Resilient Control Systems Design: Issues, Challenges, and Opportunities

Venkat Venkatasubramanian

Laboratory for Intelligent Process Systems
School of Chemical Engineering
Purdue University
W.Lafayette, IN47907

Outline

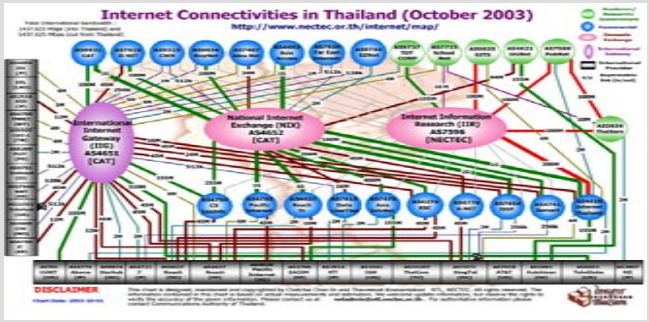
- Complex Networked Systems
- Abnormal Events Management (AEM)
- Resilient Design and Control
- Challenges and Opportunities
  - Science of Complexity and Emergent Behavior
  - Learning from Nature
- Summary

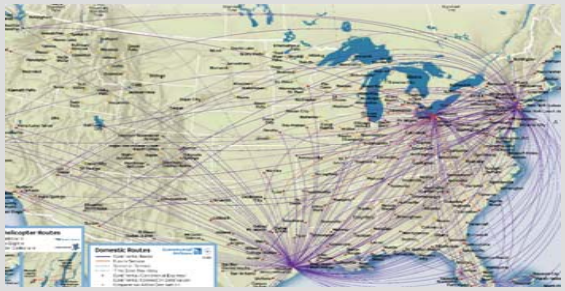
Talk Philosophy

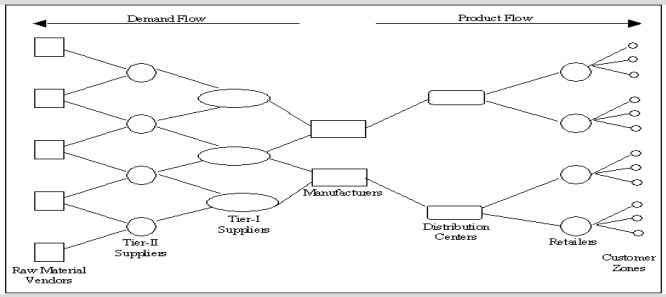
- **Broad overview**
  - Not a detailed, in-depth review
  - Identify key concepts, issues, challenges
  - Compare and contrast different approaches

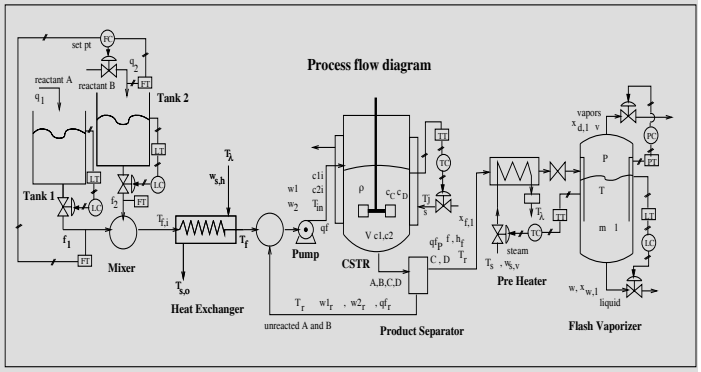
Complex Networked Systems

- Internet
- Transportation networks
- National power grids
- Global supply chain networks
- Process plants









Complex Networked Systems: Common Features

- Transport Material, Energy, Information
- Common Features:
  - Size: Thousands to billions of nodes and connections
  - Structure: Topological features and motifs
  - Interactions: Nonlinear, feedback loops, cascading, unforeseen
  - Environment: Complex interactions with the environment
  - Modes or States: Many “hidden” patterns of behavior, multiple pathways
  - Adaptation: Structure can change or evolve to optimize some performance goal
  - Complex dynamics: Leading to “Emergent” behavior
  - Behavior of the “Whole” is more than the sum of its “Parts”

Abnormal Events Management (AEM) and Resilient Control

- **Abnormal events are deviations in system behavior from normal operating regime**
  - Safety/Security problems, Environmental concerns, Quality of service problems and Economic losses
- **Why do abnormal events occur?**
  - Human errors: Design Flaws, Operational Mistakes (~70%)
  - Material/Equipment degradation and failures
  - Natural events: Hurricanes
  - Intentional attacks

AEM is a Systemic Problem

- **Generic problem of Complex Systems**
- **Unforeseen interactions and defects/mistakes leading to systemic failures over the product life**
  - Bhopal, Piper Alpha, Flixborough Disasters
  - Ford Explorer ATX Tire Tread Failure and Recalls:
    88 deaths and $1B in estimated losses
  - Electric Power Failure in the US East coast in 2003
  - Drug Recalls in the Pharmaceuticals Industry (9/3/03 WSJ)
    - 176 recalls in 1998
    - 248 recalls in 2001
    - 354 recalls in 2002
- U.S. manufacturers spend $5B annually recalling and renewing 2,500 defective products and $50B on lawsuits and warranty claims
- Increasingly frequent gridlock in transportation arteries, inadequate power from utilities, and disruptions to supply chains

AEM Lessons Learned

- **Need intelligent real-time operator support**
  - **Prognostic: Anticipate Problems**
  - **Diagnostic: Effectively and Safely Manage Problems**
- **Instead of the React-and-Fix approach, we need to anticipate and manage "emergent" behavior better**
  - **Resilient systems**
- **Need more thorough PHA and integration with AEM**
    - **New OSHA/EPA regulations**
- **Importance of Operator Training**
- **Management/Organization commitment to AEM and PHA**

Resilient Control

- **Resilient Systems**
  - Recovering or rebounding readily from adversity, *resilire* – to jump back
- **Resilient control is not a new concept – Degrees of resiliency**

Variable	**e.g. inlet flow rate high** **Regulatory Control (RegC)**
Parameters	**e.g. Fouling in heat exchanger reduces the heat transfer coefficient** **Model Predictive Control (MPC) and RegC**
Models	**e.g. process shifted to a different operating regime** **Fault Tolerant Control (FTC) and Intelligent Supervisory Control (ISC)**
Structural	**e.g. equipment failure** **Intelligent Supervisory Control (ISC)**
Systemic	**Resilient Control**

