

Countering Terrorism to Data Centers Through Surety Methods

Presented at

Critical Facilities Roundtable
Redwood City, CA

Host: Oracle Corporation
March 9, 2007

Presented by

John H. Strothman, President
Strothman Associates, Inc.
Evanston, Illinois
847-491-6700
Jstrothman@comcast.net



Technology Transfer

Alignment



Resource Sharing

Seminars
Licensed Expertise
Consulting
Product Development

Measurable Outcomes



Objectives

Highlight the Value of Surety Methods

- Analytically
- In-Common with Data Center requirements
- As Implemented through a Real World Security Example



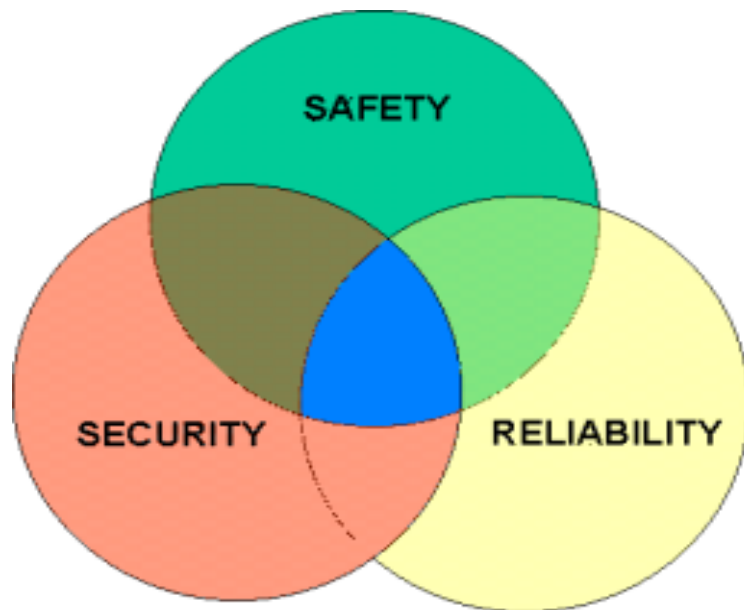
Presentation Outline

- **Surety process, analytically**
- **Surety benefits and commonality to Data Center high-consequence interests**
- **Surety security risk management mechanics**



What Is Surety ?

Surety is Confidence that a system will perform in acceptable ways under normal, abnormal, and malevolent environments.



