All-Hazards Risk and Resilience Assessment for Wastewater Utilities

NJWEA 2022 Annual Conference

Sebastian Malter, CC-P
Lauren Miller, CC-P
Agenda

- Introduction
- Methodology
- Risk and Resilience Project Framework
- Fauquier County Water & Sewer Authority Example
- Conclusion
- Q&A

www.epa.gov/waterresilience
Introduction
Risk and Resilience

**Alert (AA21-042A)**

**Compromise of U.S. Water Treatment Facility**

Original release date: February 11, 2021 | Last revised: February 12, 2021

Summary

Indictment underscores the potential for remote intrusions to have fatal consequences.

POISONING THE WELL —

Feds say man broke into public water system and shut down safety processes

Dan Goodin - 4:47 PM

Fort Frances crews attempt to pump water out of the White Pine Lift Station, which stopped working during the weekend’s storm. The exact problem hasn’t been identified, as crews have been unable to access the pump to find out why it stopped working. (Craig Miller/Provided)
America's Water Infrastructure Act (AWIA)

- Signed: October 23, 2018 and amends the Safe Drinking Water Act (SDWA)
- New requirements:
  1. Risk and Resilience Assessment
  2. Emergency Response Plan
- Community water systems serving over 3,300 people (directly or indirectly)
- Update/certify both documents every five years

**Risk and Resilience Assessment**

- Population served ≥100,000
  - Due: March 31, 2020

- Population served 50,000-99,999
  - Due: December 31, 2020

- Population served 3,301-49,999
  - Due: June 30, 2021

**Emergency Response Plan**

- No later than six months after certifying the Risk and Resilience Assessment (June 30, 2020)
Purpose of All Hazards Risk and Resilience Assessments

Evaluate
• The risk and resilience of community water systems to natural hazards and malicious acts.

Prepare
• Utilities to respond to natural hazards and malicious acts.

Protect
• The public from natural hazards and malicious acts that may occur at community water & wastewater systems.
Methodology
Risk & Resilience Assessment Methodology

Risk Analysis and Management for Critical Asset Protection

1. Asset Characterization
2. Threat Characterization
3. Consequence Analysis
4. Vulnerability Analysis
5. Threat Analysis (Likelihood)
6. Risk Analysis \( R = C \times V \times T \)
7. Risk Management \( (B:C) \)

Result: Quantified Risk Scores
Risk & Resilience Assessment Methodology

Risk ($) = Threat Likelihood (%) x Consequence ($) x Vulnerability (%)

Threat Likelihood (%)
- How likely a given threat is to occur in a given year; a percentage value ranging from nearly zero (very unlikely to occur) to one (almost certain to occur).

Consequence ($) 
- The worst reasonable consequence to an asset, assuming a threat does occur; a dollar value.
- For most threats: Consequence = Cost of Temporary Measure/ Equipment + Cost from Fatalities + Cost from Injuries + Repair/Replacement

Vulnerability (%)
- An assessment of the utility’s preparedness ahead of time for the threat, whether it will be able to respond during or immediately after the threat, and if the utility would be able to fully recover from the threat; a percentage value ranging from 0.001 (least vulnerable) to 1 (most vulnerable).
- For most threats: Vulnerability = Preparedness x Active Response x Recovery

Values from EPA, FEMA or AWWA guidance.
Values will be determined based on: workshop input, data collected, site visits, engineering judgement, best practices.
## Risk & Resilience Assessment Methodology

- **CDM Smith’s Risk and Resilience RRA Tool**

### Risk and Resilience Assessment (RRA) Tool

**To facilitate compliance with America’s Water Infrastructure Act (AWIA)**

---

**Disclaimer**

The opinions, conclusions, and recommendations contained in this report and Client’s implementation of any recommended changes are meant to reduce the risk to the Client’s facilities from natural hazards and malvolent acts but will not eliminate the risk entirely. CDM Smith does not make and hereby disclaims all warranties and guarantees including but not limited to any warranty/guarantee that Client will not experience or be impacted by a natural hazard or malvolent act at its facilities described in this report either before or after the implementation of recommendations provided by CDM Smith.

