Review and Evaluation of the J100-10 Risk and Resilience Management Standard for Water and Wastewater Systems

Thomas Ying-Jeh Chen,[1*] Valerie Nicole Washington,[1] Terje Aven,[2] and Seth David Guikema[1]

[1] University of Michigan, Ann Arbor, MI, USA.

[2] University of Stavanger, N-4036 Stavanger, Norway.

*Address correspondence to Thomas Ying-Jeh Chen, Department of Industrial and Operations Engineering, University of Michigan, 1205 Beal Avenue, Ann Arbor, MI 48109, USA.

Abstract

Risk analysis standards are often employed to protect critical infrastructures, which are vital to a nation's security, economy, and safety of its citizens. We present an analysis framework for evaluating such standards and apply it to the J100-10 risk analysis standard for water and wastewater systems. In doing so, we identify gaps between practices recommended in the standard and the state of the art. While individual processes found within infrastructure risk analysis standards have been evaluated in the past, we present a foundational review and focus specifically on water systems. By highlighting both the conceptual shortcomings and practical limitations, we aim to prioritize the

This is the author manuscript accepted for publication and has undergone full peer review but has not been through the copyediting, typesetting, pagination and proofreading process, which may lead to differences between this version and the Version of Record. Please cite this article as doi: 10.1111/risa.13421.

shortcomings needing to be addressed. Key findings from this study include 1) risk definitions fail to address notions of uncertainty, 2) the sole use of "worst reasonable case" assumptions can lead to mischaracterizations of risk, 3) analysis of risk and resilience at the threat-asset resolution ignores dependencies within the system, and 4) stakeholder values need to be assessed when balancing the tradeoffs between risk reduction and resilience enhancement.

Keywords: Drinking Water System, Asset Management, Risk Management Standard

1. INTRODUCTION

1.1. Background

Following the attacks of September 11, 2001, the federal government recognized the need to define and prioritize the requirements for protecting the nation's infrastructure (AWWA, 2010). As a result, the Homeland Security Act of 2002 (Congress, 2002) prescribed a cross-sector risk assessment plan to identify vulnerabilities for all critical infrastructure and key resources (CIKR) and define a framework to prioritize defense resource allocation. As defined in the National Infrastructure Protection Plan (NIPP) of 2009 (DHS, 2009), CIKRs include energy, water (drinking and waste), transportation, communications, and government facilities.

The potential importance of a uniform risk analysis procedure was recognized when the White House recruited the American Society of Mechanical Engineers (ASME) to develop a procedure applicable across different types of infrastructure (AWWA, 2010). The goal was that common terminology, metrics, and methodology would facilitate comparisons within and across CIKR sectors, and support decision making for risk reduction investments. In 2006, ASME released the specifications for Risk Analysis and Management for Critical Asset Protection (RAMCAP^{TM}),

which serves as the basis for J100-10 (AWWA, 2010). RAMCAP™ defines a seven-step process (discussed in Section 1.2) to assess risk and resilience for a given asset and to prioritize countermeasures.

RAMCAP™ outlines three major objectives (ASME-ITI LLC, 2005): 1) to define a common framework for owners and operators of critical infrastructure to assess consequences and vulnerabilities relating to terrorist attacks on their assets and systems, 2) to provide guidance on methods that can be used to assess and evaluate risk through this framework, and 3) to provide an efficient and consistent mechanism to report risk information to the U.S. Department of Homeland Security (DHS).

The American Water Works Association (AWWA) adopted the RAMCAP™ seven-step framework to create a water and wastewater sector specific risk analysis standard, and in 2010 published the J100-10 standard for Risk and Resilience Management of Water and Wastewater Systems (AWWA, 2010). While RAMCAP™ and J100-10 were initially developed with the intent of analyzing risks associated with terrorist attacks (ASME-ITI LLC, 2005), subsequent updates expanded the analysis breadth to include a variety of threats (e.g. natural hazards, dependency, and proximity threats). Beyond allowing utility operators to systematically assess risk, J100-10 provides methods to evaluate options for improving weaknesses in water and wastewater systems (AWWA, 2010). The aim is to prioritize the actions that better mitigate risks and can lead to more resilient critical infrastructure.

We use the term risk analysis in this paper as it is defined in the Society of Risk Analysis (SRA) glossary (Society of Risk Analysis (SRA), 2015). Risk analysis is "a systematic process to comprehend the nature of risk and to express risk with the available knowledge". A fundamental principles document from SRA highlights some key criteria for a high quality risk analysis (Society of Risk Analysis (SRA), 2018): it needs to be reliable, valid, and the decision maker needs to have

confidence in the results. Reliable means that there is reproducibility in the process (encompassing analyst, methods, procedures etc.), and valid meaning there is success at characterizing the relevant risks. A key is that the degree of knowledge (or lack thereof) of the analyst is properly communicated to the decision maker. The ultimate goal is to inform and support decision making for risk management.

In this paper, we provide an analysis framework for assessing risk analysis standards and present a holistic review of J100-10 to highlight its conceptual shortcomings and practical limitations. Our goal in this paper is to begin a conversation about how to strengthen the J100-10 moving forward.

1.2. J100-10 Definitions

Two key components of a risk management standard are the definitions and the underlying conceptualizations of risk. Before proceeding further with our assessment, we include key definitions from J100-10 (AWWA, 2010), which were adopted from RAMCAP™. The following definitions are taken verbatim from the standard, and a discussion on their sufficiency is presented in later sections. For ease of reading, we have eliminated block quotations.

Risk is "the potential for loss or harm due to the likelihood of an unwanted event and its adverse consequences" (page 18, J100-10 manual (AWWA, 2010)). J100-10 uses the RAMCAP™ approach to quantify risk using Equation (1) below (AWWA, 2010):

$$Risk = Threat\ Likelihood \times Consequence \times Vulnerability \quad (1)$$

Threat likelihood is "the probability that an undesired event will occur" (page 49, J100-10 manual (AWWA, 2010)). With natural hazards, J100-10 states that this should be "the historical frequency of similar events, unless there is a belief that the future will differ from the past. With

malevolent threats, the likelihood is a function of available intelligence, the objectives and capabilities of the adversary, and the attractiveness as a target" (page 49, J100-10 manual (AWWA, 2010)).

Consequence is defined as "the immediate, short- and long-term effects of a malevolent attack or natural incident" (page 43, J100-10 manual (AWWA, 2010)), which J100-10 specifies should be estimated exclusively on a "worst reasonable case basis" (page 8, J100-10 manual (AWWA, 2010)). These effects include fatalities, injuries, and losses suffered by the owner of the asset and by the community served by that asset.

Vulnerability is "an inherent state of the system (e.g. physical, technical, organizational, cultural) that can be exploited by an adversary or impacted by a natural hazard to cause harm or damage" (page 49, J100-10 manual (AWWA, 2010)). J100-10 specifies that vulnerability should be expressed as the likelihood of an event resulting in the estimated consequences, given that the event occurs.

Resilience is "the ability of an asset or system to withstand an attack or natural hazard without interruption of performing the asset or system's function or, if the function is interrupted, to restore the function rapidly" (page 19, J100-10 manual (AWWA, 2010)). Resilience can be considered at the threat-asset level or at the system level. Asset-level resilience is defined on a scale such that lower values indicate greater resilience. It can be calculated using the following three metrics:

1. *Operational Resilience Metric (ORM)* measures the service denial due to a threat-asset pair, weighted by vulnerability and threat likelihood. It is calculated as (AWWA, 2010):

$$ORM = Duration \times Severity \times Vulnerability \times Threat\ Likelihood \quad (2)$$

where duration is the time, in days, of service denial and severity is the amount of service denied (in gallons of water per day).

2. *Owner's Economic Resilience Metric (OERM)* converts ORM into a dollar value and characterizes the financial loss to the utility owner, and is calculated as (AWWA, 2010):

$$OERM = ORM \times Preincident\ Unit\ Price \quad (3)$$

3. *Community Economic Resilience Metric* is the lost economic activity, in dollars, to the community served by the utility. Estimating these impacts requires a regional simulator and/or economic model to fully capture the direct and indirect effects.

1.3. J100-10 Risk Analysis Process

J100-10 outlines a seven-step risk analysis process, as shown in Fig. 1 below.

