Utility System Security and Fort Future

Vicki L. Van Blaricum

U. S. Army ERDC-CERL, Champaign, IL

Presented for:

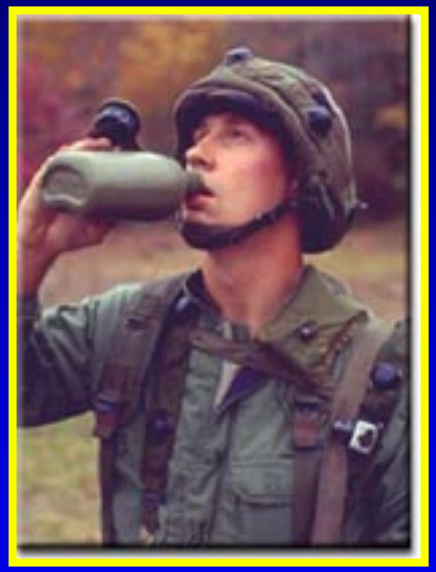
2004 Geospatial Technology Symposium & Exposition

18 August 2004

Utility systems <u>enable</u> key installation functions

Force Projection

Training



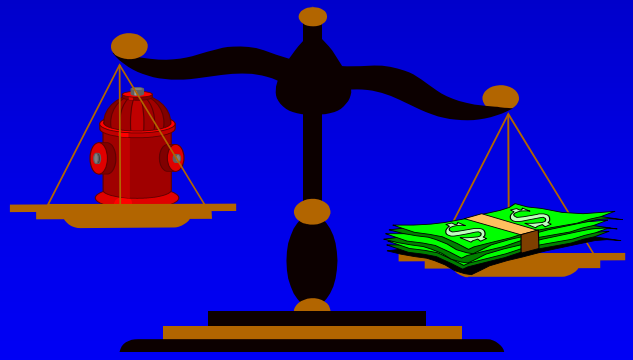
Daily activities

What is the "mission" of a utility system? The system must be:

Sufficient to meet demand– both normal and "surge"