### Intent

This tool is intended to be used to complete a Risk and Resilience assessment to facilitate compliance with the American Water Infrastructure Act (AWIA). The tool is designed to assist the utility track which of their assets are critical to fulfill their mission and determine which of these critical assets are at risk to threats posed by malvolent acts and natural hazards as required by AWIA based on existing measures in place related to preparedness, active response, and recovery. Each threat-specific risk assessment is located in an individual tab to allow the user to choose which threat to assess. Once all relevant risk assessments have been completed, the Risk Summary tab provides an overview of the critical assets that are most at risk and to which threat. The Utility Resilience Index includes a utility-wide resilience score to reflect the utility’s overall ability to absorb or cope with an incident. The tool has been designed following the process and intent of the American Water Works Association.
Risk & Resilience Assessment
Project Framework
Risk and Resilience Project Framework

- Data Collection & Review
- Threat Asset Pairing
- Stakeholder Engagement Workshops
- Risk & Resilience Assessment
- Results & Prioritization
Data Gathering and Review

- GIS/asset management program for water system assets
- Locations and facility descriptions of water system assets
- Near-term capital projects
- As-built drawings of critical facilities
- Past events (e.g., after-action reports)
- Local hazard mitigation plans
- Previously prepared vulnerability or risk assessments
- Previously prepared Business Continuity and/or Emergency Response Plans (ERP) and associated annexes.
Threats: Malevolent Acts*

- Assault on Utility - Physical
- Theft or Diversion – Physical
- Contamination
- Sabotage – Physical
- Cyber Attack
  - Business Enterprise Systems
  - Process Control Systems

Threats: Natural Hazards*

- Drought
- Earthquake
- Extreme temperatures (heat and cold)
- Flooding
- Pandemic
- Wind related hazards
- Wildfires

Asset Types

- **Operations-Treatment**
  - Wastewater treatment plants and related assets (shop areas, plant buildings, etc.)
  - Power supply

- **Operations-Collection**
  - Collection piping
  - Lift stations

- **Operations Personnel**

- **Finance and Accounting**
  - Billing, payroll, third-party suppliers
  - Personnel

- **Information Technology**
  - SCADA
  - Enterprise Servers & laptops/ workstations
Example of a Threat-Asset Pair

- **Asset:** Bat Computer (which includes the SCADA system for the Bat Cave!)
- **Threat:** Cyber Attack on Process Control Systems
Threat-Asset Pairs

**List of Typical Assets**
- Wastewater Treatment Plants
- Pump & Lift Stations
- Power Supply (Incl. Back Up Power)
- Collection & Conveyance
- Administrative Buildings & Maintenance Facilities
- SCADA
- IT & Communication Systems
- Personnel

**Natural Hazards**
- Pandemic
- Drought
- Extreme temperatures (Heat & Cold)
- Flooding
- Wind events
- Wildfires
- Earthquakes

**Malevolent Acts (recommended by EPA)**
- Assault on Utility
- Contamination
- Cyber Attack
  - Business Enterprise Systems
  - Process Control Systems
- Sabotage
- Theft or Diversion
Develop Threat-Asset Pairs Matrix

<table>
<thead>
<tr>
<th>Asset ID</th>
<th>Asset Name</th>
<th>Malevolent Threats (Based on EPA Threat Categories)</th>
<th>Natural Hazards*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Assault on Utility - Physical</td>
<td>Contamination of Wastewater</td>
<td>Cyber-attack on Business Enterprise Systems</td>
</tr>
<tr>
<td>Operations - Treatment 1</td>
<td>Marshall WWTP-Headworks</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 2</td>
<td>Marshall WWTP - Spillway Basin</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 3</td>
<td>Marshall WWTP - Notification Reactors &amp; Secondary Clarifiers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 4</td>
<td>Marshall WWTP - UV Disinfection and Cascade Aeration</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 5</td>
<td>Marshall WWTP - Chemical &amp; Chemical Feed Systems</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 6</td>
<td>Marshall WWTP - Outfall &amp; Effluent Pipeline</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 7</td>
<td>Marshall WWTP - Solids Handling</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 8</td>
<td>Marshall WWTP - Back Up Powerer</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 9</td>
<td>Vint Hill WWTP - Influent PS (New Baltimore Pt #2)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 10</td>
<td>Vint Hill WWTP - Headworks</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 11</td>
<td>Vint Hill WWTP - Sequencing Bench Reactors &amp; Post Equalization</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 12</td>
<td>Vint Hill WWTP - Filtration and Aeration</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 13</td>
<td>Vint Hill WWTP - UV Disinfection</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 14</td>
<td>Vint Hill WWTP - Chemical &amp; Chemical Feed Systems</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 15</td>
<td>Vint Hill WWTP - Sludge Stabilization &amp; Dewatering</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 16</td>
<td>Vint Hill WWTP - Outfall &amp; Effluent Pipe</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 17</td>
<td>Vint Hill WWTP - Back Up Powerer</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 18</td>
<td>Remington WWTP - Preliminary Treatment &amp; Septage Receiving</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 19</td>
<td>Remington WWTP - Aeration Tanks (Schroeder Tanks) &amp; Secondary Clarifiers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 20</td>
<td>Remington WWTP - Post Aeration</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 21</td>
<td>Remington WWTP - Disinfection &amp; Effluent Monitoring</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 22</td>
<td>Remington WWTP - Chemical &amp; Chemical Feed Systems</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 23</td>
<td>Remington WWTP - Outfall &amp; Effluent Pipe</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Operations - Treatment 24</td>
<td>Remington WWTP - Solids Handling Systems</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operations - Treatment 25</td>
<td>Remington WWTP - Back Up Powerer</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

