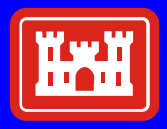
Utility System Security and Fort Future

Vicki Van Blaricum, Tom Bozada, Tim Perkins, and Vince Hock
U. S. Army Engineer Research & Development Center

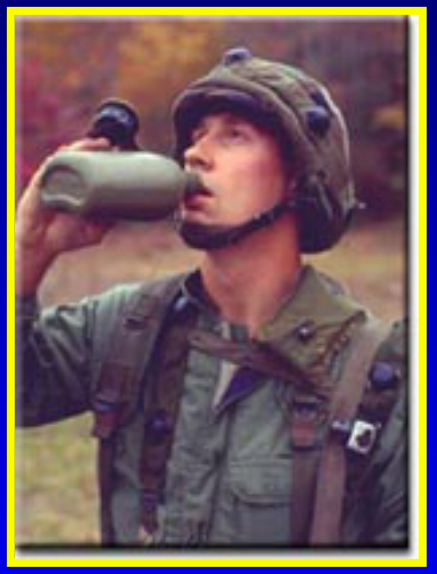
Presented at:
Tri-Services Infrastructure Systems Conference
3 August 2005



Utility systems enable key installation functions

Force Projection

Training



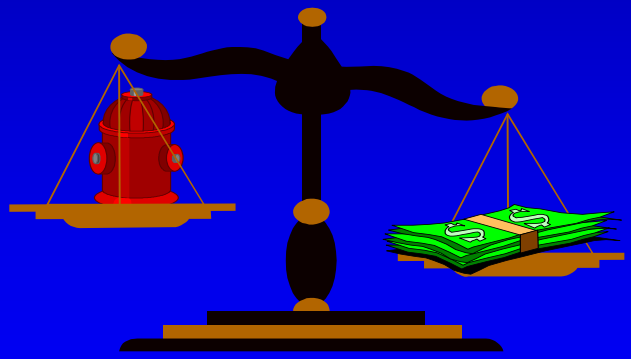
Daily activities

Utility systems must be:

Safe – does not cause harm

Reliable– always there when it's needed

Sufficient to meet demand– both normal and "surge"



