SANDIA REPORT
SAND2017-XXXX
Unlimited Release
September 2017

Understanding Risks in the Global Civilian Nuclear Enterprise: Global Nuclear Assured Security Scenarios Workshop

Sharon DeLand and Elizabeth Kistin Keller (0159), Adriane Littlefield (6833), and Douglas Osborn (8852)

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

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

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@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

SAND2017-XXXX
September 2017
Unlimited Release

Understanding Risks in the Global Civilian Nuclear Enterprise: Global Nuclear Assured Security Scenarios Workshop

Sharon DeLand and Elizabeth Kisten Keller
Strategic Futures and Policy Analysis

Adriane Littlefield
Global Security Research and Analysis

Douglas Osborn
Severe Accident Analysis

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS042

Abstract

The purpose of the scenarios workshop held for the Civilian Nuclear component of the Global Nuclear Assured Security Mission Integration Initiative was to identify sources of risk in the global civilian nuclear enterprise. The risks identified are inadequately addressed through current technical measures, regulatory frameworks and institutions and should be considered for further research. The workshop participants also developed four high level scenarios describing different sequences of events that could result in radiological releases, widespread loss of electric power, and loss of public confidence in segments of the nuclear industry. The scenarios are intended for further analysis and as the basis for simulation exercises.

This Page Intentionally Left Blank

Contents

Tables

This Page Intentionally Left Blank

Nomenclature

3S	Safety, Security, and Safeguards
DOE	Department of Energy
FLEX	On-site and off-site flexible support equipment
GNAS	Global Nuclear Assurance and Security
GNAS/CN	Global Nuclear Assurance and Security/Civilian Nuclear
NRC	Nuclear Regulatory Commission
PWR	Pressurized Water Reactor
R&D	Research and Development
SMEs	Subject Matter Experts
SNL	Sandia National Laboratories
UAVs	Unattended Aerial Vehicles – Drones
US	United States
USG	United States Government

This Page Intentionally Left Blank

1 Introduction and Purpose

The purpose of the scenarios workshop held for the Civilian Nuclear component of the Global Nuclear Assured Security (GNAS/CN) Mission Integration Initiative was to identify sources of risk in the global civilian nuclear enterprise that are inadequately addressed through current technical measures, regulatory frameworks and institutions. The workshop objectives and desired outcomes are outlined in Table 1.

Table 1. Workshop Objective and Desired Outcomes

Workshop Objectives

- Identify scenarios that illuminate sources of risk in the global civilian nuclear enterprise
  - What risks are inadequately addressed in the current approach/system?
  - Leverage Sandia experience to generate credible and important scenarios
  - Gain insights into root causes: external drivers/factors, stovepipes, systemic failures, human factors

Desired Outcomes

- Insight into underappreciated risks
  - What are they
  - What is getting in the way of addressing the risks
- Four to six candidate scenarios spanning a broad range of potential risks

The workshop organizers were particularly interested in understanding the extent to which risks arise from stovepipes between safety, security, and international safeguards domains (referred to as 3S in this document) and whether an integrated approach would be valuable. The intention was to identify risks and develop scenarios that could be used as the basis for further analysis and stakeholder engagement.

The organizers selected a workshop-based approach in order to draw upon the collective experience of a wide range of subject matter experts (SMEs). Participants were drawn from across the nuclear enterprise at Sandia National Laboratories (Sandia), with SMEs representing the safety, security, and safeguards areas, as well as those with expertise in the nuclear power and cybersecurity domains. Appendix A provides a list of SME attendees.

The following report describes the results of the workshop.

This Page Intentionally Left Blank

2 Workshop Design

The workshop was designed to collect information about risks in the global civilian nuclear enterprise through a series of exercises that identified and evaluated those risks.

2.1 Risk Identification

As a warm-up exercise, each participant was asked to identify what risks or concerns keeps him/her up at night and what are the biggest concerns that are not being thought about or addressed. This exercise resulted in a broad set of risks and provided an opportunity for participants in the various domains to hear about risks in each other's domains. The results of this exercise are discussed in Section 3.

