Trends and Prospective in Risk and Reliability Engineering Research

Mohammad Pourgol-Mohammad, Ph.D, PE
Senior Reliability Manager
Johnson Controls Inc.
York, PA
Associate Professor of Risk and Reliability
Sahand University of Technology
Tabriz-Iran

Invited Speech at
IEEE Reliability Section
MIT Lincoln Laboratory
Boston, Dec. 13, 2017
Outline

- Engineered Systems
- Failure and Complexity
- Failure and Damages
- Frontiers in:
  - Reliability Engineering
  - Risk Analysis
  - Prognosis and Health Management (PHM)
  - Resilience
Engineered Systems

Diagram showing the interplay between Hardware, Software, Human, and Environment over time.
Engineered Systems; Closer Look

Diagram showing the interaction of System, Organizational, Physical, Socioeconomic, and Regulatory Environments.
Defining the Subject of Analysis

Boundary

SYSTEM

UNIVERSE

Analysis Scope
Generalized Concept of Risk Scenario

Safety Boundary

\((x_o, r_o)\)
Conceptual Probabilistic Model of System Evolution

$$\begin{align*}
(x_0, r_0) & \quad \text{(Initial State)} \\
(x_t, r_t) & \quad \text{(Final State)}
\end{align*}$$

- High Probability
- Medium Probability
- Low Probability

Diagram: 3D representation of system evolution over time with probability levels depicted.
Anatomy of a Risk Scenario

A path from the initiating event to an end state is called a scenario.
Evolution of The Discipline

1. Complexity and Failures
2. Reliability Engineering
3. Life Cycle Risk Management
4. Prognostics Health Management
5. Resilience
Problem statement

Failures

Loss of revenues

- Unplanned shut-down, D.C. Cook NPP

Fatalities and contaminations

- Oil rig explosion in 2010, Gulf of Mexico
Problem statement

Failures

Prevented by

Design for Reliability

Maintenance

Redundancy | Training | Safety Reviews

No Hazard

Normal | Degraded | Failure

Hazard

Time
According to Network Rail (UK), rail infrastructure failures and defects are responsible for 14 million minutes of delay per year.

Delays in civilian aircraft industry cost 22 billion US $ in 2011.

Nuclear industry (France)

Maintenance (about 1.5 billions euros/year)
Where Do Failures Originate

Mature Nuclear Power Production Failures

- People: 38%
- Procedures + Processes: 34%
- Equipment: 28%

72% of all failures

10 Year ASME Boiler Test Code Equipment*

- 23,338 Accidents: 83% human oversight or lack of knowledge
- 720 injuries: 69% human oversight or lack of knowledge
- 127 deaths: 60% human oversight or lack of knowledge

Engineers--can you really reduce problems working only on the hardware?

Evolution of The Discipline

1. Complexity and failures
2. Reliability Engineering
3. Life Cycle Risk Management
4. Prognostics Health Management
5. Resilience Engineering
Reliability Engineering

- Determine *why* and *how* systems and processes fail
- Measure, track, and *predict* levels of reliability in various phases of system/process life cycle
- *Improve* system/process reliability by removing failure causes
- Provide *input to decision* makers on how to achieve the above objectives in an optimal way
Methods of Reliability Engineering

- Understanding why and how things fail
  - “science of failure”
  - Materials, Physics of Failure, Human Behavior
- Life Prediction - Statistical and Probabilistic Methods
- System Logic Modeling and Failure Path Identification
  - Fault Tree, Reliability Block Diagram, Event Sequence Diagrams
- Probabilistic Physics of Failure
- System/Process Multi-scale Probabilistic Simulation
Methods for Reliability Improvement

- Design for Reliability
  - Failure Mechanism Prevention
  - Redundancy and Functional Diversity
  - Fault Tolerance
- Reliability Growth
- Preventive Maintenance/RCM
- Health Monitoring
Key Areas of Research: Reliability