For every critical asset, identify which threats have a potential High-Consequence: Yes, No, TBD
Purpose of the Risk and Resilience Workshop

Collaborate
- To provide input to the risk and resilience assessments while creating useful documentation for participants

Validate
- The vulnerabilities and consequences from threats to critical assets to inform the Risk and Resilience Assessment

Engage
- To reveal opportunities for resilience for each participant in their day to day responsibilities.

“The biggest difficulty in this exercise will be prioritizing limited resources to all of the areas of risk.”
Which malevolent acts or natural hazards are you most concerned about?

- Sabotage
- Theft
- Contamination
- Physical assault
- Cyber attack

“Attack on our treatment facility, we are in a remote area”

“Physical damage or harm to people and property”

“Security of facilities has been ignored for years, unless there is a forced project.”
Stakeholder Engagement Workshops

Put your Leadership Hat on and think into the future...

- What critical assets are *most* vulnerable in your opinion?
- Why and how are they vulnerable?
- Based on these vulnerabilities, what are the possible “worst reasonable case” consequences that could occur?
Stakeholder Engagement Workshops

- Document how past events challenged the system?
- Capture and document Institutional Knowledge
- Consider “What if” impacts beyond recent experience to fully understand the impact of specific threats on utility business functions
Risk and Resilience Project Framework

Data Collection & Review
Threat Asset Pairing
Stakeholder Engagement Workshops
Risk & Resilience Assessment
Results & Prioritization

Example: Fauquier County
Case Study: Fauquier County
Utility Overview

- Fauquier County Water and Sanitation Authority
- 4,600 service connections
- 96 miles of sanitary sewer mains
- Fifteen (15) sanitary sewer lift stations
- Three (3) main systems
  - Marshall
  - Remington
  - Vint Hill
Assets

- Operations-Treatment
  - 3 wastewater treatment plants and related assets (shop areas, plant buildings, etc.)
  - Power supply

- Operations-Collection
  - Collection piping
  - 15 Lift stations

- Operations Personnel

- Finance and Accounting
  - Billing, payroll, third-party suppliers
  - Personnel

- Information Technology
  - SCADA
  - Enterprise Servers & laptops/ workstations
Threats

**Malevolent Acts:**
- Assault on Utility - Physical
- Contamination
- Theft or Diversion – Physical
- Cyber Attack
  - Business Enterprise Systems
  - Process Control Systems
- Sabotage – Physical

**Natural Hazards:**
- Drought
- Earthquake
- Extreme temperatures (heat and cold)
- Flooding
- Pandemic
- Wind related hazards
## Threat Asset Pairs

<table>
<thead>
<tr>
<th>Response Team Asset Grouping</th>
<th>Total Assets</th>
<th>Top / High Criticality Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations - Treatment</td>
<td>38</td>
<td>35</td>
</tr>
<tr>
<td>Operations – Conveyance</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>Finance and Accounting</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Information Technology</td>
<td>14</td>
<td>13</td>
</tr>
</tbody>
</table>

| 79 Total                          | 74 Evaluated |

- **Total of**
  - 74 Critical Assets Evaluated
  - 421 “Threat Asset Pairs” Evaluated
Example Calculation – Sabotage on Wastewater Lift Station

Threat Likelihood

- Threat likelihood is 0.05

Consequence ($)

- The **worst-case scenario** is intentional sabotage or damage of pump controls or other pump equipment. Perpetrated by insider or outsider.
- Temporary measure: FCWSA temporary bypass pump can be installed while pump is rehabilitated.