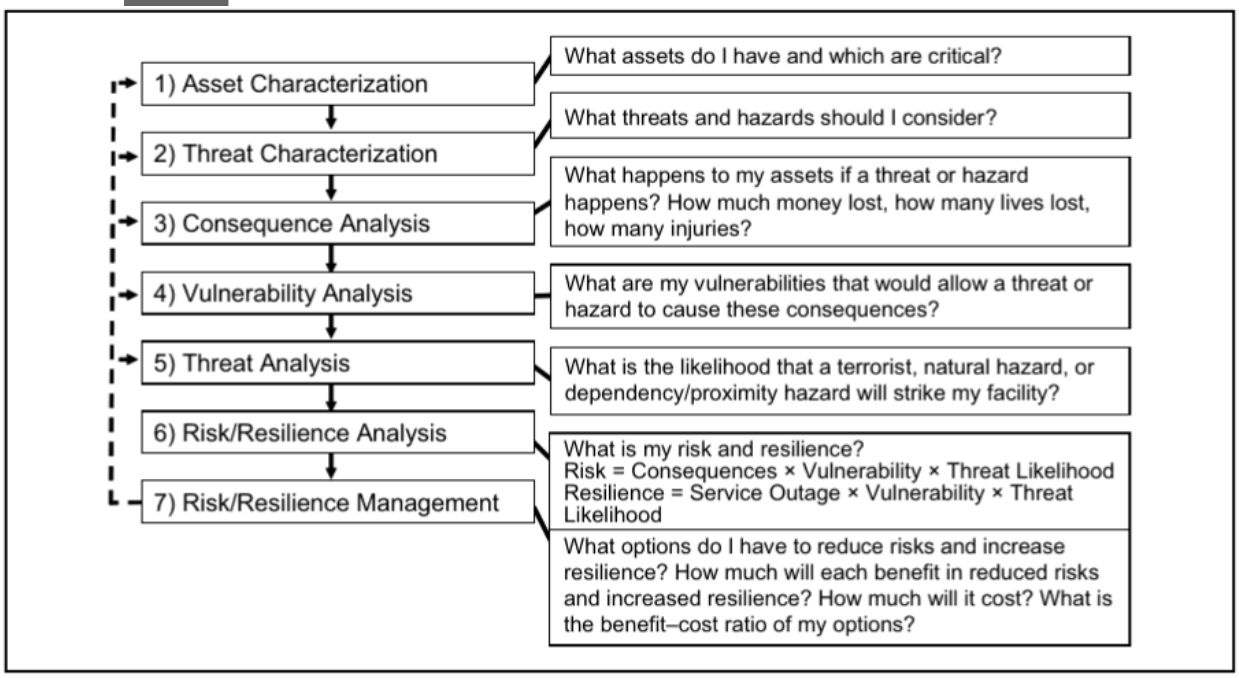

Figure 1. The adopted RAMCAP™ process in the J100-10. Taken from the J100-10 Risk Management Standard (AWWA, 2010).

Below we provide a brief description of each of the seven steps of the assessment methodology.

1) *Asset Characterization*: Identify the critical assets, which, if compromised, would inhibit the organization from carrying out its mission or operational goals. Asset ranking can be used to prioritize components for analysis if the number is too large to include them all.

2) *Threat Characterization*: Identify and describe reference threats scenarios to estimate vulnerability and consequence. Reference categories include malevolent threats, natural hazards, and proximity and dependency threats. Additional threats can be added as long as they are used in the analysis of all assets under consideration.

3) *Consequence Analysis*: Identify and estimate the "worst reasonable consequence" generated by each threat-asset combination. Consequence metric categories include fatality count, serious injury count, financial loss to the owners, and economic losses to the community.

4) *Vulnerability Analysis*: Estimate the conditional likelihood that, given an adverse event occurs on the asset, the estimated consequences will occur. Some methods for estimating this value suggested by J100-10 include direct expert elicitation, path analysis, vulnerability logic diagrams, event trees, or a hybrid of these methods.

5) *Threat Assessment*: Estimate the probability that each of the identified threats will occur in a given time frame (typically one year). J100-10 provides guidance on how to estimate these values for different types of threats, e.g., an event tree based approach for malevolent threats, or using federal agency-specific resources for various natural hazards (e.g., the Federal Emergency Management Agency (FEMA) flood insurance rate maps, or the National Hurricane Center risk analysis program, HURISK).

6) *Risk and Resilience Assessment*: Use Equation (1) to calculate the risk metric and Equations (2-3) to calculate the resilience metrics for each threat-asset pair. Resilience can also be

considered at the system level. J100-10 outlines a utility resilience index (URI), which assesses the operational and financial capabilities of the utility to cope with various incidents that have the potential to disrupt service.

7) *Risk and Resilience Management*: Implement actions to achieve a level of acceptable risk and resilience at an acceptable cost. Benefit-cost analysis is useful for suggesting potential actions, e.g. new security countermeasures or consequence mitigation features. Benefits are calculated as the expected risk reduction or resilience increase and costs are defined in dollar units.

2. LITERATURE REVIEW

2.1. Standardized Risk Analysis Methods in the Water Sector

By one estimate, there are more than 250 critical infrastructure risk analysis methods (Lewis, Darken, Mackin, & Dudenhoeffer, 2012). Many of these methods have been used in other risk analysis standards to study water infrastructure prior to the development of RAMCAP™ or J100-10. Three of these prior standards in particular have been widely documented and used (AWWA, 2010). They are 1) the Risk Assessment Methodology – Water (RAM − W™) (Jaeger, Hightower, & Torres, 2010) developed by Sandia National Laboratories, 2) the Scientech and PA Consulting Group Vulnerability Self-Assessment Tool (VSAT™) (PA Government Services & Scientech Inc., 2002), and 3) the National Rural Water Association Security and Environmental Management System (SEMS™) (NRWA, 2002). RAM − W™ was specifically developed to evaluate the risk of adversarial threats. It is a water sector-specific version of the RAMCAP™ standard (see Section 1.3 for general seven-step approach) that focuses on risk quantification, while J100-10 analyzes both risk and resilience. VSAT™ was originally intended for use by wastewater utilities, but was later adapted

to include drinking water utilities. It uses a risk matrix, estimated as a combination of qualitative criticality and vulnerability ratings, to determine which assets need security improvements (Amass, 2006). SEMS™ was developed for small systems in rural areas. It uses a simple "yes" or "no" questionnaire to help owners of utilities identify vulnerabilities and improvement actions. While it does not describe any explicit quantification of risk, SEMS™ provides information about the operating conditions and asset status of the utility.

Following the release of RAMCAP™, VSAT™ and RAM − W™ have been modified to be consistent with the RAMCAP™ seven-step framework. SEMS™ has been adapted to include questions that cover basic information required by RAMCAP™ (AWWA, 2010), such as certain security measures. Despite the wide variety of available assessment frameworks, we chose to evaluate J100-10 because it was the first standard to include both a wide range of risk sources and all types of water infrastructure in its analysis.

2.2. J100-10 and RAMCAP™ Critiques

In this section, we review some of the previous critiques and contextualize them within our broader review of J100-10. Presented critiques of J100-10 have broader implications for the parent RAMCAP™ standard. Because RAMCAP™ serves as the foundation of J100-10, we include critiques of this standard as well.

While the J100-10 and RAMCAP™ standards do not mandate that utilities report risk assessment results or implement countermeasures, some utilities have documented the use of the approach to guide decision making to improve facility security. A cross-infrastructure sector implementation is found in Krimgold (2012) (Krimgold, 2012), where the RAMCAP™ methodology is implemented to analyze power, water, transport, and communications systems in an unnamed metropolitan region. This is done to better identify specific threats and their respective consequences across sectors. The study concludes that the RAMCAP™ asset-level assessment provides useful

guidance on defining risk through operational units, which assists in the prioritization of short- and long-term risk management goals.

Herrare et al. (2017) (Herrera, Flannery, & Krimmer, 2017) examine an implementation of RAMCAP™ to Colorado's transportation sector, which helped identify system vulnerabilities and assisted in supporting federal emergency response funding requests. The Department of Transportation favored the benefit-cost analysis within the risk and resilience management step used to evaluate multiple mitigation options since it provided a data-driven approach to support decision making.

An implementation specific to the water sector is found in Kerr et al. (2015) (Kerr, Singh, & Motala, 2015), which provides a case study from a utility in Peel, CA. In this study, the utility uses the J100-10 assessment method to develop a long-term strategy to manage and reduce risk through capital investment and operational planning. The authors find that using the J100-10 analysis framework gives the utility a more complete and unbiased understanding of the assets that are at highest risk, which allows for a clearer process for capital investment decision making. In addition, the risk and resilience management guidelines provide a framework for the continual review and revision of the analysis as mitigation plans are implemented.

A number of academic studies have critiqued the risk assessment methodology outlined in the RAMCAP™ standard. High-level critiques include Cox (2008) (Cox, 2008a), which emphasizes the shortcomings of the threat-vulnerability-consequence triplet definition of risk as well as the ordinal scales used in the RAMCAP™ risk calculation. Some of the main limitations discussed by Cox (2008) (Cox, 2008a) are that RAMCAP™ fails to address possible correlations between the threat, vulnerability, and consequence components. Additionally, it does not account for non-additivity of risk when aggregating from the analysis level of threat-asset pairs to system-level risk estimates, the use of ordinal scoring values to calculate risk can lead to sub-optimal allocation of resources for

implementing countermeasures, and notions of uncertainty related to the estimates of threats and consequences are not addressed in the analysis.

