formal standards committees have been and continue to be formed to address the individual standard practices for the diverse areas of the water sector. A formal AWWA standards committee was created in 2007 to develop a standard for risk and resilience.

I.B. *History.* The first edition of this standard was approved by the AWWA Board of Directors on January 17, 2010, and approved by ANSI on May 4, 2010. It was reaffirmed on June 9, 2013. This second edition was approved by the AWWA Board of Directors on Jan. 25, 2021, and by ANSI on Dec. 3, 2020.

Following the attacks of September 11, 2001, the American Society of Mechanical Engineers (ASME) convened more than one hundred industry leaders at the request of the White House to define and prioritize the requirements for protecting our nation's critical infrastructure. The leaders' primary recommendation was to create a risk analysis and management process to support decisions allocating resources to risk-reduction initiatives within and across infrastructure sectors. This support would necessitate a common terminology, common metrics, common scenarios, and consistent methodology—tailored to the technologies, practices, and cultures of the respective

* Reuse utilities and facilities are considered included in "water and wastewater." Other critical infrastructures may also find use of this standard to enhance their security and resilience.

industries—to permit direct comparisons within and across industry sectors. Such direct comparisons were essential to supporting rational decision-making in allocating limited private and public resources to reducing risk to critical infrastructures.

In response to this recommendation, ASME convened a team of distinguished risk analysis experts from industry and academe to develop the method and framework. They defined a seven-step methodology that enabled asset owners to perform analyses of their risks and risk-reduction options relative to specific malevolent attacks. Risk is defined as a function of the likelihood of specific attacks, the asset's vulnerability to these attacks, and the consequences of the attack. With this information, alternative risk-reduction actions can be evaluated for their ability to reduce the vulnerability, likelihood, and/or consequences of a malevolent attack. Reductions in risks are the benefits that can be used in estimating net benefits (benefits less costs) and net benefit-cost ratios that will allow for the making of informed decisions to allocate resources to specific risk-reduction actions.

The initial version was the draft *Risk Analysis and Management for Critical Asset Protection: General Guidance* (2004) ("General Guidance"), a detailed description of the general process. The General Guidance was widely circulated in draft and reviewed extensively by panels of applied risk management and security experts. It was a competent and comprehensive synthesis of the best available methods and appropriate for academic or risk professionals. It was not, however, as useful to the key engineering, security, operating, and management personnel at the facilities of concern. Consequently, a key design criterion (among others) to encourage widespread application was that the methodology be appropriate for self-assessment primarily by on-site staff in a relatively short period for a typical medium-large system. In response to this feedback and the key design requirement, the General Guidance, which was never published, was streamlined and simplified into two documents, the semi-technical *Introduction to Risk Analysis and Management for Critical Asset Protection* (2005) and a nontechnical *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Applied to Terrorism and Homeland Security* (2005), written expressly for the intended audience.

The methodology described in those three initial documents was designated in the various drafts of the original National Infrastructure Protection Plan (NIPP 2006), which called it the "RAMCAP Framework," from early drafts circulated in 2004 to the 2005 Interim Draft and the final 2006 version, as meeting the NIPP requirements for a simple and efficient process to support consistent, quantitative analyses and with results that could be systematically and directly compared. In 2006, the earlier documents were updated and republished as "RAMCAP: The Framework, Version 2.0," which was still oriented to malevolent attacks only. The 2006 version of the NIPP broadened the definition of the concerns from malevolent attacks only to include natural hazards, which this standard has incorporated. In the aftermath of Hurricane Katrina, the RAMCAP framework was correspondingly extended to include hurricanes, earthquakes, floods, and tornadoes for continuing development.

In 2003, the US Department of Homeland Security (DHS) initiated development of sector-specific guidance for nuclear power plants and spent fuel transportation and storage, petroleum refineries, chemical manufacturing plants, liquefied natural gas (LNG) off-loading terminals, dams and locks, and water and wastewater systems. The guidance for water and wastewater systems, RAMCAP Approach for the Water Sector: Overview (2007) was the immediate predecessor of the ANSI/ASME-ITI/AWWA J100-10 Risk Analysis and Management for Critical Asset Protection Standard for Risk and Resilience Management of Water and Wastewater Systems.