2.2 Scenario Development

After the Risk Identification exercise, the participants broke up into cross-disciplinary teams and were asked to develop a scenario that illuminated sources of risk in the global civilian nuclear enterprise. Participants were asked to identify—as appropriate and relevant—the actors, motivation, and objective as well as the event type and consequences of the event in their scenarios. These scenarios are described in Section 4.

2.3 Scenario Evaluation

After developing their scenarios, each team presented their scenarios to the entire group and participants were asked to evaluate the scenarios on the extent to which the scenario challenged today's conventional wisdom, plausibility, and relevance. This is especially necessary in terms of identifying risks that are overlooked in today's risk management approaches. The results of this evaluation are given in Section 5.

2.4 The Role of 3S

Finally, participants were asked to address the 3S concept more directly in terms of how 3S integration might change the ability to address the challenges in each team's scenarios and what the barriers are to applying such an approach. The results of this exercise are discussed in Section 6.

This Page Intentionally Left Blank

3 Identified Risks and Concerns

To initially identify potential risks, SMEs were elicited in response to the following questions:

- What are three things that keep you up at night?
- What are the biggest things that no one is thinking about?

Risks and concerns identified by the participants ranged across economic, social, and political issues to technical and regulatory concerns.

The participants identified a confluence of economic factors that are contributing to a loss of United States' (US) influence in the global civilian nuclear enterprise. Within the US, factors and trends included asymmetric or disproportionate regulatory burdens for nuclear energy versus other forms of electric generation; increased competitiveness of renewable energy; and a decline in the US research funding. These are all contributing to an overall decline in the civilian nuclear industry within the US. At the same time, other countries—particularly China and Russia—are investing in and growing their influence on the international nuclear industry, including sales to developing regions. Given examples of industrial accidents within these countries (e.g., Chernobyl), Sandia experts are concerned about the future state of safety and security in the global civilian nuclear enterprise as the US loses influence.

Domestic political uncertainties were also a cause for concern. The new administration is still developing its policy and strategy, as well as staffing federal agencies. There are particular concerns about the future of US research and development (R&D) investment, potential changes in the regulatory environment (e.g., additional regulations resulting from the 2011 Fukushima accidents in Japan), and commitment to international engagement.

In the international environment, there were three major political concerns. The first was that the International Atomic Energy Agency, which carries out international safeguards to ensure that civilian materials are not diverted for military purposes, is under significant stress with the growth of the international civilian nuclear enterprise and the addition of monitoring responsibilities under the Joint Comprehensive Plan of Action. The second was the diffusion of nuclear power into developing regions (Africa, South America, and the Middle East) which have little practical operating or regulatory experience with these technologies. The third concern was the potential for failure of State governance or civil war within countries that have nuclear facilities. Most nuclear risk management functions rely on a functioning national government. When governance fails, there is no international organization or body responsible for stepping in and helping to maintain, repair, or restore control.

Taken together, participants generally saw a world in which nuclear risks appear to be growing, and US influence declining. However, there is a chance to change this overall pattern, but the timeframe to do so is limited (within the next three to five years).

Participants noted a number of social factors that affect 3S risks. Technical solutions are implemented in a larger social context—operator and regulator commitment, attitude and problem-solving approaches make a significant difference to the effectiveness of technical measures and approaches. Limited experience with high-consequence systems, such as those found in the nuclear enterprise, means that the 3S culture is often a factor in evaluating global nuclear energy risks. There is often a *trust* mentality or a *compliance* mentality that does not necessarily fully appreciate the true risks and vulnerabilities, including insider threats and terrorist threats. In regards to *compliance* and *trust* mentalities, consider what occurred in 2011 at Fukushima where the core meltdown accident occurred after an earthquake and tsunami. A contributing factor to the accidents was these mentalities did not allow for paradigm breaking to occur prior to or during the accidents.[1] Measures such as the post-9/11 Nuclear Regulatory Commission (NRC) requirement to develop and maintain strategies for addressing large fires and explosions (B.5.b regulations)[2], which was done in the US, could have helped preclude or minimize the accidents. Yet, the Japanese regulator and utilities felt that their existing framework was sufficient for aircraft impacts and limited this initiative with respect to other external events such as tsunamis. However, since Fukushima, the world-wide boiling water reactor and pressurized water reactor (PWR) fleets (US vendor designs) have embraced the US initiative of on-site and off-site flexible support equipment (FLEX) to preclude or minimize an accident.