Burkhart (2015) (Burkhart, 2015) identifies consistency and scope problems in the J100-10 standard; for example, the utility is given the choice to analyze the resilience at either the asset or system level, but no guidance is provided on how to choose between the two resolutions. Furthermore, no concrete process is outlined for defining a single level of acceptable risk, especially if multiple decision makers are involved. As a more general critique of assessments using risk-based scoring methods for resource allocation, Cox (2009) (Cox, 2009) specifies that such an approach often fails to account for interdependencies and risk externalities (risk for parts of a system changes as countermeasures are added) among the considered threats.

Critiques of specific steps within the J100-10 process have been discussed in the academic literature. Cox (2008) (Cox, 2008b) highlights the limitations of using risk matrices to drive prioritization decisions. Such use of risk matrix methods from RAMCAP™ can be found in the asset characterization step, which is used to screen assets for analysis to reduce the scope of the risk assessment. The study argues that risk matrices often have poor risk resolution and errors in risk estimation, which can lead to suboptimal prioritization decisions.

Consequence estimation, as defined in the J100-10 and RAMCAP™ standards, are based solely on a "worst reasonable case" (AWWA, 2010) premise, the common thinking being that this results in a conservative (inflated) estimate of risk intended to add a factor of safety. A case study in off-sea oil drilling presented by Huage et al. (2014) (Hauge et al., 2014) highlights the limitations of this approach. The authors explain that uncertainties related to characterizing extreme outcomes and their likelihoods can limit the usefulness of an assessment.

The threat analysis step in the RAMCAP™ methodology defines 41 reference threats, which include terrorist threats, natural hazards, and dependency hazards. The J100-10 standard uses the

same 41 reference threats and provides details for analyzing risk from these threats. However, White et al. (2016) (White, George, Boult, & Chow, 2016) recognize the failure of this process to account for key emerging threats (climate change, aging infrastructure, and cyber attacks) and propose 13 additional reference threats to address these emerging issues. As a follow up study, White et al. (2016) (White, Burkhart, Boult, & Chow, 2016) use a simulated RAMCAP™ model to analyze the performance under the proposed set of 54 threats.

The risk and resilience analysis step defines risk as the product of the consequence, vulnerability, and threat likelihood, which make up the triplet definition of risk. The shortcomings of this approach are well established in the risk science literature, where the main concern is that the potential for extreme outcomes is not properly reflected. Alternative and more general perspectives have been developed where risk captures the triplet events, consequences, and uncertainties, see SRA (2015) (Society of Risk Analysis (SRA), 2015) and Aven 2012 (Terje Aven, 2012), 2017 (Terje Aven, 2017b). These perspectives build on Kaplan and Garrick (1981) (Kaplan & Garrick, 1981) who refer to risk qualitatively as 'uncertainty plus damage'.

As shown above, there have been multiple case studies reported on the implementation of the J100-10 standard in the water and wastewater sector and of RAMCAP™ in other infrastructure systems. There are also a number of studies by risk analysts highlighting the limitations of RAMCAP™ and the methodologies it recommends for analyzing risk and resilience. These critiques have focused on specific issues within certain steps of the analysis. In the subsequent sections we will present a more comprehensive critique of the J100-10 assessment process as a whole.

3. ANALYSIS FRAMEWORK

Here we define our framework for evaluating the J100-10 standard. The approach can be implemented for a variety of risk analysis standards outside the water infrastructure domain. Based on the criteria for a risk analysis outlined in Section 1.1, we identify two questions of emphasis: 1) are risk and other key concepts (e.g. probability and resilience) being characterized adequately?, and 2) are the recommended procedures in line with the state-of-the-art in risk science? The point here is to determine whether the assessment process will lead to a proper characterizations of risk that adequately supports decision making. If fundamental concepts are not appropriately conceptualized, the subsequent analysis will not reveal key issues. Similarly, if state-of-the-art methods are not adopted, poor risk characterizations could impact communication and ultimately misguide the decision maker.

As a result, in this research we conceptually compare J100-10 against the state of the art in risk science. We choose this approach because it focuses on the foundational issues of the risk analysis field and measures the process against these established principles. An alternative approach is to implement both J100-10 and a second risk analysis method and compare their outputs. This can be tricky because various assessments are beset by tradeoffs of completeness, consistency, and timeliness (White, Burkhart, et al., 2016). The development of a process to directly compare multiple frameworks is beyond the scope of our analysis and is left for future research.

Our analytical framework can be divided into two categories: conceptual and practical limitations. The former addresses the theoretical shortcomings. The latter addresses specific steps which could lead to poor risk characterizations. We primarily focus on the risk analysis portion of J100-10, but also discuss its guidelines for assessing resilience. We present our findings of the conceptual and practical limitations in Sections 4 and 5, respectively.

4. CONCEPTUAL LIMITAIONS

In the following section, we identify conceptual gaps related to definitions of key terms, how they are calculated and interpreted in the standard, and how they relate to the state of the art in the field of risk analysis.

4.1. Definitions of Risk

The operating risk definition in the J100-10 standard falls short because concept of uncertainty is not included. J100-10 uses the expected consequences definition of risk, which is calculated as the product of the probability of a threat event, the conditional probability that the event will lead to the worst-case consequences, and the consequences themselves (see Equation 1). As discussed in Section 2.2, this understanding of risk has severe limitations and its use can seriously mislead decision makers.

An analysis of the literature shows that there are multiple definitions of risk: some are broader, while others lead more naturally to quantifiable equations. By distinguishing between the concept of risk and how it is measured, a consensus can be reached on characteristics of risk, as shown by the Society for Risk Analysis Glossary (2015) (Society of Risk Analysis (SRA), 2015). Aven (2012) (Terje Aven, 2012) discusses the issue and argues that a notion of uncertainty is required to capture the concept of risk. Analysts classify uncertainty in two ways (M.Elisabeth Paté-Cornell, 1996): 1) aleatory uncertainty, which reflects variation in populations and 2) epistemic uncertainty, which reflects lack of knowledge. The latter type of uncertainty is key to understanding and characterizing risk, while the former is used to build probabilistic models, when justified, and support the epistemic uncertainty characterizations. Understanding where sources of uncertainty lie can help utilities better interpret assessment results and guide management decisions to reduce uncertainty for future analyses. J100-10 does not attempt to address uncertainty in the analysis process, evidenced by the fact the word ‘uncertainty’ does not appear anywhere in the standard. While there is debate regarding how uncertainties should be characterized and propagated in assessments, e.g., some

arguing probabilities fully capture uncertainty (Winkler, 1996) and others advocating for other methods (Flage, Aven, Zio, & Baraldi, 2014; Hoffman & Hammonds, 1994; M.Elisabeth Paté-Cornell, 1996), it is evident that the current J100-10 framework falls short because uncertainty is not addressed at all.

Including the concept of uncertainty in the definition of risk can improve the assessment framework of J100-10. The most common method is probabilistic risk assessments (PRA) (Apostolakis, 2004), which uses probabilities as the sole measure of uncertainty. Flage et al. (2014) (Flage et al., 2014) and Shortridge et al. (2017) (Shortridge, Aven, & Guikema, 2017) outline a variety of other analysis methods, from simpler models that use qualitative assessments of uncertainty, to more sophisticated technical models (e.g. use of possibility bounds and evidence theory).

Another approach is to assess the underlying strength of knowledge when using probabilistic judgements, for example, in relation to expert opinions. Experts include utility operators and shareholders, and they can be used to assess threat likelihoods and consequence measures when data is unavailable (AWWA, 2010). Typically, a stronger background knowledge is correlated with lower degrees of uncertainty. In performing this assessment, the uncertainty description becomes a function of their strength of background knowledge (Askeland, Flage, & Aven, 2017). Askeland et al. (2017) (Askeland et al., 2017) present a framework to evaluate strength of knowledge, categorizing it as "weak", "moderate", or "strong" based on five criteria: 1) expert's understanding of the phenomena, 2) reliability and availability of data, 3) agreement among experts, 4) identification, documentation, and soundness of assumptions, and 5) evaluation of knowledge gaps and changes in knowledge over time. Aven et al. (2013) (Terge Aven, Baraldi, Roger, & Zio, 2013) present an alternative method for assessing strength of knowledge through assumption deviation risk scores. Assumption deviation risk is defined as "risk related to a deviation between what has been assumed and what actually occurs" (Apostolakis, 2004). To assess the risk, consideration is given to deviation probabilities, consequences

of deviation, and related strength of knowledge judgements. Subsequent updates to the J100-10 standard can employ one or more of these methods or develop methods more suitable for application in the water industry.

4.2. Concepts of Probability

Probabilities are an integral part of the risk assessment process in J100-10. The standard defines probability on page 43 as follows:

"*A measure of the likelihood, degree of belief, frequency, or chance that a particular event will occur in a period of time (usually one year) or number of iterations or trials. This is usually expressed quantitatively as a value between 0 and 1, a range of values between 0 and 1, a distribution (density function), or the mean of such a distribution. Probability can also be expressed in qualitative terms, e.g. low, medium, or high, if there is a common understanding of the meaning of the qualitative terms."* (AWWA, 2010)

The definition presented is unclear in two ways. First, there are multiple ways outlined to represent probabilities. For clear interpretation of results to drive decision making, it is vital to have a consistent probability representation. Second, how these probabilities should be interpreted is left ambiguous. Aven and Reniers (2013) (Terje Aven & Reniers, 2013) highlight the practical importance for decision makers to understand what the risk analysis is communicating. For this reason, a concise definition of probability and its interpretation is required. Many previous studies have discussed this issue at length (see for example, White et al. (2016) (White, Burkhart, et al., 2016; White, George, et al., 2016), Aven and Reiners (2013) (Terje Aven & Reniers, 2013)). The body of work categorizes probability into two major schools of thought: frequentist and Bayesian.