- **What is new is perhaps the systemic perspective of resiliency**

Resilient Control Challenges

- **Large Network of Interacting, Interdependent, Systems and Sub-systems**
  - **Thousands of Components or more**
  - **Complex configurations**
  - **Nonlinear interactions leading to "Emergent" behavior**

- **Difficult to predict, control, diagnose, and manage**
  - Running systems near their limits due to RTO reduces margin for error
  - System-wide integration makes reasoning difficult
  - Difficult to anticipate reaction to changes to inputs, structure, or environment
  - Uncertain and/or incomplete data and information
  - Many potential modes of failures, combinatorially large search space
  - Fewer experienced operating personnel due to downsizing
  - Lack of adequate training of operators

Decision Support Needs of Operators

- Inadequate precision of temporal information (e.g. lack of true alarm order)
- Excessive nuisance alarms due to weak conditional alarming capabilities.
- Inadequate anticipation of process disturbances
- lack of real-time, root-cause analysis (symptom-based alarming)
- Lack of distinctions between instrument failures and true process deviations
- Poor integration of multiple information and control system components.
- Limited capabilities to view interrelated process data.
- Lack of adequate tools to measure, track, and access past records of abnormal situations.
- Limited or time-consuming access to procedures or operating instructions.
- Cumbersome and un-integrated communications between and within plant units.

Resilience requires Intelligence

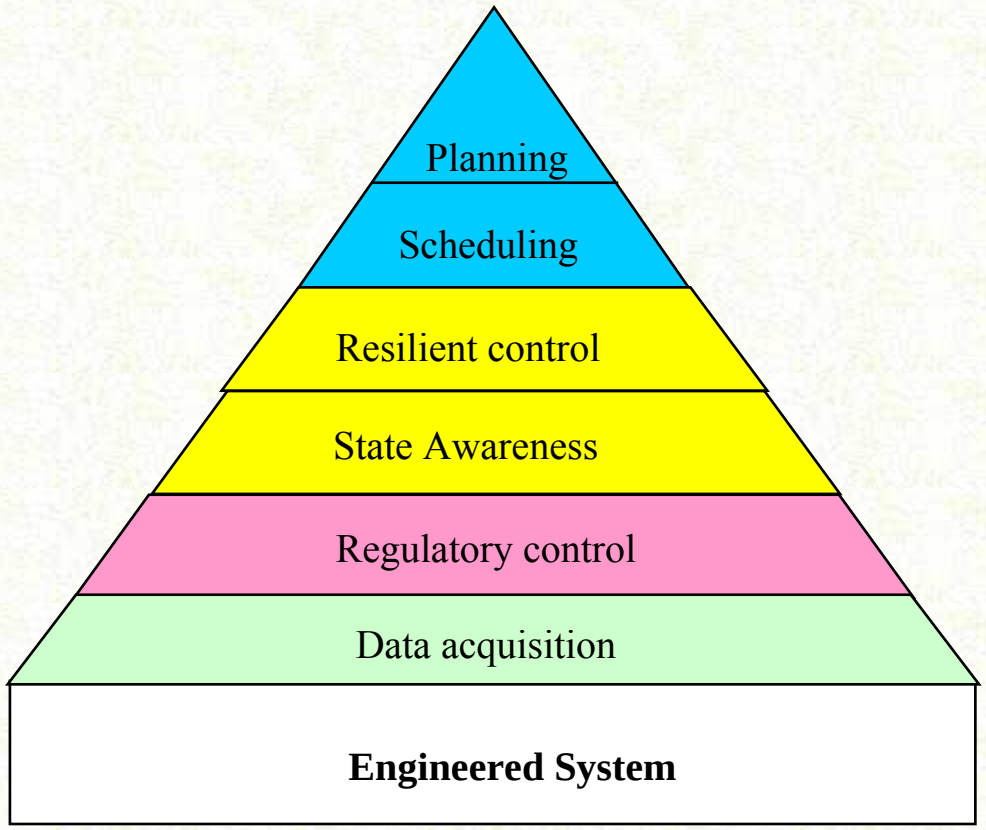
Resilient Systems: Performance Expectations

- State Awareness
  - Be aware of what is happening to itself and the environment in real-time all the time
  - Quick abnormality or anomaly detection and diagnosis
  - Robustness to noise and uncertainties
- Adaptability
- Autonomy: Empowered to make decisions
- Leverage human intelligence
- Graceful degradation, not catastrophic
- Reliability, Safety, and Security

