



Quantifying Vulnerability to Critical Infrastructure



by

Barry Charles Ezell
Major, US Army

Deputy Director
The Army School System Directorate (ATTG-X)
355 Fenwick Road, BLDG 260, Fort Monroe, VA 23651
757.788.5949 DSN 680- Fax 757.788.5719
Email: barry.ezell@us.army.mil

Background and Motivation

- Nine years of research in critical infrastructure
 - SCADA
 - Water Supply (Clean water systems)
- Infrastructure Risk Assessment Model (IRAM)
- Dissertation Research

Purpose

Present the results of my research
on quantifying vulnerability to critical
infrastructure

Agenda

- Research Questions
- Definitions
- Model Design and Deployment
 - Value Model
 - Parameters
 - Inputs, Transformation, and Output
- Demonstration
- Future work
- Discussion

Research Questions

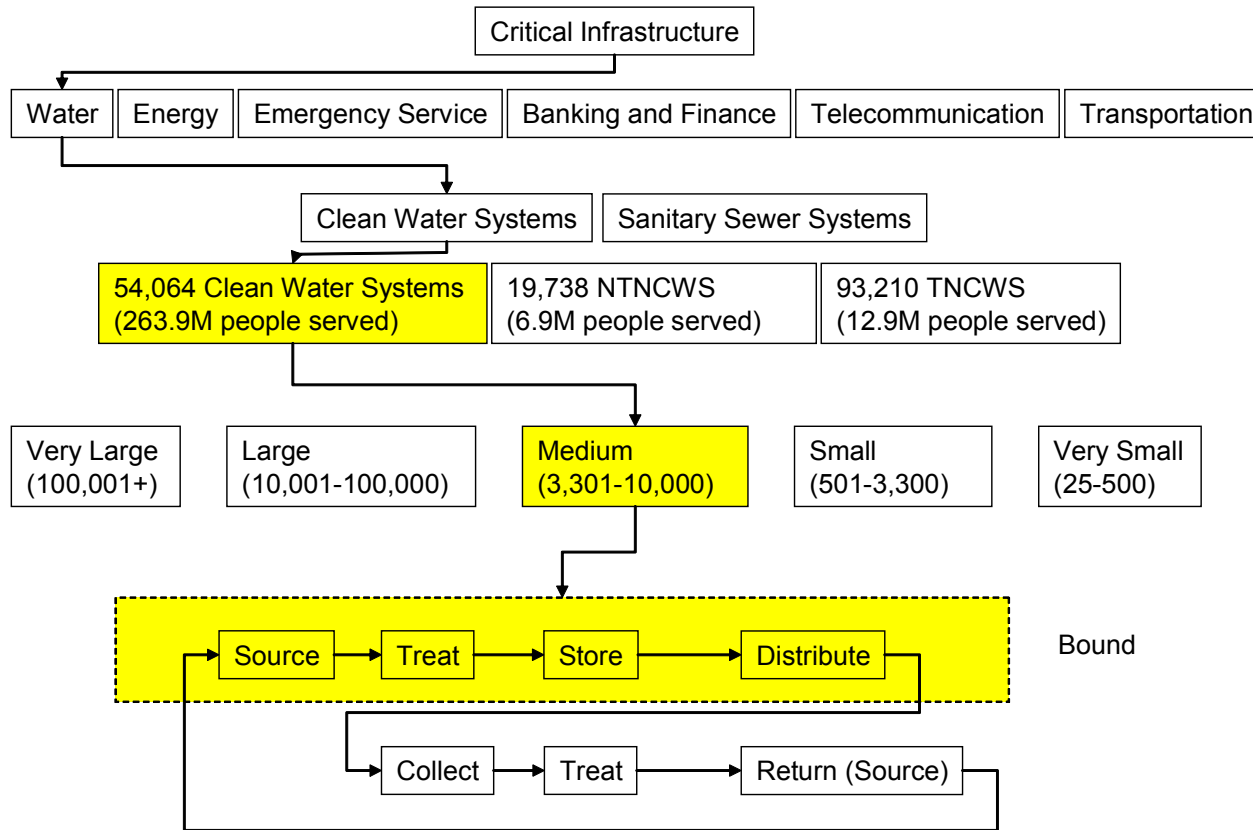
- What is vulnerability as it applies to critical infrastructure systems?
- How does risk and systems theory apply to critical infrastructure vulnerability?
- How can critical infrastructure vulnerability be quantified?
- What results from the deployment of a systems-based model that quantifies vulnerability to a critical infrastructure such as a water system?

Definition of Critical Infrastructure Vulnerability

- Whereas, risk is a function of threat scenario, likelihood of occurrence, and consequence....
- Critical infrastructure vulnerability is a measure of the *susceptibility* of critical infrastructure to < > :
 - an initiating event
 - threat scenario
 - what can go wrong

< > : The first question asked in risk assessment: what can go wrong?