The "frequentist" interpretation defines the probability of an event as the fraction of 'successes' over a hypothetical infinite series of independent and identical trials. An asymptotic relationship is assumed where, as the number of trials increases, the fraction of successes will

converge to the 'true' value (according to the law of large numbers), which is interpreted as the probability of the event. The true probability is in most cases, unknown and needs to be estimated. On the other hand, the "Bayesian" view defines probability as a measure of the assessor's degree of belief about the event. This numerical encoding of one's belief is always conditional on the assessor's knowledge base. Often, an example of drawing balls from an urn is used to provide an interpretation of the probabilities (Terje Aven & Reniers, 2013).

The J100-10 standard needs to be clear on which form of probability is used in each of the risk analysis steps because the two approaches can lead to different interpretations of the analysis, and ultimately lead to different actions in practice (Terje Aven & Reniers, 2013). When a frequentist view is used, it is important that the historical records are representative of future scenarios. The uncertainties of the frequentist estimates also need to be addressed. Similarly, when a Bayesian probability is adopted, evaluating the analyst's strength of knowledge on the matter is critical to understanding the usefulness of the assessment. Furthermore, communicating this knowledge level is essential for the accurate interpretation of a Bayesian probability. This results in the need to see beyond just the numerical value. An assessment process is required to evaluate the strength of knowledge as well, where a high strength of subject knowledge gives the analysis more authority and vice versa (Terje Aven, 2013, 2017b).

The J100-10 standard gives some flexibility for the analysts to decide which type of probability they wish to use (see page 29 of the J100-10 standard for eliciting probabilities for proximity and dependency hazards). Making the different types of probability clear and how they are to be interpreted can help the analyst choose the more suitable method depending on data availability and their strength of knowledge on the system.

While the J100-10 standard deals with threats from many different sources, a particular emphasis is misplaced on terrorism risk, as evidenced by 31 of the 41 reference hazards being

malevolent threats. J100-10 acknowledges that a true terrorism threat likelihood estimation is beyond the scope of most water sector risk analysis (AWWA, 2010), but suggests that estimating a proxy for this value can provide useful information for decision making. Equation (1) indicates that determining the annual likelihood of attack and the conditional likelihood of certain outcomes given an attack are key components of quantifying terrorism risk.

However, there is debate in the risk analysis literature regarding whether assigning static probabilities is even feasible. One side (see (Terje Aven & Guikema, 2015; Terje Aven & Renn, 2009; Brown & Cox, 2011; Cox, 2009)) argues that the intelligent nature of the adversary makes assigning meaningful and useful probabilities problematic if not impossible. Bayesian probabilities of attack can be elicited through experts, but are misleading because the defender and attacker act on different knowledge bases. Others argue that employing a game theoretic approach (Pate-Cornell & Guikema, 2002; Sandler & Enders, 2004; Sandler & M., 2003), which requires some simplifying assumptions on the adversary, provides a foundation from which probabilities can be assigned. Unfortunately these basic assumptions are rarely met in practice and renders the method deeply flawed. For example, there is not common knowledge between all actors, nor do the attackers always behave rationally.

J100-10 takes a more simplistic approach for estimating static probabilities, adopting a method developed by Risk Management Solutions, LLC. The process is outlined in a RAND Corporation report (Dixon, Lempert, LaTournette, & Reville, 2007) and detailed in Appendix F of J100-10 (AWWA, 2010). The method characterizes attack probability as the product of six values: 1) the likelihood an attack will occur, 2) the likelihood the attack will occur in a given metro area, 3) the likelihood water infrastructure will be targeted for attack, 4) the likelihood a subclass of facilities will be selected out of all water infrastructure (e.g. reservoirs, treatment plants, etc.), 5) the likelihood of a certain facility being targeted, and finally 6) the likelihood of the specific threat-asset pair being chosen.

Determining the likelihoods at each step uses a mixture of both frequentist and Bayesian perspectives. The approach J100-10 adopts is a Bayesian driven analysis when eliciting probabilities of attack for a metro region (step 2) and for a specific threat-asset pair (step 6). It is important that an appropriate elicitation from subject experts include consideration of adversary intent, capabilities, and options. In contrast, a frequentist approach is used when estimating the likelihood of which facility type (e.g. reservoir or pump station) and which specific site will be selected for attack. Because of the deep uncertainty surrounding intelligent adversaries, we argue that the J100-10 approach in trying to capture likelihoods of terrorism attack in a single value is inadequate and misleading as the process assumptions, the adequacy of historical data, and the strength of the assessor's knowledge all need to be communicated.

4.3 Evaluation of Resilience

While we focus our analysis on the risk analysis portion of J100-10, resilience is also an integral part of the decision making process in J100-10. Here we highlight some limitations regarding how resilience is evaluated.

There are various definitions of resilience across different disciplines. SRA defines resilience as the "ability of a system to sustain or restore its basic functionality following a risk source or an event" (Society of Risk Analysis (SRA), 2015). This is in line with the popular engineering (in particular infrastructure) view that conceptualizes resilience as the ability to 'bounce back' following shocks (Cutter, 2016). Other characterizations of resilience, particularly in the social sciences, focus more on the capacity for adaptive learning and change following events (Cutter, 2016).

A literature review by Hosseini et al. (Hosseini, Barker, & Ramirez-Marquez, 2016) highlights two key attributes for characterizing engineering resilience: 1) the system's preparedness to absorb disruptions to performance, and 2) the ability for performance recovery. To this end, the definition provided by J100-10 (see section 1.2) is in line with the engineering state of the art.

However, the approaches J100-10 provides for characterizing resilience are too narrow. The Operational Resilience Metric (ORM) metric in Equation (2) quantifies the expected amount of service denial because of a lost asset, and the Owner's Economic Resilience Metric (OERM) in Equation (3) measures the dollar value of this loss to the utility. These metrics are not adequate reflections of system resilience but rather measures of consequence, and using them as characterizations of resilience can seriously misguide the decision maker.

Since J100-10 is specific to water infrastructure, the key function for utilities to sustain or recovery is to meet demand for clean water supply and to prevent wastewater overflow. The temporal and dynamic aspects of service recovery is crucial for determining resilience (Alderson, Brown, & Carlyle, 2015b; Haimes, 2009) but is completely omitted in J100-10. J100-10 instructs that individual component resilience be quantified using Equations (2) and (3); however, this notion has been thoroughly discredited in the literature. Park et al. (2013) (Park, Seager, Rao, Convertino, & Linkov, 2013) argue that the nonlinear and self-organizing features in complex systems makes resilience impossible to measure when solely focusing on individual assets. Rather an emphasis should be placed on the performance of the entire system as a whole.

Some alternative assessments of resilience which J100-10 can apply are presented here. Two survey-based methods for measuring system-wide resilience are provided in Shirali et al. (2013) (Shirali, Mohammadfam, & Ebrahimipour, 2013) and Cutter et al. (2008) (Cutter et al., 2008). In both case studies, the authors worked with domain experts to characterize indicators of resilience (e.g. redundancy, robustness) and developed specific criteria to identify whether an organization met these indicators. Examples of quantitative methods for evaluating resilience involve stochastic simulation and optimization. In simulation driven methods (Albores & Shaw, 2008; Spiegler, Naim, & Wikner, 2012), infrastructure models are subjected to hypothetical hazards and key performance indicators (e.g. percentage of on-time deliveries for supply chains) are tracked. Optimization modelling

(Alderson, Brown, & Carlyle, 2015a; Faturechi, Levenberg, & Miller-Hooks, 2014), in contrast, aims to estimate least cost recovery or best-case performance for a system after damage.

The above examples analyze resilience in relation to well-defined objectives and disruptions. Haimes (2009) (Haimes, 2009) argues that resilience should be further expanded as the performance of a system can be different for different types of shocks (e.g. natural hazards vs intentional attacks). To address this issue, Aven (2017) (Terje Aven, 2017a) argues that risk and resilience assessments can be coupled together for a more complete analysis.

Finally, the notion of community resilience in J100-10 only references the economic impacts of hazards, ignoring the multi-faceted aspects of community resilience and the need for all attributes to be adequately captured in an analysis, as highlighted in Koloui et al. (2017) (Cutler et al., 2018). These multi-faceted aspects include physical, environmental, financial, and social impacts.

5. PRACTICAL LIMITATIONS

Here, we discuss some of the practical limitations of the J100-10 assessment framework. One such limitation is that the employed methods can lead to inaccurate representations of risk. Other limitations involve cases of ambiguity as a result of how key metrics are estimated and interpreted.