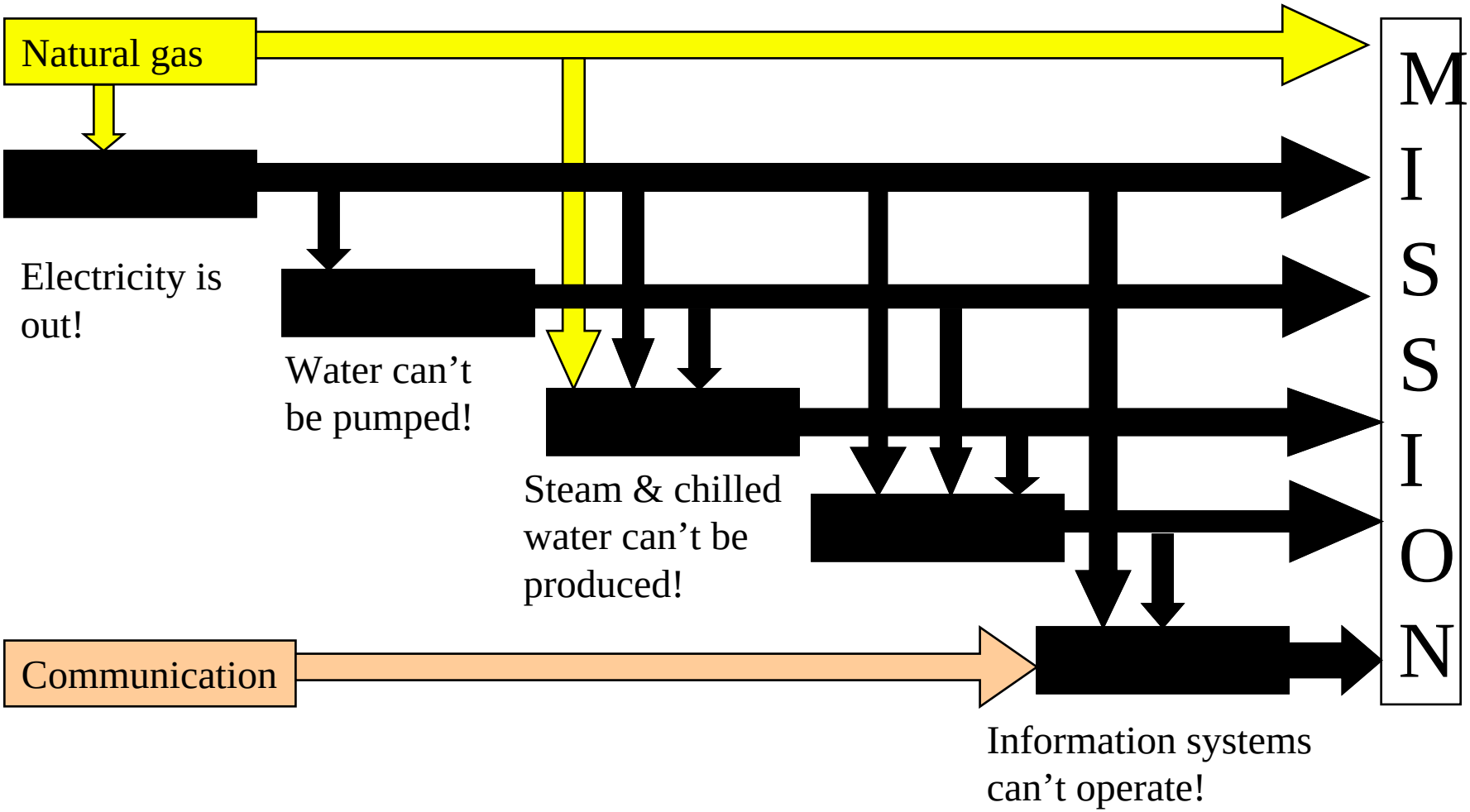
Reliable– always there when it's needed

Safe – does not cause harm



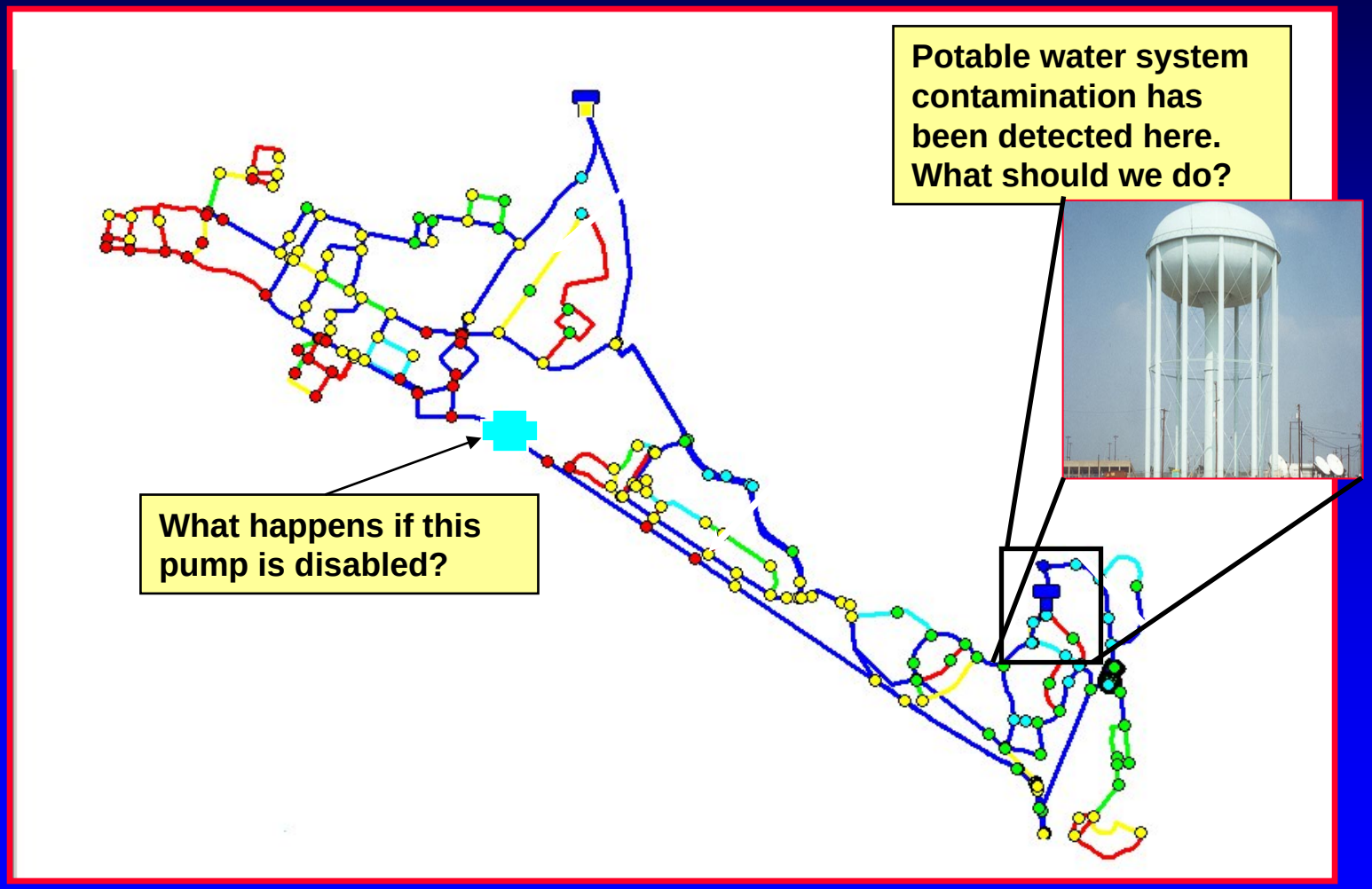
Affordable– a balance between cost & service

Utility systems are highly interdependent--disruption of one utility service often causes disruption of the others.



Force Protection

Utility systems are potential targets to terrorists.



Security and Risk

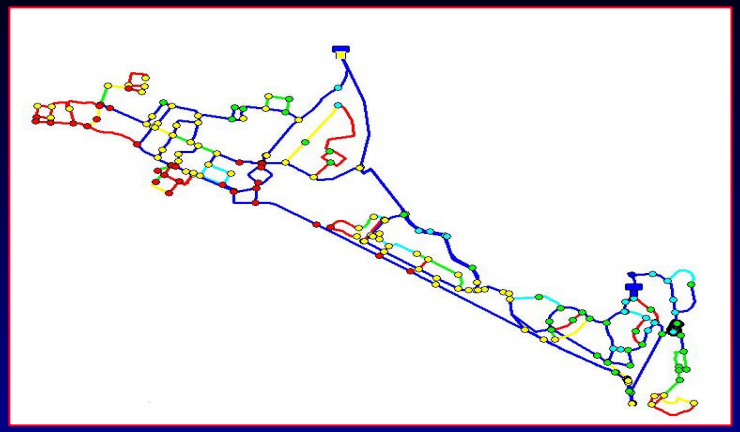
- Decisions must be made because we don't have the resources to protect everything from everything.
- Risk assessment methods seek to help:
  - Sort through all the possibilities and focus on what's important
  - Identify and analyze courses of action for situations where the risk is unacceptably high

The problem with assessing risk in utility systems

Engineering knowledge and quantitative data are required to understand how a specific utility system operates…..

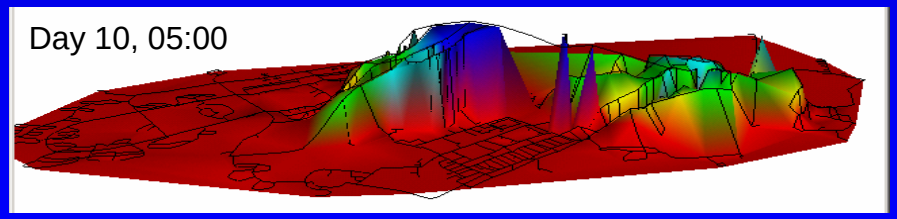
…HOWEVER, traditional risk assessment methods are:

- Primarily based on subjective judgments and knowledge of system operator
- Focused on physical security
- Semi-quantitative at best



Proposed solution:

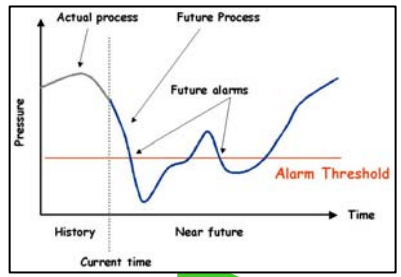
Use engineering models of utility systems to support various steps of the risk assessment process



Some background on types of utility system modeling

Steady state model:
"Snapshot" at one point in time

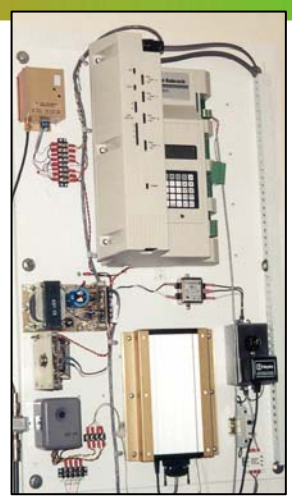
On-line dynamic model
Data is obtained from SCADA and model is updated once a day.



Accuracy, functionality and reliability of method

Problem-solving by experience:
"Seat of the pants" methods for dealing with new situations/ problems

