Evolution of Sandia's Risk Assessment Methodology for Water and Wastewater Utilities (RAM-W™)

Calvin D. Jaeger, M. Michael Hightower and Teresa Torres
Sandia National Laboratories
Albuquerque, New Mexico 87185

Abstract
The initial version of RAM-W was issued in November 2001. The Public Health Security and Bioterrorism Preparedness and Response Act was issued in 2002 and in October 2002, version 2 of RAM-W was distributed to the water sector. In August 2007, RAM-W was revised to be compliant with specific RAMCAP requirements. In addition, this version of RAM-W incorporated a number of other changes and improvements to the RAM process. All of these RAM-W versions were manual, paper-based methods which allowed an analyst to estimate security risk for their specific utility. In September 2008, an automated RAM prototype tool was developed which provided the basic RAM framework for critical infrastructures. In 2009, water sector stakeholders identified a need to automate RAM-W and this development effort was started in January 2009. This presentation will discuss the evolution of the RAM-W approach, capabilities and the new automated RAM-W tool (ARAM-W which will be available in mid-2010).

Background
Violence, vandalism, and terrorism are prevalent in the world today. Managers and decision-makers must have a reliable way of estimating risk to help them decide how much security is needed at their facility. Sandia National Laboratories (Sandia) has developed a series of Risk Assessment Methodologies (RAMs) for different critical infrastructures (CI) to assess vulnerabilities and risks at various types of facilities and CI systems. The Sandia RAM approach is based on the traditional risk equation:

$$\text{Risk} = P_A * (1 - P_E) * C,$$

R	=	risk associated with the adversary attack
P_A	=	is the likelihood of adversary attack,
P_E	=	is security system effectiveness,
$1 - P_E$	=	is adversary success, and
C	=	is consequence of loss of the asset.

The RAM process begins with planning for a Risk Assessment (RA) (including understanding the utility's mission) followed by characterization of the facility which includes identification of the undesired events and the respective critical assets. Guidance for defining threats is included, as well as for using the definition of the threat to estimate the likelihood of adversary attack at a specific facility. Relative values of consequence are estimated and used to prioritize undesired events and impacts on assets. Analytical methods are also included for estimating the effectiveness of the security system against the adversary attack. Finally, risk is calculated. In the event that

the value of risk is deemed to be unacceptable (too high), the methodology addresses a process for identifying and evaluating security system upgrades and mitigation strategies in order to reduce risk.

The Risk Assessment Methodologies developed for Water and Wastewater Utilities provide a systematic, risk-based approach to evaluate water and wastewater utilities from a range of threats that could cause an undesired event. The different RAM-W methodologies provide the user the ability to determine a relative risk based on the threat, consequences and protection system effectiveness/vulnerability and help answer the basic question "How much protection do I need, and how much is enough?" Figure 1 provides a simple representation of how RAM-W addresses this question. The basic RAM framework for water and waste water systems has generally remained constant since it was introduced in 2001, with some minor changes and enhancements for the different process steps. The current RAM-W process steps include: top-level screen; plan for the risk assessment; characterize the utility, facilities and assets; define the threat; identify undesired events and consequences; define the protection objectives; evaluate protection system effectiveness; determine risk; and propose and evaluate upgrades if risk is not acceptable and report on the assessment results. The following sections will briefly discuss some of the RAM-W upgrades, improved approaches, and associated capabilities.