- Issues with the Traditional Field / Test Data
  - “One Size Fits All” concept! E.g., Constant Failure Rate
  - Reliability Estimates Rarely Match Reality

- Probabilistic Physics-of-Failure (PPoF)
  - More than 50-Years of History in PoF (More Recently PPoF)
  - Accelerated Reliability Testing for PPoF Model Development
  - Empirical Model for Unit-Specific Models of Reliability Assessment
  - Simulation-Based Reliability Assessment / Numerical Complexity
Key Areas of Research: Reliability

- **Hybrid Reliability**
  - Combined System Analysis Techniques: BBN, DBN, FT, ET, Markov and Semi-Markov, FEM and FDM, FM, RBD.

- **Sensor-Based (Precursors) / Big Data Reliability Analysis**
  - Data Fusion, Machine Learning (GRP, SVM,..)
  - Signal Processing, Detection Probability
  - Representative Sample-Based Approach
  - Massively Parallel Processing (MPP)

- **PHM of Cyber-Physical Complex Systems and Structures**

- **Science of Reliability Engineering**
Soft Causal Relations
Human, Organizational, and Regulatory Environment

Influence Diagram
Software Failure Modeling

Functional Decomposition

Requirement Analysis of TRAC-M Level Controller-Design

X(1) (m) Vessel Water Level
SVT 106

Cbcon1 (m): Water level set-point

X(2) (kg/sec) Current time step feed-water line mass flow rate (mtm)

X(3) (kg/sec) Current time step steam line mass flow rate (mtm)

Cbcon2 (kg/sec): nominal steady state feed-water line mass flow rate

Yout = f (X1, X2, X3, C1, C2)

Water Level
Int. Lev. Err
(Ki+Kp)term
m
m_y - m
Δm_w (dem)
Δm_w (act)
m

SUBTC
INT
WSUM
DEAD
LAG
ADD
Level Controller

©UQAM/ nkececl
Phenomenological and Logic Based Models

**Top Level Summary Event Tree**

- Boosters
- Main Stage
- Upper Stage
- Destruct System

<table>
<thead>
<tr>
<th>Missn. Success</th>
<th>LOM / no publ. impact</th>
<th>LOM / no publ. impact</th>
<th>LOM / mod. publ. impact</th>
<th>LOM / mod. publ. impact</th>
<th>LOM / serious. publ. impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

**Event Sequence Diagrams**

- Vehicle Malfnctn.
- Mission completed before malfunction becomes critical?
  - Yes
  - No
  - Loss of Mission
- Mission completion before malfunction becomes critical?
  - Yes
  - No
  - Loss of Mission

**Physical Models**

- Impact /Effects Density Distributions
- Population Center

**Health Effects / Casualty Expectation Models**

- Propellant Explosion
  - Inert or Explosive Debris
  - Toxic Plume

**Fault Trees**

- System Malfunction
  - t-1
  - t+1
  - Mean Wind Direction
  - Launch Site

- Impact /Effects Density Distributions
- Population Center

- Health Effects / Casualty Expectation Models
Evolution of The Thinking

1. Complexity and failures
2. Reliability Engineering
3. Life Cycle Risk Management
4. Prognostics Health Management
5. Resilience Engineering
Risk Analysis

- Determine potential *undesirable consequences* associated with use of systems and processes
- Identify *scenarios by which* such consequences could materialize
- Estimate the *likelihood* (e.g., probability) of the scenarios
- Provide *input to decision* makers on optimal strategies to reduce the levels of risk
Decision maker whether risk manager or communicator must be part of risk assessment
Applied to System Life Cycle

- Design
- Development
- Installation
- Operation
- Decommissioning
Probabilistic Risk Assessment in the Nuclear Power Industry

- 1975, Reactor Safety Study, WAHS-1400
  - Public health risk due to potential accidents in commercial nuclear power plants
  - First comprehensive, large scale probabilistic risk assessment (PRA) of a complex system
  - Established the core techniques of engineering systems PRA

