SANDIA REPORT

SAND2009-5569
Unlimited Release
Printed September 2009

Final Report: Impacts Analysis for Cyber Attack on Electric Power Systems (National SCADA Test Bed FY09)

Jason E. Stamp, Judith D. Gardiner, and Randall A. LaViolette

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-AC04-94-AL85000.

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.osti.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 ordering: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2009-5569
Unlimited Release
Printed September 2009

Final Report: Impacts Analysis for Cyber Attack on Electric Power Systems (National SCADA Test Bed FY09)

Jason Stamp, Ph.D.
Energy Systems Analysis
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1108
jestamp@sandia.gov

Judith D. Gardiner, Ph.D.
Ohio Supercomputer Center
The Ohio State University
1224 Kinnear Road
Columbus, OH 43212
judithg@osc.edu

Randall A. LaViolette, Ph.D.
Advanced Analytic Concepts
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1235
ralavio@sandia.gov

Abstract

The development continues for Finite State Abstraction (FSA) methods to enable Impacts Analysis (IA) for cyber attack against power grid control systems. Building upon previous work, we successfully demonstrated the addition of Bounded Model Checking (BMC) to the FSA method, which constrains grid conditions to reasonable behavior. The new FSA feature was successfully implemented and tested.

Acknowledgments

Thanks to the National SCADA Test Bed (NSTB) program at the United States Department of Energy's Office of Electricity Delivery and Energy Reliability which provided the funding for this research.

Executive Summary

FSA is an important part of IA for the power grid, complementing steady-state approaches. It enables the simultaneous evaluation of myriad dynamic trajectories for the system, which in turn facilitates IA for whole ranges of system conditions simultaneously. Given the potentially wide range and subtle nature of potential control system attacks, this is a promising research approach. In this report, we will explain the addition of BMC to the previous FSA work and some testing/simulation upon the implemented code using a two-bus test system. The current FSA approach and code allow the calculation of the acceptability of power grid conditions post-cyber attack (over a given time horizon and for a specific grid topology). Future work will enable analysis spanning various topologies (to account for switching events), as well as an understanding of the cyber attack stimuli that can lead to undesirable grid conditions.

Contents

Executive Summary **6**

1 Introduction **11**

1.1 Research Goals 11

1.2 Project Deliverables 12

2 Theoretical Development **13**

2.1 Algorithm Formulation 13

2.2 Metrics for Grid Performance 15

2.3 Sensitivity Analysis for Control Setpoints 15

3 Testing and Results **17**

4 Conclusions **21**

5 Recommendations **23**

Appendix

A References **25**

B Acronyms, Symbols, and Abbreviations **27**

C Glossary **29**

D For More Information **31**

List of Figures

3.1 Two bus test system. 17

List of Tables

B.1 Acronyms 27

B.2 Symbols 27

B.3 Abbreviations 28

C.1 Definitions 29

D.1 Contact Information 31

Chapter 1

Introduction

The IA program at Sandia National Laboratories (SNL) is continuing to investigate modeling of power system dynamic behavior caused by cyber attacks using FSA. Last year's work (detailed in reference [1]) successfully analyzed a two-bus model and converted its continuous-time-domain representation into a finite state system. A significant missing feature of the previous work is an inability to evaluate the acceptability of the system with bounded inputs (the former work has assumed unbounded inputs); this is successfully addressed in the FY09 work using a BMC approach.

1.1 Research Goals

The goal of the FSA research is simply to improve the tractability of grid dynamic analysis under cyber attack conditions. The space of attack possibilities is very high and is not solvable exhaustively, even when considering only the power system's static model (although we can sort this space heuristically). Adding the element of time to the problem makes impossible the evaluation of any significant part of the potential system dynamic trajectories. Current practice involves selecting one (or at best a very few) dynamic grid responses for analysis.

The FSA approach changes all of this. Assuming that we can sort the grid's permutations into interesting and uninteresting groups, we can apply the FSA to the former in order *to immediately and exhaustively evaluate all of the dynamic response trajectories associated with any grid topology* (for a given time horizon). There are many existing approaches for the sorting problem, but to date there has not been an way to approach the dynamic analysis. The FSA method fills this need, and it is a necessary enabling complement for effective IA.