Resilient Systems

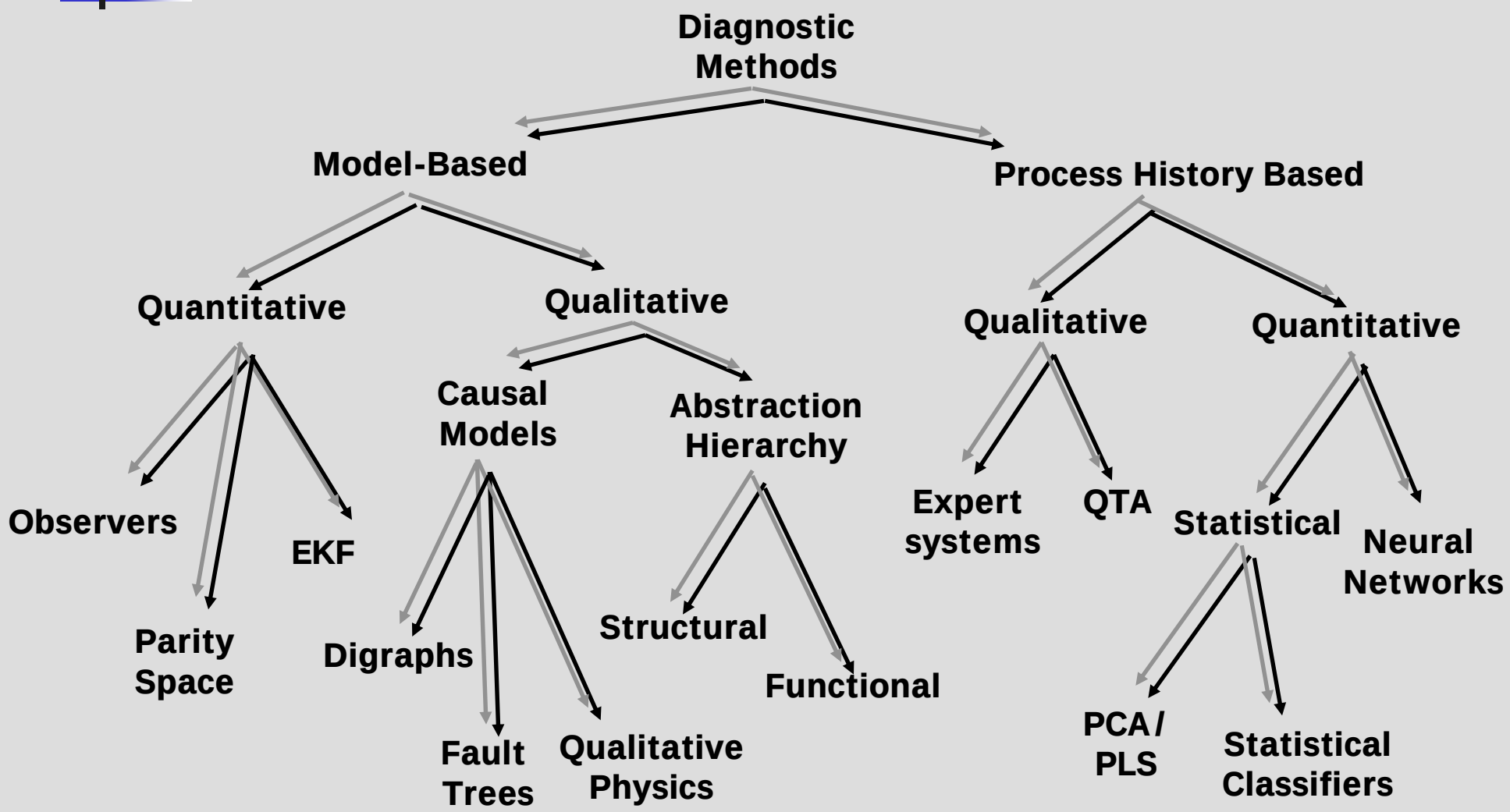
- Achieving Resiliency
  - Resilient Design
  - Resilient Control

Resilient Control Hierarchy



©V. Venkatasubramanian, 2008

Fault Diagnosis is Crucial to Resiliency



Model based Framework: Challenges

- **Appropriate level of modeling**
  - Too Coarse: Not very useful results
  - Too Fine: Too complex and buried in details
  - Quantitative vs Qualitative

- **“ALL MODELS ARE WRONG, SOME ARE USEFUL”**

  -- George Box (U. Wisconsin)

Comparison of Different Diagnostic Methods

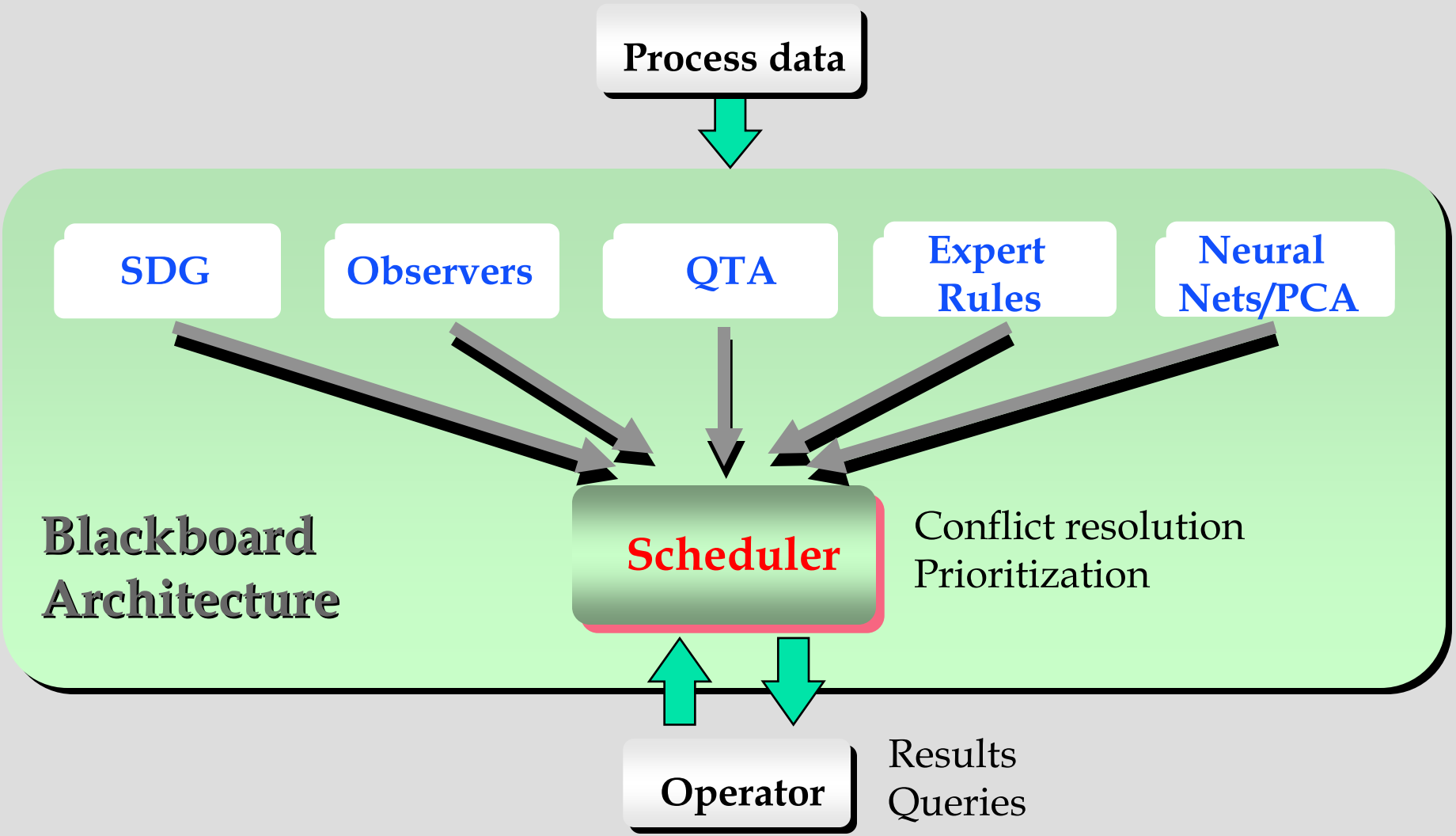
	Observer	Digraphs	Abstraction Hierarchy	Expert Systems	QTA	PCA	Neural Networks
Quick Detection and Diagnosis	✓	?	?	✓	✓	✓	✓
Isolability	✓	×	×	✓	✓	×	✓
Robustness	✓	✓	✓	✓	✓	✓	✓
Novelty Identifiability	?	✓	✓	×	?	✓	✓
Classification Error	×	×	×	×	×	×	×
Adaptability	×	✓	✓	×	?	×	×
Explanation Facility	×	✓	✓	✓	✓	×	×
Modelling Requirement	?	✓	✓	✓	✓	✓	✓
Storage & Computation	✓	?	?	✓	✓	✓	✓
Multiple Fault Identifiability	✓	✓	✓	×	×	×	×

