Provocative Talk:

Affordable, Adaptable and Effective: The Case for Engineered Resilient Systems

Dr. Azad M. Madni

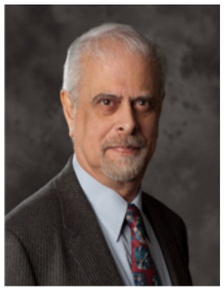
Professor, Viterbi School of Engineering
Director, Systems Architecting & Engineering Program
Co-Director, Center for Systems and Software Engineering
Professor, Keck School of Medicine and Rossier School of Education

Engineering Resilient Systems Workshop
Keck Institute for Space Studies
California Institute of Technology, Pasadena, CA

USC Viterbi School of Engineering

July 30- August 3, 2012

Azad M. Madni Biosketch



- Director, Systems Architecting and Engineering Program
- Co-Director, Center for Systems and Software Engineering
- Professor, Viterbi School of Engineering, Keck School of Medicine, Rossier School of Education, University of Southern California
- Founder and CEO, Intelligent Systems Technology, Inc.
- Life Fellow, IEEE & IETE; Fellow, AIAA; Fellow, INCOSE; Fellow, SDPS
- Ph.D., M.S., B.S. in Engineering from University of California, Los Angeles
- 2011 INCOSE Pioneer Award
- 2012 INCOSE-LA Exceptional Achievement Award
- 2008 President Award and 2006 C.V. Ramamoorthy Distinguished Scholar Award from SDPS
- 2004 and 2000 Developer of the Year Award from Software Council of Southern California
- 2004 DARPA IPTO Sustained Excellence by a Performer and Significant Technical Achievement Awards
- 2000 Blue Chip Enterprise Award from Mass Mutual & US Chamber of Commerce
- 1999 SBA's National Tibbetts Award for California
- Past President of Society for Design and Process Science
- **Research Interests: model-based engineering, engineered resilient systems, cyber physical systems, educational games, STEM education, big data analytics**

USC Viterbi School of Engineering

Overview

- Motivation
- Resilience in Different Domains
- Resilience Engineering Challenges
- Engineering Ecosystem Vision
- Closed Loop Concept Engineering
- Strategic Research Directions
- Desired Outcomes
- References

Motivation

- Need to overcome:
  - drawbacks of current engineering practices
  - challenges of 21st century
- Drawbacks
  - linear, sequential, and slow (time-inefficient)
  - unnecessary rework and extraneous iterations (cost-inefficient)
  - premature elimination of alternatives (potential loss of competitive advantage)
  - information loss at every step (lack of traceability and inadequate design rationale)
  - inability to keep track of and manage risks
- Challenges
  - pace of technology advances
  - increasing scale and complexity of systems
  - uncertain sociopolitical futures
  - technology commoditization (technology widely available to global competitors)

Resilient systems engineering: a means to develop **affordably adaptable** and **effective** systems for **a range of operations** and **across multiple alternative futures**

USC Viterbi School of Engineering

Resilience: An Evolving Concept

- Ability of a system to **adjust its functioning** prior to, during, or following changes and disturbances, so that it can **sustain required operations,** even **after a major mishap** or in the **presence of continuous stress** (Nemeth et al, 2009)
- Ability of a system to offer **broad utility** in a **wide range of operations** across many **potential alternative futures** despite experiencing disruptions (Neches & Madni, 2012)
- Ability of a system to **return to its original state** or **move to a new, more desirable state** after being disturbed (Christopher & Peck, 2004)
- Ability of a of a system to achieve envisioned (science) objectives even if the system (spacecraft**) performance, health, and/or environment** are **not as expected** (Murray, Ingham, Day, & Williams, 2012)

USC Viterbi
School of Engineering

Resilience

Ability of a system to **circumvent, survive, and recover from failures** to ultimately achieve mission objectives. A resilient system is able to **reason about own/environmental states** in the presence of environmental uncertainty

USC Viterbi School of Engineering

Definitions Illuminate Various Characteristics of Resilience

- Adaptability (anticipation, responding, learning)
- Adaptive capacity
- Range of operational missions
- Variety of adverse conditions (unexpected/unforeseen)
- Range of possible futures
- Reaction (short-term) and adaptation (long-term)
- Graceful degradation outside operational performance envelope
- Environmental uncertainty
- Reasoning about own/environmental states
- Recovering fully/partially from disruption
- Real-time trade-offs
- Achievement of end objectives
- Learning from experience (successes, failures)

Resilience in Nature (Rapid Recovery)

The bamboo that bends is stronger than the oak that resists.