Social factors such as public perception of the nuclear industry can affect its viability both internationally and at home; an accident/incident anywhere affects the industry everywhere. One concern that was raised was accidents are resulting in US industry decline, presumably due to loss of public confidence.

With respect to resources and environmental concerns, several participants stressed the value of nuclear energy in meeting growing energy and water demands, as well as enabling high levels of availability for these demands. Nuclear energy can also play a role in managing carbon emissions. Participants noted that long-term waste disposal continues to be an unresolved issue.

Participants also identified a number of technical risks that could further raise the risk of accidents or attacks. Aging infrastructure and the spread of less safe (foreign) designs throughout the world were noted as safety concerns. In addition, transitions to newer technologies, new designs, passive systems, and digital control systems, mean that weaknesses and vulnerabilities are less understood and harder to quantify. Co-location with population centers and the expansion of nuclear energy into places with less of a safety culture were also seen as factors that could degrade safety or amplify consequences. Participants expressed concerns about several newer types of attack pathways including cyber, biological agent attacks on nuclear infrastructure, supply chain attacks, and unattended aerial vehicles

[1] Institute of Nuclear Power Operators (INPO), "Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, Revision 0," INPO 11-005, November 2011.

[2] NRC, "Compliance with 10 CFR 50.54 (hh)(2) and 10 CFR 52.80(d) Loss of Large Areas of the Plant due to Explosions or Fires from Beyond-Design Basis Event," DC/COL-ISG-016, Adams Assertion No. ML101940484, 2009.

(UAVs). Such threat vectors could be used to achieve a wide range of consequences ranging from material theft and radiological release to larger systemic impacts including inducing panic or terror and economic disruption. Even if an attack were to occur outside the US, the impact to the domestic fleet could do significant economic damage (i.e., shutting down plants) which in turn would have impact on US National Security because of a reduced diversity of the electric grid and base load generation.

This Page Intentionally Left Blank

4 Scenario Descriptions

Participants broke up into teams with varied SMEs (i.e., a combination of safety, security, international safeguards and nuclear energy expertise) and developed scenarios that embodied potential risks to the global civilian nuclear enterprise. Teams were asked to consider and include different elements of a scenario including;

- Who the actors were
- What their motivation and objectives were
- What type of event it was
- What initiated the event

4.1 Scenario 1: Shutting Down the Nuclear Power Industry in a Major Supplier/Consumer

This scenario imagines a non-state terrorist actor using an insider to cause a core meltdown at one or more nuclear power plants in a country that is both a major supplier and consumer of nuclear-power generated electricity. The nuclear power plants are PWR designs which are also very similar to Chinese and Russian designs. In this design a pressurizer, located physically higher than the core, is used to maintain a high pressure in the core, which enables it to run at high temperatures without the water in the core boiling. The pressurizer maintains a two-phase (steam-water) environment; the steam bubble in this environment will shrink or grow depending on changes in reactor power. The scenario suggests that an insider causes a failure in the high-pressure injection system that shifts this bubble from the pressurizer to the core, causing a core melt down. The 1979 Three Mile Island accident included such a shift in the bubble.

The suggested impact of this scenario included a potential shut down of approximately 70% of the country's grid for some period of time, resulting in significant economic impacts and loss of confidence in the nuclear power industry.

4.2 Scenario 2: Weaponization of Fail-Safe Mode

In this scenario, an adversary wants to destabilize a Western country in which there is also significant public confidence in the nuclear energy industry. The adversary is another nuclear power plant supplier that wishes to undermine confidence in Western nuclear power technology and diminish Western political influence.