No single method achieves all

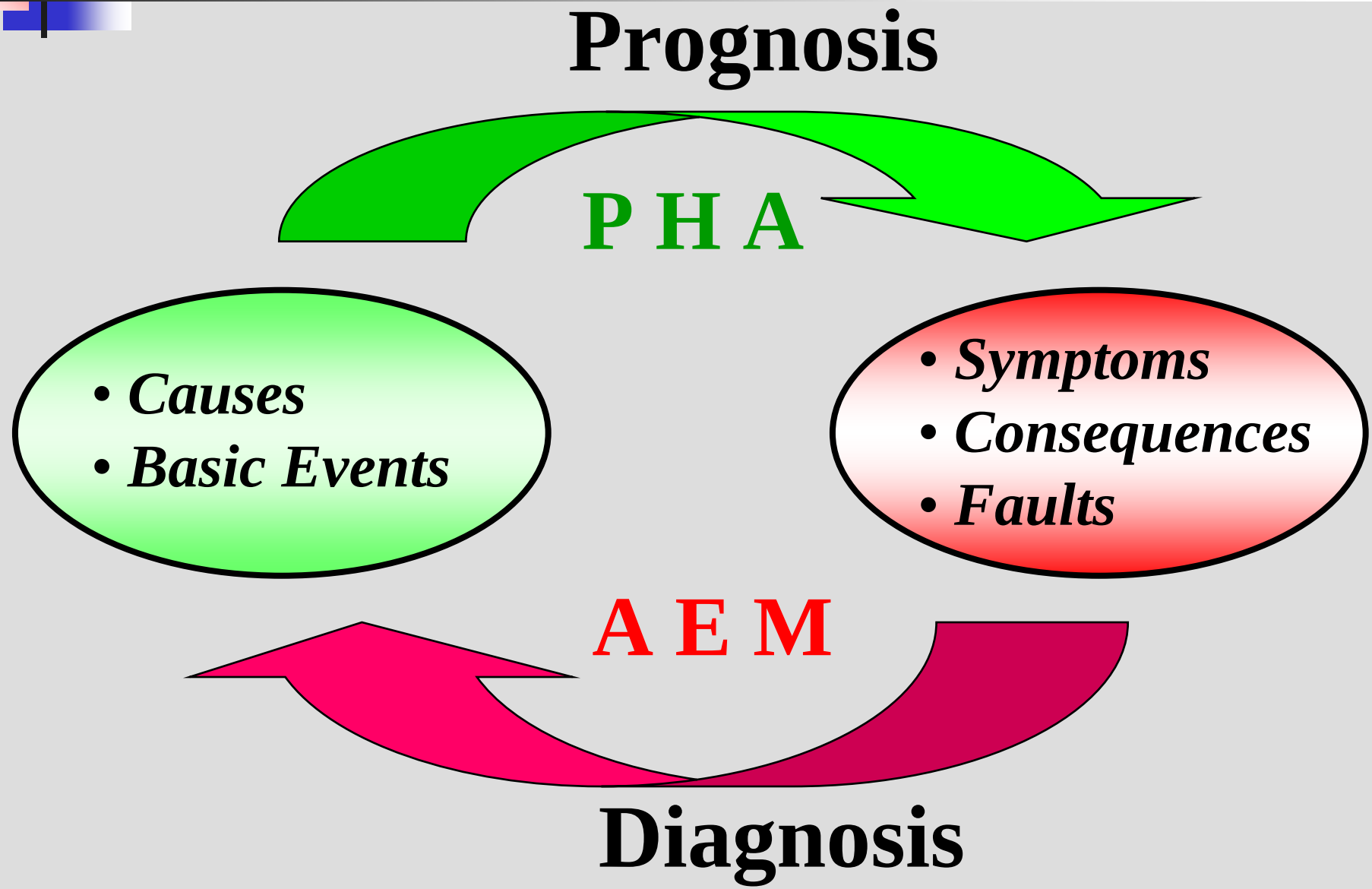
Hybrid Framework

- **No single** method meets all the criteria of a ‘good’ diagnostic method
- **A Hybrid** Framework
  - Involving different methodologies
  - Based on a collective and synergistic approach to problem solving seems most promising (Mylaraswamy & Venkatasubramanian, 1997)
  - Compensate one method’s weakness with the strengths of another’s
- **Dkit** implemented in G2
  - Effectiveness demonstrated on Model IV FCCU by successfully diagnosing wide varieties of faults
  - Combined causal model-based diagnosis with statistical classifiers
  - Basis for the prototype of the Honeywell ASM Consortium
  - Licensed to Honeywell by Purdue University

Diagnostic ToolKit (Dkit)