-- Japanese Proverb

USC Viterbi School of Engineering

Resilience in Nature (Adaptation)

http://www.thisisourstory.net/2010/02/resilience/

Resilience in Networked Systems

- Resilience is an important property of networked systems
  - e.g., mobile ad-hoc networks, sensor networks, energy grids
- Large body of research in **compromise-resilient** systems
  - as opposed to failure-resilient systems
- In sensor networks, resilience is measured in terms of:
  - number of nodes that must be captured/compromised by an adversary before entire network is compromised
- In mobile ad hoc networks (e.g., UAV system or mobile vehicular networks), mobile nodes act not only as sources and sinks of information but also as relay to router nodes;
  - so, compromising a certain number of nodes beyond a threshold can result in total disruption of the entire network routing regime
- Can also study **resilience in the context of security/survivability**

USC Viterbi School of Engineering

Resilience in Space Platforms

- Ability of spacecraft to achieve envisioned (science) objectives of space missions in the face of unexpected/unforeseen operational environment and off-nominal spacecraft performance
- Requires that spacecraft has **the ability to reason about its own & environmental states** in the face of **environmental uncertainty**, and **recover from failures**

USC Viterbi School of Engineering

Resilience in Energy Grids

- To deal with power outages and adapt power distribution based on demand
  - goal of self-monitoring and self-healing
  - electronically diagnosing problems & rerouting power around them
  - merge energy grid with Internet so we can adjust our appliances with our iPhones when away from our homes
  - program our appliances so we can save energy
- Move from few large centralized plants to large network of distributed power plants
  - prevent disasters (e.g., recent Japan disaster)
  - acknowledge trend for increasing energy
  - overlapping microgrids to re-stabilize system after one goes down
  - communication and coordination are keys to a resilient network

Resilience in Health Care

- Resilience in health care (service sector)
  - how well sector responds to changes in output demand over time
  - demand for care varies widely in volume and type
  - resources needed to respond to demand tend to be limited and constrained in various ways (e.g., civilians, beds, machines, time)
- Resilience strategies vary with type of demand
  - temporary patient surge….add temporary resources
  - extended patient surge…extend work shifts, work double shifts
  - sustained patient surge (trend)…expand facility, recruit staff
- Making electronic medical records resilient is an important area
  - interoperability of patient data and portability of medical records

Resilience Engineering

- A proactive, risk-mitigated approach to building adaptability into systems that are complex, underspecified, and with multiple interdependent elements

- Resilience engineering is concerned with building systems that are able to circumvent accidents through anticipation, survive disruption through recovery, and grow through adaptation (Madni & Jackson, 2008)

USC Viterbi School of Engineering

Resilience Engineering Challenges

- Calculating Leading Indicators
  - key to assessing consequence of risky decisions and controlling risks
- Conducting the right trade-offs in timely fashion
  - key to maintaining safety margins and control/avoidance of drift
- Developing an accurate model of drift
  - key to understanding risk factors and effective risk management
- Developing realizable resilience heuristics
  - key to informing and guiding resilient system design
- Developing appropriate resilience metrics
  - key to evaluating candidate resilience strategies

Toward a New Engineering Ecosystem

- Build on industry trends in **model-based engineering**
- Closed loop **concept engineering** with active stakeholder participation
- Automated tools and **decision aids** (analysis, evaluation, data collection)
- **Exploration** of mission scenario space to uncover “surprises”
- **Rapid insertion and evaluation** of key technologies/concepts that enable resilience
- **Resilience methods** to successfully counter surprises
- **Resilience heuristics** to inform and guide system design
- Continual **cross-feed of multiple data types** by stakeholders to each other to inform their respective activities

Key Technology Concepts

- Co-evolution of systems, missions, and ConOps
  - information sharing and decision aiding
- Rapid trade space exploration
  - alternatives kept longer, explored deeper
  - enhances ability to exploit new technologies and adapt to new circumstances
- Closed loop concept engineering
  - analyze/evaluate system concepts/designs wrt life cycle concerns
  - continually inform requirements and CONOPS (operational mission context)
- Accelerated Design and Testing
  - rapidly composable modeling and analysis tools
  - risk-sensitive engineering planning aids
  - model-based T & E

Need new Methods, Processes, and Tools to help engineers & users understand interactions, identify implications, and manage consequences