Affordable– a balance between cost & service

Causes for utility service failures

Weather/ natural disasters

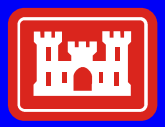
Equipment failure

Accident

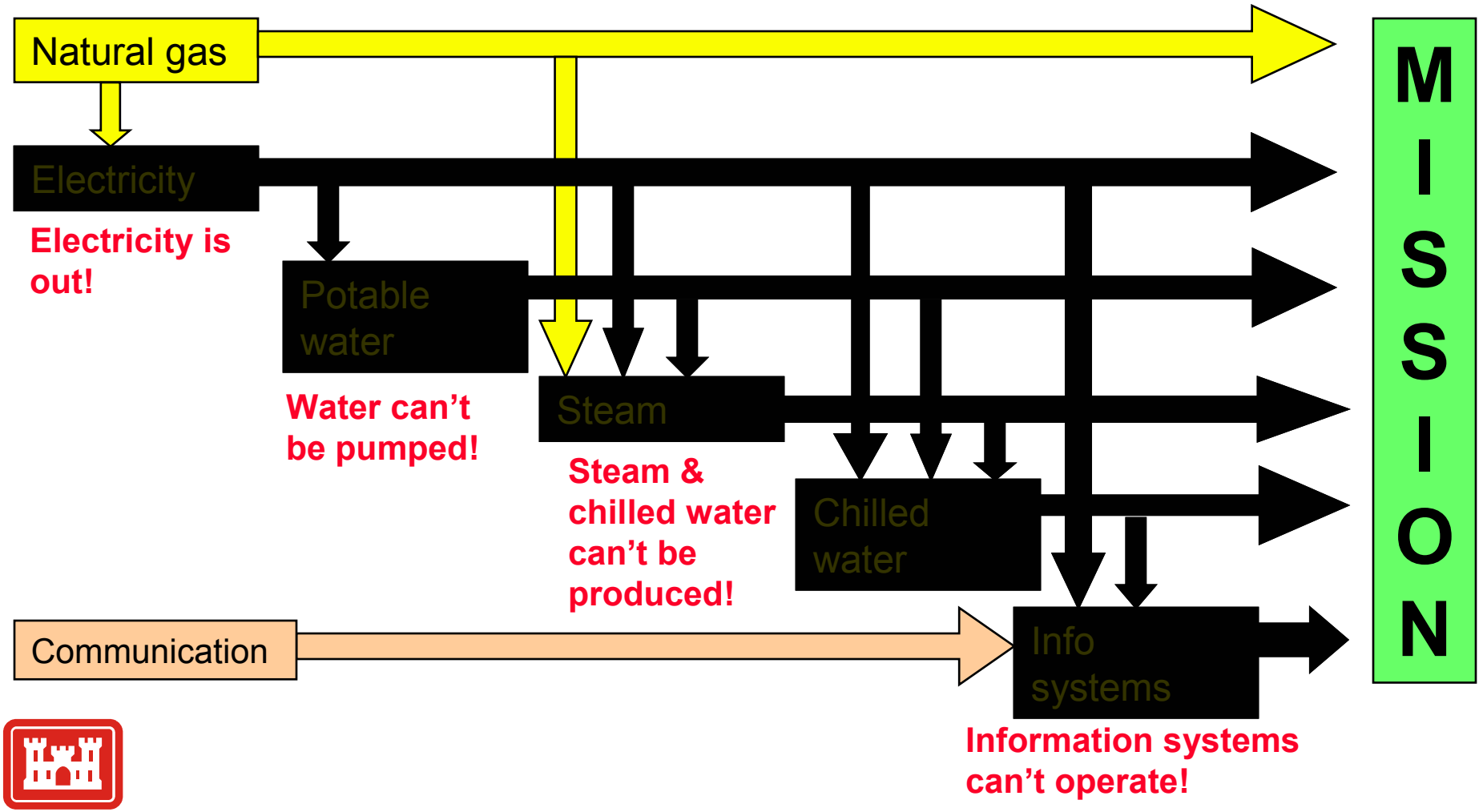
Terrorism / sabotage / vandalism

Security and Risk

- Decisions must be made because we don't have the resources to protect everything from everything.
- Risk cannot be entirely eliminated, only reduced.
- Risk management is a process that:
  - Considers the likelihood that a threat will endanger an asset, individual, or function
  - Identifies actions to reduce the risk and mitigate the consequences of an attack.



Problem: Utility systems are interdependent…yet traditional risk assessment methods usually consider only one system at a time.



Some Risk Assessment & Management Methods for Utility Systems

METHOD	DEVELOPER
Risk Assessment Methodology for Water (RAM-W)	Sandia National Laboratories
Vulnerability Self Assessment Tool (VSAT)	Association of Metropolitan Sewerage Agencies (AMSA)
Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems	National Rural Water Association
Security Guidelines for the Electricity Sector	North American Electric Reliability Council

Generalized risk assessment procedure

- Characterize the utility system, including its mission and objectives.
- Identify and prioritize critical assets. Critical assets are the utility system components that are determined to be most vital to meeting the system's mission and objectives.
- Assess the threat of emergencies and disasters. Both intentional and unintentional acts should be considered.
- Identify and rank the possible consequences of the identified threats.
- Evaluate existing countermeasures.
- Analyze risk based on the preceding information.
- Analyze alternatives for reducing unacceptable risk.

Problems with traditional utility risk assessment methods

- Application is usually subjective, or semi-quantitative at best
- Focus is on physical security
- Generally ignores interdependencies between utilities (such as “cascade effect” of power outage)

SOLUTION: Use integrated engineering-based simulations to support the risk assessment process.

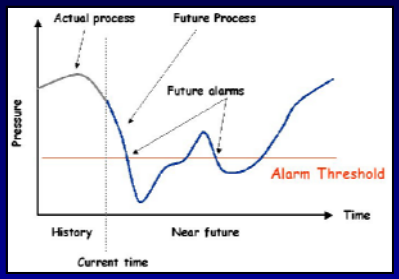
Types of Utility System Simulations

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.



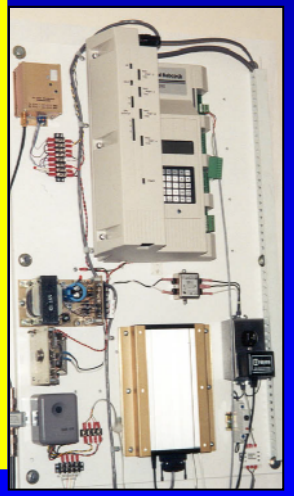
Accuracy, functionality and reliability of method

CAD Diagrams, Static Data

"Seat of the pants" methods for dealing with new situations & problems

Off-line Dynamic Model

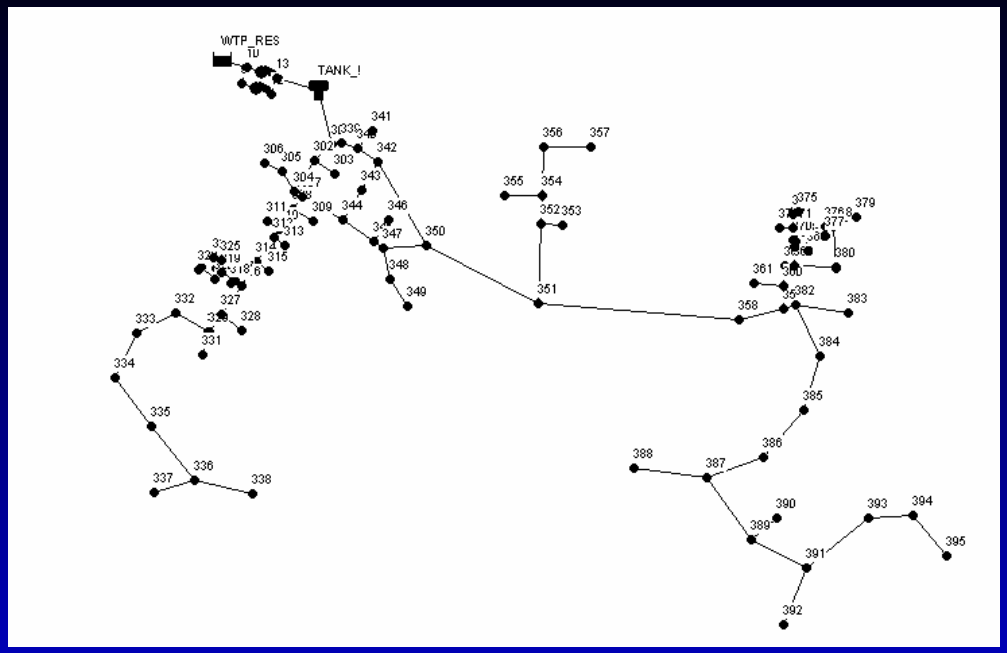
Time-varying processes can be modeled but data input is not automated