5.1. Use of Worst Case Scenarios

As discussed in Section 2.2, relying exclusively on worst-case assumptions when performing risk assessments can result in misleading conclusions. Even if there is certainty on the most extreme consequence, analysis on worst-case outcomes alone will always lead to mischaracterizations of risk because all other possible outcomes are excluded. Consider for example, the threat-asset pair summarized in Table I.

Table I. Summary of Example Threat-Asset Pair 1 with Divergent Outcomes. Risk calculated using Equation (1).

Scenario	Threat	Consequence	Vulnerability	Risk
1-1	0.1	10000	0.001	1*
1-2	0.1	500	0.049	2.45
1-3	0.1	100	0.950	9.5
			Expected Value	1 + 2.45 + 9.5 = 12.95

*Worst case only risk.

For the same threat event, which has probability 0.1 of occurrence, there are three possible outcome scenarios with varying likelihoods. This is shown by the different consequence values and their associated vulnerabilities. A worst-case-only analysis would conclude that the associated risk is 1 (based on scenario 1-1). However, if the other two outcome scenarios are taken into account, the expected value is 12.95. In comparison, consider the threat-asset pair shown in Table II. For the same threat with likelihood 0.1, there are two possible consequence scenarios. A worst-case-only analysis would determine that the associated risk for this example is 0.4 (under scenario 2-1). However, the expected value of risk, which considers both outcomes weighted by their respective likelihoods, is 50.3.

Table II. Summary of Example Threat-Asset Pair 2 with Divergent Outcomes. Risk calculated using Equation (1).

Scenario	Threat	Consequence	Vulnerability	Risk
2-1	0.1	2000	0.002	0.4*
2-2	0.1	500	0.998	49.9

	Expected Value	0.4 + 49.9 = 50.3

*Worst case only risk

These examples serve as simple illustrations as to why a full representation of all consequence scenarios is needed for an accurate representation of risk. Both example threat-asset pairs have high worst-case consequences with low associated vulnerabilities, which lead to very similar risk scoring (1 and 0.4 respectively). Taking a worst-case only approach would lead risk analysts to conclude that both threat-asset pairs are subject to a similar level of risk as measured by Equation (1). Worst-case scenarios alone, however, do not accurately represent the risk of the threat-asset pairs. In both examples, the worst-case scenarios are also the least likely to occur. After considering the other possible scenarios, the resulting risk calculations again using Equation (1) (12.95 and 50.3 respectively) show that the second example is clearly the riskier threat-asset pair, with close to four times the risk value. The assumption here is that the expected value is an adequate risk measure, which is a very questionable assumption. This clear distinction in the risk description is overlooked when a worst-case-only basis is used.

A worst-case-only approach is quite popular in other domains beyond critical infrastructure analysis (e.g. financial (Zhu & Fukushima, 2009) and environmental risk assessments (Huysman, Madarasz, & Dassargues, 2006; Karl, Wright, Berglen, & Denby, 2011)). The limitations of using conservative 'worst-case' methods have been thoroughly discussed and criticized in the literature (M Elizabeth Paté-Cornell, 1999). We refer the reader to Aven (2016) (Terje Aven, 2016) for an expanded discussion. Considering the full range of possible outcomes and their consequences in the analysis will lead to more informative descriptions of risk. In addition to the probabilistic characterizations, judgements of the strength of knowledge supporting these should be included as highlighted in Section 4.2.

An alternate characterization of risk is to present information on the underlying consequence distributions, for example, showing the 25^{th}, 50^{th}, and 75^{th} percentiles as well as the expected and worst-case scenarios. A common and more complete probabilistic representation in the risk analysis literature is the use of Frequency-Number types of curves (e.g. inverse cumulative distributions), discussed in Aven (2013) (Terje Aven, 2003), which plot all possible consequence values against their respective inverse cumulative probabilities, i.e. the probabilities for events leading to at least N units of loss (e.g., fatalities).

5.2. Defining and Estimating Consequences

It is important to display a full range of consequence scenarios for risk estimations. The J100-10 framework defines four baseline metrics for measuring consequence. These are 1) number of fatalities, 2) number of serious injuries, 3) financial loss to utility owners, and 4) economic losses to the community. The standard suggests that other facets of consequence, such as degradation in public confidence and environmental impacts, can also be included if the analyst deems necessary. Detailed calculations using simulation and economic models or direct estimation by qualified experts are acceptable methods of determining consequences according to J100-10.

The risk valuation in Equation (1) requires a single value for the consequence metric. However it is unclear how, or even if, an analyst should aggregate across metrics. For example, no guidance is offered for combining the metric estimates of 10 deaths, 5 injuries, $5 million in financial losses to the utility, and $15 million in economic losses to the serviced community. This process becomes more difficult when qualitative assessments of consequences are also considered.

There are a number of ways to encode consequences into a single metric. One method is to monetize fatalities and injuries to provide a common unit of measure to sum consequences from each category. A similar approach is to normalize each metric into an ordinal scale (e.g. 1-10) and sum the normalizations. J100-10 provides a 0-10 consequence scale for each category (AWWA, 2010) which

the analyst can opt to use. This approach makes an implicit assumption about the inherent value of different consequence outcomes, and disagreements about these valuations may arise when multiple decision makers are involved. For example, according to the J100-10, one fatality is equal to $1 million in economic losses to either the utility or the community. These assumptions need to be made explicit to the decision maker and J100-10 does not provide any direction on doing so.

Additional outcome aggregating methods are also presented in the risk analysis literature. The field of decision analysis supports the use of multi-attribute utility theory (MAUT) to encode a variety of decision maker preferences into a numerical value, and has been demonstrated in many engineering risk assessments (Brito & de Almeida, 2009; Merkhofer & Keeney, 1987; Michaud & Apostolakis, 2006). Ayyub (2014) (Ayyub, 2014) introduces other methods for assessing consequences and severities, including cause-consequence (CS) diagrams and total economic valuation (TEV). CS diagrams use a tree representation of multiple consequence categories (e.g. fatalities, economic costs) and assess their respective severities using logic diagrams. These severities are combined additively in an ordinal scale. TEV uses willingness to pay or accept methods to estimate the market value, measured in dollars, of lost goods and services.

While there is a host of processes for combining consequence metrics into a single value, it is unclear what this single value represents. In making this calculation, the system operator must make assumptions regarding the value of consequences to other stakeholders, and in doing so, the utility imposes its own value structure on these stakeholders. According to Arrow's impossibility theorem (Arrow, 1950), it is generally impossible for any analyst to accurately encompass each stakeholder's diverse preferences under a set of numerical weights. Survey methods are available as a foundation to begin the analysis of contrasting value judgements, but they require time and resources that the utility may not be willing to commit.

Therefore, in some situations utilities may find it beneficial to keep the consequence categories disaggregated. While this can lead to a less quantifiable measure of risk (i.e. Equation (1) can no longer be applied), more information can be communicated in the assessment results. Lundberg and Willis (2019) (Lundberg & Willis, 2019) present one approach for carrying out risk assessments while dealing with non-aggregate outcomes. The authors use a survey-based method to identify a ranking of consequences attributes. This information allows the analyst to prioritize one category over another. Kabir et al. (2018) (Kabir, Balek, & Tesfamariam, 2018) presents a quantitative Bayesian network model for modelling consequences due to infrastructure failures. The model disaggregates outcomes based on health and safety, environmental, societal, and economic impacts. Expert judgement is used to define the dependencies between various outcome measures.

5.3. Analysis Resolution of Threat-Asset Pairs

An accurate estimation of the consequences of a hazard on complex systems requires the analysis of multiple components together and the consideration of their interdependencies. Consequently, analyzing risk and resilience only at the threat-asset pair resolution overlooks the dependency between components (Alderson et al., 2015b).

This integrated relationship between assets can be illustrated through a simple example. A reliability block diagram (RBD) is a visual method that describes how individual components contribute to the overall functioning of a complex system (Terje Aven, 2003). Here, the functioning or success of the system is defined as the extent to which it can carry out its mission. In the case of water systems, this involves the adequate delivery of clean drinking water to end users. Each block in a diagram represents a system function, which can correspond to individual components of the system (e.g., treatment plant or storage tank) that can fail with a given probability upon an incident hazard. Blocks can be connected in parallel or series; parallel paths introduce redundancy into the system,

where all blocks within a parallel block must fail before the network fails. On the other hand, any failure to a single block in a group of blocks connected in series will cause system failure.

Fig. 2 illustrates a simple system with three components, represented by blocks A, B, and C. Component A is connected in series to a parallel set of components B and C. This means failures to A alone, or B and C together, or to all three components can lead to system failure. Risk analysis of this system at the threat-asset level involves only evaluating the consequences of failure when components A, B, and C fail individually. The redundancy relationship between B and C is not captured in the analysis at this resolution. A consequence estimate on the failure of asset B assuming asset C is functional may only include costs of damage repair; however, if asset C also fails, the consequence may be much more severe as it involves repairs to both components and economic losses due to service interruption.

