

SANDIA REPORT

SAND2003-2138
Unlimited Release
Printed June 2003

Workshop on Concepts for Self-Healing Critical Infrastructures

S. Y. Goldsmith

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.



Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: <http://www.doe.gov/bridge>

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: <http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online>



SAND 2003-2138

Unlimited Release

Printed June 2003

Workshop on Concepts for Self-Healing Critical Infrastructures

Steven Y. Goldsmith

Sandia National Laboratories

P. O. Box 5800

Albuquerque, NM 87185-0455

and

Infrastructure & Information Systems Division Massachusetts Institute of Technology

Engineering Systems Division

Abstract

This report describes a workshop on self-healing infrastructures conducted jointly by Sandia National Laboratories, Infrastructure & Information Division, and the Massachusetts Institute of Technology, Engineering Systems Division. The workshop was held in summer, 2002 and funded under Laboratory-Directed Research and Development (LDRD) #51540. The purpose of the workshop was to obtain a working definition of a self-healing infrastructure, explore concepts for self-healing infrastructures systems, and to propose engineering studies that would lay the foundation for the realization of such systems. The workshop produced a number of useful working documents that clarified the concept of self-healing applied to large-scale system-of-systems exemplified by the US National Critical Infrastructure. The workshop eventually resulted in a joint proposal to the National Science Foundation and a continuing collaboration on intelligent agent based approaches to coordination of infrastructure systems in a self-healing regime.

Contents

Acknowledgements.....	4
1 Introduction.....	5
2 Concepts of Self-healing Infrastructure	5
2.1 Autonomic Infrastructures	5
2.2 Introspection & Intercession in Self-healing Infrastructures.....	7
3 Models of Critical Infrastructures	15
3.1 Modeling, Monitoring, and Coordinating Critical Infrastructures.....	15
3.2 A Survey of Infrastructure Modeling and Simulation	19
4 MIT/SNL Workshop on Self-healing Infrastructures	22
4.1 Workshop Prospectus.....	22
4.2 Self-Healing Infrastructures: MIT Final Report on the Workshop.....	22
4.3 Workshop Announcement	25
4.4 Workshop Contact List	28
Appendix A: Self Healing Infrastructure Proposal	31
Appendix B: Self-Healing Infrastructures Initiative First Draft of Slide Proposal	
MIT Version 9/17/02	44

Acknowledgements

This project was conducted by three teams working closely together. The Sandia core team consisted of Sam Varnado, Reynold Tamashiro, Ben Cook, Steven Goldsmith, Dianne Barton, John Ganter, and Rick Craft. The MIT team members were George Apostolakis, Fred Mohavenzadeh, John Carroll, Nazli Choucri, Stephen R. Connors, Tina Ghosh, Chris Magee, David Marks, Stella Maris Oggianu, and Brian Zuckerman. Additional team members from Sandia contributed to the workshop and are listed in Section 5.

1 Introduction

The Workshop on Self-Healing Infrastructures was an effort conducted over the summer of 2002 to identify and clarify the very concept and to explore opportunities for collaboration between Sandia and MIT's Engineering Systems Division. Technical discussions and planning sessions were held throughout the summer by both the individual Sandia and MIT teams and in joint teleconferences. The actual workshop proper was held on August 20 and 21 in Albuquerque, NM. The workshop project produced four outputs: 1) a better understanding of the concept of self-healing applied to critical infrastructures captured in a report and in slide presentations; 2) a foundation for collaboration between Sandia and MIT's Engineering Systems Division; 3) a joint proposal developed in subsequent sessions held at MIT in October 2002; and 4) a second joint proposal for agent-based coordination of infrastructure elements developed by a spin-off of the main group. The activity was very broad in scope, considering engineering, information, policy and political issues in a holistic forum. Experts from Sandia and MIT engaged in mutually informative discussions on a wide range of scenarios involving natural and deliberate attacks on US Critical Infrastructures.

The report is organized as follows. Chapter 2 includes notes on the concept of self-healing infrastructures. Chapter 3 provides some material on models of self-healing infrastructures. Chapter 4 describes the workshop format and participants, and includes a final report from the MIT team. Some slide presentations are included in Appendix A. A.1 is a presentation made to the Singapore DSO to determine their interest in participating in the project (they subsequently declined). A.2 workshop-derived presentation that summarizes the ideas developed during the discussions.

2 Concepts of Self-Healing Infrastructures

2.1 Some Aspects Of Self-Healing Infrastructures

The term "self-healing" is troublesome. So is the "infrastructure" term to a lesser degree. The former conjurs up images of biological healing, i.e. tissue regeneration in response to a wound or other insult to the body. The latter is very general, denoting the large-scale technological systems we encounter but ignore as commonplace in everyday life that allow us to survive and function in society. Its hard to imagine these engineered systems regenerating their components on the spot in a material or physical sense in response to faults or deliberate damage. It might be easier to envision a broken system ordering a new part from some JIT factory, perhaps arranging for its transportation and scheduling its installation automatically. People in organizations do this job now. Computers help them. Its called systems management and supply chain management.

We can include humans in the definition of the supreme system but then what does "self" refer to if not the engineered system distinct from its human creators and operators? Don't we include humans in our existing socio-technological systems anyway? What is new and novel? Intuitively are we suggesting tighter integration and more reliable operations? Do we mean a system coordinated on a larger scale? Do we mean responding to a wider range of circumstances? Don't we assume some regulation occurs that maintains invariant properties such as levels of services and energy and material flows? It seems we might mean all of these things. Most importantly we mean humans and technical systems closely integrated and situated in a larger organizational context that includes policy and political considerations, local, state, and national governments, public works, private industry, and individual citizens whom the system benefits. What we need is a couple of definitions and a manifesto declaring what we stand for when we say "self-healing" infrastructure.

Def: Public Infrastructure - Large scale technological systems that provide the services, materials and energy necessary to sustain human life and self-actualized human activity at an acceptable level within a society. This infrastructure is not coordinated at its highest level.

Def: Autonomic Infrastructure - A public infrastructure that is coordinated at a high level (scale) and responds to disturbances to maintain acceptable levels of service. Coordination is achieved through integration of previously disparate systems, introspection on the part of component systems and the macro-system, and intercession (intervention) on the part of subsystems and the macro-system to maintain coherence and cohesion.

1. Autonomic (self-healing) Technological Infrastructures - A technological infrastructure that is coordinated at a high level in the hierarchy to maintain certain performance measures.

2. Ultimate (Macroscopic) Measures of Infrastructure Performance - A technological infrastructure supports a society- people, their biological needs, their machines, their values, their culture and their institutions. How do we rate the performance of an infrastructure? This becomes important when the infrastructure is experiencing failures of a significant magnitude. What does the concept of *graceful degradation* from the field of fault tolerance mean when applied to a public technological infrastructure? Clearly there are many inter-coupled parameters being maintained simultaneously when the infrastructure is functioning. Which ones are the most important when trade-offs must be made in the face of critical resource shortages caused by massive failures of machines and disruption of human organizations? Some suggestions for the sake of discussion:
 - a) Number of Lives Sustained
 - b) Preservation of Social Order
 - c) Continuation of Government
 - d) Regulation of Social Entropy
 - e) Preservation of Social Structures
 - f) Preservation of Wealth
 - e) Preservation of Critical Resources
 - g) Criticality to Autonomy
 - h) Preservation of Key Persons

A few scenario-based analyses considering these parameters will quickly lead to conflicts and sub-optimal tradeoffs.

2. Response Horizon - Time required to intervene to stabilize the macroscopic variables to acceptable values. The goal of automation is to reduce impacts of failures by quickly responding to more system elements concomitantly.
3. Magnitude of the Disturbance - A relative measure of the magnitude of the infrastructure failure.
4. Kind of Disturbance - Disturbances can be caused by; 1) environmental conditions considered in the design of the system; 2) hidden states or conditions of the environment not considered in the design; 3) violations of axiomatic design assumptions; 4) misuse of common control inputs by human operators; 5) complex combinations of deviations along many dimensions.
5. Dynamics of a Regime Change - Changes in the infrastructure macro-state occur in response to a disturbance. Cascading failures and delayed effects can occur. The state trajectories that follow from an event must be understood so intervention can steer the systems to an admissible and stable state before violations of constraints occur.
5. Scale and Hierarchy - Integration involves creating a super level in a hierarchy of systems to facilitate information flow. This does not mean that coordination is centralized. The super level in a multi-level system may still be composed of distributed elements. High-scale controls and measurements refer to aggregated or abstracted variables (macro-state variables) measured in the super layer.
6. Signaling between many scales of organization - Communications among same-level elements and between the levels in the hierarchy determines the range of response. At the highest level behavior is emergent, resulting from interactions among subsystems in lower levels.

Stakeholders in the Design of Autonomic Infrastructures

Many different organizations have a significant interest in the design of autonomic infrastructures.

1. Architects and Civil Engineers - Human habitats designed by architects are the ultimate consumers of the outputs of the infrastructure. At any given hour human life is sustained by a physical structure fed by electricity, water, sewer, information, communications, and transportation systems. These structures are the ultimate point-of-delivery within the infrastructure. Instruments placed at these (millions of) points would measure actual state of service. Hence, human habitats must be instrumented with the proper sensors and controls. Transformation of resources through human consumption and processing also occurs here.

2. Public Utilities - In the US private corporations or local governments typically operate the generation and distribution systems comprising the infrastructure. These entities can make selections regarding operating parameters when a crisis arises. The high-scale control inputs reside within these entities. Capacity constraints are known within these entities.
3. Manufacturers - The manufacturing sector is responsible for providing the material components of the infrastructure. Replacements for damaged or destroyed components are created here. Availability of the components for rapid repair is controlled within these entities. Schedules for production and creation of inventory are controlled within these entities. Transportation of material entities is controlled here. Hence, high-scale control inputs also reside here.
4. State/Local Governments - The safety and security of citizens is the responsibility of state and local governments in the US. These governments operate and maintain the common emergency resources for a geographic region. Knowledge of local organization and technological structure resides here. Exercises to test the readiness of autonomic components would be conducted by local governments.
5. Policy Makers - Any policy regarding emergency plans that involve the trade off human lives must be approved through the legislative process. Policy makers must understand the decision structures incorporated into an autonomic infrastructure and vet them through public debate and opinion.
6. National Government – Recent anti-terrorist and homeland security activities have given the US federal government an integrative role in public safety and security. The DHS has resources and authority for many aspects of infrastructure protection.

2.2 Introspection, Integration and Intercession: Towards Self-Healing Critical Infrastructures (Steven Goldsmith, John Ganter, Rick Craft)

The economic and military security of the US depends on the steady operation of an interconnected and complex “system of systems” that includes telecommunications, electric power, transportation, oil and gas, manufacturing, and financial infrastructures. Both fixed elements and external forces (e.g., market conditions) combine to create flows that aggregate and distribute material, information, energy, and capital. While not widely recognized, both the normal delivery of services and the failure of services are *emergent* behaviors that result from complex interactions--they are not easily predicted from the properties of components. Characterizing and adjusting these behaviors requires a multi-level strategy that detects initial and changing conditions through sensors, predicts responses at multiple time scales with models, alerts decision-makers with situational analysis and options, and responds through actuators to optimize, protect, or repair the system.

Infrastructures have formed in response to both technological and economic forces. They are geo-spatially-distributed networks of producer, transport, and consumer elements that are also organized hierarchically. Dependencies among component systems are numerous and involve feedback coupling at many different levels. Malfunctions in elements of one component system may cause cascading malfunctions in elements of other systems. Coordination of an infrastructure system requires that the flow of information among distributed decision actors account for both upstream and downstream effects on other infrastructure elements. Tradeoffs are common but poorly characterized. For example, tight coupling and low excess capacity are desirable in the current deregulated markets, yet they raise both the probabilities and consequences of failures. The nation must rapidly develop an understanding of, and capability to protect and repair, a distributed asset that is increasingly vulnerable to both local and widespread threats.

Increasingly there is a recognized need to endow the national infrastructures with defenses against both external and internal insults that will diminish the probability of high-consequence failures. There is also the need for continued service under both malevolent attacks and natural failures, but concern that the dimensions, constraints, and opportunities of future threats will differ greatly from past experience. A research program must identify both strategic and tactical opportunities to contribute high-value science and engineering to these quests.

Based on both our current knowledge of unmet infrastructure needs and Sandia expertise, we will explore the concept of I3 to give infrastructure systems three new properties: (1) integration; (2) introspection; and (3) intercession. These

properties will be explored with a prototype information system designed for operation with historical, live, or simulated data. Initially, our scope will be a single municipality and simulated data.

