
Development of an Integrated Methodology and Software Prototype for Aviation Systems Risk and Safety Assessment and Management

Ali Mosleh

Center For Risk and Reliability
University of Maryland

Hossein Eghbali

Hi-Tec Systems

Presented at

Sixth Annual FAA-NASA Workshop on
Risk Analysis and Safety Performance Measurements in Aviation
August 16-19 2004, Arlington VA



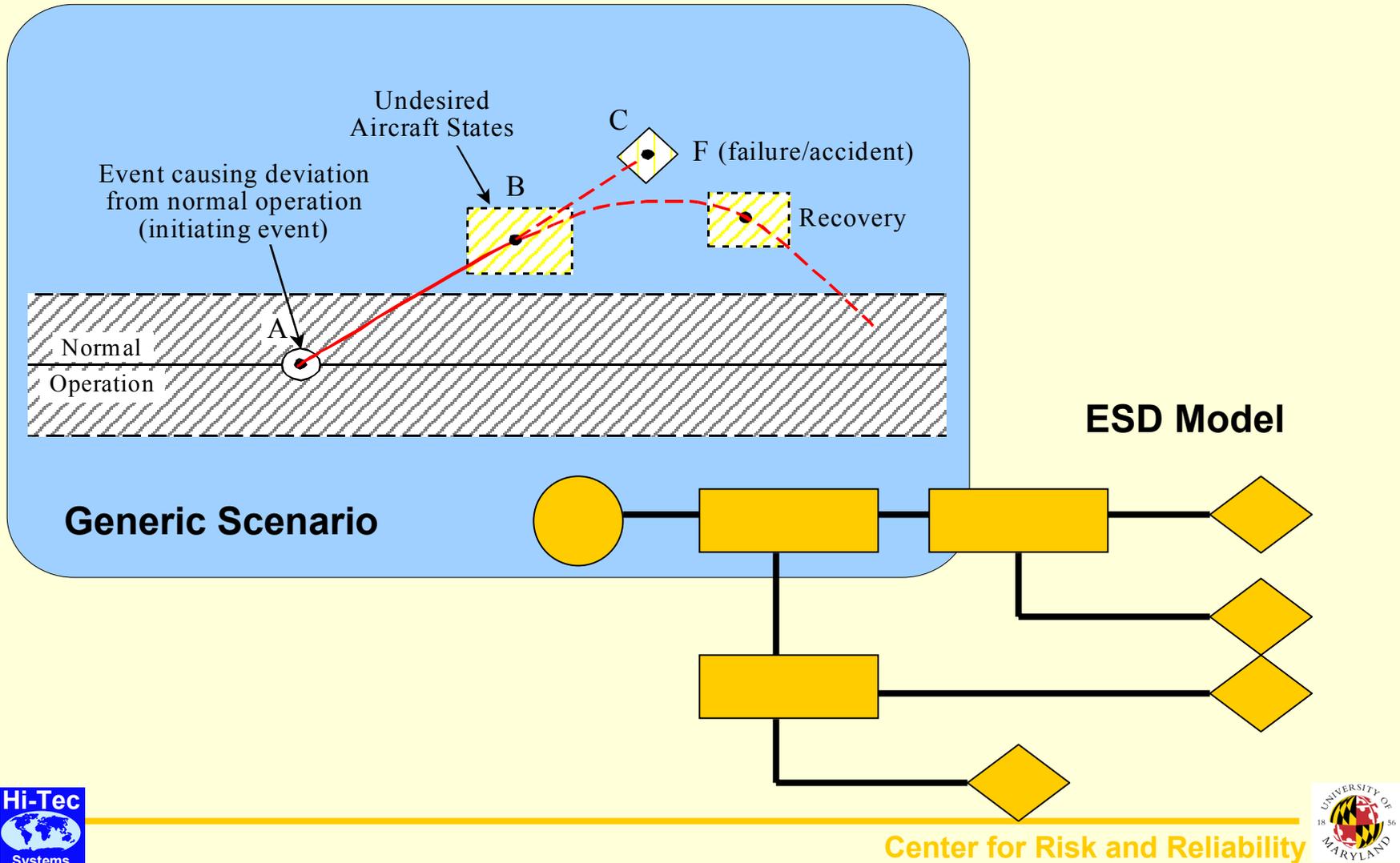
Key Attributes of the Methodology

- Inherently capable of addressing multiple objectives
 - System Safety and Hazard Analysis
 - Risk Analysis
 - Security Assessment
- Provides a vehicle for
 - **identification of causal relations** including those associated with human and organizational influences
 - **Identification and prioritization of hazards**
 - **analysis of events** (mishaps, incidents and accidents)

Key Attributes of the Methodology

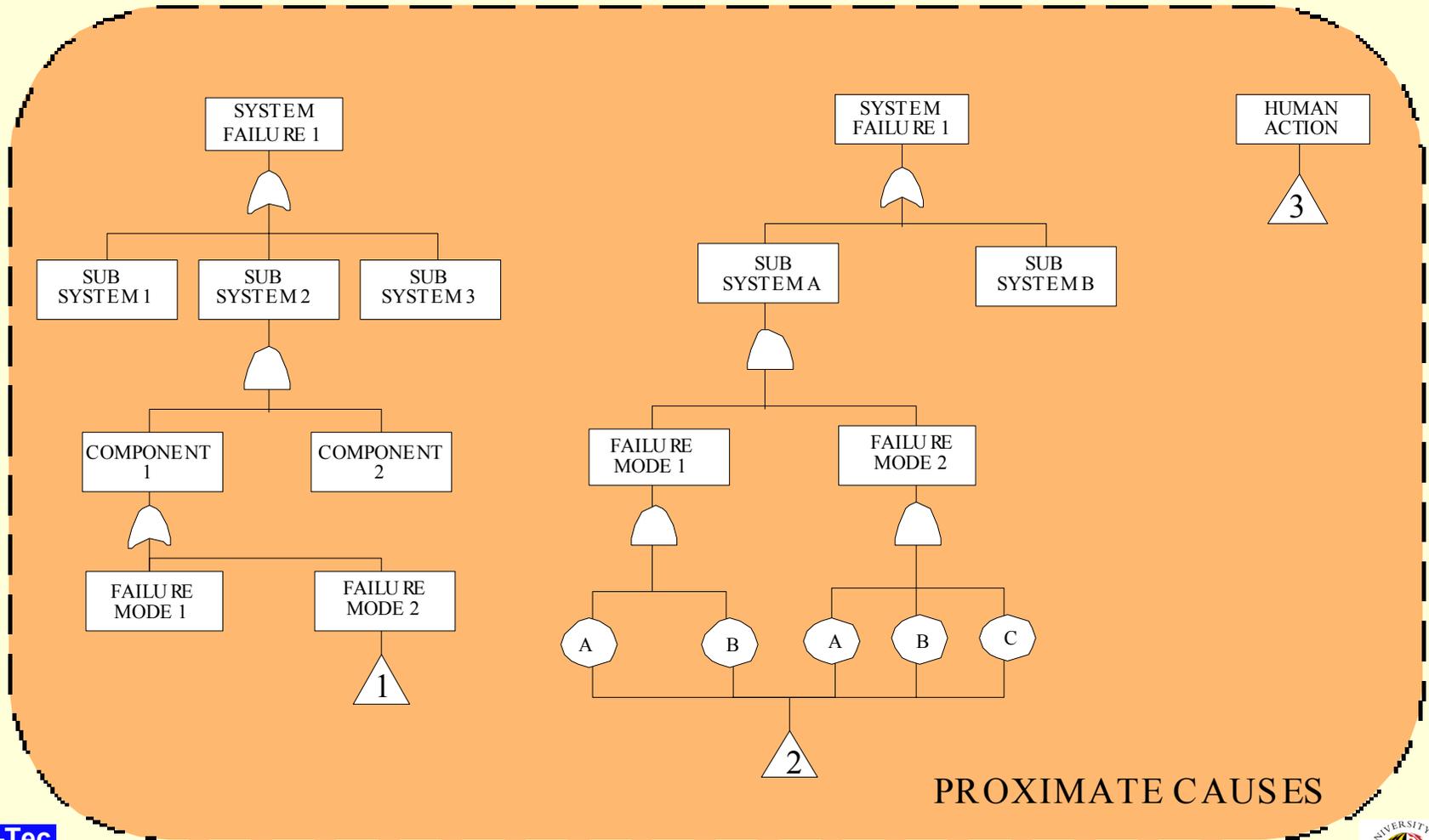
- Enables the analysts to develop a “safety model” of the aviation system
- Key elements of the safety model
 - Safety/Risk Scenarios (context)
 - Causes
 - System
 - Physical Environment
 - Organizational and Human Environment