Advances in smart grid technologies have created a delivery pathway for such a computer virus. The attacking country releases a virus that introduces a control issue in nuclear power plants that result in the wrong response to an operational directive. This virus is designed to affect multiple designs in a phased approach; the attack masquerades as a mechanical system failure. Infection with the virus leads to an immediate plant shutdown. The attack takes place during summer, when there are high electricity load demands. The resulting panic and crisis from electricity shortages, derived from apparent failures in the nuclear power plants affects *trust* in Western nuclear power technologies. The attacking country

highlights that its designs are immune from these failures. The electricity shortages also affect socio-political stability.

4.3 Scenario 3: Drone Attack

This scenario imagines an attack on a nuclear power plant or facility carried out by one or more commercially available UAVs (drones). Multiple drones would operate cooperatively in a swarm. The attack results in sabotage on the nuclear facility, but is actually a diversion to aid in material theft. The scenario team noted that a wide range of actors could potentially initiate such an attack, from a lone wolf up to a nation state. Additional goals for this type of attack could include creating civil unrest, economic loss, and undermining or shuttering the country's nuclear industry. The scenario team noted that current approaches focused on sabotage do not generally consider the potential for civil unrest and economic loss or measures to mitigate them. Current approaches also do not necessarily consider lower probability outcomes, such as a potential core meltdown or concurrent theft. The team also noted that there were potential opportunities for innovation including use of radar or wireless communications for detection and perhaps directed energy for a response countermeasure.

4.4 Scenario 4: Trojan-Caused Safety Incident

This scenario imagines an environment in which a *turn-key trusted* design for a civilian reactor has been deployed in one or more countries. This system includes a Trojan or stealth design omission that affects safety, security, safeguards systems including cyber and hardware aspects.

Once the Trojan is triggered, it causes a safety incident, coordinated with a security attack. The initiator for this could either be the country that sold the reactor in the first place, another country aware of the Trojan and seeking to cause economic disruption, or a non-state actor seeking to create international embarrassment.

This scenario could evolve in a few different ways. First, if the Trojan is triggered and a severe accident occurs, there could be a radioactive release and economic disruption. Alternatively, the Trojan could be used as a threat for geopolitical advantage through economic leverage. For example, the Trojan could be uncovered by the selling country, the vendor, or some other party who could gain recognition as a *hero* and also profit by fixing the problem for a (potentially large) fee.

The scenario team identified a number of possible responses including potential detection and clean up in a quality assurance-like program applied to security (in either the purchasing country or third parties) and post-incident forensics. The team noted that the US might have limited risk management options because US influence is reduced in the civilian nuclear enterprise. However, international non-regulatory engagement could be helpful.

5 Scenario Evaluations

Once the teams developed scenarios, each team then presented the scenario to the rest of the workshop participants. Each participant was asked to score the scenarios based on three criteria, each scored qualitatively on a scale from 1 to 5:

- Challenging – the scenario is thought-provoking; challenges today's conventional wisdom
- Plausible – the scenario could actually happen
- Relevant – the scenario is pertinent to identifying overlooked risks affecting global civilian nuclear energy

The results are summarized in Table 2. Of the scenarios, the drone attack was the highest rated overall and with respect to relevance. The fail-safe attack was rated higher on the challenging criterion.

The comments received on the scenarios suggest that the teams were generally able to construct interesting scenarios that highlighted important risks. These scenarios could be improved or developed further to strengthen their impact and identify technical gaps which Sandia could address through R&D. While the scenarios generally highlight important risks that presented challenges that are difficult to address effectively, there was skepticism that they are novel or overlooked. A second observation is that at least two of the four did not cross into the safeguards domain (recall these scenarios were to look at all 3S aspects). While this exercise was too limited to draw firm conclusions, these results suggest challenges in identifying scenarios that impact all 3S domains.

