ANSI/ASME-ITI/AWWA J100-10
(First Edition)

ASME INNOVATIVE TECHNOLOGIES INSTITUTE, LLC

American Water Works Association

Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for

Risk and Resilience Management of Water and Wastewater Systems

Using the ASME-ITI RAMCAP Plus® Methodology

Approved American National Standard

ANSI

Effective date: July 1, 2010.
Approved by ASME-ITI Management Committee January 15, 2010.
Approved by AWWA Board of Directors January 17, 2010.
Approved by American National Standards Institute May 4, 2010.

Disclaimer

Effective date: July 1, 2010

This document is a standard developed jointly by the American Water Works Association (AWWA) and the ASME Innovative Technologies Institute, LLC (ASME-ITI).

This standard will be revised when both of the above organizations approve the issuance of a new edition. There will be no addenda issued to this edition.

ASME-ITI and AWWA accept responsibility for only those interpretations of this document issued in accordance with the established ASME-ITI procedures and policies, which precludes the issuance of interpretations by individuals.

ASME-ITI and AWWA jointly issue written replies to inquiries concerning interpretations of technical aspects of this standard. Interpretations are published on the ASME-ITI and AWWA Web sites.

ASME-ITI is the registered trademark for ASME Innovative Technologies Institute, LLC. AWWA is the registered trademark of the American Water Works Association.

This standard is not a specification. Standards do not contain all of the engineering and administrative information normally contained in specifications.

This standard was developed under procedures accredited as meeting the criteria for American National Standards. The Standards Committee that approved the standard was balanced to ensure that individuals from competent and concerned interests had the opportunity to participate. The proposed standard was made available for public review and comment, with the opportunity for public comment from industry, academia, regulatory agencies, and the public-at-large.

Participation by federal agency representative(s) or person(s) affiliated with industry is not to be interpreted as government or industry endorsement of this standard.

Publication of this standard does not constitute endorsement of any product or product type, nor does AWWA or ASME-ITI "approve," "test," "rate," "certify," "endorse," or otherwise approve any item, construction, proprietary device, process, or activity. The use of this standard is entirely voluntary.

This standard does not supersede or take precedence over or displace the applicable laws, regulations, or codes of any governmental authority. It is intended to represent a consensus of the water sector. "Consensus" does not necessarily mean there is or was unanimous agreement among every person participating in the development of this standard.

When AWWA and ASME-ITI revise or withdraw this standard, an official notice of action will be placed in the classified advertising section of Journal AWWA and, concurrently, on the ASME-ITI Web site. The action becomes effective on the first day of the month following the month of Journal AWWA publication of the official notice.

Neither AWWA nor ASME-ITI takes any position with respect to the validity of any patent rights asserted in connection with any items mentioned in this document. AWWA and ASME-ITI do not undertake to ensure anyone utilizing a standard against liability for infringement of any applicable letters patent, nor do they assume any such liability. Users of a standard are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

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 publication. 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.

For additional information regarding the RAMCAP® process, please contact:

ASME Innovative Technologies Institute, LLC
1828 L Street, NW, Suite 906
Washington, DC 20036
itiinfo@asme.org
(202) 785-7499
www.asme-iti.org

To order additional copies of this document, please contact either ASME-ITI at the above address or:

The American Water Works Association
6666 West Quincy Avenue
Denver, CO 80235
(303) 794-7711 or (800) 926-7337
www.awwa.org

ASME Innovative Technologies Institute, LLC (ASME-ITI) is a not-for-profit Limited Liability Company that is a wholly owned subsidiary of ASME. ASME-ITI provides market-relevant engineering and technology-based products and services to the government, industry, and academic markets. Services provided by ASME-ITI include risk and vulnerability analysis for national and homeland security; program management for government, industry, and academic clients; consortia; and coalition management.

This page intentionally blank.

Contents

This page intentionally blank.

List of Tables

This page intentionally blank.

List of Figures

This page intentionally blank.

Foreword

1 Introduction

This foreword discusses the origin and evolution of Risk Analysis and Management for Critical Asset Protection (RAMCAP®), adaptation of existing tools to be consistent with RAMCAP for the water sector, history and approval dates of the standard, a brief overview of the process, and directions for commenting on or seeking interpretation of the standard.

1.1 Origin

Following the attacks of September 11, 2001, the American Society of Mechanical Engineers (now 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. This support would necessitate a common terminology, common metrics, and consistent methodology—tailored to the technologies, practices, and cultures of the respective industries—to permit direct comparisons within and across industry sectors. Such direct comparisons were seen as essential to supporting rational decision-making in allocating limited private and public resources to reducing risk to critical infrastructures. The critical infrastructures recognized by the US Department of Homeland Security may be found in the National Infrastructure Protection Plan (2009), page 3.