Flight Safely Scenario Context for Causal Modeling (ESD Methodology)



Causal Modeling

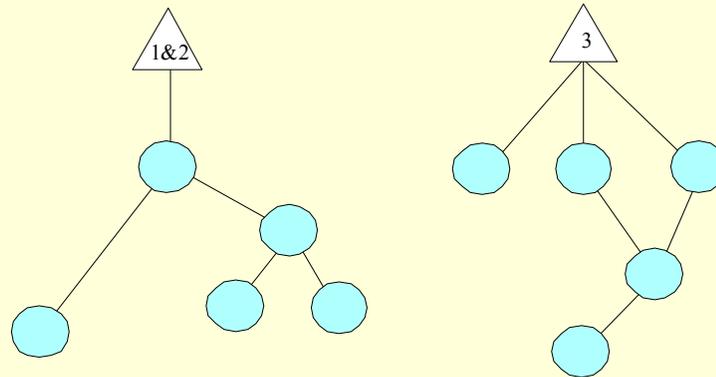
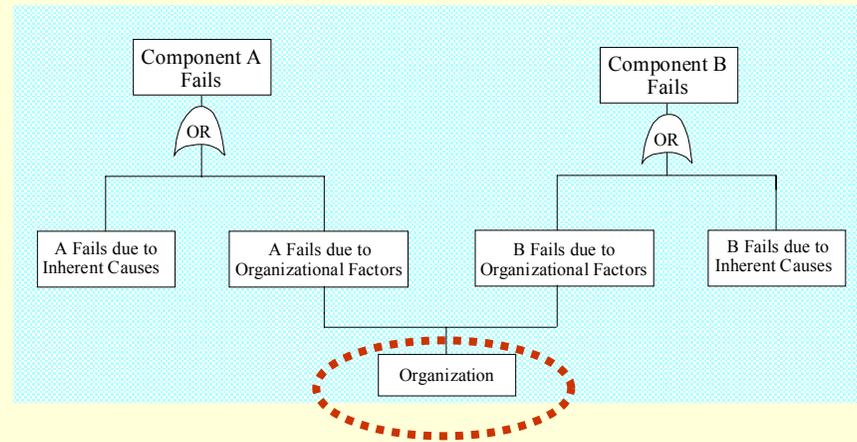
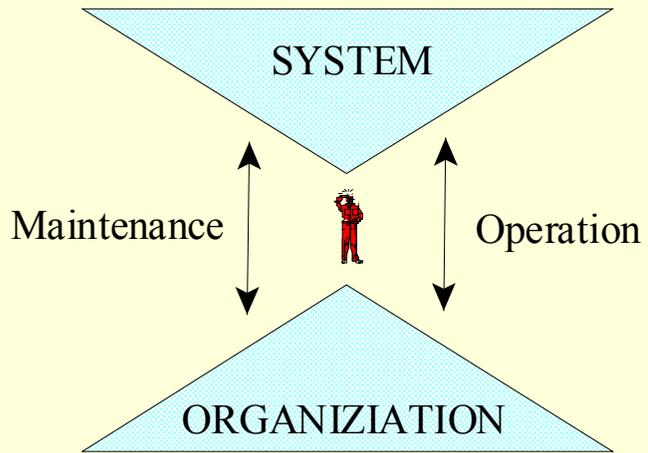
Deterministic Causal Relations



