Surety Theoretics: The Forest or the Trees?

Michael Senglaub Ph.D.
Sandia National Laboratories
PO Box 5800 MS0435
Albuquerque, NM 87185
mesengl@sandia.gov

Abstract. Periodically we need to re-examine the objectives and the efforts associated with a field of study. In the case of "surety" which comprises, safety, security and reliability we need to be sure that theoretical efforts support the needs of systems and design engineers in satisfying stakeholder requirements. The current focus in the "Surety" areas does not appear to address the theoretical foundations needed by the systems engineer. Examination of papers / abstracts demonstrate significant effort along the lines of thermal hydraulics, chemistry, structural response, control theory, etc. which are analytical disciplines which provide support for a Surety theoretic but do not constitute a theoretic. The representations currently employed, fault trees etc., define static representations of a system, not the dynamic representation characteristic of response in abnormal, hostile or under degrading conditions. Current methodologies would require a semi-infinite set of scenarios to be examined before a system could be certified as satisfying a Surety requirement. The elements that are required of a Surety theoretic must include; (1) A dynamic representation of the system. (2) The ability to automatically identify terminal states of the system. (3) Determine the probabilities of specified terminal states under dynamic conditions.

Introduction

Engineering design and development is a complex trade between many disciplines, technologies and system objectives. The systems engineer must identify objectives and requirements and formulate metrics that can be used by the design teams to assess the viability of concepts in satisfying the design and development objectives. One of the more difficult tasks of the systems and design engineer is the assurance that the final product satisfies those requirements established through analysis, capture or edict. It is the certification / verification element of the design and development problem that is being addressed in this article. How do we ensure that the surety requirements of a system are being satisfied?

In the following sections we examine the requirements of a surety theoretic that will support the efforts of the design and development engineer. Identifying the needs of the design and development engineer enable us to ascertain the gaps between the current state of surety technology and these needs. There will follow in later sections speculations on technologies that might provide the theoretical and support foundations needed by the systems engineering community to form a robust surety analysis and design environment.

State Of Affairs.

Surety Definition. Surety is a concept which may have been coined at Sandia National Labs and constitutes an emphasis on the integration, throughout the life-cycle, of safety, security, and reliability. Surety is establishing the confidence that a system will operate in an acceptable manner in normal, hostile, and abnormal environments. "Acceptable manner" is dependent on the system, its function/mission and

DISCLAIMER

the environment it must operate in. In many arenas this means having to deal with inappropriate use. The problem faced by today's systems and safety engineers is to design a fool proof system. The problem as we are well aware nature seems to continually improve the "fool".

In a traditional systems engineering design environment, safety, security and reliability are considered as part of the "ilities" of design and often are not afforded the emphasis that is required. Safety and security are considered as adjunct efforts by isolated engineers loosely associated with a design effort. The concepts of "surety" refocus design effort to ensure a greater emphasis on these aspects of design. The greater emphasis results in design processes, reviews, and technology choices at system levels to enhance the surety of a system.

Systems & Design Requirements. The current approach employed by surety analysts is extremely labor and cost intensive because of the number of potential scenarios which must be assessed. The design engineer must be able to quantitatively assess the surety of a system concept without impacting the solvency of a company or the GNP of a country. This problem has resulted in a tendency to mitigate examination of a broad spectrum of concepts and technologies.

The fundamentals of a surety theoretic must possess a number of attributes as defined below: (1) The theoretic must assess system surety from a dynamics perspective. In hostile or abnormal environments the systems respond in a transient manner to forces and actions being imposed on them. Can we realistically represent a system statically as it is being crushed or subjected to extremes in temperature? Under these conditions, structural responses are changing, effective circuits are changing and evolving, constituting emergent designs that were not considered originally by the design engineer.

(2) The theoretical framework must provide a mechanism for assessing the probabilities of acceptable terminal states of the system. The large numbers of scenarios, and dynamic configurations that may evolve in a system requires a technique that can assess probabilities of terminal system states. The ability to quantify high probability terminal states provides the design engineer with a technology for quickly assessing design architectures and system configurations to lower or eliminate undesired system risk. This theoretic needs to provide the design engineer, in a concept development effort, to bound the probabilities of terminal system states exhibiting high risk. Recognizing the upper limits (or lower limits) of the surety of a concept can enable rapid assessments of the viability of a proposed architecture in satisfying surety requirements.