The J100 standard was developed to meet three major objectives in the water sector: (1) to define a common framework that can be used by the water sector to assess human-caused and natural hazards risk to their systems and the communities they serve; (2) to develop risk-based vulnerability analyses and value-based prioritized actions to reduce risk and enhance resilience; and (3) to provide an efficient and consistent mechanism that can be applied to both private and governmental (federal, state, and local) sectors to share essential risk and benefit information to operators of the utilities, local and state governments, DHS, US Environmental Protection Agency (USEPA), and others with a need to know. The present standard also seeks to advance these goals.

In 2009, *All-Hazards Risk and Resilience: Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach* was published, updating the "RAMCAP: The Framework, Version 2.0." This updated version contained several improvements over the 2007 RAMCAP water guidance that were subsequently incorporated into J100-10.

The NIPP (versions in 2006, 2009, and 2013) outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes. Presidential Policy Directive 21 (PPD-21) assigned a federal agency, known as a Sector-Specific Agency (SSA), to lead a collaborative process for critical infrastructure security within each of the 16 critical infrastructure sectors. Each SSA is responsible for developing and implementing a sector-specific plan (SSP), which details the application of the NIPP concepts to the unique characteristics and conditions of their sector. The Environmental Protection Agency is responsible for the Water Sector.

The water sector includes drinking water and wastewater systems. *The Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (PL 107-188) required community water systems serving a population of more than 3,300 to perform security vulnerability assessments principally focused on terrorist threats. Subsequently, the water sector spent considerable resources and efforts to refine a voluntary approach that would provide a reasonably balanced assessment of risk and resilience considering all-hazards. This resulted in the first edition of the J100 standard in 2010. The Water Sector Coordinating Council, official representative of the nation's water sector under the NIPP, determined that the J100-10 standard was the preferred approach for their sector to support the goals outlined in the Sector Specific Plan. Multiple water systems have voluntarily implemented J100 to inform their risk and resilience management strategy to facilitate efficient allocation of resources to actions that seek to maximize risk reduction and/or enhance resilience.

In 2013, AWWA reaffirmed this standard with ANSI following the withdraw of ASME-ITI from management of the standard. The J100 standard is solely managed by AWWA. In addition, use of the term "RAMCAP" will cease given the trademark is held exclusively by ASME. All future references will be "J100" or "J100 methodology" when describing this standard.

The America's Water Infrastructure Act (AWIA) of 2018 (PL 115-270), requires community water systems serving a population of more than 3,300 to prepare a risk and resilience assessment and emergency response plan every five years. The risk and resilience assessment must consider threats from both malevolent acts and natural hazards that could impact the mission of the utility due to physical or cyber incidents. The findings of the risk and resilience assessment must then be used to inform the development of an emergency response plan that considers plans and procedures that can be implemented to "obviate or significantly lessen the impact" on the health, safety, and supply of drinking water from malevolent acts or natural hazards. The J100 methodology provides the necessary framework to prepare the required risk and resilience assessment, including consideration of actions that reduce risk or enhance resilience as called for in the emergency response plan requirement of AWIA. A J100-based risk and resilience assessment is enhanced when applied with related standards and resources, including:

- ANSI/AWWA G430: Security Practices for Operations and Management,
- ANSI/AWWA G440: Emergency Preparedness Practices,
- ANSI/AWWA G300: Source Water Protection,
- M19: Emergency Planning for Water and Wastewater Utilities,

- Emergency Power Source Planning for Water and Wastewater, and
- AWWA Cybersecurity Guidance and Use-Case Tool.

I.C. *Acceptance.* No applicable information for this standard.

II. Special Issues

II.A. *Advisory Information on Application of Standards*. The J100 standard is divided into two basic parts: (1) the Main Body of the standard and (2) the Appendixes. Additional information that is advisory in nature, educational, and/or provides illustrative examples has been developed to support the application of the standard and will be included in a new J100 Operational Guide that is under development.

II.B. *Possible Topics for Future Standards*. Future revisions to the standard may include requirements and considerations for the following topical areas related to this standard:

- Sea Level Rise and Water Scarcity/Drought. The utility should consider these as modifiers of various natural hazards particularly flood and drought.
- Shifts in Consideration of Malevolent Threats. Initially, the focus was on major terrorist incidents such as the Alfred P. Murrah Federal Building bombing in Oklahoma City and the September 11 attacks. Today, there is also concern with domestic groups, sleeper cells, social media-influenced terrorism, and new tendencies modes of attack.
- Electromagnetic Pulse (EMP). EMP is a short burst of electromagnetic energy whose origins may be from a natural occurrence or from a man-made event. EMP is a relatively new threat because of the short history of electronic devices that would suffer consequences from an EMP.
- Environmental Degradation. Including environmental degradation among the obligatory consequences.
- Interdependencies not Previously Considered. Frequently dependencies and interdependencies in assessments include (if any are included) only the electrical power systems, the chemical suppliers-delivery systems, or even transportation access to key facilities. Today's complex water and wastewater systems, however, have growing dependency on an array of support systems that must be functional when needed if sustainability of operations is to be achieved. Many of these supporting systems are publicly owned and operated.

