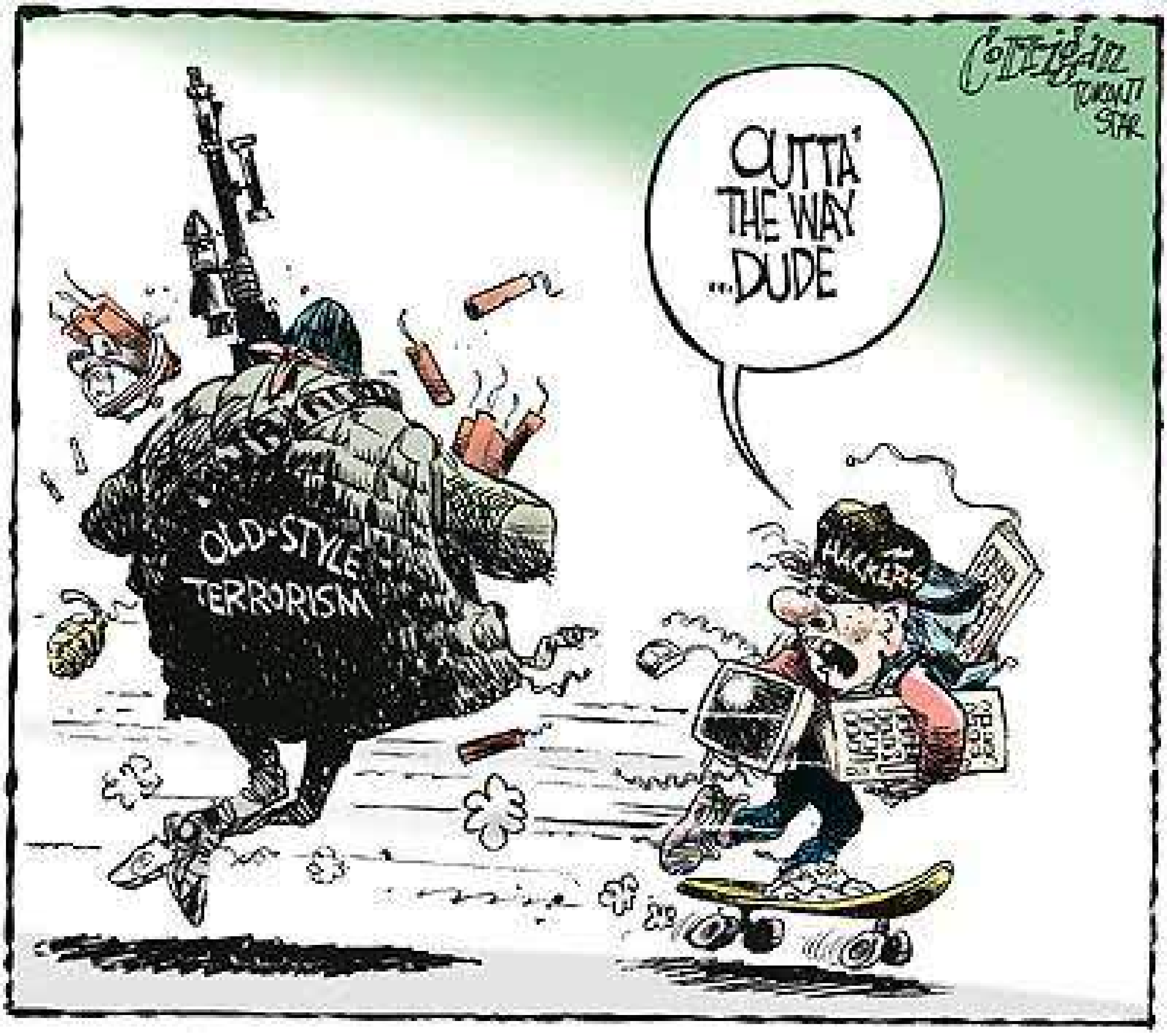
Cyber Terrorism of Water Supply Infrastructure

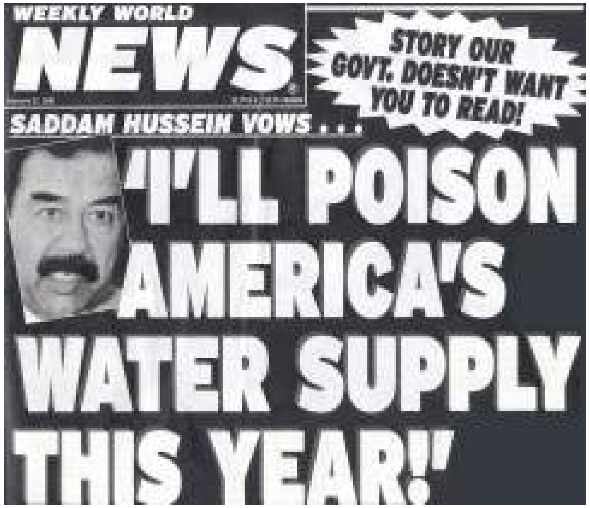
MAJ John B. Willis
LTC Thomas M. Cioppa, Ph.D.

TRADOC Analysis Center (TRAC)
Monterey, CA


TORONTO STAR
OUTTA' THE WAY ...DUDE
OLD-STYLE TERRORISM
HACKER

BEWARE
INTERNET SECURITY
GABLE

US water infrastructure faces large uncertainties in the character of threats and nature of system vulnerabilities


WEEKLY WORLD
NEWS
STORY OUR GOVT. DOESN'T WANT YOU TO READ!
SADDAM HUSSEIN VOWS . . .
'I'LL POISON AMERICA'S WATER SUPPLY THIS YEAR!'

February 2001 Tabloid Headline

"URGENT! Last night, the FBI received a signed threat from a very credible, well-funded, North Africa-based terrorist group indicating that they intend to disrupt water operations in 28 US cities.

Because the threat comes from a credible, well-known source, with an organizational structure capable of carrying out such a threat, the FBI has asked utilities, particularly large drinking water systems, to take precautions and to be on the look-out for anyone or anything out of the ordinary."

January 2001 AMWA E-mail to US Water Utilities

Time/CNN October 12, 2001 Poll

Do you think the following types of terrorist attacks are likely to occur in the US in the next 12 months?

Attack	Likely	Not Likely
At major public event	67%	29%
On some part of nation's water supply	**64%**	**32%**
Against the internet	59%	32%
On a nuclear power plant	58%	37%
Against another sky scraper	47%	50%

U.S. Forces discover files related to computerized water systems on al Qaeda computers in Afghan camps.

President's Critical Infrastructure Protection Board, Feb 2002

Cyber Terrorism of Water Supply Infrastructure

Problem

•President's Commission on Critical Infrastructure Protection (PCCIP) study concluded that cyber threats are a clear danger (risk) to all infrastructures.

•Among these critical infrastructures are the nation's water supply systems.

•Civilian water utilities support military installations and force projection

Objective

•Review/compare risk and vulnerability assessment methodologies

•Conduct survey of water providers

•Demonstrate value of these methodologies for military M&S

Client

- TRADOC HLS Directorate
- TRADOC DCSINT HISTO
- JFHQ-HLS NORTHCOM
- ERDC Fort Future (Army STO)

Deliverables

•Vulnerability Assessment Analysis

•Initiated Oct 02 (complete)

•Survey Analysis

•Web-based survey posted July 03

•Technical Report

•Sep 03

Executive Summary (1/2)

1. Military/civilian leaders are responsible for protecting our Nation’s critical infrastructure, communities, and symbols of national power from terrorists, home and abroad, as well as from natural disasters.
2. Public utilities support military force projection and DoD has a role in protecting critical infrastructure.
3. Cyber risk awareness to SCADA systems has increased significantly since 1996.
4. Internet-based attack trends indicate that the level of sophistication in attacks is increasing.
5. Consensus is forming that the trusted insider/disgruntled employee is more dangerous than other culprits of cyber attack.

Executive Summary (2/2)

6. Very little has been published in the way of rigorous vulnerability assessment methodologies.
7. Risk assessments are difficult to acquire because assessments are proprietary or classified.
8. Most risk assessments listed in the public domain are soft system studies relying almost exclusively on qualitative measures and SME.
9. A quantitative systems-based risk assessment and management methodology appears to provide the best approach.
10. Military M&S can support and benefit from risk assessment and management methodologies.

Motivation for Work

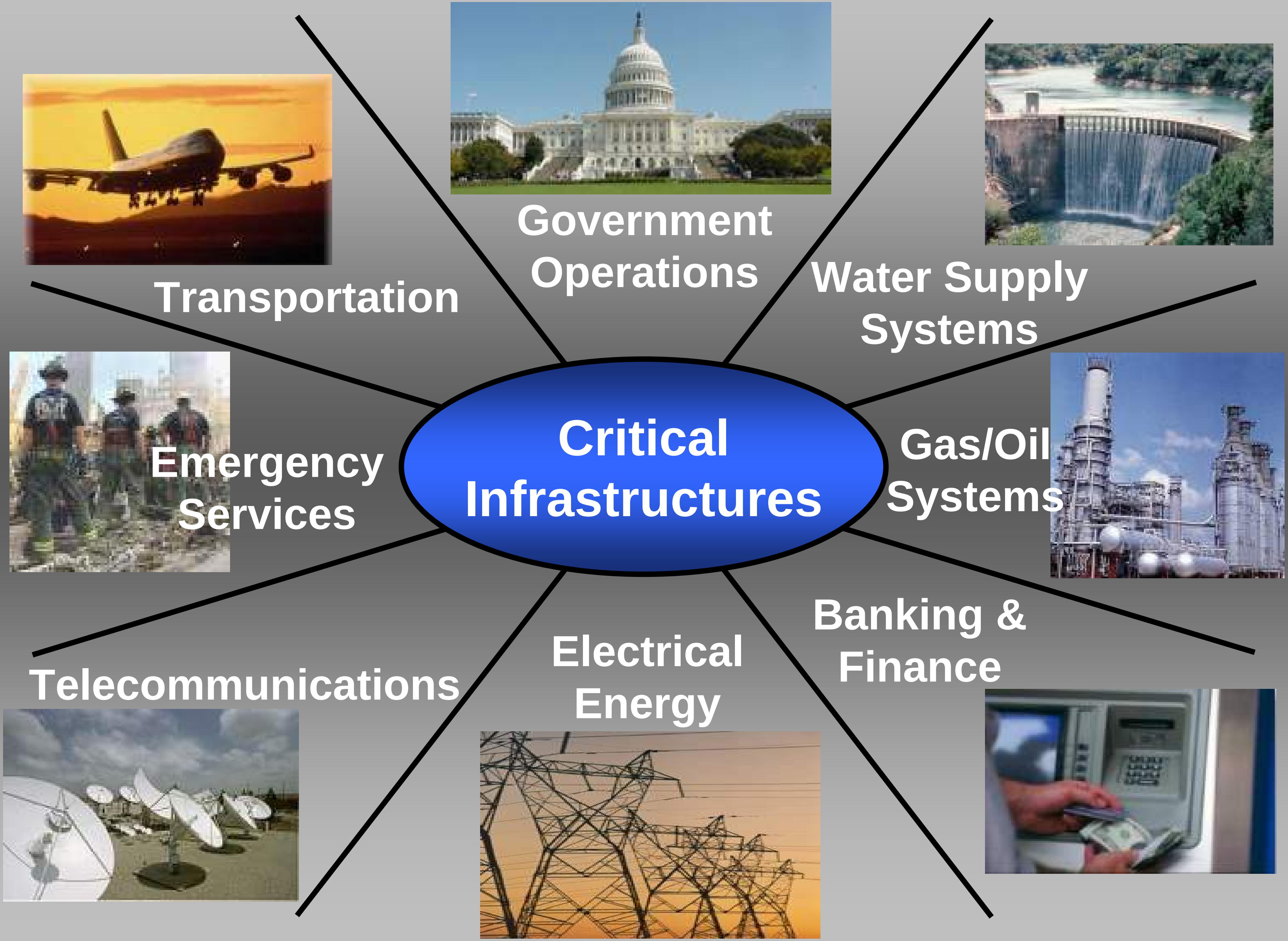
- DOJ-NPS Interagency Agreement
  - HLS Research and Technology Initiative
  - Focus on opportunities to strengthen U.S. capacity to deter, defeat and respond to threats to Homeland Security
- TRADOC HLS ICT Charter (signed May 02)
  - Requirement for Future Operation Capabilities that "…clearly address the Army's Homeland Security requirements in the preparation, prevention, deterrence, preemption, defense, and <u>response to threats and aggressions</u> directed towards U.S. territories, sovereignty, domestic population and <u>infrastructure</u>…"
- Army Homeland Operations (HLO) Concept
  - Defines Army's role in <u>infrastructure protection</u> and in <u>defense against cyber attacks</u>

Fort Future – Force Projection/Protection

- Construction Engineering Research Lab (CERL), Engineer Research and Development Center (ERDC)
- Reliable utility systems are key to Force Projection and Protection
- Developing methods, tools, models to plan, assess, optimize, and monitor the ability of utility systems to support Army Force Projection
- Water utility applications
  - Pilot testing water dynamic system models
  - System vulnerability assessments
  - CBR contaminant scenarios
  - Analysis of system operation modifications based on real-time modeling data

Definitions

- Homeland Security (HLS) is the prevention, preemption, and deterrence of, and defense against, aggression targeted at U.S. territory, sovereignty, domestic population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies. Homeland security is a national team effort that begins with local, state and federal organizations.
- DoD and NORTHCOM's HLS roles include Homeland Defense and Civil Support.
- Homeland Defense (HLD) is the protection of U.S. territory, domestic population and critical infrastructure against military attacks emanating from outside the United States.