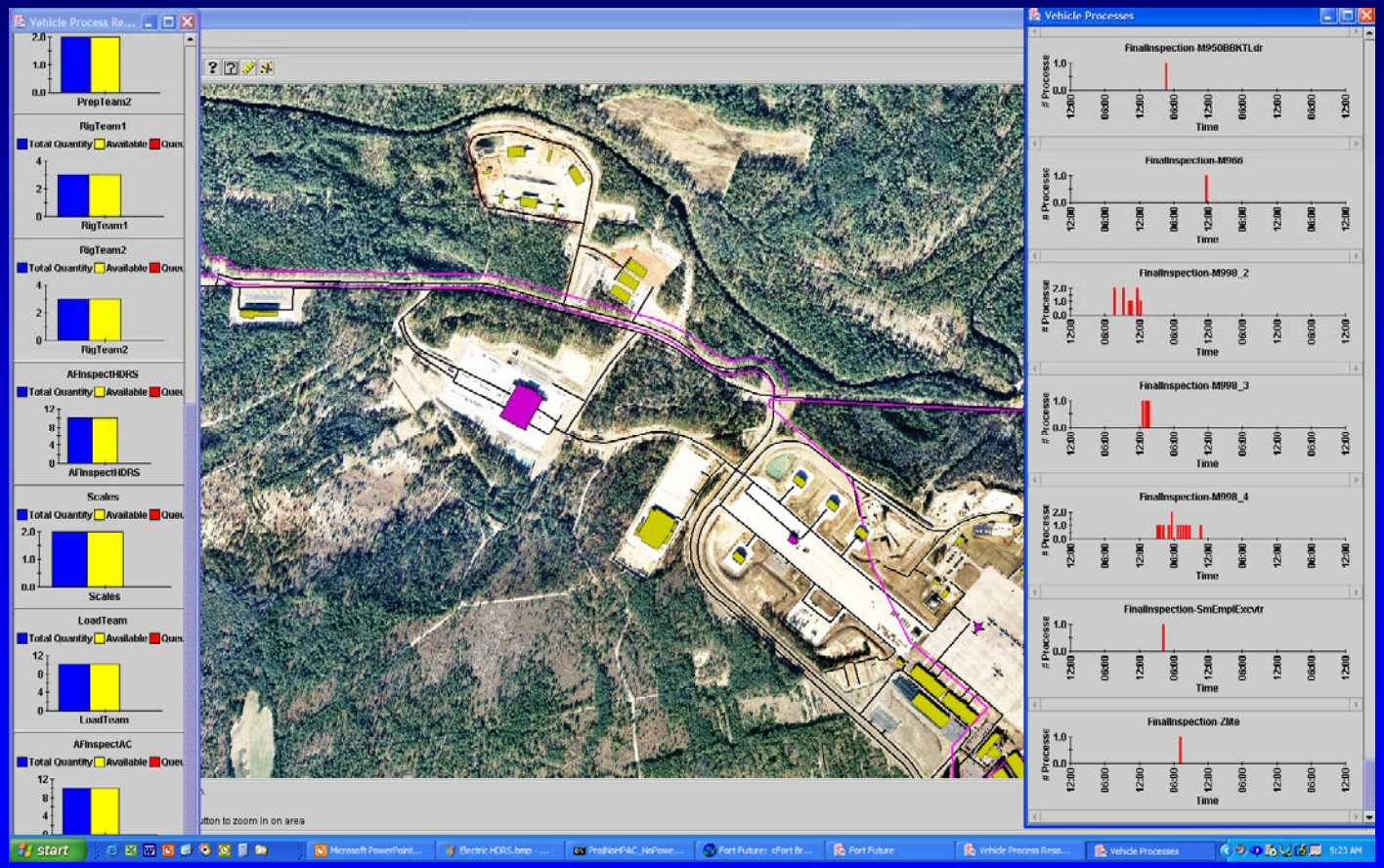
Off-line dynamic model: **Time-varying processes can be modeled but data is input manually**



"Real-time" dynamic model
Model updated with SCADA data at intervals of 15 minutes or less.

The Fort Future Virtual Installation

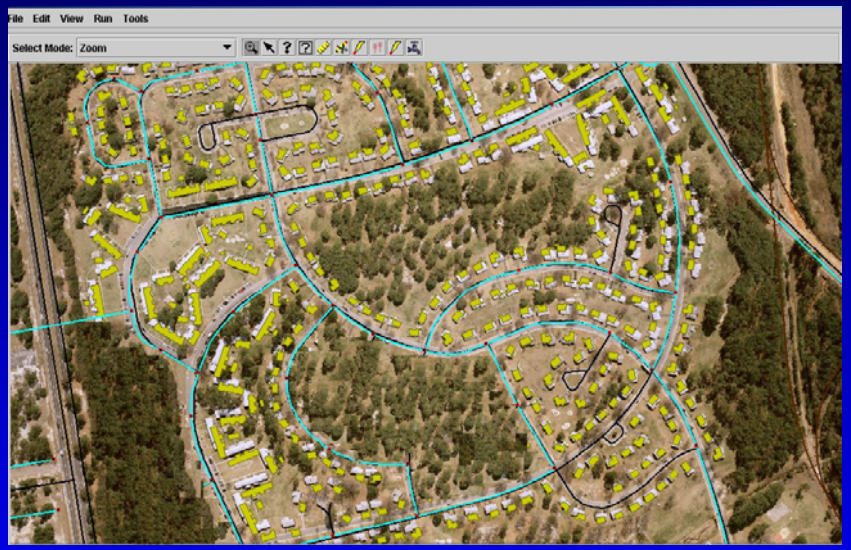
- Computable model of any geographic location
- Allows overlay of processes onto infrastructure (including utility systems)

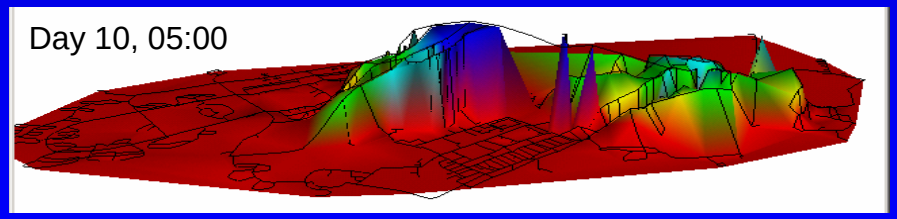


Utilities Models in the Virtual Installation

Water, Power, Fuel

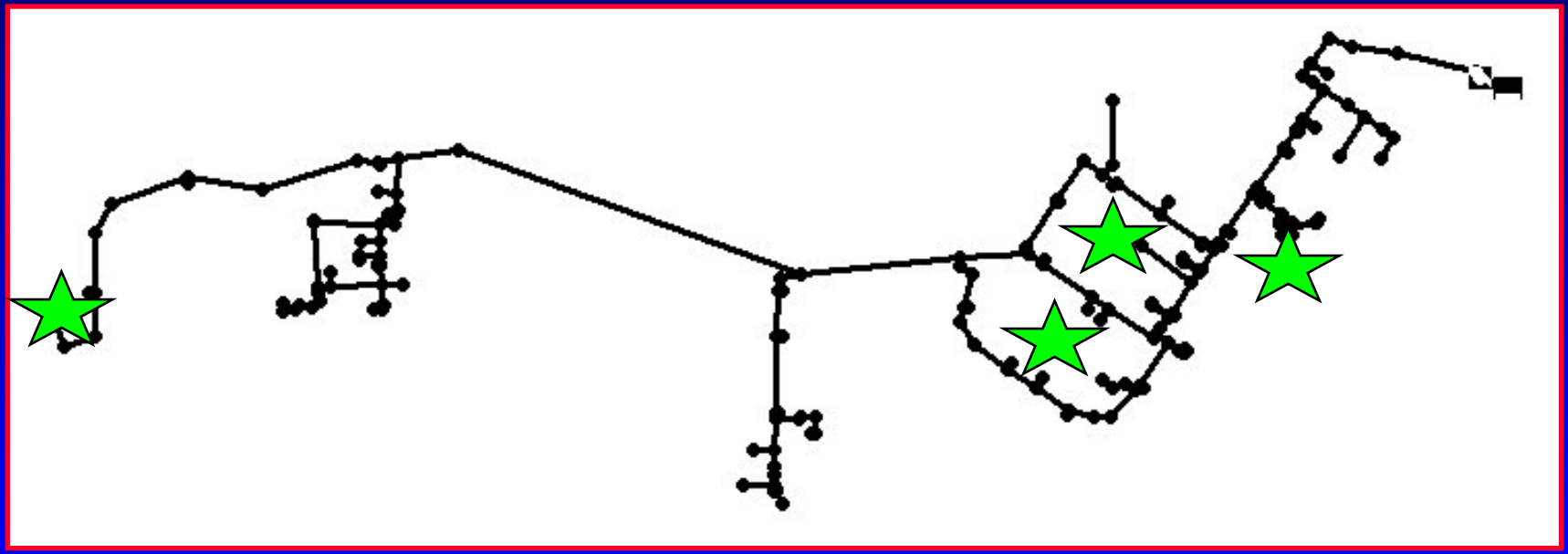
- Virtual model of "as-is" Utilities distribution systems
- Simulate utility system behavior:
  - Capacity issues
  - Interruption or denial of utility service
  - Contamination events (water and fuel)
- Test alternative solutions to problems and plan responses to emergencies
- Link with live sensors (future)





Spread of contaminants or other substances can be predicted.