Scope: Medium-sized Clean Water System



*

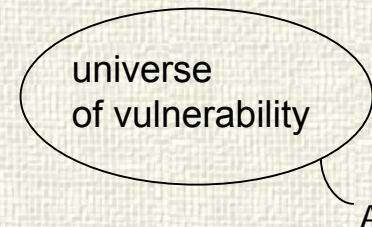
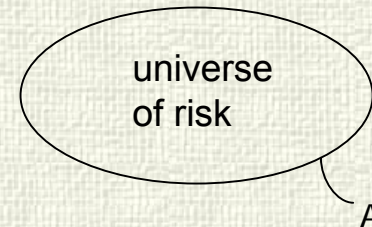
**

* PDD 63

** AWWA

Relationship: Risk and Vulnerability

- From the risk literature*:
 - the universal set of the triplet: scenario, likelihood and consequence.
- Vulnerability: $(\Omega) = \{s_a, p_a, w_a\} A$
 - In words: vulnerability is the universal set of the triplet: scenario, protection, and importance



The question “what can go wrong”, i.e. the scenario is the relationship.

Vulnerability highlights the notion of susceptibility to a scenario whereas risk focuses on the severity of consequences to a scenario.

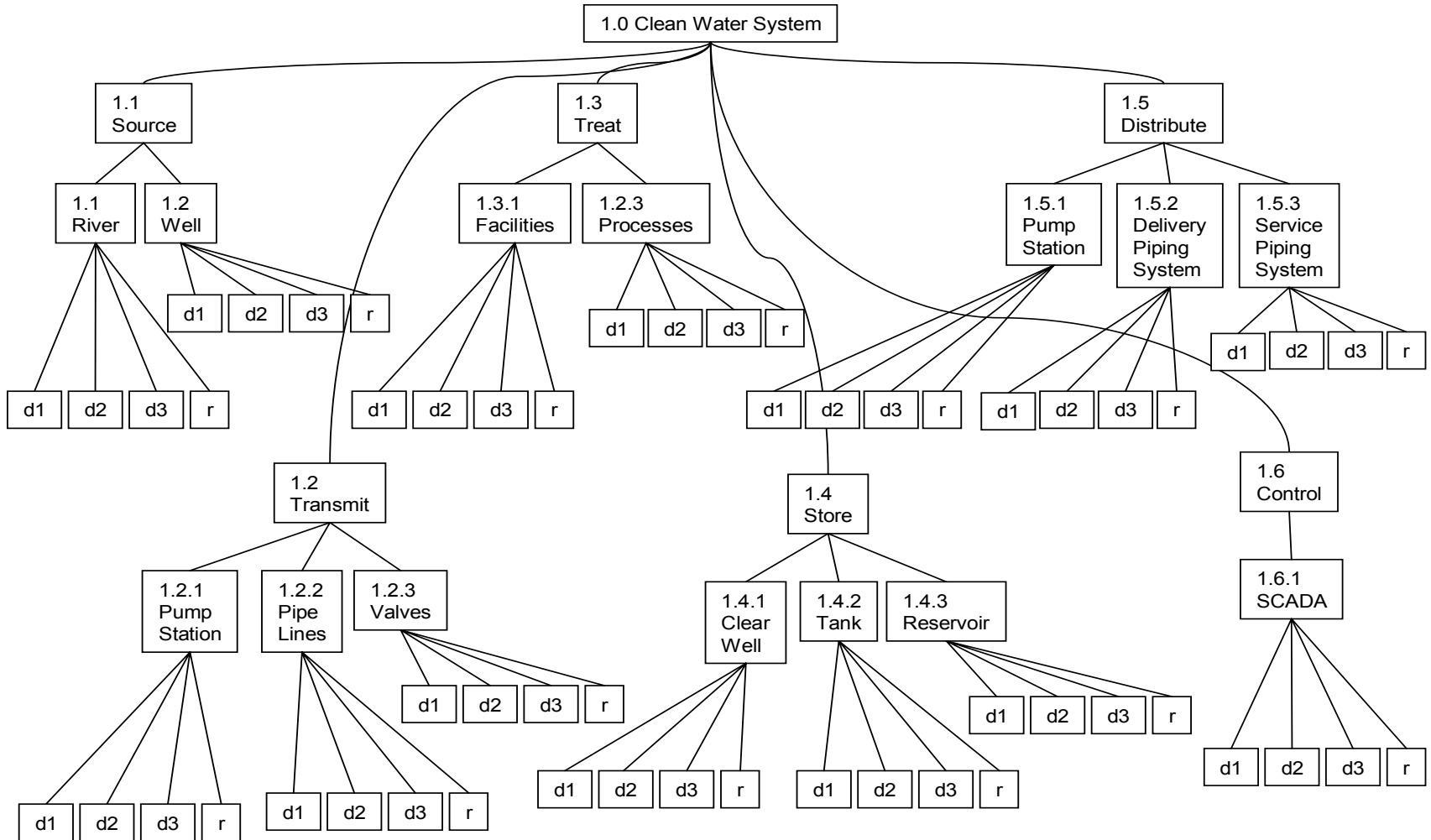
Model Design

- Systems decomposition of a clean water system
- Evaluation Measures: deter, detect, delay, and respond
- Value functions
- SME
 - value functions
 - weight assignment
 - assess a system