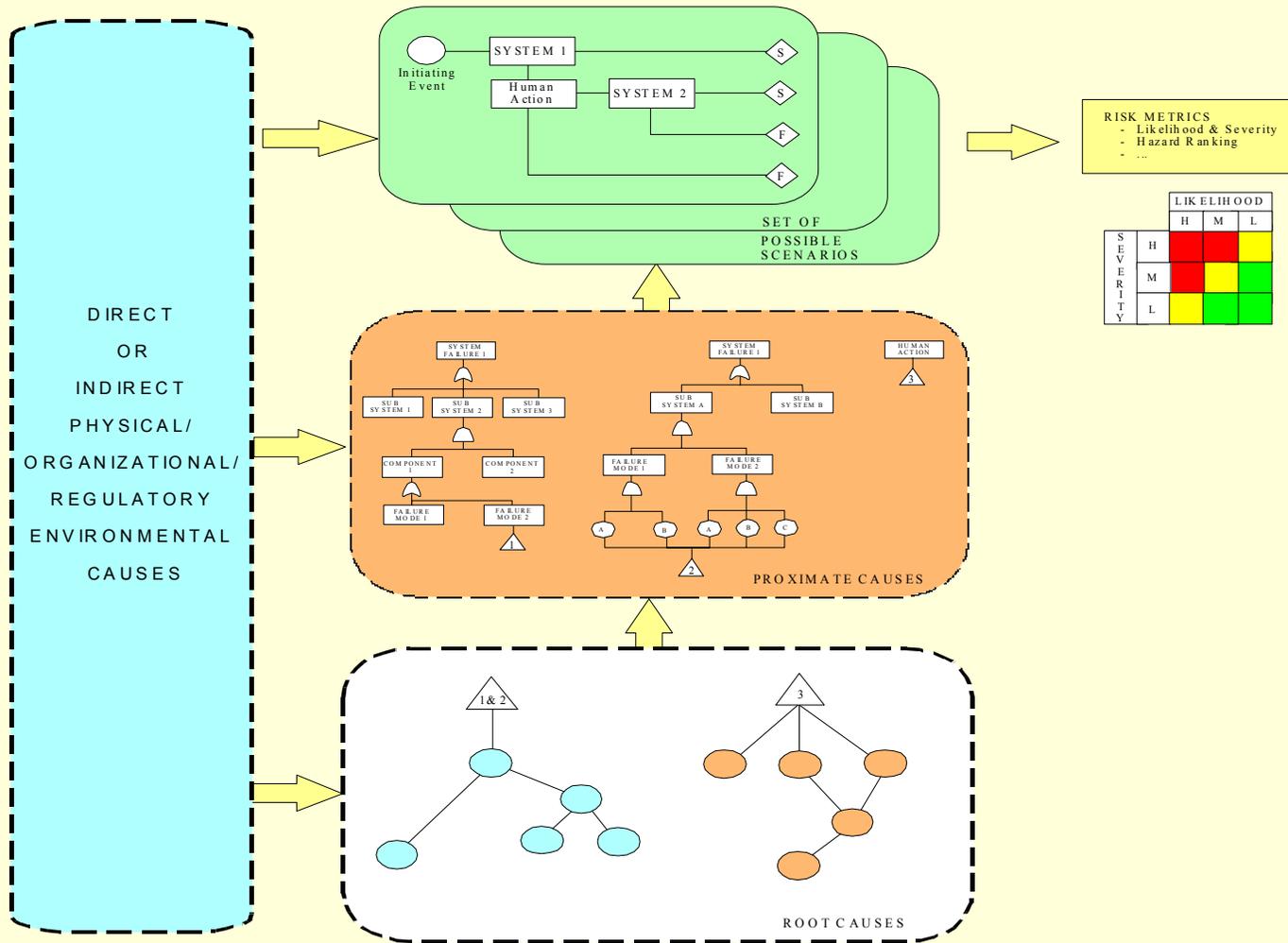
PROXIMATE CAUSES

Soft Causal Relations

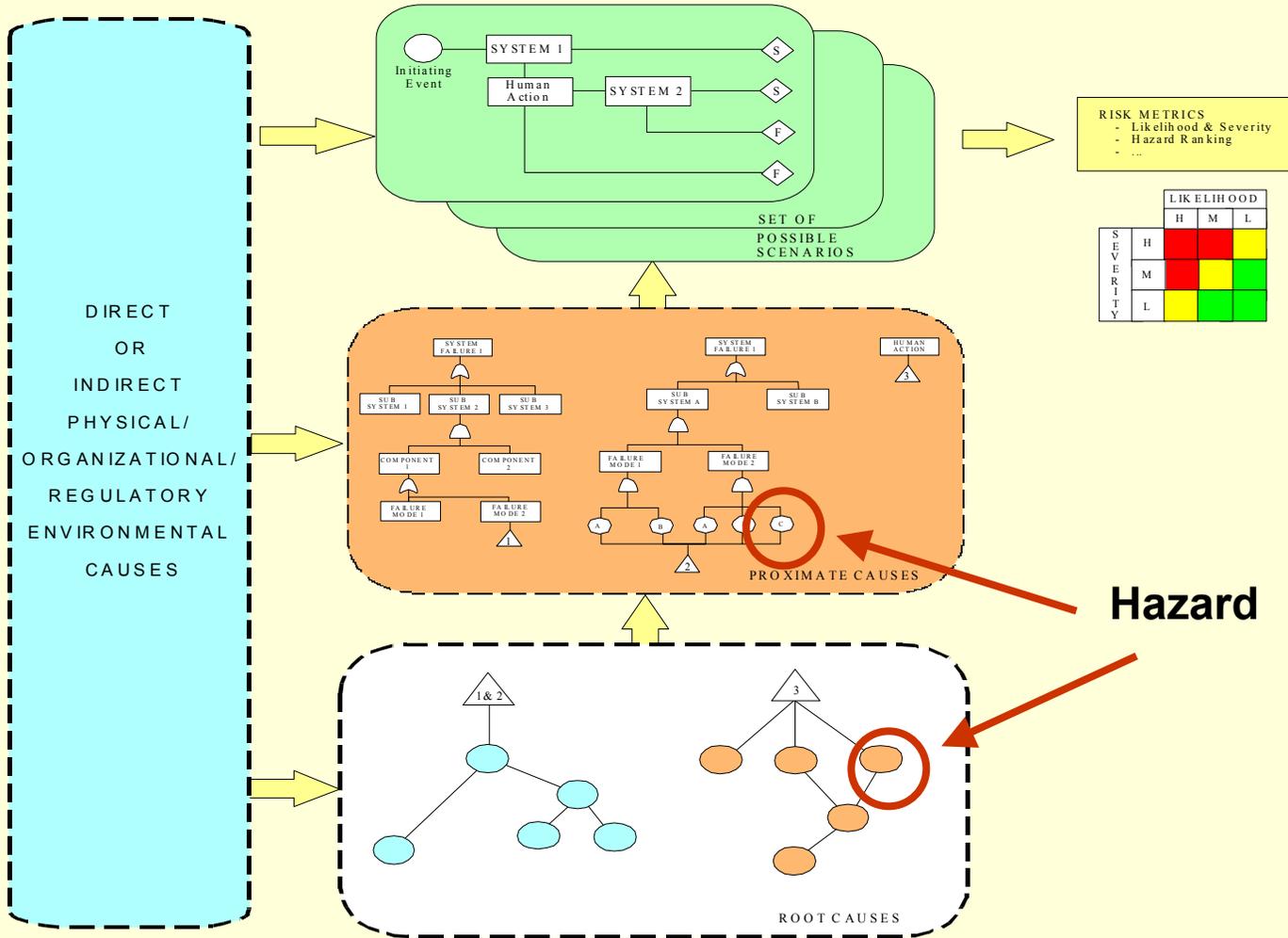
Human, Organizational, and Regulatory Factors



Integrated Safety Model (Framework)