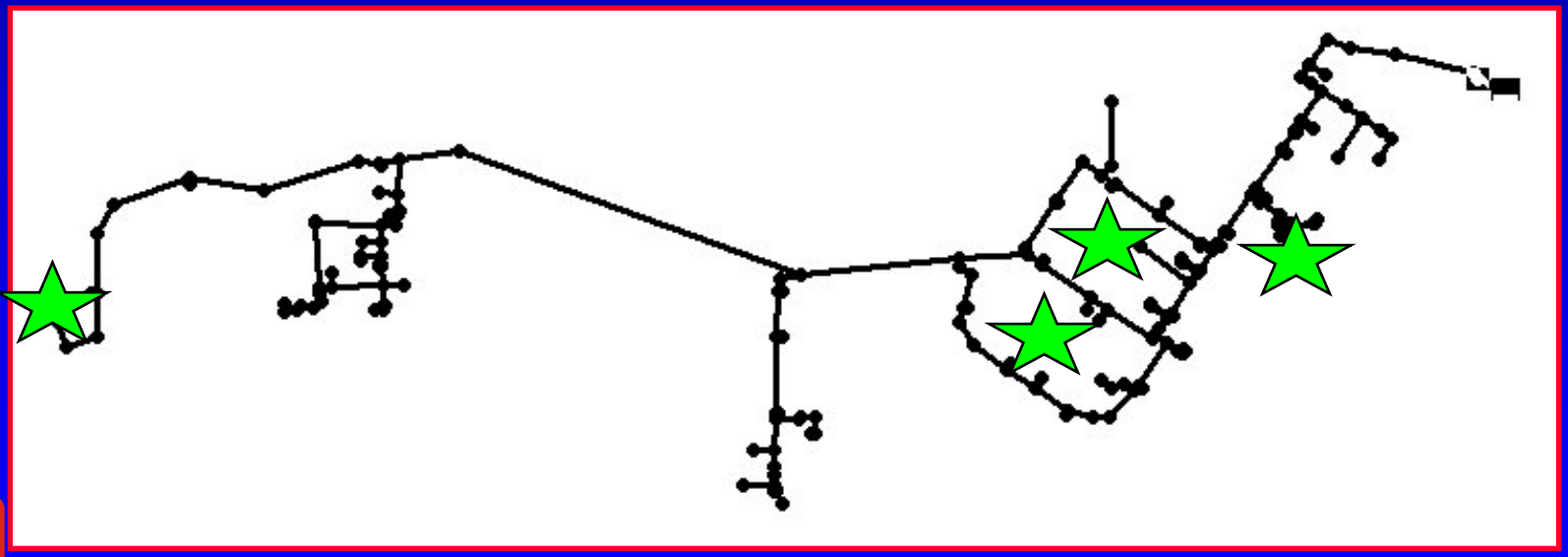
Example water system



★ = Building that is critical to the installation's mission

Step 1: Identify mission criteria of utility system.

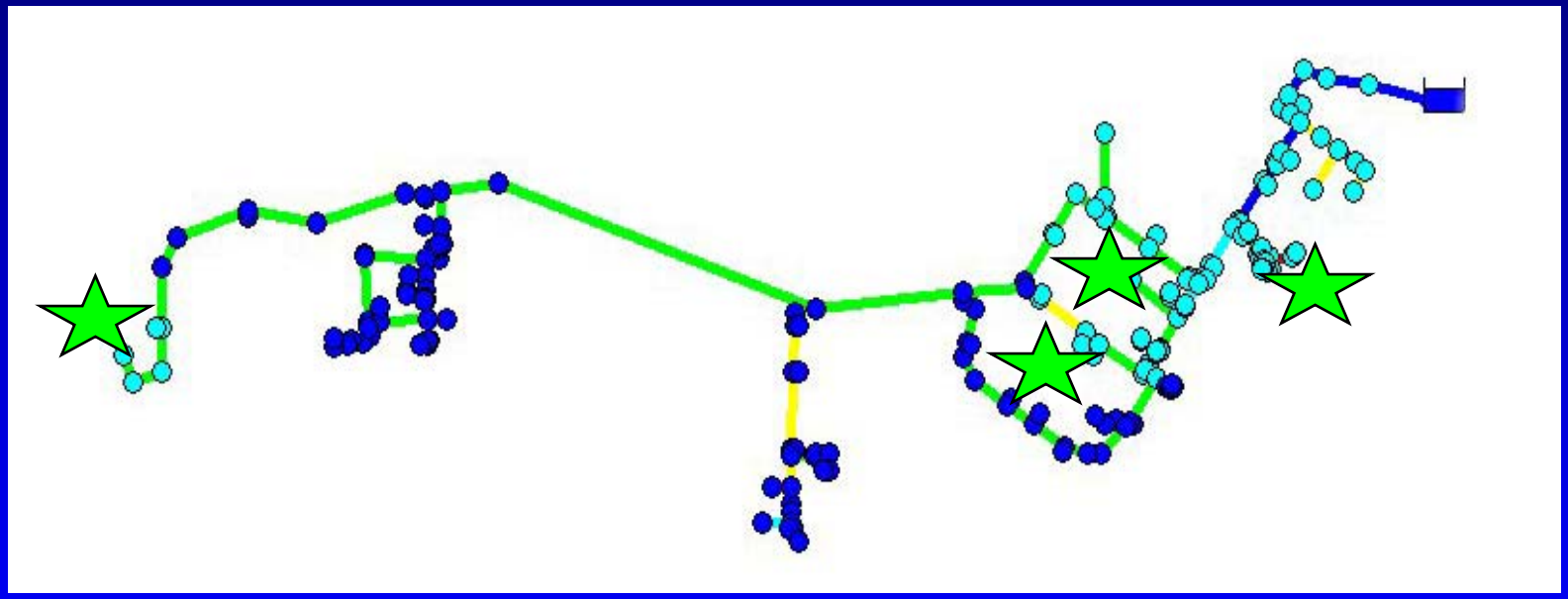
- Ensure adequate water pressure for operation of fire suppression systems
- Furnish adequate pressure and quantity of water to support work in critical buildings
- Provide safe drinking water