Surety has dimensions of

Safety

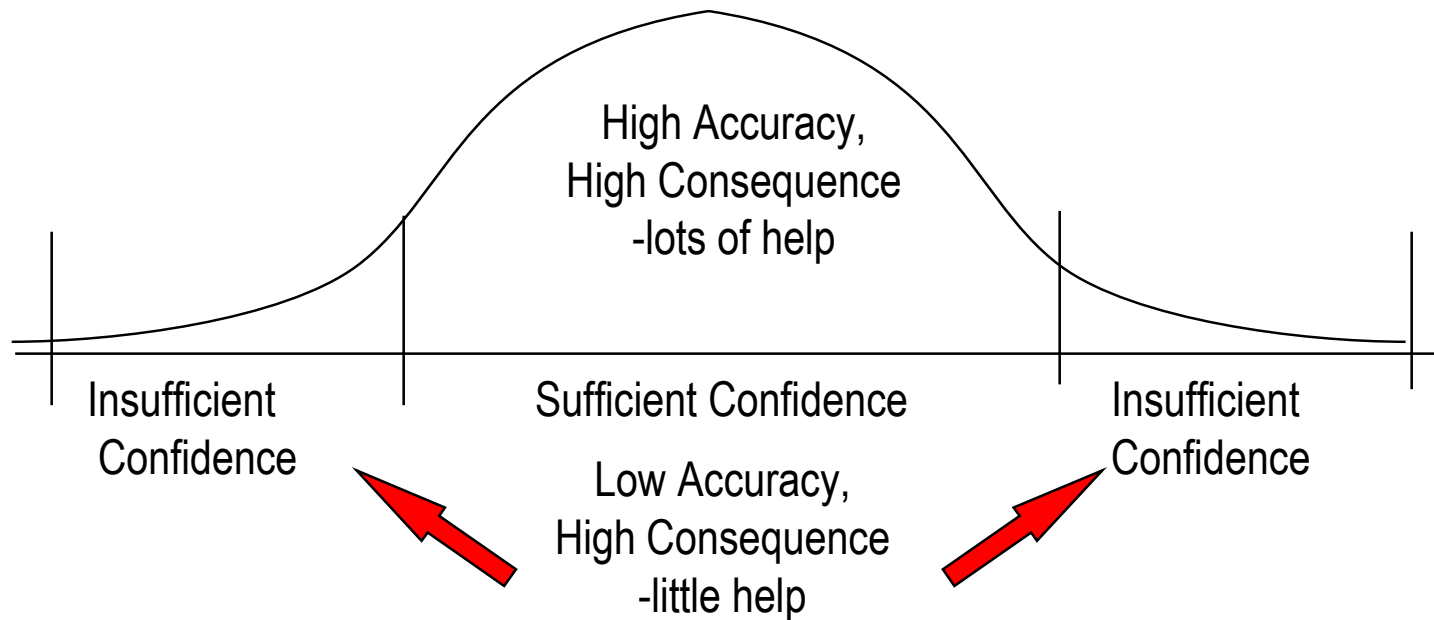
Reliability

Security



Surety Methods Elicit Confidence

Confidence through rigorous risk management methods. Surety methods approach security issues and needs where experience is missing




Managing 'Retained Risk'



Surety Methods

Surety comes in four levels*

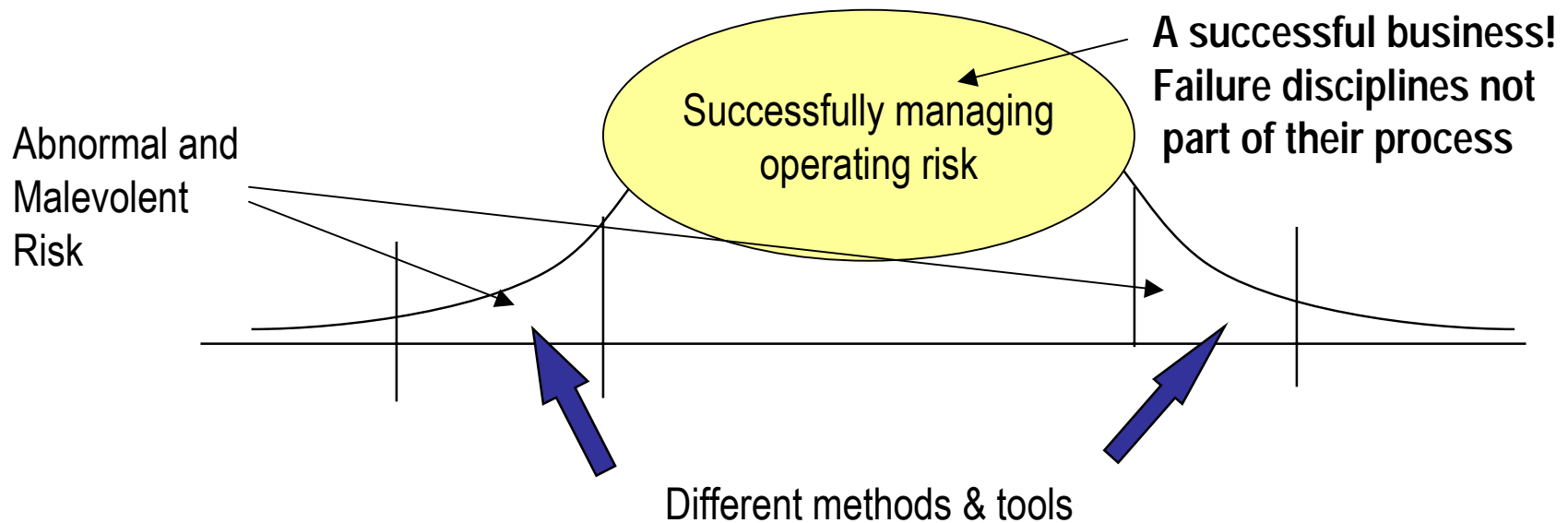
1. Working sufficiently as expected and buying insurance to cover upsets
2. **Surety by Proactive Human Intervention** 
3. Surety by positive Measures from Science and Engineering
4. Surety from Laws of Nature and Mathematics

*Sandia National Laboratories presentation to the National Academy of Sciences, September 1998



A Risk Management Mindset

Levels of Confidence, risk adjusted, through proactive human intervention



Mitigating and Managing Retained Risk

Surety Methods Benefit Complex Systems Management

- A risk-management approach
- Being anticipatory, rather than reactive
- A systems engineering approach
- High-consequence engineering 50 yr. knowledge-base