Critical Infrastructures

Government Operations

Water Supply Systems

Gas/Oil Systems

Banking & Finance

Electrical Energy

Telecommunications

Emergency Services

Transportation

Current National Situation

- **US is faced with a significant force projection challenges**
  - **Southwest Asia**
  - **Eastern Europe**
  - **North Korea**
  - **Africa**
- **Hostile groups continue to threaten all aspects of the critical infrastructure with a hybrid (asymmetric) attack (Physical and Cyber)**
- **Private industry understands the risks, but lacks a unified methodology and funding to harden their assets**

Major Agencies/Programs

- Critical Infrastructure Assurance Office (CIAO)
  - DHS
- Cybersecurity Tracking, Analysis and Response Center (CSTARC)
  - DHS
- National Infrastructure Protection Center (NIPC)
  - FBI
- Water Information Sharing and Analysis Center (ISAC)
  - EPA, AMWA, AWWA
- Computer Crime and Intellectual Property Section (CCIPS)
  - DoJ
- Critical Infrastructure Protection Program (CIPP)
  - GMU/JMU
- TRADOC HLS Directorate
  - US Army
- JFHQ-HLS NORTHCOM
  - DoD
- National Infrastructure Simulation and Analysis Center (NISAC)
  - LANL, SNL
- Homeland Infrastructure Security Threats Office (HISTO)
  - Critical Infrastructure Assurance Program (CIAP) and Critical Infrastructure Vulnerability Assessment Program (CIVAP)
  - LANL, NORTHCOM
- JTF-Computer Network Operations (“Cyber Army”)
  - DoD
- Terrorist Threat Integration Center (TTIC)
  - DHS, FBI, CIA, DoD

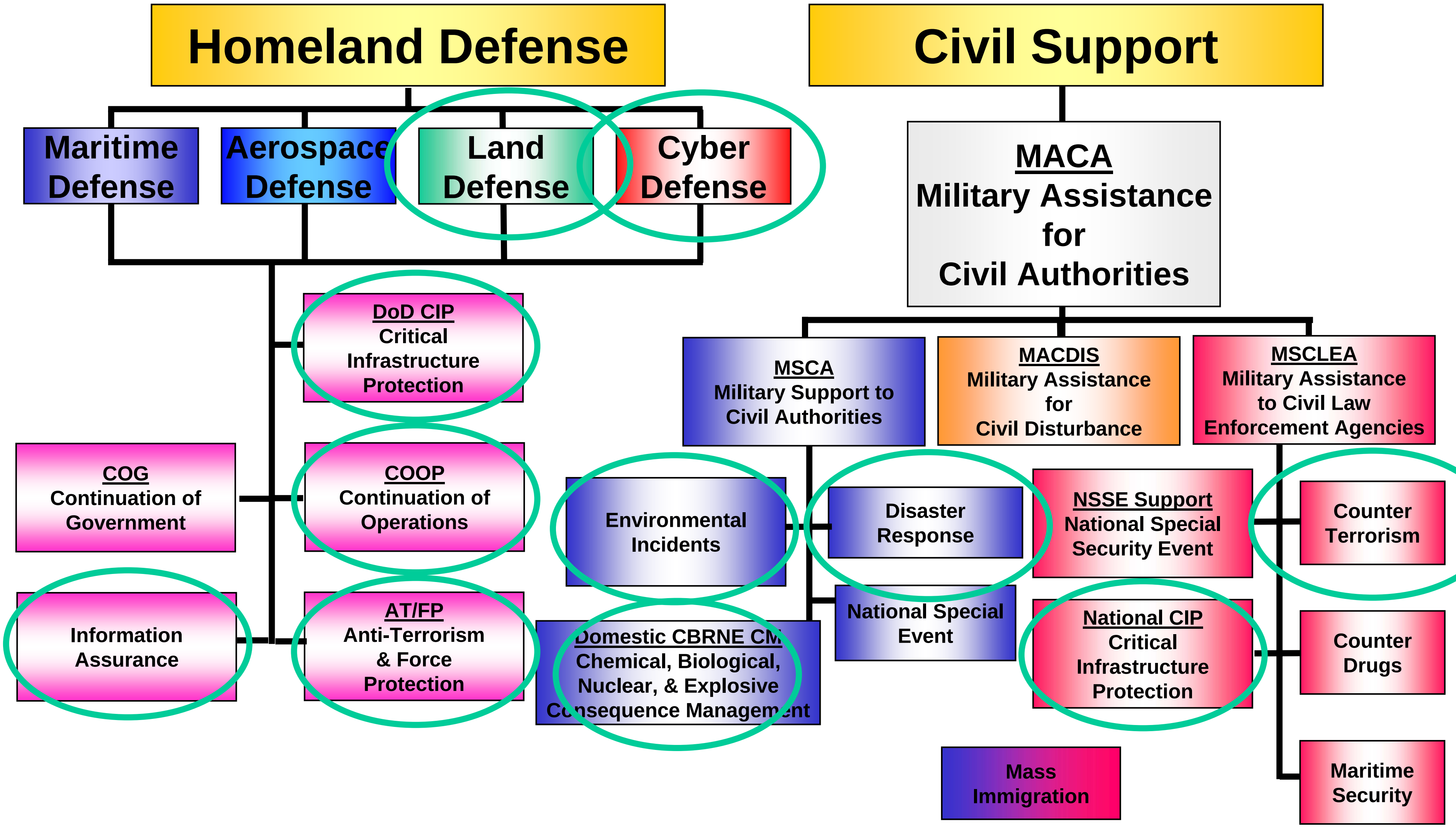
Stakeholders

- General Public
  - – Expect uninterrupted flow of water service
- Water Utility Companies
  - – Provide services that are potential targets of attack
  - – ~160,000 public drinking water systems in US
  - – ~370 systems serve over 100,000 customers each
- Industry
  - – Designs utility systems and software
- Government/Military
  - – Responsible for public safety/defense

DoD Focus

- Secretary of Defense 2002 Annual Report and 2001 QDR
  - Military forces need to be sized for defending the US
  - Homeland Security is DoD’s primary mission
    - Reserve Component focus (e.g. National Guard WMD-Civil Support Teams)
    - Required capabilities/specific units – undefined
- NORTHCOM
  - Responsible for defending the US including:
    - Ocean approaches
    - Coastline
    - Seaports
    - Airspace
  - Assist civil authorities during emergencies within the US
- Army
  - Top Priority: Protecting military forces and their installations, embarkation ports/airfields, and information systems.

DoD HLS Key Functions



Homeland Defense

Maritime Defense

Aerospace Defense

Land Defense

Cyber Defense

DoD CIP
Critical Infrastructure Protection

COG
Continuation of Government

COOP
Continuation of Operations

Information Assurance

AT/FP
Anti-Terrorism & Force Protection

Civil Support

MACA
Military Assistance for Civil Authorities

MSCA
Military Support to Civil Authorities

MACDIS
Military Assistance for Civil Disturbance

MSCLEA
Military Assistance to Civil Law Enforcement Agencies

Environmental Incidents

Domestic CBRNE CM
Chemical, Biological, Nuclear, & Explosive Consequence Management

Disaster Response

National Special Event

NSSE Support
National Special Security Event

National CIP
Critical Infrastructure Protection

Mass Immigration

Counter Terrorism

Counter Drugs

Maritime Security

○ = Link to Cyber Attacks vs. Water Infrastructure

Army Homeland Security Capabilities

- Detection and Decontamination
  - WMD-Civil Support Teams
  - Chemical/Chemical Recon and Decon
  - Biological Integrated Detection System
  - Technical Escort
  - Chem/Bio Rapid Response Team
- Medical Services
  - Medical Groups
  - Preventive Maintenance
  - Field Hospitals
  - Aviation-Evacuation
- Perimeter Security
  - Military Police
  - Infantry
- Emergency Services
  - Corps of Engineers
  - Quartermaster

Army Tasks for Critical Infrastructure Protection

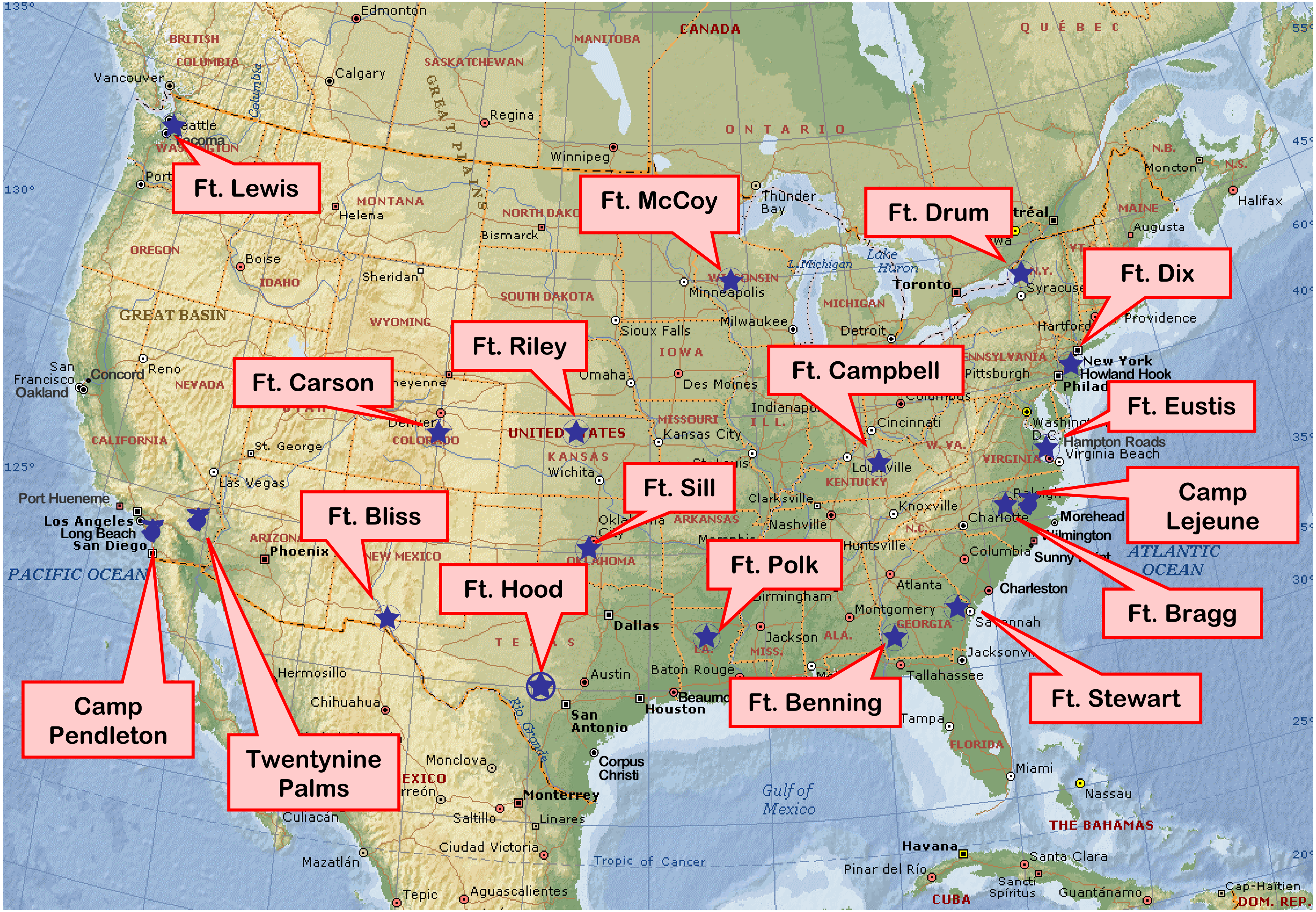
- Ensure continuity of government operations by protecting facilities and personnel
- Reduce vulnerabilities of civilian physical infrastructure and information systems
- Provide area defense of critical infrastructure assets
- Consequence management
- Military presence to provide reassurance to American people

Source: *The US Army and the New National Security Strategy*, RAND, 2003

Force Projection

- Power Projection Platforms
  - – 15 Army Installations
  - – 3 Marine Corps Installations
  - – Navy and Air Force project power directly from home bases
- Strategic Sea Ports
  - – 17 ports support Army and Marine deployments
- Strategic Aerial Ports
  - – 17 airports support Army and Marine Corps deployments

Force Projection Platforms (18)



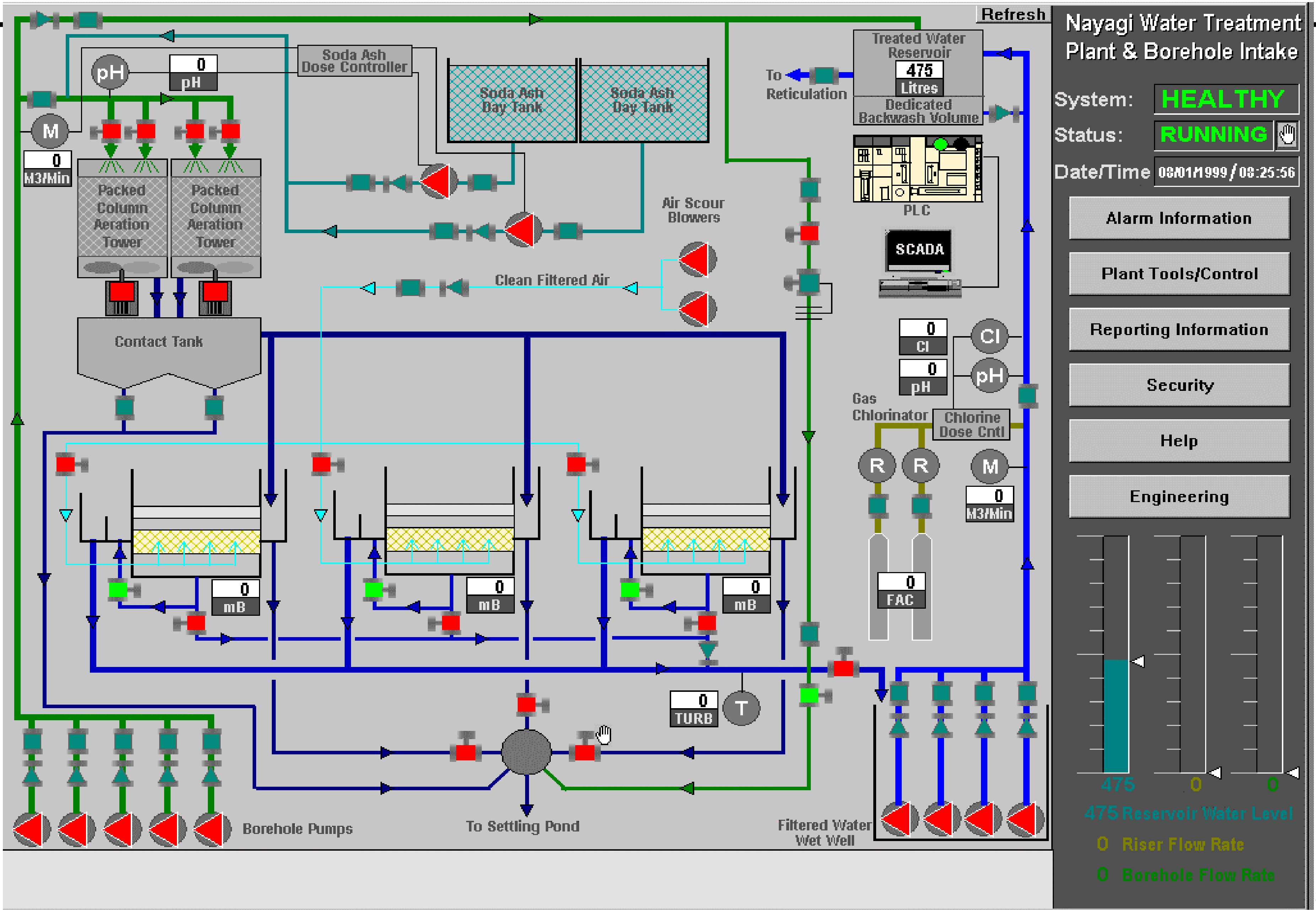
Water Supply Systems

- Reservoirs; holding facilities
- Aqueducts; transport systems
- Filtration; cleaning systems
- Pipelines
- Cooling systems
- Waste water systems
- Firefighting systems

Water Supply Control Systems

- SCADA – Supervisory Control and Data Acquisition
  - Uses MTU (Master Terminal Unit) and RTUs (Remote Terminal Units)
  - Open-loop; long distance
- DCS – Distributed Control System
  - Uses PLC (Programmed Language Controllers)
  - Closed-loop; local area network (LAN)

SCADA Display



Nayagi Water Treatment Plant & Borehole Intake

System: HEALTHY

Status: RUNNING

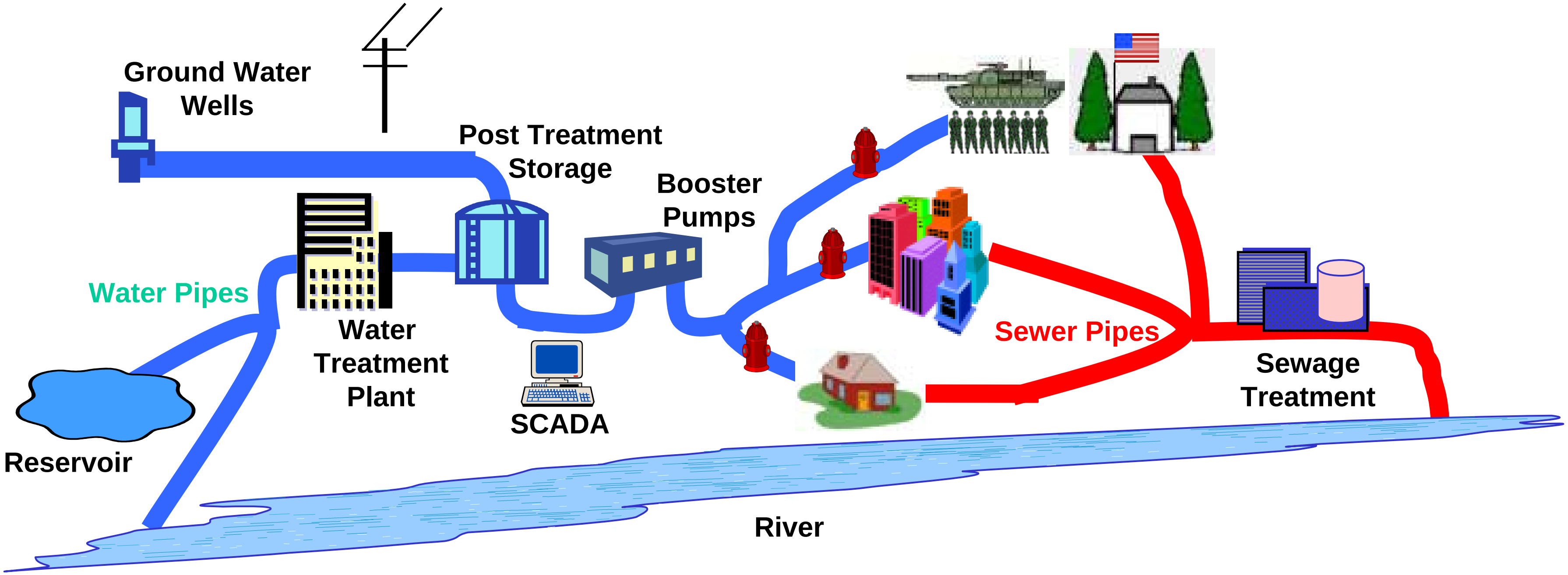
Date/Time 08/01/1999 / 08:25:56

475 Reservoir Water Level

0 Riser Flow Rate

0 Borehole Flow Rate

Water systems are vulnerable to attack at multiple points: Risks and consequences vary by threat and location