USC Viterbi School of Engineering

Closed Loop Concept Engineering

- Co-evolution of system, mission & ConOps (stakeholder participation)
  - possible because of increased computational power and availability
  - greater flexibility in exploiting data and applying services
- Affords opportunity to evaluate and iterate on capabilities
  - in light of mission utility
  - avoids premature lock into requirements and key performance parameters
- Basis for developing trust in ConOps and architectural design
  - what-if exploration of capabilities with stakeholders in the loop

USC Viterbi School of Engineering

Exemplar Resilience Heuristics
(Madni & Jackson, 2008)

- Functional Redundancy
  - alternative ways to perform a function without physical redundancy
- Drift Detection & Correction
  - monitor & correct drift toward brittleness through corrective action
- Graceful Degradation
  - self-aware gradual performance degradation in the face of unanticipated/unexpected events
- Learning & Adaptation
  - ongoing knowledge acquisition from environment to reconfigure, re-optimize, and grow

Strategic Research Directions
(Neches & Madni, 2012; Madni, 2012)

- System Representation and Modeling
- Characterizing Changing Operational Environments
- Cross-Domain Coupling
- Trade-Space Analysis
- Collaborative Design and Decision Support
- Quantitative Assessment of Technologies
- Resilience Games

USC Viterbi School of Engineering

System Representation and Modeling

- Representation of multiple perspectives
  - physical and logical structures, and system behaviors
  - interactions with environment & interoperability with other systems/SoSs
- Multiple classes and types of models
  - classes: executable, depictional, statistical, non-parametric
  - types: device/environmental physics, comm, sensors, effectors, sw, systems
- New models need to be developed & made interoperable
  - rate at which they can be developed and validated is a key issue
- Models & simulations of live and virtual elements can fill gaps
  - cross-integration of physics-based and statistical models
  - integration of multidisciplinary, multi-scale physics models
  - automated/semi-automated techniques for model acquisition
  - techniques and tools to build adaptable models

USC Viterbi
School of Engineering

Characterizing Changing Operational Environments

- Complement system models with models of dynamic operational environments (drive system behavior)
  - to develop deeper understanding
- Gather and model operational data
  - to experiment with alternative designs and understand impact
- Go beyond how design and test are conducted today
  - e.g., achieve desired performance under specific conditions
  - optimizing in this fashion leads to brittle systems
- Need to understand a range of “likely” conditions
  - requires modeling of ConOps, environment, operational context
- Need:
  - **instrumentation** (collect data from live/virtual env., system tests)
  - **synthetic environments** for experimentation and learning

USC Viterbi
School of Engineering

Cross-Domain Coupling

- Many models that exist are not interoperable
  - model complex system across multiple domains & environments
  - example domains: materials, fluids, physics, chemistry
- Need new computing technologies and standards
  - models differ in type, detail, coverage, representation, data reqs
- Key challenges are:
  - achieving superior interchange between incommensurate models
  - resolving temporal, multiscale, multiphysics integration mismatches
- Promising solution approaches (examples)
  - creating libraries with reusable content
  - accelerating workflow definition and conversion between models
  - on-demand composition of modeling and analysis workflows
  - consistency maintenance across hybrid models (data abstraction)

USC Viterbi School of Engineering

Trade-Space Analysis

- Enhanced trade-space analysis enabled by computing advances
  - generate a larger number of options
  - explore them in greater depth
  - keep them open longer
  - manage added complexity
  - test more extensively
- Need to:
  - automate exploration of multiple conditions
  - generate and test more alternative solutions
  - analyze results and rapidly deliver findings to decision makers
  - assist decision makers in exploring most important options

USC Viterbi School of Engineering

Collaborative Design & Decision Support

- Ultimately, all technological advances lead to people
- Advances needed in:
  - collaboration technologies
  - information abstraction and summarization
  - multimedia presentation and visualization
  - human-computer interaction
- Need specific advances in:
  - usable multidimensional trade spaces
  - rationale capture
  - tradeoffs prioritization aids
  - explainable decisions
  - physics-based and behavioral models
  - information push-pull w/o exceeding cognitive limitations

Quantitative Assessment of Technologies

- Models to examine total performance and potential payoff of resilience technologies
- Tools to assess real benefits of resilience technologies and provide quantitative basis for strategic research decisions
- Methods to increase confidence that the technology trade space has been sufficiently explored, circumscribed and populated
- Techniques to visualize and interact with multidimensional trade spaces to assess sensitivities and draw implications
- Techniques to assess the sensitivities of design alternatives to changes in design parameters, requirements, and technologies
- Modeling and analysis capabilities to assess technology trade space and enhance understanding of the magnitude of impact on desired capabilities based on design tradeoffs