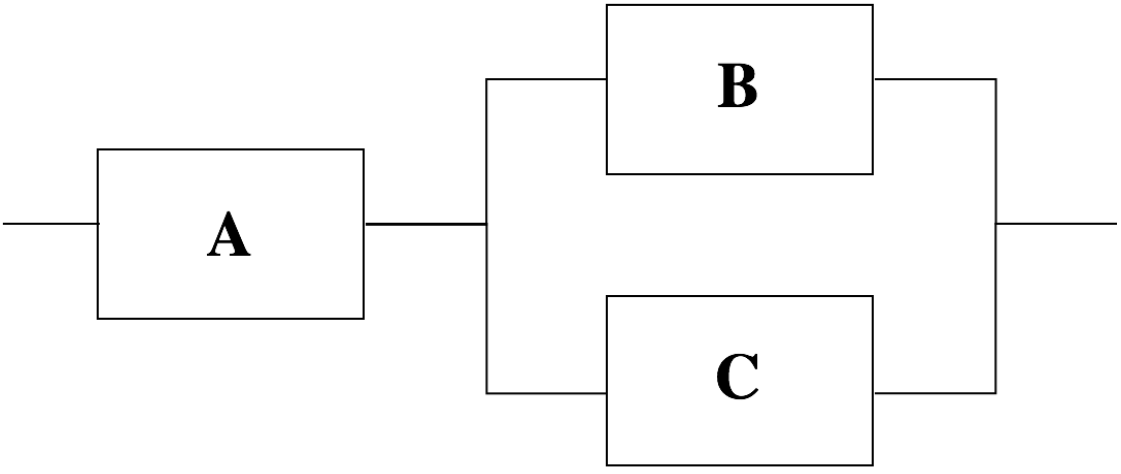

Figure 2. Reliability Block Diagram of Example System.

The simplifying example above serves to illustrate that an accurate assessment of threat consequences requires information from multiple components of the system, and examining risk at the asset levels overlooks this relationship by requiring the analyst to make implicit assumptions about the condition of other components. The assessment can be improved where joint impacts, particularly cases where consequences of failures to a group of assets will exceed the sum of consequences from individual failures itself, are captured.

Aside from reliability block diagrams, graph theory (or network theory) is another method researchers have used to study the system-wide impacts related to individual component failure (see (Alenazi & Sterbenz, 2015; Larocca & Guikema, 2011; A. Yazdani & Jeffrey, 2012; Alireza Yazdani & Jeffrey, 2012)). In these network models, infrastructure components are represented through a series of arcs and nodes (Dunn, Fu, Wilkinson, & Dawson, 2013). Each node represents a demand point, storage site, treatment site, or generation facility. Arcs represent distribution assets (e.g. wire cables for power systems, pipelines for water and gas networks). These studies have aimed to examine which network metrics (betweenness, centrality, etc.) are most useful in providing an accurate characterization of network resilience. Papers by Alderson et al. (Alderson, Brown, Carlyle, & Anthony Cox, 2013; Alderson et al., 2015b) emphasize the use of physical infrastructure models rather than simple topological representations to provide the most accurate reflections of network performance. LaRocca et al. (2015) (Larocca, Johansson, Hassel, & Guikema, 2015) compared a range of topological metrics and physical models to measure power system performance, and found that combining graph theory with physical flow models provided the most accurate insights.

5.4. Threats Defined

Another issue of implementation is the limited scope of the 41 reference threats listed in Fig. 3. The RAMCAP™ framework, which the J100-10 standard is based on, was originally developed to deal with terrorism threats, and 31 out of the 41 reference threats deal with malevolent threats. As a

result, the analysis scope can be biased towards this single threat category. This can lead to a suboptimal allocation of resources to countermeasures that are dedicated to increasing the physical security of the system at the expense of hardening the system against (arguably) more frequent natural hazards. For example, a countermeasure, such as adding more security personnel, can decrease the risk for many of the 31 reference terrorist threats. Because of the large overlap in the types of threats and how to defend against them, implementing mitigation options for one of these threats also serves to mitigate several other threats. As a result, the estimated net benefit of counter-terrorism defenses will be over inflated.

On the other hand, countermeasures for natural hazards tend to be more specific to the threat, e.g., installing floodwalls around coastal treatment plants to reduce flood damage. The limited overlap in affected threats from these countermeasures can lead to lower net benefits after summing over all threat-asset pairs. This shows that the J100-10 reference threat set typically biases the user to allocate resources to defend against terrorist threats over other hazard categories. For some general guidance on how to use cost-benefit type analysis, see Aven (2017) (Terge Aven, 2017) and Ale et al. (2018) (Ale, Hartford, & Slater, 2018).

Hazard Type	Hazard Description			
Natural	N(H) Hurricanes	N(E) Earthquakes	N(T) Tornadoes	N(F) Floods
	N(W) Wildfire		N(I) Ice storms	
Dependency & Proximity	D(U) Loss of Utilities	D(S) Loss of Suppliers	D(E) Loss of Employees	D(C)Loss of Customers
	D(T) Loss of Transportation		D(P) Proximity to other targets	
Product Contamination	C(C) Chemical	C(R) Radionuclide	C(B) Biotoxin	C(P) Pathogen
	C(W) Weaponization of water disposal system			
Sabotage	S(PI) Physical–Insider	S(PU) Physical–Outsider	S(CI) Cyber–Insider	S(CU) Cyber–Outsider
Theft or Diversion	T(PI) Physical–Insider	T(PU) Physical–Outsider	T(CI) Cyber–Insider	T(CU) Cyber–Outsider
Attack: Marine	(M1) Small Boat	(M2) Fast Boat	(M3) Barge	(M4) Ocean Ship
Attack: Aircraft	(A1) Helicopter	(A2) Small Plane	(A3) Medium, Regional Jet	(A4) Long-Flight Jet
Attack: Automotive	(V1) Car	(V2) Van	(V3) Midsize Truck	(V4) Large Truck (18 Wheeler)
Attack: Assault Team	(AT1) 1 Assailant	(AT2) 2-4 Assailants	(AT3) 5-8 Assailants	(AT4) 9-16 Assailants

Figure 3. RAMCAP^{TM} Reference Hazards used in J100-10. Figure taken from the J100-10 Risk Management Standard [1].

As noted in Section 2.2, two studies presented by White et al. (White, Burkhart, et al., 2016; White, George, et al., 2016) argue that the operating 41 reference threats do not adequately address the emerging threats of climate change, aging infrastructure, and cybersecurity. While J100-10 allows analysts to include additional threats, it lacks guidance in how to define events that encompass these emerging threats and how to calculate the respective threat likelihoods. Furthermore, the subjectivity involved in adding more events can lead to inconsistencies when different analysts are performing the risk assessments.

5.5. Risk versus Resilience Tradeoff

In Steps 6 and 7 of the J100-10 methodology, risk and resilience are calculated, countermeasures are defined, and resources are allocated based on cost-benefit analysis. However there is ambiguity in choosing how to allocate these resources based on the different metrics. Step 7 (risk and resilience management) specifies that utilities need to define what acceptable levels of risk and resilience are, and implement countermeasures to meet these pre-defined thresholds.

As defined by J100-10, resilience and risk are two different outcomes. When dealing with various outcomes, an analyst must work with the stakeholders to elicit the value of resilience enhancement versus risk reduction. Decision makers need to understand the tradeoffs between the risk and resilience objectives in order for the assessment to be actionable. Unfortunately, the importance of eliciting these value judgements is omitted from J100-10.

There is, however, a strong argument in the risk research community that the separation between risk and resilience is artificial and that the risk concept should cover resilience (Terje Aven, 2018). This is because any actions performed to affect one will also affect the other: reductions in risk will also increase resilience, and vice versa. Aven (2017) (Terje Aven, 2017a) argues that assessments are more effective when the two outcomes are considered together, rather than treated as separated objectives.

As it currently stands, J100-10 is too vague in its definition of the relationship between risk and resilience. Improvements to the standard can either solely focus on risk, and target reductions in risk, or integrate risk and resilience together for a more holistic assessment.

6. DISCUSSION

In this study, we performed a comprehensive review of the risk and resilience assessment framework in the J100-10, a certified standard adopted by the water and wastewater industry. The framework adopts the seven-step methodology outlined in RAMCAP^{TM}, which applies to multiple sectors of critical infrastructure and key resources. Our analysis examined both conceptual limitations within the standard and practical issues with carrying out the risk and resilience assessment processes.

The main conceptual shortcomings are 1) the exclusion of notions of uncertainty when defining risk, 2) a clear definition for probability and how to interpret the values is not presented, and 3) resilience measures are too narrow. In particular, the differences between frequentist and Bayesian probability needs to be highlighted, and the conceptualizations used need to be communicated in the final analysis results. Our key findings on the practical limitations relate to the mischaracterization of risk, the biased emphasis placed on malevolent threats, and the general ambiguity in defining and comparing key metrics.