In response to this recommendation, ASME convened a team of distinguished risk analysis experts from industry and academe to develop the Risk Analysis and Management for Critical Asset Protection (RAMCAP). They defined a seven-step methodology that enables 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 terrorist attack. Reductions in risks are the benefits that can be used in estimating net benefits (benefits less costs) and benefit–cost ratios that will allow for the making of informed decisions to allocate resources to specific risk-reduction actions.

1.2 Evolution of RAMCAP

The initial version of RAMCAP was the draft Risk Analysis and Management for Critical Asset Protection: General Guidance (2004), 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 seen as a highly competent and comprehensive synthesis of the best of available methods and appropriate for academic or risk professionals. It was not, however, as useful to the key engineering, security, and operating personnel at the facilities of concern. Consequently, a key design criterion (among others) in order to encourage widespread application was that the methodology be appropriate for self-assessment primarily by on-site staff in a relatively short period of time (typically less than a week of work by a team of 3–6 people, after assembly of the necessary documents). 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 semitechnical 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 RAMCAP documents was designated in the various drafts of the National Infrastructure Protection Plan (NIPP), 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 terrorism only. The 2006 version of the NIPP broadened the definition of the concerns from terrorism only to include natural hazards, which all later RAMCAP documents, including this standard, have incorporated.

In 2003, DHS initiated development of sector-specific guidance for nuclear power plants and spent fuel transportation and storage, petroleum refineries, chemical manufacturing plants, LNG off-loading terminals, dams and locks, and water and wastewater systems. The latter is the origin of the present standard. In 2009, All-Hazards Risk and Resilience: Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach was published, updating RAMCAP Framework 2.0 and providing the basis for a generic, all-sector standard by ASME Codes and Standards. The 2009 publication and the all-sector standard, when available, are the point of comparison for judging consistency with the RAMCAP methodology.

1.3 RAMCAP in the Water Sector

The water sector includes drinking water and wastewater systems. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 required all water utilities serving more than 3,300 people to perform security vulnerability assessments. Three methodologies discussed here were developed and applied. Because the water sector had spent considerable resources and efforts to develop these methodologies, the Water Sector Coordinating Council, official representative of the nation's potable water and wastewater utilities under the National Infrastructure Protection Plan, determined that the preferred approach for their sector was to adapt two of the existing tools (Risk Assessment Methodology—Water (RAM-W™) and Vulnerability Self Assessment Tool™ (VSAT™)—to be consistent with RAMCAP and to adapt the third (Security and Environmental Management System [SEMS™]) to provide certain basic information required by RAMCAP. RAM-W had been developed by Sandia National Laboratories with funding from Awwa Research Foundation (now the Water Research Foundation and support from AWWA) and was renamed Automated Risk Analysis Method—Water and Wastewater (ARAM-W™) when it moved to computerized form. VSAT was developed by Scientech and PA Consulting Group, under sponsorship of the Association of Metropolitan Sewerage Agencies (now the National Association of Clean Water Agencies), originally for use by wastewater utilities and later adapted to drinking water utilities. SEMS was developed by the National Rural Water Association specifically for its small systems. RAMCAP Approach for the Water Sector: Overview (2007) summarizes the RAMCAP process as it applies to water and wastewater utilities.

Modifications have been made to VSAT to be consistent with RAMCAP Framework 2.0 and the Overview. Similar work is progressing for ARAM-W and SEMS. Additional RAMCAP-consistent tools may follow. The Overview and the RAMCAP-consistent tools were 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; (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 report essential risk and benefit information to operators of the utilities, local and state governments, DHS, USEPA, and others with a need to know. The present standard also seeks to advance these goals. It supersedes the Overview and is consistent with the 2009 RAMCAP publication and the all-sectors standard as developed to date.

1.4 History of the Standard

This is the first edition of this standard.

1.5 ANSI Approval Dates

This standard was approved by the American National Standards Institute on May 4, 2010.

2 RAMCAP Overview

RAMCAP is a process for analyzing and managing the risks associated with malevolent attacks and naturally occurring hazards against critical infrastructure. When applied to the water sector, it provides a consistent, efficient, and technically sound methodology to identify, analyze, quantify, and communicate the level of risk and resilience (i.e., the ability to withstand disruption or to quickly return to an acceptable level of service after an interruption) and the benefits of risk reduction and resilience enhancement. It documents a process for identifying security vulnerabilities, consequences, and incident likelihood and provides methods to evaluate the options for reducing these elements of risk.