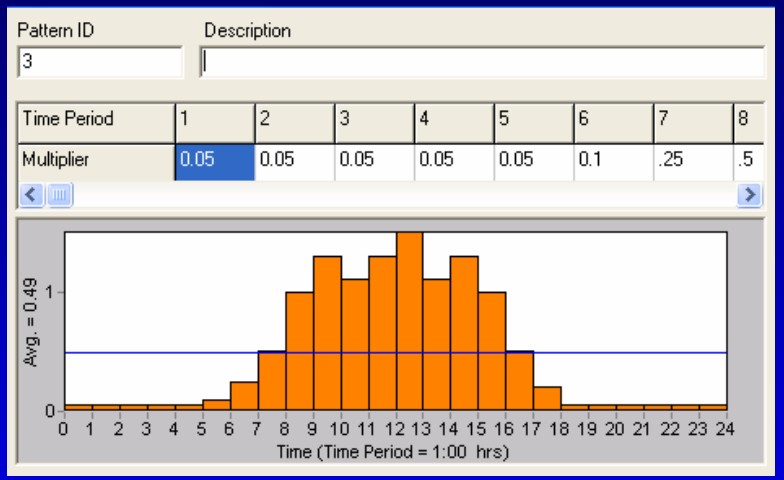


'Real-Time' Dynamic Model

Model updated with SCADA data at intervals of 15 minutes or less.

Example: Creating a water system model



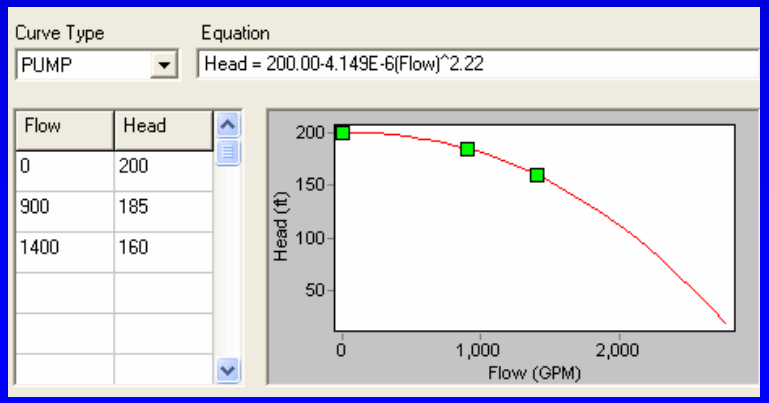


Pipe 12

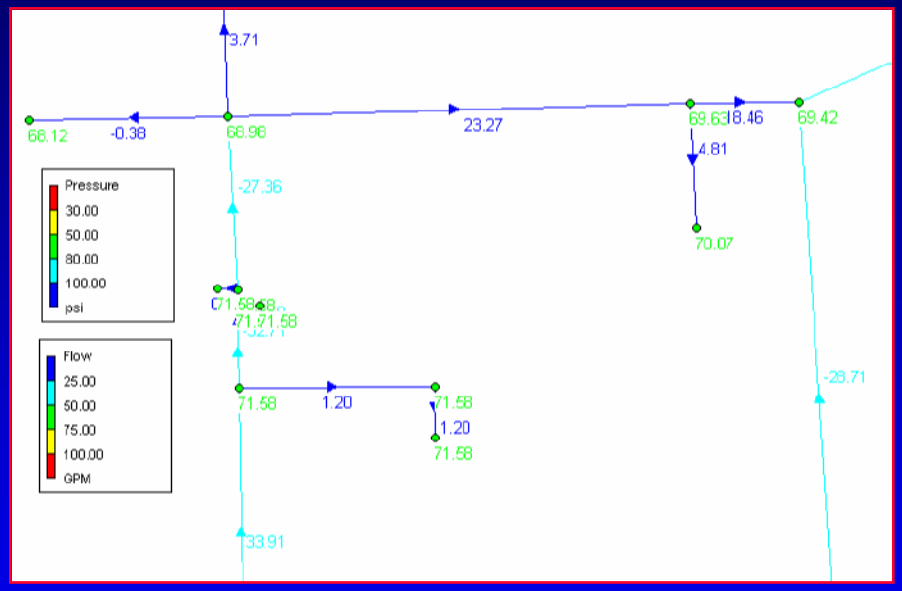
Property	Value
*Pipe ID	12
*Start Node	N071
*End Node	N077
Description	
Tag	
*Length	402
*Diameter	10
*Roughness	100
Loss Coeff.	0
Initial Status	Open
Bulk Coeff.	
Wall Coeff.	