Mission Critical Facility Systems Have Similar Concerns and Activities

- **Share key Surety risk concerns**
 - Aging systems management is very important
 - Survivability in abnormal environments
 - Resistant to adversary attack
- **Benefit significantly from automation**
- **Benefit significantly from technology**
- **Should be systems engineered**
 - Require a risk management approach
 - Require anticipatory processes, not reactive



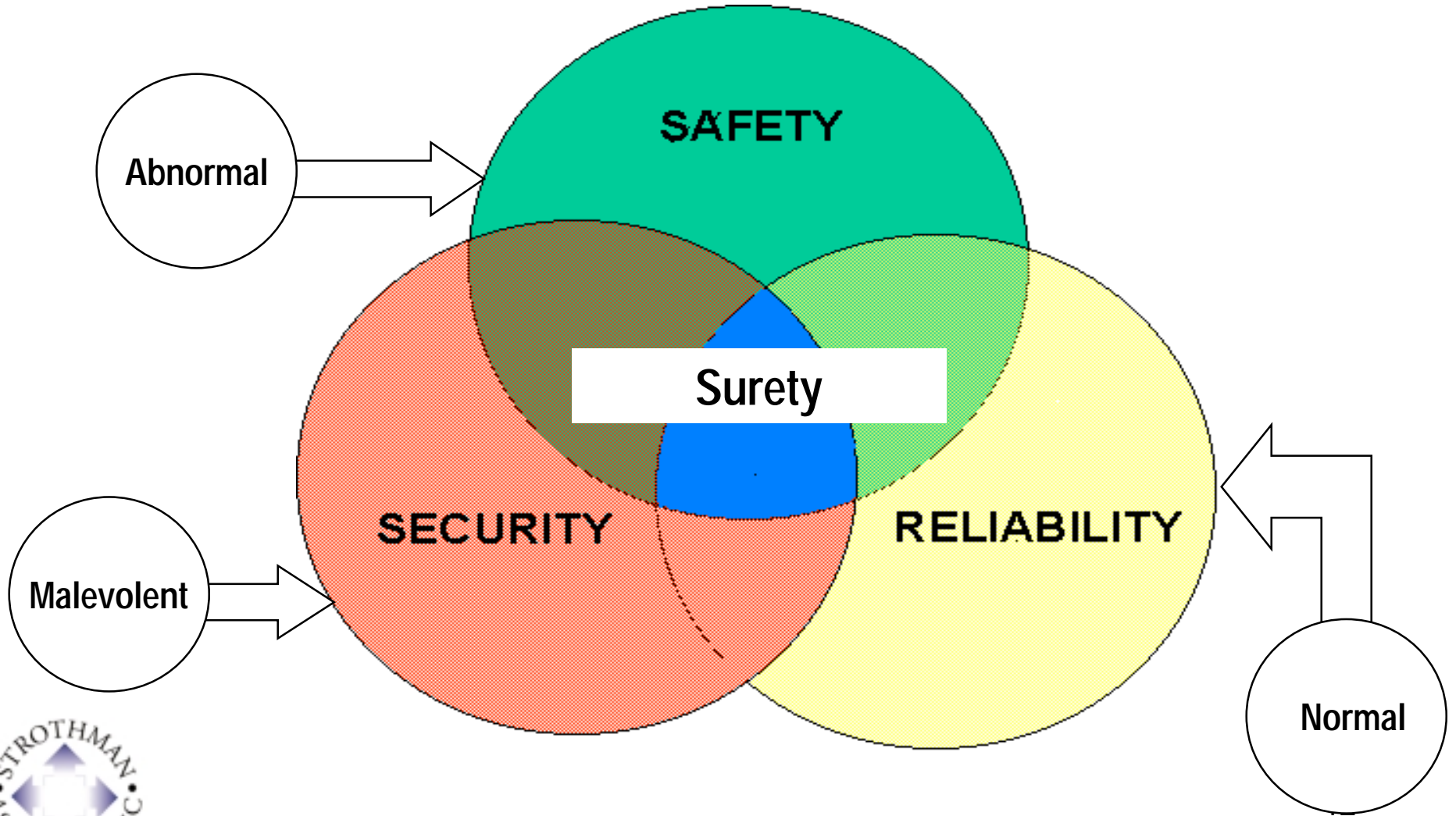
Cross-Culture Commonality and Benefits

Focus on Risk Mechanics

- **Commonality in heritage-type complexity growth**
- **Surety methods leverage 50 year security knowledge base**
- **Risk based assessment approaches mitigate current security threats and vulnerabilities**
- **Risk Analysis Methods as practiced by U.S. Department of Homeland Security**