- EPA Guidance

- 60 days of downtime
- $0 cost of temporary measure
- $110,000 repair/replacement costs
**Example Calculation – Sabotage on Wastewater Lift Station**

**Threat Likelihood (%)**
- Threat likelihood is 0.05

**Consequence ($)**
- The worst-case scenario is intentional sabotage or damage of pump controls or other pump equipment. Perpetrated by insider or outsider.
- Temporary measure: FCWSA temporary bypass pump can be installed while pump is rehabilitated.

**Vulnerability (%)**
- **Vulnerability = Preparedness x Active Response x Recovery**
- Preparedness: This site is not secured with a fence; lift station is not housed in a building; an intruder would have full access to every control panel; locks on the wet well hatches and control panel; site is equipped with an alarm system; two pumps are required to handle the average flow.
- Active Response: Use temporary bypass pump until pump station operation can resume; generator is at the site with sufficient fuel for a week; FCWSA has contracts with electricians, septage haulers, generator vendors and SCADA contractor.
- Recovery: Total recovery is anticipated.

- 5% Likelihood
- 60 days of downtime
- $0 cost of temporary measure
- $110,000 repair/replacement costs
- Little preparation
- Strong response
- Strong recovery

**Risk Score: $55**
Example Calculation – Sabotage on Wastewater Lift Station
Example Calculation – Flood Risk at Lift Station

Threat Likelihood (%)

- Lift Station is in the 100-year FEMA floodplain

Consequence ($)

- An assessment of the utility’s preparedness ahead of time for the threat, whether it will be able to respond during or immediately after the threat, and if the utility would be able to fully recover from the threat; a percentage value ranging from 0.001 (least vulnerable) to 1 (most vulnerable).

- For most threats: Vulnerability = Preparedness x Active Response x Recovery

Example Calculation – Flood Risk at Lift Station

1.0% Likelihood
Example Calculation – Flood Risk at Lift Station

Threat Likelihood (%)
- Lift Station is in the 100-year FEMA floodplain

Consequence ($)
- Damage to above ground equipment, in particular pump motors and electrical equipment

- 1.0% Likelihood

- 7 Days downtime,
- $0 cost of temporary measure
- $220,000 repair/replacement costs
Example Calculation – Flood Risk at Lift Station

**Threat Likelihood (%)**
- Lift Station is in the 100-year FEMA floodplain

**Consequence ($)**
- Damage to above ground equipment, in particular pump motors and electrical equipment

**Vulnerability (%)**
- *Vulnerability = Preparedness x Active Response x Recovery*
  - Preparedness: Electrical equipment is in electrical building and elevated; back-up generator is on site; no additional flood protection measures on site.
  - Active Response: If damaged use temporary bypass pump until pump station operation can resume; generator is at the site with sufficient fuel for a week; FCWSA has contracts with electricians, septage haulers, generator vendors
  - Recovery: Total recovery is anticipated.

- **1.0% Likelihood**
- **7 Days downtime,**
- **$0 cost of temporary measure**
- **$220,000 repair/replacement costs**

- **Moderate Preparation**
- **Strong Response**
- **Strong Recovery**

**Risk Score: $110**
Example Calculation – Flood Risk at Lift Station
FCWSA Lessons Learnt

- Natural Hazards typically higher risks due to higher likelihoods compared to malevolent acts
- Assets most at risks are:
  - Personnel
  - Biological treatment of WWTPs
  - Electrical & control equipment
  - Higher criticality lift stations
  - Vint Hill WWTP (batch reactors & post equalization)
- Factors contributing to higher level of preparation & response
  - Cross-training of staff
  - Ability to manually run plants & bypass pump stations
  - Spare parts, back-up power, emergency contracts & temporary pumps

Vint Hill WWTP
Conclusion
Conclusion

A comprehensive risk assessment can...

- Help utilities to identify vulnerabilities and prioritize actions
- Identify risks that are easily reduced or eliminated
- Clarify what is known and unknown about critical assets
A comprehensive risk assessment can...

- Provide an objective basis for decisions on controlling risks
- Provide opportunities for staff engagement and awareness raising
- Provide basis for funding opportunities, for example
  - FEMA funding
  - Bipartisan Infrastructure Bill

"Makes the largest investment in clean drinking water and waste water infrastructure in American history..."
Questions?

Sebastian Malter, CC-P
CDM Smith
malters@cdmsmith.com