USC Viterbi School of Engineering

Educational Games to Teach Resilience Concepts

- Resilience continues to be an evolving concept
- Each definition introduces a unique perspective on resilience
- People frequently confuse resilience with other quality attributes of systems
- An effective way to teach resilience concepts is within the framework of educational games
- Examples of concepts that can be taught through games are: adaptability, functional redundancy, and dynamic tradeoffs
- Concepts learned this way will persist in the sense that games with an underlying storyline tend to be memorable and can facilitate recall of the underlying concepts

USC Viterbi School of Engineering

Castle Wall: Example Resilience Game
(Spraragen & Madni, 2012)

- **Storyline**: Invading army on horseback equipped with catapults seeking ingress into castle (medieval backdrop)
- **Learning Objective**: Understand number of invaders denied ingress and be able to perform key tradeoffs in building a resilient wall
- **Player Objective**: Prevent invaders from getting into castle by building a brick and mortar wall
- **Invader Tactic**: Catapult shots and horseback sorties
- **Wall Design Problem**: Choose stone, design a rectangular brick, then a pattern of bricks and mortar
- **Design Parameters**: Brick size, brick weight, and distance brick has to be carried
- **Design Tradeoffs**: Brick size vs. portability; brick size vs. vulnerability
- **Key Resilience Concepts**: Dynamic tradeoffs, absorption of disruption, recovery from disruption
- **Key Metrics**: Speed of wall repair; number of invaders denied ingress into castle

USC Viterbi School of Engineering

Desired Outcomes / Envisioned End State

- Enhanced Capability Engineering
  - context-sensitive (environment, mission)
  - expanded option set (more alternatives developed, evaluated, maintained)
  - superior trade-offs analysis & management (interactions, choices, outcomes)
- Effective Systems
  - easy to adjust, adapt, reconfigure, replace (mission context)
  - graceful function degradation with high confidence
  - superior performance and mission effectiveness in face of contingencies
- Accelerated Engineering Processes
  - fewer rework cycles
  - faster cycle times
  - timely management of requirements shifts

USC Viterbi
School of Engineering

Recommendations

- Need to transform the engineering of complex systems
  - to make systems affordable, effective, and adaptable (i.e., resilient)
  - to control costs, make schedules, and proactively manage risks
- Resilient systems need to provide utility
  - in a wide range of missions/operations
  - across many potential alternative futures
- Closed loop concept engineering is key to enhancing trust in architectural design and system ConOps
- Need strategic research advances on several fronts
  - system representation and modeling
  - characterizing changing operational environments
  - cross-domain coupling
  - trade-space analysis
  - collaborative design and decision support

USC Viterbi School of Engineering

References

- Neches, R. and Madni, A.M. “Towards Affordably Adaptable and Effective Systems,” to appear in INCOSE Journal *Systems Engineering*, Vol. 15, No. 1, 2012.
- Madni, A.M., and Jackson, S. “Towards a Conceptual Framework for Resilience Engineering,” *IEEE Systems Journal, Special issue on Resilience Engineering*, Paper No. 132, 2008.
- Madni A.M. “Adaptable Platform-Based Engineering: Key Enablers and Outlook for the Future,” INCOSE Journal *Systems Engineering*, Volume 15, Number 1, 2012.
- Madni, A.M. “Elegant Systems Design: Creative Fusion of Simplicity and Power, INCOSE Journal *Systems Engineering*, Vol. 15, No. 3, 2012.
- Christopher, M. & Peck, H. Building the Resilient Supply Chain, The International Journal of Logistics Management, Vol. 15, Iss:2, pp1-14

USC Viterbi School of Engineering

Suggested Reading

- Coutu, D. *How resiliency works*. Harvard Business Review, Vol. 80(5):46-55, 2002
- Deevy, E. *Creating the resilient organization*, Englewood Cliffs, NJ: Prentice Hall, 1995
- Hamel, G., & Vilikangas, L. *The quest for resiliency*. Harvard Business Review, Vol. 81(9), 2003
- Sheffi, Y*. The resilient enterprise: Overcoming vulnerability for competitive advantage*. Boston:MIT Press, 2005
- Weick, K. & Sutcliffe, K.M*. Managing the unexpected: Resilient performance in an age of uncertainty*. San Francisco: Jossey-Bass, 2007
- Westrum, R. A typology of resilient situations, Resilience Engineering: Concepts and Precepts, E. Hollnagel, D.D. Woods, and Leveson, N. (eds),Ashgate, Aldershot, UK, 2006

USC Viterbi
School of Engineering

Thank You