Chosen Protection Evaluation Measure and Definitions

- Deterrence : measures implemented that are perceived by adversaries as too difficult to defeat
- Detection: probability of determining that an unauthorized action has occurred or is occurring including: sensing, communicating alarm to control center, and assessing the alarm
- Delay: time, measured in minutes that an element of a physical protection system designed to impede adversary penetration into or exit from the protected area
- Response: time (minutes) to respond to a threat

Value Model Design



Aggregate Expert Assessments

- Weighted Linear Opinion Pool
- Aggregation Methodology (Chytka 2003)
- Triangle Distribution for each measure

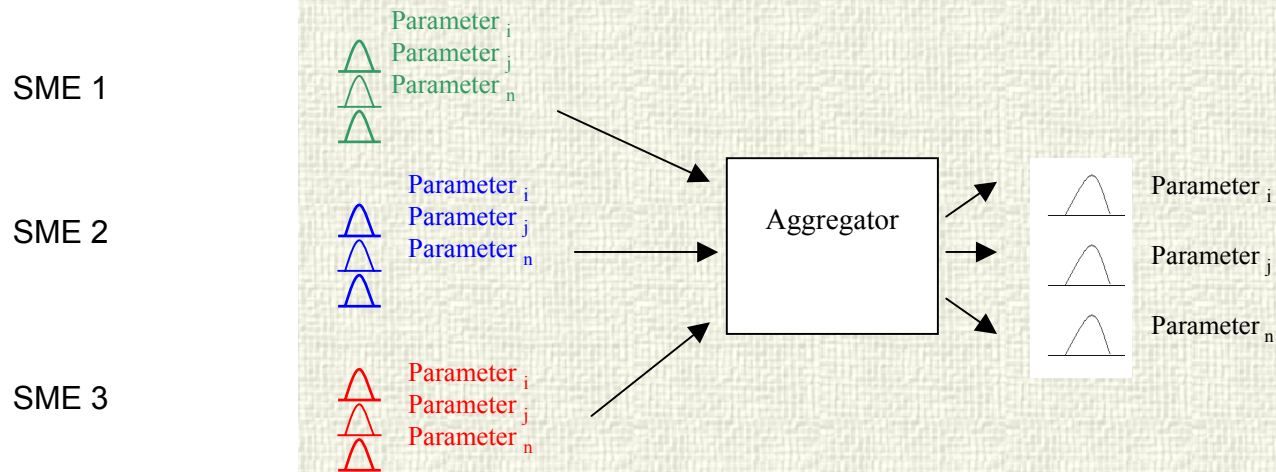


Figure Source Chytka (2003)