Table 2. Scenario Ratings and Summary of Comments

Scenario	Challenging (1-5)	Plausible (1-5)	Relevant (1-5)	Summary of Comments
Shut Down Nuclear Power in Major Consumer/Supplier **(Section 4.1)**	3.0	3.1	3.5	• Several participants noted that a high degree of technical knowledge is indicated for this scenario • There was some disagreement as whether this constituted a novel or overlooked risk. Some thought that plausibility would increase with increasing prevalence of digital systems, while others thought such a scenario would be difficult to execute • A broader focus on potential negative effects was suggested
Weaponization of Fail-safe Mode **(Section 4.2)**	3.7	3.4	3.7	• Multiple comments suggested that the scenario represented an important risk, but again some challenged whether it was novel • At least one participant found the motivation of reducing confidence in US nuclear power (design and regulator) interesting. Others questioned whether the scenario was attractive if nuclear power is on the decline in the US • The scenario did not obviously cross into the safeguards domain
Drone Attack **(Section 4.3)**	3.5	4	4	• Multiple participants found this scenario to be important, although again there were questions as to whether this represented an overlooked risk. The scenario does highlight the need to consider potential air or coordinated air/ground attacks rather than just ground based attacks • As stated, the scenario was considered too broad – the goal of theft versus sabotage was not clear • Defining the policy and response options was seen as important; there could be a lot of opportunity to develop methods to deal with or avoid drones
Turnkey Trojan and Extortion (Trojan) **(Section 4.4)**	3.5	2.9	3.2	• Participants cited the novelty of a quality assurance-like program for security although it would need to be extensive and well thought out • A second feature that represented a potential overlooked risk was the concept of misdirection of responsibility. Of note however, several participants questioned the motivations of a vendor to engage in this type of a scenario and the plausibility of it • The scenario did not obviously cross into the safeguards domain

6 Integrated 3S Discussion: Opportunities and Barriers

The workshop concluded with a discussion of the potential value of integration across the 3S domains and the barriers to gaining acceptance for such an approach.

With respect to the value of an integrated approach, participants identified three ways that this approach would change the ability to anticipate, assess, or address the challenges highlighted in the scenarios.

1. Identify attack vectors
2. Identify *outside the box* solutions
    a. Reverse engineer analog
    b. Subsidize analog
    c. Relax quality assurance and regulation on analog as weighted against security risks
3. Quality assurance is a safety concept that could be leveraged to other domains

One participant noted that 3S is a subset of concurrent engineering and it would be worthwhile to consider other industry examples for lessons learned (e.g., NASA).

The group identified a number of factors that stand in the way of applying an integrated 3S approach. These included social, technical, economic, and political factors as summarized in the Table 3.

Table 3. Social, Technical, Economic, and Political Factors Summary

What is standing in the way of an integrated 3S approach to Civilian Nuclear?	
Category	***Causal Factors***
Social	• Perception of nuclear risk can drive up regulation, resulting in an already overburdened industry with respect to other industries • This approach could miss the actual drivers of risk • Stovepipes within Sandia • Education/expertise; there is limited knowledge of how to do this • No 3S event markers, metrics, or figures of merit • Public perception driven by safety (tangible examples) and not security or safeguards • Specialization is emphasized in technical/professional domains • Complexity of integration increases the technical burden on staff/resources
Technical	• Difficult to show benefit; no proven methods to show this approach gains anything • Lack of training for design review, etc. • 3S knowledge is extremely deep and experience-laden • Compartmentalization is a fundamental security principle, but integration countermands this • Weighted differences for different facilities (e.g., power plant vs. reprocessing) • Codes incompatible
Economic	• Large upfront cost; costly to vendors to implement (3S by design) • Requires regulatory push to implement
Political	• Government organizations are stovepiped • Congressional funding not based on long-term or cross-institutional research. • Little motivation to change from proven methods unless external drivers prove otherwise • Protecting turf and lack of interest • Hard to get the NRC involved in initial 3S training since their mission is strictly domestic civilian nuclear power
Other	• US has low influence in the global nuclear industry • Information necessary for such an endeavor is purposely compartmentalized security and safeguards information

7 Summary and Conclusions

The GNAS/CN Scenarios Workshop participants identified a wide range of risks to the global civilian nuclear enterprise spanning economic, social, and political issues to technical and regulatory concerns. Continued investment in and expansion of the global civilian nuclear enterprise, combined with the continuing decline of US nuclear industry is leading to a loss of US influence in managing these global risks. On the technical side—aging infrastructure, the spread of less safe foreign designs, and transitions to newer technologies—contribute to 3S risks. While these and other concerns (highlighted in Section 3) are not necessarily new, the group of SMEs considered them inadequately addressed by current regimes and policies. Furthermore, the range of concerns across technical and non-technical domains highlight the complexity of the global civilian nuclear enterprise.