Step 2: Identify & prioritize critical assets

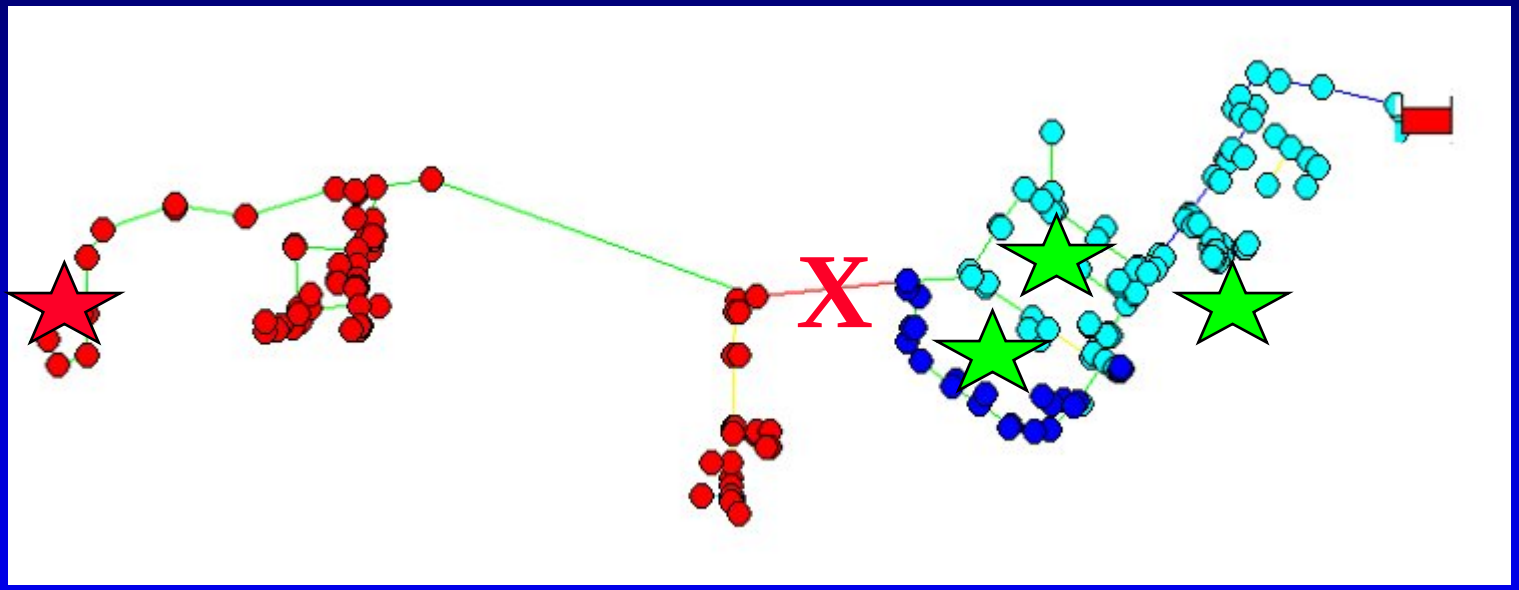
- Critical asset = utility system component that is critical to mission
- Traditional method: Use interviews with system operators and pairwise comparison
- Improved method: Use the system model to simulate asset loss, then evaluate impact quantitatively against mission criteria.
- Greater impact means higher priority

Normal operation for example system



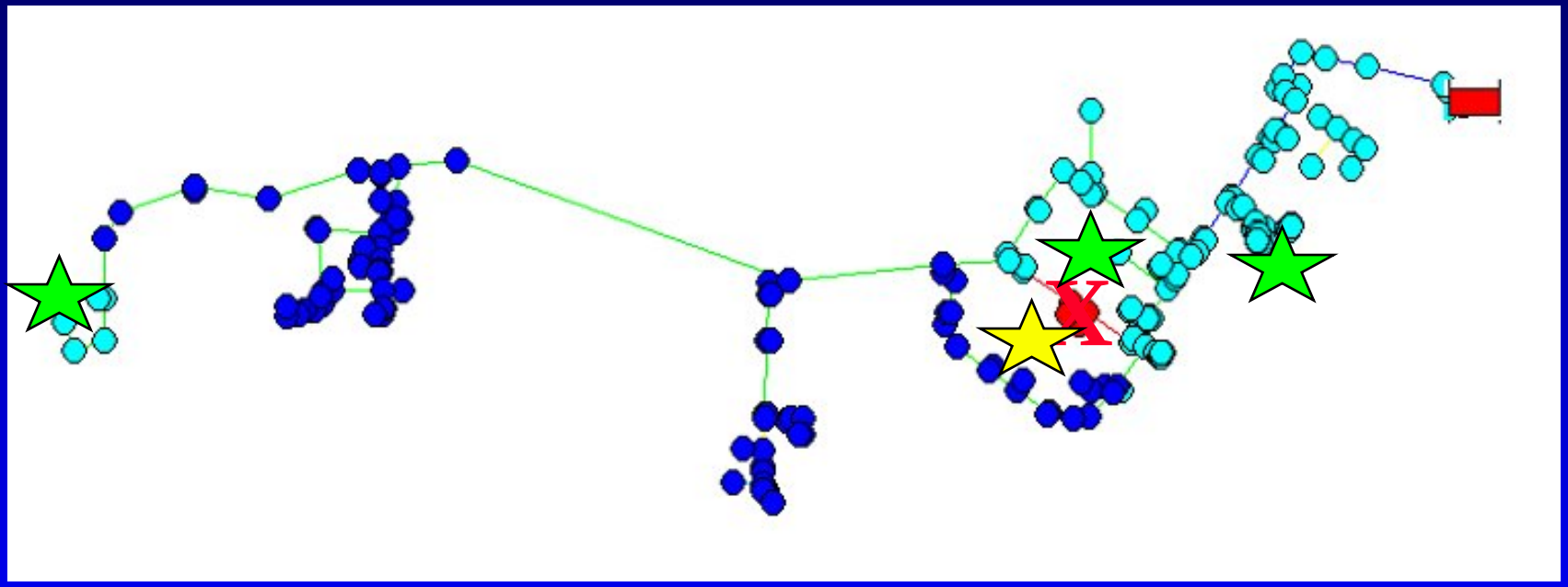
System water pressures and flows are adequate.
Drinking water is safe at all facilities.

Example: Impact assessment of loss of the aboveground water main



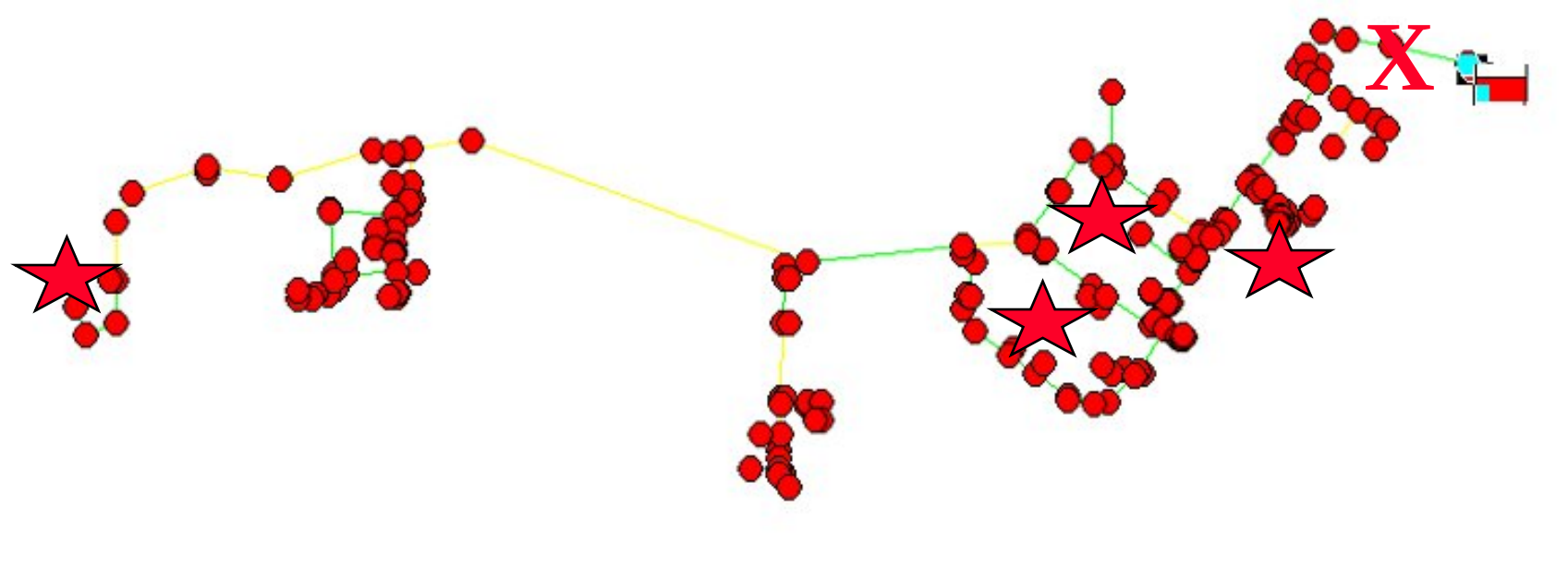
Result: Inadequate pressure at 59 nodes, 1 critical building.