Integration creates a single “super-infrastructure” by coordinating the flow of information among disparate infrastructure elements. There are significant unmet needs for instrumentation by sensors and sensor clusters, and integrating these information streams. Such a monitoring system will support experiments with populations of software agents that form a multi-agent society. The agents would conduct collaborative activities on behalf of client systems with the objective of maintaining the holistic state while allowing each system to operate on its local objectives. They may be assembled into composite actors and supply-chains that cross infrastructures. This object architecture will allow exploration of optimal degrees of agent autonomy, responsibility, and control, which are particularly important since infrastructures cross jurisdictions and involve competition, cooperation, and hybrid relationships.

Introspection enables the super-infrastructure to reason about its internal structure (macro-state). This situated monitoring system will track the current state of health of the infrastructure, enabling it to detect failures in component systems and to predict inadmissible states that lead to high-consequence failures. We will explore the relationships between high level objectives and system state of health. Introspection could provide identification of both faults (pre-symptomatic error states) and sentinel events (subtle predictors of impending failures) that pass unnoticed in existing systems. Meta-sensors could be assembled from the data streams of both multiple identical, and multiple different, sensors. Patterns that reveal both normal and inadmissible states could be detected and provided to both human and agent decision-makers. Both deductive (knowledge-based) and inductive (predictive fitness-based, e.g. Genetic Programming) approaches will be explored.

Intercession provides the super-infrastructure with the effectors necessary to influence its state and to reorganize its structure in response to internal and external disturbances. A coordination process intercedes when necessary either through human actors or directly through automatic instruments.

We propose to develop a multi-agent architecture that implements the I3 concept. The first year would involve the examination of existing infrastructure models resulting in the design of I3 agents for some infrastructure complex (e.g. power, transportation, healthcare - for response to chem-bio attack). We will then propose a larger project if deemed promising.

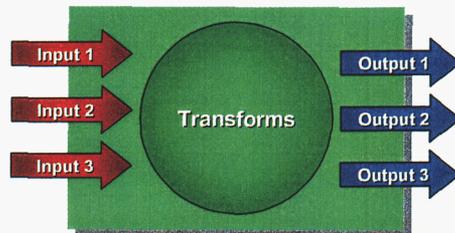


Goals of Original Proposal

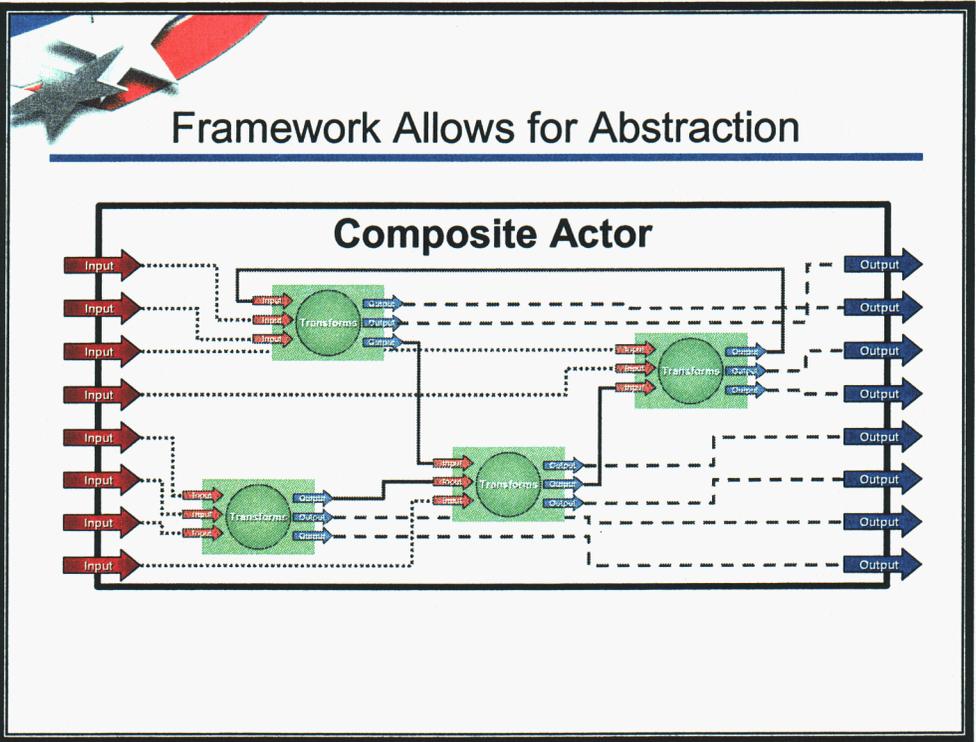
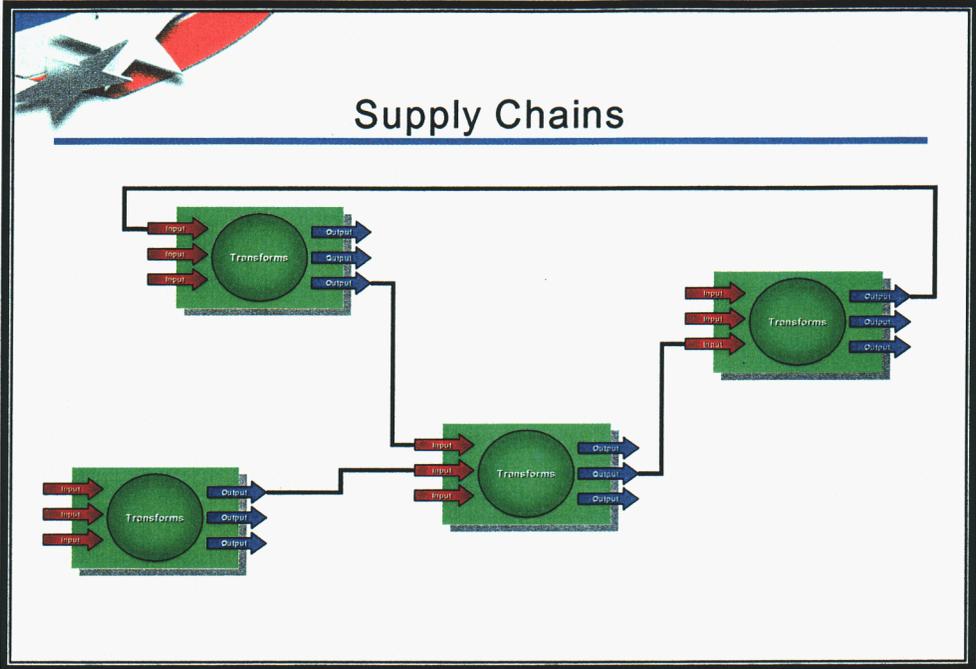
- Enable deep understanding of critical infrastructures and their vulnerabilities through the use of integrated, large-scale, detailed models of the infrastructures created using a common “supply chain actor” building block
- Create a suite of intelligent agents that enable humans to deal with the enormity of this task

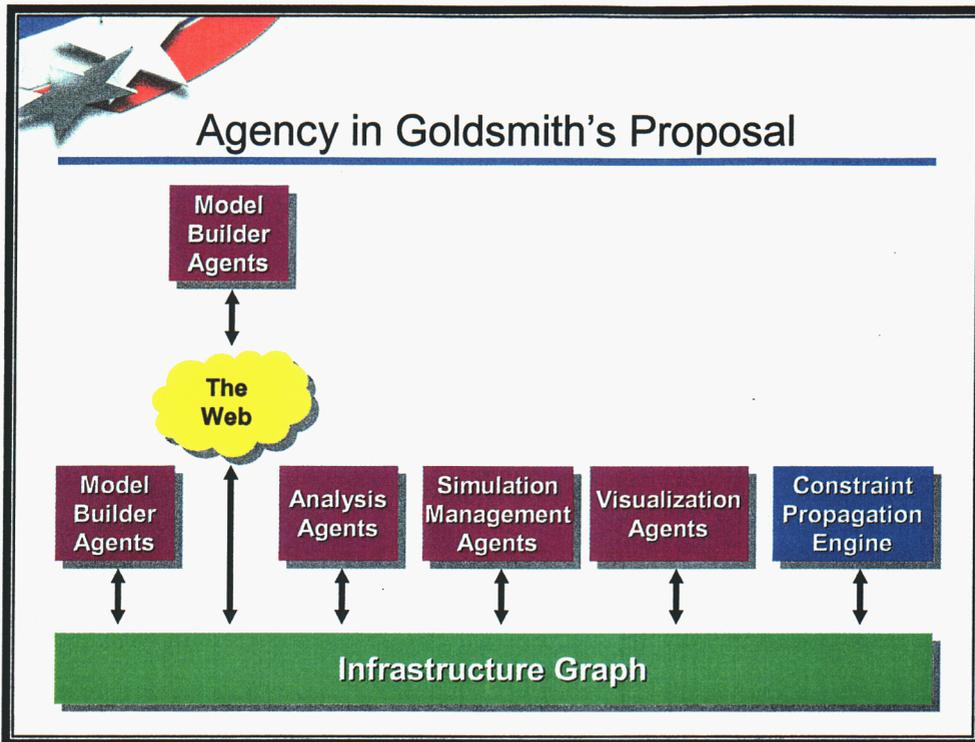


Supply Chain Actor



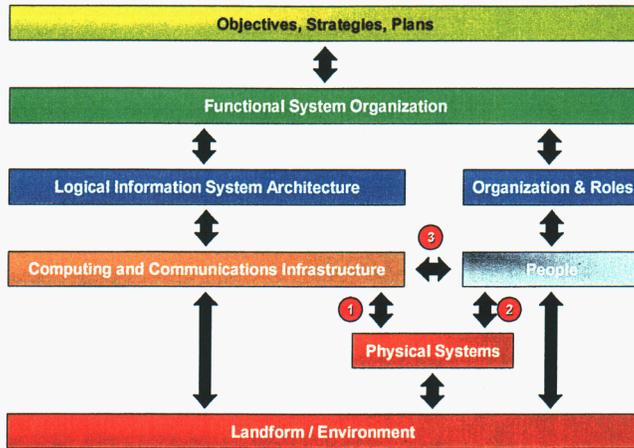
- Actor may be stateless or stateful
- In the case of the first, each output is a function of some or all of the inputs $\rightarrow O_1 = F(I_1, I_2, I_3)$
- In the case of the second, each output is a function of some or all of the inputs as well as the actor's state $\rightarrow O_1 = F(I_1, I_2, I_3, S)$





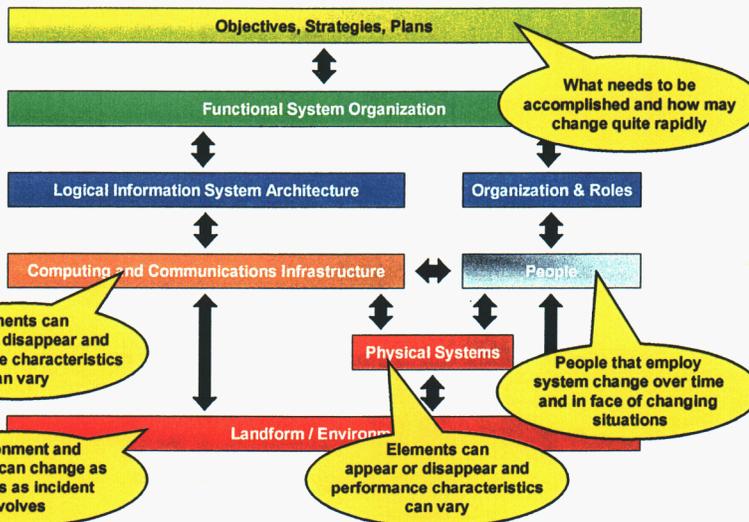
-
- Addressing Self-Healing Infrastructures**
- Add "intercession" capabilities referred to in the introduction of the original proposal
 - Refactor "actors" into three-layered entities
 - Physical dimension
 - Functional cyber dimension
 - System component dimension