Source ⟶ Treatment ⟶ Distribution ⟶ Sewer/Treatment ⟶ Discharge

Types of Attacks:
Physical, Contamination, Cyber

Water System Vulnerabilities

- Source Water
  - Drought, Flood, Contamination, Degradation
- Treatment Plant
  - Facility Attack, CBRNE
- Pump Station
  - Lack of Redundancy
- Tankage
  - Isolation
- Distribution
  - Hydrants, Valve Pressure Transients
- SCADA
  - Interdependency with Power, Interception, Lack of Encryption, Physical or Cyber Attack, Data Corruption

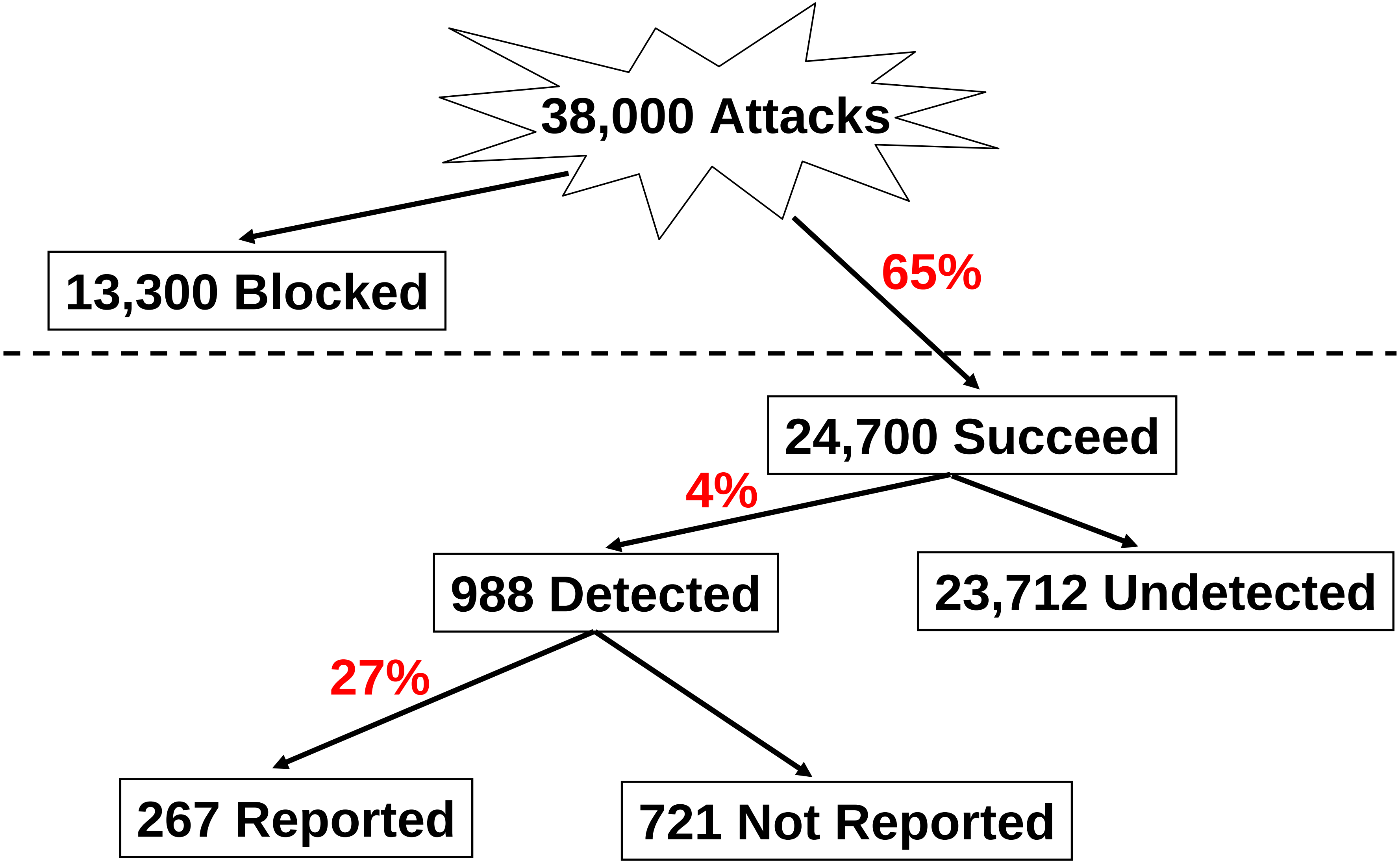
Vulnerabilities

- Software and hardware weaknesses
  - 40% of water facilities allow operators direct access via internet
  - 60% of water SCADA systems accessible by modem
- Human weaknesses (e.g. training)
- Lack of a security culture
  - Productivity vs. Security
  - Example: Power plant with all control systems set for access using the same password

Each of these vulnerabilities can be exploited to allow intruders unauthorized access to information systems, leaving the information or those systems subject to manipulation or other forms of attack.

1995 GAO Computer System Vulnerability Study

DISA (Defense Information Systems Agency)



38,000 Attacks

13,300 Blocked

65%

24,700 Succeed

4%

988 Detected

23,712 Undetected

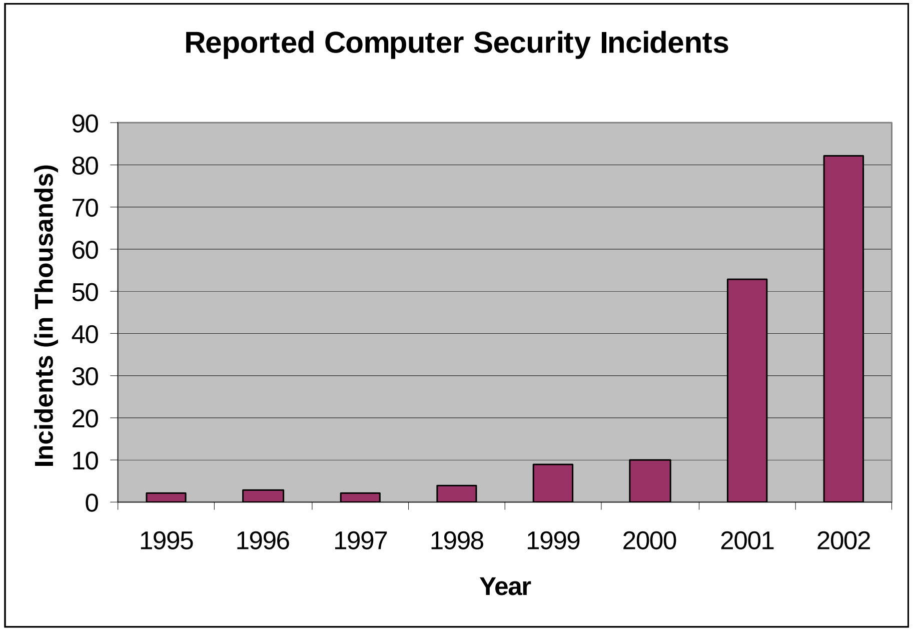
27%

267 Reported

721 Not Reported

Computer Security Breaches

- **2002 Report: Computer Crime and Security Survey**
  (Computer Security Institute and FBI's Computer Intrusion Squad)
  - **90% of respondents had detected breaches**
- **Reported incidents to CERT Coordination Center**
  - **1999 – 9,859 incidents**
  - **2001 – 52,658 incidents**
  - **2002 – 82,094 incidents**



  - **80% of incidents likely go unreported**
    - **Not recognized as attack**
    - **Reluctance to report**

Two Forms of Cyber Attack

- **Against Data**
  - Stealing/corrupting data and denying services
  - Credit card number theft, web site vandalism, occasional denial-of-service assault
- **Against Control Systems**
  - Disable or take power over distributed control systems that regulate water, electricity, railroads, etc.
  - Systems are increasingly using the internet to transmit data or use LANs with “leaky” firewalls

Types of Cyber Attack

- Denial of Service
  - Preventing a computer from performing its function
  - Smurf, Spam, DNS redirect
- Web Page Defacements
  - Replace HTML files
  - Hacker war after US spy plane incident in China
- Viruses/Worms
  - Destructive code inserted and executed on victims' computer; worms are self-propagating
  - Nimda, Code Red
- Trojan Horses
  - Destructive code hidden within useful code
  - Badtrans – sends system and password info back to author
- Network Intrusions
  - Unauthorized network entry to gain "root" access
  - Gain network administrator functions

SCADA vulnerabilities

- Old software or standard vendor software with well known vulnerabilities
  - Hacker: “If you are running a Microsoft-based SCADA system, you have a target painted on your head. The volume of reading material on how to close the security holes in Windows NT is huge and the knowledge required to follow even the step-by-step instructions is very high and not the in the skill set of Joe Water Supply Company.”
- Can be penetrated without detection
- Can’t distinguish between attacks and system failure
- Can be manipulated remotely
- Could potentially inflict physical damage
- Courses on how to use control systems open to anyone with $
- Psychological impact of attacks to critical infrastructures
  - Could affect the confidence of the population on a particular sector/activity related to SCADA systems.

Cyber Terrorists – Who are they?

- Hacktivists
  - Politically motivated (e.g. Israeli vs. Palestinian hackers; website defacement)
- Terrorist Organizations
  - Web sites used for recruiting, fund-raising, target research
- Foreign Governments
  - Government trained hackers used to attack other nation's computer power
- Individuals
  - Hackers, Script Kiddies, <u>Insiders</u>

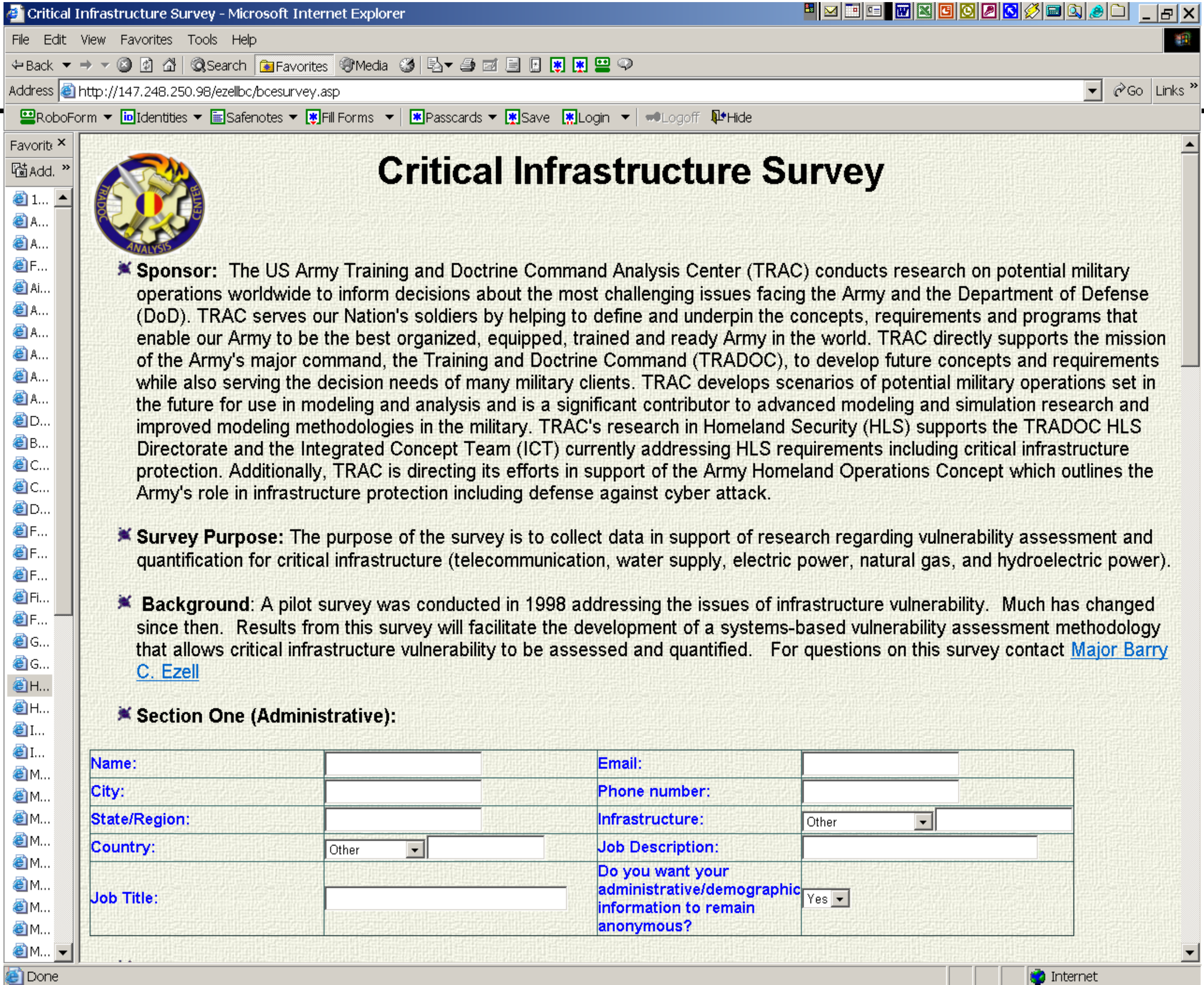
#1 Threat to SCADA

Are Cyber Attacks a Real Threat?

- **Skeptics:**
  - Cyber attacks do not have the shock effect sought by terrorists
  - Difficult to knock out infrastructure with cyber attacks; easier to bomb
  - Lots of money and sophisticated skills are needed for successful attacks
- **Believers:**
  - Millions of black boxes controlling infrastructure systems
  - Systems are now internetted (but were initially designed as stand alone systems)
  - Encryption programs and security culture needed now

Water Supply Survey

- Control systems in use
- Access
  - LAN, Dial-in, etc.
- Threats
  - Hackers, employees, terrorists, etc.
- Attack tools
  - User command, scripts, programs, etc.
- Consequences of attacks
  - Information corruption/disclosure
  - Denial of service


Critical Infrastructure Survey - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
RoboForm Identities Safenotes Fill Forms Passcards Save Login Logoff Hide
Favorites
Add.
TRADOC ANALYSIS CENTER
Done
Internet

http://147.248.250.98/ezellbc/bcesurvey.asp

Critical Infrastructure Survey

- **Sponsor:** The US Army Training and Doctrine Command Analysis Center (TRAC) conducts research on potential military operations worldwide to inform decisions about the most challenging issues facing the Army and the Department of Defense (DoD). TRAC serves our Nation's soldiers by helping to define and underpin the concepts, requirements and programs that enable our Army to be the best organized, equipped, trained and ready Army in the world. TRAC directly supports the mission of the Army's major command, the Training and Doctrine Command (TRADOC), to develop future concepts and requirements while also serving the decision needs of many military clients. TRAC develops scenarios of potential military operations set in the future for use in modeling and analysis and is a significant contributor to advanced modeling and simulation research and improved modeling methodologies in the military. TRAC's research in Homeland Security (HLS) supports the TRADOC HLS Directorate and the Integrated Concept Team (ICT) currently addressing HLS requirements including critical infrastructure protection. Additionally, TRAC is directing its efforts in support of the Army Homeland Operations Concept which outlines the Army's role in infrastructure protection including defense against cyber attack.