... Integrating Threat Elements



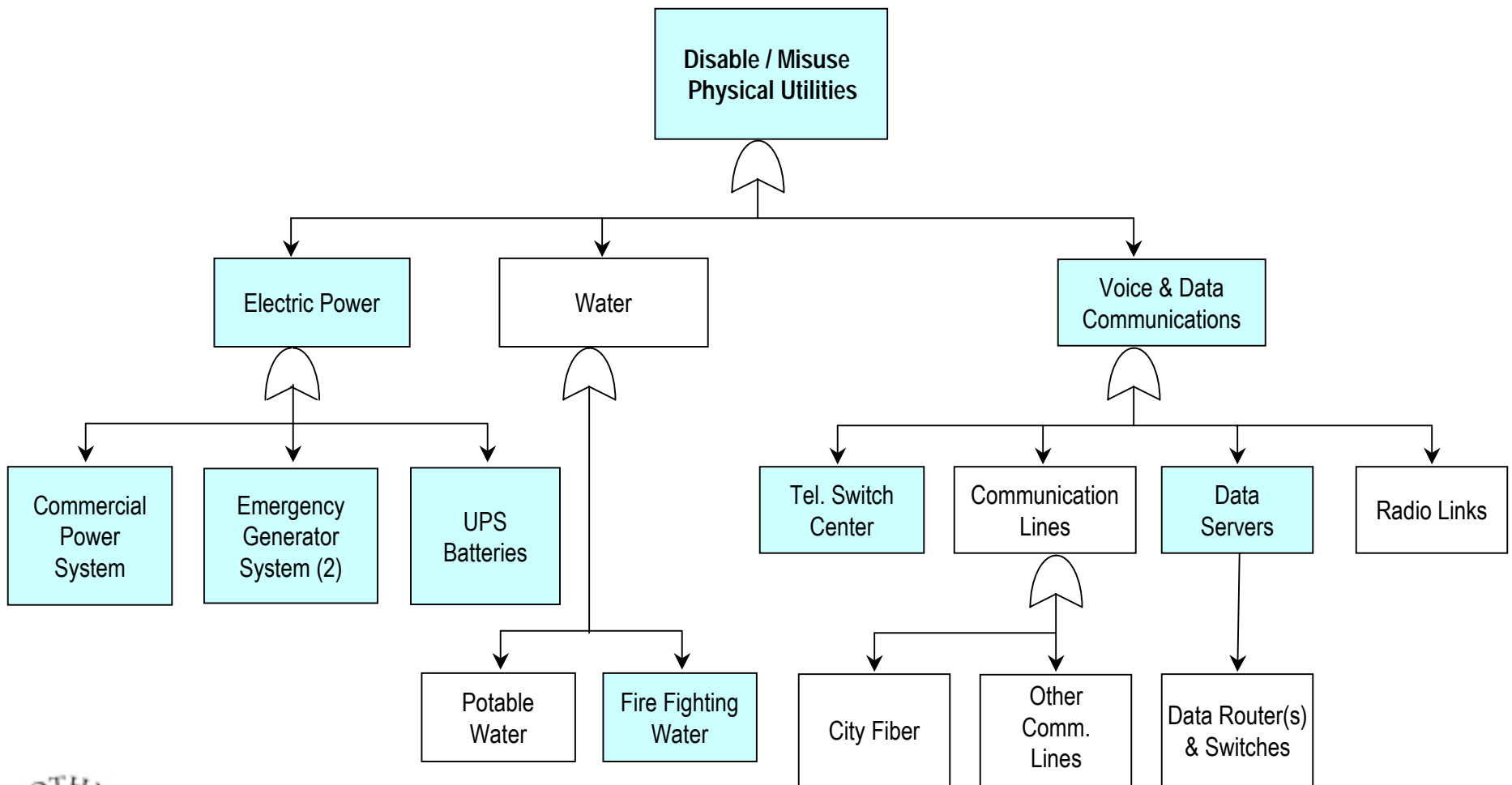
Decision Support Activities

Risk Management Tool Examples

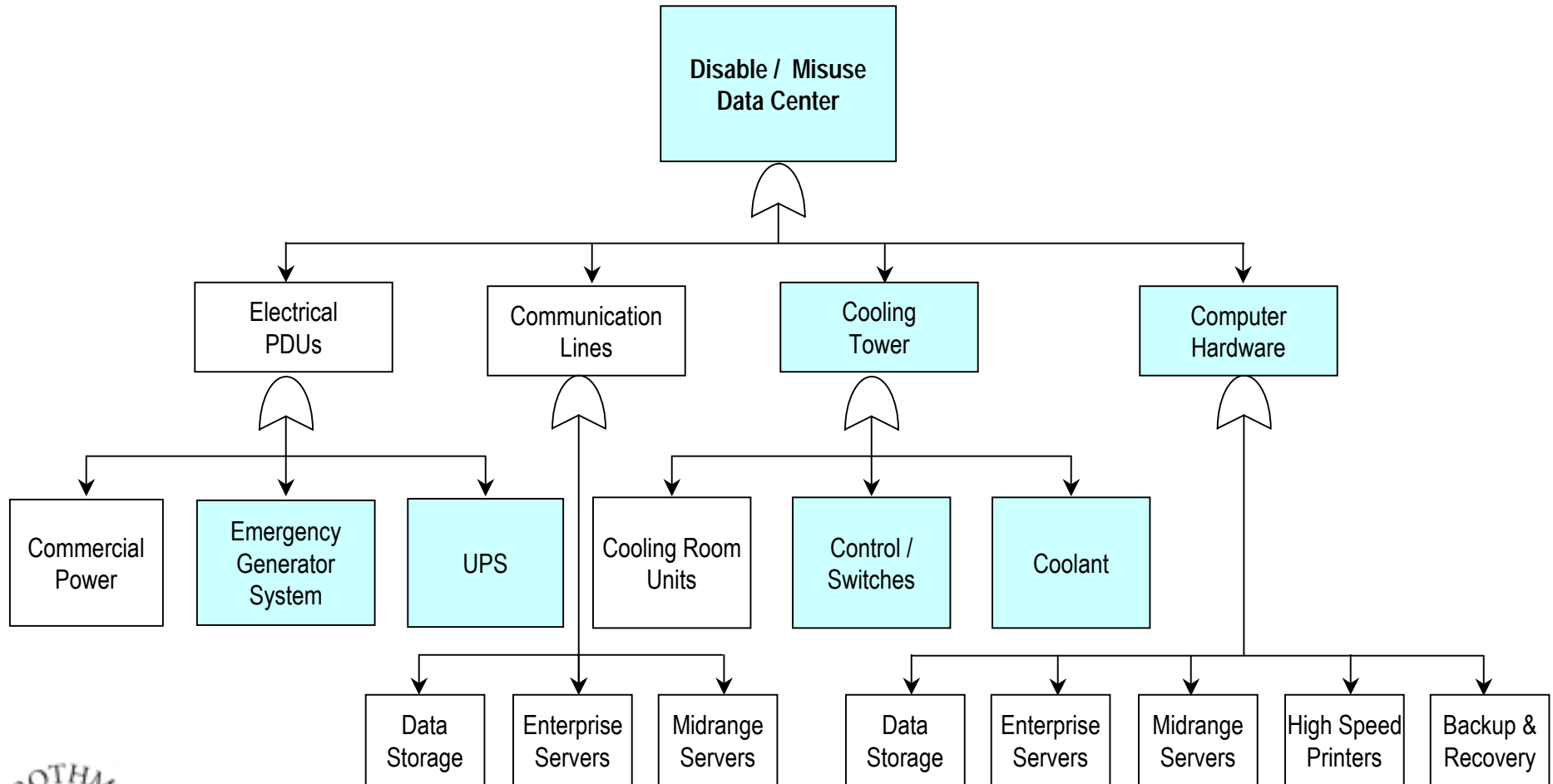
- Fault trees (examples follows)
- Adversary Sequence Diagram (ASDs)
- Screening sequence
- Response capability
- Risk analysis and reduction process



Utility Failures That Impact Building Operations



Failure Of System-Wide IT Function



Risk Elements

- Threats*
- Consequences*
- Vulnerabilities (Security System In-Effectiveness)*



Risk Analysis Methodology

- **Threat assessment**
 - Threat definition
 - Site-specific threat
 - Likelihood of occurrence
- **Consequence assessment**
 - Loss of mission, revenue, property, life
 - Loss of symbolic value
- **Vulnerability assessment**
 - Attack scenarios
 - Site characteristics
 - Critical assets (fault-tree analysis)
 - System in-effectiveness



Risk Analysis Methodology *(Continued)*

- Risk management (business case approach)
 - Strategy for protection
 - Acceptable risk (?)
 - Upgrades and mitigation
 - Define design basis threat (DBT)
 - Cost and operational impacts