1.2 Project Deliverables

The budget for the IA project in FY09 was $100k, and four deliverables were proscribed:

- Metrics for grid performance that work effectively with FSA,
- Sensitivity analysis technique for selected grid control setpoints,
- Test algorithms on representative systems, and
- Final report.

Each was met successfully (this document is the final item), with one caveat: the proposed sensitivity analysis for control setpoints was not tested due to unexpected budgetary pressures caused by the difficulty of implementing BMC in the FSA code. We will address the development of the first two requirements in the next section, although each of these are predicated on the development of BMC. That need was identified late in the FY08 research cycle, and the bulk of the work in FY09 was spent in addressing this requirement. The details of the testing are included in the subsequent chapter.

Chapter 2

Theoretical Development

Clearly, the goal of the FSA work is to understand the potential impacts to the Electric Power Grid (EPG) caused by malevolent cyber attack. To this end, we presume that a successful cyber attack against some control system will introduce a perturbation on the grid (through some cyber to physical linkage, see [2]). The effects of the perturbation will evolve dynamically within the grid, and may negatively affect load and generation.

For example, consider a potential cyber attack against the trip settings of a cyber-based distance relay for an electrical transmission line. (A distance relay constantly checks to see if an electrical line has touched the ground – which would be unsafe – by measuring the impedance between the line and ground. If the measured value is less than the the impedance of the line itself, then there is a fault. Although this is a simplified explanation, it will suffice for examples in this report.) If an attacker were to lower the trip threshold on the relay such that a period of elevated load (rather than an actual fault) caused it to trip a line, then the conditions where power is delivered to the load may become unacceptable (the voltage too low, perhaps).

2.1 Algorithm Formulation

The goal of the reachability analysis for dynamical control systems is: Given an initial region x_0 (a dense set) in state-space R^N, compute whether a "bad" state Z (described in terms of power grid metrics) can be reached in a specified time horizon T. One can imagine many ways to do this but we can immediately eliminate as impractical for all but trivial systems the idea that we could simply and directly simulate an endless number of trajectories with initial conditions in x_0 and see if they reach Z for times $t < T$. Therefore we settled on the FSA approach developed explicitly by Giorgetti, Pappas, and Bemporad [3] that involves no direct simulation of the system and in principle is able to provide a rigorous algorithmic proof of the acceptability (or not) of the system given x_0, Z, and T. We employed an implementation in Matlab[1] of [3] developed by one of the authors (Gardiner [4]), in collaboration with R. Colbaugh [5].

Helpful pedagogical discussions (with illustrations) can be found in [5, 6, 7] which we won't reproduce here; instead we'll note some of the key assumptions employed in this study. We employ throughout the framework of the FSA. In order to directly apply Gardiner's implementation of [3],

[1] commercial mathematical analysis software published by The MathWorks (www.mathworks.com)

we transformed the continuous-time nonlinear system representing the power grid (and potentially some of its control laws):

$$\dot{x} = f(x, y, u, q) \tag{2.1}$$

$$0 = g(x, y) \tag{2.2}$$

into a discrete-time linearized (affine) system to obtain the following hybrid dynamical control system [4]:

$$x'(t+1) = A_q \Delta x'(t) + B_q u(t, q) + f_q \tag{2.3}$$

for each discrete state q, where the discrete-state region is defined by a group of linear inequalities $C_q x' \leq d_q$. Physically discrete states correspond to different configurations of the power grid that result from constituent elements in-service or not, e.g., lines or generators switched on or off. Each row of C_q, d_q is a constraint that represents a half space, with the intersection of all the constraints forming a polytope in state space. Generally, if a constraint is violated, the system switches to a different q, but in this study, we studied only reachability of a constraint violation, so we stopped the calculation when either the first constraint violation or the time horizon was obtained. In effect our Z is the other side of the polytope defined by the constraints. The state variables have been rewritten as x' to highlight the fact that the algebraic variables have been eliminated by rewriting them in terms of state variables.