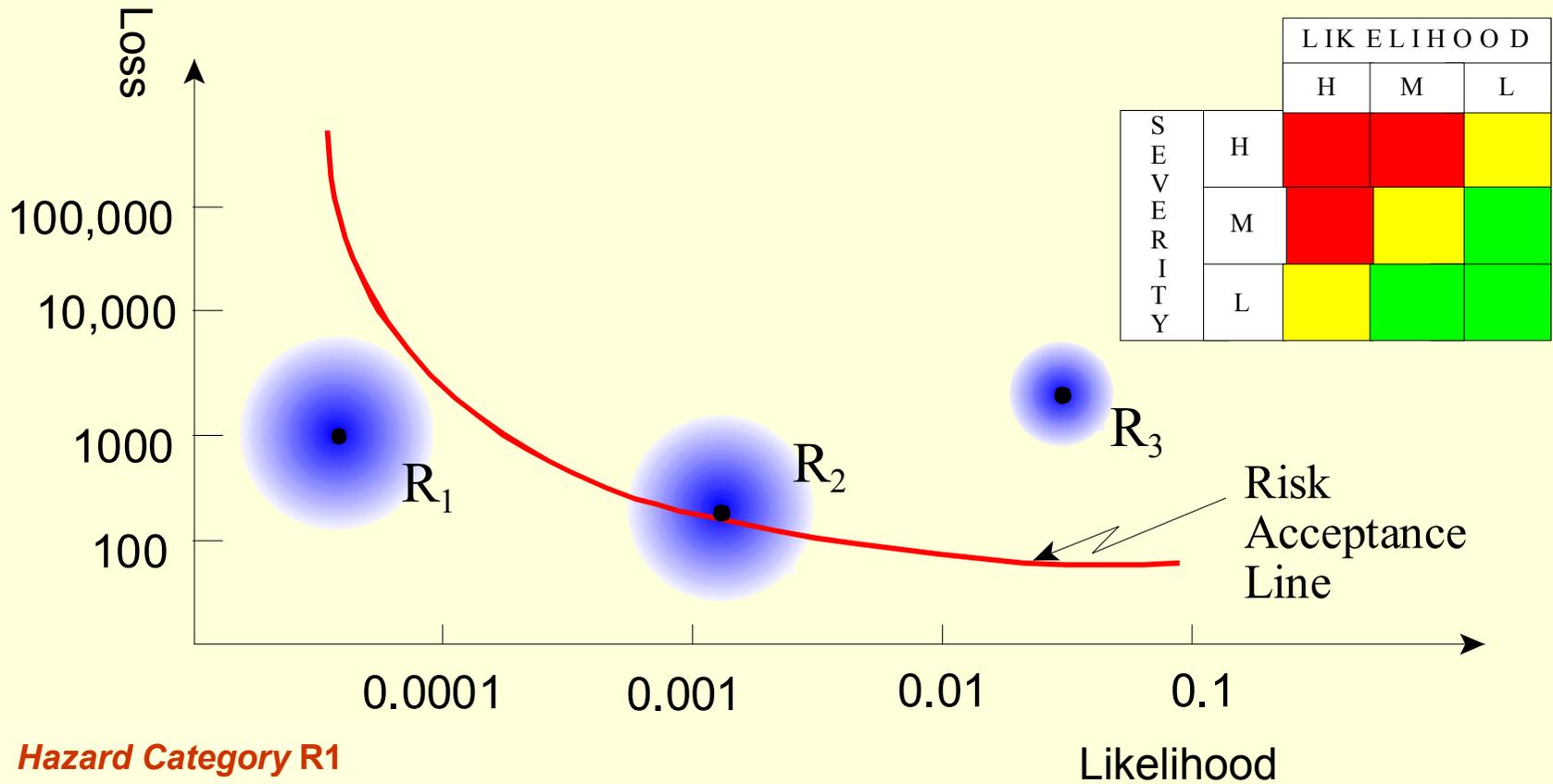
Hazard Identification Process



Hazard Ranking and Other Insights

ET Scenario	Min Cut Sets	Prob./ Freq	Cutset Freq.	Total Frequency
Scenario 3	IE	1.00E-02		
	/A1	1.00E-05	1.00E-07	
Scenario 9	IE	1.00E-02		
	/A2	1.00E-01		
	PP	1.00E-04	1.00E-07	
	IE	1.00E-02		
	CN	1.00E-04		
	/A2	1.00E-01	1.00E-07	
	IE	1.00E-02		
	/A2	1.00E-01		
	P1	1.00E-03		
	P2	1.00E-03	1.00E-09	
Scenario 6	IE	1.00E-02		
	L	1.00E-01		
	/A2	1.00E-01	1.00E-04	
	IE	1.00E-02		
	/L	9.00E-01		
	V2	1.00E-03		
	/A2	1.00E-01	9.00E-07	
	IE	1.00E-02		
	V1	1.00E-03		
	/A2	1.00E-01		
/L	9.00E-01	9.00E-07		
Sum				1.02E-04

Input to Decision Making (Risk, Safety, Hazard)



Hazard Category R1

Hazard Category R2

Hazard Category R3

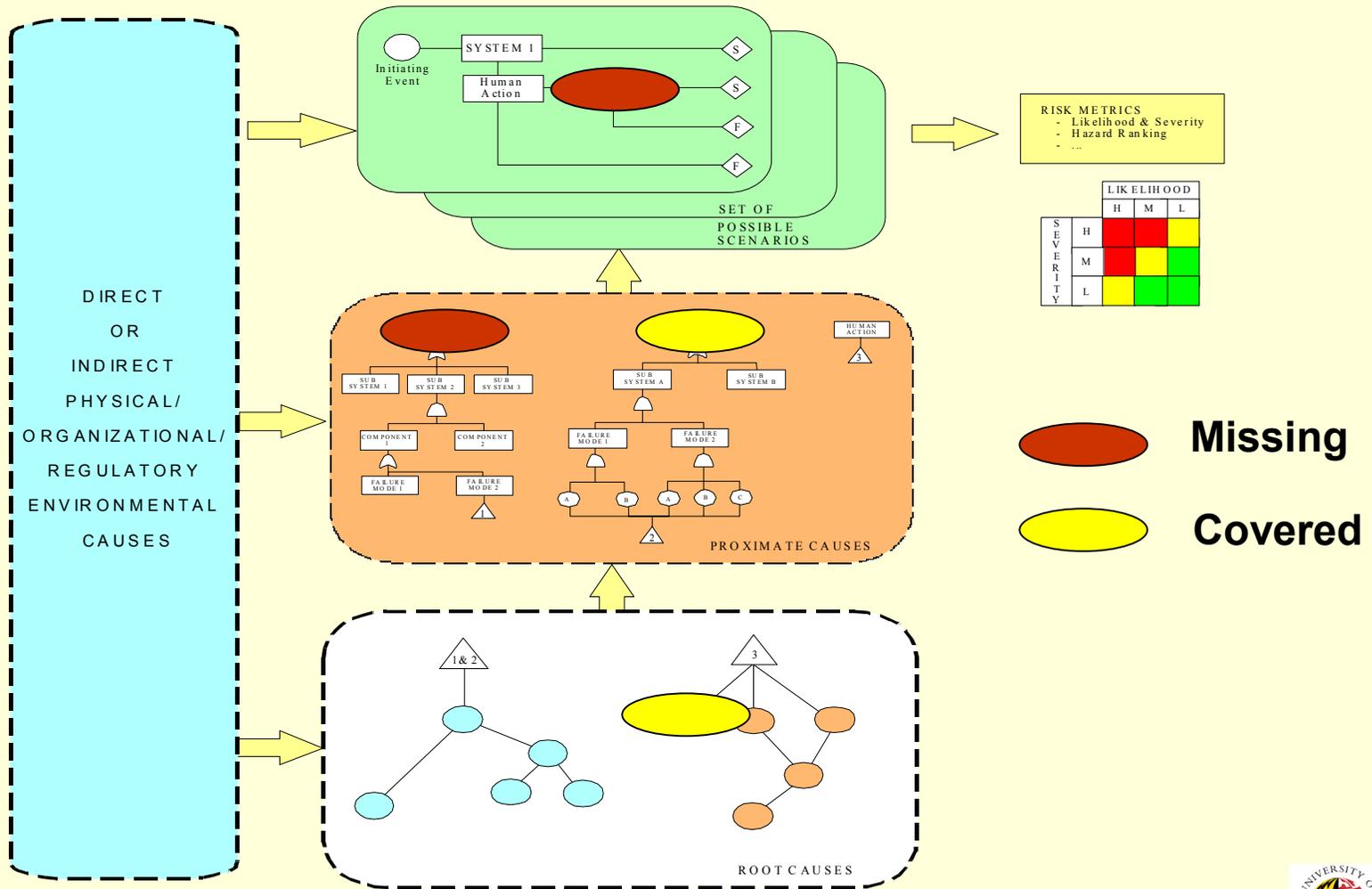
Areas of Application

- **Model-Based Hazard Analysis**
 - Explicit qualitative causal relation
 - Flexibility in level of detail through a hierarchical decomposition process
 - Capable of capturing deterministic and probabilistic causal relations
 - Capable of hazard ranking and prioritization