- **Survey Purpose:** The purpose of the survey is to collect data in support of research regarding vulnerability assessment and quantification for critical infrastructure (telecommunication, water supply, electric power, natural gas, and hydroelectric power).

- **Background**: A pilot survey was conducted in 1998 addressing the issues of infrastructure vulnerability. Much has changed since then. Results from this survey will facilitate the development of a systems-based vulnerability assessment methodology that allows critical infrastructure vulnerability to be assessed and quantified. For questions on this survey contact Major Barry C. Ezell

- **Section One (Administrative):**

Name:		Email:	
City:		Phone number:	
State/Region:		Infrastructure:	Other ▾
Country:	Other ▾	Job Description:	
Job Title:		Do you want your administrative/demographic information to remain anonymous?	Yes ▾

Survey of Water Utilities (1998)

- 47% believe the disgruntled employee is the number one concern followed by 13% for internet hackers
- 41% spend less than 10% of time on system security. 51% spend no time
- Ten utilities (10 out of 50) reported attempts, successful unauthorized access, or use of their system
- Corruption of information and denial of service were seen by respondents as the major concerns from a cyber intrusion
- 17% did not know the number of valves and 11% were unclear regarding the number pumps they controlled
- 39% felt their system was safe from unauthorized access and only 37% from unauthorized use
- 55% agreed that the ultimate objective of an attacker is damage followed by challenge or status

Survey of Water Utilities (2003)

Case Study – Monterey Peninsula

- **Water services provided by Cal-Am**
- **38,900 Customers**
  - **Monterey, Carmel, Pacific Grove, Pebble Beach, Sand City, Seaside**
- **Largest Customer Groups**
  1. **La Mesa Navy Housing Area**
  2. **Presidio of Monterey – Defense Language Institute**
  3. **Community Hospital of Monterey Peninsula**
  4. **Naval Postgraduate School**
- **Water Source: San Clemente Reservoir and 28 wells**
- **Components**
  - **59 tanks**
  - **49 pumping plants**
  - **Water treatment plant**

Case Study – Monterey Peninsula

- Greatest perceived human threat:
  - Disgruntled employee or other insider
- Worst Consequence (physical attack):
  - Damage/contamination at treatment plant
- Worst Consequence (cyber attack):
  - Disrupting telephone line-based control system
- Scenarios studied in the past:
  - Earthquakes and floods
- Current Focus:
  - Installation of new SCADA system

Cyber Security Efforts

- DHS agencies addressing cyber security
  - Critical Infrastructure Assurance Office (CIAO)
  - National Infrastructure Protection Center (NIPC)
  - Federal Computer Incident Response Center (FCIRC)
  - National Communications System (NCS)
- In the summer of 2002, the U.S. EPA mandated that all community water utilities that serve more than 3,300 people complete vulnerability assessments by the end of June 2004.
- EPA provided $51M in grants to assist water utilities in conducting vulnerability assessments and response plans

Very little has been published in the way of rigorous vulnerability assessment methodologies.

- No agreed upon definition of vulnerability
- Vulnerability assessment guidance: ad hoc checklists
- SCADA should be viewed as system of a larger complex organizational system.
- Implication: Classic risk assessment questions:
  - what can go wrong,
  - what is the likelihood, and
  - what are the consequences, should be preceded by the question:
  - what is the system in focus
- The system in focus and the context must be understood before meaningful risk and vulnerability assessment is undertaken.

Risk/Vulnerability Assessment Methodologies

- Risk Assessment Methodology – Water (RAM-W)
  - Sandia National Laboratory
- CARVER + Shock
  - Joint Pub 3-05.5
- Infrastructure Risk Analysis Model (IRAM)
  - ODU, Stevens Institute of Technology, Tek Soft

RAM-W Program

- How to plan and prioritize for your assessment
- How to identify threats to your utility
- How to identify facilities and assets that need to be protected
- How to understand the consequences of the loss of an asset
- How to evaluate your system's effectiveness in preventing an attack
- How to assess your risks
- How to develop a plan to reduce risk through operational changes

RAM-W Methodology

- Risk Equation

$R = P_a \times C \times (1-P_e)$ where:

R = Risk

P_a = Probability that something will happen

C = Consequences if something happens

P_e = Effectiveness of the security and response mitigation system

R, P_a, C, and P_e all have values from 0 to 1

If P_a, C, or $(1 – P_e) = 0$, then there is no risk

RAM-W Methodology (cont.)

- Identify System
  - Population/customers served
  - Critical customers (hospitals, military/govt., high-usage commercial users
  - High profile events attracting national attention (sports, conferences, etc.)
  - Location of water systems emergency command center
- Assemble Risk Assessment Team
  - Identify Lead Associate
  - Identify associates from management, operations, quality, engineering, loss control, and personnel.
- Identify Facilities and Pressure Gradients
  - Sources, pumps, plants, boosters, storage, mains, dams, distribution systems
- Compile Information for each Facility
  - e.g. for SCADA: hardware/software, users, access, redundancies

RAM-W Methodology (cont.)

- Gather Facility Documentation
  - Site plans, system maps, risk management plans
- Identify System Demands
  - Flow rates, gradients, critical levels
- Weight Criteria Critical to Operations
  - Water quality, service, critical customers
- Rank/Weight all Facilities using Critical Criteria

Threat Assessment

- Focus on “Design Basis Threats” (DBT) – Maximum credible threat against which a water system’s security and operational practices should be designed to defend
- Intrusion
  - – Destroy/disable equipment, contamination, hazardous chemical release
- Blast
  - – Destroy/disable facilities, hazardous chemical release
- Cyber Threat
  - – Access SCADA/DCS and disrupt operations
- Distribution System Contamination
  - – Toxic substances introduced through main or hydrant

Facility Characterization (Calculating “C”)

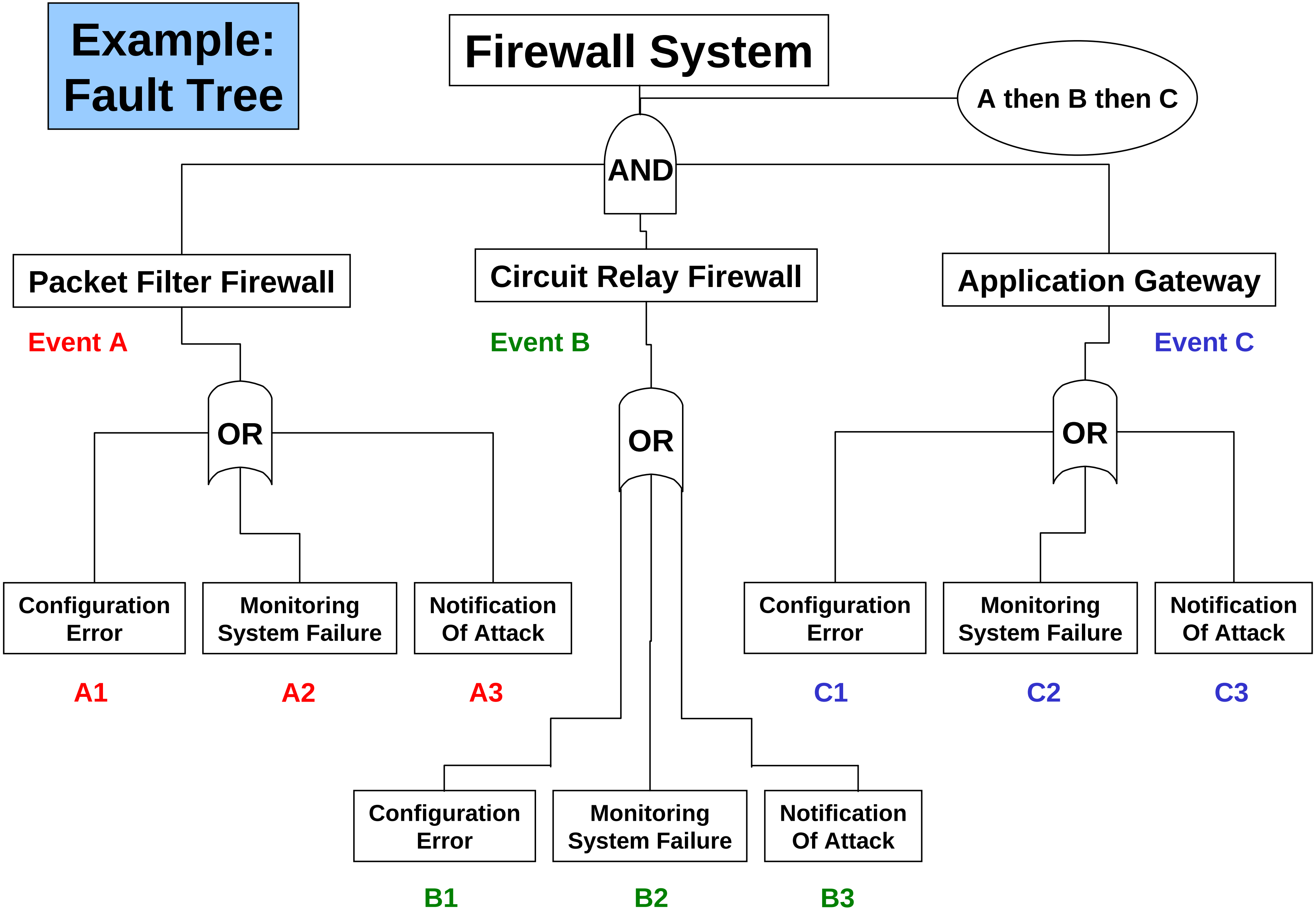
- Understand Redundancy and Reliability of Facility
  - Multiple water sources, manual vs. DCS operation, emergency recovery means (generators, bottled water, etc.)
- Create Facility Specific Consequence Table for each Threat Condition
- Prioritize and Weight Measures of Consequence
- Calculate Consequence (C) Value for Components and Overall System
  - High: 1.0 – 0.7
  - Medium: 0.6 – 0.4
  - Low: 0.3 – 0.0

Security System Effectiveness (Calculating “P_e”)

- Identify existing Physical Protection Systems (PPS)
  - Fencing/gates, access control, lighting, alarms, sensors, guards, firewalls/passwords
- Identify Operational Aspects of the System
  - System storage/supplies, remote monitoring/control, emergency power
- Create an Adversary Sequence Diagram (ASD) or Fault Tree
  - Identify potential target assets, route/sequence of attack, centers of gravity
- Perform Path Analysis
  - Identify PPS(s) for the ASD that could detect/delay an adversary
  - Assign probabilities for each PPS to detect adversary and estimate delay times
- Estimate PPS Effectiveness

$0.0 < P_e < 0.2$	Destruction and departure before response
$0.2 < P_e < 0.4$	Destruction with arrival of response team
$0.4 < P_e < 0.6$	Caught during destructive act
$0.6 < P_e < 0.8$	Response before destructive act begins
$0.8 < P_e < 1.0$	Response before intrusion

Example: Fault Tree



Firewall System

A then B then C

AND

Packet Filter Firewall

Circuit Relay Firewall

Application Gateway

Event A

Event B

Event C

OR

OR

OR

Configuration Error

Monitoring System Failure

Notification Of Attack

Configuration Error

Monitoring System Failure

Notification Of Attack

A1

A2

A3

C1

C2

C3

Configuration Error

Monitoring System Failure

Notification Of Attack

B1

B2

B3

Risk Equation Analysis (Calculate “R”)

- Use values of C and P_e determined from analysis

$$R = P_a \text{ x } C \text{ x } (1-P_e)$$

- Determine if Risk is acceptable

$R > 0.75$	High Risk Facility
$0.75 > R > 0.50$	Med/High Risk Facility
$0.50 > R > 0.25$	Med/Low Risk Facility
$R < 0.25$	Low Risk Facility

- Identify Potential Improvements to Lower Risk
  - Prioritize (R x Critical Ranking)
  - Identify Improvements in Operations, Security, Response, etc.

CARVER + Shock

- Criticality
- Accessibility
- Recuperability
- Vulnerability
- Effect
- Recognizability
- Shock

(Consider Asymmetric Threat, at a minimum cyber and physical)

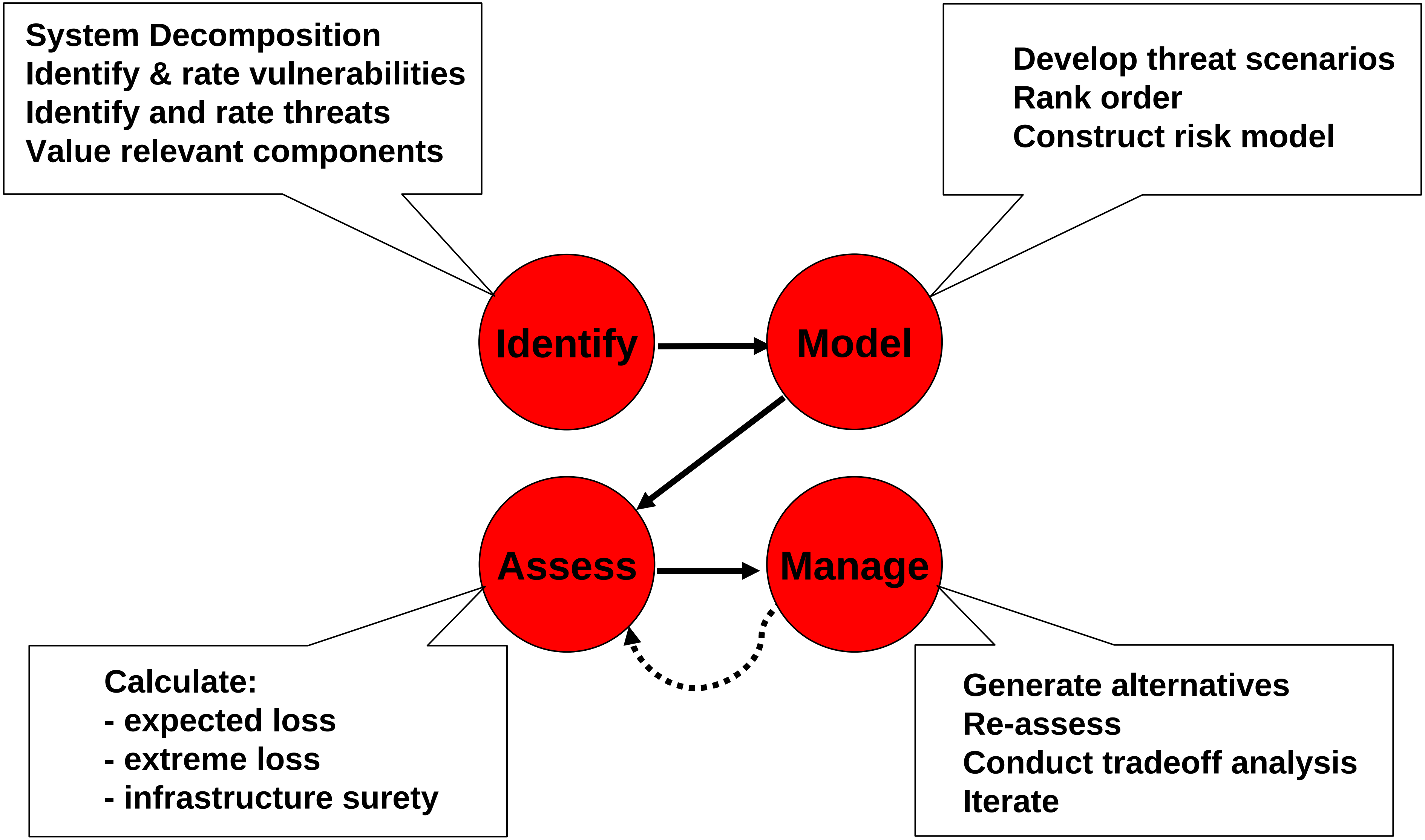
Source: Joint Pub 3-05.5 Joint Special Operations Targeting and Mission Planning Procedures, 10 Aug 93

CARVER + Shock Matrix

Target	C	A	R	V	E	R	Shock	Total
Intake Pump Station	7	3	6	2	3	9	6	35
Pump System	9	3	8	1	9	9	6	45
Source	5	4	4	3	3	9	6	34
Water Transfer	5	8	3	8	5	8	3	42
Mains	6	9	7	9	5	8	3	47
Backflow Valves	3	6	3	4	3	8	3	30
Water Treatment	9	9	9	10	9	10	8	64
Chemical Treatment	8	10	9	10	9	9	8	63
Control Center	10	8	10	9	9	10	8	64
Monitor/Control Center	9	7	9	9	10	5	9	58
SCADA/Switches	9	7	3	8	10	8	10	55
Computer Hardware	9	8	10	9	9	10	9	64

Ratings are 1 to 10 with 10 highest. Highest total scores annotate preferred targets.