The FSA formulation as written in equation 2.3 is slightly different from previous work in the IA program, as it enables BMC, whereby the constraint set can be checked for all $t < T$ for a *range* of u. The power grid application of this is that potentially variable grid conditions (like uncertainty in terms of the actual loads, generation, or setpoints) can be represented as ranges in u and evaluated for constraint violations (bad states, indicating success to a cyber adversary) *all at once*, rather than by individual dynamic simulations.

2.2 Metrics for Grid Performance

The following metrics are considered for scoring FSA scenario evaluations:

1. *Amount of load supplied*: This may be less than the desired amount (either active or reactive power) as a result of automatic load curtailment, outright disconnection, or system instability.
2. *Delivery frequency at loads*: .Due to control system attack, the frequency of the AC voltage at one or more loads may be off-nominal for a significant interval.
3. *Delivery voltage at loads*: Attacks may limit reactive flow in the power grid to cause off nominal load voltage (meaning more than 5% off-nominal).
4. *System lack of stability*: The grid interconnection encounters significant periods of poorly controlled evolution.

While this is not intended to completely cover the full range of potential metrics, they will serve as a foundation for the analysis in this report. The current metrics are more suited to load delivery points; future work will consider better metrics for generator sites.

2.3 Sensitivity Analysis for Control Setpoints

FSA is suited to analyzing many types of cyber attacks. In many cases, we can assume that an adversary will cause outages on constituent elements for the power grid. A more subtle attack would be to alter the control setpoint inside one or more grid control devices.

The FSA technique has been evaluated for its suitability to analyze these subtle attacks, and there are significant advantages here. Using conventional analysis, the effects of the altered control can be evaluated pretty accurately, but each potential set of grid conditions must be considered individually.

As an example, consider the distance relay setting mentioned above. A dynamic grid simulation can determine the system dynamic trajectory based on a single set of grid conditions, after which the results can be scored based on some pre-supplied set of metrics. In contrast, the FSA method allows the advantage of understanding the reachability of Z for ranges of potential operating states. In the long run, we would like to investigate the possibility of parameterizing the control system setpoint itself, and calculate a critical value which allows Z to become reachable.

Chapter 3

Testing and Results

The two-bus test model is shown in Figure 3.1.

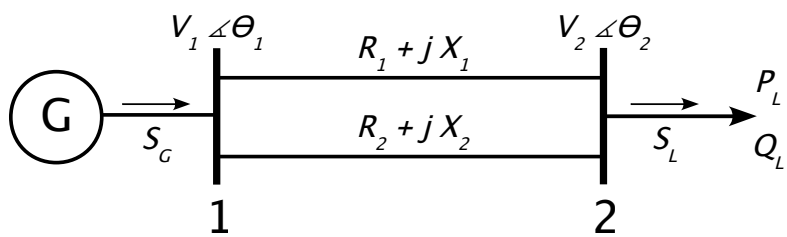

Figure 3.1: Two bus test system.

For future reference we'll note that $x = \left[\delta, \Delta\omega, E'_q, P_L, Q_L\right]^T$ and $y = [V_1, V_2, \theta_1, \theta_2]^T$. E_f for the generator is set to 1.025 (for descriptions of these variables, please see [1]). With both lines in service, the stable equilibrium conditions and values for the system variables are:

$$x_0 = \begin{bmatrix} -71.92855 \\ 0.19080 \\ 0.98302 \\ 0.18945 \\ 0.03654 \end{bmatrix} \quad y_0 = \begin{bmatrix} 0.97364 \\ 0.96449 \\ -72.08317 \\ -72.09532 \end{bmatrix} \quad u_0 = \begin{bmatrix} 1.025 \\ 0.2 \\ 0.04 \end{bmatrix} \tag{3.1}$$

Compared to reference [1], we are rolling up the generator field voltage and load base demand into a single input u. With both lines in service, a distance relay at the generator end of line 1 sensing toward the load measured $Z_1 = 14.60\angle 11.62^\circ\,\Omega$ and the relay for line 2 measured $Z_2 = 7.301\angle 11.61^\circ\,\Omega$. We would like to analyze the sensitivity of the system with respect to setpoints for these hypothetical distance relays under differing ranges of system inputs/conditions.