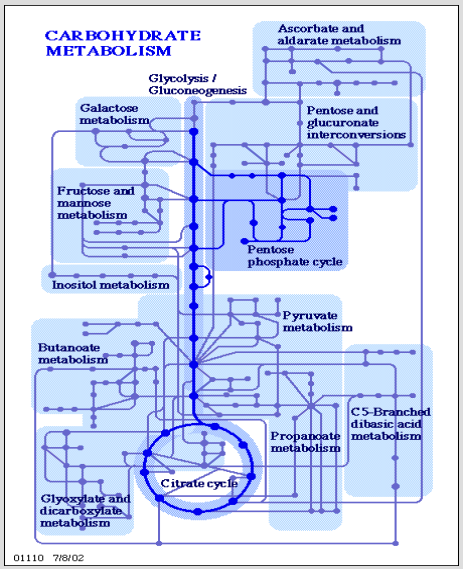


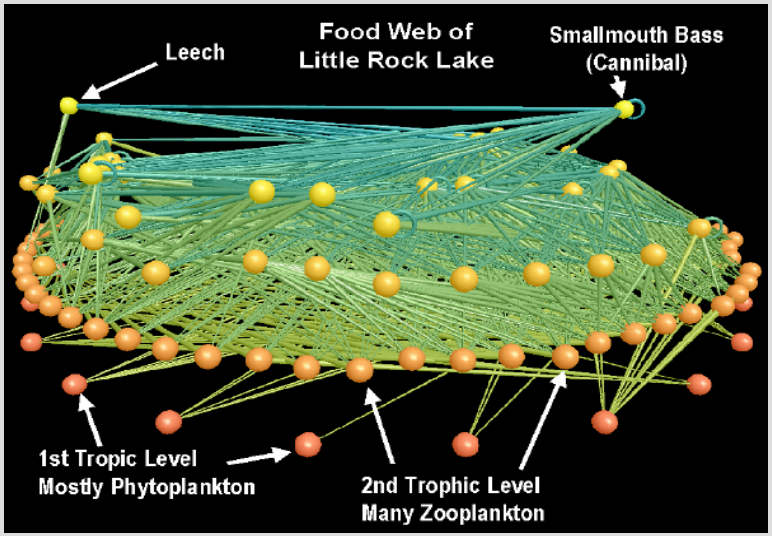
Abnormal Events Management (AEM) and Process Hazards Analysis (PHA)

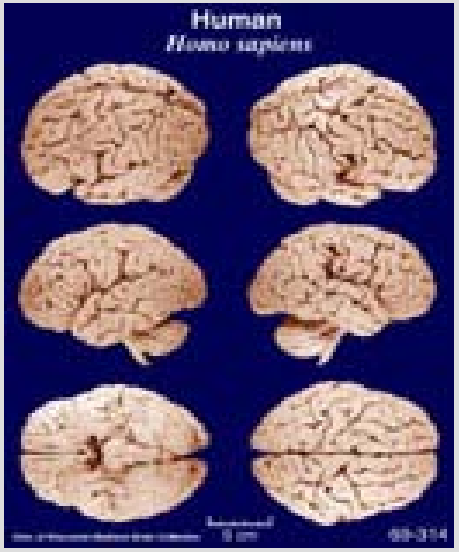


Resilient Networked Systems in Nature

- Cellular and metabolic networks
- Protein interaction networks
- Food webs, ecosystems
- Brain







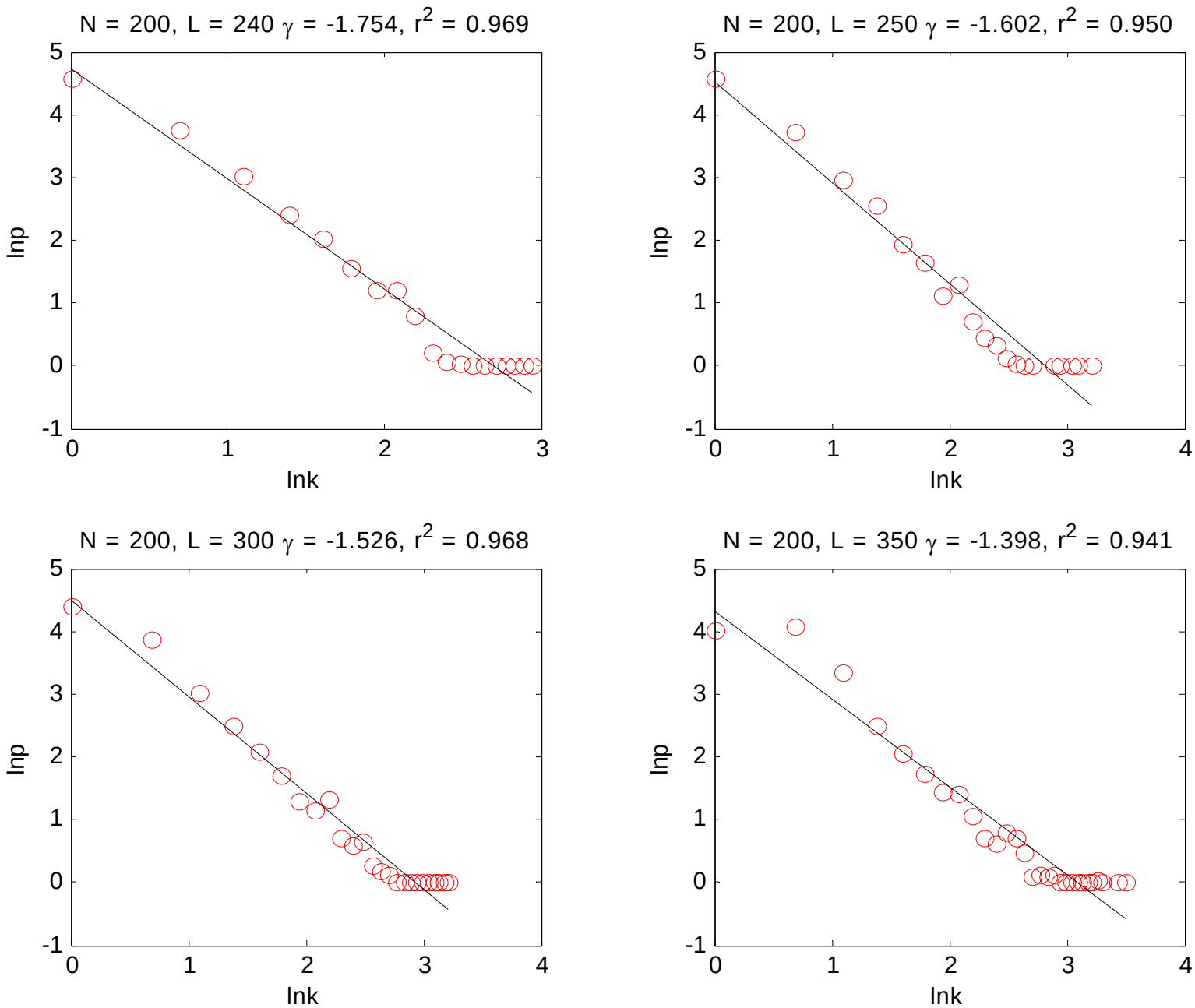
What can we learn from Nature?