Infrastructure Risk Analysis Model (IRAM)



System Decomposition
Identify & rate vulnerabilities
Identify and rate threats
Value relevant components

Develop threat scenarios
Rank order
Construct risk model

Identify

Model

Assess

Manage

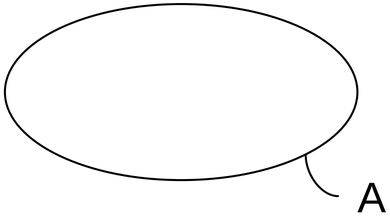
Calculate:
- expected loss
- extreme loss
- infrastructure surety

Generate alternatives
Re-assess
Conduct tradeoff analysis
Iterate

Risk Assessment and Management

- **What can go wrong?**
- **How likely is it?**
- **What are the consequences?**

Risk = $\{S_a,L_a,X_a\}_A$

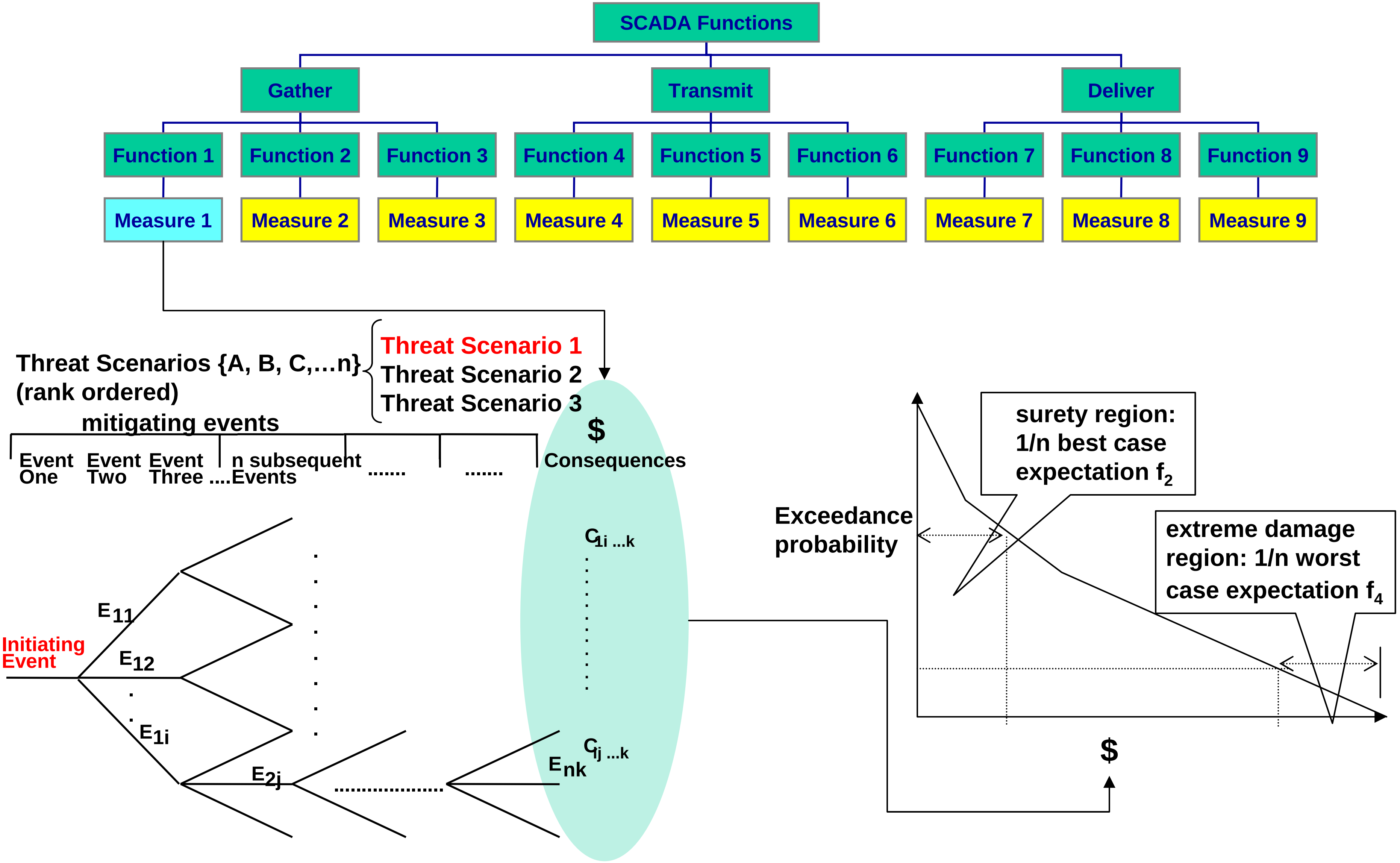


Kaplan and Garrick 1981. “On the quantitative definition of risk”, <u>Risk Analysis</u> 1(1): 11-27

- **What can be done?**
- **What are the tradeoffs in terms of all costs, risks, and benefits?**
- **What are the impacts of current decisions to future options?**

Haimes 1991. “Total risk management”, <u>Risk Analysis</u> 11(2):169-171.

Dynamic multiple-objective decision analysis models incorporate risk and uncertainty by placing distributions on extreme event probabilities or on the weights assigned to value model evaluation measures. Component vulnerability is used to decide on threat scenarios.



SCADA Functions

Gather

Transmit

Deliver

Function 1

Function 2

Function 3

Function 4

Function 5

Function 6

Function 7

Function 8

Function 9

Measure 1

Measure 2

Measure 3

Measure 4

Measure 5

Measure 6

Measure 7

Measure 8

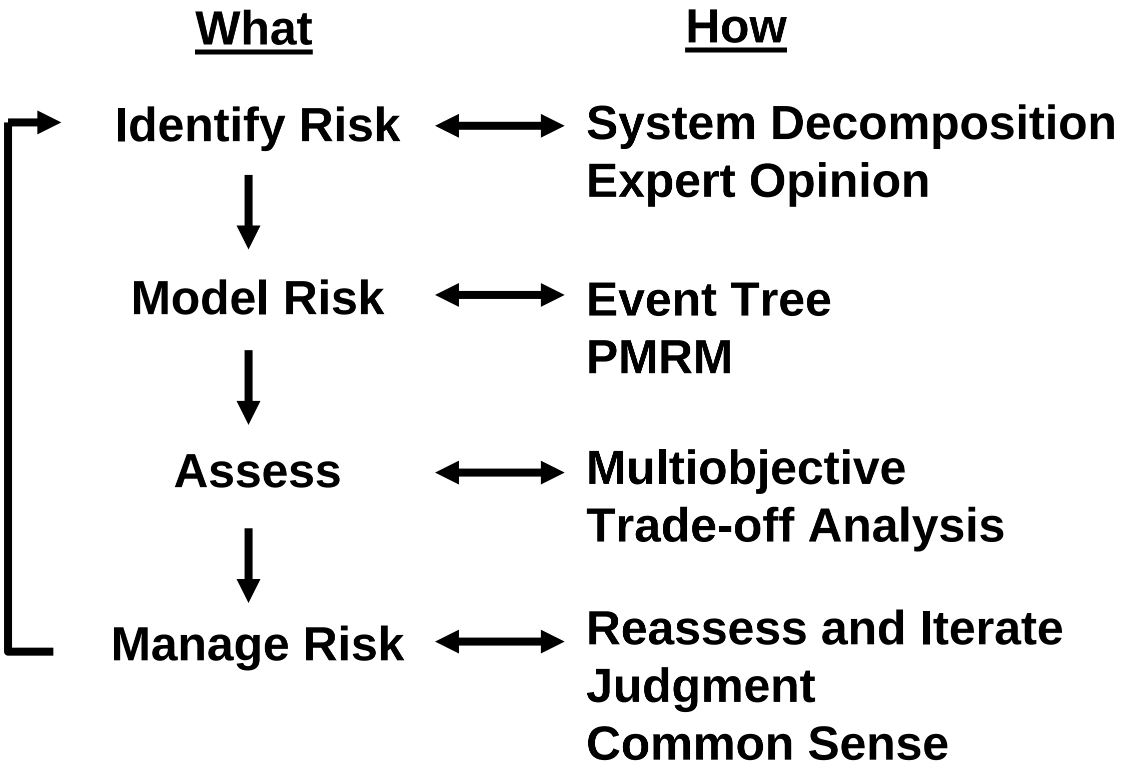
Measure 9

Threat Scenarios {A, B, C,…n}
(rank ordered)

Threat Scenario 1
Threat Scenario 2
Threat Scenario 3

SCADA System Risk Management Framework

- Builds on existing probabilistic risk assessment (PRA) methodology
- May assist decision-makers in understanding cyber intrusion risk, consequences, trade-offs



What

How

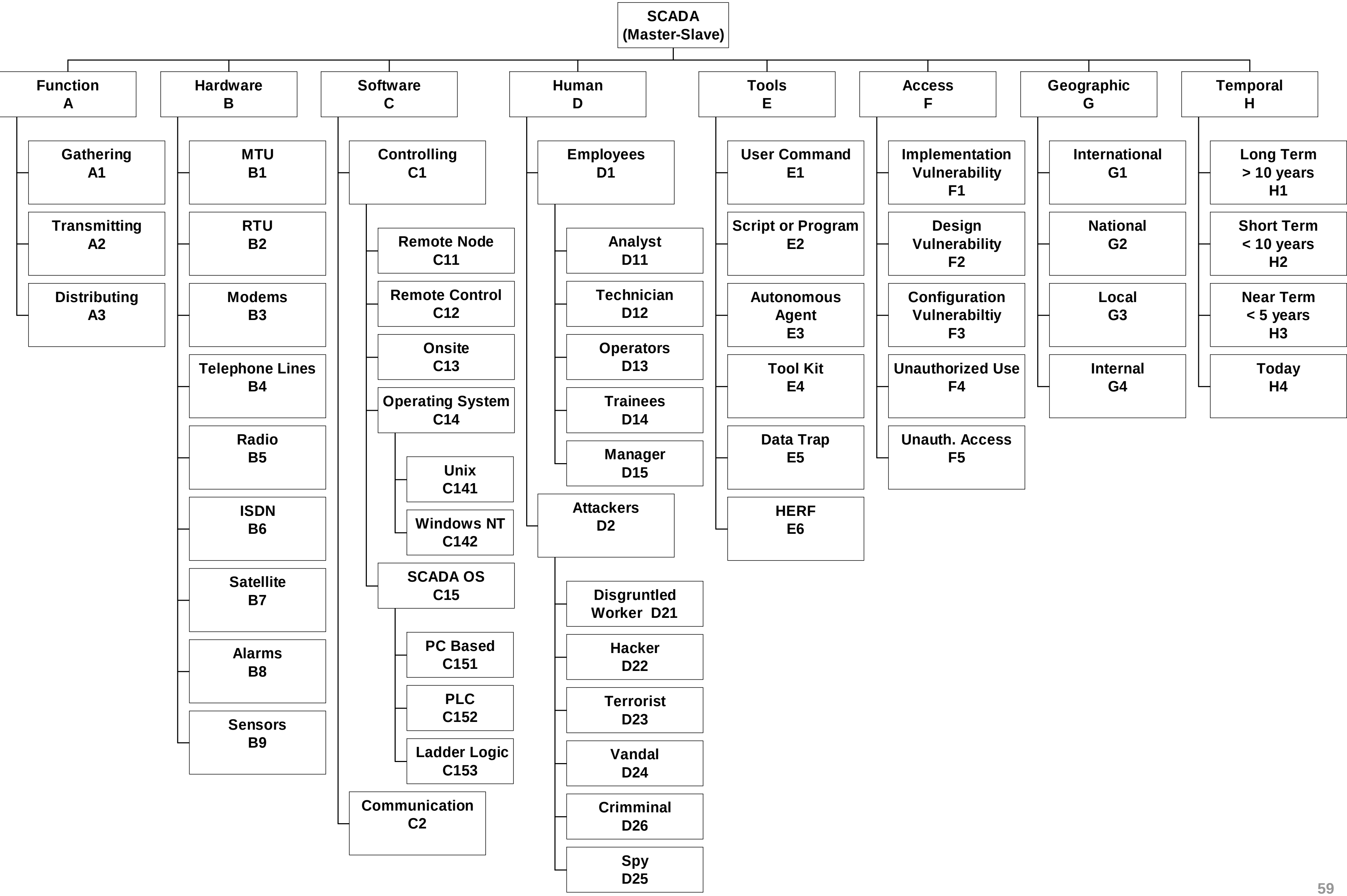
Identify Risk ⟷ System Decomposition, Expert Opinion