For this demonstration we studied one kind of perturbation, i.e., the possibility of extra reactive power demand ΔQ_L. Additional reactive power (unless accompanied by proportionate extra active power) reduces the power factor that in turn drops the voltage below acceptable levels. The FSA demonstration shows that for this model only a modest $\Delta Q_L/Q_L \geq 8\%$ is required to do this. We suspect that the actual lower limit is actually below the one we obtained but for purely numerical (not theoretical) reasons we were unable to obtain the lowest ΔQ_L needed to cause system failure (see the Recommendations section).

Therefore we considered only q corresponding to both lines active (leaving the question of control point sensitivity for future work). We chose for constraints[1] that $V_1,\ V_2 \geq 0.95$. We also set $B_0 = 0$ and obtained A_0 and $\Delta x'$ by expanding around the steady state solution x_0 of the nonlinear dynamics of the two-bus model.

We took as the perturbation to the system the addition of pure reactive load ΔQ_L, i.e.,

$$f_0 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \Delta Q_L \end{bmatrix} \tag{3.2}$$

because a positive ΔQ_L lowers the power factor that in turn can lower at least one of the bus voltages.

Again, the equations for x and y can be generally represented as

$$\dot{x} = f(x, y, u) \tag{3.3}$$
$$0 = g(x, y) \tag{3.4}$$

where $x \in R^n$ and $y \in R^m$. We won't here "drive" the system with the input u, so here u will just be a parameter and $q = 0$ (both lines in service). The first step in converting (3.3, 3.4) into a pure linear Ordinary Differential Equation (ODE) is to linearize around an equilibrium (x_q^0, y_q^0) and substitute, as follows:

$$\dot{x} = f_x \Delta x + f_y \Delta y \tag{3.5}$$
$$0 = g_x \Delta x + g_y \Delta y \tag{3.6}$$

where, e.g., $\Delta x = x - x_q^0$ and f_x is the Jacobian $\frac{\partial f(x,y)}{\partial x}$ evaluated at (x_q^0, y_q^0); here we confine our attention to $q = 0$. If g_y is invertible[2] then we can solve for Δy to get the n dimensional linear dynamics[3]:

$$\dot{x} = A_0 \Delta x, \tag{3.7}$$
$$A_0 = f_x - f_y H, \tag{3.8}$$
$$H = g_y^{-1} g_x. \tag{3.9}$$

The constraints that we care about are in $\Delta y = H \Delta x$. In particular the constraints whose violation cause a "bad" state are $0.95 \leq V_1$ and $0.95 \leq V_2$. As a consequence of the linearization and (3.9) we need only for both $H^{(1)}\Delta x$ and $H^{(2)}\Delta x$ (where $H^{(k)}$ is the kth row of H) to be less than

[1] This choice was complicated by the fact that the voltages are not state variables but the constraints are expressed here for the state variables. We took advantage of the linear approximation employed here to write the voltage constraints explicitly in terms of the state variables.

[2] Although that isn't the most general case it'll be true here.

[3] Often H is written as C but here we want to distinguish H from the C employed below to describe constraints.

or equal to 0.95, a requirement easily accomodated in the half-plane description of the constraints (i.e., $C_q x \leq d_q$). Now we have the two-bus model in the form (2.3) that we need in order to apply [3] to the reachability question, i.e., given a set X_0 in X (the state space), is the set Z where the voltage constraints are violated reachable in a finite time horizon T?

We studied the initial set generated by

$$X_0 = x_0 \pm \begin{bmatrix} 10 \\ 0.001 \\ 0.001 \\ 0.005 \\ 0.005 \end{bmatrix},$$

a ten-vertex polytope in the five-dimensional state space X. First we verified that with no perturbation (i.e, $\Delta Q_L = 0$ in Eq. 3.2), no violation of the constraints (i.e., no overlap of X_0 with Z) occurs for time horizons as long as $T = 1000$ seconds[4]. Then with $\Delta Q_L = 0.0029$, i.e., 8% of the equilibrium value for Q_L, the constraint on V_2 was violated in 4s. This value of ΔQ_L is most likely not the lowest ΔQ_L to cause a constraint violation in a reasonable time but it is as low as we could go due to the numerical difficulties in the evaluation of X_0 at subsequent discrete time steps. A fix for these difficulties is the subject of proposed work. Of course, higher values of ΔQ_L cause violations in even less time. Each of these calculations took at most a few seconds on an Intel-based laptop running Matlab.