Model Recap

SMEs Assessment

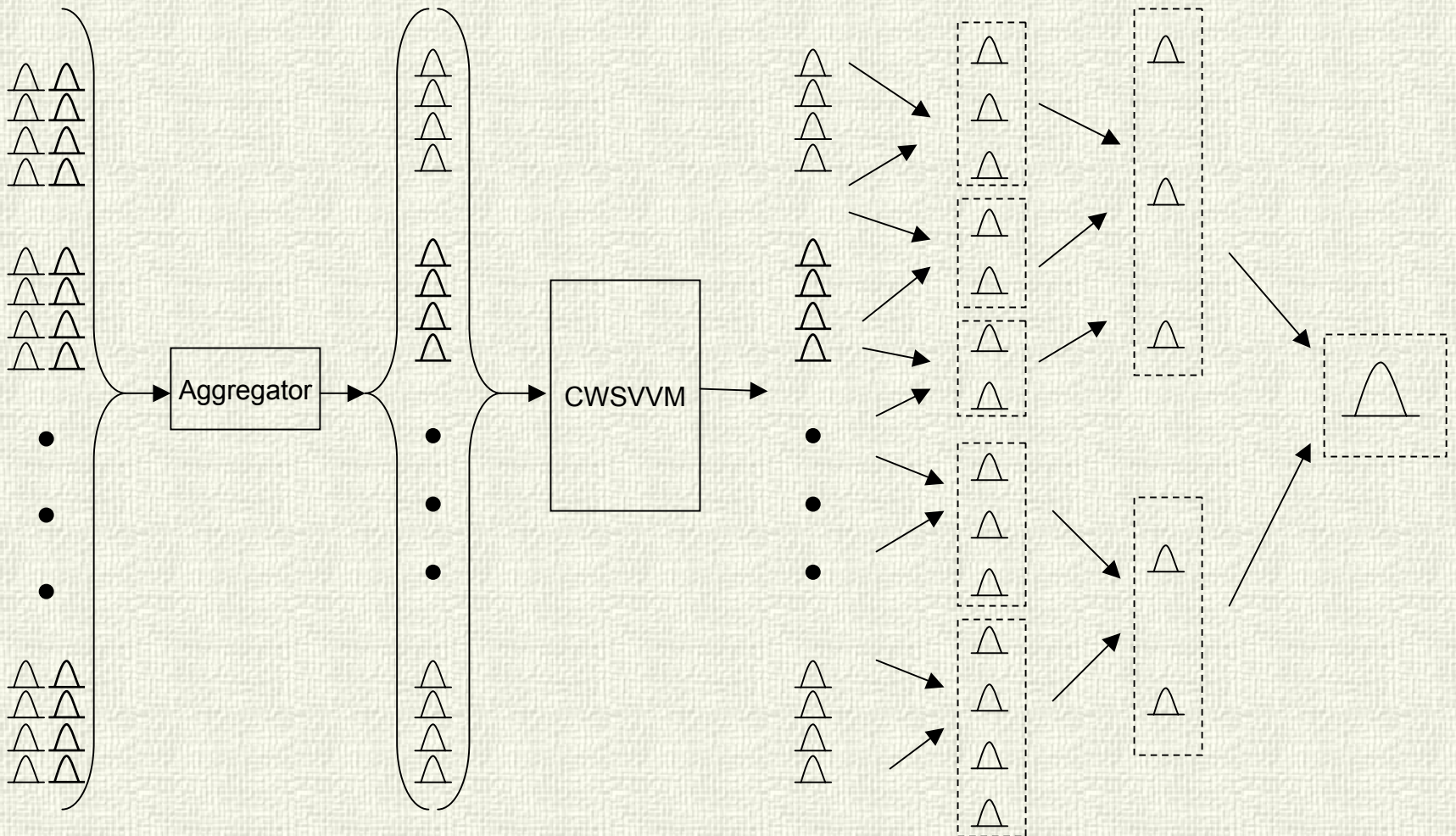
Combined Assessment

Measure Value

Component Ω

Subsystem Ω

System Ω



Demonstration

System-->	Source (1.1)															Transmit (1.2)														
Subsystem-->	3															9														
Relative Importance Factor-->	0.09															0.26														
Component-->	River (1.1.1)					Well (1.1.2)					Pump Station (1.2.1)					Pipelines (1.2.2)					Valves (1.2.3)					Facilities (1.3.1)				
Relative Importance Factor-->	9					3					9					8					4					10				
local wt-->	0.75					0.25					0.43					0.38					0.19					0.53				
Eval Measure-->	Delter	Delay	Detect	Respond	Delter	Delay	Detect	Respond	Delter	Delay	Detect	Respond	Delter	Delay	Detect	Respond	Delter	Delay	Detect	Respond	Delter	Delay	Detect	Respond	Delter	Delay	Detect	Respond		
Relative Importance Factor-->	10	9	10	9	7	6	8	6	9	8	9	8	8	9	10	10	9	8	9	7	10	9	10	10	9	10	10			
local wt-->	0.26	0.24	0.26	0.24	0.26	0.22	0.30	0.22	0.26	0.24	0.26	0.24	0.22	0.24	0.27	0.27	0.27	0.24	0.27	0.21	0.26	0.23	0.26	0.26	0.23	0.26	0.26			
global wt-->	0.0169	0.0152	0.0169	0.0152	0.0056	0.0048	0.0063	0.0048	0.0292	0.0259	0.0292	0.0259	0.0212	0.0238	0.0265	0.0265	0.0134	0.0119	0.0134	0.0104	0.0347	0.0312	0.0347	0.0347	0.0312	0.0347	0.0347			
input coding	2	1	3	3	5	4	6	6	8	7	9	9	11	10	12	14	13	15	17	18										

RAW DATA MATRIX

Ideal-->	3.0	120.0	1.0	0.0	3.0	120.0	1.0	0.0	4.0	120.0	1.0	0.0	4.0	120.0	1.0	0.0	4.0	120.0	1.0	0.0	4.0	120.0	1.0	0.0	4.0	120.0	1.0
SME Score-->	3.0	35.2	0.6	33.6	3.0	5.2	0.8	42.1	3.0	9.5	0.9	17.7	0.4	25.6	0.7	39.3	3.0	24.0	0.7	34.3	4.0	23.7	0.8				

VALUE MATRIX

PROTECTION MEASURES

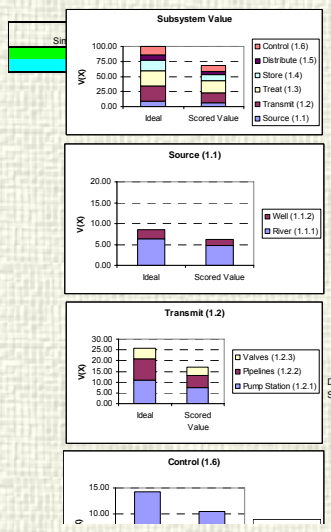
Ideal-->	1.69	1.52	1.69	1.52	0.56	0.68	0.63	0.48	2.92	2.59	2.92	2.59	2.12	2.38	2.65	2.65	1.34	1.19	1.34	1.04	3.47	3.12	3.47
Scored Value-->	1.69	1.16	0.51	1.29	0.56	0.11	0.48	0.39	1.76	0.79	2.53	2.44	0.04	1.72	1.64	2.23	1.20	0.76	0.99	0.89	3.47	1.95	2.37