Model Risk ⟷ Event Tree, PMRM

Assess ⟷ Multiobjective Trade-off Analysis

Manage Risk ⟷ Reassess and Iterate, Judgment, Common Sense

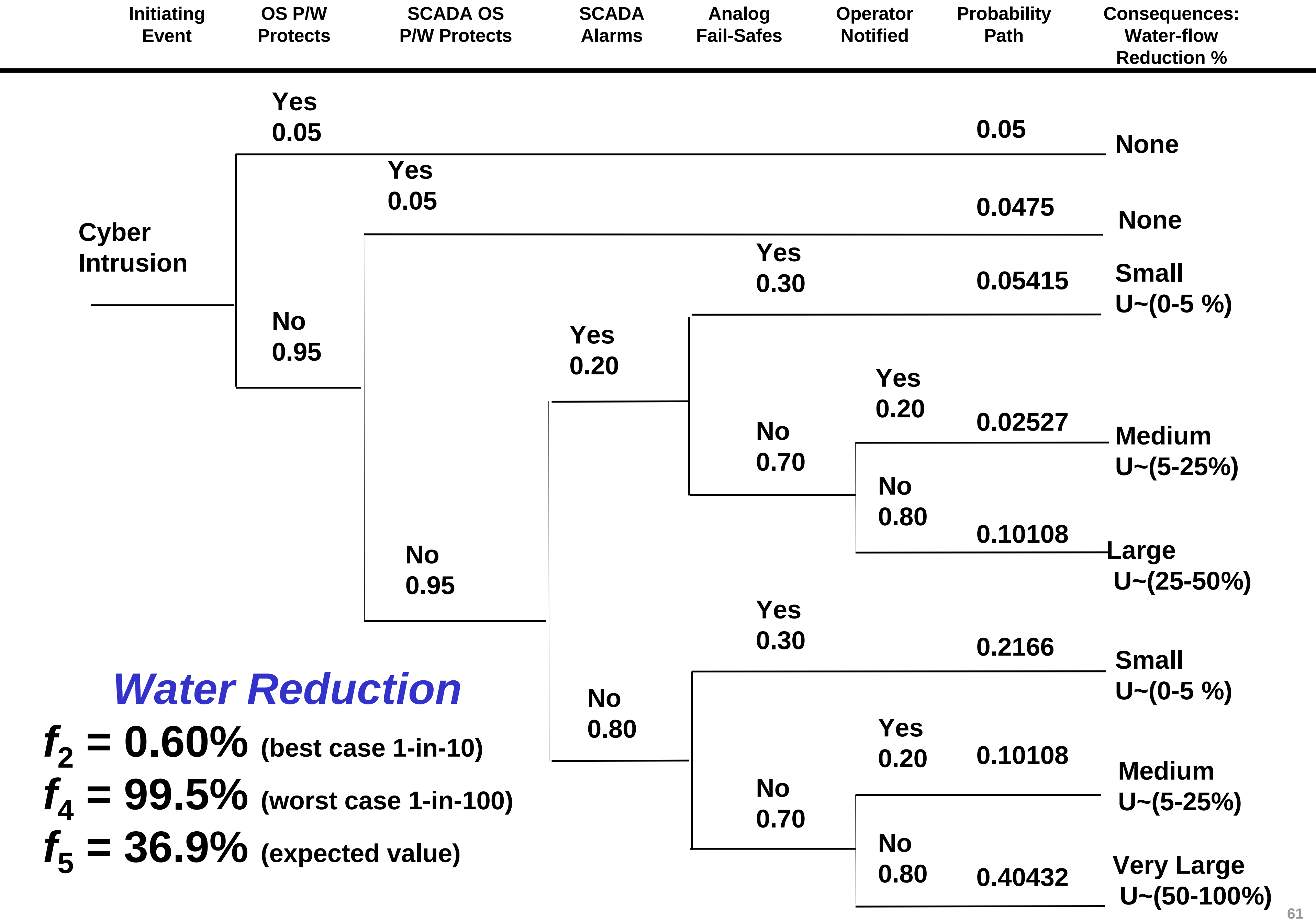
SCADA System Decomposition



- SCADA (Master-Slave)
  - Function A
    - Gathering A1
    - Transmitting A2
    - Distributing A3
  - Hardware B
    - MTU B1
    - RTU B2
    - Modems B3
    - Telephone Lines B4
    - Radio B5
    - ISDN B6
    - Satellite B7
    - Alarms B8
    - Sensors B9
  - Software C
    - Controlling C1
      - Remote Node C11
      - Remote Control C12
      - Onsite C13
      - Operating System C14
        - Unix C141
        - Windows NT C142
      - SCADA OS C15
        - PC Based C151
        - PLC C152
        - Ladder Logic C153
    - Communication C2
  - Human D
    - Employees D1
      - Analyst D11
      - Technician D12
      - Operators D13
      - Trainees D14
      - Manager D15
    - Attackers D2
      - Disgruntled Worker D21
      - Hacker D22
      - Terrorist D23
      - Vandal D24
      - Crimminal D26
      - Spy D25
  - Tools E
    - User Command E1
    - Script or Program E2
    - Autonomous Agent E3
    - Tool Kit E4
    - Data Trap E5
    - HERF E6
  - Access F
    - Implementation Vulnerability F1
    - Design Vulnerability F2
    - Configuration Vulnerabiltiy F3
    - Unauthorized Use F4
    - Unauth. Access F5
  - Geographic G
    - International G1
    - National G2
    - Local G3
    - Internal G4
  - Temporal H
    - Long Term > 10 years H1
    - Short Term < 10 years H2
    - Near Term < 5 years H3
    - Today H4

Partitioned Multi-objective Risk Method (PMRM)

- Tool for quantifying/reducing risks of extreme events
  - Low probability and High consequence events
  - Event Trees used to develop probability functions
- Decision maker desires:
  - Expected % water-flow reduction in best 1-in-10 outcomes (f_2)
  - Expected % water-flow reduction in worst 1-in-100 outcomes (f_4)
  - Expected value of water-flow reduction (f_5)



Initiating Event | OS P/W Protects | SCADA OS P/W Protects | SCADA Alarms | Analog Fail-Safes | Operator Notified | Probability Path | Consequences: Water-flow Reduction %

Cyber Intrusion

OS P/W Protects: Yes 0.05 → Probability Path 0.05 → None

OS P/W Protects: No 0.95

SCADA OS P/W Protects: Yes 0.05 → 0.0475 → None

SCADA OS P/W Protects: No 0.95

SCADA Alarms: Yes 0.20

Analog Fail-Safes: Yes 0.30 → 0.05415 → Small U~(0-5 %)

Analog Fail-Safes: No 0.70

Operator Notified: Yes 0.20 → 0.02527 → Medium U~(5-25%)

Operator Notified: No 0.80 → 0.10108 → Large U~(25-50%)

SCADA Alarms: No 0.80

Analog Fail-Safes: Yes 0.30 → 0.2166 → Small U~(0-5 %)

Analog Fail-Safes: No 0.70

Operator Notified: Yes 0.20 → 0.10108 → Medium U~(5-25%)

Operator Notified: No 0.80 → 0.40432 → Very Large U~(50-100%)

Water Reduction

f_2 = 0.60% (best case 1-in-10)

f_4 = 99.5% (worst case 1-in-100)

f_5 = 36.9% (expected value)

Alternative Generation

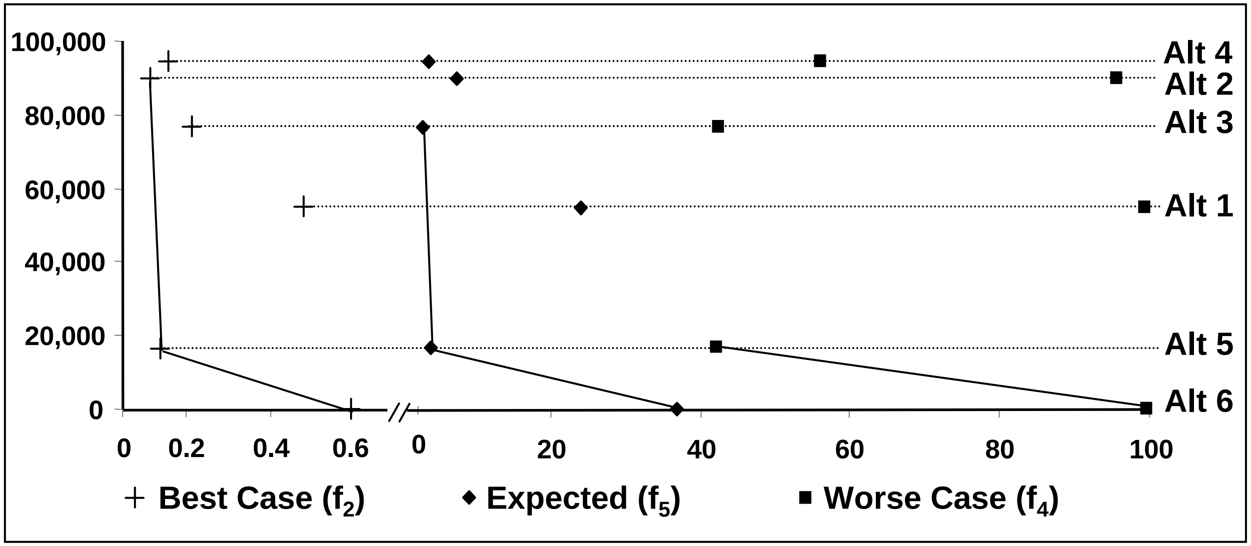
- Outsource web hosting
- Password sharing policy
- Filter firewall to isolate internal SCADA system from web server
- Configure call-back/logging features of dial-up modem
- Cancel access upon employee termination
- Token-based authentication
- Alarm suppression detection
- Alarms for unusual pump/tank usage
- Separate admin and operations servers

Multi-objective Trade-off Analysis

	OS Penetrated	SCADA Accessed	Alarms Defeated	Fail-safes (averted)	Operator Notified (paged)	Discount rate of 7% for 10 years ($)
Alt 1	0.70	0.80	0.80	0.70	0.80	51,504
Alt 2	0.30	0.40	0.80	0.70	0.80	84,721
Alt 3	0.01	0.01	0.80	0.70	0.80	72,515
Alt 4	0.50	0.50	0.30	0.10	0.10	88,870
Alt 5	0.75	0.75	0.20	0.10	0.10	15,904
Alt 6	0.95	0.95	0.80	0.70	0.80	0.00

Multi-objective Trade-off Analysis (cont.)

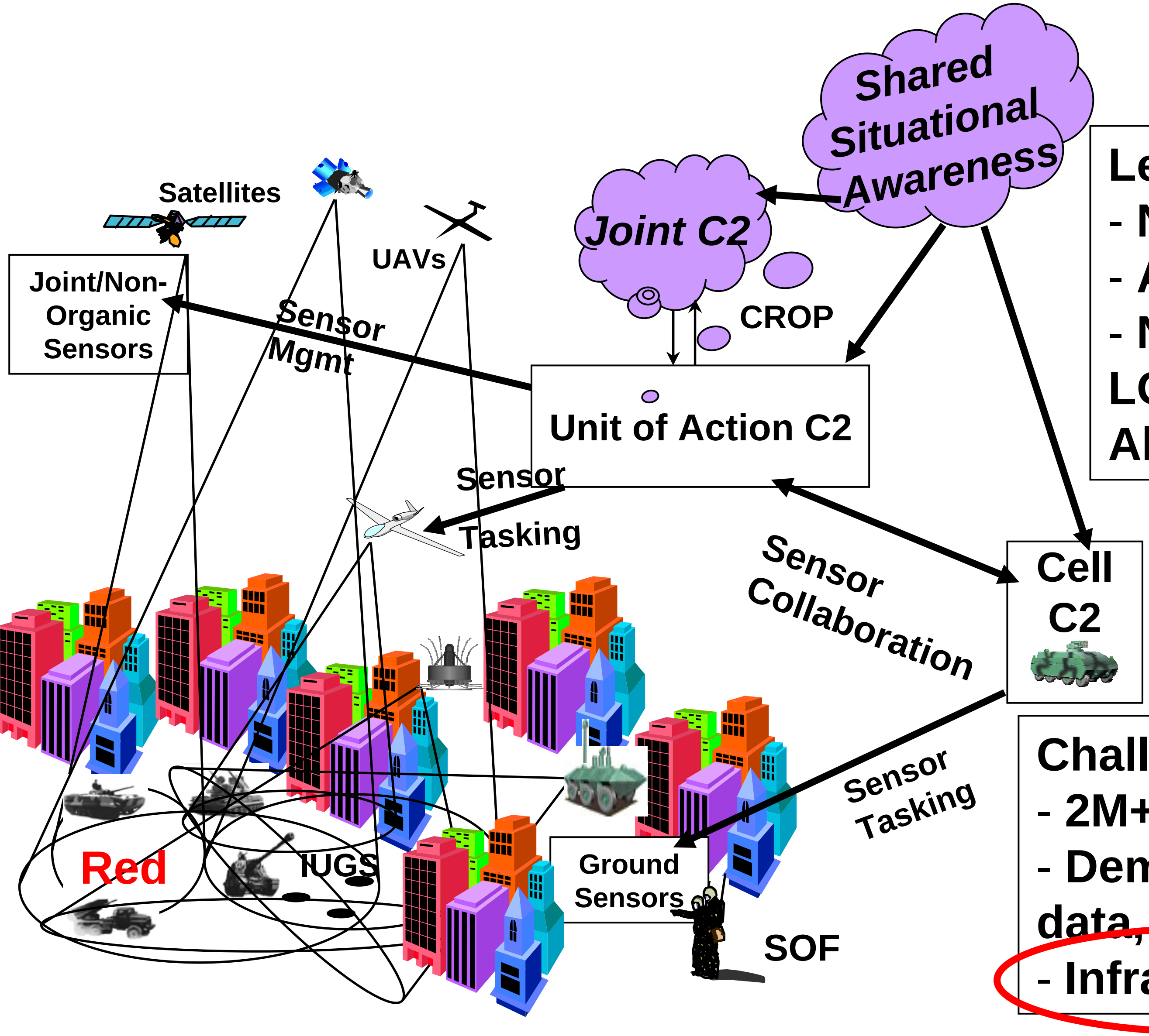
Risk Objective Functions	Alternatives					
	1	2	3	4	5	6
f_1 Cost ($)	51,500	84,700	72,500	88,900	15,900	0.00
f_2 Best Case for 1-in-10 Expected Value of Water-flow Reduction(%)	0.5	0.17	0.20	0.18	0.18	0.60
f_5 Expected Value of Water- flow Reduction (%)	24.1	7.5	3.02	3.73	4.0	36.9
f_4Worst Case for 1-in-100 Expected Value of Water-flow (%)	99.5	95.6	42.5	56.1	42.3	99.5



Applicability to Military Simulation

- Reliability, Maintainability
- Survivability, Vulnerability
  - Human and Machine Failures
- C4ISR/Battle Command System Assurance
- Intelligence Analysis
- Risk Assessment
- Installation Infrastructure (e.g. Fort Future)
- HLS-Sim, AVERT, EPiCs

Legacy Simulation Issues – Multi-Resolution



Legacy Simulations:
- No Civilian Traffic
- Areas are small
- No analytic quality LOS, Collateral Damage Algorithms

Challenges:
- 2M+ entities
- Demographically correct data, traffic, behaviors, etc.
- Infrastructure

Summary

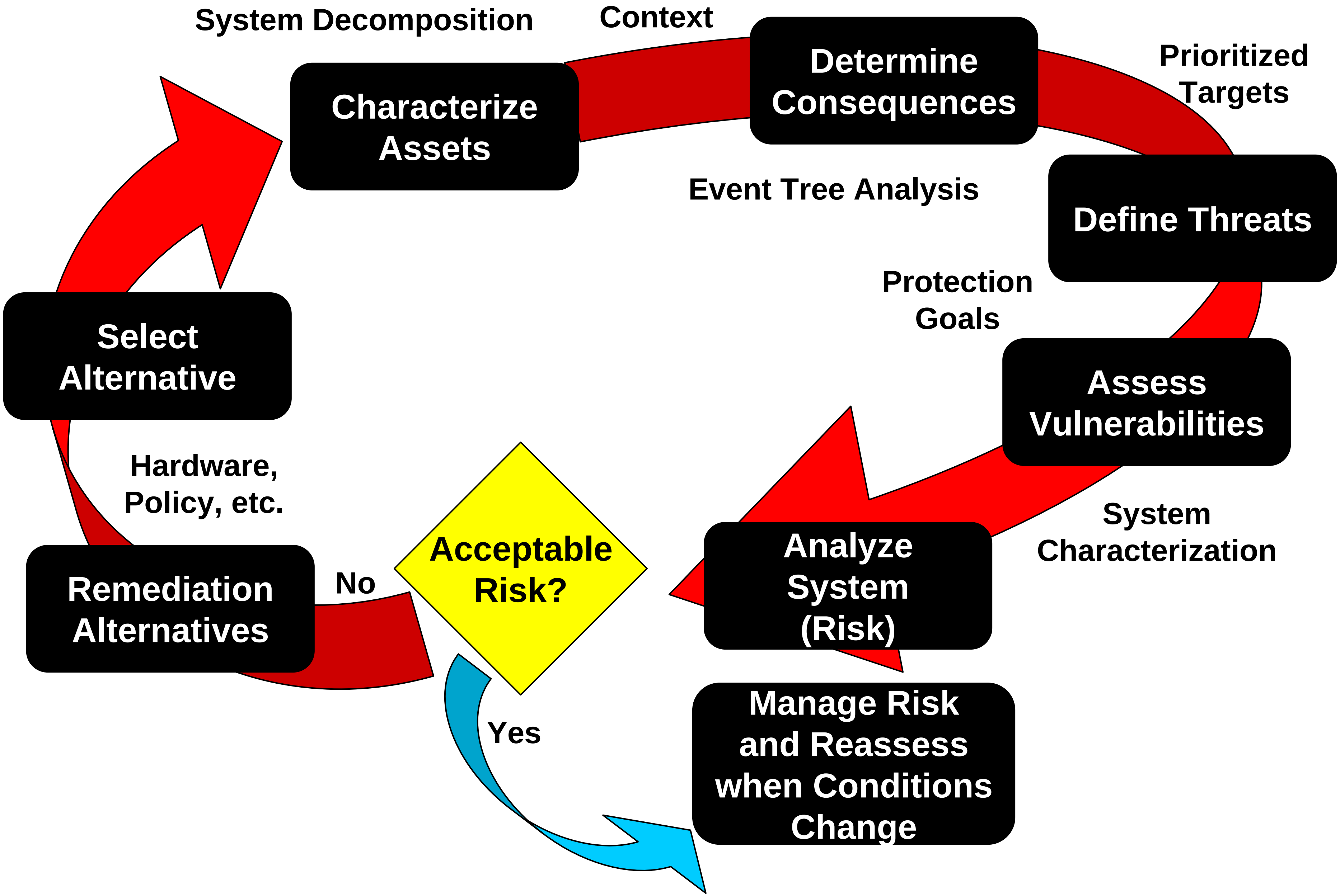
- DoD has a role in critical infrastructure protection
- Public utilities support military force projection
- Cyber terrorism is an existing threat to utility SCADA
- Systems-based risk/vulnerability assessments will mitigate threats
- Military M&S can support and benefit from risk assessment and management methodologies

QUESTIONS?