(3) The theoretical framework must enable the integration of new analytical technologies into a this framework as they prove their utility in solving aspects of the surety objectives. Scenario based approaches to surety analysis are highly susceptible to errors on the part of design engineers. It is usually the scenario that was missed during the design process that results in the system failure. Modern search techniques could aid in the search for common fault configurations, or state transitions that lead to unacceptable terminal system states. The theoretic should also look to the future and technologies that may provide the computational foundation for comprehensive surety analyses that can capture all possible dynamic terminal states for a system configuration.

(4) A less recognized requirement, (it may constitute a solution to a theoretic) is the ability to define transformations between design configurations and fault configurations. Given the ability to define these transformations and attribute an "energy" function with these trans-

formation we provide another methodology for assessing the likelihood of transitions to these unacceptable terminal states. Development of energy of transitions may allow us to employ quantum type principles to problems of surety, recognizing that quantum mechanics is a theoretic for addressing the states of compounds, and nuclear systems.

Current Efforts.

Searches for efforts in the theoretical development of surety reveal a significant gap to exist between activities related to surety and the surety fundamentals needed to address the requirements delineated earlier. A number of literature searches were conducted in an effort to locate surety theoretical efforts. The best literature search reveled keyword distributions emphasizing technologies that might support a theoretic but only a handful of papers that explore these foundations. Of the 182 abstracts focusing on safety, security, and reliability theoretics, 1579 unique keywords were identified, 240 of which had 2 or more citations. The first 12 categories reflected generalizations associated with the directed field of endeavor, such as, safety, safety analysis, etc. The remaining 228 begin to identify areas of specialization within the border class of surety topics.

Screening the remaining keywords for topics which might address the foundations or fundamentals of surety we arrive at a reduced set of topics delineated in the next table.

Table 1: Potential literature citations addressing surety fundamentals.

Keyword	Citations	References of Potential Theoretic Value
Failure Analysis	17	Non found
Modeling	12	Non found
Fault Tree Analysis	8	~ An AI extension of the computer aided fault tree synthesis (CAFTS) environment
Fuzzy Set Theory	7	~ Assessment of the potential applicability of fuzzy set theory to accident progression event trees with phenomenological uncertainties ~ Application of fuzzy - sets methods for calculating the reliability of safety systems of NPP ~ The application of fuzzy mathematics in safety analysis
Graph Theory	7	~ A graph-theoretic approach for timing analysis and its implementation ~ Digraphs and fault trees
Dynamic Security Analysis	6	~ A general approach to evaluation of secure systems
Probabilistic Safety Analysis	6	~ Uncertainties in system analysis: probabilistic versus nonprobabilistic theories
Algorithms	5	~ New algorithms for fault trees analysis
Stability	5	~ Fourier methods for estimating power system stability limits

Table 1: Potential literature citations addressing surety fundamentals.

Keyword	Citations	References of Potential Theoretic Value
Bayes Methods	4	~ Systematic Bayes prior-assignment by coupling the mini-max entropy and moment-matching methods
Systems Analysis	4	~ On reliability theory and its applications
Formal Logic	3	Non found
Probabilistic Safety Assessment	3	~ Probabilistic dynamics: need and methods
State Estimation	3	~ State estimation and unobservable networks
Chaos/Non-linear Dynamics	2	~ Stochastic non-linear reactor model near the Hopf bifurcation
Markov Processes	2	Non found
Mathematical Model	2	Non found
AI & Neural Nets	2	~ Probabilistic risk assessment: a look at the role of artificial intelligence ~ Security analysis using fuzzy logic and neural network
Sparse Vector Methods	2	Non found

The list in Table 1 is not intended to list all applicable references but to provide an indication of the types of topics which might relate to theoretical foundations of security. The first column captures a keyword or phrase that might relate to theoretical work, the second column identifies the number of corresponding citations and the last column identifies the titles of papers which might provide theoretical insights to the problems of surety. The majority of the theoretical work in the literature relates to reactor physics, thermal hydraulics, control theory, reliability theory, probability theory and modeling power systems from operational perspectives. The topic not found is the framework for performing dynamic systems analyses of surety objectives.