Example: Impact assessment of loss of water main serving critical building



Result: Inadequate pressure at 4 system nodes, including one (but not all) inlets to one critical building.

Example: Impact assessment of loss of the 10 inch water main



Result: Inadequate pressure at all 194 system nodes and all 4 critical facilities. This is the most critical of the assets analyzed.

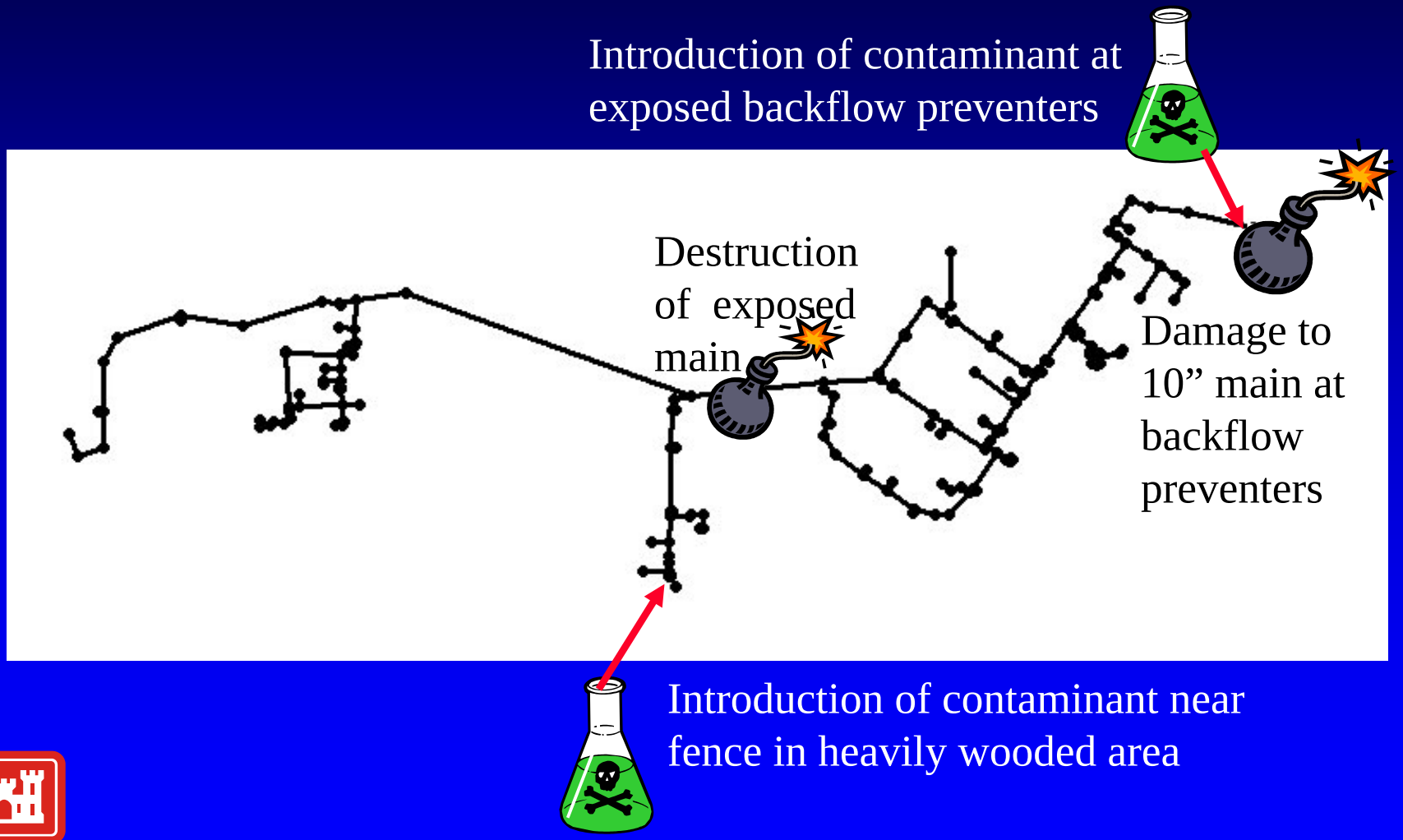
Step 3: Identify likely threats

- Based on available intelligence, law enforcement, and open-source information
- Outsider threat examples: terrorists, protesters, criminals, extremist groups
- Insider threat examples: disgruntled employee seeking revenge, terrorist insider
- Weapons & tactics

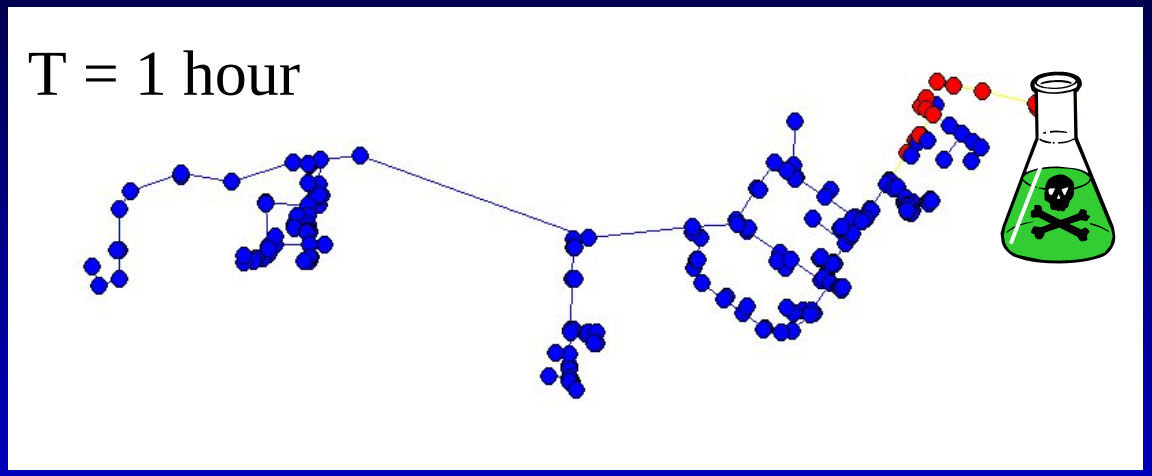
Step 4: Determine consequences of critical asset/threat pairs