COMPONENT VULNERABILITY

Ideal-->	River (1.1.1)					Well (1.1.2)					Pump Station (1.2.1)					Pipelines (1.2.2)					Valves (1.2.3)					Facilities (1.3.1)				
Scored Value-->	6.43					2.14					11.02					9.80					4.90					13.53				
Vulnerability-->	4.66					1.54					7.51					5.63					3.84					11.23				
Vulnerability-->	1.77					0.61					3.51					4.16					1.06					2.30				

SUBSYSTEM VULNERABILITY

Ideal-->	Source (1.1)															Transmit (1.2)														
Scored Value-->	8.57															25.71														
Vulnerability-->	6.20															16.99														
Vulnerability-->	2.38															8.72														



Data for charts

Source (1.1)	8.57	6.20
Transmit (1.2)	25.71	16.99
Treat (1.3)	25.71	19.76
Store (1.4)	17.14	10.37
Distribute (1.5)	8.57	4.84
Control (1.6)	14.29	10.46

Source (1.1) Ideal **Scored Value**

River (1.1.1)	6.43	4.66
Well (1.1.2)	2.14	1.54

Transmit (1.2) Ideal **Scored Value**

Pump Station (1.2.1)	11.02	7.51
Pipelines (1.2.2)	9.80	5.63
Valves (1.2.3)	4.90	3.84

Treat (1.3) Ideal **Scored Value**

Facilities (1.3.1)	13.53	11.23
Processes (1.3.2)	12.18	8.53

Store (1.4) Ideal **Scored Value**

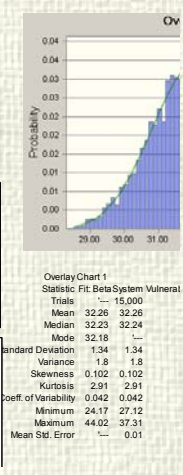
Cleanwell (1.4.1)	6.37	3.61
Tank (1.4.2)	4.11	2.80
Reservoir (1.4.3)	6.86	3.96

Distribute (1.5) Ideal **Scored Value**

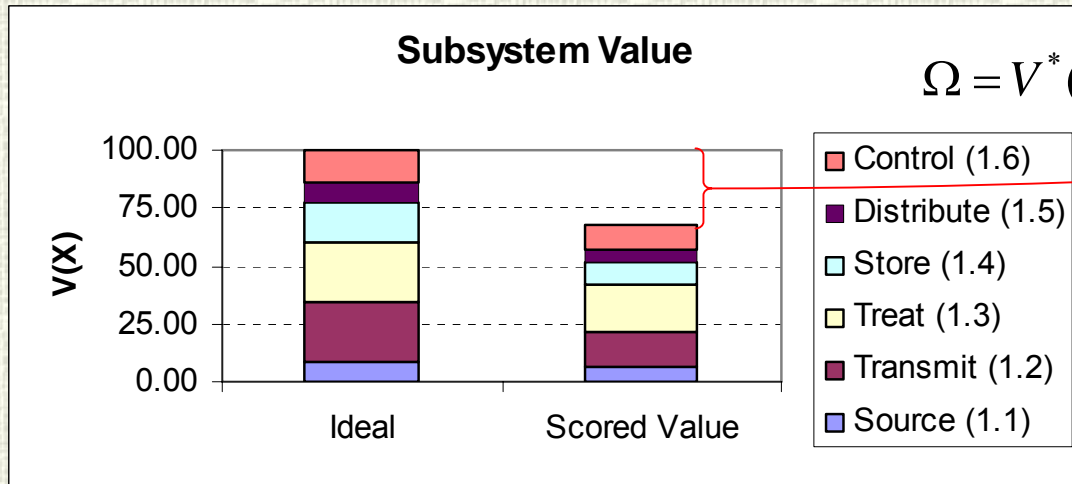
Pump Station (1.5.1)	4.68	2.96
Del Piping System (1.5.2)	2.34	1.29
Svc Piping System (1.5.3)	1.56	0.58