Why A Theoretic?

Gap Analysis. The current approach to surety analysis can be characterized as a scenario based steady state analysis of a system. The first problem with this approach is that in order to verify a systems compliance with a surety requirement, an infinite number of scenarios may need to be analyzed. The practicality of attempting to explore even a representative subset of scenarios is not within the scope of any design effort. The result is that qualitative arguments must be employed in place of quantitative techniques to verify a systems surety requirements.

A second problem that must be addressed is the transient nature of surety problems. The infinite number of scenarios alluded to earlier is compounded be the fact that a system in abnormal and hostile environments is evolving on a time scale commensurate with the external drivers. Taking a cue from transient numerical analysis techniques we might approximate the dynamic aspects of surety analysis by examining scenarios and fault trees taken at discrete points in time. The number of scenarios increases dramatically with this

approach, and the difficulty of propagating a fault tree through time is not likely to be the most cost effective approach.

Caution. It must be realized at this point that following discussions and the technologies to be discussed later are speculations on technologies that might be brought to bear in a search for a surety theoretic. Significant amounts of work needs to be performed to validate techniques and methodologies.

Theoretics. Engineering and science disciplines possess mathematical constructs that capture a response under external influences. Structural analysis possesses statics and dynamic models which describe the behavior under mechanical drivers, the equations of electro-magnetism provide the framework needed to design a circuit or assess the trajectory of a charged particle in a magnetic field. The efforts involve the search for techniques to solve the fundamental equations in a particular field. The disciplines associated with surety do not possess these fundamental laws representative of a systems response to external drivers. In order for the science of surety to advance as a professional discipline a search for theoretical foundations need to be pursued. With a theoretic in hand we can begin to explore techniques for solving problems associated with surety.

Representations. The first step is to find a representation of systems that can capture aspects of a system from its color to its dynamic response to crush. One representation that may possess qualities that satisfy the requirements delineated earlier is a hybrid crisp and fuzzy state space characterization of a system. The general form for first order non-linear dynamic equations as defined by Strogatz [S94] is provided in equation 1.

$$\dot{x}_i = f_i(x_1, \ldots, x_n) \qquad \text{Eqn. 1}$$

The index i ranges from 1 to n. The equation is general there exists n time dependent state variables and n mapping functions. The mapping functions $f_i(\ )$ are independent of time in this formulation but should be expanded to include time for surety problems.

$$\dot{x}_i = f_i(x_1, \ldots, x_n, t) \qquad \text{Eqn. 2}$$

This is needed to handle aging, radiation embrittlement, fatigue and other temporal conditions as well as the basic transient aspects of surety problems. A discrete representation for the dynamics equations in equation 1, was provided by Kim, et.al. [K95] and shown in equation 3 and 4. These equations were part of a discussion of stability in fuzzy state space models.

$$\hat{x}(k+1) = f(\hat{x}(k), \hat{u}(k)) \qquad \text{Eqn. 3}$$

$$\hat{x}(k+1) = F(\hat{x}(k), \hat{u}(k)) \qquad \text{Eqn. 4}$$

In these equations x represents the state of the system at discrete times k and k+1, u is the input while f( ) is the crisp mapping between states and in equation 4, F( ), is the fuzzy mapping between states. Equation 4 is of particular interest due to a transformation involving semantic fuzzy mappings which lead the to a set of equations defined by equation 5.

$$x(k+1) = \sum_{i=1}^{m} \alpha_i (A_i \cdot x(k) + b_i \cdot u(k)) \qquad \text{Eqn. 5}$$

The vector description of the system has been transformed into a matrix representation. The equation can be interpreted as a representation of a state transformation which involves all fuzzy rules/relations as well as considering all transformations based on a weighting distribu-

tion α_i. The term contained within the brackets of the summation is a mathematical description of a fuzzy rule or relationship. The details of the conversion should be examined in the original paper by Kim et. al.[K95]. What we may be seeing is a potential for defining state transitions based on fuzzy rules or dynamics that permit a surety analyst to treatment multiple transitions as well as associating transition likelihoods.