Natural systems are perhaps the most resilient

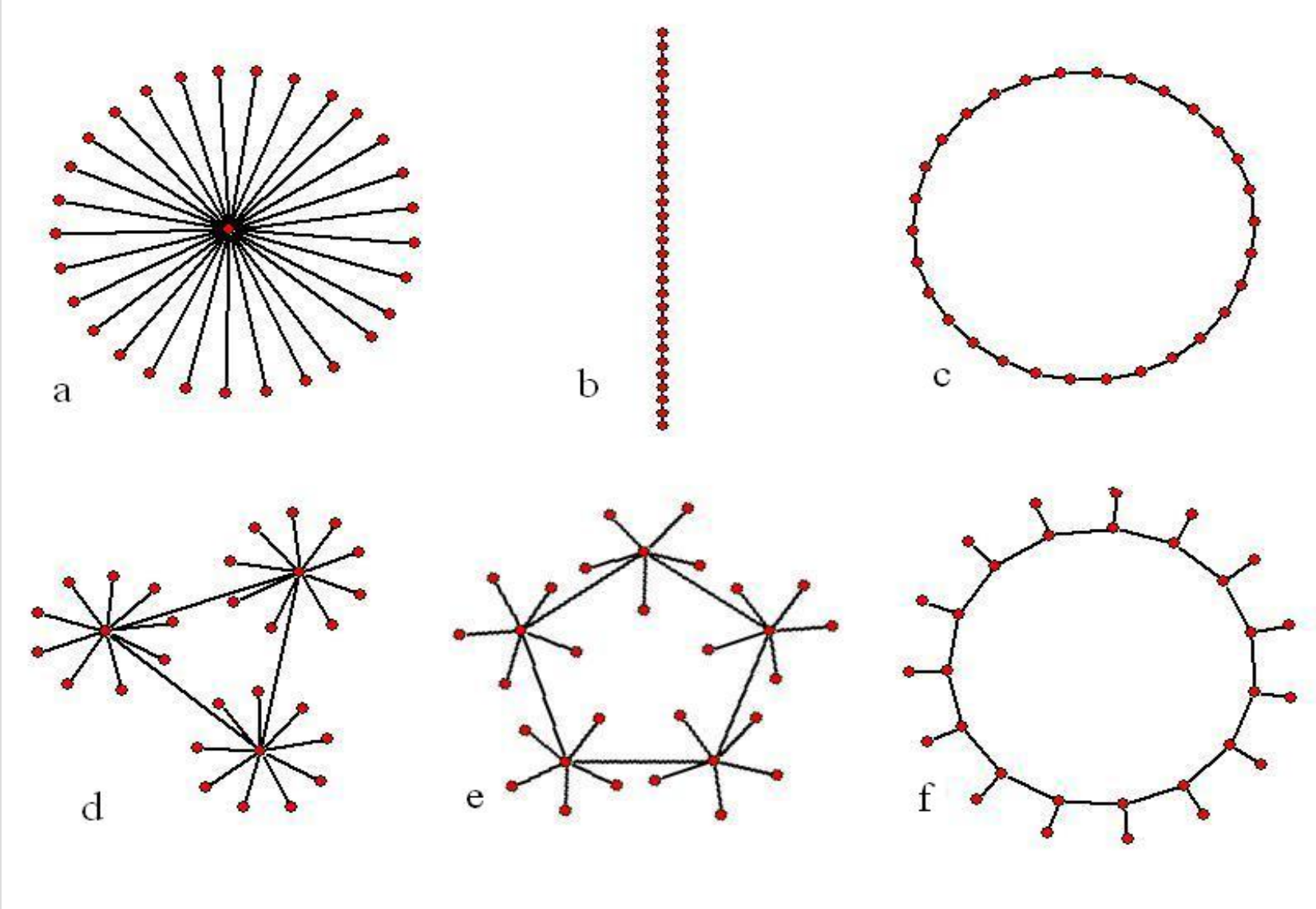
- Robustness to upsets: e.g. loss of species
- Distributed systems
- Decentralized control: e.g. ant foraging, swarms
- Evolutionary
- Adaptive
- Self-organized
- Emergent

Science of Complexity and Network Science

Degree Distribution (Medium L) : Power Law with Cutoff



Some Model Network Topologies



(a) Star (b) Line (c) Circle (d) Triangular Hub (e) Pentagonal Hub (f) Perfect Hub