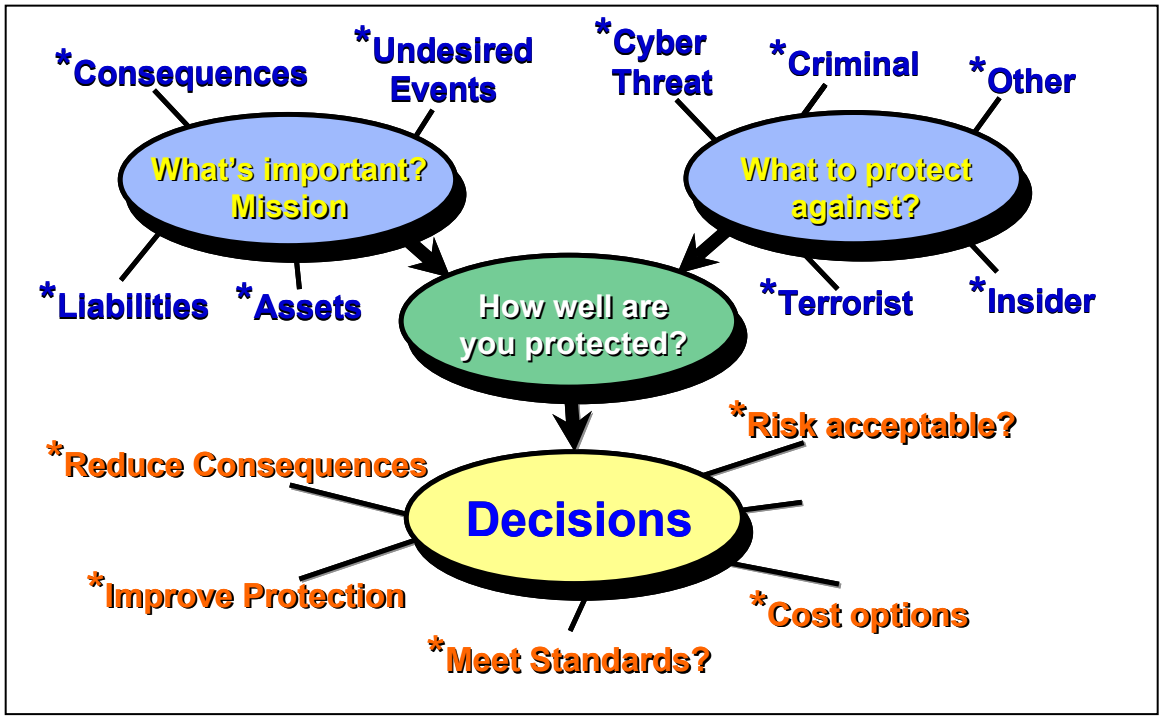

Figure 1 How much protection is enough

Risk Assessment Methodology for Water Utilities (RAM-W^{TM})
In partnership with the American Water Works Association Research Foundation (AwwaRF) and Sandia National Laboratories, the Environmental Protection Agency (EPA) undertook a program in 2000 to improve security at water utilities across the

United States. Version 1 of RAM-W^{TM} was issued in November 2001 and was designed to assist large water utilities and security professionals in assessing the risks from malevolent threats. Version 2 RAM-W^{TM} was issued in October 2002. Through a systematic, thorough evaluation of the water utility operations, a prioritized plan for consequence mitigation, security upgrades, modifications to operational procedures, and/or policy changes can be developed to mitigate identified risks. The goal of RAM-W^{TM} was to provide a plan for balanced risk reduction measures by appropriately applying valuable and limited water utility resources to the most important needs.

In 2003, in partnership with AwwaRF, a streamlined version of RAM-W^{TM} along with case studies for hypothetical utilities to demonstrate the application of RAM principles and concepts were developed to provide guidance for small and medium water utilities. This methodology is a condensed version of RAM-W^{TM} and was designed to be less computationally intensive relative to the methodology used for the large water utilities. The streamlined version of RAM-W^{TM} was intended to assist those responsible for conducting an assessment at small and medium water utilities in understanding and applying security concepts appropriately.

The process flow diagram for RAM-W^{TM} is shown in Figure 2.