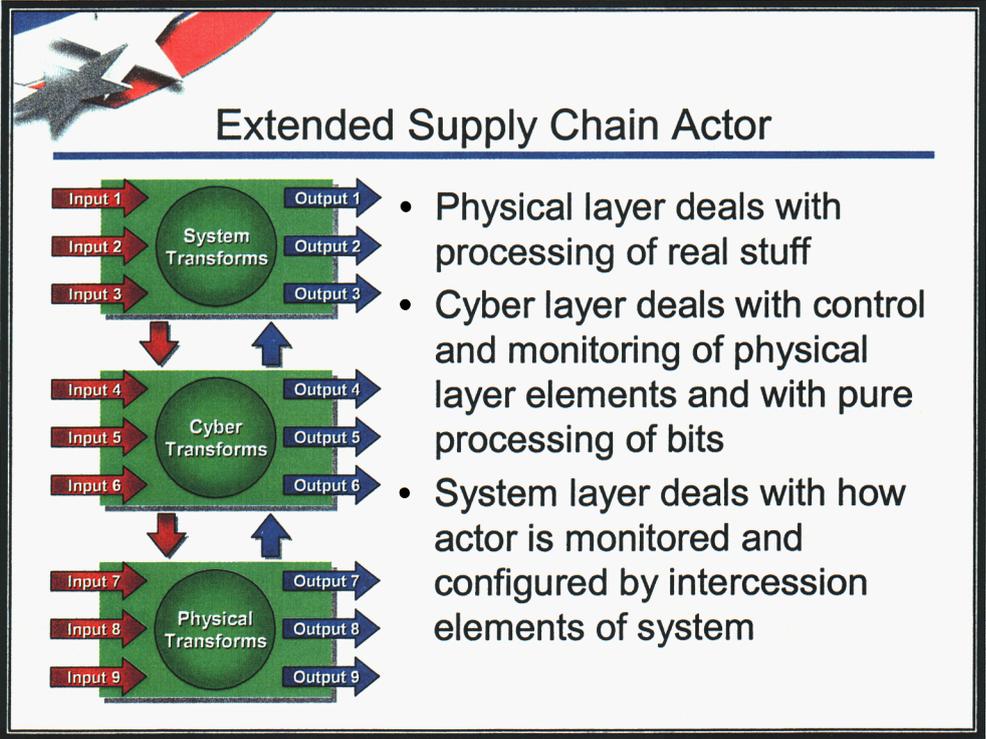
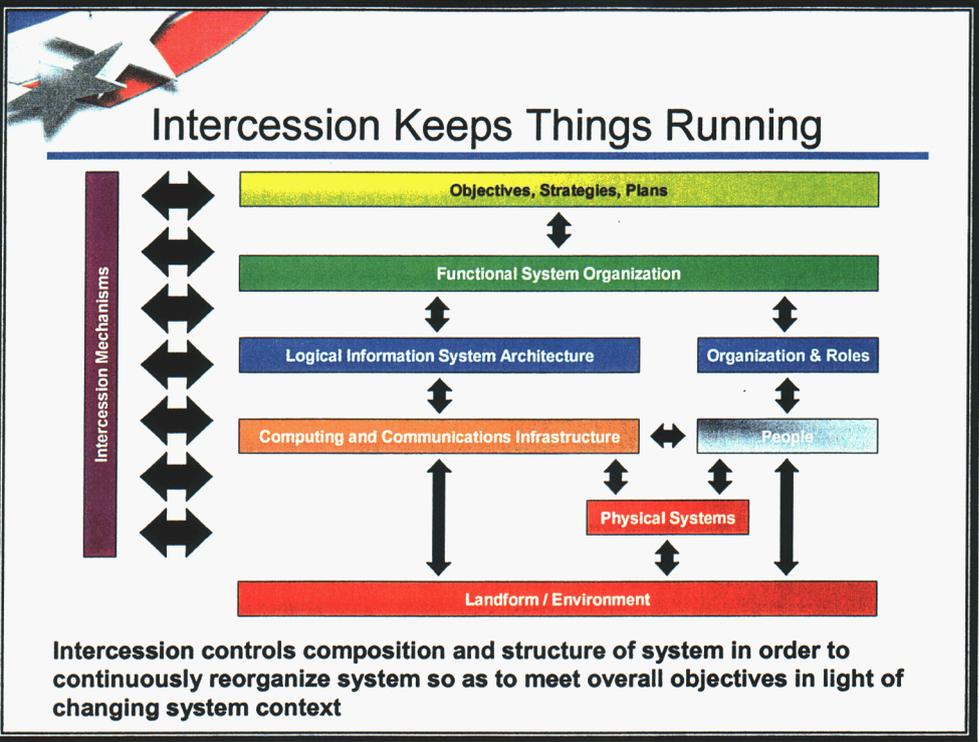
Another View Of The Infrastructure Graph



- ① Includes sensors and effectors that interact with physical systems
- ② Includes all interactions between people and physical systems
- ③ Includes both HMI/visualization functions and monitoring of humans

Introspection Captures Range of Changes







Framework May Support Other Methods

- Depending on how $O_1 = F(I_1, I_2, I_3, S)$ is represented, may be able to extract:
 - “Slices” and “chops”
 - Fault and event trees
- If functions and flows are cleavable from actors, may be able to refactor system to identify new kinds of actors and novel system organizations

3.0 Models of Critical Infrastructures

3.1 Modeling, Monitoring, and Coordinating Critical Infrastructures

This paper discusses an approach to improving the surety of critical infrastructures be used to endow the national infrastructure systems with a measure of reliability and fault tolerance that diminishes the probability of high-consequence failure regimes and ensures continued service under malevolent attacks, natural failures, or natural disasters. We propose the concept of I3 that gives infrastructure systems three new properties: (1) integration; (2) introspection; and (3) intercession. Integration creates a single “super-infrastructure” by augmenting the flow of information among currently disparate infrastructure elements, enabling coordinated decision-making to occur. Introspection endows the super-infrastructure with the ability to identify and reason about its macro-state, enabling it to detect failures in elements and to predict inadmissible states that lead to high-consequence failures. Intercession endows the super-infrastructure with the ability to influence the states of multiple elements in a coordinated manner to reorganize its structure in a manner that moves it to an admissible macro-state.

Introduction

We propose to develop an information system that will consist of two parts: a predictive model of the infrastructure that receives “live” information on model components via agents operating on the Internet; and a situated monitoring system that determines the current state of the infrastructure and intercedes when necessary either through human actors or directly through its instruments. The monitoring system will be inhabited by autonomous software agents that form a multi-agent society situated within the infrastructure. The agents conduct collaborative activities *semper et ubique* and *semper mentis* on behalf of client systems with the objective of maintaining the holistic state while allowing each system to operate on its local objectives. This proposal addresses the properties of integration and introspection, and will realize those properties by developing an on-line model of the national infrastructure. A second proposal addresses situated monitoring for intercession.

Technical Problem

Traditional modeling approaches are based on abstraction, hiding selected details and ignoring irrelevant aspects of the system to make the modeling effort practical. The scope and granularity of the model are carefully negotiated in light of the ultimate purpose of the model and the available information describing the system. Ahsby’s Law of Requisite Complexity suggests that a system with a great many states must be modeled at some minimum level of complexity or the level of uncertainty present in the model will be unacceptable. A very complex system-one with many actors and interactions- challenges the modelers to identify the proper set of primitives, abstractions, and aggregations that make the model tractable to existing modeling technology but still capture the essential behaviors of interest. If significant causal interactions occur at a level beneath the chosen level of primitives, then the model will have poor fidelity with respect to the system and model states will not be consistent with observations of the real system. Complexity therefore stymies the use of hypothetical high-level abstractions, and requires an empirical approach in which modelers must incrementally build the model to eventually discover the representation having requisite complexity. At intermediate levels of complexity, hierarchical structure and other system regularities are exploited to economize the representation. To conduct such an exploratory modeling effort, modelers must have access to exemplars of the real system state to validate the model and identify elements needing elaboration. Alternatively, the modelers must have access to highly accurate conceptual information on individual elements and behaviors and an error-free means of realizing the elements. In summary, system complexity is relative to the representational and information handling capabilities of the modeler that wishes to understand it.

The national infrastructure is a complex system that includes energy production & distribution, transportation, manufacturing & service industries, data and voice communications, health care, banking and finance, food and fresh water production, waste disposal, governments, and the military. Infrastructure systems produce and/or distribute materials, services, energy, information, capital, and human beings. It is composed primarily of private sector elements. Its dynamics arise from commercial transactions and the use of products and services by human consumers. An ideal national infrastructure model is essentially a macro-model of the United States that includes the entire industrial complex, all public works and agencies, the financial community, and the state and federal governments.

The governments and military are primarily consumers of materials, energy, and services and suppliers of capital and services. At the ultimate level of representation lies hundreds of millions of human actors making independent decisions that drive the infrastructure state. Human actors are influenced by, but not controlled by, policy, laws, and social norms. Even if a grand engineering model of the infrastructure is achieved, its dynamics originate in the individual and collective behaviors of an inscrutable swarm.

The purpose of the proposed infrastructure model is to identify and predict catastrophic failures in the infrastructure resulting from subtle couplings and counter intuitive behaviors. Therefore modeling efforts can be scenario-driven to focus resources on uncovering the high-consequence states. The sheer scope and depth required to capture counter intuitive and subtle interactions that may lead to critical failures identifies this as a research activity.

Realistic simulation of critical faults requires a deep understanding of the interaction dynamics [couplings] between component systems during operation. A model must capture essential aspects of the inter operation of the infrastructure systems in situ, with each system is functioning in a realistic context to fulfill its ultimate purpose. This describes an engineering "process and operations" model, and is different from economic and policy models. This model must be capable of supporting simulations over varying temporal horizons with geo-spatial representations of the infrastructure. The model must evolve incrementally, accept data of varying quality, and must function with incomplete and uncertain components.

Federated models obtained from stakeholder organizations and connected together with interstitial functions (hardware and software) have several disadvantages. First, access to the internal structure of the model to expose the inter facial variables may not be possible if the model is proprietary or if it was developed without explicit representation of the interfacial flows. The models are likely to be represented by different computer languages, implemented on different platforms, and have been developed for different purposes. This diversity will place a great burden on the project team and the resulting model will exhibit inherent constraints in its capabilities that will be costly to overcome. Microsimulation is the approach to modeling the national infrastructure that poses the least risk for an organization that has world-class capabilities in systems engineering, computing, networks, robotics, and computational physics.

Infrastructure models are naturally represented as specialized supply-chain graphs.

The premise of the supply-chain modeling approach is that the infrastructure can be represented by flow graphs, directed cyclic graphs whose nodes are infrastructure elements such as telephone switching centers, inter-modal ports, roads & rails, airports, manufacturing plants, power plants, military bases, packs of attorneys, etc. The links between nodes are directed from producer to consumer and represent the flow of materials, energy, services, etc. among the elements. The sub-graph identified by a node and its inputs represents the "supply-chain" for the node. The sub-graph identified by a node and its outputs represents the "consumer chain" for the node.

Each node has a finite "maximum capacity per time" with respect to its outputs, producing an output saturation when driven beyond this limit. Each node also has mathematical transform relating the consumption of inputs to the production of outputs. These transforms may be linear functions of input quantities, with conservative laws applying (mass & energy), or nonlinear in input quantities, producing binary "all-or-nothing" behavior. Electric power and unionized work forces are possible examples of inputs with binary transforms. The basic requirement is that the qualitative and quantitative effect of an input on an output within an element is captured so propagation of material events can be studied and reasoning about causality is possible. The transforms should also include switchover functions that enable alternative supply input sources to substitute for failed supply inputs. Finally, storage of excess production and limits on the inventory capacity must be captured as well. Each link identifies a "product" (material, device, energy, money, person, service, etc.) that flows from a producer to a consumer. Flows may be either concrete, such as electricity or fuel oil, or may be abstract, such as. Flows do not represent transportation entities such as trucks and pipelines; nodes represent all elements with transformational character. Cycles in the supply-chain graph indicate feedback couplings that carry a fraction of an output from a node that is eventually used to produce an input to the node. The cycles must obey conservative laws, and require ascribing identity to flowing entities. Causal supply chain models are similar to product life-cycle models developed to determine environmental loadings associated with the production, use and service, and disposal of a product. The objective of causal supply chain modeling is to investigate what happens to other products when a product or producer in the chain becomes temporarily disabled or unavailable. A detailed supply-chain model is needed to achieve both objectives. In many life-cycle modeling applications aggregate data is used to provide a composite "industry representative" of an infrastructure element. This is probably

not adequate for causal supply-chains because in many cases individual element data does not exist or is proprietary. The development of individual infrastructure node models will progress at different rates and will result in element models of differing fidelity. Propagation of uncertainties along the supply-chain graph is crucial when elements are not uniform with respect to their error budgets and fidelity.

Studying the supply-chain graph can lead to insights into infrastructure dependencies. A node with high indegree may indicate reliance of an element on a large number of diverse infrastructure elements, or may represent redundancies in supply [feedstocks] deliberately introduced for economic or reliability purposes. These nodes may be highly sensitive to failures of other elements. A node with high outdegree may indicate a critical resource [commons] that supplies a large number of infrastructure elements. These nodes may be the source of high-consequence or cascading failures. A node appearing in many cycles may indicate a complex node that produces services consumed by many elements that the node itself ultimately relies on to maintain its function. Sub-trees such as the spanning arborescence identify the ultimate customers of an element and the intervening elements required to deliver its services. Examination of this tree should identify higher order downstream effects of nodal failure.