Risk Assessment

- Analysis*
- Risk Acceptability And Management*
- Risk Reduction*



Risk Equation

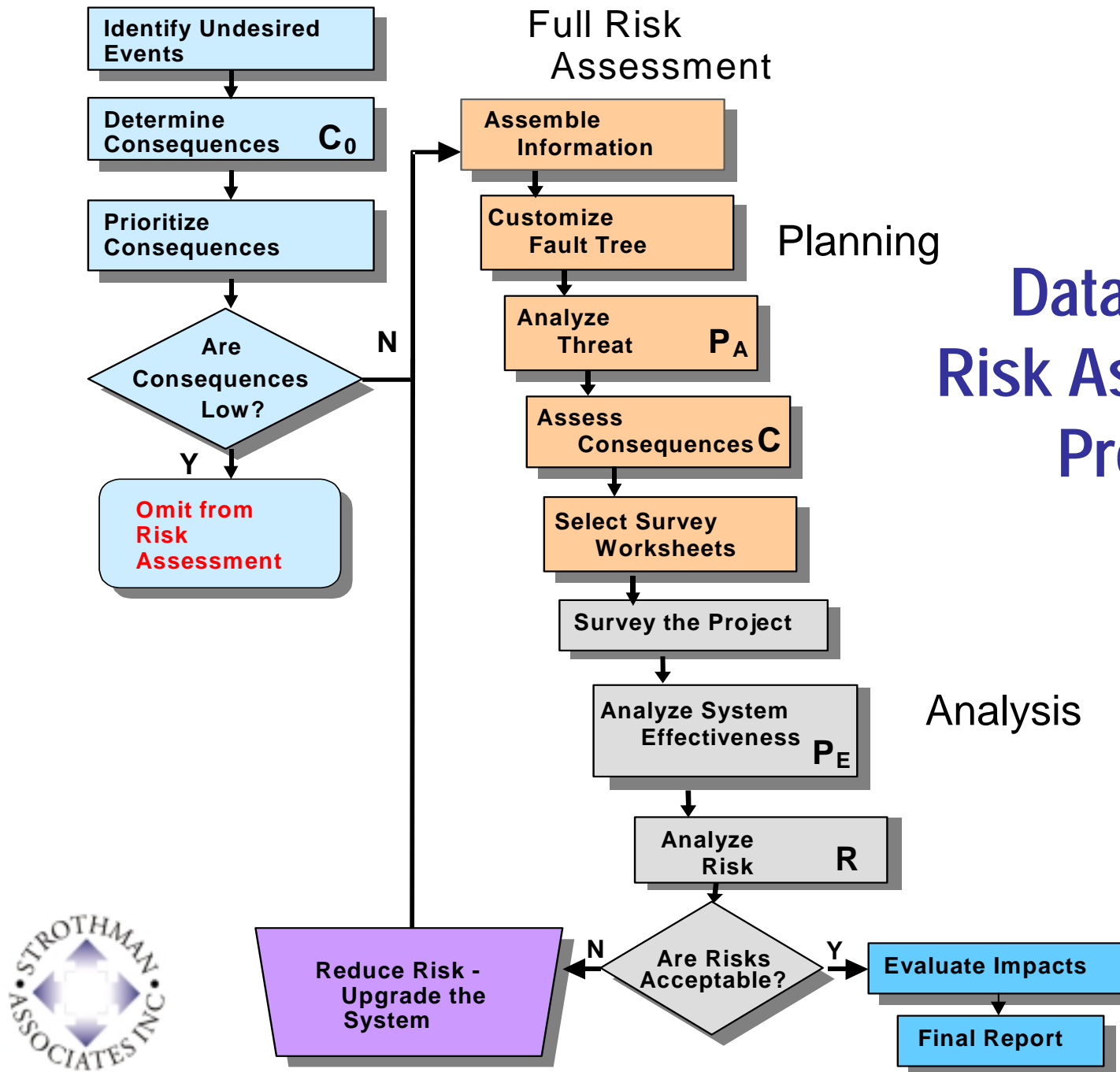
$$P_A \times C \times (1 - P_E) = \text{Risk}$$