[4]We aren't suggesting that violations occurred at $T > 1000$s, but only that we didn't examine $T > 1000$s.

Chapter 4

Conclusions

As we noted in the introduction, no amount of direct simulation would exhaustively check trajectories for constraint violations, but with this approach based on FSA, only a few seconds of processing time on a laptop running Matlab is enough to rigorously verify reachability of bad states over long times and for all trajectories emanating from the initial conditions. The bad states are characterized in terms of conventional grid metrics like voltage, system stability, etc. The current code implementation is not yet robust enough to allow sensitivity analysis for control setpoints, but the algorithm is certainly amenable to doing so.

Chapter 5

Recommendations

The demonstration that we have accomplished here gives us the confidence to recommend:

- Revise code to increase numerical robustness
- Revise code to automate features that are now manually controlled
- Discovery of precursors to failure states
- Discovery of recovery paths from failure states

As mentioned in the Testing and Results, there are numerical sensitivities that for this particular two-bus model (and the selected perturbation) limited the range and the ease with which we could obtain results. These singularity-like sensitivities (e.g., dimensional reduction of the initial set) have been encountered before in other applications [5] of this code. Avoiding these and other well-understood numerical problems will likely require revisions of the Matlab test code, which (to be fair) was intended only as a test of the feasibility of these sort of calculations and not a final, numerically robust product. Furthermore, the code could made easier to use by automating certain features that are now manually controlled by the user. We did not here exploit the ability of the present code to answer questions other than reachability. For example, this approach permits us to explore recovery scenarios not attempted here. This approach also permits us to discover precursors to failure states, which also wasn't attempted here.

Appendix A

References

[1] Jason Stamp, Randall Laviolette, Laurie Phillips, and Bryan Richardson, *Final Report: Impacts Analysis for Cyber Attack on Electric Power Systems (National SCADA Test Bed FY08)*, Sandia National Laboratories report SAND2009-1673: Albuquerque, New Mexico (2008).

[2] Jason Stamp, Rich Colbaugh, Randall Laviolette, Annie McIntyre, and Bryan Richardson, *Final Report: Impacts Analysis for Cyber Attack on Electric Power Systems (National SCADA Test Bed FY07)*, Sandia National Laboratories report SAND2008-7066: Albuquerque, New Mexico (2008).

[3] Nicolò Giorgetti, George Pappas, and Alberto Bemporad, "Bounded Model Checking of Hybrid Dynamical Systems," 44th IEEE Conference on Decision and Control — European Control Conference 2005, Seville, Spain, pp. 672-677 (December 2005)

[4] Judith D. Gardiner, "Faster Checking of Discrete-Time Hybrid Systems," Final Report, Ohio Supercomputer Center, Sept. 29, 2008 (unpublished).

[5] Richard Colbaugh, Kristin Glass, and Gerald Willard, *Analysis of Complex Networks Using Aggressive Abstraction*, Sandia National Laboratories report SAND2008-7327, Albuquerque, New Mexico (October 2008).

[6] Antoine Girard, "Approximate abstraction for verification of continuous and hybrid systems," Guest lecture, Hybrid System Course ESE 601, (March 2006), University of Pennsylvania, Philadelphia, PA, USA, http://www-lmc.imag.fr/membres/Antoine.Girard/publi.html

[7] Meeko Oishi, "Hybrid Reachability", Lecture 18, EEC 571M/491M, (Spring 2007), University of British Colombia, Vancouver, BC, Canada, http://courses.ece.ubc.ca/491m/lecture_notes.html