Junction N016

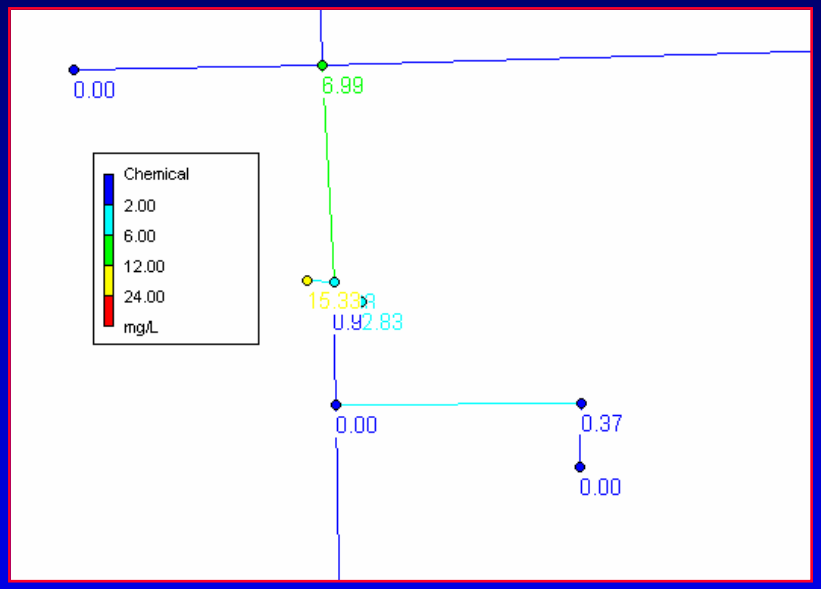
Property	Value
*Junction ID	N016
X-Coordinate	1234.37
Y-Coordinate	-422.92
Description	
Tag	
*Elevation	255
Base Demand	33
Demand Pattern	3
Demand Categories	1
Emitter Coeff.	
Initial Quality	
Source Quality	



Example: Water system model output



Pressures & flow rates



Chemical concentrations

The Fort Future Virtual Installation

- Creates a computable model of any geographic location using GIS Data, and standard system characteristics
- Integrates processes with infrastructure including utilities

- Utilities
  - Power
  - Water
  - Fuel (FY05)
  - Natural Gas (FY05)
- Process Simulation
  - Projection
  - Dining Facilities
  - Barracks Utilization

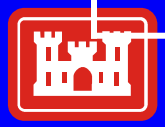
Capabilities of Utilities Simulations within the Virtual Installation

- Describes quantitatively how utility systems will behave under actual or hypothetical conditions
  - Capacity
  - Locations of service interruptions
  - Contamination
- Shows what the results mean
- Allows interdependencies to be considered
  - Between utility systems
  - Activities (process model)

Generalized risk assessment procedure & roles for engineering-based simulations

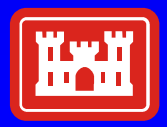
Step	Description	Can simulations help?
1	Characterize system mission & objectives.	No
2	Identify & prioritize critical assets	Yes
3	Assess threat of emergencies & disasters (intentional & unintentional)	No
4	Determine & rank possible consequences of the identified events.	Yes
5	Evaluate existing countermeasures.	Sometimes
6	Analyze risk based on the above information	No
7	Analyze courses of action for reducing unacceptable risk.	Yes

Step	Description	Can simulations help?
1	Characterize system mission & objectives.	No
2	Identify & prioritize critical assets	Yes
3	Assess threat of emergencies & disasters (intentional & unintentional)	No
4	Determine & rank possible consequences of the identified events.	Yes
5	Evaluate existing countermeasures.	Sometimes
6	Analyze risk based on the above information	No
7	Analyze courses of action for reducing unacceptable risk.	Yes