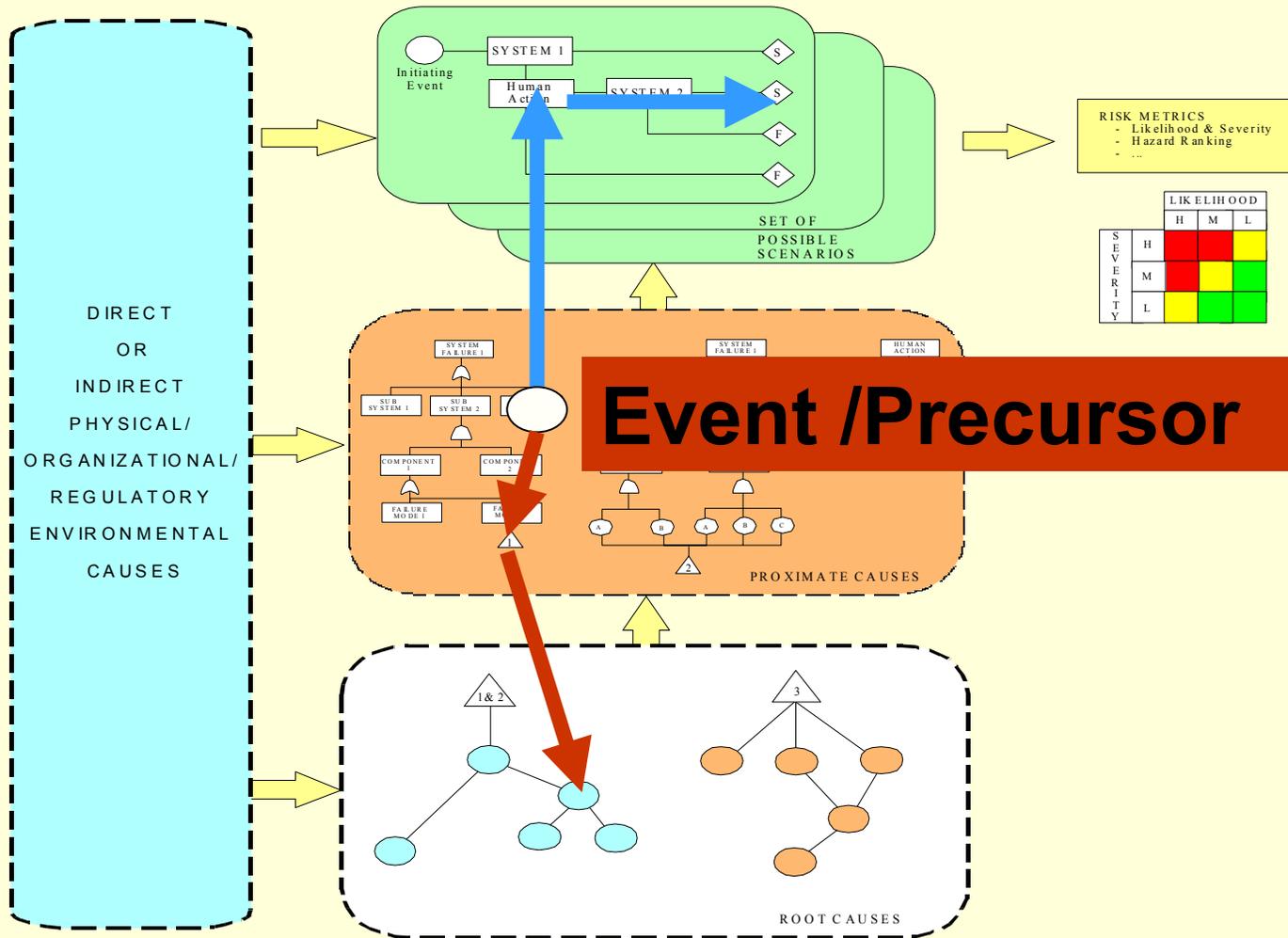
Areas of Application

- **Predictive and descriptive capabilities**
 - a quantitative risk analysis platform for
 - Safety and risk assessment
 - Evaluation of effectiveness of preventive measures
 - Evaluation of safety performance indicators
 - an environment for model-based
 - Data gathering and analysis (basis for taxonomy and level of detail for data collection)
 - Analysis of accident precursors
 - Basis for more systematic and more effective surveillance and inspection

Identification/Evaluation of Performance Indicators



Application to Precursor and Event Analysis

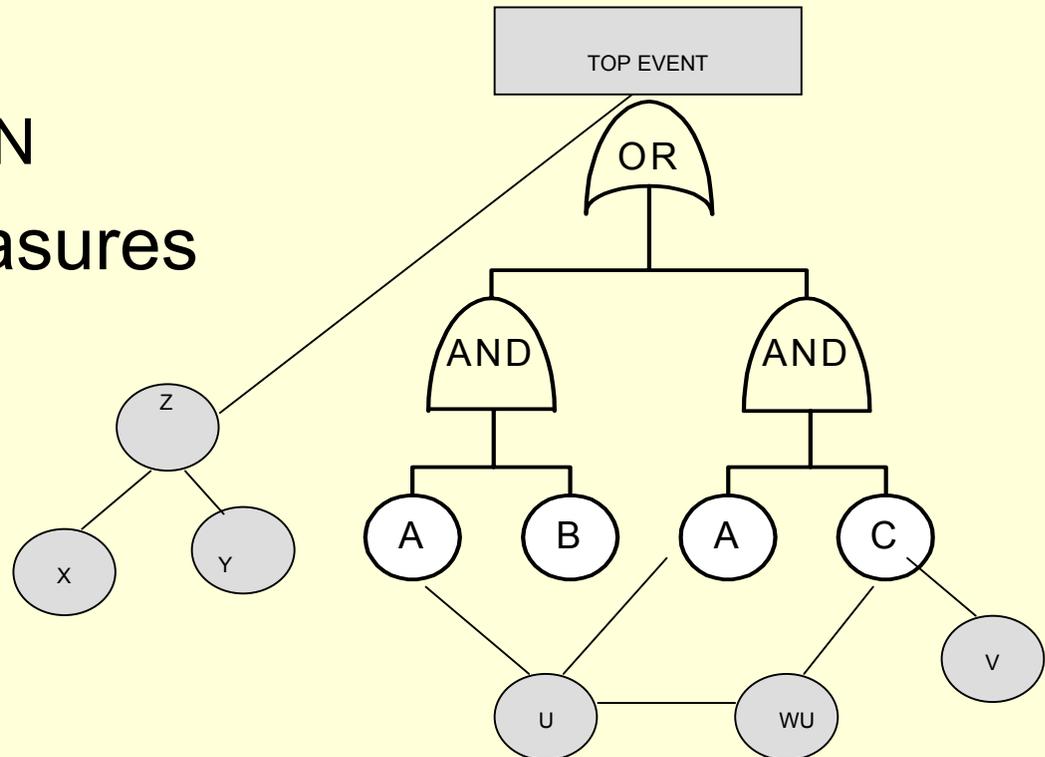
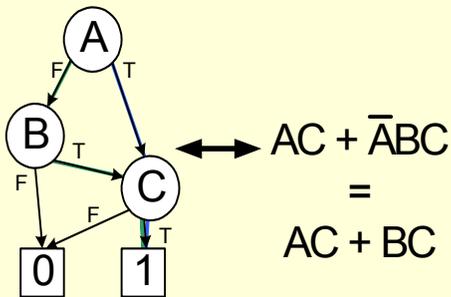