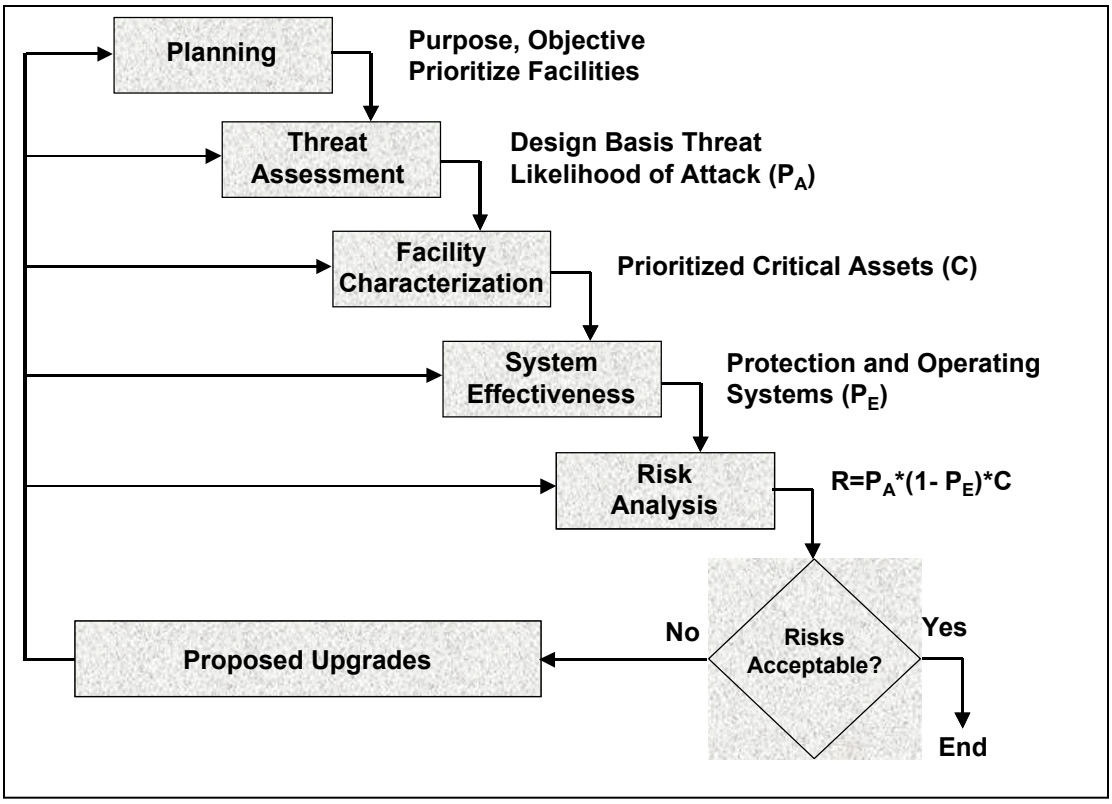

Figure 2 RAM-W waterfall flow diagram

Some of the features of RAM-W™ are:

- Pair-wise comparison for screening a utility's facilities and prioritizing based on missions
- Generic undesired event fault tree for a water supply system
- Adversary path analysis for estimating protection system effectiveness/vulnerability
- Cyber threat and SCADA risk analysis
- Worked example of a water utility to demonstrate the methodology
- Questionnaires to support various process steps
- Input from recommendations from assessment teams and water utilities and associations.

RAMCAP Compliant Risk Assessment Methodology for Water Utilities (RC RAM-W™)

In support of the Department of Homeland Security (DHS), the Risk Analysis and Management for Critical Asset Protection (RAMCAP™) process was created by the American Society of Mechanical Engineers-Innovative Technologies Institute, LLC (ASME-ITI) and documented in *RAMCAP The Framework*©. As a result of this initiative by DHS and ASME, a decision was made by DHS to take existing risk assessment tools that have been or are currently being used within the water sector, including RAM-W™ and make them RAMCAP compliant (RC).

In 2007, Sandia worked with ASME-ITI to develop a RAMCAP compliant RAM-W™ approach. The RC RAM-W™ incorporates lessons learned updates to the RAM-W™ version 2 methodology in addition to revisions to make it compliant with both RAMCAP and the baseline criteria identified in Appendix 3A of the National Infrastructure Protection Plan (NIPP), *NIPP Baseline Criteria for Assessment Methodologies*. The RC RAM-W™ follows both the *RAMCAP The Framework*, 7-step process and the Sandia RAM process. Figure 3 shows the RAMCAP process and Figure 4 the RC RAM-W™ process. The colors indicate the relative correlation and similarity between the two approaches. The RAMCAP content is very similar to that found in RAM-W™, with some of the primary differences being the addition of the RAMCAP-specific threat, consequence, vulnerability, and risk tables. The RC RAM-W™ primarily focuses on the evaluation of the physical protection systems (PPSs) against the malevolent threat, but also includes discussions relevant to non-malevolent threats. Some of the newer features of RC RAM-W™ are:

- Uses RAMCAP threat spectrums and tables for consequence, vulnerability and risk
- High level discussion of the cyber/Supervisory Control and Data Acquisition (SCADA)/process control system security
- High-level consideration of natural (earthquake, tornado, hurricane and flood) and non-malevolent threats is included in the methodology
- Consistent with RAMCAP and NIPP definitions

- The methodology uses fault trees but references those in RAM-W™ version 2 (omission of the fault trees was intended to keep the document unclassified)