Appendix B

Acronyms, Symbols, and Abbreviations

Table B.1: Acronyms

Acronym	Phrase
BMC	Bounded Model Checking
DOE	Department of Energy
EPG	Electric Power Grid
FSA	Finite State Abstraction
FY	Fiscal Year
IA	Impacts Analysis
NSTB	National SCADA Test Bed
ODE	Ordinary Differential Equation
SCADA	Supervisory Control and Data Acquisition
SNL	Sandia National Laboratories

Table B.2: Symbols

Symbol	Units	Description
A_q	varies	Jacobian of the system for configuration q with respect to x at equilibrium
B_q	varies	Jacobian of the system for configuration q with respect to u at equilibrium
C_q	varies	Matrix relating state variables to allowable ranges for state q
δ	radians	Electrical angle between its voltage and the rotor major axis
d_q	varies	Allowable range of state variables for state q
ΔQ_L	per-unit	Change in load reactive power
Δx	varies	Difference between state variables and equilibrium values
Δy	varies	Difference between algebraic variables and equilibrium values
E_f	per-unit	Generator field circuit voltage
f	varies	System differential equations
f_x	varies	Jacobian of f with respect to x at equilibrium

Continued on next page

Table B.2 – *continued from previous page*

Symbol	Units	Description
f_y	varies	Jacobian of f with respect to y at equilibrium
g	varies	System algebraic equations
g_x	varies	Jacobian of g with respect to x at equilibrium
g_y	varies	Jacobian of g with respect to y at equilibrium
H	varies	Matrix relating x and y
P_L	per-unit	Load active power
q	varies	Vector of discrete control variables
Q_L	per-unit	Load reactive power
R_k	per-unit	Resistance of line k
R^n	per-unit	Vector space of dimension n
S_G	per-unit	Generator complex power
S_L	per-unit	Load complex power
θ_i	radians	Phasor voltage phase angle of bus i
t	seconds	Time
T	seconds	Time horison of FSA simulation
u	varies	Vector of continuous control variables
u_0	varies	Initial condition of control variables
V	per-unit	Phasor voltage magnitude
x	varies	Vector of state variables
$\dot{x}$	varies	First derivative with respect to time of state variable x
x_0	varies	Initial condition of state variables
X_k	per-unit	Reactance of line k
y	varies	Vector of algebraic variables
y_0	varies	Initial condition of algebraic variables
Z	varies	Region of unacceptable states
Z_k	varies	Measured impedance of circuit k

Table B.3: Abbreviations

pu	per-unit
rad	radians
s	seconds
Ω	Ohms

Appendix C

Glossary

Table C.1: Definitions

Term	Definition
Finite State Abstraction (FSA) Algorithm	The FSA approach represents a possible method to determine the stability and suitability of operations for an electrical power grid utilizing a fully descriptive model (including dynamics and control action) under a wide range of potential cyber attack scenarios. The underlying premise for this work is the conversion of the hybrid grid/control model dynamics into a representative FSA, which greatly improves the tractability of the problem. The new approach is expected to scale to larger systems and modeling complexity much better than traditional analysis for grid dynamics.

Appendix D

For More Information

Table D.1: Contact Information

Name	Organization
Jason Stamp *Sandia Project Lead*	Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-1108 jestamp@sandia.gov
Bob Pollock *Sandia NSTB Lead*	Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0671 rdpollo@sandia.gov
Jennifer Depoy *Sandia NSTB Manager*	Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0671 jmdepoy@sandia.gov
Hank Kenchington *DOE NSTB Manager*	U.S. Department of Energy 1000 Independence Avenue, SW Washington, DC 20585 henry.kenchington@hq.doe.gov

DISTRIBUTION:

1 Hank Kenchington, U.S. Department of Energy (electronic)
1 Judith D. Gardiner, Ohio Supercomputer Center (electronic)

1 MS 1108 Jason Stamp, 06332 (electronic)
1 MS 1235 Randall LaViolette, 05635 (electronic)
1 MS 0671 Laurie Phillips, 05628 (electronic)
1 MS 0671 Bob Pollock, 05633 (electronic)
1 MS 0671 Jennifer DePoy, 05628 (electronic)
1 MS 0899 Technical Library, 9536 (electronic)

Sandia National Laboratories