Future Directions

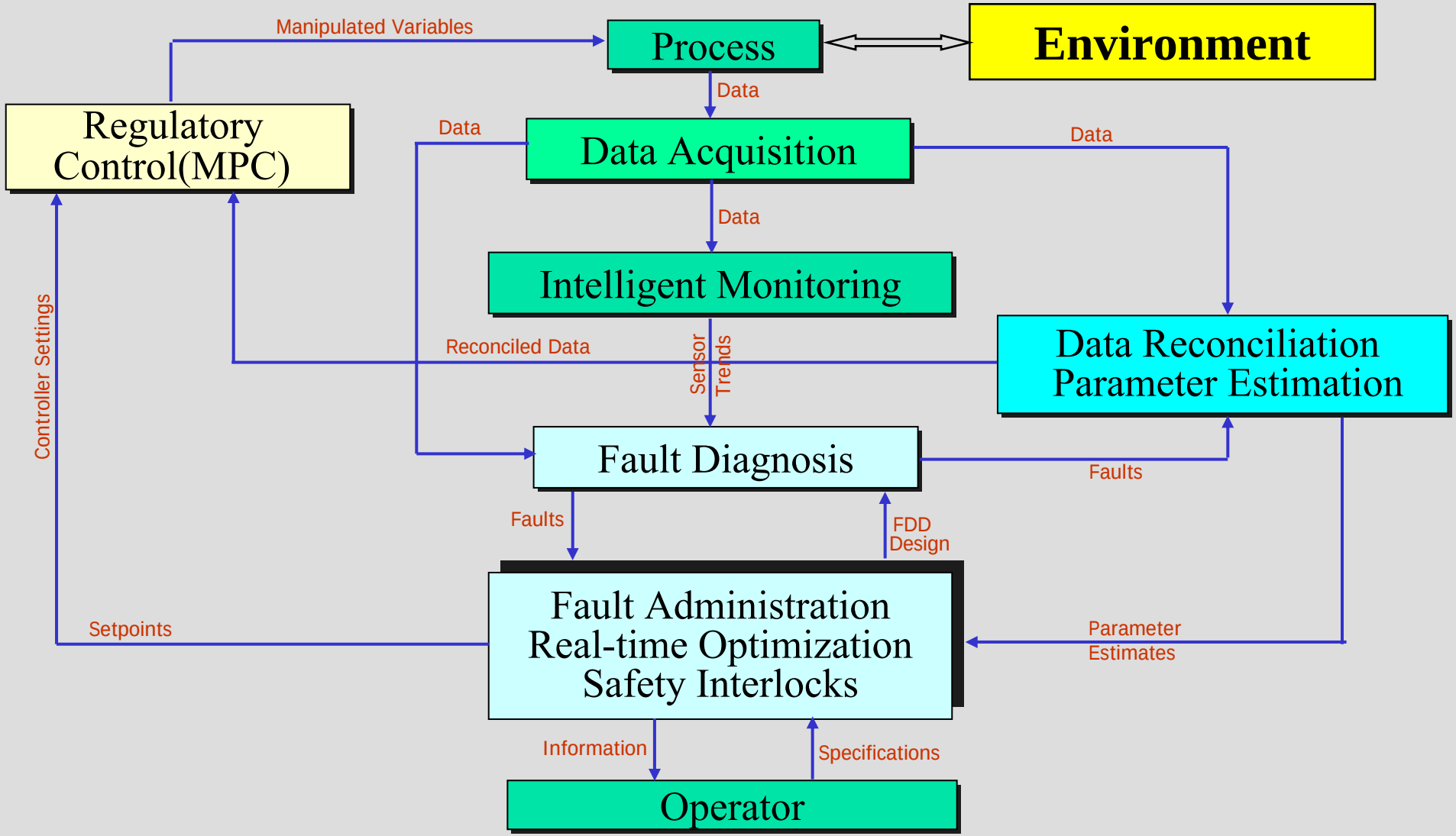
Prediction is Difficult, particularly about the Future.....

Niels Bohr

Future Directions in Resilient Systems

- Science of Complex Adaptive Systems
  - From `Parts to Whole´: Systems Biology
  - Predicting and controlling Emergent Behavior
- Hybrid Intelligent Control Systems
  - System development/implementation, knowledge maintenance/management
- AEM-PHA Integration
- Integration with other systems
- People/Organization Issues
  - Operator Acceptance, Training
  - Commitment, Liability

Resilient Control Design: One Vision



Summary

- Complexity of modern engineered systems make it difficult to predict and manage abnormal events (AEM)
- AEM has been identified as a very important problem by all industries
  - Next Control Frontier: Resilient Intelligent Control Systems
- Reviewed various conceptual issues
- Considerable challenges remain but we have made good progress in the last decade and the future potential is enormous and exciting
- Science of Complex Adaptive Systems: Challenges and Opportuntites

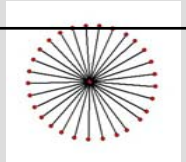
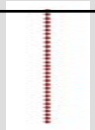
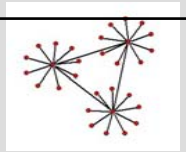
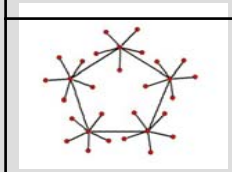
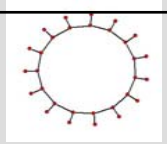
Acknowledgements

- Collaborators
  - Prof. Raghu Rengaswamy, Clarkson
  - Dr. Sourabh Dash, ExxonMobil
  - Dr. Mano Ram Maurya, UCSD
  - Past grad students and co-workers
- Funding Agencies
  - Honeywell ASM Consortium
  - Indiana 21st Century Science&Technology Fund
  - ExxonMobil, ICI, Air Products, Mitsubishi, A. D. Little, Searle, Eli Lilly, Nova Chemicals, IBM
  - NSF, NIOSH
  - Purdue Trask Fund

Thank You for Your Attention!

Any Questions?