P_A - Likelihood of occurrence

C - Consequence

P_E - System effectiveness

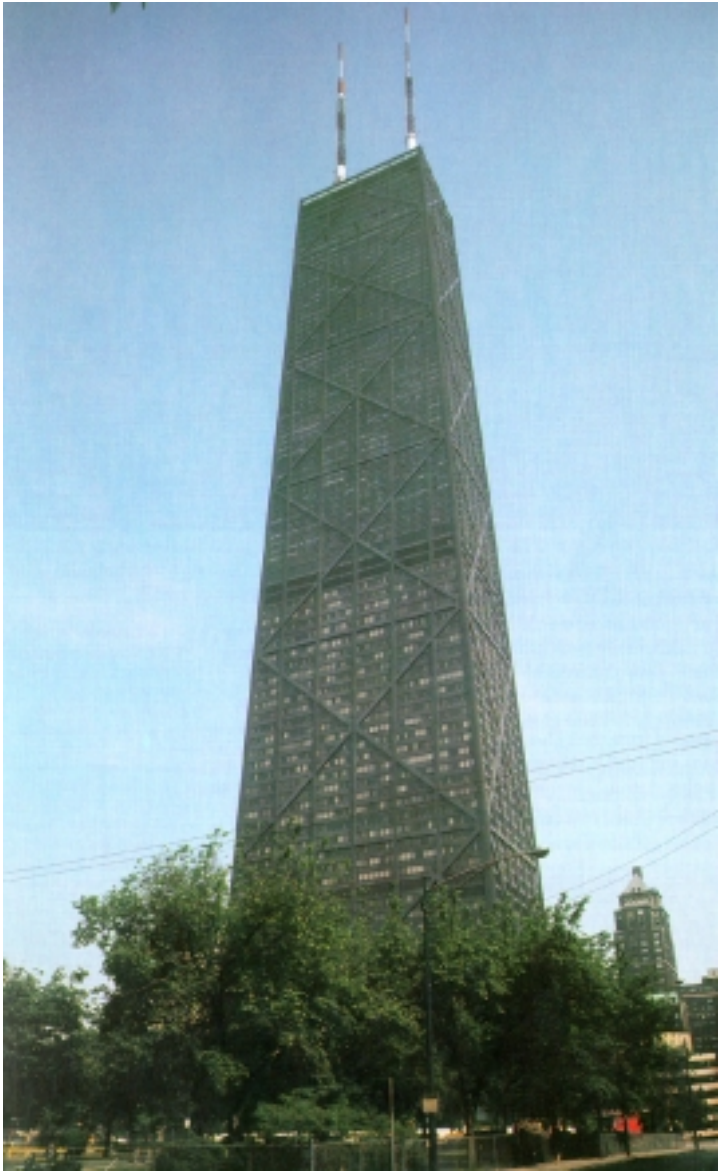




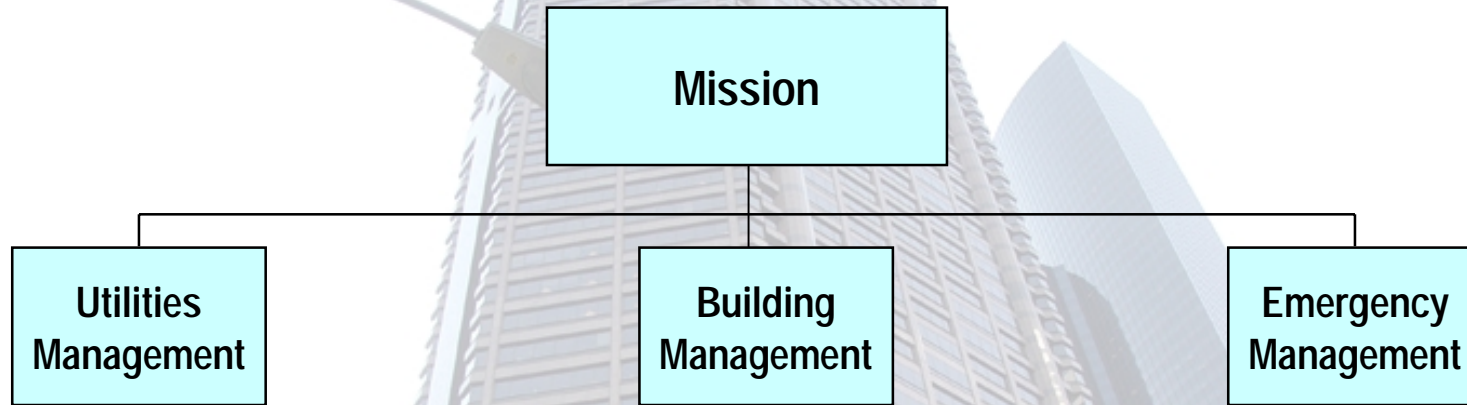
Data Center Risk Assessment Process



Which "High-Rise" Has Surety® ?