In a RAMCAP analysis, specific reference threat scenarios, included in this standard, are provided to the user. Use of these threats is essential to establishing comparability. The utility may also want to apply threats other than those provided.

With the consistent baseline parameters used in a RAMCAP analysis, the consequence analysis results are reported in terms of potential fatalities, injuries, and losses to the utility and the community in the event of a successful direct attack or a naturally occurring event (e.g., flood, hurricane, tornado, wildfire, ice storm, and earthquake). Because of the rigor and consistency in estimating risks, resilience, and benefits quantitatively, the results of the evaluation can also be used by the utilities to inform their own planning process. In addition, the results of RAMCAP-consistent analyses are consistent across the water sector and also across all other critical infrastructure sectors. This inherent direct comparability of RAMCAP-consistent analyses, together with the quantification of risks, resilience, and benefits, can provide an actionable foundation upon which to base resource allocation decisions in terms of fatalities, injuries, costs to the utility to recover, economic losses to the community, and speed of recovery from disruptions in service.

The RAMCAP process is composed of seven interrelated analytic steps, as illustrated in Figure 1. These steps provide a foundation for data collection and interpretation, analysis, and decision-making valuable for understanding and managing risk and resilience.

The feedback arrows imply that, given baseline estimates of risk and resilience, all or some of steps 3 through 5 may be repeated or modified for assessing benefits. Reducing risks requires that the options being considered reduce/mitigate at least one of the three elements of risk—consequences, vulnerability, and the likelihood of occurrence. Enhancing resilience requires that the options reduce at least one of the three elements of resilience—service denial, vulnerability, or likelihood. The process estimates the changes attributable to a countermeasure or mitigation option, in which the benefits are defined as the change in risk or resil-

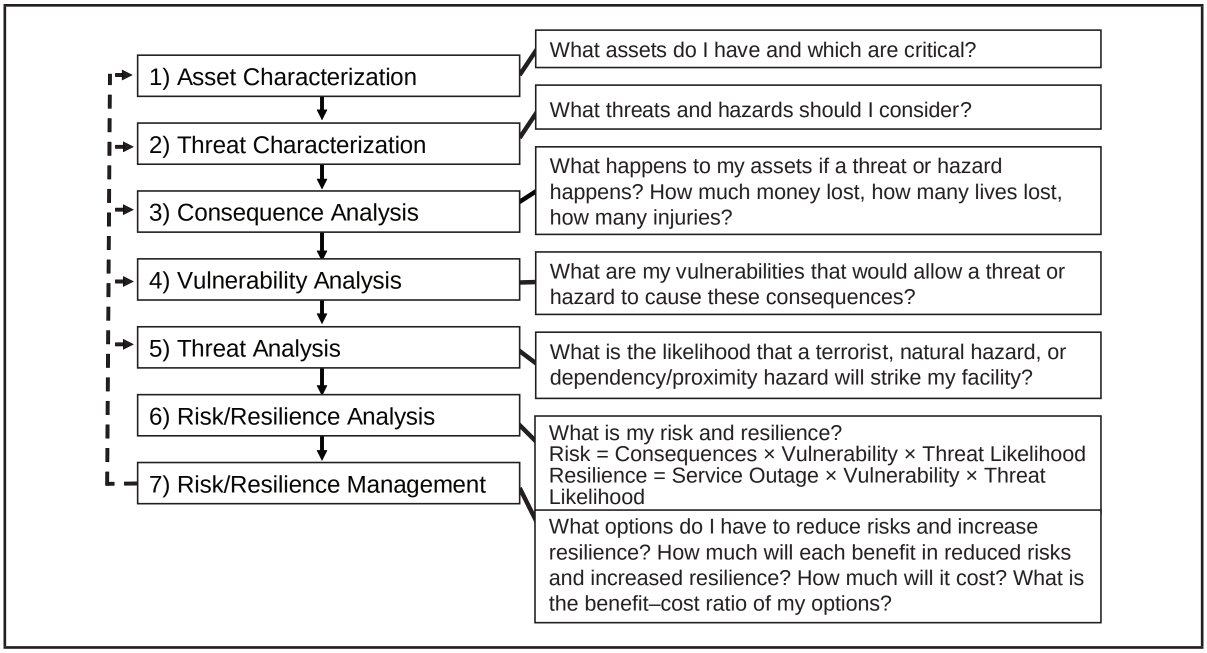

Figure 1 The Seven-Step RAMCAP Process

ience and the costs include the investment and operating costs of the option. This allows calculation of net benefits and a benefit–cost ratio that can be used to rank the options by the total amount of risk reduction and/or resilience enhancement and by the amount per dollar of cost.