II.C. *SAFETY Act Designation. The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002* ("SAFETY Act") was enacted in the wake of the attacks of September 11, 2001. The SAFETY Act was created in part because of the extraordinarily large liability entities might face if a malevolent attack occurs despite deployment of anti-terrorism security measures. Congress designed the SAFETY Act as an incentive for the creation and deployment of technologies and services with anti-terrorism capabilities. Standards such as J100 are included among these technologies. Under the SAFETY Act designation, both the entity that creates the anti-terrorism security standard and the entity that deploys the anti-terrorism standard are eligible for certain liability protections.

The American Water Works Association Standards G430 and J100 have been awarded SAFETY Act designation by the DHS. The designation carries important liability protection for the Association and for entities that properly apply these standards.

III. Use of This Standard

It is the responsibility of the user of an AWWA standard to determine that the standard is suitable for use in the particular application being considered.

III.A. *Purchaser Options and Alternatives.* There is no applicable information in this section.

III.B. *Modification to Standard.* No applicable information for this section.

III.C. *Risk Assessment Technical Considerations and Comments.* The fundamental methodology used in J100-10 is clarified but unchanged in J100-21, although many detailed improvements and clarifications have been included. Three aspects of the methodology attracted comments and suggestions. Each is summarized as follows:

III.C.1 Use of point estimates for threat likelihood, vulnerability, and consequences to estimate risk. Risk is defined in this standard (as well as in the NIPP and numerous other sources) as the product of threat likelihood, vulnerability, and consequences, or $R = T \times V \times C$, in chronological order, or $R = C \times V \times T$, the order they are estimated in the J100 process, both equations being the same mathematically. The classic definition of risk is a function of the likelihood of an event and its consequences ($R = Pr(E) \times C$). In security analyses, it has proven useful to break down the overall likelihood into two components (1) likelihood of the event occurring and (2) vulnerability defined as the conditional likelihood of the estimated consequences happening, *given* that the event occurs. For malicious threats, this allows the interpretation of vulnerability as the likelihood of the adversary's success in carrying out the threat. Whereas the likelihood of the event's occurrence is usually beyond the control of an asset owner, vulnerability can often be reduced by security countermeasures and other risk mitigation options, making this formulation a useful way to think about risk and risk reduction. T, V, and C are treated as though they are the means of likelihood distributions and the product C × V × T is used as though it is the mean of the risk distribution. Probability-weighted values are also called the "expected values."

The three variables that make up risk in this formulation are all uncertain, some highly so, yet the standard treats them as single-point estimates rather than as probability distributions that include the estimated uncertainties, as would be prescribed by contemporary risk analysis experts. Such distributions would be combined using Monte Carlo simulation, resulting in a probability distribution of risk, the mean of which is its best single summary descriptor, which might or might not approximate the product of the three variables, depending on the skewness (asymmetry) of the three distributions. This approach is termed below as the "full uncertainty" method because it results in not only the mean risk but a distribution of the uncertainty around that mean. While this more sophisticated method would be preferred by most risk experts, the Committee decided to use the simpler single-point method (and follow the precedents of the NIPP and J100-10) to encourage application of risk management by the majority of potential users, while discouraging even simpler, more flawed approaches (e.g., those using rank orders in processes requiring ratio scales). Users who wish to employ the full uncertainty method would be in compliance with this Standard, provided all other conditions are met. Organizations may start with the single-point approach and, with experience, adopt the full uncertainty method to exploit its enhanced features. Future versions of the standard may consider explicitly recommending the full uncertainty method, at least as an option.

III.C.2 Appropriateness of using R = C × V × T for both natural and malevolent events. The issue is whether risk as a function of potentially interdependent variables Threat (T), Vulnerability (V), and Consequence (C) is a reasonable problem breakdown for analysis of risks posed by both malicious threats and natural hazards. For natural hazards, independence among the three terms can usually be assumed, so the equation Risk = C × V × T applies.