MAJ John B. Willis
TRADOC Analysis Center (TRAC)
Monterey, CA
john.willis@trac.nps.navy.mil

(831) 656-7580 DSN 756

Back-Up Slides



System Decomposition

Characterize Assets

Context

Determine Consequences

Event Tree Analysis

Prioritized Targets

Define Threats

Protection Goals

Assess Vulnerabilities

System Characterization

Analyze System (Risk)

Acceptable Risk?

Yes

Manage Risk and Reassess when Conditions Change

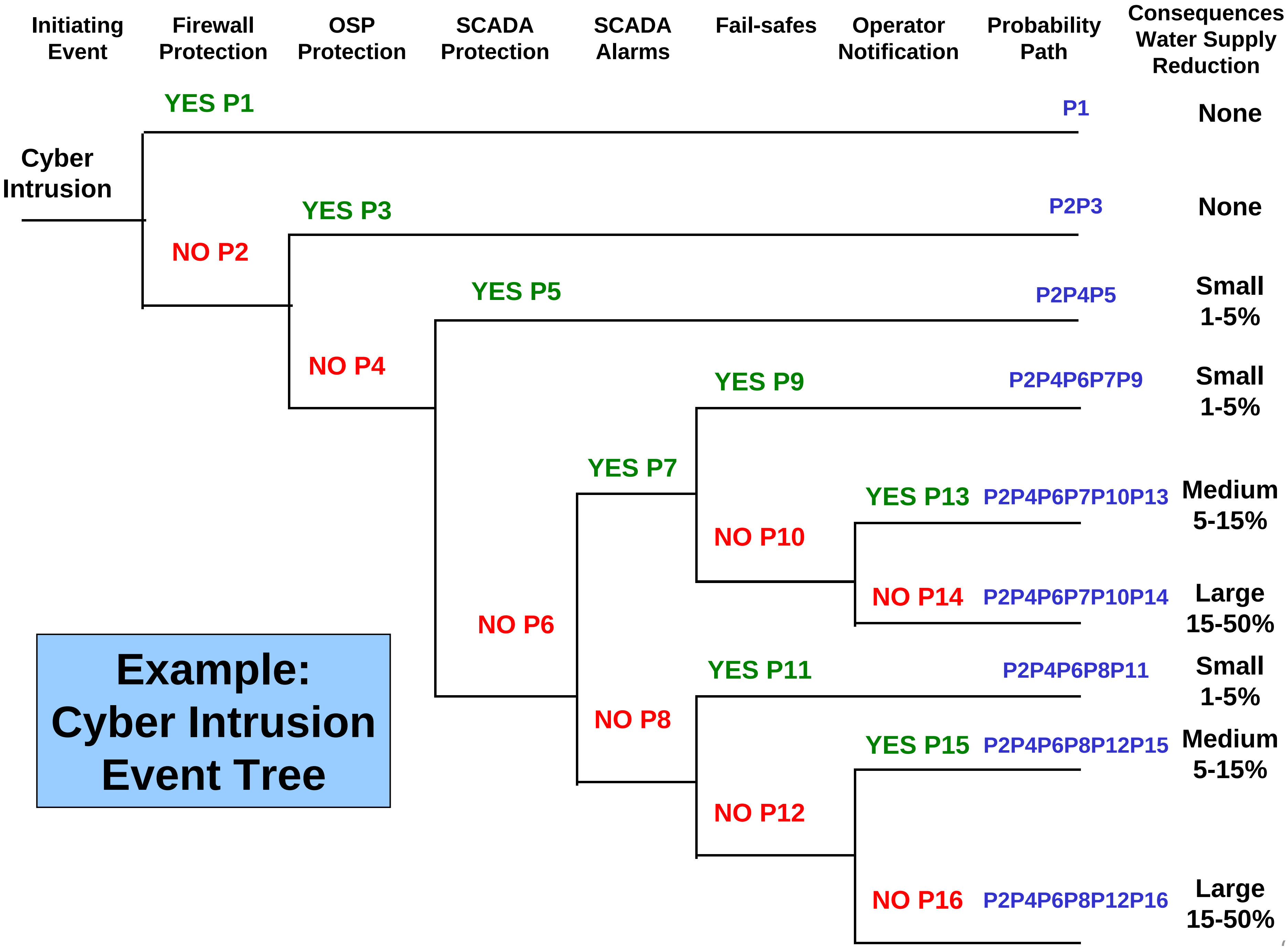
No

Remediation Alternatives

Hardware, Policy, etc.

Select Alternative

Example: Cyber Intrusion Event Tree



Initiating Event

Firewall Protection

OSP Protection

SCADA Protection

SCADA Alarms

Fail-safes

Operator Notification

Probability Path

Consequences Water Supply Reduction

Cyber Intrusion

YES P1 — P1 — None

NO P2

YES P3 — P2P3 — None

NO P4

YES P5 — P2P4P5 — Small 1-5%

NO P6

YES P7

YES P9 — P2P4P6P7P9 — Small 1-5%

NO P10

YES P13 — P2P4P6P7P10P13 — Medium 5-15%

NO P14 — P2P4P6P7P10P14 — Large 15-50%

NO P8

YES P11 — P2P4P6P8P11 — Small 1-5%

NO P12

YES P15 — P2P4P6P8P12P15 — Medium 5-15%

NO P16 — P2P4P6P8P12P16 — Large 15-50%

- **Can’t tell if the enemy has good weapons until he uses them (unlike counting bombers/tanks)**
- **“Swarming Attack” Scenario: Terrorist organization uses physical/cyber attacks on U.S. infrastructure combined with cyber attacks which disrupt the abilities of first responders (e.g. 911 system)**
- **Feb 02 Letter to Pres. Bush:**
  - ***“The critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense and the Internet, is highly vulnerable to cyber attack. Fast and resolute mitigating action is needed to avoid national disaster.”***
  - ***Signed by 54 scientists, former national leaders, intelligence community recommending a Cyber Warfare Defense Project modeled on the Manhattan Project***

- Recent cyber attacks
  - Legion of Doom – 89 – seized control of much of Southwestern Bell’s telephone network infrastructure. Could have tapped lines and shut down 911 service
  - Queensland, Australia – Mar 00 – man used the internet, a wireless radio, and stolen control software to release up to 1M liters of sewage into a river and coastal waters
  - Slammer – Jan 02 – worm that took down internet in South Korea and affected 911, airline, and banking systems in U.S. Exploited vulnerability in MS SQL Server 2000. 90% of damage in first 10 minutes
  - Nimda – 18 Sep 01 – worm attacked Wall Street and millions of computers by infecting email programs and slowing internet access
  - Moonlight Maze – Mar 98 – 2-year probing of DoD, DoE, NASA, universities, research labs traced to mainframe computer in Russia
  - Code Red – Jul 01 – worm that affected 300k U.S. computers and targeted the White House web site with denial of service attacks
  - Mountain View, CA – Aug 01 – “multiple casings of sites” emanating from the Middle East and South Asia looking for information on utilities, government offices and emergency systems

- **Captured Al Qaeda computers/documents reveal:**
  - **Reconnaissance plans of U.S. critical infrastructure**
  - **Models of catastrophic dam failure**
  - **Information about digital switches used by power and water company system infrastructures**
  - **Ties to Inter Services Intelligence (Pakistani) which has contacts in various hacker groups**
  - **Use of sophisticated cryptography equipment**
  - **Use of one-time use email addresses**
  - **“Franchise-model” of independent partners**
- **Electrical control system engineer: “Worst case could be loss of power for 6 months or more.”**

- **Cyber Security History**
  - **Pres. Reagan first addressed the problem (Computer Security Act of 1987)**
  - **Pres. Clinton established PCCIP**
  - **Pres. G.W. Bush established PCIAB**
  - **Feb 03, Pres. Bush released *National Strategy to Secure Cyberspace***
    - **Implement public-private partnerships**
    - **85-95% of cyberspace owned/managed by private sector**

- Awareness of infrastructure vulnerabilities
  - Precipitating event: Oklahoma City bombing
- DoD “Eligible Receiver” exercise
  - NSA Red Team (hackers) used to attack Pentagon systems
  - Could only use publicly available computer equipment/software
  - Results – Infiltration and control of:
    - PACOM computer network
    - Power grids and 911 systems in 9 major U.S. cities

- Amit Yoran
  - Years from now, cyber attack will be a primary method of war; cyberspace a primary theater of operations
- Richard Clarke
  - “Red Teams” (government employed hackers) have succeeded every time in hacking into sensitive government computers, and gained total control of the networks involved, without the owner/operators even knowing it happened.
  - Focus needs to be on the fact that attacks are possible and not on who is doing it.
  - Osama bin Laden is not going to come for you on the Internet.
  - Cyber disruptions could be similar to anthrax attacks or DC area sniper.

- **O. Sami Saydjari**
  - **Some systems use “honeypots” which are fake systems that don’t have any critical content but have interesting keywords/content that might attract cyber intrusion.**
- **James Lewis**
  - **The people thinking about the seriousness of cyber warfare tend to be computer people. We need to broaden the debate and get the involvement of more national security people, military people, etc.**
  - **You’d be shocked to discover how infrequently we have assessed nuts and bolts vulnerabilities, for instance the links from a guy sitting in front of his keyboard all the way to the floodgate on the dam.**

- **John Arquilla**
  - **We have to worry about the possibility of a campaign approach being taken by the cyber attackers in which they mount several attacks over a period of hours or days. Think about the economic impact of deploying a Nimda virus once a week for three months.**
  - **Cyber attacks will transform 21st century warfare, as militaries which are highly dependent on secure information systems will be absolutely crippled.**

- **Michael Skroch**
  - **To secure SCADA systems, we need end-to-end authentication and encryption to help prevent attacks.**
  - **SCADA systems currently don’t have the firewalls, routers, anti-viral software, etc. that are needed to secure them from attack.**
  - **Industry has not developed a business case for cyber security. It may take a cyber Pearl Harbor before we implement the security that is required.**
  - **We understand physical security and know how to achieve it. SCADA systems are a component of U.S. critical infrastructure that we don’t understand well today.**
  - **Most of the U.S. infrastructures that use SCADA systems underestimate the vulnerabilities associated with those systems, particularly because they’re not interested in security, they’re interested in delivering a product, and security is not viewed as a part of that process.**
  - **Industry is using common internet technologies, IP-based communications and operating systems that are popular and prevalent in our economy. In so doing, they are adopting the broad base of vulnerabilities and adversaries that are able to take advantage of those vulnerabilities.**
  - **SCADA is not protected to the same degree as IT infrastructure.**

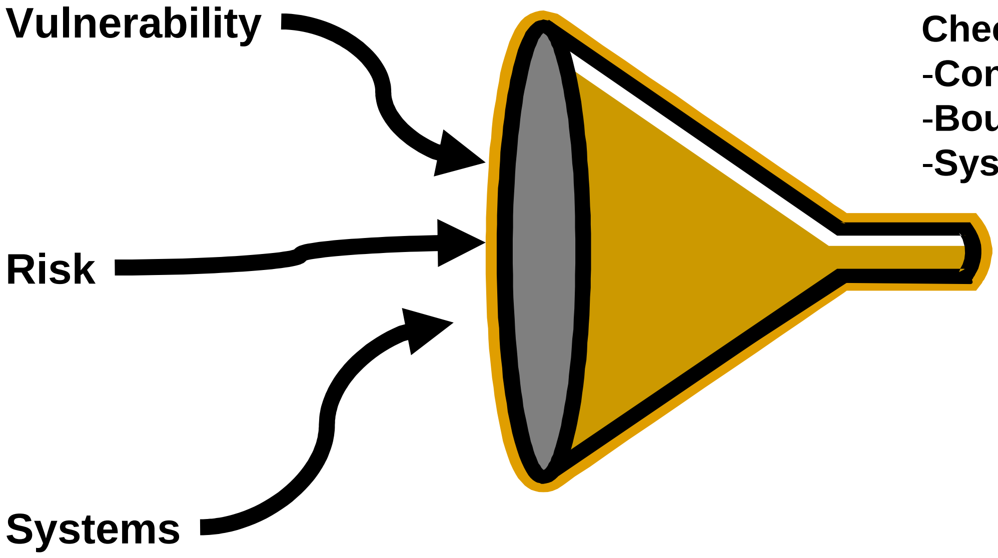
- **Hacker:**
  - **Penetrating a water or electrical SCADA system running a Microsoft operating system takes less than 2 minutes.**
  - **Typical hacker is 12-16 year-old**
  - **“Exploits” (published sample bit of code or program that demonstrates a flaw in software or hardware) are shared among hacker community. Digital Millennium Copyright Act seeks to prevent the sharing of such things.**
  - **Can use “zombies” to make the attack appear like it’s coming from a computer in another country.**
  - **U.S. is the most vulnerable nation-state because IT is so essential. This makes vital infrastructures highly vulnerable.**
  - **Scenarios:**
    - **“Pearl Harbor” – multiple cyber attacks by terrorist/rogue groups against water, power, etc.**
    - **Insider – e.g. altering calibration of precision parts production of military equipment.**
  - **Information acquisition costs – the knowledge necessary to launch a sophisticated attack is provided by our own side for free. Groups like Al Qaeda are willing to spend the time, energy and money to learn what they need to know to carry out effective attacks.**
  - **In 90 days, a team of 6 to 10 people could acquire very cheaply the equipment and knowledge needed to take out huge sections of U.S. infrastructure.**
  - **If you bring in the FBI to lecture you on computer security and to tell you what you need to worry about, SCADA is at the very top of the list.**
  - **If somebody was surveying our infrastructures for a potential missile attack, we would be very excited about it. The fact that water and electrical supply SCADA systems are being probed and mapped for holes and choke points doesn’t get attention because there’s no flash, bang or blood.**
  - **In my world, firewalls are referred to as “speed bumps”.**
  - **Hackers have broken into SCADA systems of critical infrastructure but had no idea what they were looking at. To them, it was just another insecure Windows box.**
  - **Government regulation won’t solve the problem. What’s needed is to stop providing protection to the Microsofts and the business models of security providers.**
  - **DoD networks, including SIPRNET, have numerous poorly secured nodes.**
  - **FBI and CIA are fully competent and are working diligently to secure their systems. NSA and DoD are not.**
  - **Neither the government nor the private sector firmly grasp the dangers. Vulnerabilities will stay in place until there are bodies in the streets.**

- Diane VanDe Hei
  - Most of water system security funds go to physical protections, not cyber
- Rep. Lamar Smith (R-TX)
  - A mouse can be as dangerous as a bullet or a bomb

Vulnerability, Risk, and Systems Theory are emerging as three fundamental literature streams

What is vulnerability as it applies to critical infrastructure systems?
How does risk and systems theory apply to vulnerability assessment of critical infrastructure?
How can system vulnerability be quantified?
What results from deployment of the system vulnerability methodology?