Qualitative simulations on the supply-chain model are possible if a versatile constraint propagation engine supports fixing certain inputs and outputs and computing the relaxation of the graph to a new state. In a zero-output simulation a critical node, probably with high outdegree, is identified and its outputs are clamped to zero, essentially denying its customers any service. The denial of service is propagated downstream until a significant event occurs or until a new steady-state is reached. The state-of-health and operating characteristics of the infrastructure model are then examined under the new regime. A demand saturation study involves increasing the input demands on a critical node until its output capacity is saturated.

In a dependency identification study, the supply-chain of a critical node is searched for specific supplier nodes or specific classes of supplier nodes. Prominent dependencies are catalogued to identify important scenarios for future simulations.

Technical Issues

The overarching technical issues are representation and complexity. The complexity required of an infrastructure model that can accurately predict high-consequence faults is an open issue. The granularity of the model elements and their representation is another related open issue.

Microsimulation- Microsimulation is not just an option. It is the only means to capture subtle, highly-coupled states. If the system does not exhibit regularities at different levels of aggregation, then only the behaviors and interaction of the most primitive elements of the system give rise to important system-level phenomenon.

Complexity of the System Graph - The complexity of system graph appears to be linear in the number of nodes, even if iteration of cycles is required to determine steady state behavior. However, nonlinear transformations between inputs and outputs, and vice versa, may increase the complexity.

Sensitivity - Our hypothesis is that the macrostate of a highly interconnected system is sensitive to small changes in individual state variables. Therefore, errors in the model's representation of individual element's may cause apparent state changes that do not arise in the real system. Strict error budgets must therefore be represented and maintained for each element.

Computational Irreducibility - A truly complex system cannot be simulated by a model of less complexity than itself. Requisite complexity is reached at the most primitive level of representation. Computational irreducibility implies that mathematical abstractions that improve computability cannot be formulated. Simulation using a model with a fine granularity is needed to capture critical behaviors. It is not clear that the proposed infrastructure model falls into this category. Research into continuum representations conducted in parallel with full simulations should be conducted.

Model Validation - A complex operational system such as the US infrastructure cannot be identified on-line (unless we succeed in providing situated monitoring under this LDRD). There is not opportunity to drive the system and observe its behavior. Generally we can gain confidence by using some real state data to drive the model, looking for correlations in the model's state variables and actual measurements. Validation of the functions of individual elements may be the only means to obtain confidence in the model.

Compositional Semantics and Locality - Validation may be possible if the meaning of macro-phenomena can be understood in terms the models components and their local interactions.

Teleology - Since an element of the infrastructure is engineered by human designers, its structure, function, and behavior has a known context and can be understood in terms of its ultimate purpose.

Heterogeneous Actors - Each kind of element in the infrastructure has a different purpose and different behavior. The number of classes of different elements may be large. Swarm simulations and cellular automata generally involve large numbers of homogeneous actors. The amount of subject matter knowledge that must be captured from many different organizations is daunting.

Representational Adequacy and Notational Efficacy - The modeling language used to represent the infrastructure graph must be expressive enough to capture the broad range of system elements. Moreover, the notational elements must lend themselves to efficient computation to ensure the performance (and thus the predictive horizon) is adequate.

Performance and Capacity -The computing capabilities, processor speed, memory capacity, and disk storage are unknowns. It is likely that high-performance servers connected on a high-speed bus or a parallel processor will necessary.

Dynamic Topology and Functionality - Interconnections between nodes of the infrastructure and the nodal transfer functions themselves are dynamic. Changes in the real world must be reflected in the model in a timely manner or “model drift” will eventually increase to the point of obsolescence.

Search - The size of the state space that must be searched to discover interesting or critical behaviors is probably very large. A variety of search strategies, including genetic algorithms, simulated annealing, and knowledge-directed search may be required.

Scalability - Existing object-oriented systems may not be scalable to the dimension required by a national infrastructure system.

Technical Approach

The approach advocated in this paper is to develop a programming framework and computing test bed that supports long-term, incremental development of large-scale models of complex systems, particularly industrial systems and public works. We will represent heterogeneous actors as nodes in a scalable flow graph with interactions between the actors captured by links. Actors will be linked to a geographic information system to enable geo-spatial reasoning about the flow graph. We will use a mature object-oriented programming language to enable the very high degree of object reuse necessary to keep the coding of a large-scale problem manageable.

The flow graph development requires expertise in supply-chain modeling, GIS, constraint propagation, graph theory and discrete optimization, dynamic object programming, and complex systems. This team will obtain subject matter knowledge on infrastructure elements, perform mathematical analyses and investigate complexity issues, and construct the basic flow graph framework and constraint propagation (CP) engine. The graph model framework will contain mechanisms to ensure robust operation with incomplete and uncertain information. The graph model and CP engine frameworks will be coded in an advanced dynamic object-oriented language executing in a distributed processor environment to ensure scalability. Geographic information will be obtained from existing GIS sources but re-rendered into object-oriented format.

Because of the huge number of nodes and links in an infrastructure graph, and the enormous amount of subject matter knowledge required to capture the behavior of individual nodes, everything from power plants to inter-modal facilities to hospitals, innovation in managing the construction and operation the model will be required. A meta-model comprising intelligent agents that can reason about the flow graph model will assist researchers in searching large graphs for important features, in discovering interesting regularities, and in identifying high-consequence faults. It will include specialized intelligent agents that assist researchers with data entry, scenario development, simulation, data analysis, and visualization. The agents will mediate information exchanges between researchers and model and will mitigate the complexity of the model.

The model must have a very large number of human “transducers” to obtain modeling data on elements and to keep up with changes in the actual infrastructure. We will develop WWW-based intelligent agents operating within a secure Internet partition to continuously monitor infrastructure changes and update the appropriate model classes and instances. These agents will conduct elicitation sessions with human informants at the various stake holder organizations to obtain the latest changes to the particular element of class. The agents will then convert the stake holder inputs to new model objects. Researchers can manage the model by exception, “gardening” the new objects created by agents to handle idiosyncratic structures and behaviors if necessary.

Microsimulation using a fine-grained representation is appropriate to this problem because there is really no other alternative. We don’t know the level within the infrastructure at which critical faults are propagated. One failure of the entire AT&T network that put air traffic at risk was caused by three lines of computer code in a switching computer. We must take an exploratory approach and we must be able to increase the complexity of the model as we discover new behaviors. The size of the proposed model requires intelligent agents and information handling technology such as the Internet be used to construct and operate the model.

3. 2 A Survey of Infrastructure Modeling and Simulation (Dianne Barton, SNL)

At this time, research on modeling and simulation of infrastructure interdependencies is concentrated at National Laboratories (Sandia National Laboratories, Argonne National Laboratory, and Los Alamos National Laboratory) and at a consortium of academic institutions that is supported by a DoD/EPRI initiative. Work on modeling and simulation of individual infrastructures is more widely conducted but this report focuses on infrastructure interdependencies.

Research on infrastructure interdependencies at Sandia National Laboratories uses a systems viewpoint. Sandia uses dynamic simulation and agent-based microsimulation to model infrastructure interdependencies. Dynamic simulation modeling is used to simulate the interconnections between infrastructures, track the flow of commodities necessary to maintain system operation and identify chains of interdependencies, which could create unexpected vulnerabilities or robustness. (Brown, et. al, 2001, Brown and Beyeler, 2001). Analyses supported by the dynamic system models include: identification of system limitations, limiting elements or conditions, potential vulnerabilities, potential unintended consequences of preventative, regulatory or other procedural system changes, indicators of system manipulation, and economic impacts. Agent-based modeling provides a means for understanding properties of complex social systems and offers a new way of experimenting with, and theorizing about, dynamic economic systems. Agent-based models typically consist of many dispersed agents acting in parallel without a global controller responsible for the behavior of all. The actions of each agent depend upon the states and actions of a limited number of other agents, and the overall direction of the system is determined by competition and coordination subject to the system’s defined constraints. Complexity in the system arises more from interactions occurring between agents than from any complexity inherent in an individual agent. Analyses supported by the agent-based models include power market pricing and purchasing strategies and the economic costs of policy decisions like price caps on short term trading of electric power. (Backus and Barton, 2002, Barton et al., 2000, Barton and Stamber, 2000, Barton 2001).

Argonne National Laboratory uses agent-based models to study complex social systems. EMCAS is an electricity market model related to several earlier models (VanKuiken, et al., 1994; Veselka, et al., 1994). The underlying structure of EMCAS is that of a time continuum ranging from hours to decades. Modeling over this range of time scales is necessary to understand the complex operation of electricity marketplaces. EMCAS agents are highly specialized to perform diverse tasks ranging from acting as generation companies to modeling transmission lines. To support specialization, EMCAS agents include large numbers of highly specific rules. EMCAS, makes it possible to represent power markets with multiple agents, each with their own objectives and decision rules. The agent-based approach allows analysis of the effects of agent learning and adaptation. EMCAS can be used as an e-laboratory, where regulatory structures can be tested before they are applied to real systems. (North 2001, North 2000a, North 2000b, North et al. 2002).

Los Alamos National Laboratory uses a cellular automata model to simulate transportation, power, and communication infrastructure systems. Dynamics and movement are executed on a grid that is discretized into cellular automata. The result is an extremely fast simulation that can handle millions of individual agents. (Nagel et al. 1996, 1998). The TRANSIMS model is intended for transportation planners to forecast traffic congestion and pollution.

The Complex Interactive Networks/Systems Initiative (CIN/SI) was initiated in mid-1998 in response to growing concerns over the vulnerability of national infrastructures. CIN/SI is a 5-year, \$30 million Government-Industry Collaborative University Research (GICUR) program funded equally by EPRI and through the Army Research Office - the Deputy Under Secretary of Defense for Science and Technology. CIN/SI is working to advance basic knowledge in infrastructure vulnerabilities through the development of practical modeling, simulation, and analysis tools. A total of 28 universities are involved, along with two energy companies. The first consortia includes Harvard, Boston University, University of Massachusetts, Amherst, and Washington University that are investigating "*Modeling and Diagnosis Methods for Large-Scale Complex Networks*". The second consortia includes Cornell, University of Illinois, University of California, Berkeley, George Washington University, Washington State University and University of Wisconsin that are investigating "*Minimizing Failures While Maintaining Efficiency of Complex Interactive Network Systems*". The third consortia includes Caltech, Stanford, MIT, University of California, University of Illinois that are investigating "*From Power Grids to Power Laws: A Mathematics Foundation for Complex Interactive Networks*". The fourth consortia includes University of Washington, Arizona State, Iowa State, and Virginia Tech that are investigating "*Innovative Techniques for Defense Against Catastrophic Failures of Complex, Interactive Power Networks*". The fifth consortia includes Purdue, University of Tennessee, Fisk University, Exelon Corp., and the TVA that are investigating "*Intelligent Management of the Electric Power Grid through an Innovative Anticipatory, Multiagent, High Performance Computing Approach*". The sixth consortia includes Carnegie Mellon University, RPI, Texas A&M, University of Minnesota, and University of Illinois that are investigating "*Context-Dependent Network Agents*". (EPRI 2000, EPRI 2001)

Backus G. and Barton D.C.. (2002) An Example of Infrastructure Interdependency Analysis: Local, Regional, and National Economic Impacts. SAND Report 2002-0911.

Barton, D.C. (2001) Analysis of Complexity in Infrastructure Systems Using Agent Based Microsimulation, in RAND Complexity Conference Proceedings, ed. Kadtke, J.

Barton, D.C., Eidson, E.D., Schoenwald, D.A., Stamber, K.L., and Reinert, R.K. Aspen-EE: An Agent-Based Model of Infrastructure Interdependency, SAND2000-2925, 61 pp.

Barton, D.C. and Stamber, K.L. (2000). An Agent-Based Microsimulation of Critical Infrastructure Systems. in Energy 2000: The Beginning of a New Millennium, eds. Catania, P., Golchert, B., and Zhou, C.Q., pp. 709 – 714, Technomic Publishing Company, Lancaster, PA.

Brown, T. and W. Beyeler. Analysis of the Potential Economic Impacts of Electric Power Outages in California, Sandia National Laboratories, Project Report to DOE/OCIP, Albuquerque NM, SAND 2001-3368P, 2001, 32 pp.

