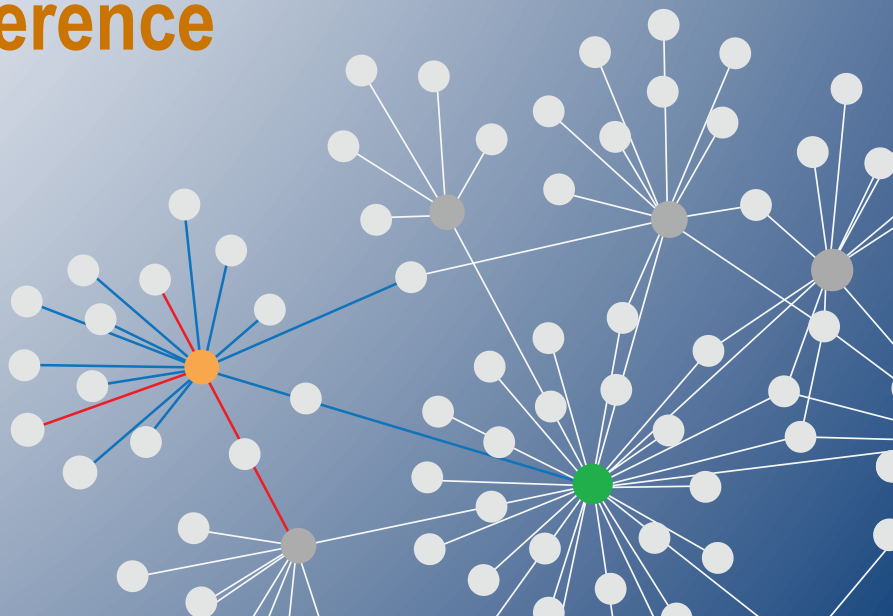
GRADIENT
PLANNING

The J100 Standard: A Catalyst for an All-Hazards Vulnerability Assessment

NEWEA 2016 Annual Conference
January 25, 2016

Marian H. Long, P.E.
Gradient Planning, LLC



GRADIENT PLANNING

Welcome and game plan for discussion

- Lets face reality
- And, then it is time for tough questions
- Critical elements of the J100 Standard
- The benefits of taking action

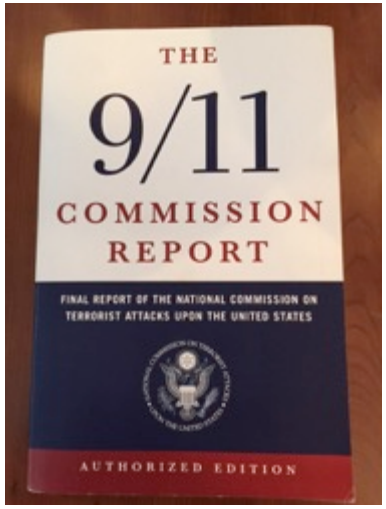
Here's a sobering dose of reality…

- March 2010 – Rhode Island floods
- April, May 2011 – Vermont floods
- August 2011 – CT and Vermont – Tropical Storm Irene
- October 2011 – CT – Winter Storm Alfred
- October 2012 – NJ -- Superstorm Sandy
- December, 2015 – Missouri floods
- 2016 – And our next disaster is…?

Lets prepare for a future of disasters…

- Huffington Post Blog of December 19, 2015…

- The 911 Commission Report…



Tough questions to ask yourself

- How do I know that we have identified our threats?
- How do I know that we have mitigated them successfully?
- With finite resources, what improvements should I fund?
- Am I managing our program consistent with relevant industry standards?
- Are we going to have an event that impacts the entire community?
- Will there be negative press for me and our utility?

What is RAMCAP?

- Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard
- First edition published on July 1, 2010
- Developed through a joint collaboration:
  - American Water Works Association (AWWA)
  - American Society of Mechanical Engineers- Innovative Technologies Institute (ASME-ITI)
  - American National Standard Institute (ANSI)
- Standard is also referred to as "ANSI/ASME-ITI/AWWA J100-10"

Origin of the RAMCAP Standard

- After the attacks of September 11, 2001, the White House requested ASME leaders to define and prioritize the requirements for protecting our nation's critical infrastructure.
- Their recommendation was to create a risk analysis and management process to support decisions allocating resources to risk-reduction activities.
- Also recommended was for this process to permit direct comparisons within and across industry sectors
  - Common terminology
  - Common metrics
  - Consistent methodology

Evolution of the RAMCAP Standard

- In 2003, U.S. DHS initiated development of sector-specific guidance for critical sectors including water and wastewater systems.
- The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 required all water utilities service more than 3,300 people to perform security vulnerability assessments (did not include natural hazards).
- Three methodologies were accepted and applied:
  - Risk Assessment Methodology- Water (RAM-W™)
  - Vulnerability Self Assessment Tool (VSAT™)
  - Security Environmental Management System (SEMS™)