The ultimate representation will not be either a crisp state representation or a fuzzy representation but some hybrid of these technologies. A second state representation was defined by Grantner[G94]. In this representation A set of equations have been defined to model a dynamic equation. The are reproduced below.

$$Z = X \bullet R(y_F)$$
$$z_c = DF(Z) \qquad \text{Eqn. 6}$$
$$Y_F = f_{y_F}(X, y_F)$$

X and Z represent a set of fuzzy inputs and outputs, while DF is the defuzzification operator, $R(y_F)$ is the linguistic model, z_c are the crisp outputs, f_{yF} is the mapping to successor states, and Y_F is the fuzzy successor state. This formulation needs to be generalized on two levels. The first is the definition of successor state needs to be expanded to include crisp as well as fuzzy components. The mapping function must be modified or split to define a crisp component as well as the fuzzy component, something like equation 7. To clean up some notation Y(k+1) is the successor fuzzy state, and y(k+1) is the crisp component of the successor state.

$$Y(k+1) = F(X, Y(k), y(k))) \qquad \text{Eqn. 7}$$
$$y(k+1) = f(X, y(k), Y(k))$$

The second extension to these equations is to convert the mapping functions to include a time dependent component. Surety problems in general do not exhibit behaviors that might be represented by a single time constant, this complicates the problem. An interesting technique employed in nonlinear dynamic analysis is to expand the dynamics equation in terms of "long" time and "short" time(s), this enables the analyst to track phenomena on independent time scales. Before this approach is fully recommended stability and representational analyses need to be conducted to assess the fidelity of the approach, similar to the work of Kim et.al.[K95].

Dynamic representations of systems enables us to explore the stability of a system by selecting from the technique rich fields of non-linear dynamics and chaos. We might be able, through analysis, to identify stable nodes, orbits in phase space and draw conclusions concerning system stability by invoking theorems such as Poincare's theorem.

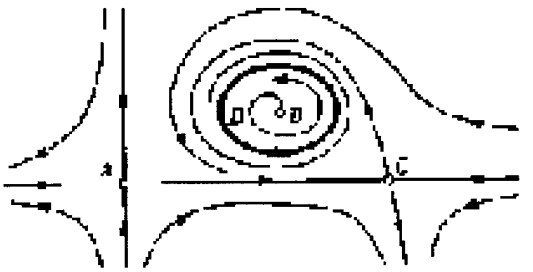

Figure 1. Phase plot.

Poincare's theorem states that if a stable phase space orbit exists such a D in Figure 1, any trajectory with initial conditions within the orbit will remain there. The system will not achieve run-away conditions. The design engineer can search for design conditions maximizing the size of these orbits, ensuring sufficient design margin, and introduce design constraints that ensure initial conditions, temperature, impulse, etc. are at levels falling within the phase space stable orbit. There are a number of additional approaches from these fields which may be used in during concept development to assess

designs which are inherently stable.

State representations and the desire to identify probabilities associated with terminal states leads one to consider the mathematics of quantum mechanics. In quantum mechanics we are endeavoring to identify the states of an atom, compounds or a nucleus. The state of the system is defined by a state vector defined in "ket" notation as: $|\Psi\rangle$. Once the state vector is known the expected value for any attribute can be determined. State changes are dictated by Schroedingers equation.

$$((ih)/(2\pi))\frac{\partial}{\partial t}|\Psi(t)\rangle = \hat{H}|\Psi(t)\rangle \qquad \text{Eqn. 8}$$

h is Plank's constant, H is the Hamiltonian operator and Ψ is the state vector. If the Hamiltonian is time independent, the solution to Schroedinger's equation is;

$$|\Psi(t)\rangle = e^{-i2\pi\hat{H}(t/h)}|\Psi(0)\rangle = \hat{U}|\Psi(0)\rangle \qquad \text{Eqn. 9}$$

U become the evolution operator. Why is there interest in this technology? The time independent Hamiltonian is unitary and invertible which means that the solution to equation 9 can provide forward or reversed time calculations. How useful would it be to identify an unacceptable terminal state, perform the inverse calculation and identify all initial conditions that could lead to the terminal state? There is work being performed at Stanford[W96] which is exploring concepts of quantum computing in which the system dynamics is modeled through the Hamiltonian and the transitions or the propagation of the state vector is defined by Schroedingers equation.