Control (1.6) Ideal **Scored Value**

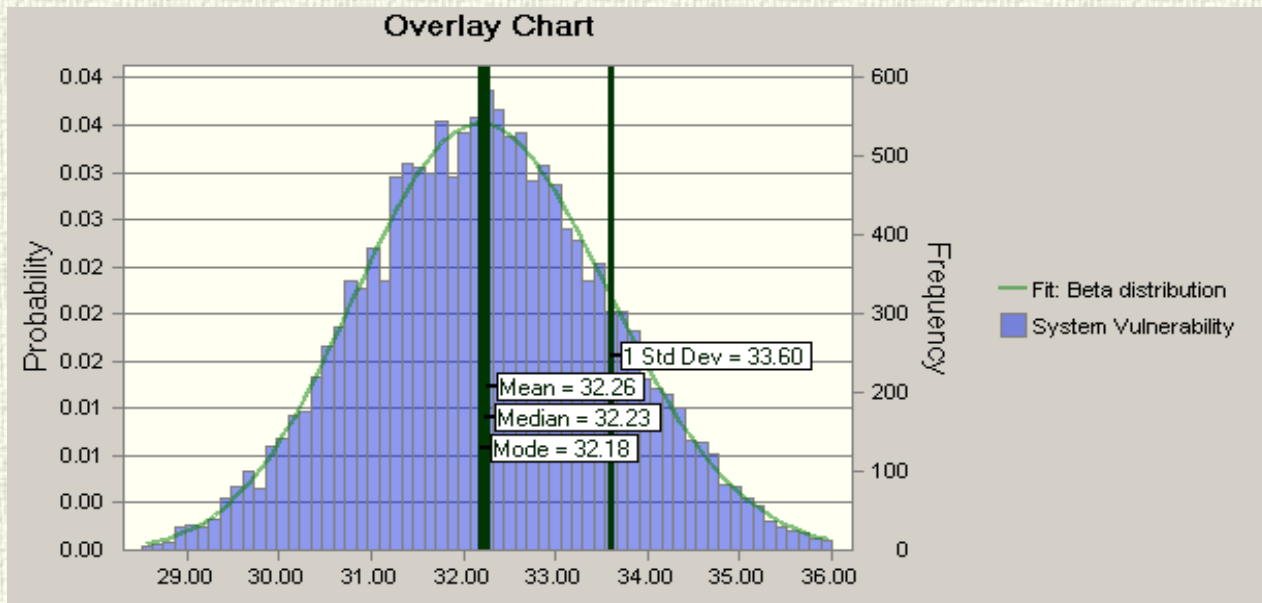
SCADA (1.5.1)	14.29	10.46
---------------	-------	-------



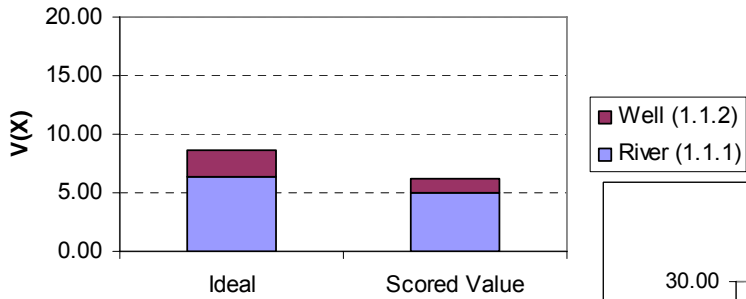
Model Output



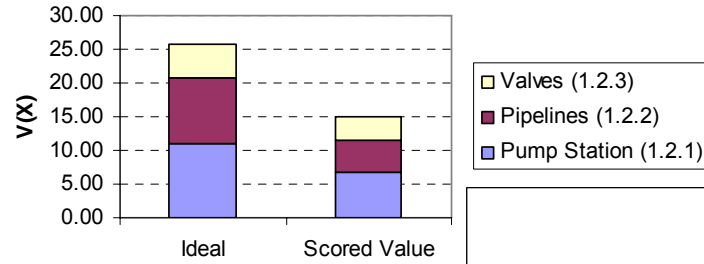
$$\Omega = V^*(X) - V(X) = 100 - 67.74 = 32.26$$



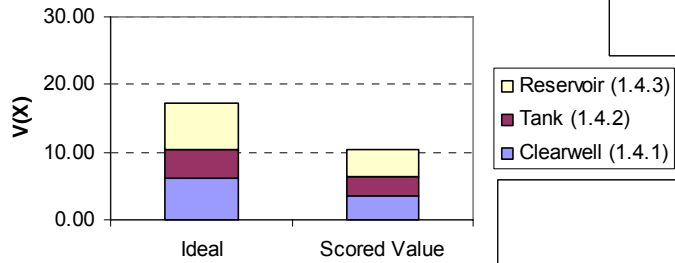
Source (1.1)



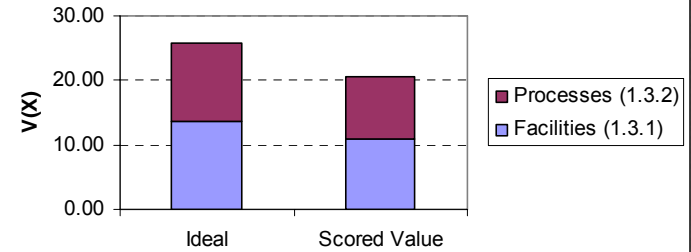
Transmit (1.2)



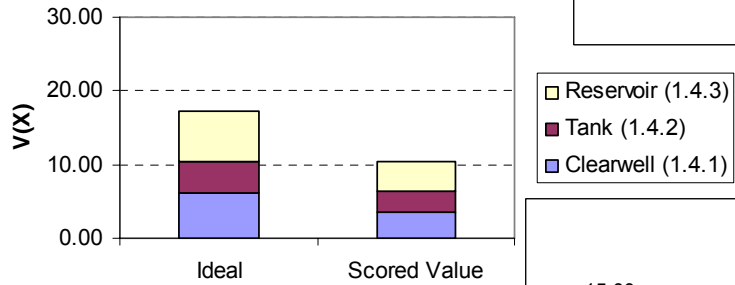
Store (1.4)