Brown, T., Beyeler, W., and Barton, D.C. (2001) Assessing Infrastructure Interdependencies: The Challenge of Risk Analysis for complex Adaptive Systems. SAND Report 2001-3677., pp.

EPRI, Complex Interactive Networks/Systems Initiative: First Annual Report, EPRI TP-114660, June 2000, 74pp.

EPRI, Intelligent Management of the Power Grid: An Anticipatory, Multi-Agent, High Performance Computing Approach – EPRI/DoD CIN/SI Program: Second Annual Report, EPRI 1006091- 1006095, June 2001.

Nagel, K., Barrett, C.L., and Rickert, 1996, Parallel Traffic Microsimulation by Cellular Automata and Application for Large-scale Transportation Modeling, LA-UR 96-50, 17 pp.

Nagel, K., Beckman, R.J., and Barrett, C.L., 1998, TRANSIMS for transportation planning. LA-UR 98-4369.

Nagel, K., Rasmussen, and Barrett, 1996, Network traffic as a self-organized critical phenomenon., LA-UR 96-659.

North, M.J., Agent-Based Infrastructure Modeling, Social Science Computer Review, Sage Publications, Thousand Oaks, California: Fall 2001.

North, M.J., "SMART II+: The Spot Market Agent Research Tool Version 2.0 Plus Natural Gas," Proceedings of the Computational Analysis of Social and Organizational Science Conference, Carnegie Mellon University, Pittsburgh, Pennsylvania: 2000a

North, M.J., "SMART II: The Spot Market Agent Research Tool Version 2.0," Proceedings of SwarmFest 2000, Swarm Development Group, Logan, Utah: 2000b.

North, M, Guenter Conzelmann, Vladimir Koritarov, Charles Macal, Prakash Thimmapuram, Thomas Veselka 2002 E-Laboratories: Agent-Based Modeling of Electricity Markets, 2002 American Power Conference, Chicago, IL, 19pp.

VanKuiken, J.C., T.D. Veselka, K.A. Guziel, D.W. Blodgett, S. Hamilton, J.A. Kavicky, V.S. Koritarov, M.J. North, A.A. Novickas, K.R. Paprockas, E.C. Portante, and D.L. Willing, APEX User's Guide (Argonne Production, Expansion, and Exchange Model for Electrical Systems) Version 3.0, Argonne National Laboratory, Argonne, Illinois: 1994.

Veselka, T.D., E.C. Portante, V.S. Koritarov, S. Hamilton, J.C. VanKuiken, K.R. Paprockas, M.J. North, J.A. Kavicky, K.A. Guziel, L.A. Poch, S. Folga, M.M. Tompkins, and A.A. Novickas, Impacts of Western Area Power Administration's Power Marketing Alternatives on Electric Utility Systems, Argonne National Laboratory, Argonne, Illinois: 1994.

4. SNL/MIT Workshop on Self-Healing Critical Infrastructures

4.1 Workshop Prospectus

The economic and military security of the US depends on the steady operation of an interconnected, complex “system of systems” that includes telecommunications, electric power, transportation, oil and gas, manufacturing, and financial infrastructures. The ultimate purpose of the infrastructure system is to distribute material, information, energy, or capital. Most infrastructure systems are geospatially distributed. Dependencies among component systems are numerous and involve feedback coupling at many different levels. Malfunctions in elements of one component system may cause cascading malfunctions in elements of other systems. The normal delivery of services and failures are emergent behaviors that result from complex interactions.

This workshop will explore the theme of coordination. Coordination of an infrastructure system requires the flow of information among distributed decision actors that attempt to regulate local operations according to local cost functions or optimization criteria. These local decisions often do not account for “downstream” effects on other infrastructure elements. We wish to explore the concept of a large scale coordination system that integrates infrastructure elements through a common information system and enable s interoperation during attacks or large-scale failures. There are five areas of interest:

- Concepts for High-level Coordination Systems - Explore candidate system architectures that will coordinate infrastructure elements during large scale failures
- Large Scale Computer Systems & Networks - Understand the challenges of building and safely operating a large scale on-line computer network
- Sensors, Indications and Warnings - Develop concepts for sensing the state of the infrastructure and developing situation awareness
- Social & Political Issues - Explore social, economic, and political ramifications of an autonomic coordination system and its effects on local, state and federal governments
- Industrial Concerns - Understand the positions of industrial stakeholders (architects, civil engineers, urban planners, construction companies)

4.2 Self-Healing Infrastructures: MIT Final Report on the Workshop

In the wake of the terrorist attacks almost a year ago, greater attention is being paid to domestic security in the United States. The intent of the attacks was to damage symbolically important targets with high loss of life. But the destruction of the World Trade Center, and the resulting damage to the transportation and communications infrastructures in the New York City area, highlighted the potential vulnerability of the nation’s interconnected infrastructures. This summer, faculty and staff of MIT’s Engineering Systems Division (ESD) engaged in a summer study, funded by Sandia National Laboratories, to consider the problem. The study’s scope of work stated:

- There is a need to endow the infrastructure systems with self-healing capabilities, which would provide defensive and repair mechanisms (e.g., reconfiguration) against malevolent attacks and natural failures.
- Such opportunities may exist in the information infrastructure used for controlling the nation's electric power grid.
- ESD will identify research questions and possible approaches to self-healing infrastructures.
- ESD faculty will prepare for and participate in a workshop with staff from Sandia National Laboratories to explore ideas for self-healing infrastructures.

Ten MIT staff joined their Sandia counterparts in Albuquerque, New Mexico, on the 20th and 21st of August for a workshop on self-healing infrastructures. At the meeting, the participants agreed to continue their collaboration and develop a proposal for a research program. This report, along with accompanying slides, completes the summer study.

“Self-healing”

The first area considered by the summer study group was the meaning of the term “self-healing.” The definition implied by the term is that infrastructures should automatically repair themselves in the event of a disturbance. Such a response would require infrastructures to be aware of their condition and to adapt rapidly to changes in order to maintain adequate working order. Making infrastructures “self-healing,” in this view, would require outfitting the physical elements with sensors, linking them through the Internet or other communications channels, and imbuing the system as a whole, and possibly the individual components of the infrastructure, with the intelligence to comprehend the state of the infrastructure and to respond.

The ESD study group had several concerns with this definition. First, we were not sure to what degree a system was technologically feasible. Concerns raised included the difficulty of designing a system with the “appropriate” level of intelligence and complexity that also was sufficiently reliable to operate the infrastructures. Another concern lay in whether the “self-healing” component had the potential to make the infrastructure, on balance, more vulnerable from cyberattacks, for example. Damage to the information system, or an attack designed to produce false readings or other disruption to the sensors and control mechanisms, could have effects similar to, or potentially greater than, damage to the physical elements of the infrastructure. Finally, the group agreed that even if such systems were to be built successfully in the future, current vulnerabilities required short-term action.

The ESD group therefore settled on an alternate definition of “self-healing.” “Self”, in this view, applies not only to the physical elements of the infrastructure and the information systems that allow communication among those elements, but also to the humans who are the overall supervisors and final arbiters of action. Making infrastructures more “self-healing” has both organizational and technological aspects.

History

The statement of work suggested the electric power grid as a potential early application of “self-healing” concepts. The ESD study group considered how various “self-healing” definitions and applications might apply to the electric power industry. One group, focused on reviewing past incidents, showed that information technologies would respond better to some types of disruptions than others. The group examined several regional blackouts, including the 1977 New York City blackout, the 1996 Western states outage, and the 1998 Quebec outage. The 1977 and 1996 outages were caused by cascading failures. In such cases improved information technologies have the potential to reduce the likelihood and extent of system failure. Even during the 1996 blackouts, human controllers reacted slowly to the emerging failure, and much data that suggested the growing loss of stability was poorly appreciated and collated. Improved data collection, and more importantly, better processing and system awareness, would have given operators more time to react, improving their performance. At the same time, though, the 1996 blackout suggested the difficulty of designing such an information-collation system. A contributing cause to the Western states blackout lay in the failure of relays to behave as expected by controllers. Unless the model of the system embodied in the collation and awareness programs accurately represents the behavior of the physical elements, it may not improve decision-making or adequately protect the infrastructure.

Unlike the 1977 and 1996 outages, the physical freezing of more than one hundred transmission lines following a multi-day ice storm caused the 1998 Quebec blackout. The frozen lines had to be thawed individually. Although crews restored service to much of the province within hours, isolated areas remained without power for up to three weeks. Even perfect system awareness could not have significantly mitigated this event. Rather, “self-healing” in this case would require more and better-trained repair crews, broad availability of spare parts, and potentially even broader use of portable generators and other distributed energy technologies.

Aspects of Self-Healing

A second study group compared “self-healing” with other potential paradigms for reducing the vulnerability of the electric grid, including “redundancy,” “decentralization,” and “repairability.” This group examined the ISO-New England’s plans to ease transmission constraints within its service territory; the ISO has concluded that transmission is the greatest current source of vulnerability of the power grid in the New England area, although access to natural gas

supplies may be a future concern. ISO-New England has pressed for increasing system redundancy to ease constraints in Southwestern Connecticut, where vulnerability is greatest. The group concluded that one barrier to any paradigm for reducing vulnerability lay in an organizational concern; two utilities provide power in the area, and plans for maintaining, let alone improving, transmission in the area had been slowed by the lack of incentives for them to make such investments in a deregulating industry. The move toward regional transmission organizations, therefore, may provide new incentives for investment in technologies that reduce transmission constraints, with varying degrees of local and regional impact. A second conclusion was that “self-healing” information technologies, greater redundancy, decentralization, and investments in reparability all could reduce the vulnerability of the electric power grid, but implied very different responsibilities, and expenditures on labor and technology, than exist under the current system.

Information Technology

A third study group, focused on information technologies, identified several promising areas for developing technologies that would begin to move the electric utility industry, as well as others, farther down the road toward self-healing. One highlighted approach was large-scale agent-based systems. Agent-based models can be helpful in analysis and planning, as they complement top-down modeling methods like system dynamics. Agent-based approaches also provide new methods for developing systems that can potentially control entire infrastructures in a distributed fashion. A second highlighted approach involved improved data mining and visualization tools. The experiences of human controllers in large-scale blackouts discussed above suggest that these tools would assist supervisors in mitigating certain classes of terrorist attacks or infrastructure disruptions that they had not previously encountered.

Cross-cutting Issues

In synthesizing the views of the various study groups, one idea common to them all is the importance of context in determining the usefulness of self-healing approaches or other mitigation strategies. As the electric power example shows, even the best self-healing systems will respond more rapidly to some classes of threats than others. A second common theme was the importance of determining the vulnerability of different types of infrastructures, and the risk posed by classes of attacks on those infrastructure types. For example, most ESD participants believed that electric power grids are inherently vulnerable, especially to localized and small attacks, the risk of death and economic impacts from short-term disruption was low relative to attacks on other infrastructures (e.g. water, food supplies). The group as a whole also concluded that economic disruption resulting from changes in behavior in response to an attack (owing to panic or even government response) could in many cases be considerably greater than the disruption of the attack itself. Costly responses to terrorist threats without a strong quantitative assessment of risk, therefore, were likely to misallocate resources and fail to prepare the American public for future terrorist attacks.

Broad conclusions and research questions

The group came to several broad conclusions regarding the vulnerability of infrastructures and the use of self-healing strategies to reduce those vulnerabilities:

1. Currently, the vulnerability of national infrastructures, and the risks associated with damage to them from terrorist assaults, has not been well quantified.
2. National policies have not yet been articulated regarding the long-term goals of risk reduction. But it appears that risk reduction strategies flowing from the response to September 11th are likely to have overemphasized politically salient risks such as airline security relative to other terrorism-related risks.
3. At least for current research purposes, a broader definition of “self-healing” that encompasses the stakeholders who own, operate, and make policy regarding the nation’s infrastructures should be used.
4. Multiple approaches, with self-healing playing an important, but not exclusive role, will need to be used to reduce infrastructure vulnerabilities and related risks.

These conclusions led to a research agenda, which will be developed in collaboration with Sandia into proposals for a large research program.

1. Infrastructure vulnerability
 - a. How should the vulnerability of infrastructures be measured?
 - b. What are the risks associated with that vulnerability and how should they be measured?