- 1980-1988: Numerous full scope PRAs of commercial nuclear power plants performed by the industry

- 1994-2000 PRA-based IPEs of all NPPs

- 1998: Risk-informed regulatory approach embraced by NRC

- Long Term Waste Disposal (e.g., Total System Performance Assessment for Yucca Mountain Site, DOE)
NIST IT Security Risk Management Framework

- Boundaries/Scope
  - System Boundary
  - Analysis Boundary

- Analysis
  - Asset Valuation
  - Threats
  - Safeguards
  - Impacts
  - Vulnerabilities
  - Likelihood

- Measure of Risk

- Acceptance Test

- Actions/Change
  - Requirements
  - System
  - Environment

- Risk Assessment

- Uncertainty
NASA Risk Management Perspective

NASA RM Process Terms
(NPG8705.x, Dec. 2000)

IDENTIFY
Identify risk issues and concerns

ANALYZE
Evaluate (impact/severity, probability, time frame), classify, and prioritize risks

PLAN
Decide what, if anything, should be done about risks

TRACK
Monitor risk metrics and verify/validate mitigation actions

CONTROL
Replan mitigations, close risks, invoke contingency plans, or track risks

NASA Risk Element Terms

Mission Risk

Technical Risk

Trade-off

Programmatic Risk

Safety

Performance

Other

Cost

Schedule

Other
Key Areas of Research: Risk Frontiers

- Infrastructure Safety-Security-Resilience (SSR)
  - Electronic Information Flow Embedded in Nearly Every Aspect of Modern Life
  - Integrity of Complex Systems and Networks: Cyber-Human-Software-
- Physical Systems
  - Highly Connected Infrastructure Networks: Electricity, Gas, and Water
- Pose Major Societal Risks Through Cyberspace Attacks
  - Risk Management and Resilience
  - Societal Disruption, Health, Safety and Resilience Goals
Key Areas of Research: Risk Frontiers-Cont.

- Life-Cycle Risks of Advanced Energy Systems
  - Renewable Systems (Building, Environmental, Internal and External)
  - Nuclear Energy (Fission and Fusion)
  - Climate Change Risks of Disruptions in Sustained Energy Supply
- Health System Risks
- Simulation-Based Dynamic Probabilistic Risk Assessment
  - High Power Computing Leading to Less Inductive Risk Models
  - More Deductive Computer-Assisted Risk Scenario Generation
Understanding the Limitations
Aviation Accident Rates

1970-2005
Number of fatal accidents/ million departures

35 years of technology improvements, only a factor of 10 decrease in risk
Calculated vs. Real: the case of CCF

\[ Q_S = Q_A + Q_B + Q_C \]

\[ Q_S = Q_A + (Q_B)^2 + Q_C \]

\[ Q_S = Q_A + [(1-\beta)(Q_B)]^2 + \beta Q_B + Q_C \]
Numbers Move Faster Than Reality
Selection of a System Solely Based on its Reliability Can Be Miss-Leading,

Even If All Components In The System Are Characterized By Constant Failure Rates

Are Arranged In Series.

\[
\overline{L}_1 = f_{A1}C_{A1} + f_{B1}C_{B1} = 1 \times 2000 + 9 \times 100 = 2900
\]

\[
\overline{L}_2 = f_{A2}C_{A2} + f_{B2}C_{B2} = 3 \times 2000 + 2 \times 100 = 6200
\]
\[ PV = \frac{1}{(1 + r)^k} \]

\( r = \text{Interest rate} \)

\( k = \text{Operation Duration in Years} \)

discount rate \( r = 7.5\% \), \( k1 = 25 \) and \( k2 = 2 \), yields

\[ \frac{PV_2}{PV_1} = \frac{(1 + r)^{k1}}{(1 + r)^{k2}} \approx 5.28 \]