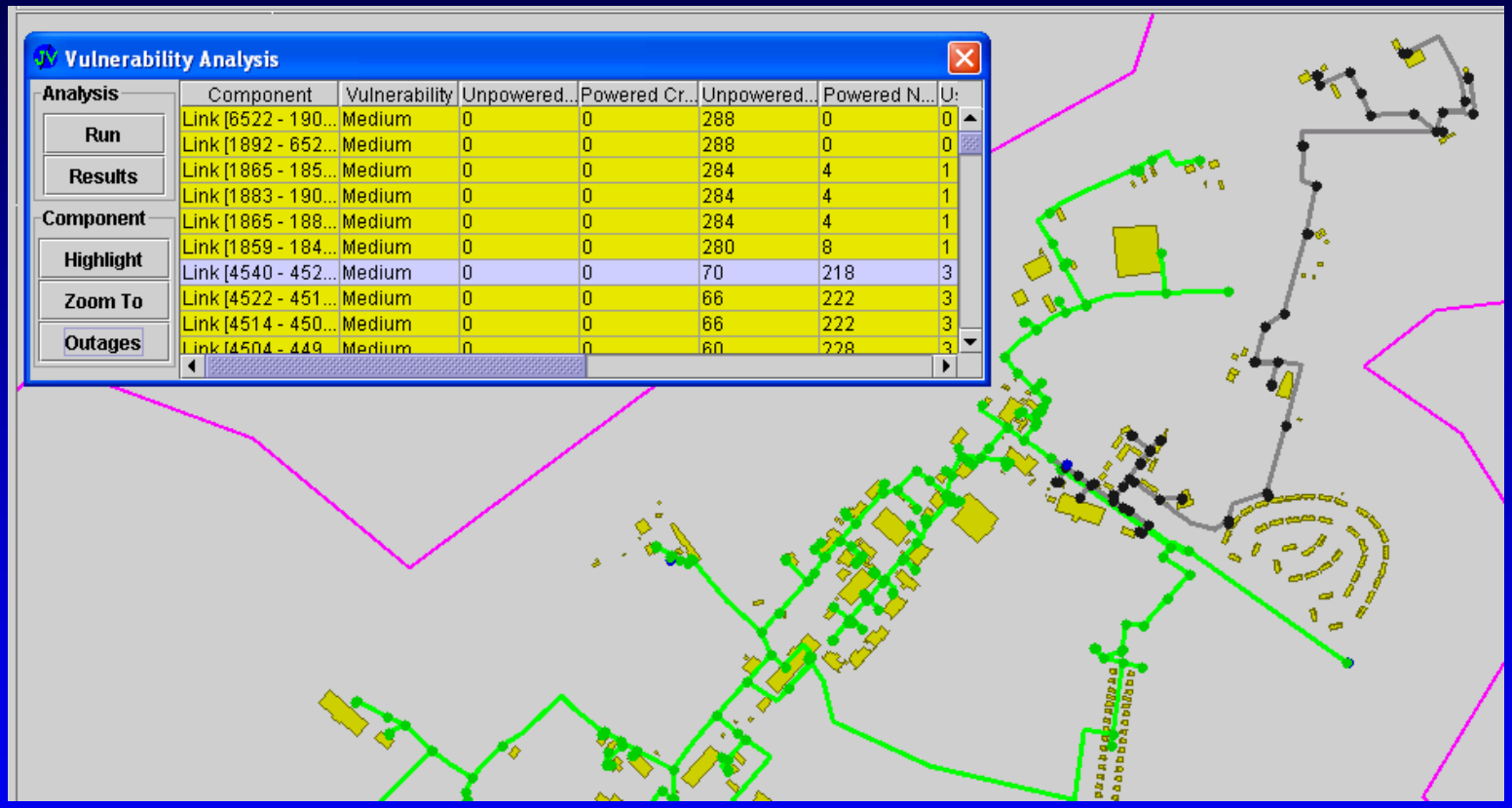


Step 2: Identify & prioritize critical assets

- 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

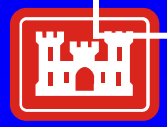


Step 2 Use Case:
Identify & prioritize critical assets



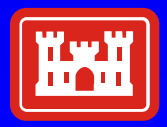
Each system asset is removed from the network and the simulation is run. Assets are ranked according to the impact of their removal (for example, how many "critical consumers" will lose power)

Step	Description	Can simulations help?
1	Characterize system mission & objectives.	No
2	Identify & prioritize critical assets	Yes
3	Assess threat of emergencies & disasters (intentional & unintentional)	No
4	Determine & rank possible consequences of the identified events.	Yes
5	Evaluate existing countermeasures.	Sometimes
6	Analyze risk based on the above information	No
7	Analyze courses of action for reducing unacceptable risk.	Yes