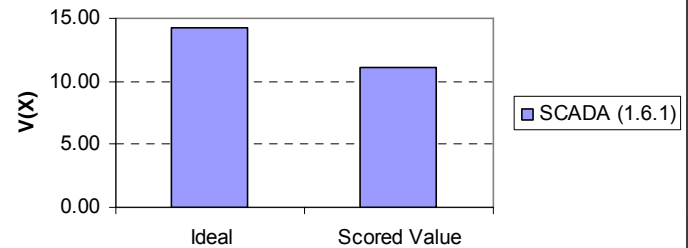
Treat (1.3)



Store (1.4)



Control (1.6)



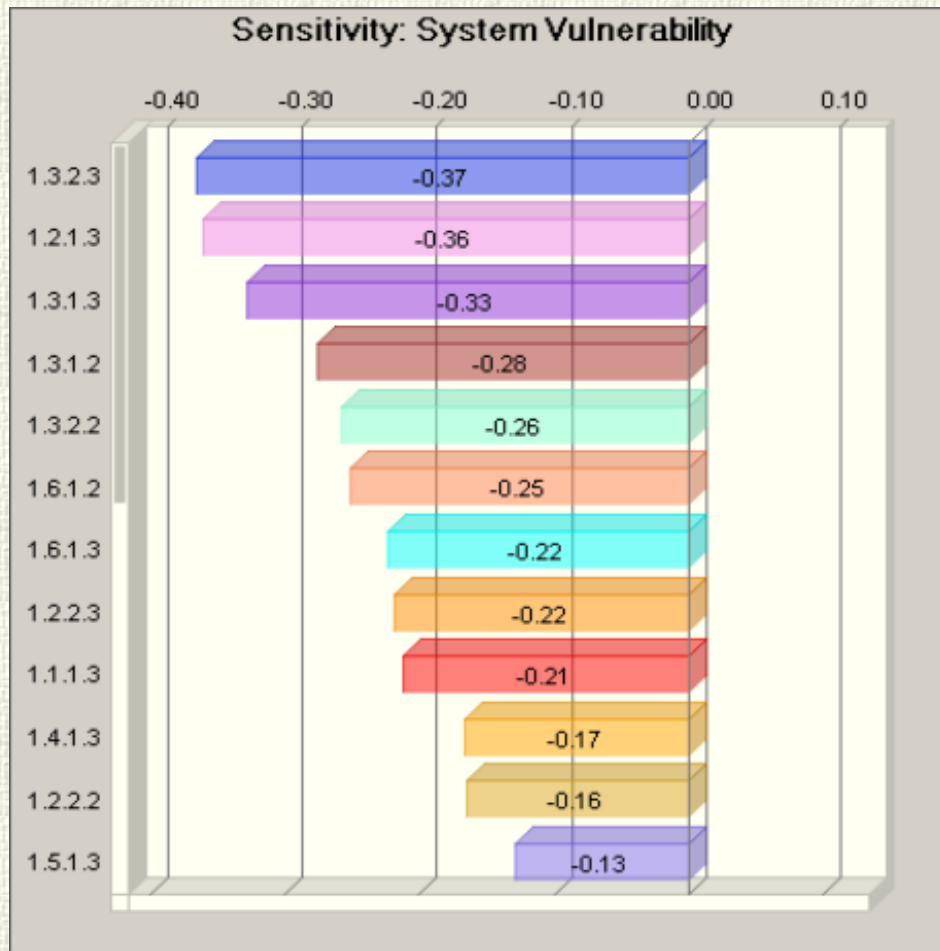
Sensitivity Analysis

- Monte Carlo and Latin Hyper-cube
- Model Parameter Sensitivity

Trials	Monte Carlo	Latin Hyper-cube
150,000	Mean: 32.26	Mean: 32.27
	Median: 32.23	Median: 32.22
	Mode: 32.18	Mode: 32.13
	Standard Dev: 33.60	Standard Dev: 33.63
	Distribution: Beta	Distribution: Beta

Parameter Sensitivity

- Contribution to Variance



- Model output is sensitive to
 - Detection probability
 - Delay is sensitive
- Useful information
 - Clues on where we can focus first to improve system
 - What-if analysis

Significance

- Solved a problem not addressed in the literature
- Clean water systems constitute a very large sample of water systems (54,000 systems providing water to 263 million customers)
- Quantification of vulnerability is meaningful because the omega value of vulnerability can be readily compared to the system's ideal score

Future Research

- Quantify vulnerability to other systems or critical infrastructures
- Vulnerability Index Score to support Homeland Security
- Threat Scenario Analysis

Thank you!