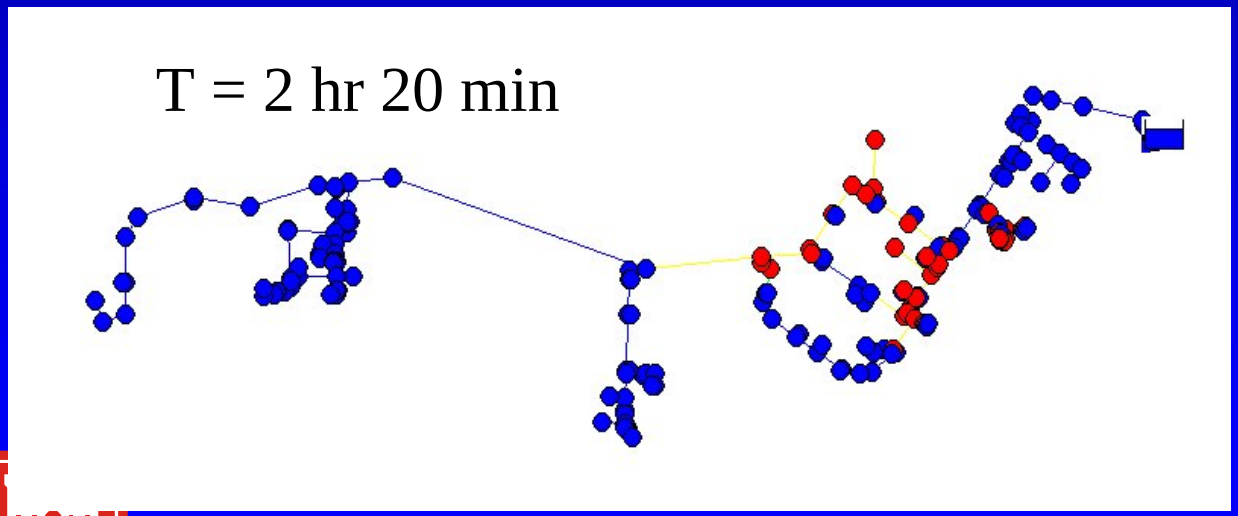
- Some example consequence measures:
  - Number of users impacted
  - Magnitude of mission degradation
  - Value of infrastructure damaged/destroyed
- Traditional method: Interview system operators and ask them to estimate consequences
- Improved method: Use models to simulate attacks and quantify consequences.

Examples of critical asset/threat pairs



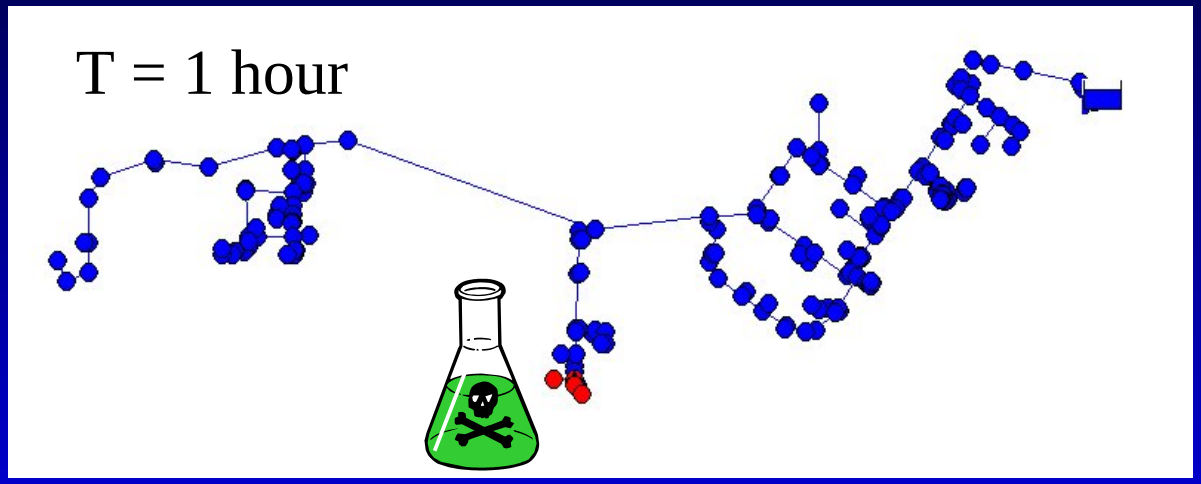
Consequence analysis: Terrorist introduces contaminant at backflow preventers

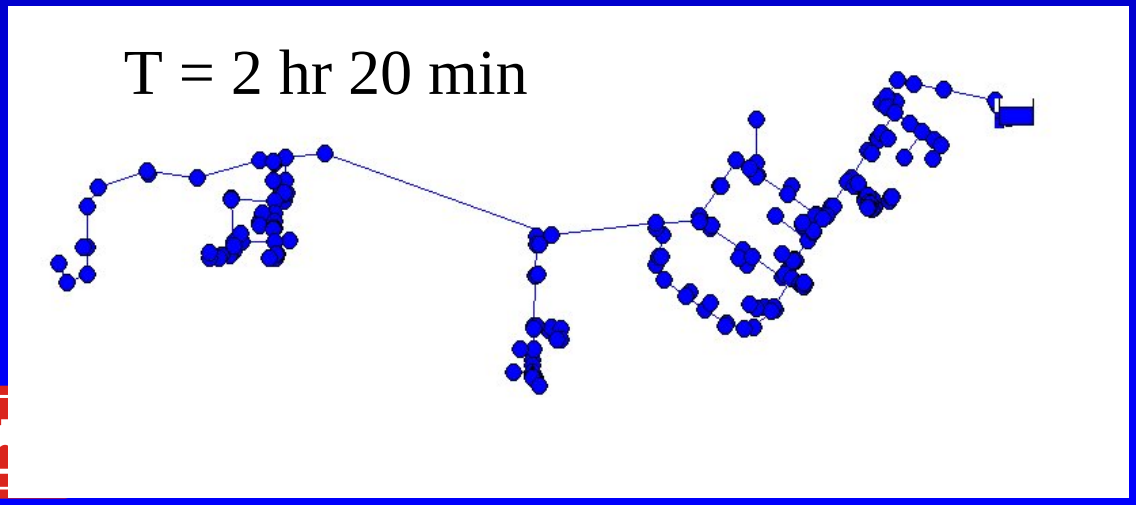




Result: Contaminant spreads throughout entire system over a 12-hour period; all facilities are impacted

Consequence analysis: Terrorist introduces contaminant near fence in wooded area





Result:
Contaminant travel is restricted to 2 small remote buildings before being flushed from the system. Consequence score would be lower than for previous case.

Next steps of assessment process

- **Step 5: Evaluate protection systems currently in place**
- **Step 6: Calculate risk score for each combination of threats and assets. Example: In RAM-W for water systems:**

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

P_A = Potential for adversary attack (threat)