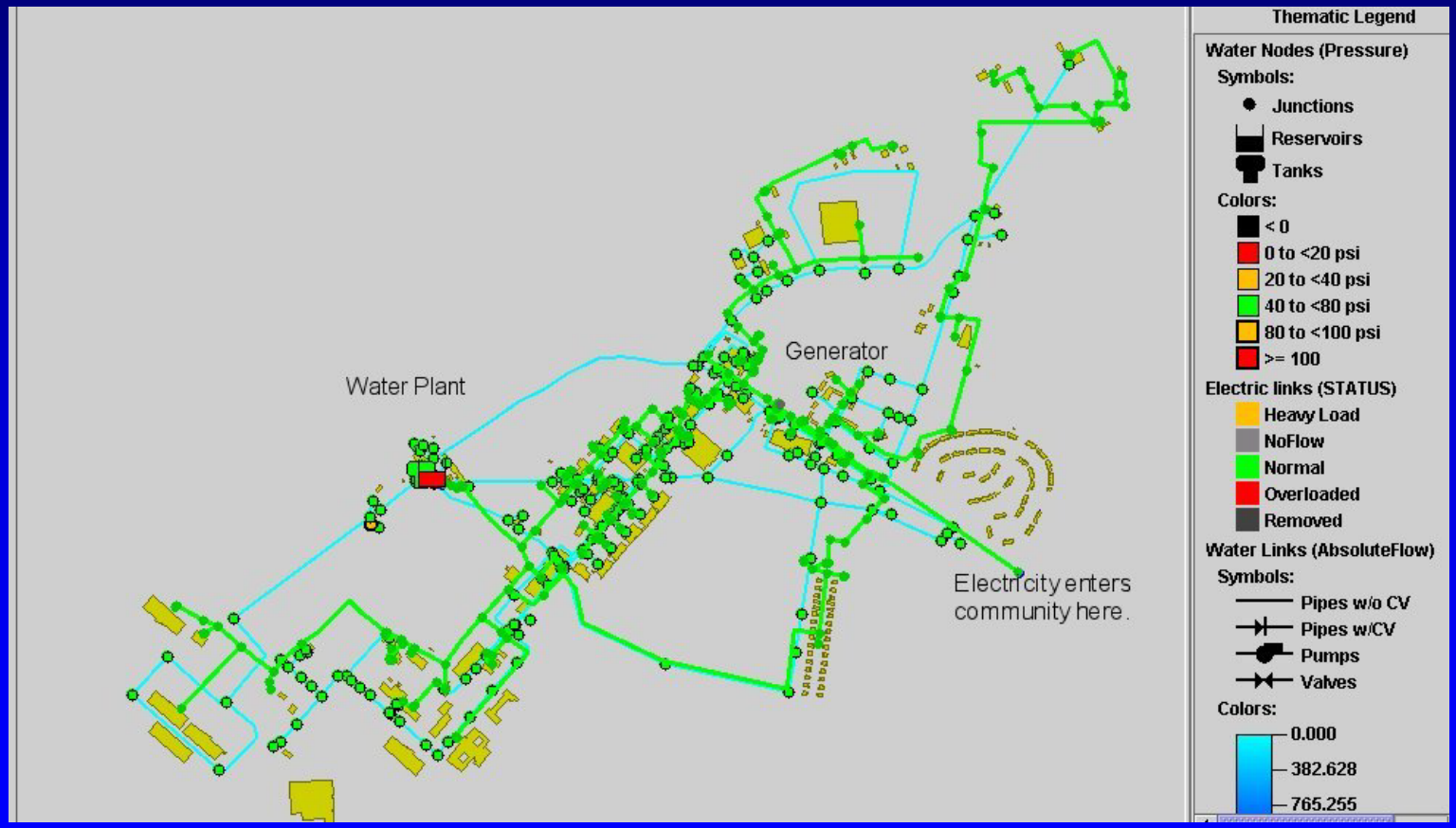
Step 4: Determine & rank possible consequences of the identified events

- 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.



Step 4 Use Case: Determine & rank possible consequences of the identified events

Electrical distribution system is shown in green; water in blue.



Determine & rank possible consequences of the identified events

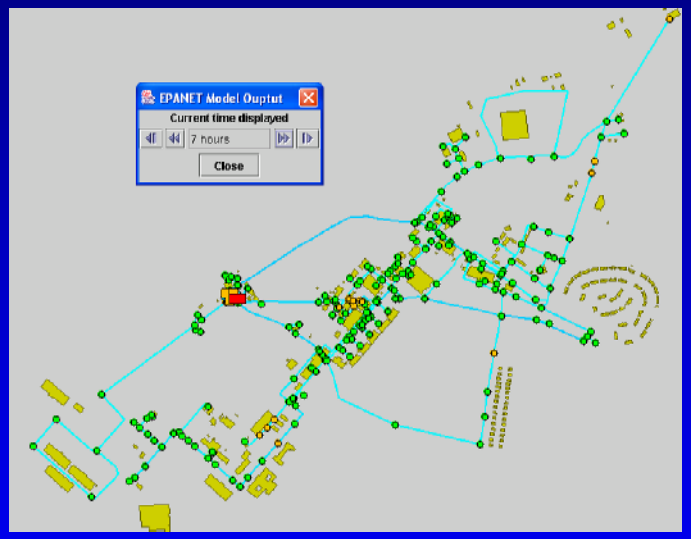
Scenario: An ice storm has damaged the three electrical lines indicated by XXs. The darkened electrical lines and blackened electrical nodes indicate locations where power has been lost.