Questions / Discussion

BACKUP

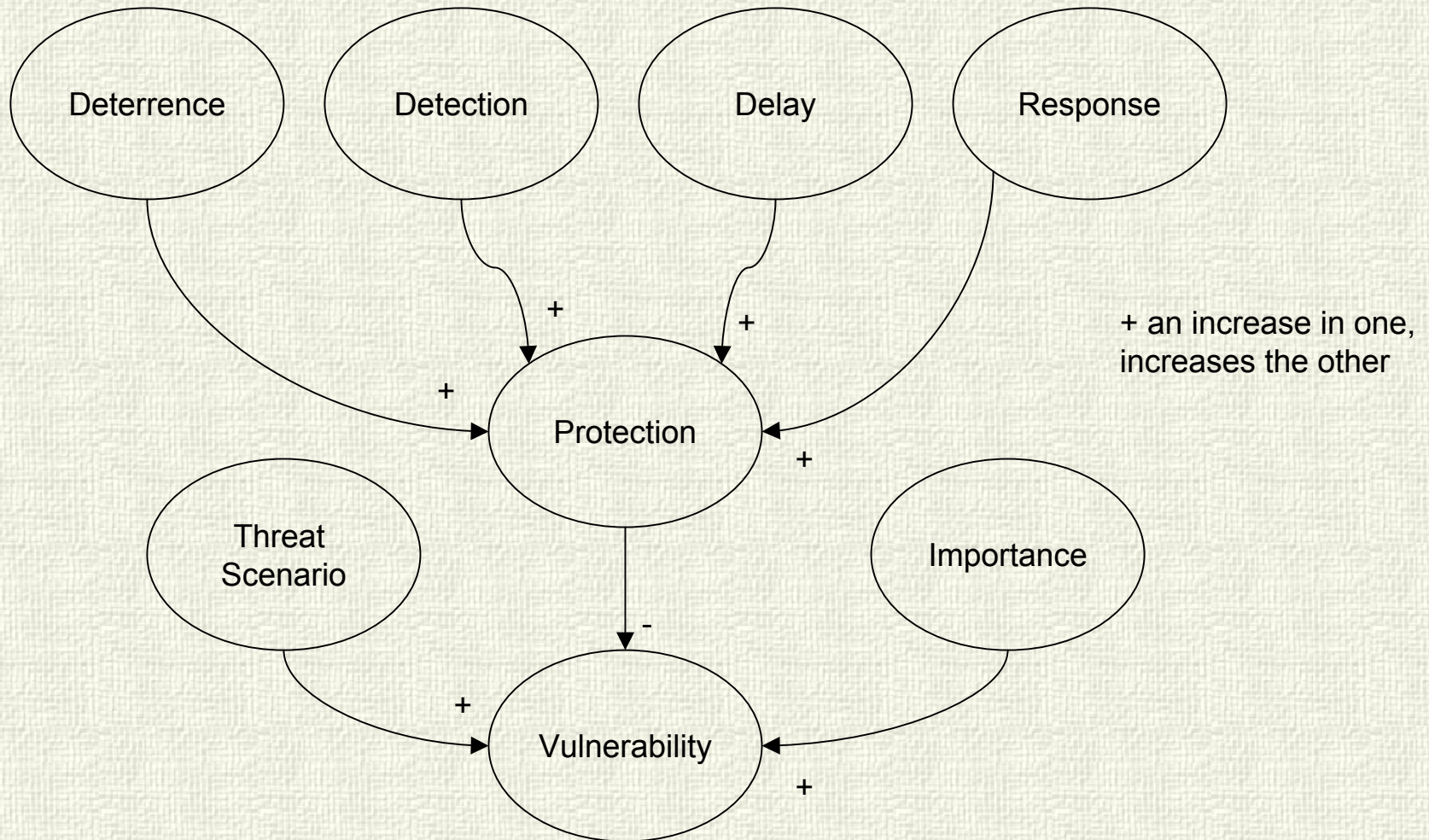
Literature Review: Risk

- Lowrance (1976): a measure of the probability and severity of adverse effects
- Kaplan (1997): a triplet of scenario, likelihood, and consequences
- Kaplan (1997): the notion of scenario(s) as a euphemism for “what can go wrong”
- Blaike (1994), Buckle (2000a, 2000b), NOAA (2002): vulnerability is *susceptibility* to risk (i.e. what can go wrong)

Literature: Critical Infrastructure

- “those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private” (PDD 63, p. 1, 1998).

Chosen Evaluation Measures *



Value Model Parameters

Notation	Description	Type
X	Protection measure assessment	Variable
$v(x)$, $V(X)$	Value associated with x measure, Total value score	Variable
Ω	Vulnerability	Variable
M	Location in model	Parameter
W	Global Weight	Parameter
L	Local Weight	Parameter
D	deterrence (d_1), detection (d_2), delay (d_3) and response (r)	Variable
N	Number of Trials	Parameter

User comments

- Model Checks on structure
- Face validity:
 - SMEs 1,2,and 3 was shown the model and engaged in a discussion of its design and use guided by the semi-structured interview
 - Agreement that the model does what it claims and would be useful especially with what-if analysis
 - Hang up on defining vulnerability (not that big of a deal in practice)
 - User interface poor
 - Generalizeability: Yes, but decomposition although a very good approximation of most systems, might have to be changed to account for unique designs.
 - SCADA applicability and electric power
 - Model based on values
 - Weights, value functions and scores could be done with an entire team from the treatment plant.
 - The omega value sends a signal to the management: We need to “fill this gap.”