Potential Solution Technologies. This section is highly speculative but the objectives delineated are features which would provide the systems and design engineers with tools that could be used in the search for system concepts that satisfy surety requirements. The first area involves the capture of the combinatorics associated with identifying unacceptable terminal system states. A number of people at Sandia National Labs have been exploring the multi-Graph Architecture (MGA) tool being developed at Vanderbilt University[S95] as a foundation for state space analyses of systems. The tool provides a capability of transforming discrete event systems(DES) into ordered binary decision diagrams (OBDD) for use by symbolic binary analysis operators[S96]. There has been demonstrated utility in the OBDD approach in hardware verification, testing, among other difficult combinatoric problems.

Complex systems can produce large amounts of combinatoric information which may not be analyzable by a team of engineers. Pattern recognition technologies could be modified to search for patterns in the state information that are common to unacceptable terminal conditions. This would guide the design engineer in seeking alternate solutions that mitigate unacceptable terminal states such as fault conditions.

Genetic programming or evolutionary programing technologies could also provide insight into design configurations that could result in fault configurations under sets of environmental drivers. recognizing the basic elements of the design configurations and introducing specialized "abnormal environment" operators, genetic programs(GP) could be tasked with finding all possible fault configurations that result in unacceptable states for a sub-system. A great deal of work has been performed in which GP's have been tasked with designing circuits, structures, and algorithms. This technology in conjunction with the state space representations and search algorithms could provide a foundation and solution

hybrid that would make surety analysis tractable.

Conclusions

The technologies and theoretics needed to certify a system surety requirement are not in place. Technologies are on the horizon which may enable a theoretic to be defined but a number of modifications must be made to enable these technologies to be implemented. Much of the effort expended in the surety arena is directed toward improving physical modeling capabilities such as thermal hydraulics, or reactor physics, but little is being done to explore the larger surety issues. Systems are dynamic, are becoming more complex, and the demands being placed on the design engineer more stringent. As systems and design engineers we need the tools to do our job, a theoretic and solution techniques to solve surety problems. The technologies, the computational power, and the imperative for advancements in surety theoretics are in place, we need to explore and define the foundations needed to address surety in a comprehensive mannar. Studying the single tree adds little to the overall understanding of a forest ecosystem.

REFERENCES

[K95] W. Kim, S. Ahn, W. Kwon. "Stability analysis and stabilization of fuzzy state space models". Fuzzy sets and systems, Elsevier, 1995.

[S94] S. Strogatz, *Nonlinear Dynamics and Chaos*,Addison-Wesley, 1994, ISBN 0-201-54344-3.

[G94] J. Grantner, M. Patyra, Fuzzy logic Finite State Machine Models For Real Time Systems, 0-7803-2125-1/94, IEEE

[S96] J. Sztipanovits, A. Misra: "Diagnosis of Discrete Event Systems Using Ordered Binary Decision Diagrams", Proc. of the 7th International Workshop on Principles of Diagnosis (DX96), pp. 232-238 Val Morin, Quebec, Canada, October 13-16, 1996

[S95] Sztipanovits, J., Karsai, G., Biegl, C., Bapty, T., Ledeczi, A., Misra, A., "MULTIGRAPH: An Architecture for Model-Integrated Computing," Proc. of the ICECCS'95, pp. 361-368, Ft. Lauderdale, Florida, Nov. 6-10, 1995.

[W96] Williams, *Tutorial SP2: Quantum Computing*, 13th National Conference On Artificial Intelligence, AAAI & IAAI, August 1996, Portland, Oregon.

Sandia is multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-ACO4-94AL85000.

Report Number (14) SAND--97-1920C
CONF-970703--

Publ. Date (11) 1997 10
Sponsor Code (18) DOE/DP, XF
UC Category (19) UC-706, DOE/ER

DOE