- c. What new tools should be developed to assess the vulnerability of the nation's linked infrastructures?
 - d. To what extent should the links between U.S. infrastructures and those of other countries (e.g. transportation, energy) be included?
2. Risk assessment and risk mitigation policies
- a. What would a scenario-based risk assessment conclude regarding the overall risk from terrorism in the United States?
 - b. What would be the relative risk associated with infrastructures and methods of attack?
 - c. What would be the best risk mitigation approaches to reduce those risks considered worth mitigating?
 - d. How should the nation organize to handle "unforeseen" – and not well-characterized – threats?
 - e. What policies (prevention, R&D, regulation, tax and other incentives) would be desirable in mitigating risks, and what would their implementation imply in terms of the burden of mitigation?
3. Self-healing
- a. Could technologies such as agent-based modeling be used to better simulate and control the nation's interlinked infrastructures?
 - b. Could information technologies and their accompanying sensors and communication links be designed and built that would improve the performance of already highly automated infrastructures like communications and energy?
 - c. What other technologies would be desirable to make infrastructures more self-healing?
 - d. What organizational changes would be desirable to make infrastructures more self-healing?
 - e. How would these technologies and organizational strategies best be disseminated to infrastructure owners, designers, and regulators?
 - f. What would these technologies and organizational strategies cost to implement, and what other benefits might flow from using them?

The attached slides elaborate further on these conclusions.

4.3 Workshop Announcement



Massachusetts Institute of Technology (MIT):
Self-Healing & Infrastructure Workshop
August 20-21, 2002
Pecos Room
Albuquerque Marriott Hotel
2101 Louisiana Blvd. NE; Albuquerque, NM 87110

Facilitator:

Phil Chamberlin
 Strategic Technologies, Inc. (STI)
 (505) 271-0131
 Cell: (505) 363-5797

Host:

MIT:
 Dr. George Apostolakis, (617) 252-1570
 SNL:
 Dr. Tim McDonald, (505) 844-9616

Alternate Sandia POCs:

Meeting coordination:
 Dr. Ben Cook, (505) 844-3795
 Barbara Macias (505) 844-2219

August 20, 2002

7:30am-8:00am	Welcome and Continental Breakfast	Pecos Room	
8:00am-8:15am	Setting the Stage	Pecos Room	Phil Chamberlin, Facilitator
8:15am-8:45am	Introduction	Pecos Room	Dr. Sam Varnado, SNL (505) 845-9555
8:45am-9:15am	NISAC	Pecos Room	Dr. Steve Rinaldi, SNL (505) 844-2153
9:15am-9:45am	Sandia's Perspective on Self-Healing	Pecos Room	Dr. Steven Goldsmith, SNL (505) 845-8926
9:45am-11:00am	MIT's Perspective on Self-Healing	Pecos Room	Dr. George Apostolakis, MIT
11:00am-12:00pm	Discussions: <ul style="list-style-type: none"> • Finalize breakout topics and prioritize order 	Pecos Room	All
12:00pm-1:00pm	Working Lunch	Pecos Room	All
1:00pm-2:30pm	Session 1: Breakout and report back	Pecos Room	All
2:30-4:00pm	Session 2: Breakout and report back	Pecos Room	All
4:00pm-5:00pm	Discussions/Wrap-Up	Pecos Room	All
6:15pm	Board Bus to El Pinto Restaurant	Marriott Lobby	All
7:00pm	Dinner at El Pinto Restaurant (10500 4 th NW)	El Pinto	All
8:30pm-8:45pm	Return to Marriott		All



Massachusetts Institute of Technology (MIT):
Self-Healing & Infrastructure Workshop
August 20-21, 2002
Pecos Room
Albuquerque Marriott Hotel
2101 Louisiana Blve. NE; Albuquerque, NM 87110

Facilitator:

Phil Chamberlin
 Strategic Technologies, Inc. (STI)
 (505) 271-0131
 Cell: (505) 363-5797

Host:

MIT:
 Dr. George Apostolakis, (617) 252-1570

 SNL:
 Dr. Tim McDonald, (505) 844-9616

Alternate Sandia POCs:

Meeting coordination:
 Dr. Ben Cook, (505) 844-3795
 Barbara Macias (505) 844-2219

August 21, 2002

7:30am-8:00am	Continental Breakfast	Pecos Room	All
8:00am-8:30am	Review/Recap/Regroup	Pecos Room	Phil Chamberlin, Facilitator
8:30am-9:30am	Session 3: Breakout and Report Back	Pecos Room	All
9:30am-10:30am	Session 4: Breakout and Report Back	Pecos Room	All
10:30am-12:00pm	Wrap-Up & Next Steps	Pecos Room	All
12:00pm-1:00pm	Working Lunch	Pecos Room	All

4.4 Workshop Contact List

Self-Healing & Infrastructure Workshop Contact List			
Name/Contact Info.	Level	Title	Expertise
SNL			
Dr. Sam Varnado sgvarna@sandia.gov (505) 845-9555	Director	Infrastructure & Information Systems	Critical Infrastructure Protection
Dr. Steven Rinaldi smrinal@sandia.gov (505) 844-2153	Manager	National Infrastructure Simulation & Analysis Center (NISAC) Program Director	Modeling & Simulation
Dr. Stephen Martin sjmarti@sandia.gov (505) 844-9723	Manager	National Security & Sensors	Sensors
Dr. Tim McDonald tsmcdon@sandia.gov (505) 844-9616	Manager	Cryptographic Research	Information Surety
Mr. Gordon Smith gjsmith@sandia.gov (505) 844-2773	Manager	Public Safety Technologies	Architectural Surety
Dr. Dave Borns djborns@sandia.gov (505) 844-7333	Distinguished Member of Technical Staff	Program Manager Fossil Energy	Fossil Energy Research
Dr. Steven Goldsmith sygolds@sandia.gov (505) 845-8926	Distinguished Member of Technical Staff	Chief Scientist Advanced Information Systems Lab (AISL)	Agent-Based Research
Mr. Mike Hightower mmhight@sandia.gov (505) 844-5499	Distinguished Member of Technical Staff	Program Manager	Energy/Water Infrastructures
Dr. Dianne Barton dcmaroz@sandia.gov (505) 844-5504	Principal Member of Technical Staff	Lead Research	Agent-Based
Mr. Shannon Spires svspire@sandia.gov (505) 844-4287	Principal Member of Technical Staff	Advanced Information Systems Lab (AISL) Technical Research	Agent Research

Name/Contact Info.	Level	Title	Expertise
Mr. John Ganter jganter@sandia.gov (505) 844-1304	Senior Member of Technical Staff	Advanced Decision Support Applications	Information Systems
Dr. Ben Cook bkcook@sandia.gov (505) 844-3795	Senior Member of Technical Staff	Mission Engineering & Analysis	Information Systems/Civil Engineering
MIT			
Dr. George Apostolakis apostola@MIT.edu (617) 252-1570	Professor	Nuclear Engineering and Engineering Systems	Risk Management, Safety
Dr. John S. Carroll jcarroll@MIT.edu (617) 253-2617	Professor	Management Behavioral Policy Science (BPS)	Organizational learning and change, leadership, safety, individual and group decision making.
Dr. Nazli Choucri nchoucri@MIT.edu (617) 253-6198	Professor	Associate Director of the Technology and Development Program	International Relations and International Political Economy
Dr. Stephen R. Connors connorsr@MIT.edu (617) 253-7985	Director	Analysis Group for Regional Electricity Alternatives (AGREA)	Strategic Energy Planning in Electricity
Ms. S. Tina Ghosh tinag@MIT.edu (617) 225-8181	Ph.D Candidate	Engineering Systems	Risk-Informed Decision-Making for Significant Uncertainty
Dr. Christopher Magee cmagee@MIT.edu (617) 252-1077	Director	Center for Innovation in Product Development	Systems Engineering, Metallurgy and Materials Science
Dr. David Hunter Marks dhmarks@MIT.edu (617) 253-1992	Director	Laboratory for Energy and the Environment	Large-Scale Computer-Based Simulation and Optimization Modeling
Dr. Fred Moavenzadeh moaven@MIT.edu (617) 253-7178	Director	Center for Technology, Policy and Industrial Development	Technology Development & Formulation of Technological Policies

Name/Contact Info.	Level	Title	Expertise
Dr. Stella Maris Oggianu soggianu@MIT.edu (617) 225-8510	Researcher	Engineering Systems	Systems Engineering and System Dynamics for Energy Policymaking
Dr. Brian L. Zuckerman brianz@MIT.edu (617) 452-2962	Postdoctoral Fellow	Engineering Systems Division	Technology Management and Policy
Phil Chamberlin epcham@strategic-technologies.net (505) 271-0131	Facilitator	Strategic Technologies, Inc.	
Visitors			
Dr. Bob Eagan rjeagan@sandia.gov (505) 845-8943	Vice President	Energy, Information & Infrastructure Surety	
Dr. Don Cook dlcook@sandia.gov (505) 845-7446	Director	MESA Program Office	
Dr. Gerry Yonas gyonas@sandia.gov (505) 845-9820	Vice President	Advanced Concepts Group	
Mr. Chuck Meyers cemeyer@sandia.gov (505) 844-3459	Manager	Laboratory & University Research	
Dr. Judy Moore jhmoore@sandia.gov (505) 845-9415	Manager	Advanced Concepts Group	
Dr. John Whitley jbwhitl@sandia.gov (505) 845-9763	Manager	Advanced Concepts Group	
Mr. Mike Tebo matebo@sandia.gov (505) 284-3287	Manager	Software & Information Engineering	
Ms. Marie Garcia mgarci@sandia.gov (505) 844-7661	Staff-Lab	Laboratory & University Research	
Ms. Renae Perrine rjperri@sandia.gov (505) 284-2824	Staff-Lab	Human Resources for VP 6000	

Appendix A: Self-Healing Infrastructure Proposal



Self-Healing Infrastructure Proposal

Embassy of Singapore
Peng-Yam Tan
Head of Defence Technology Office
Jonathan Ng
Assistant Head of Defence Technology Office

June 20, 2001

Reynold S. Tamashiro
Manager
Advanced Information & Control Systems
Ph. 505-845-9804
Email: rstamas@sandia.gov

Steven Goldsmith, Ph.D.
Principle Investigator
AISL
Ph. 505-845-8926
Email: sygolds@sandia.gov

AISL
advanced information systems laboratory

Page 1



Self-Healing Infrastructure Proposal

Embassy of Singapore
Peng-Yam Tan
Head of Defence Technology Office
Jonathan Ng
Assistant Head of Defence Technology Office

June 20, 2001

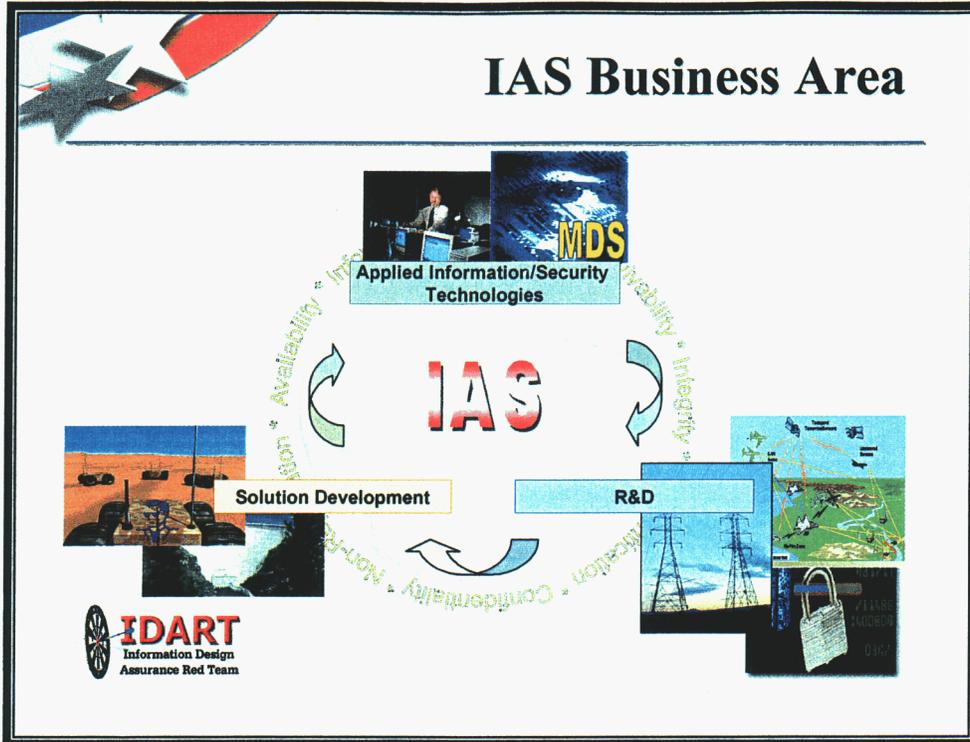
Reynold S. Tamashiro
Manager
Advanced Information & Control Systems
Ph. 505-845-9804
Email: rstamas@sandia.gov

Steven Goldsmith, Ph.D.
Principle Investigator
AISL
Ph. 505-845-8926
Email: sygolds@sandia.gov

AISL
advanced information systems laboratory

Page 2





- ## Discussion Topics
- Who are we?
 - Some background and motivation for this research
 - Our research approach
 - Questions?