When calculating risk, using only a worst-case assumption of the associated consequences without considering the full range of possible outcome scenarios will result in a poor risk characterization. Furthermore, risk and resilience analysis at the resolution of individual threat-asset pairs ignores key dependencies between assets in connected systems. This resolution can lead to risk judgements that are too low in cases where combined consequences of hazards on multiple assets at a time will be far greater than the sum of the individual parts.

On the same note of accurately representing consequences, the standard uses four key metrics: fatalities, injuries, and economic losses to both the utility and community. Additional qualitative evaluations of consequence can also be included. The J100-10 standard does not provide adequate guidance on how to bring these four metrics, measured in different units, and other

qualitative aspects of consequence, together into a single consequence value. This ambiguity can lead to inconsistencies in the risk analysis process.

The J100-10 defines 41 reference threats as part of the assessment, 31 of which are related to malevolent threats. The disproportionate representation of risk related to one category of threat can lead to biased conclusions about inflated benefits gained from counter-terrorism defenses. It is important for resulting updates of the J100-10 and RAMCAP™ standard to account for any overlap when weighing the tradeoff between countermeasures designed to address malevolent threats versus natural hazards versus proximity and dependency hazards.

Lastly, the J100-10 standard needs to better address the relationship between the concepts of risk and resilience. This is critical for using the J100-10 in an effective decision making context. The vagueness of the current standard can also introduce arbitrariness and inconsistencies, with potential for poor investments of available resources.

The shortcomings summarized above can assist with prioritization in redrafts of the standard by highlighting areas that need to be addressed. By closing the gap between the standard's methods and those that are the state of the art in the risk analysis literature, more informed risk-driven decisions can be made to better protect the nation's critical lifeline infrastructure.

ACKNOWLEDGEMENTS

We thank the University of Michigan for funding this research. The opinions and views expressed are those of the researchers and do not necessarily reflect those of the sponsors.

REFERENCES

Albores, P., & Shaw, D. (2008). Government preparedness: Using simulation to prepare for a terrorist attack. *Computers and Operations Research*, *35*(6), 1924–1943. https://doi.org/10.1016/j.cor.2006.09.021

Alderson, D. L., Brown, G. G., Carlyle, M. W., & Anthony Cox, L. (2013). Sometimes There Is No "'Most-Vital'" Arc: Assessing and Improving the Operational Resilience of Systems. *Military Operations Research*, *18*(1), 21–37. https://doi.org/10.5711/1082598318121

Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015a). *Assessing and Improving Operational Resilience of Critical Infrastructures and Other Systems*. *Bridging Data and Decisions*. https://doi.org/10.1287/educ.2014.0131

Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015b). Operational Models of Infrastructure Resilience. *Risk Analysis*, *35*(4), 562–586. https://doi.org/10.1111/risa.12333

Ale, B. J. M., Hartford, D. N. D., & Slater, D. H. (2018). The practical value of a life : priceless, or a CBA calculation? *Medical Research Archives*, *6*(3), 1–12.

Alenazi, M. J. F., & Sterbenz, J. P. G. (2015). Evaluation and comparison of several graph robustness metrics to improve network resilience. In *Proceedings of 2015 7th International Workshop on Reliable Networks Design and Modeling, RNDM 2015* (pp. 7–13). https://doi.org/10.1109/RNDM.2015.7324302

Amass, S. F. (2006). *The Science of Homeland Security, Volume 1*. Wast Lafayette, Ind.: Purdue University Press.

American Society of Mechanical Engineerins and Innovative Technologies Institute (ASME-ITI LLC). (2005). *RAMCAP™ Executive Summary - A 7 Step Approach*. New York, NY: American

Society of Mechanical Engineers.

American Water Works Association (AWWA), American Society of Mechanical Engineers, American National Standards Institute, and Innovative Technologies Instiitute LLC. (2010). *J100-10 RAMCAP™ Standard for Risk and REsilience Management for Water and Wastewater Systems*. Denver, CO: American Water Works Association. 0

Apostolakis, G. E. (2004). How Useful Is Quantitative Risk Assessment? *Risk Analysis*, *24*(3), 515–520.

Arrow, K. J. (1950). A Difficulty in the Concept of Social Welfare. *The Journal of Political Economy*, *58*(4), 328–346.

Askeland, T., Flage, R., & Aven, T. (2017). Moving beyond probabilities – Strength of knowledge characterisations applied to security. *Reliability Engineering and System Safety*, *159*, 196–205. https://doi.org/10.1016/j.ress.2016.10.035

Aven, Terge. (2017). On some foundational issues related to cost-benefit and risk. *International Journal of Business Continuity and Risk Management*, *7*(3), 182–191.

Aven, Terge, Baraldi, P., Roger, F., & Zio, E. (2013). *Uncertainty in risk assessment: the representation and treatment of uncertainties by probabilistic and non-probabilistic methods*. *John Wiley & Sons*. https://doi.org/10.1016/j.asoc.2014.05.024

Aven, Terje. (2003). *Foundations of Risk Analysis. A Knowledge and Decision-Oriented Pespective*. John Wiley & Sons, Ltd. https://doi.org/10.1198/jasa.2005.s16

Aven, Terje. (2012). The risk concept-historical and recent development trends. *Reliability Engineering and System Safety*, *99*, 33–44. https://doi.org/10.1016/j.ress.2011.11.006

Aven, Terje. (2013). Practical implications of the new risk perspectives. *Reliability Engineering and*

System Safety, *115*, 136–145. https://doi.org/10.1016/j.ress.2013.02.020

Aven, Terje. (2016). On the use of conservatism in risk assessments. *Reliability Engineering and System Safety*, *146*, 33–38. https://doi.org/10.1016/j.ress.2015.10.011

Aven, Terje. (2017a). How some types of risk assessments can support resilience analysis and management. *Reliability Engineering and System Safety*, *167*(August 2016), 536–543. https://doi.org/10.1016/j.ress.2017.07.005

Aven, Terje. (2017b). Improving risk characterisations in practical situations by highlighting knowledge aspects, with applications to risk matrices. *Reliability Engineering and System Safety*, *167*, 42–48. https://doi.org/10.1016/j.ress.2017.05.006

Aven, Terje. (2018). The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Analysis*, (2009). https://doi.org/10.1111/risa.13247

Aven, Terje, & Guikema, S. (2015). On the Concept and Definition of Terrorism Risk. *Risk Analysis*, *35*(12), 2162–2171. https://doi.org/10.1111/risa.12518

Aven, Terje, & Reniers, G. (2013). How to define and interpret a probability in a risk and safety setting. *Safety Science*, *51*(1), 223–231. https://doi.org/10.1016/j.ssci.2012.06.005

Aven, Terje, & Renn, O. (2009). The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk. *Risk Analysis*, *29*(4), 587–600. https://doi.org/10.1111/j.1539-6924.2008.01175.x

Ayyub, B. M. (2014). *Risk Analysis in Engineering and Economics* (2nd ed.). CRC Press.

Brito, A. J., & de Almeida, A. T. (2009). Multi-attribute risk assessment for risk ranking of natural gas pipelines. *Reliability Engineering and System Safety*, *94*(2), 187–198.

https://doi.org/10.1016/j.ress.2008.02.014

Brown, G. G., & Cox, L. A. T. (2011). How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts. *Risk Analysis*, *31*(2), 196–204. https://doi.org/10.1111/j.1539-6924.2010.01492.x

Burkhart, A. (2015). *Lifeline Infrastructure Risk Analysis Application*. University of Colorado at Colorado Springs.

U. S. Homeland Security Act of 2002, Pub. L. No. 2135, 2135 (2002). United States of America Congress.

Cox, L. A. (2008a). Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *Risk Analysis*, *28*(6), 1749–1761. https://doi.org/10.1111/j.1539-6924.2008.01142.x

Cox, L. A. (2008b). What's Wrong with Risk Matrices? *Risk Analysis*, *28*(2), 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Cox, L. A. (2009). Improving Risk-Based Decision Making for Terrorism Applications. *Risk Analysis*, *29*(3), 336–341. https://doi.org/10.1111/j.1539-6924.2009.01206.x

Cutler, H., Dillard, M., McAllister, T. P., van de Lindt, J. W., Koliou, M., & Ellingwood, B. R. (2018). State of the research in community resilience: progress and challenges. *Sustainable and Resilient Infrastructure*, *9689*, 1–21. https://doi.org/10.1080/23789689.2017.1418547

Cutter, S. L. (2016). Resilience to What? Resilience for Whom? *Geographical Journal*, *182*(2), 110–113. https://doi.org/10.1111/geoj.12174

Cutter, S. L., Barnes, L., Berry, M., Burton, C., Evans, E., Tate, E., & Webb, J. (2008). A place-based model for understanding community resilience to natural disasters. *Global Environmental Change*, *18*(4), 598–606. https://doi.org/10.1016/j.gloenvcha.2008.07.013

Department of Homeland Security (DHS). (2009). *National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security.