3 Organization of This Document

This document contains the body of the standard proper and the appendixes listed below that clarify or assist in applying the standard. The appendixes are all nonmandatory except as noted in the standard. It is encouraged that the analysis of utility-wide resilience defined in Nonmandatory Appendix H be completed in conjunction with the RAMCAP analysis proper.

A. Guidance on the use of this standard
B. Optional use of RAMCAP scales for recording consequence and vulnerability estimates
C. Glossary
D. Expanded bibliography
E. RAMCAP reference threats
F. Proxy indicator of terrorism threat likelihood for the water sector
G. Integrated analysis of natural hazards
H. Water sector utility resilience analysis approach

4 Comments

Suggestions for improvement to this standard or requests for interpretation are welcome. They should be addressed to both ASME Innovative Technologies Institute, LLC, Secretary, RAMCAP Standards Committee, 1828 L Street, NW, Washington, DC 20036, and the American Water Works Association, Security and Preparedness Program Manager, 1300 Eye Street NW, Suite 701W, Washington, DC 20005.

Joint ASME-ITI/AWWA J-100-10 Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for

Risk and Resilience Management of Water and Wastewater Systems

The following is the roster of the Committee at the time of approval of this standard.

STANDARDS COMMITTEE OFFICERS

David Binning, PE, *Chair, AEM Corporation*

Bryon Elwell, PE, *Vice Chair, ABS Consulting Inc.*

Jerry P. Brashear, PhD, *Secretary, ASME Innovative Technologies Institute*

Kevin M. Morley, *AWWA Standards Committee Liaison, American Water Works Association*

STANDARDS COMMITTEE PERSONNEL

Vic Burchfield, Columbus (Ga.) Water Works

Leonard Casson, PhD, PE, University of Pittsburgh

Steve Clark, US Environmental Protection Agency

Steve Gerwin, PE, Howard County (Md.) Public Works

Calvin D. Jaeger, PhD, Sandia National Laboratories

John Laws, US Department of Homeland Security

John W. McLaughlin, PE, Jordan, Jones & Goulding

Daniel C. Rees, Scientech

Nicholas Santillo, Jr., PSP, American Water

Shannon Spence, PE, Malcolm Pirnie

Jean Voelkel, Pima County Regional Wastewater Reclamation Department

This page intentionally blank.

Risk and Resilience Management of Water and Wastewater Systems

1 SCOPE

1.1 This standard sets the requirements for all-hazards risk and resilience analysis and management for the water sector and prescribes methods that can be used for addressing these requirements. The standard documents a process for identifying vulnerabilities to man-made threats, natural hazards, and dependencies and proximity to hazardous sites and provides methods to evaluate the options for improving these weaknesses in water and wastewater utilities. This standard is and will be maintained to be consistent with the current all-sector Risk Analysis and Management for Critical Asset Protection (RAMCAP) standard developed and maintained by ASME Codes and Standards. The current version of the general, all-sector RAMCAP standard is in development by ASME Codes and Standards, based on ASME-ITI (2009). The all-sector RAMCAP standard is general to all sectors of the economy; the present standard is specific to the water sector.

1.2 Jurisdiction. This standard is an American National Standard, so designated by the American National Standards Institute, and falls under the joint jurisdiction of the American Water Works Association (AWWA) and ASME Innovative Technologies Institute, LLC (ASME-ITI). This jurisdiction is exercised by the Joint ASME-ITI/AWWA RAMCAP Standards Committee for Risk and Resilience Management of Water and Wastewater Systems.

2 DEFINITIONS

Below, certain key terms are defined as used in this standard. Where possible, these definitions are aligned with harmonized definitions from the National Infrastructure Protection Plan (NIPP), National Incident Management System (NIMS), and National Response Framework (NRF). A full glossary is provided in Appendix C.

2.1 ***Asset*** is an item of value or importance. In the context of critical water and wastewater infrastructure, an asset is something of importance or value that if targeted, exploited, destroyed, or incapacitated could result in injury, death, economic damage to the owner of the asset or to the community it serves, destruction of property, or could profoundly damage a nation's prestige and confidence. Assets may include physical elements (tangible property), cyber elements (information and communication systems), and human or living elements (critical knowledge and functions of people).