Technical Issues and Progress

- Development of mathematical algorithms
 - Integrating different causal modeling techniques
 - Treating model size and complexity
- Addressing data gaps and assessment issues
- Prototype software engine
- Procedures for use of existing information bases

Hybrid Causal Logic Concept

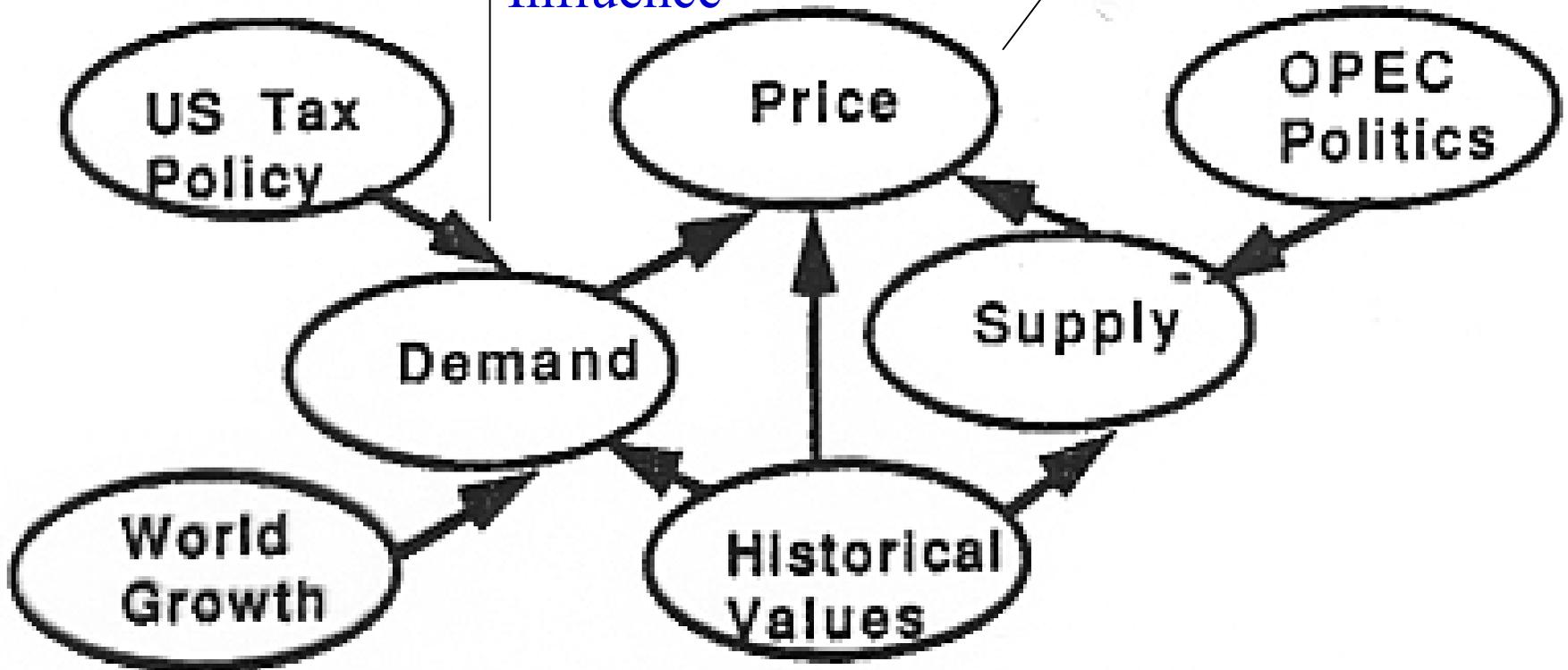
- Algorithms for solution
 - Mixed BDD-BBN
- Importance measures



Example 1: Forecasting Oil Prices

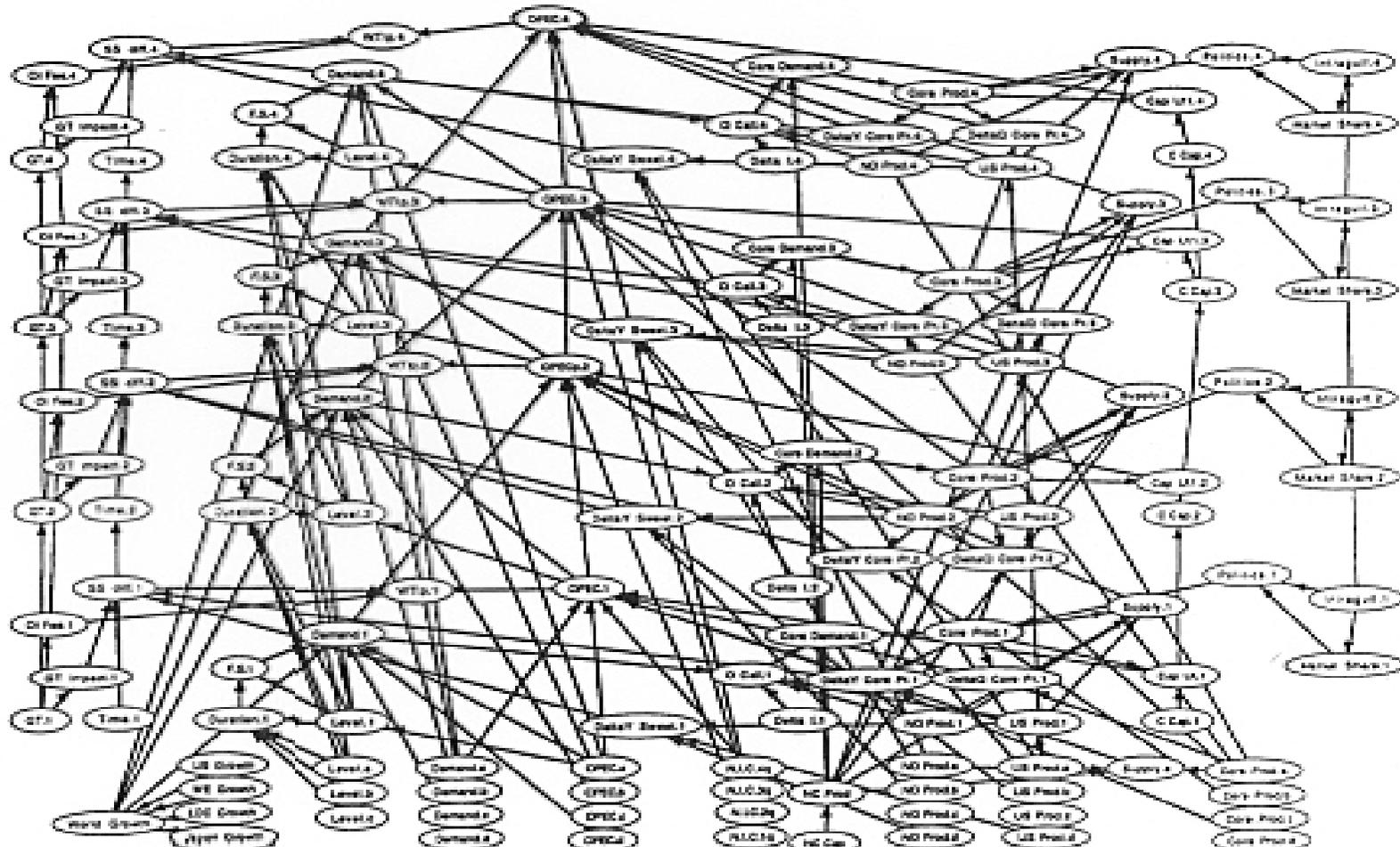
Links represents
Probabilistic
Influence