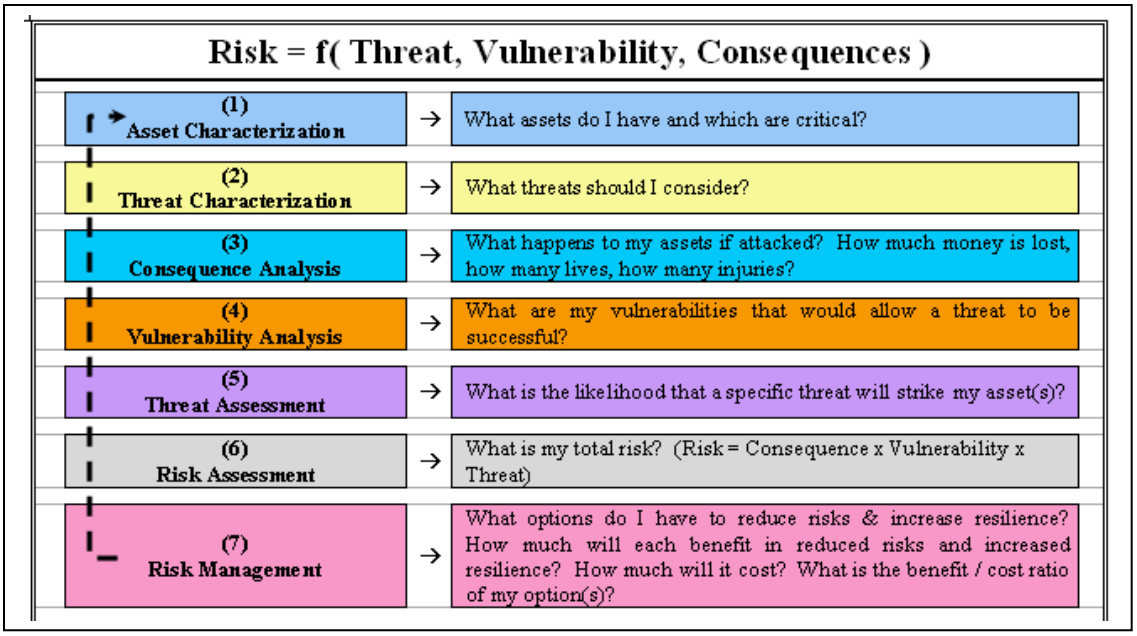

Figure 3 RAMCAP 7-step process

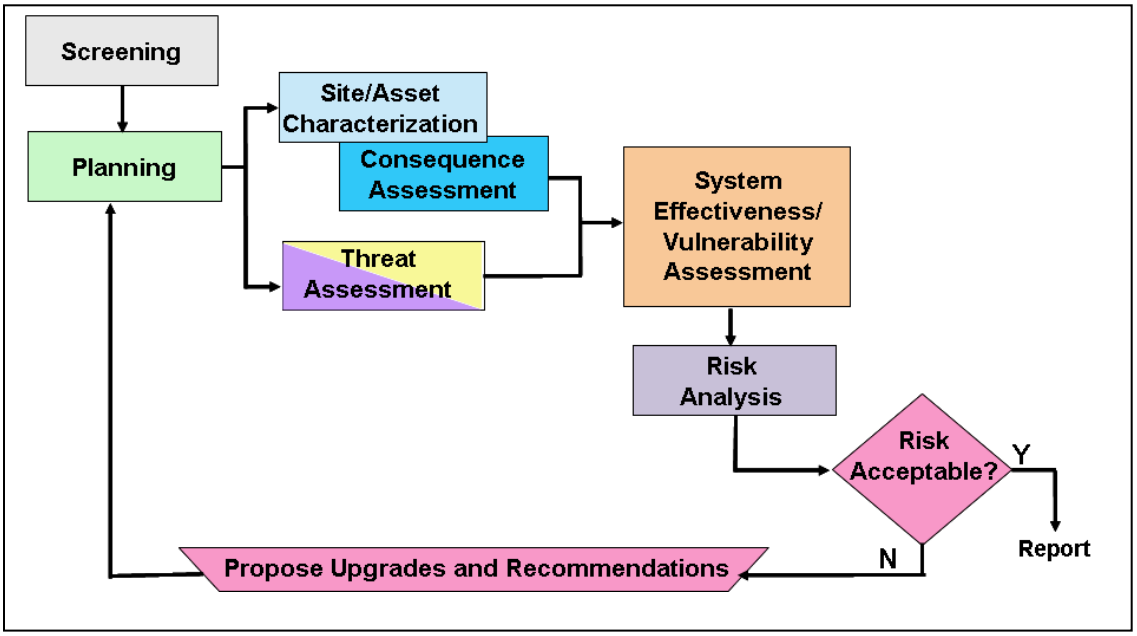

Figure 4 RC RAM-W™ process flow diagram

Automated Risk Assessment Methodology for Water and Wastewater Utilities (ARAM-W™)

The Automated Risk Assessment Methodology for Water and Wastewater Utilities, ARAM-W™, is an automated, systematic, risk-based approach used to evaluate water and wastewater utilities from a range of threats that could cause an undesired event. It leverages the previous RAM-W efforts as well as RAM activities in other CI areas and other Sandia risk/vulnerability assessment software tools. ARAM-W™ determines a relative risk based on threat, consequences and protection system effectiveness. It is a stand alone PC-based tool and can use input from other tools/sources (consequence, blast effects tools, and other data sources). The tool follows the basic RAM process and all the process modules are linked. Figure 5 shows the ARAM-W™ process.