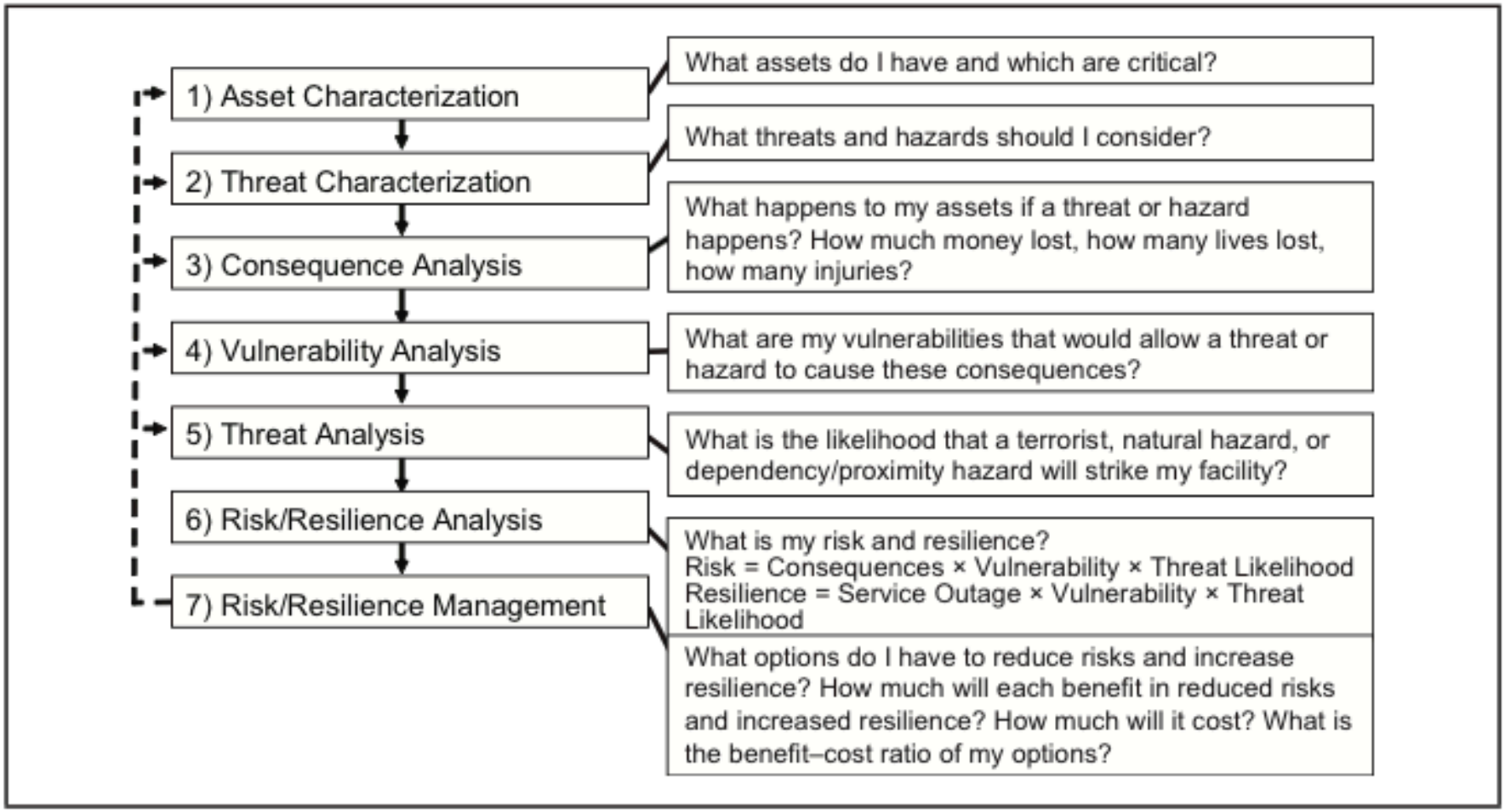
Tools for the RAMCAP Standard

- VSAT™ continues to evolve with the RAMCAP Standard
- Similar work is progressing for ARAM-W (the computerized form of RAM-W™) and SEMS™
- Additional RAMCAP-consistent tools have followed including PARRE

RAMCAP Overview

- RAMCAP is a process for analyzing and managing the risks associated with malevolent attacks and naturally occurring hazards against critical infrastructure
- Provides consistent, efficient, and technically sound methodology:
  - To identify, analyze, quantify, and communicate the level of risk and resilience
  - To measure risk reduction

7-Step RAMCAP Process



Step 1. Asset Characterization

- Which assets are most critical?
- Purpose is to determine the assets that, if compromised, could result in prolonged or widespread service interruption, degradation, injuries, fatalities, detrimental economic impact, or any combination thereof.
- This step produces a list of critical assets that must be considered in subsequent RAMCAP steps.
- Because the number of assets can be substantial, the analysis team may undertake an initial ranking and screening to quickly identify the highest priority assets.