Determine & rank possible consequences of the identified events

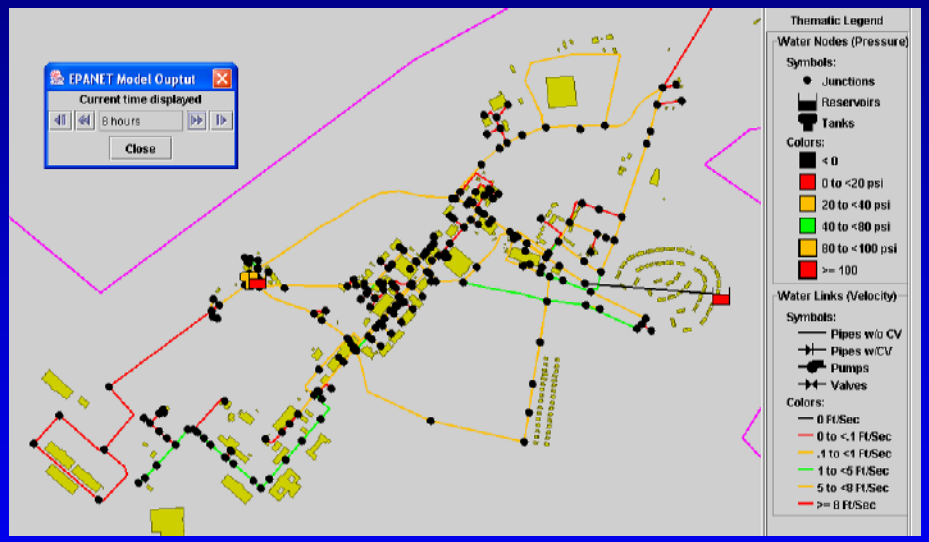
It is observed that power has been lost at the water treatment plant. The backup generator at the plant fails to start.

Determine & rank possible consequences of the identified events

How long will adequate pressure be maintained in the water distribution system? The water system simulation is run.



Hour 7



Hour 8

The simulation shows that the water storage tank maintains pressure for 7 hours. <u>At hour 8, the supply is exhausted.</u>

Step	Description	Can simulations help?
1	Characterize system mission & objectives.	No
2	Identify & prioritize critical assets	Yes
3	Assess threat of emergencies & disasters (intentional & unintentional)	No
4	Determine & rank possible consequences of the identified events.	Yes
5	Evaluate existing countermeasures.	Sometimes
6	Analyze risk based on the above information	No
7	Analyze courses of action for reducing unacceptable risk.	Yes

Step	Description	Can simulations help?
1	Characterize system mission & objectives.	No
2	Identify & prioritize critical assets	Yes
3	Assess threat of emergencies & disasters (intentional & unintentional)	No
4	Determine & rank possible consequences of the identified events.	Yes
5	Evaluate existing countermeasures.	Sometimes
6	Analyze risk based on the above information	No
7	Analyze courses of action for reducing unacceptable risk.	Yes

Step 6: Analyze risk based on above information

- **Example: In RAM-W for water systems:**

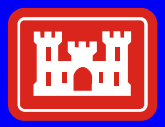
$$Risk = P_A * (1 - P_E) * C$$

P_A = Potential for adversary attack (threat)

P_E = Effectiveness of protection systems

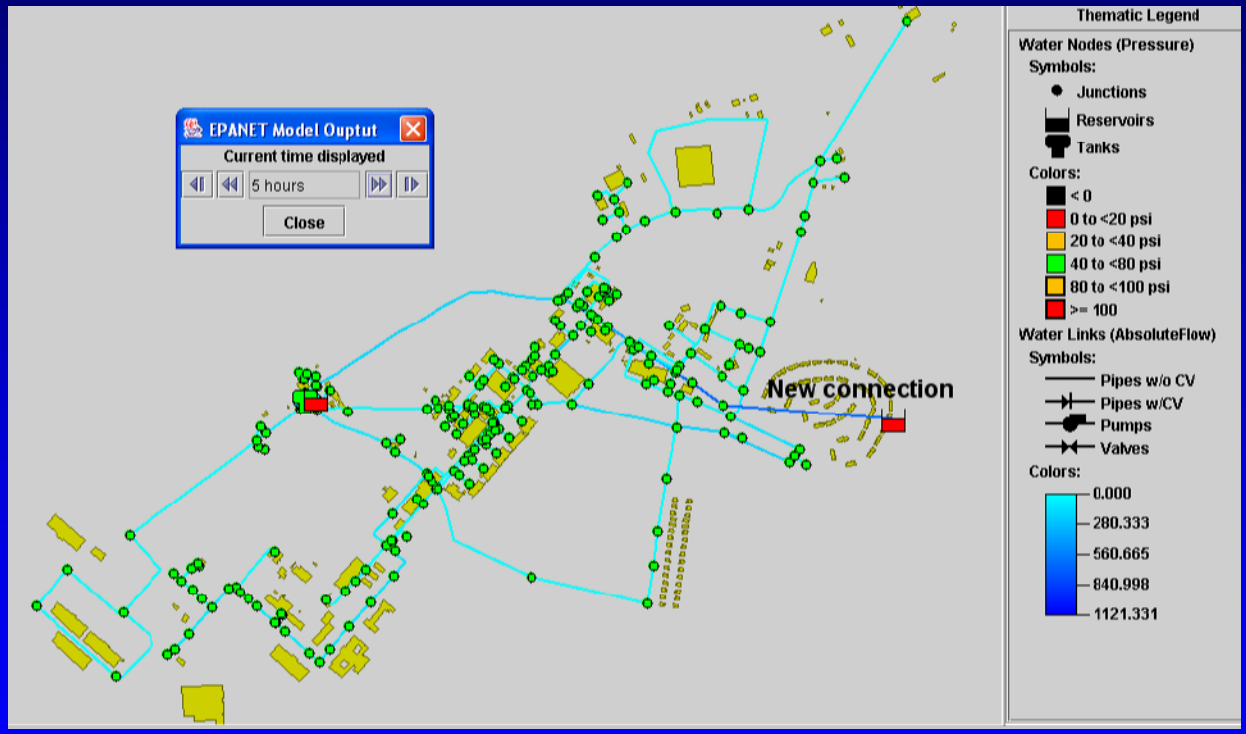
C = Consequence

- **Is the identified risk level acceptable?**



Step 7 Use Case:
Analyze courses of action for reducing unacceptable risk.