➢ OUR Proposal is Risk-Based Design for Reliability
➢ Corporate better understands the values on the reliability improvement
Challenges

- Believability of results
  - Model vs. reality
  - Quality of analysis (Numbers that do not correlate with reality)
- Overly simplistic methods for complex problems
  - and the opposite...
- Legacy methods that have outlived their usefulness
  - FMEA – unraveling complexity
  - Weibull – answer to all questions
- Statistical angle of reliability
Evolution of The Thinking

1. Failures and Complexity
2. Reliability Engineering
3. Life Cycle Risk Management
4. Prognostics Health Management
5. Resilience Engineering
Enablers

- Rapid advancements in
  - Sensor technologies
  - Information processing capabilities
  - Data Fusion & Inference methods
  - PHM of Cyber-Physical Complex Systems and Structures

Challenges include

- Science Based or Empirical Degradation Models for Various Failure Mechanisms
  - Failure Mechanisms Interactions
- System-Level PHM
- X-ware Complexity Issues
Enablers

- Rapid advancements in
  - Sensor technologies
  - Information processing capabilities
  - Data Fusion & Inference methods

Challenges include

- Science Based or Empirical Degradation Models for Various Failure Mechanisms
  - Failure Mechanisms Interactions
- System-Level PHM
- X-ware Complexity Issues
Compact and seamless integration of the data model and System model
BBN Based Online Health Monitoring

State (Presence of gas in oil)

<table>
<thead>
<tr>
<th>Presence of Gas in Oil</th>
<th>Prob. of Oil Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>%5.08</td>
</tr>
<tr>
<td>0</td>
<td>%0.07</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Presence of Gas in Oil</th>
<th>Prob. of System Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>%3.16</td>
</tr>
<tr>
<td>0</td>
<td>%2.66</td>
</tr>
</tbody>
</table>

Dynamic Bayesian Network
Dynamic Health / Integrity Management System

Sand Monitoring
Acoustic Signal

External Corrosion
Ambient Temperature
Soil Resistivity

Leakage
Pressure

Internal Corrosion
Temperature
Hydrogen
Sulfide
Concentration
Fatigue Damage Characterization Based of Thermodynamic Entropy

- Diminishing the strength until failure [J. Lemaitre and J. Dufailly, 1987]

- Engineering context:

  External work
  (mechanical, thermal, electrical, chemical or their combinations)

  • gradual alteration of matter
  • dissipation of energy.

- The definition of damage varies at different geometric scales:

  Fatigue Mechanism

  Nanoscale: the configuration of the atomic bonds
  Microscale: the accumulation of the slip bands
  Mesoscale: the growth and coalescence of microcracks
  Macroscale: the growth of macrocracks

  The definition of damage is relative to a reference state:

  Fatigue Mechanism

  reduction in the Young’s modulus
  load-carrying
  crack length …
Thermodynamic Damage

- Thermodynamically, all damage mechanisms share a common feature, which is dissipation of energy.

\[ \text{Damage} \equiv \text{Dissipation (entropy generation)} \]

\[ d_i S = \dot{\gamma} = X_i J_i, \quad i = 1, 2, \ldots, n \]

- \( d_e S \): entropy exchange (flow) with the surroundings
- \( d_i S \): the entropy generation inside the system
- \( X_i \): Generalized thermodynamic forces
- \( J_i \): Thermodynamic fluxes
- \( i \): the number of different processes acting on the system.
Advantages

- Commonly Mechanical Element of entropy generation dominate the total entropy generation.
- The entropy generation can be explicitly expressed in terms of physically measureable quantities.
- Thermodynamics allows for quantifying every dissipative process in the system that gives rise to the entropy generation, irrespective of the underlying degradation phenomena.
- For reliability study, entropy approach includes all degrading mechanisms when multiple competing and common cause failure mechanisms are involved,
  - a damage parameter for diagnosis and prognostics is more favorable in comparison with the PoF models
Fatigue Damage

\[ \dot{\gamma} = \frac{1}{T} \left( \boldsymbol{\sigma} : \dot{\varepsilon}_p - A_k V_k - Y \dot{D} - \frac{\mathbf{q}}{T} \cdot \nabla T \right) \geq 0 \]