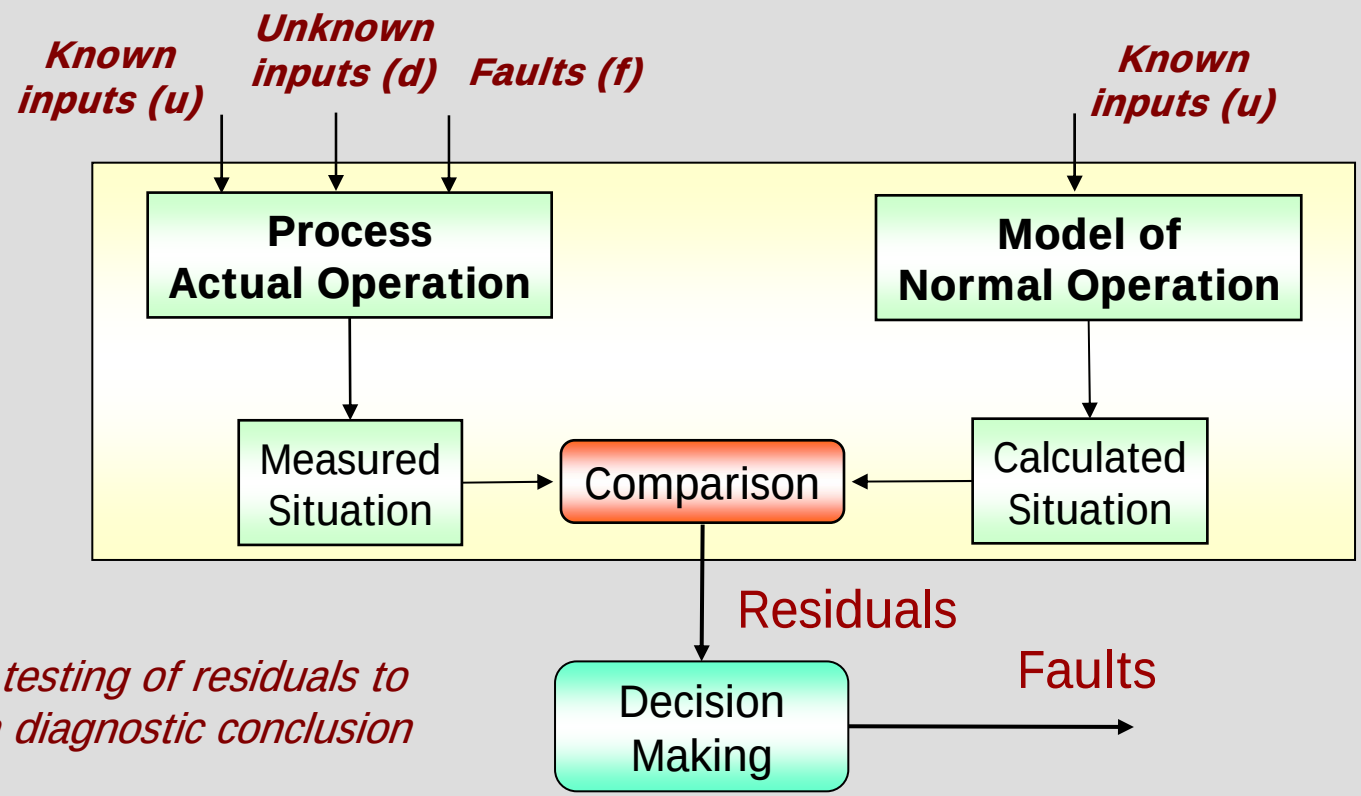
Results (cont.)

Structure	Effncy	Robustness		γ	<k>	Average Path Length
		Worst Case	Average Case			
 Star	1.00	0	0.97	-1.0	1.93	1.93
 Line	0.19	0.96	0.97	3.81	1.93	10.33
Circle	0.25	1.00	1.00	-	2.00	7.76
 Triangular-Hub	0.78	0.68	0.97	-0.92	2.00	2.49
 Pentagonal Hub	0.66	0.82	0.97	-0.83	2.00	2.91
 Perfect Hub	0.40	0.96	0.98	0	2.00	4.86

Model-based Diagnosis

Residual Generation

Unknown fault modes, uncertain nominal model, system/measurement noise



Residual Analysis

Statistical testing of residuals to arrive at a diagnostic conclusion

<u>Consistency Checking (Analytical Redundancy):</u> Compare actual behavior with a nominal fault-free model driven by same inputs, using *residuals.*

<u>Residuals:</u> Functions accentuated by faults representing this inconsistency

Diagnostic Approaches – Brief Review

- Process Fault Diagnosis: First Step in Intelligent Control
- Diagnostic Philosophies
  - Source of Process knowledge
    - Process Model
    - Process History
  - Form of Process knowledge
    - Qualitative
    - Quantitative
- Process Model : *Deep, Causal or Model-Based knowledge*
- Process History : *Shallow, Compiled, Evidential knowledge*

V. Venkatasubramanian, R. Rengaswamy, K. Yin and S. N. Kavuri, "Review of Process Fault Diagnosis - Part I, II and III", Computers and Chemical Engineering, 27(3), 293-346, 2003.

Issues in Model-Based Diagnosis

- Modeling uncertainty: Availability of a ‘decent’ model
  - Perfectly accurate/complete model of a physical system is rarely available
  - Uncertainty: Mismatch between actual process and its math model
  - Effect of modeling uncertainties is very crucial
- Sensitizing/Desensitizing & Robustness
  - Decoupling fault effects, system/measurement noise
  - Insensitive to modeling uncertainty, noise, disturbances with increased sensitivity to faults
- Online speed: Computations Vs Performance
- Theory
  - Well developed for linear systems, nonlinear systems’ still not mature

Qualitative Models

- Fault Trees
  - Qualitative cause-effect relationships represented as a tree
  - Fault Trees (Lapp & Powers, 1977)
    - Top-down, symptom-driven approach
    - Qualitative ambiguities
- Signed Digraphs and Causal Models
  - Qualitative cause-effect relationships as a directed graph with nodes and arcs
  - Bottom-up, cause-driven approach
  - Qualitative ambiguities
  - Single fault diagnosis (Iri et.al., 1979; Kramer and Palowitch, 1987;Wilcox and Himmelblau, 1994)
  - Multiple fault diagnosis (Morales and Garcia, 1990; Vedam and Venkatasubramanian, 1999)
- Abstraction Hierarchy

Qualitative Model Based

- **Merits**
  - Qualitative nature facilitates their development without exact model equations
  - Completeness: Enumerates all possible root causes
- **Demerits**
  - Need to develop and maintain SDG
  - Qualitative nature results in poor resolution
  - Number of spurious solutions

Process History Based Techniques

Process-History Data from normal/abnormal operation

- Quantitative Methods
  - Neural Networks : Easy learning & interpolation capabilities leading to numerous diagnostic applications (Venkatasubramanian et. al. 1989, 93, 94)
  - Statistical Techniques :
    - Univariate SPC based on limit-checking
    - Multivariate PCA/PLS based monitoring (MacGregor et. al., 1994)
- Qualitative Methods
  - Qualitative Trend Analysis : Sensor Trend Information
    - Trend Language, Trend Identification and Mapping to faults (Cheung & Stephanopoulos, 1990; Janusz & Venkatasubramanian, 1991; Rengaswamy & Venkatasubramanian, 1995)
  - Rule-Based Expert-Systems : Mapping of known symptoms to root causes (Kramer, 1987; Rich & Venkatasubramanian, 1987)
    - Process History enters the antecedent and consequent of rules
    - Lack of generality; Poor handling of novel situations

Quantitative Process History based

- Merits
  - NN: Can capture nonlinear correlation
  - PCA:Diagnosis is based on correlation among variables
    - Detect changes in correlations and robust to controller action

- Demerits
  - Quality and Quantity of training data
  - NN: Architecture of network, extrapolation,
    lack of transparency: black box
  - PCA: Interpretation of contribution plots may be difficult
    - Root cause information is needed to perform supervisory tasks