Nodes represent
random variables

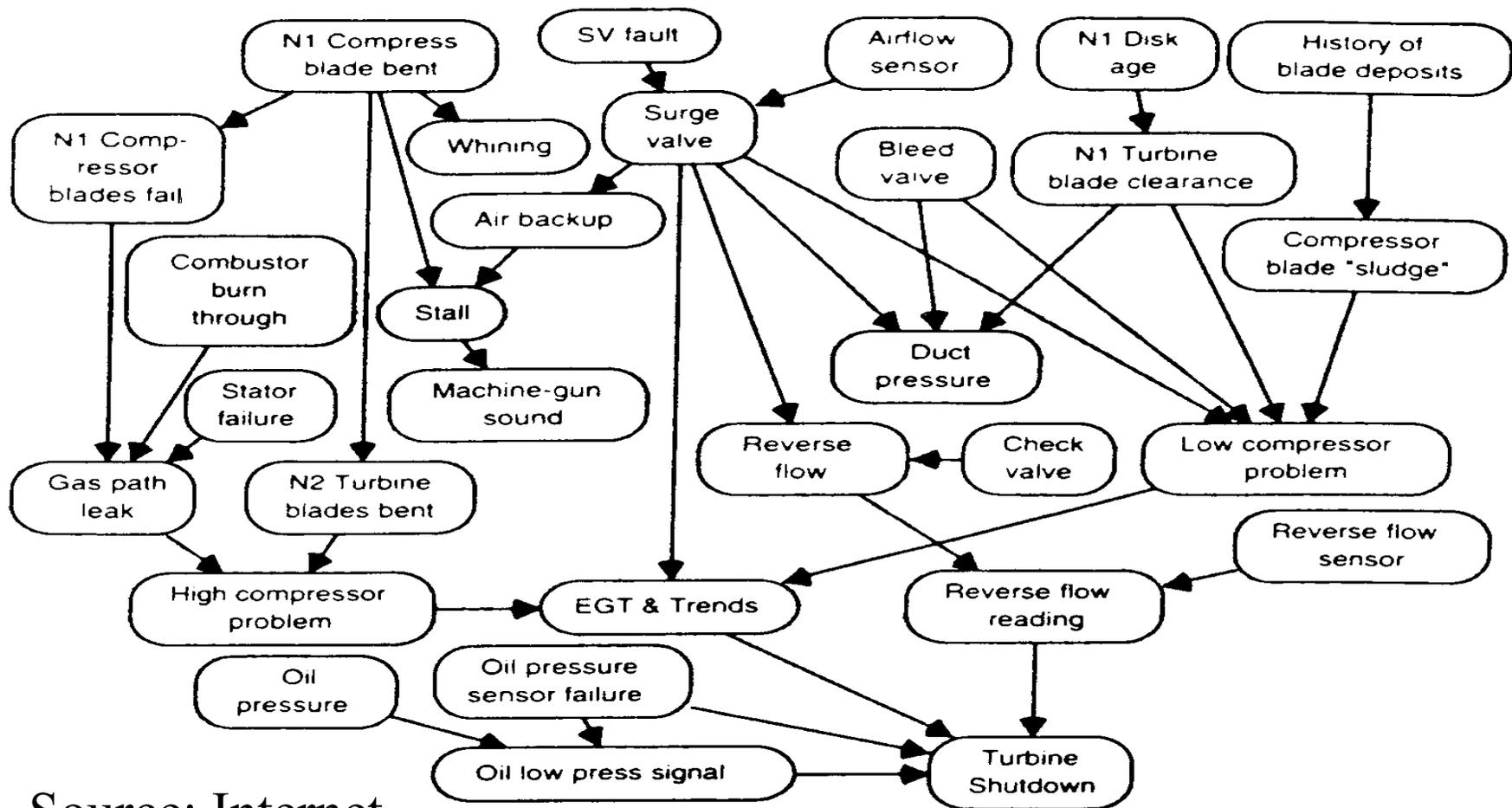


The structure of the network represents the probabilistic dependence/independence relationships among the factors (nodes).

Example 1 (Cont)