IAS Mission Statement

“To provide information assurance solutions to our customers (DOE, DoD, & others) through research, modeling, and implementation of secure information technologies.”



Information Assurance and Survivability Program Areas

- Enhancing information security for the nation's critical infrastructure systems such as electric power and gas pipeline control systems
- Nuclear weapons Use-Control Systems
- Securing information in treaty verification systems in both satellite and ground-based sensor systems
- Improving information assurance and survivability in military information operations and C3 systems



Motivation for this research

- Two main reasons – my bosses, Sam Varnado and Bob Eagan
- Sam has been working Critical Infrastructure for over seven years. He has been engaged in policy changes as well as identifying R&D gaps.
- Sam’s far vision has been 20/20. He “spear-headed” Interdependency modeling and the SCADA security initiatives here at Sandia before the rest of the country recognized the need.
- Sam’s “big” worry today - infrastructure robustness and reliability to survive malevolent and non-malevolent acts and guarantee deliver of commodities to users.
 - **There is no communications and control between infrastructures for operators to coordinate**
- He believes the infrastructures must have “self-healing” type properties that process emergent features.



New Initiatives with Singapore

- Self-Healing Infrastructures¹
 - Explore the Concept of Infrastructures That Can Heal Themselves After an Intrusion or Upset
 - Formulating Ideas Now. Best Bet Is to Concentrate First on Information Systems Using Agent-Based Technology to Provide Repair and Remediation
 - First Efforts Will Be Funded in FY ‘02 by a Small LDRD Project
 - MIT Will Be a Strategic Partner Because of Previous Work in This Area
 - Singapore/DSO Will Provide Large Scale Testing Opportunities. Initial Discussions Have Begun

¹ Global Infrastructure Security Integrating Initiatives (Robert J. Eagan, Roger Hagengruber, Jim Tegnalia)



The Nation's Infrastructure is a Complex System of Systems



- **Infrastructure**

Interdependent Networks and Systems That Provides a Continual Flow of Goods and Services Essential to the Defense and Economic Security of the United States

- **Critical National Infrastructures**

- Infrastructures That Are Deemed to Be So Vital That Their Incapacity or Destruction Would Have a Debilitating Regional or National Impact or Severely Disrupt the Behavior and Activities of Large Numbers of People Who Depend Upon the Infrastructure



The Nation's Infrastructure Faces a Broad Spectrum of Threats

- **Physical Threats**
 - Terrorists
 - Aging and Degradation
 - Natural Disasters

- **Cyber Threats**
 - Malicious Intrusion
 - Inadvertent Error

- **System Complexity**
 - Increasing Number of Interconnections and Automation
 - Cascading Effects
 - Increasing Interdependencies





The US Infrastructure is Difficult to Protect so how do you guarantee continuity of service?

- Coordination of Protection Activities within the Government is Just Now Beginning
- Precise Threat Definition is Not Available
- Interdependencies Complicate the Definition of Critical Nodes
- Most of the Infrastructure is Owned by Private Industry



Motivation since 9/11

- 9/11 infrastructure failures.....from Lil.
- There are many initiatives as well as technology solutions that provide a piece of the puzzle. Some provide added benefit, some
- We realized from our interdependency activities that no one was addressing this concern from a “holistic” system perspective.
 - We are addressing technology from an operational deployment concept and technology evolution perspective and not system lifecycle issues (CM, policy, maintenance, funding, training,...) which may result as a by product from this research



Research Objectives

- Improve the safety, security and reliability of an infrastructure
- Coordinate the operation of a national infrastructure as a single “super-system”
- Develop an interoperating computer network of intelligent agent programs based on core AISL technology



Our Approach: I3

- Integration - Interconnect disparate infrastructure control elements
- Introspection - Provide each element with self-awareness
- Intercession - Develop controls to regulate operation of the integrated system

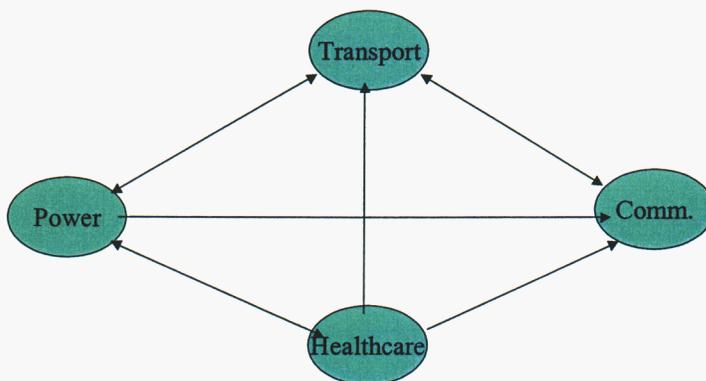


Integration

- Connect information systems (agent) at each node and interoperate on-line operational models
- Explicitly model customer/supplier and support relationships, failure modes, alternative sources



Integration



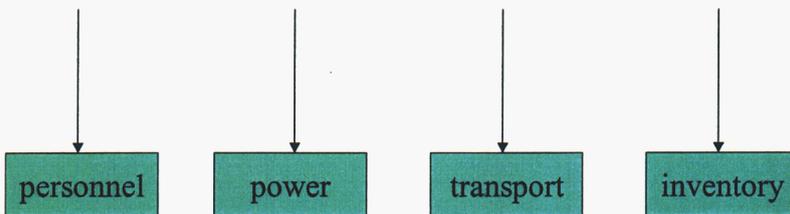


Introspection

- Instrument critical variables and parameters
- Model dynamics of the operation at an appropriate level
- Explicitly model inputs and dynamics from other infrastructure elements
- Explicitly model outputs to other infrastructure elements



Introspection





Intercession

- Identify macroscopic properties and operating ranges
- Negotiate changes in operation to achieve regulation of the super-system
- Respond to large-scale failure modes
- Prioritize critical resources under failure modes



Interdependency Management

- Predicting level of service for the local element
- Analyzing control decisions made at an element that affect other elements
- Informing other elements of current state-of-health and predicted performance
- Coordinating interoperation of elements



Situated Models

- Agent analyzes local inputs and predicts state of the local element
- Agent analyzes information from other agents and predicts dependency impacts
- Agent analyzes future states for inadmissible regions
- Agent shares predictions with other agents



Look-ahead

- Time horizon vs. certainty of predictions is Look-ahead
- Response regimes are sensitive to effective Look-ahead of agent system
- Response regimes in the 0-10 minute range are needed for local responses
- Response regimes in 0-24 hours may be adequate for some large scale faults



Security

- Security of agent systems is critical
- Secure network communications
- Secure agent operation



Approaches to Implementation

- Retrofit existing infrastructure elements
 - Develop models incrementally
 - Gradually improve Integration and Introspection
 - Add Intercession as needed
 - Test system (challenging)



Approaches to Implementation

- Greenfield- Develop infrastructure elements with intrinsic I3
 - Buildings, Industrial Plants, Power Plants
 - Transportation Networks, Ports-of-Entry
 - Hospitals, Police Stations, Fire Stations
 - Schools, Grocery stores



Status

- Developing Roadmap - September 2002

- Questions - ???

**Appendix B: Self-Healing Infrastructures Initiative
First Draft of Slide Presentation Proposal
MIT Version 9/17/02**



**Self-Healing Infrastructures Initiative
First draft of slide proposal
MIT version
9/17/02**

Self-Healing Infrastructure Initiative
Page 1
September 17, 2002 DRAFT – DO NOT QUOTE OR CITE

MIT  Sandia National Laboratories



Overview

- **I. Challenges and Vision**
- **II. National Vulnerability Assessment**
- **III. Risk Management Strategies**
- **IV. Moving Toward Self-Healing**
 - ❖ **Information Technology for Infrastructure Surety**
 - **Enabling Technologies**
 - ❖ **Designing Organizations for Self-Healing**
- **V. Implementation and Education**
- **VI. Policy Analysis**

Self-Healing Infrastructure Initiative
Page 2
September 17, 2002 DRAFT – DO NOT QUOTE OR CITE

MIT  Sandia National Laboratories



I. Challenge #1: Growing Interconnectedness

➤ The Nation's infrastructures are *Increasingly Interconnected*, presenting *New Vulnerabilities*

❖ Examples include:

- Power Plants need upstream fuel extraction and delivery systems, on-site cooling water, down-stream waste management, and integrated communications and control with the regional power system operator.
- Many industries and organizations, such as banking, finance, and emergency response are reliant on robust, near real-time communications.
- Food Supplies need disease resistant seeds, a geographically and meteorologically robust farm sector, food storage, processing and distribution, with monitoring for health safety at many steps.



I. Challenge #2: Overlapping Responsibilities

➤ The Nation's infrastructures operate simultaneously on national, regional and local levels, with the private sector and markets acting more independently.

❖ Examples include:

- Electricity competition with investment and operational decisions made by private firms with little attention to industry-wide coordination and long-term performance.
- “Regional Transmission Organization” performance dependent on the actions of NIMBY prone State and local permitting agencies.
- Similar trends affecting investments (or lack thereof) in fuel refineries, and fuel distribution and storage.
- Growing competition for uses of water (cities, agriculture, etc.) as infrastructures age and surplus supplies dwindle.



I. Challenge #3: Coordination Across Levels

- **Out of sight/Out of mind?**
 - ❖ **Recognizing Complexities** and where they help or hurt infrastructures' vulnerabilities.
 - ❖ **Recognizing Interdependencies** and how these contribute to potential cascading impacts.
- **Looking under lampposts?**
 - ❖ **Certain infrastructures** are well understood and often well prepared for "contingencies." Daily power system and water system operations are an example. Which ones aren't, and need to get on the radar screen?
- **Falling through cracks?**
 - ❖ **To be relevant the technical and analytic aspects of the program** must be tailored to the needs of end-users, at Federal, state and local levels, both public and private. **Bringing such people together is beneficial on its own.**



I. Overall Vision

- **Objective:**
 - ❖ **To develop the capabilities that would allow the nation's interconnected infrastructures to be self-healing**, i.e. to maintain minimum functionality or rapidly restore their functions and protect their assets under malevolent attacks and other disturbances.
- **Approach:**
 - ❖ **This would be achieved by developing knowledge and tools to put in place the organizational structure and processes, science and technology, as well as the social and political support.**
- **Products:**
 - ❖ **These capabilities will enable the infrastructures to be aware, active and adaptive.**
 - ❖ **To tailor the program from the beginning to address the needs of end-users.**

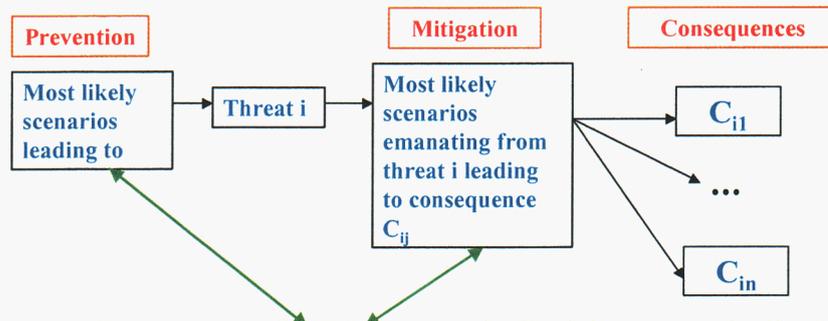


II. National Vulnerability Assessment

- Infrastructure analysis will assess vulnerability
 - ❖ But which vulnerabilities are most important?
- Program will identify threats with greatest consequences through scenario-based approach
- “Consequences” combines infrastructure vulnerability and potential for damage
 - ❖ Loss of life
 - ❖ Destruction of assets
 - ❖ Economic effects flowing from attacks
- Developing a comprehensive list of scenarios may not be feasible in all cases; incompleteness is an issue



II. Risk Assessment



- Risk Management (scenario-based; defense in depth)
- Policies Regarding:
 - How secure is secure enough?