Research Disciplines



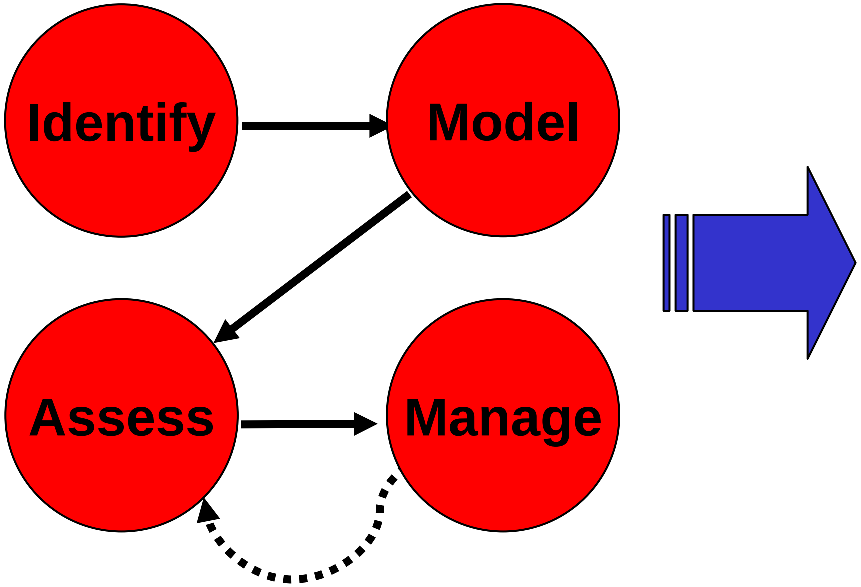
Gaps/Implications

Divergent views regarding vulnerability
Confusion on definitions of risk and vulnerability
Checklists without:
-Context
-Boundary
-System view:
- -Emergence
- -Equifinality
- -Holography
- -Variety
- -Complexity
- -Interdependencies
- -Interactions
- -Open, Natural, Rational, Cybernetic
- -Social-technical
- -Negative Entropy

Relationship between risk and vulnerability is under study

- Risk: a measure of the probability and severity of adverse effects
- Vulnerability: suggests *susceptibility* to risk
- Risk = $\{S_a, L_a, X_a\}_A$
  - The issue with extreme event probability L_a, is that it may cause a misleading rank ordering of threat scenarios
  - Perhaps threat scenarios and risk mitigation strategies should focus on system points of vulnerabilities rather than the expected value of damage

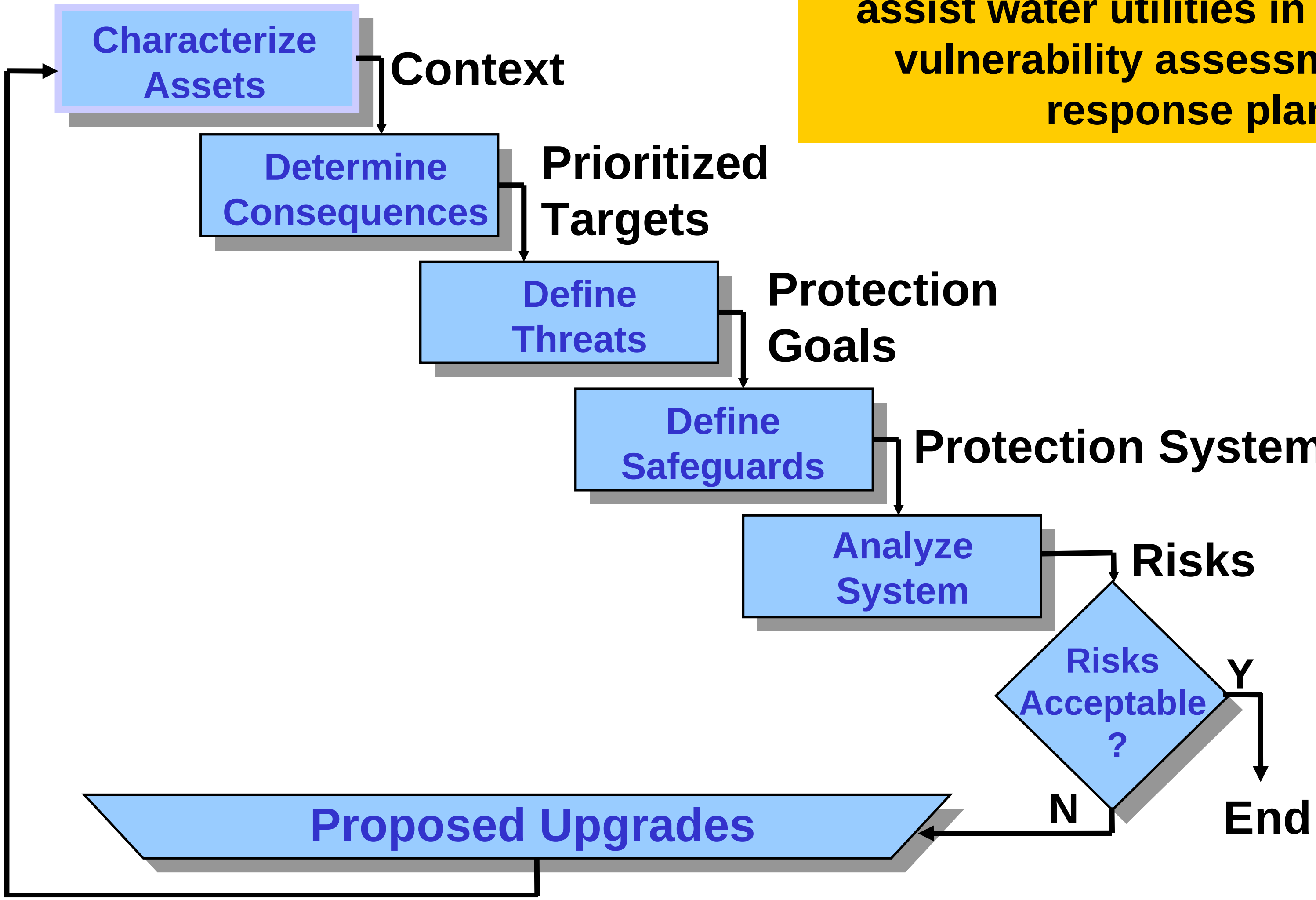
Improving IRAM would include systems perspective as a preceding step, making an systems description an explicit step in the assessment.



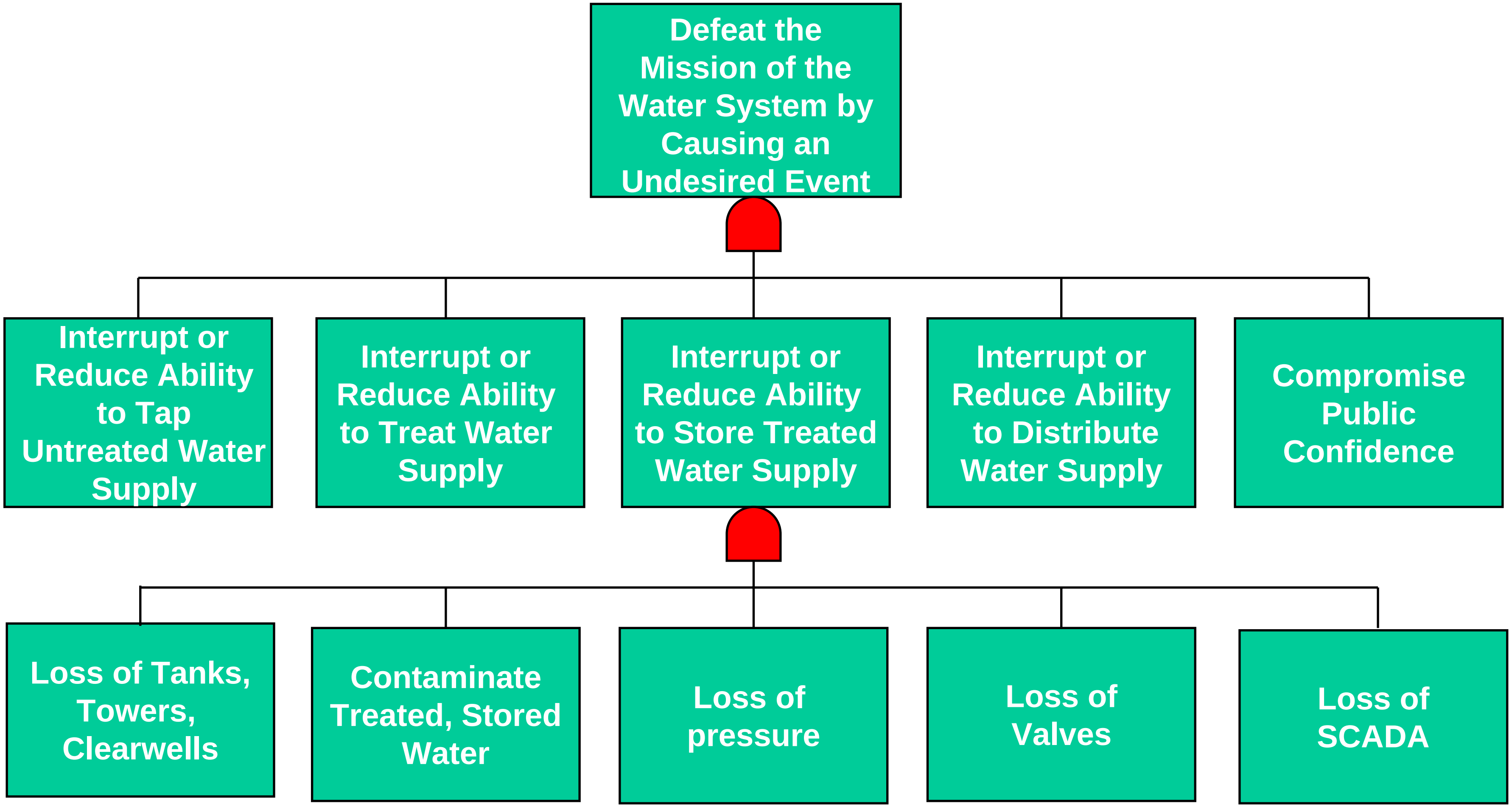
- Identify system and boundaries
- Decompose
  - Function
  - Component
  - State
- Ideate threat scenarios
- Assess mitigating aspects of the systems
- Assess Consequences
- Identify vulnerable points in the system
- Ideate risk mitigation strategies
- Model risk mitigation strategies
- Assess strategy performance
- Decide
- Implement

Risk Assessment Process

EPA has provided $51M in grants to assist water utilities in conducting vulnerability assessments and response plans



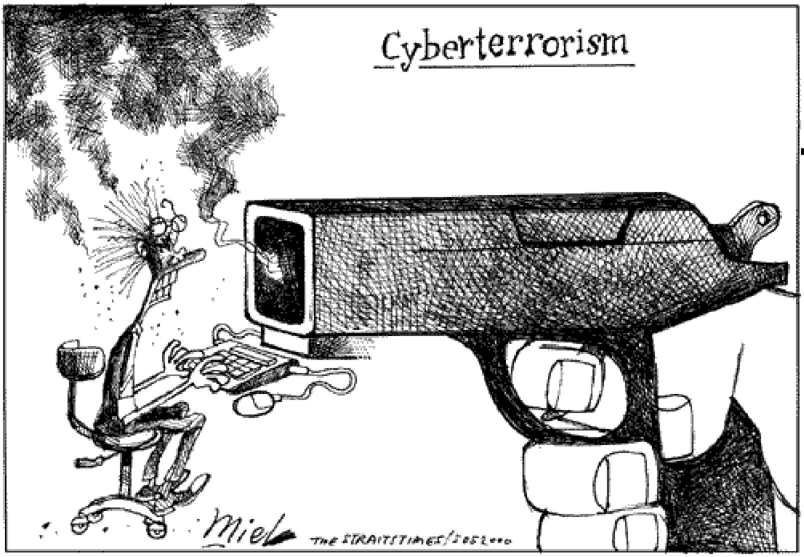
Generic Modular Fault Tree


Defeat the Mission of the Water System by Causing an Undesired Event
Interrupt or Reduce Ability to Tap Untreated Water Supply
Interrupt or Reduce Ability to Treat Water Supply
Interrupt or Reduce Ability to Store Treated Water Supply
Interrupt or Reduce Ability to Distribute Water Supply
Compromise Public Confidence
Loss of Tanks, Towers, Clearwells
Contaminate Treated, Stored Water
Loss of pressure
Loss of Valves
Loss of SCADA

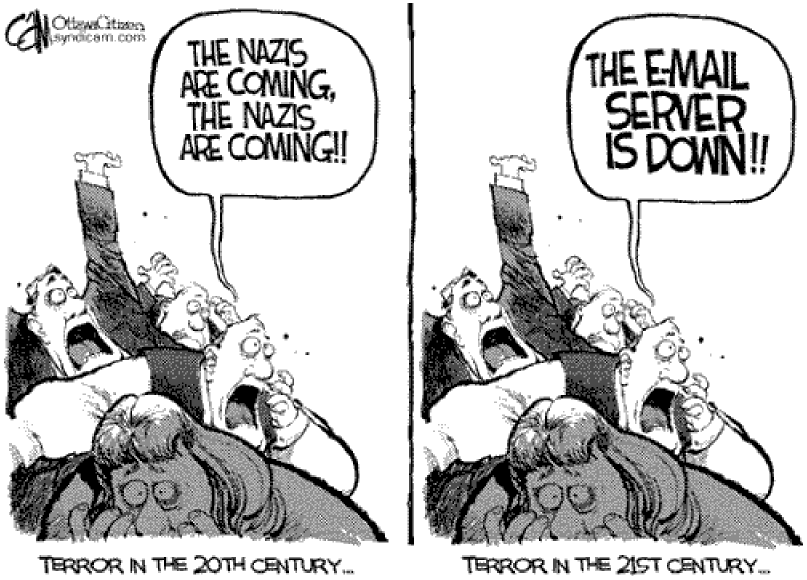
Debunking the Threat to Water Utilities [1] asserts the threat to water utilities is fear mongering.

- Really?
  - "As you've probably heard, there was an interesting case of hacking at Maroochy, on the Queensland coast just north of Brisbane." […] "Over several months Maroochy Water Services experienced intermittent faults with its computerized sewerage SCADA system including numerous pump stations shut downs without any alarms, resulting in the first recorded conviction of a computer hacker causing serious environmental harm."[2]
  - "As many of you know, the SQL Slammer worm struck last weekend (1/25/03) and caused overload conditions in the world wide Telco infrastructure."[3]
- Wishful thinking or simply waiting for a disaster is dangerous and foolhardy.
- We know there are risks but how do we assess and mitigate?

[1] CIO Magazine
[2] http://www.courts.qld.gov.au/qjudgment/ca02_151.htm
[3] SCADA Mail List


Cyberterrorism
Miel
THE STRAITS TIMES/ 5 05 2000

BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KELLOGG


OttawaCitizen
syndicam.com
THE NAZIS ARE COMING, THE NAZIS ARE COMING!!
TERROR IN THE 20TH CENTURY...
THE E-MAIL SERVER IS DOWN!!
TERROR IN THE 21ST CENTURY...

BROOKINS
SO, WHADDA YA WANT TO DO TODAY?... HANG OUT AT THE MALL, GO TO THE MOVIES OR SCREW UP HALF THE WORLD'S COMPUTERS?! ...
PIZZA