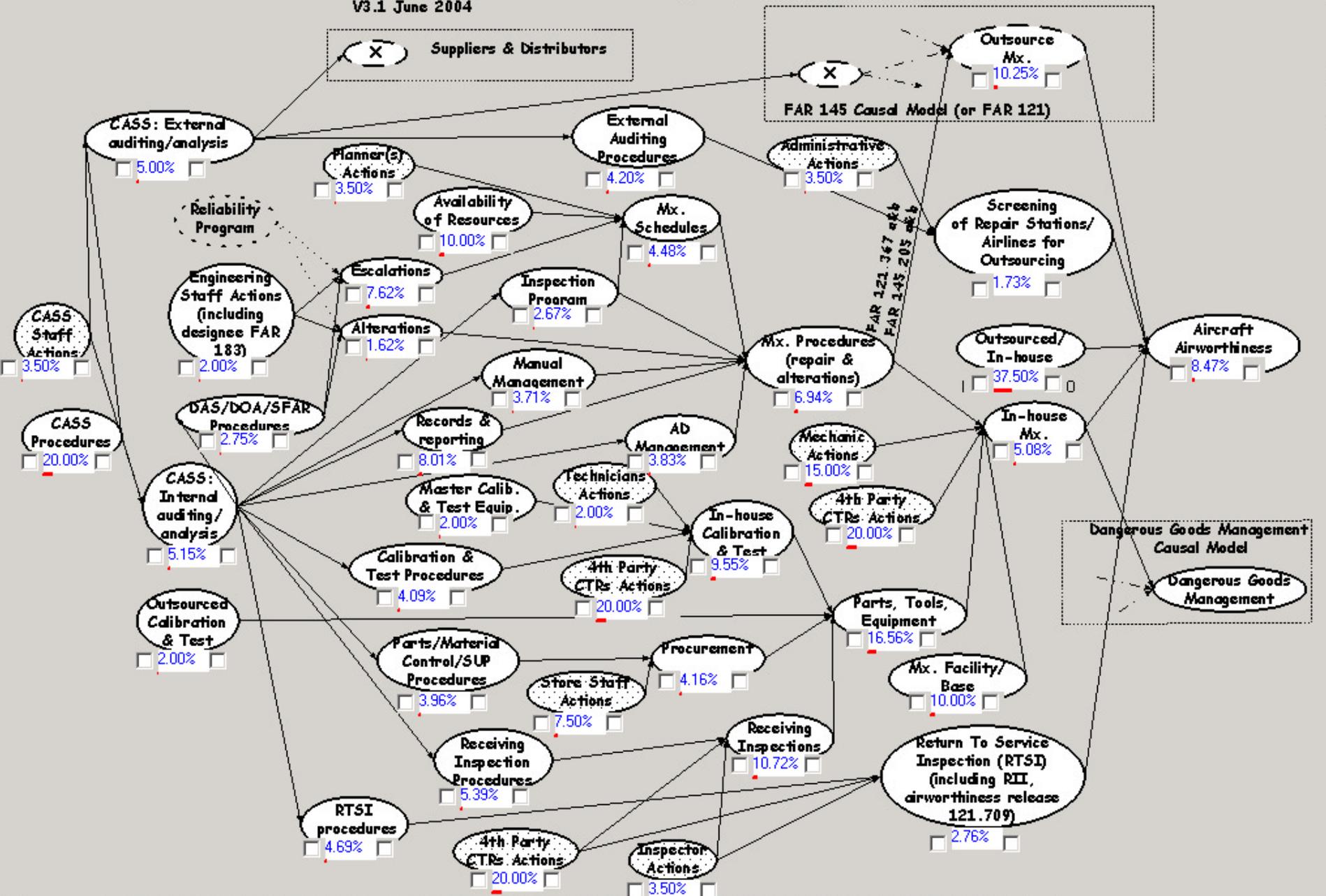


Example 2: Turbine Shutdown



Source: Internet

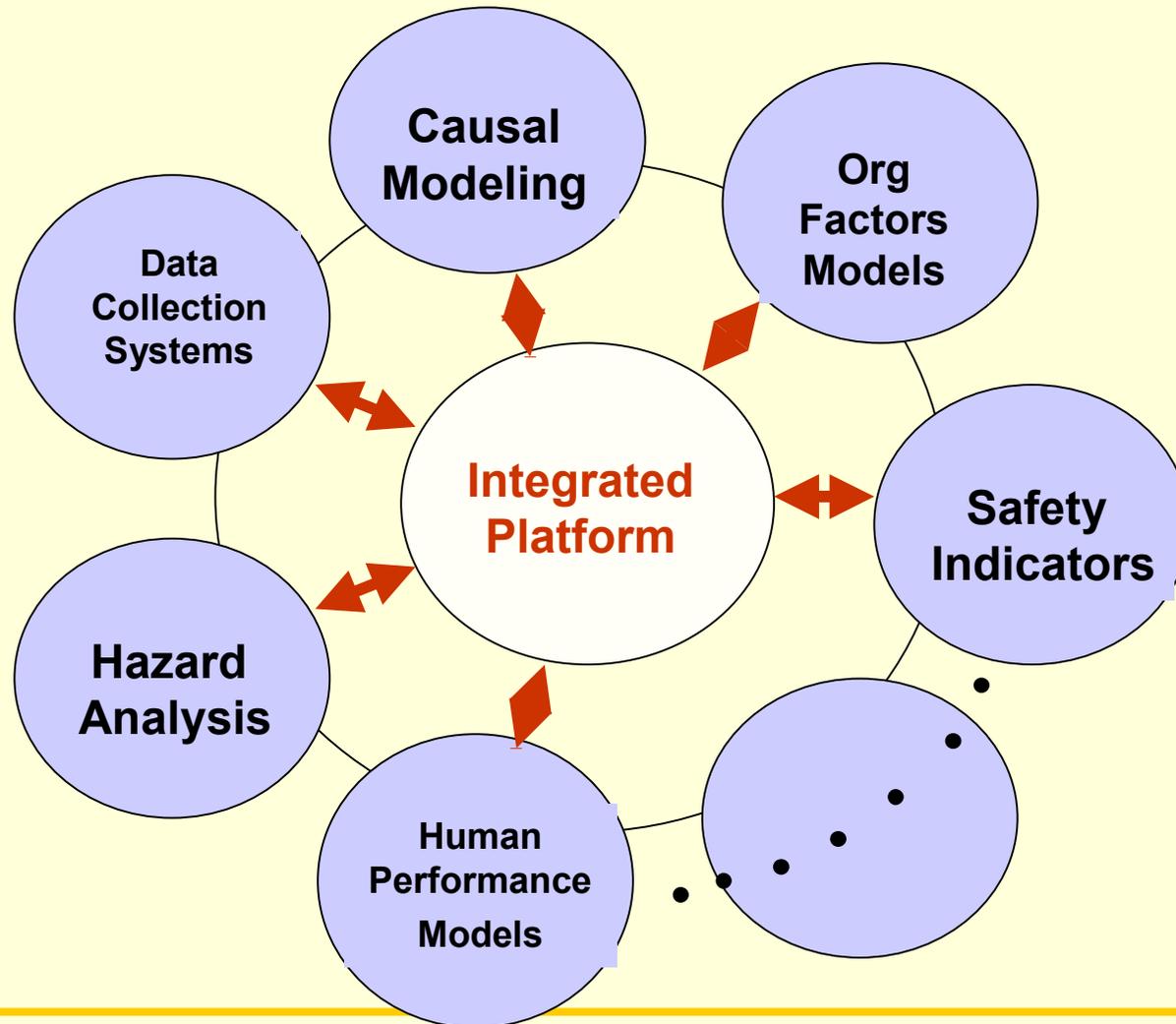
GENERIC CAUSAL MODEL OF
 AIR CARRIER'S CONTINUOUS AIRWORTHINESS MAINTENANCE PROGRAM (CAMP)
 V3.1 June 2004



Proposed Framework

- Systems Approach
- Systematic, Top Down, Context Driven
- Comprehensive framework covering various causal factors
 - Hardware/Software
 - Physical Environment
 - Human Actions
 - Organizational and Regulatory Environment
- Scalable
- Qualitative and Quantitative
- Solid Theoretical and Application Heritage

Integration of Various Research Results



Future Efforts

Methodology Development

- Improvement of HCL algorithms for
 - Scalability to large scale causal models
 - Incorporation of QQ-BBN capability
- Inference methods and algorithms for use of data and expert judgment in support of HCL (qualitative and quantitative) assessment
- Algorithms for combined ESD/HCL

Future Efforts

Methodology Development

- Development of methods and guidelines for
 - Delineation of generic hazard scenarios (hazard context ESDs)
 - Development of HCL causal models using existing and evolving results from other research and developing activities
 - How to build HCLs with
 - human causal factors
 - organizational causal factors
 - hardware causal factors

Future Efforts

Methodology Development

- Development of methods and guidelines for
 - Risk Analysis
 - Hazard Identification
 - Use of precursor data for safety model enhancements and quantification

Future Efforts

Methodology Implementation and Validation

- Implementation of the entire framework in form an integrated platform
 - Based on NASA QRAS experience
- User need determination
- Further methodological development to support possible gaps
- Design and prototyping of interface for identified needs and applications
- Full scale demonstration and validation in few application areas