One possible course of action for reducing risk in the power outage scenario is to add a "backup" connection to the municipal water system.



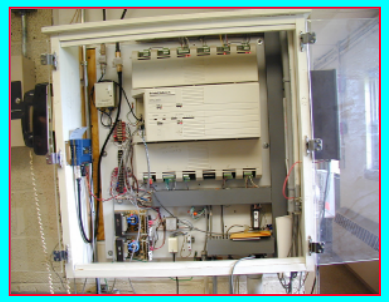
The power outage is simulated again.

The new connection begins delivering water 5 hours after the outage.

<u>Pressures are maintained adequately.</u>

The Future: On-Line Dynamic Simulations

Flow sensor

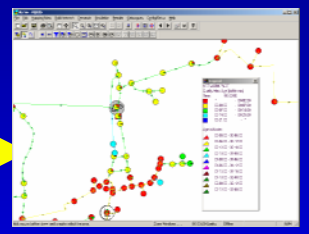


Remote Terminal Unit

Water system outfitted with sensors and RTUs

Connection via LAN and/or radio

Master computer for SCADA system

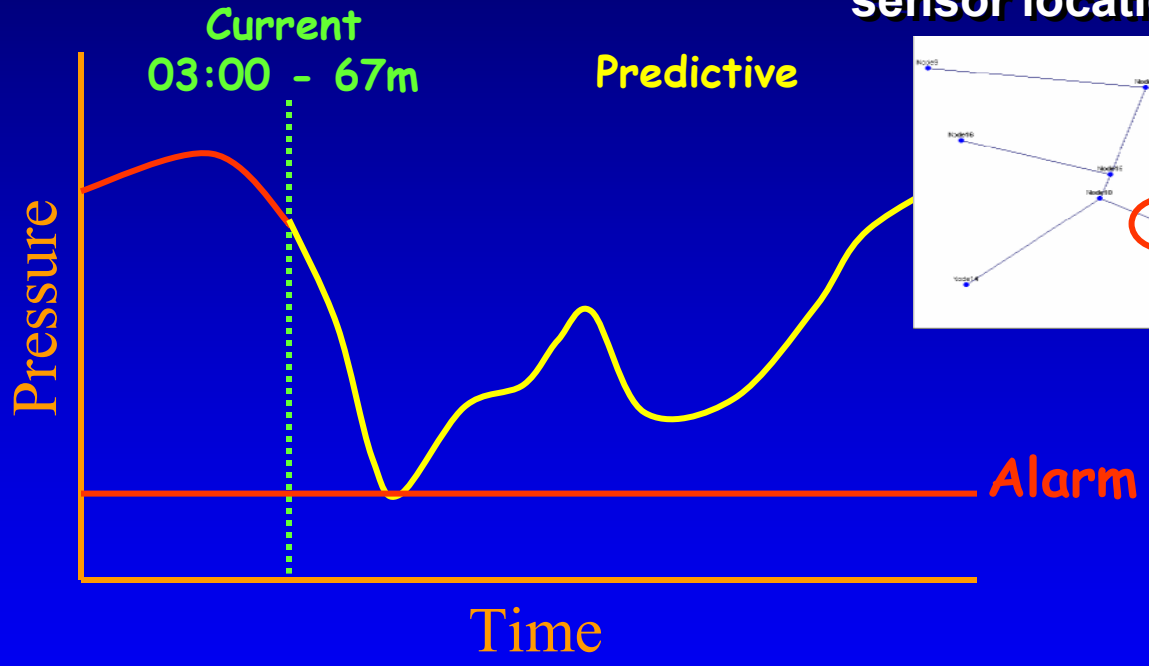


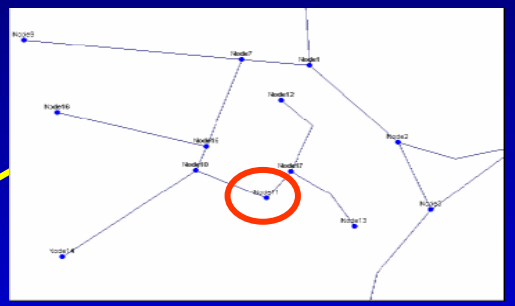
Utility system models

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

Real time modeling allows proactive identification of problems

System behavior at all locations is extrapolated from relatively few sensor locations.





The operator always knows what is happening everywhere in the water system.

Summary

- Risk management is a method for prioritizing allocation of limited security and reliability resources
- Fort Future Virtual Installation can be used to overcome some known difficulties in utility system risk assessment
- It provides quantitative, engineering based information and analysis to help overcome knowledge gaps and reduce subjectivity