P_E = Effectiveness of protection systems

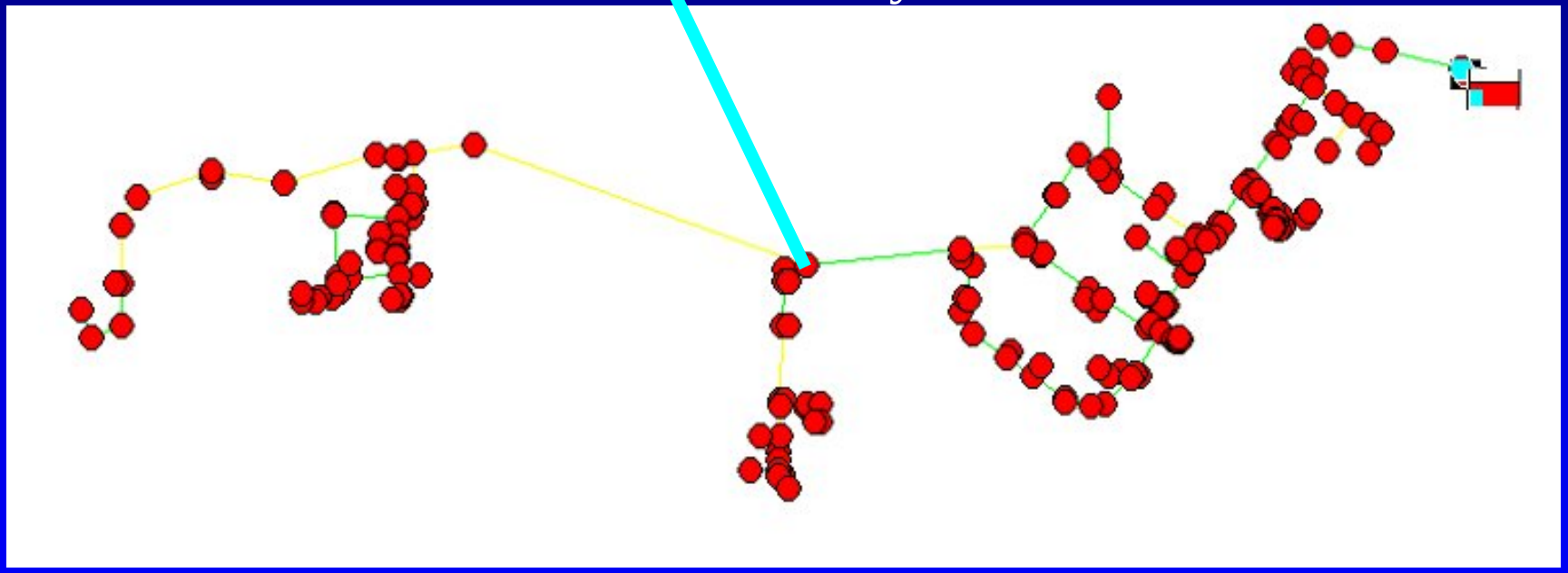
C = Consequence

Step 7: Develop Potential Courses of Action (COA) to Mitigate Unacceptable Risks

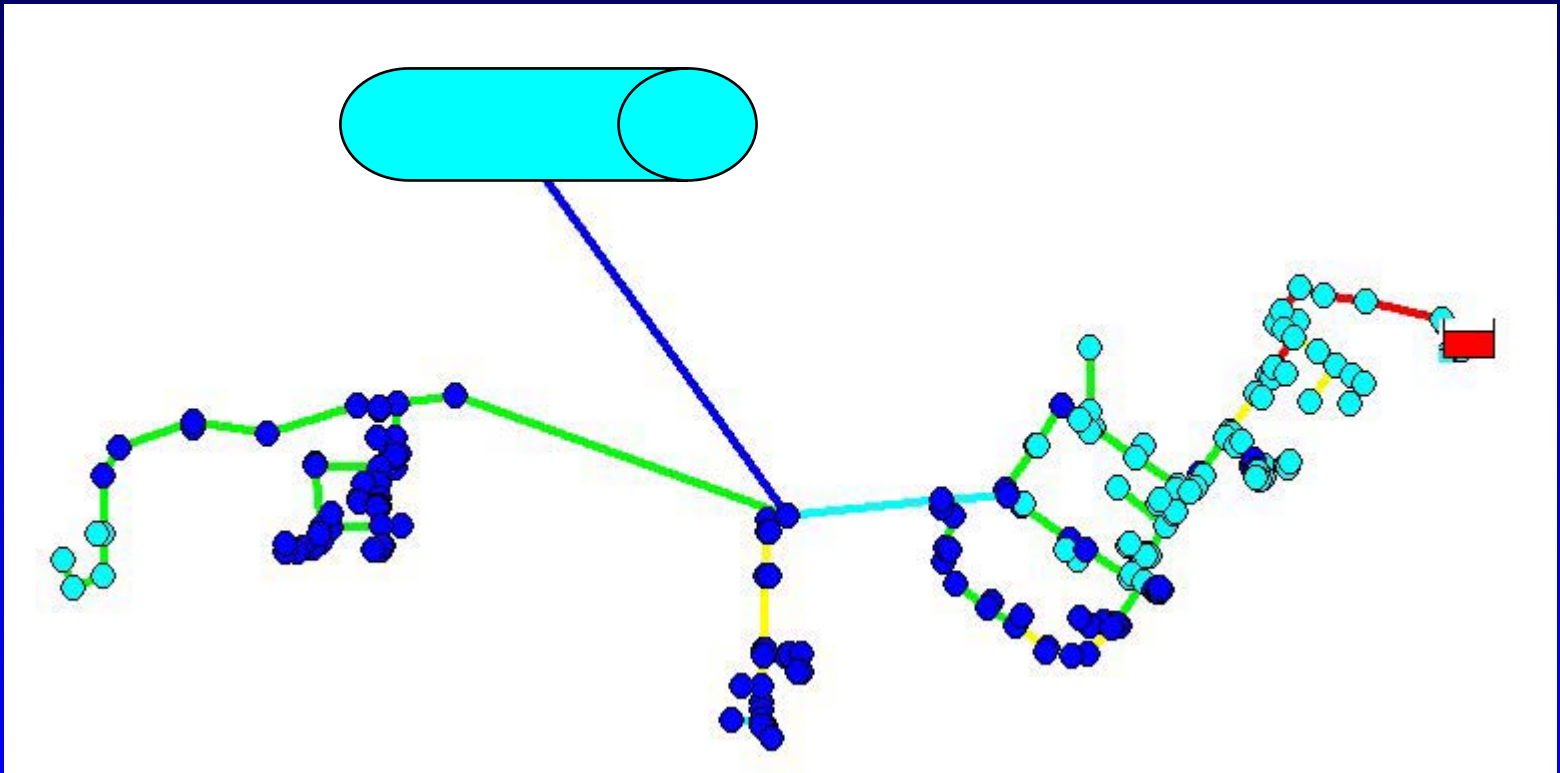
- Examples:
  - Redundancy in the utility network
  - Enhanced physical security
  - Sensors that detect and report tampering
  - Readily available backup service
  - Stockpiling of critical spare parts
- Modeling can help:
  - Quantify the effectiveness of some proposed COAs
  - Filter potential COA to reject losers and avoid

Recall the previous scenario where the 10” main was damaged….

What if I add a connection to the nearby municipal water system?



System now provides adequate pressure and flow to all consumers.



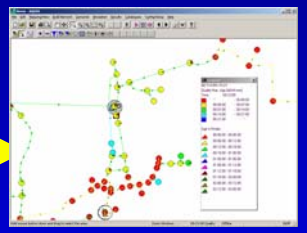
Consequence value “C” can be reduced.

The Future: On-Line Real Time Model

Flow sensor

Remote Terminal Unit

Master computer for SCADA system



Connection via LAN and/or radio

Utility system models

Water system outfitted with sensors and RTUs

RTU = Remote Terminal Unit
SCADA = Supervisory Control and Data Acquisition
LAN = Local Area Network

Water Security Test Loop

- Only research facility in the U. S. that allows experiments with live CB agents in an instrumented and computer-controlled environment
- Allows agent fate and transport behavior to be studied and modeled
- Allows validation of emerging sensors and countermeasure technologies
- Designed by ERDC and constructed at ECBC in FY03

Summary

- Utility systems are vital and vulnerable
- Traditional risk/ vulnerability assessment methods are difficult to apply to utility systems
- Fort Future includes engineering-based models that can be used to enhance and support several steps of the risk/ vulnerability assessment process
- Future research directions include incorporation of sensors and improved contaminant fate & transport models