Representative City Building



Commercial Water
Commercial Power
Transportation Management and Services
Voice and Data Communications
Computing Operations and Data Center
HVAC
Telecommunications
Others

Engineering
Property
Space
Security and Public Access
Mail
Payment
Shipment - Delivery
Non-Government Functions
Others

Department Emergency Operations
Safety and Security
Law Enforcement Coordination
HAZMAT Materials Management
Contingency Planning
First Responders Coordination
Continuity of Government
Others



City Building Example

(Proprietary-Examples Deleted)

- Development of Credible Threat Scenarios
 - Example
- Likelihood of Threat Occurrence
 - Example
- Consequence Measurements and Judgments
 - Example
- Vulnerability -from Threat Scenarios + Analysis
 - Example
- Risk Analysis Summary
 - Example



Risk Management Benefits

- **Repeatable**
- **Approaching “More Quantified” Values**
- **Standardized Baseline**
- **Accountable**
 - Assumptions
 - Decisions
 - Acceptable Risk Levels
- **Traceable Path**
- **Consistent Terminology**
- **Defendable Record**
- **Ease of Automation**



Surety's Approach and Summary

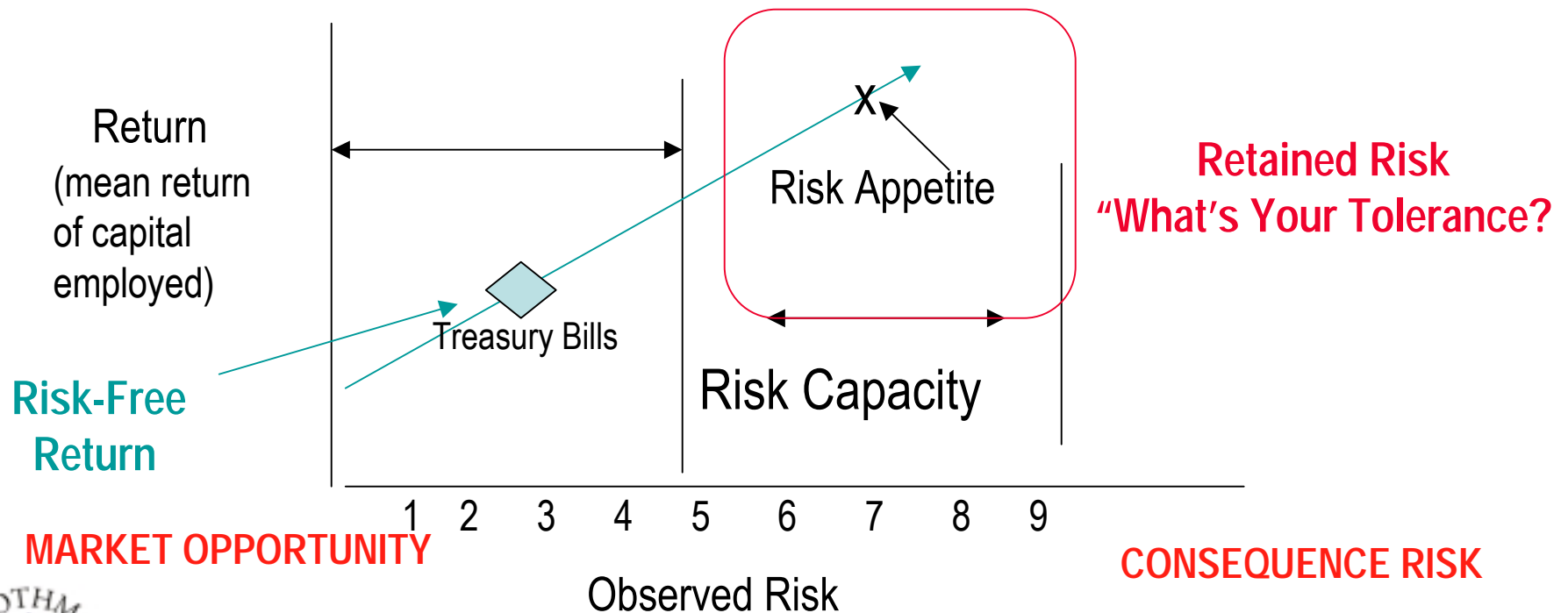
- *Step #1: Complete The Risk Process*
- *Step # 2: Performance-Based Upgrades*
- *Step # 3: Risk Reduction Options*



Managing Business Risk

Conceptual

Quantitatively-- Assessing Mixed Risk
Risk/Return Matrix



(Expressed as % variation of return: SD/Mean)

Strothman Assoc.
847-491-6700