II. Products And Methods

- **Full risk assessment**
 - ❖ Synergy with NISAC models and data
- **Case studies**
 - ❖ Apply tools in local areas as interim step
 - ❖ Seek partnership with urban, rural locations for data
- **Infrastructure vulnerability scenario studies**
 - ❖ Goal is to produce relative risk rankings
 - ❖ “Generic,” geography-independent risk assessments
- **Probabilistic risk assessment methods; system dynamics; agent-based modeling**



II. Setting Priorities

- **Program will create thousands of scenarios**
- **Prioritization is vital**
- **Terrorists are strategic actors**
 - ❖ Can't reliably assign probabilities to attack scenarios
 - ❖ Can assign consequences to successful attacks
- **Uncertainty in estimation of vulnerability and consequences**
 - ❖ Elicitation of judgment from wide range of experts
 - ❖ Multiple modeling methods to give confidence estimates are reasonable
- **Other ranking methods will be explored**

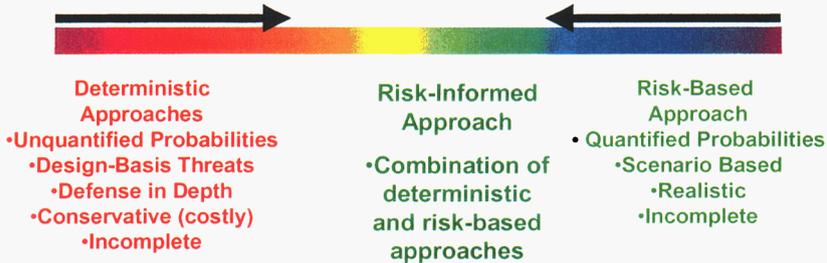


III. Risk Management Strategies

- **What should be done to reduce significant risks?**
 - ❖ **By how much could risk be reduced?**
 - ❖ **Using which policies?**
 - ❖ **Who pays/what incentives?**
- **Program will perform two sets of risk reduction studies**
 - ❖ **Scenario-based risk management**
 - ❖ **Deterministic approaches**
- **Combining them is the basis for risk-informed threat management**



III. Risk-Informed Threat Management





III. Scenario-based Risk Management

- The significant scenarios from the vulnerability assessment are the basis for risk management
- Analysis recommends measures that cost-effectively reduce risk
 - ❖ If risks are unacceptable, reduce probability/consequences of dominant scenarios
 - ❖ For lower risks, consider costs (decision analysis)



III. Deterministic Approaches

- Incompleteness of the scenario list is an issue
- Program will research methods for handling “unforeseen” threats
 - ❖ Concept of “design-basis accidents” in nuclear industry a starting point for “design-basis threats”
 - ❖ Scenarios are still useful
- Building “self-healing” infrastructures provides broad capabilities that do not respond solely to anticipated threats



IV. Moving Toward Self-Healing

- **Vulnerability Assessment Examines Current Infrastructures in Light of New Threats**
- **Self-healing Will Require New Knowledge and Tools**
- **Three Thrusts of Research Effort**
 - ❖ **Information Technology for Infrastructure Surety**
 - **Enabling Technologies**
 - **Condition assessment**
 - **Sensors, monitoring, decisions**
 - ❖ **Designing Organizations for Self-Healing**



IVA. Information Infrastructure - Key Issues -

- **US information Infrastructure - Vulnerability Measures**
- **Information Infrastructure Used by Other Infrastructures**
- **Information Infrastructure Needs for Content Transmission**



IVA. Information Infrastructure Vulnerability

- **Potential Targets for Terrorism**
 - ❖ **Target Types & Damages**
 - ❖ **Diffusion Potentials of Damages**
 - ❖ **Contingency Responses-Modes**
- **Potential Target for Other Disruptions**
 - ❖ **Types of Vulnerabilities & Spillover Effects**
 - ❖ **Current vs. Alternative « Protection »**
- **Synergy With Sandia Critical Infrastructure Surety Program**



IVA. IT Infrastructure & Other Infrastructures

- **Information Infrastructure Used by Other Infrastructures**
 - ❖ **Mutual vs. distinct linkages**
 - ❖ **Interdependences, spillover effects**
- **Critical Infrastructure Systems in the Information Age**
 - ❖ **Interdependencies & mutual dependencies**
 - ❖ **Human-infrastructure interactions**
- **Interconnections with Socio-Economic Systems**
 - ❖ **Connections in 'loosely coupled' behavior systems**
 - ❖ **Linking heterogenous functions & structures**

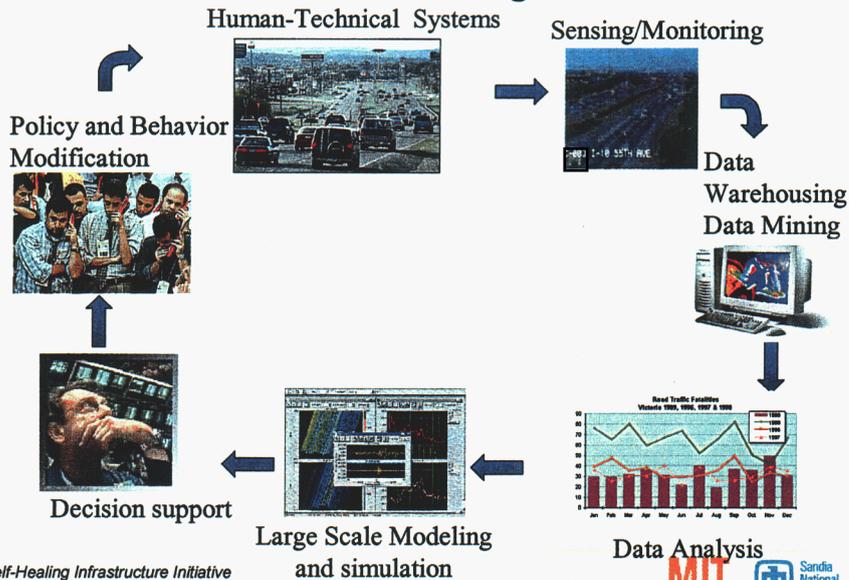


IVA. Information Infrastructure IT Needs for Content Transmission

- IT-Tools to Support 'Best-Uses' of Information from Diverse & Distributed Sources & Supporting Institutions
- Tools for Contextualization, Improved Uses of Information on Terrorism & Other Disruptions
- Value-added of Tools as Agent Based Simulation
- Methods for Managing Trade-offs: Volume vs. Utility; Transparency vs. Vulnerability; etc.
- Robust Organizational & Managerial Content Support



IVA. Critical Infrastructure Systems in the Information Age





IVB. Enabling Technologies

- **Integrated Simulation for Interconnected Infrastructures**
- **Mechanisms of Condition Assessment**
 - ❖ **Anticipatory sensing**
 - ❖ **Data distribution, integrity, aggregation**
 - ❖ **Adaptive detection**
 - ❖ **Decision robustness**



IVC. Designing Organizations For Self-Healing

- **Organizational resilience and self-healing in face of attack may be more important than resilience of physical systems**
- **Not everything can be automated, and automation can become a source of vulnerability**
- **Not everything can be anticipated, and organizations must be capable of learning and adapting while attacked or recovering**
- **Self-healing organizations must be able to operate under a wide range of conditions – normal circumstances, crises, and slow accretion of small challenges intended to induce chaos**
- **Operating under the constant threat of crisis and chaos places an unusual burden on people for (1) detection and situational awareness, (2) dissemination of information to coordinate distributed action, (3) imagination, and (4) broad action capabilities (requisite variety)**



IVC. What Do We Know?

- **High Reliability Organizations** such as nuclear power plants, air traffic controllers, and aircraft carriers are characterized by **unusual awareness of the current situation and imagined possibilities, encouragement of diverse interpretations, commitment to resilience, and deference to local expertise**
 - ❖ **Successful crisis mitigation depends on shared understanding of critical functions, substitutability of personnel and careful scripting of initial actions**
 - ❖ **Plans and resources prepared in advance become the building blocks of effective responses**
 - ❖ **Pre-crisis planning and anticipatory exercises have learning value in revealing gaps and diversity of viewpoints prior to crises and in building effective, trusting relationships**



IVC. What Do We Need To Know?

- **How much do separate infrastructure elements have to coordinate? How can we organize local, regional, and global networks to build flexible information sharing and joint action capabilities?**
- **Which organizations in these networks should be “high-reliability”?**
- **What happens when “high-reliability” organizations have to integrate their actions with “low-reliability” organizations?**
- **How can we prepare for different kinds of crises which may have distributed locations, unanticipated impacts, etc. and no one authority in charge?**
- **How does small-scale simulation practice “scale up” to large-scale disaster response?**
- **How do we develop new ways of mapping or assessing capabilities, interrelationships, and readiness for crises?**



V. Implementation and Education

- **Education and Training in Infrastructure-Operating Organizations is Usually:**
 - ❖ Highly decentralized and variable
 - ❖ Often misaligned with adult learning principles and organizational learning principles
 - ❖ Not focused on prevention or “self-healing” concepts

- **Educational Institutions Are Generally:**
 - ❖ Focused on research rather than implementation
 - ❖ Lacking consensus on recommended implementation strategies and practices

- **A Successful Program Will Translate Research into Capability and Action**



V. Implementation of Research Findings

- **Success Will Create A Climate of Learning, Experimentation, and Action That Translates Research into Change and Increased Capability**
 - ❖ Current state assessment of implementation capability among the interconnected infrastructure organizations in a defined region
 - ❖ Case studies on translation of cutting edge research into systems change initiatives relevant to prevention and “self-healing” infrastructure
 - ❖ Identification of implementation implications associated with threats not identifiable through probabilistic risk assessment methods
 - ❖ Exploration of metrics and methods to foster communications, feedback, and continuous improvement during implementation of systems change initiatives on prevention and “self-healing”
 - ❖ Establishment of our own project “infrastructure” to translate research findings into education and implementation initiatives



V. Education to Support Prevention and Self-Healing Infrastructures

- **Success Requires Getting the Right Knowledge to the Right People at the Right Time**
 - ❖ Educational stakeholder analysis among infrastructure elements within a defined geographic area
 - ❖ Current state assessment of learning methods associated with education on prevention and “self-healing” capability
 - ❖ Identification of education implications associated with threats not identifiable through probabilistic risk assessment methods
 - ❖ Development of “engineering systems studies” on the principles of prevention and self-healing within the interconnected infrastructure learning modules
 - ❖ Development of relevant professional education seminars and university curricula



VI. Policy Analysis Customized to Infrastructures Selected

- **Institutions & Decision Contexts**
- **Social Dimensions & Constraints**
- **Methods & Approaches**



VI. Policy Analysis Institutions & Decision Contexts

- **Identify Infrastructure(s) Specific Actors & Agents**
 - ❖ Key players in private & public sectors
 - ❖ Legal & legislative parameters
 - ❖ Defining 'Security' -- how secure is security?
- **Define Relevant Decision Contexts & Levels**
 - ❖ Formal vs. informal locus & process of decision
 - ❖ Bargaining Systems of "Games" & Nature of 'utilities', payoffs
 - ❖ Modes of consensus - forging bargains
 - ❖ Decision disconnects – institutional & or behavioral
- **Determine Policy Constraints versus Parameters of Permissible Action**
 - ❖ Type of constraints – cost, legal structure, etc.
 - ❖ Implicit vs. explicit parameters of permissibility



VI. Policy Analysis Social Dimensions & Constraints

- **Prevailing Perceptions of Opinion Leaders**
- **Types of Policy Debates in Public Forums**
- **Profiles of Dominant Contentions – who says what, when, and how?**
- **Nature of Transmission Mechanisms – for information, ideas, posture, etc.**
- **Range of Social views of Expected Outcomes - who gets what, when, how?**



VI. Policy Analysis Methods & Approaches

- **Context Analysis:**
 - ❖ Focus on institutional contexts & linkages
 - ❖ Private and public sector
- **Interest Analysis:**
 - ❖ Focus on interests of key actors, constituencies & stakeholders
 - ❖ Identify nature of trade-offs, gains & losses
- **Levels Analysis:**
 - ❖ Mapping interdependences among local, regional, national
 - ❖ Tracking international infrastructure-related contexts and interests

Self-Healing Infrastructure Initiative
Page 31
September 17, 2002 DRAFT – DO NOT QUOTE OR CITE



Distribution:

MS0188 1011 D. L. Chavez (LDRD Office)
MS0451 6500 S. G. Varnado
MS0455 6517 R. S. Tamashiro
MS0455 6517 S. Y. Goldsmith (8)
MS0750 6116 D. J. Borns
MS0318 9216 D. C. Barton
MS1138 6533 J. H. Ganter
MS0839 16000 R. L. Craft
MS1138 6531 B. K. Cook
MS9018 8945-1 Central Technical Files
MS0899 9616 Technical Library (2)
MS0612 9612 Review & Approval Desk for DOE/OSTI