For terrorism and other malevolent events, however, it may be the case that T, V, and C are functionally interdependent. Specifically, malevolent actors choose their targets and attack modes, establishing correlations based on their objectives, capabilities, and biases. One can reasonably assume the malevolent actor prefers greater consequences to lesser and greater vulnerability (i.e., higher likelihood of success) to lesser, so threat likelihood—the likelihood of a specific threat-asset pair being chosen—is correlated with both consequences and vulnerability, possibly with the expected value of the consequences, the product V × C. This standard recognizes this correlation in the way that consequence and vulnerability are used in estimating threat likelihood using the "proxy" estimation method. The likelihood of the malevolent actor selecting a specific threat-asset pair is biased to favor higher (V × C) over lower (V × C), reflecting typical preference curves.

III.C.3 Correlated consequences. The consequence of losing an asset often depends strongly upon the condition of other assets—i.e., the consequences are correlated. This is particularly true for systems like water systems that have continuous flows in core processes. While these processes have been consciously designed to tolerate loss of individual assets without serious loss of function, situations arise where two or more physical assets are integrated by a process flow such that loss of the asset interrupts the whole flow or a major portion of the flow. In such situations, the standard suggests combining these assets into a subsystem and treating the subsystem as a single asset. Combining assets that are correlated because they are parts of a common process into subsystems captures the conditional probabilities without making them intellectually, combinatorially and computationally overwhelming.

III.C.4 Correlated likelihoods. Where an incident (e.g., a hurricane or an earthquake) affecting one asset would be expected to damage nearby or many or all assets at a given location, whether functionally related or not, the same threat likelihood should be assigned to all relevant threat-asset pairs.

IV. Major Revisions. The major changes made to the standard in this revision include the following:

1. Revised the standard's title to J100 Risk and Resilience Management for Water and Wastewater Systems.
2. Clarified and refined the terms in this standard, including realignment of terminology.
3. Added reference to ANSI/AWWA G440, Emergency Preparedness Practices, and ANSI/AWWA G300, Source Water Protection.
4. Updated the descriptions of federal directives that were changed or added since 2010, such as Sec. 2013 of America's Water Infrastructure Act (AWIA) of 2018.
5. Updated the Proxy Method of estimating malevolent threat likelihood.
6. Updated the Utility Resilience Index (URI) and associated language.
7. The asset resilience metric has been integrated into the Combined Utility Loss formula which includes an estimate of service outage.
8. Updated the Reference Threats.
9. Transitioned information previously included in the Appendixes to the new J100 Operational Guide that is under development.

10. Added the use of findings from ANSI/AWWA G300 (Operational Guide to AWWA G300, Source Water Protection) to inform the J100 assessment process.

11. Revised the decision-making process in Step 7.

12. Included cyber threats more explicitly.

V. Comments. If you have any comments or questions about this standard, please contact AWWA Engineering and Technical Services at 303.794.7711, FAX at 303.795.7603, write to the department at 6666 West Quincy Avenue, Denver, CO 80235-3098, or e-mail at standards@awwa.org.

This page intentionally blank.

American Water Works Association

Dedicated to the World's Most Important Resource®

ANSI/AWWA J100-21
(Revision of ANSI/AWWA J100-10[R13])

AWWA Standard

Risk and Resilience Management for Water and Wastewater Systems

SECTION 1: GENERAL

Sec. 1.1 Scope and Purpose

The purpose of this standard is to enable water and wastewater utility owners and operators to make sound decisions when allocating limited resources to reducing risk and improving resilience. This standard sets the requirements for all-hazards risk and resilience analysis and management for the water sector. It provides methodology and resource material that can be used for satisfying these requirements. This standard describes and documents a process for identifying risk as a function of the consequences, vulnerabilities, and likelihood of man-made threats, natural hazards, and dependency and proximity hazards. By following this standard, the Water Sector is enabled to consistently evaluate risk and support reduction in risk and/or improvement in resilience in water and wastewater utilities.

Sec. 1.2 Jurisdiction

This standard is an American National Standard, as designated by the American National Standards Institute, and falls under the jurisdiction of the American Water Works Association (AWWA). This jurisdiction is exercised by the AWWA J100 Risk and Resilience Management Standards Committee. This standard is aligned with the intent of National Homeland Security Policy, including the National Infrastructure Protection Plan (NIPP), National Incident