Step 2. Threat Characterization

- Specific reference threat scenarios are included in the Standard
  - Natural events
  - Man-made events
  - Dependency and proximity hazards
- Threats are paired with critical assets
- Uniform set of threats facilitates cross-asset and cross-sector comparison of risk and resilience values

Step 3. Consequence Analysis

- Worst reasonable consequences for each threat-asset pair
  - Fatalities and serious injuries (number of people)
  - Financial consequences to the utility ($)
    - Repair and replacement, abandoning and decommissioning, site and environmental cleanup, revenue losses while service is reduced, direct liability for casualties, fines for environmental damage, etc…
  - Economic impacts to the area in terms of direct and indirect expenses ($)
    - Direct losses include length of time, quantity, and sometimes quality of service denied may cause economic consequences to the community.
    - Indirect losses may include reduced economic activity in general called the "ripple effect."
    - How resilient the community, how well consumers cope with denial of service, affects the degree of loss.

Step 4. Vulnerability Analysis

- The probability that the estimated consequences would result if a certain hazard occurred.
- In the case of a malevolent attack, this is the probability that the attack would successfully result in the estimated consequences.
- This analysis involves an examination of existing security capabilities and structural components, as well as countermeasures/mitigation measures and their effectiveness in reducing damages from threats or hazards.

Step 5. Threat Analysis

- The threat analysis produces the probability that a particular threat will occur in a year.
  - **Malevolent attacks**- threat analysis is based on the adversary's objectives and capabilities and attractiveness of the facility relative to alternative targets.
  - **Natural hazards**- threat analysis is based on historical records for the specific location of this asset and trends for the future.
  - **Dependency hazards**- threat analysis is based on local historical records for the frequency, severity, and duration of service denials.
  - **Proximity hazards**- threat analysis is based on the local situation and historical records for frequency, severity, and duration of service denials.

Step 6. Risk/Resilience Analysis

- Calculate risk for each threat-asset pair as the product of the results from the Consequence Analysis (Step 3), the Vulnerability Analysis (Step 4), and the Threat Analysis (Step 5)
- Risk = Consequences x Vulnerability x Threat Likelihood

Step 7. Risk/Resilience Management

- Decide whether actions are needed to enhance the all-hazards risk management or resilience, consider their cost-benefit and, if needed, decide on an implementation plan
- Examples include establishing or improving security countermeasures, improve consequence mitigation tactics, build in redundancy, enter into mutual aid agreements, create/update emergency response plans, etc.
- Asset Resilience = Duration x Severity x Vulnerability x Threat Likelihood
- Economic resilience is measured for both the utility and the community

The J100 Appendices

- In addition to the mandatory appendix on reference threats, there are numerous non-mandatory appendices
- Provides overall guidance on using the standard
- Includes a tool to help estimate the likelihood of terrorism
- Facilitates analysis of natural hazards risk for earthquake, hurricane, tornado, and flood
- Can add other events as appropriate

Other critical standards include

- ANSI / AWWA G430 – 14: Security Practices for Operation and Management
- ANSI / AWWA G440-11: Emergency Preparedness Practices

GRADIENT PLANNING

Benefits of RAMCAP implementation

- Serves as a guidance document for assessing risk
- Addresses all hazards
- Helps support resource allocations when funding is finite
- Can assist with the design and implementation of mitigation measures
- Uses a methodology common to DHS and other critical infrastructure sectors
- Demonstrates proactive preparation to minimize the consequences of natural, malevolent, dependency and proximity events

Risk and resilience management is a continuous process

- Repeat the risk analysis cycle at least every 5 years per AWWA G440-11, Emergency Preparedness Practices
- Review and update sooner as new hazards and threats emerge, when new facilities are constructed or removed from service, and when other changes occur that would significantly the risk assessment

Embark on a path of continuous learning:

- Embrace the NEWEA position paper on WARN,
- Attend the NEWEA specialty conference on Managing Risk & Resiliency in April, and
- Invest in knowledge, strong relationships, and established, risk-based methodologies to minimize future losses and keep your reputation untarnished.

GRADIENT PLANNING

Questions?

Marian H. Long, P.E.
Gradient Planning, LLC
mlong@gradientplanning.com
207-939-0101