- \( \boldsymbol{\sigma} \) the stress
- \( \varepsilon_p \) the plastic strain rate
- \( T \) the temperature
- \( V_k \) internal variable
- \( A_k \) the thermodynamic force associated with an internal variable
- \( \mathbf{q} \) the heat flux
- \( Y \) the elastic energy release rate
- \( D \) the damage

- **Heat Equation**

\[ \rho C T \dot{T} - k \nabla^2 T = \dot{W}_p \]

- \( \rho \) density
- \( C \) the specific heat
- \( k \) the thermal conductivity
- \( \dot{W}_p \) plastic work
Evolution of The Thinking

1. Failures and Complexity
2. Reliability Engineering
3. Life Cycle Risk Management
4. Prognostics Health Management
5. Resilience Engineering
Resilience

The resilience integrates robustness, resourcefulness and recovery for system adaptation with all undesired conditions.

- **Robustness**: the ability of a system to withstand extreme weather events as well as gradual changes (e.g. sea level rise) and continue operating.

- **Resourcefulness**: the ability to effectively manage operations during extreme weather events.

- **Recovery**: the ability to restore operations to desired performance levels following a disruption.

- **Adaptation** of an energy system to climate change refers to the process of adjustment of all components of the energy system to actual or expected climate and its effects.
The ultimate safeguard is to make systems resilient by design.

Resilient systems would have inherent abilities to:
- adapt to changing environment,
- tolerate emergent failure mechanisms,
- self-recover.
There are several quantitative and qualitative approaches for the resilience analysis.

The quantitative methods include probabilistic resilience analysis.

- **S**: system with $n$ components,
- the probabilistic resilience $\text{res}_{pr}(S; \beta)$: largest number of component failures
- such that $S$ is still *up* with the probability $1 - \beta$, that is

$$\text{res}_{pr}(S; \beta) = \max\{I : \sum_{i=1}^{I} P(S, i) \leq \beta\}$$
Pathway to Resilience

1. Materials
2. Mechanical and Electrical Function Delivery
3. Sensing, Monitoring, and Control
4. Software
5. Human (operators, maintainers, users, decision-makers)
Shape Memory Alloys (SMAs)

- Metals that "remember" their original shapes.
- Nickel-titanium alloys one of the most useful SMAs
  - Applications: military, medical, safety, and robotics
    - Surgical Tweezers
    - Orthodontic wires
    - Eyeglass frames
    - Guide for catheters
“Self-Healing Plastic”

- Human Skin:
  - Flexible
  - Sensitive to stimuli: touch & pressure,
  - Conducts electricity
  - Survives wear & Tear: self-healing

- Composite material composed of an organic polymer with embedded nickel nanostructured microparticles, which shows mechanical and electrical self-healing properties at ambient conditions.

* Benjamin C-K. Tee, Chao Wang, Ranulfo Allen & Zhenan Bao Nature Nanotechnology 7, Published online 11 November 2012
Software Functionality

- Easier to achieve
  - Functional Linkages are soft, can be rerouted or reconfigured

- Fault Tolerance is well established

- “Safe mode”
Mechanical and Electrical Functionality

- Most difficult
  - Hard functional coupling (in contrast to software)
  - Need New design paradigms
  - Solution is closely tied to materials issues
Mechanical and Electrical Functionality

- Achievable first steps at system level
  - Design to migrate to different states for different environments
    - Multiple anticipated states
    - Detect and deflects (seen in some resilient networks)
  - Function in degraded state
    - “Safe mode” for essential function in response to unanticipated events
    - “Sleep mode” while recovery is in progress

- 3-D printing of failed parts?
Thank You