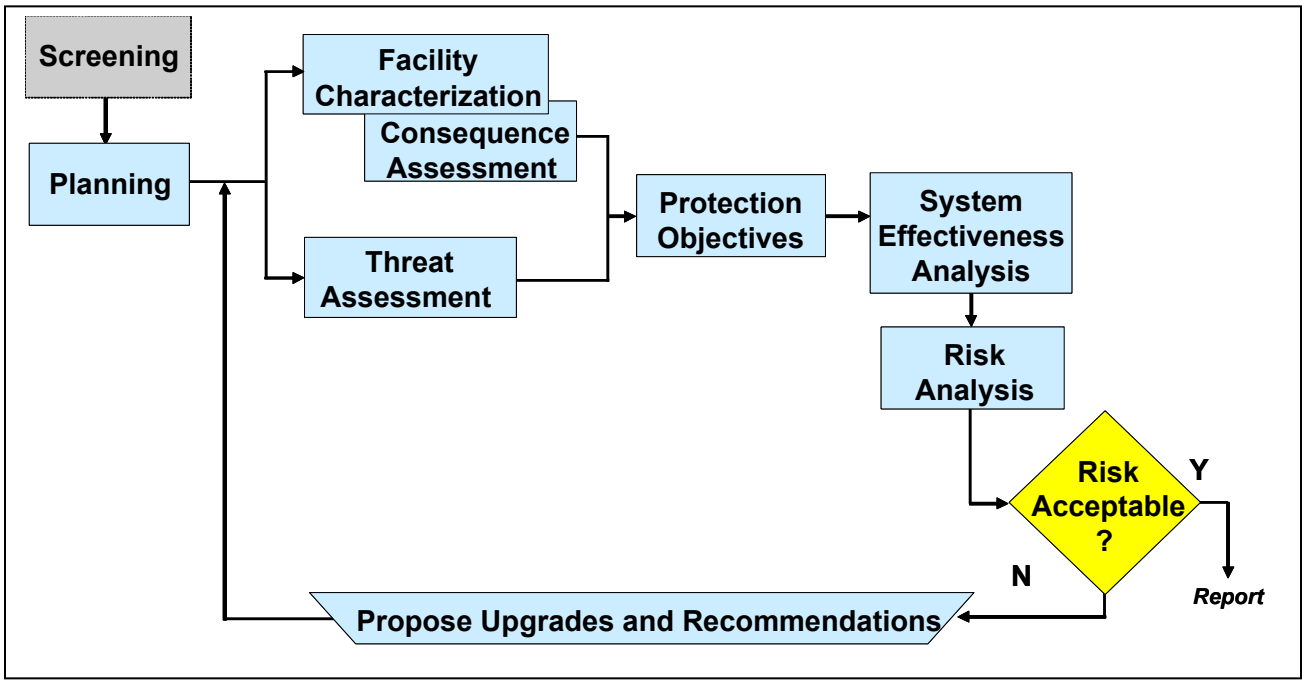

Figure 5 ARAM-W™ process flow diagram

Some of the features of ARAM-W™ are:

- Ability to electronically transfer selected information
- Integrated help capability and user's manual
- Pair-wise comparison
- Generic fault trees for water supply and wastewater utilities; ability to customize for utility; undesired events from fault trees and associate assets and locations
- High level consideration of natural threats, malevolent threats including RAMCAP threats
- For malevolent outsider threats user creates an adversary sequence diagram (security layers and safeguards path elements between layers, inputs attributes for protection elements), Software estimates probability of interruption for worst case,

- User can estimate response/effectiveness of response forces (probability of neutralization),
- Software estimates probability of system effectiveness,
- User identifies vulnerabilities
- Software estimates risk
- Electronic reports generated

Summary

The risked based RAM-W tools developed by Sandia for water and waste water utilities have continued to evolve and improve since they were first introduced in 2001. The more significant recent improvements include: minor changes to make the RAM-W approaches compatible and compliant with DHS RAMCAP guidance, inclusion of non-malevolent threats, and automation of the risk assessment process to speed up evaluations and reviews. In doing this, Sandia has used experience gained from the development of other critical infrastructure risk analysis and vulnerability/risk-based tools to provide water utilities a proven risk-based approach to aid them in making cost-effective security decisions that is based on a rigorous systematic process while being more user friendly.

Acknowledgments

During the development of the various RAM-W tools there were many important contributors. They included the water utilities, water associations, government organizations (e.g., DHS, EPA) and users of the various RAM-W tools.