Dixon, L., Lempert, R. J., LaTournette, T., & Reville, R. T. (2007). *The Federal Role in Terrorism Insurance: Evaluating Alternatives in an Uncertain World*. *Rand Corporation*. https://doi.org/10.4135/9781412950558.n465

Dunn, S., Fu, G., Wilkinson, S., & Dawson, R. (2013). Network theory for infrastructure systems modelling. In *Proceedings of the ICE - Engineering Sustainability* (Vol. 166, pp. 281–292). https://doi.org/10.1680/ensu.12.00039

Faturechi, R., Levenberg, E., & Miller-Hooks, E. (2014). Evaluating and optimizing resilience of airport pavement networks. *Computers and Operations Research*, *43*, 335–348. https://doi.org/10.1016/j.cor.2013.10.009

Flage, R., Aven, T., Zio, E., & Baraldi, P. (2014). Concerns, Challenges, and Directions of Development for the Issue of Representing Uncertainty in Risk Assessment. *Risk Analysis*, *34*(7), 1196–1207. https://doi.org/10.1111/risa.12247

Haimes, Y. Y. (2009). On the Definition of Resilience in Systems. *Risk Analysis*, *29*(4), 498–501. https://doi.org/10.1111/j.1539-6924.2009.01216.x

Hauge, K. H., Blanchard, A., Andersen, G., Boland, R., Einar, B., Howell, D., … Vikebø, F. (2014). Inadequate risk assessments – A study on worst-case scenarios related to petroleum exploitation in the Lofoten area. *Marine Policy*, *44*, 82–89. https://doi.org/10.1016/j.marpol.2013.07.008

Herrera, E. K., Flannery, A., & Krimmer, M. (2017). Risk and Resilience Analysis for Highway Assets. *Transportation Research Record: Journal of the Transportation Research Board*, *2604*(1), 1–8.

Hoffman, F. O., & Hammonds, J. S. (1994). Propagation of Uncertainty in Risk Assessments: The

Need to Distinguish Between Uncertainty Due to Lack of Knowledge and Uncertainty Due to Variability. *Risk Analysis*, *14*(5), 707–712. https://doi.org/10.1111/j.1539-6924.1994.tb00281.x

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety*, *145*, 47–61. https://doi.org/10.1016/j.ress.2015.08.006

Huysman, M., Madarasz, T., & Dassargues, A. (2006). Risk Assessment of Groundwater Pollution Using Sensitivity Analysis and Worst Case Scenario Analysis. *Environmental Geology*, *50*(2), 180–193.

Jaeger, C. D., Hightower, M. M., & Torres, T. (2010). Evolution of Sandia's Risk Assessment Methodology for Water and Wastewater Utilities (RAM-W). In *World Environmental and Water Resources Congress 2010* (pp. 3804–3010).

Kabir, G., Balek, N. B. S., & Tesfamariam, S. (2018). Consequence-based framework for buried infrastructure systems: A Bayesian belief network model. *Reliability Engineering and System Safety*, *180*, 290–301. https://doi.org/10.1016/j.ress.2018.07.037

Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. *Risk Analysis*, *1*(1), 11–27.

Karl, M., Wright, R. F., Berglen, T. F., & Denby, B. (2011). Worst Case Scenario Study to Assess the Environmental Impact of Amine Emissions from a CO2 Capture Plant. *International Journal of Greenhouse Gas Control*, *5*(3), 439–447. https://doi.org/10.1016/j.ijggc.2010.11.001

Kerr, D. J., Singh, A., & Motala, I. (2015). Understanding Risk and Resilience to Better Manage Water Transmission Systems. In *Pipelines 2015* (pp. 1772–1785).

Krimgold, F. (2012). Regional Resilience and Security for Critical Infrastructure. In *Comparative Analysis of Technological and Intelligent Terrorism Impacts on Complex Technical Systems* (pp.

61–68).

Larocca, S., & Guikema, S. (2011). A survey of network theoretic approaches for risk analysis of complex infrastructure systems. In *Vulnerability, Uncertainty, and Risk: Analysis, Modeling, and Management* (pp. 155–162).

Larocca, S., Johansson, J., Hassel, H., & Guikema, S. (2015). Topological Performance Measures as Surrogates for Physical Flow Models for Risk and Vulnerability Analysis for Electric Power Systems. *Risk Analysis*, *35*(4), 608–623. https://doi.org/10.1111/risa.12281

Lewis, T. G., Darken, R. P., Mackin, T., & Dudenhoeffer, D. (2012). Model-based risk analysis for critical infrastructures. *WIT Transactions on State-of-the-Art in Science and Engineering*, *54*, 3–19. https://doi.org/10.2495/978-1-84564-

Lundberg, R., & Willis, H. H. (2019). Examining the effectiveness of risk elicitations: comparing a deliberative risk ranking to a nationally representative survey on homeland security risk. *Journal of Risk Research*, 1–15. https://doi.org/10.1080/13669877.2018.1501593

Merkhofer, M. W., & Keeney, R. L. (1987). A Multiattribute Utility Analysis of Alternative Sites for the Disposal of Nuclear Waste. *Risk Analysis*, 7(2), 173-194.

Michaud, D., & Apostolakis, G. E. G. E. (2006). Methodology for Ranking the Elements of Water-Supply Networks. *Journal of Infrastructure Systems*, *12*(4), 230–242. https://doi.org/10.1061/(ASCE)1076-0342(2006)12:4(230)

National Rural Water Assocation (NRWA). (2002). *Security and Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations Between 3300 and 10000*. Duncan, OK: National Rural Water Assocation.

PA Government Services and Scientech Inc. (2002). *VSAT™ User's Manual (Vulnerability Self-Assessment Tool)*. Washington, D.C.: National Association of Clean Water Agencies.

Park, J., Seager, T. P., Rao, P. S. C., Convertino, M., & Linkov, I. (2013). Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. *Risk Analysis*, *33*(3), 356–367. https://doi.org/10.1111/j.1539-6924.2012.01885.x

Pate-Cornell, E., & Guikema, S. (2002). Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures. *Military Operations Research*, *7*(4), 5–20. https://doi.org/10.5711/morj.7.4.5

Paté-Cornell, M.Elisabeth. (1996). Uncertainties in Risk Analysis: Six Levels of Treatment. *Reliability Engineering & System Safety*, *54*(2), 95–111. https://doi.org/10.1016/S0951-8320(96)00067-1

Paté-Cornell, M Elizabeth. (1999). Conditional uncertainty analysis and implications for decision making: The case of WIPP. *Risk Analysis*, *19*(5), 995–1002. https://doi.org/10.1023/A:1007030913871

Sandler, T., & Enders, W. (2004). An Economic Perspective of Transnational Terrorism. *European Journal of Political Economy*, *20*(2), 301–316.

Sandler, T., & M., D. G. A. (2003). Terrorism & Game Theory. *Simulation & Gaming*, *34*(3), 319–337. https://doi.org/10.1177/1046878103255492

Shirali, G. A., Mohammadfam, I., & Ebrahimipour, V. (2013). A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry. *Reliability Engineering and System Safety*, *119*, 88–94. https://doi.org/10.1016/j.ress.2013.05.003

Shortridge, J., Aven, T., & Guikema, S. (2017). Risk assessment under deep uncertainty: A methodological comparison. *Reliability Engineering and System Safety*, *159*, 12–23. https://doi.org/10.1016/j.ress.2016.10.017

Society of Risk Analysis (SRA). (2015). *Society of Risk Analysis Glossary*. *Society for Risk Analysis. Committee on Foundations of Risk Analysis*. McLean, VA.

Society of Risk Analysis (SRA). (2018). *Society for Risk Analysis: Fundamental Principles*. McLean, VA.

Spiegler, V. L. M., Naim, M. M., & Wikner, J. (2012). A control engineering approach to the assessment of supply chain resilience. *International Journal of Production Research*, *50*(21), 6162–6187. https://doi.org/10.1080/00207543.2012.710764

White, R., Burkhart, A., Boult, T., & Chow, E. (2016). Towards a Comparable Cross-Sector Risk Analysis: RAMCAP Revisited. In *Critical Infrastructure Protection X* (pp. 221–238).

White, R., George, R., Boult, T., & Chow, C. E. (2016). Apples to Apples: RAMCAP and Emerging Threats to Lifeline Infrastructure. *Homeland Security Affairs 12*, *1*(1).

Winkler, R. L. (1996). Uncertainty in probabilistic risk assessment. *Reliability Engineering & System Safety*, *54*(2–3), 127–132. https://doi.org/10.1016/S0951-8320(96)00070-1

Yazdani, A., & Jeffrey, P. (2012). Applying network theory to quantify the redundancy and structural robustness of water distribution systems. *Journal of Water Resources Planning and Management*, *138*(2), 153–161. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000159.

Yazdani, Alireza, & Jeffrey, P. (2012). Water distribution system vulnerability analysis using weighted and directed network models. *Water Resources Research*, *48*(6), 1–10. https://doi.org/10.1029/2012WR011897

Zhu, S., & Fukushima, M. (2009). Worst-Case Conditional Value-at-Risk with Application to Robust Portfolio Management. *Operations Research*, *57*(5), 1155–1168. https://doi.org/10.1287/opre.