The workshop participants also developed four high level scenarios describing different sequences of events that could result in radiological releases, widespread loss of electric power, and loss of public confidence in segments of the nuclear industry. Three of the four scenarios imagined attacks where cyber or UAVs were used as enablers. The emergence of these scenarios is indicative that current regimes and policies have not fully adapted to newer technologies.

Finally, the workshop identified potential integrated 3S benefits and barriers to implementing such an integrated risk management approach in the global civilian nuclear enterprise. The wide range of factors again brings out the complexity of facilitating change to the current environment.

The results of this workshop can advance the knowledge and understanding of risks in the global civilian nuclear enterprise in two ways.

1. To use these scenarios in one or more role-playing simulation exercises with SMEs drawn from across stakeholder organizations (e.g., industry user groups, regulators such as NRC, NNSA, representative local governments). Such exercises can be used to explore in more depth the extent to which current regimes, policies, and capabilities can or cannot address the scenarios in question. The results of such exercises can be used to identify technology gaps and inform the need for collaboration, information sharing, and R&D for new tools and capabilities.
2. To use these results to inform the development of system-level tools to enable managing 3S risks across all domains. An example of this is the Global Nuclear Enterprise System Framework [Ben Bonin et al., internal communication] being developed through a related effort. This framework could provide a common organizing principle for approaching problems and questions sets posed by diverse stakeholders across the USG and Sandia.

The set of 3S risks, as well as benefits and barriers for adoption of an integrated risk management approach, can be used to inform and validate the scope of a proposed GNAS/CN framework.

This Page Intentionally Left Blank

Appendices

Appendix A. Attendees

Name	Title	Organization	Number
Sharon DeLand	R&D S&E, Systems Research & Analysis	Strategic Futures & Policy Analysis	0159
Elizabeth Kistin Keller	R&D S&E, Systems Research & Analysis	Strategic Futures & Policy Analysis	0159
Rubel Martinez	R&D S&E, Systems Engineering	Systems Analysis Dept.	5814
Kamyar Rahimian	R&D S&E, Materials Science	Systems Analysis Dept.	5814
Joshua Daley	R&D S&E, Cybersecurity	Resilient Control Systems	6613
Adriane Littlefield	Engineering Systems Integration/ Implementation Professional	Global Security Research & Analysis	6833
Amir Mohagheghi	Manager, R&D Science & Engineering	Global Security Research & Analysis	6833
Tommy Goolsby	R&D S&E, Mechanical Engineering	International Nuclear Security Engineering	6835
Mark Snell	R&D S&E, Systems Research & Analysis	International Nuclear Security Engineering	6835
Richard Griffith	Sr. Mgr, R&D Science & Engineering	Nuclear Energy Safety Technology	8850
Matthew Denman	R&D S&E, Nuclear Engineering	Risk & Reliability Analysis	8851
Mitch McCrory	Manager, R&D Science & Engineering	Risk & Reliability Analysis	8851
Nathan Andrews	R&D S&E, Nuclear Engineering	Severe Accident Analysis	8852
Douglas Osborn	R&D S&E, Nuclear Engineering	Severe Accident Analysis	8852

Distribution

1	MS0158	Dan Briand	00150 (electronic copy)	dbriand@sandia.gov
1	MS0159	Thomas Nelson	00159 (electronic copy	trnelso@sandia.gov
1	MS0736	Richard Griffith	08850 (electronic copy)	rogrif@sandia.gov
1	MS0748	Randall Gauntt	08852 (electronic copy)	rogaunt@sandia.gov
1	MS1371	Dianna Blair	06830 (electronic copy)	dsblair@sandia.gov
1	MS1371	Amir Mohagheghi	06833 (electronic copy)	ahmohag@sandia.gov
1	MS1371	Eric Wallace	06833 (electronic copy)	eawalla@sandia.gov
1	MS1371	Adam Williams	06833 (electronic copy)	adwilli@sandia.gov
1	MS9406	Ben Bonin	08712 (electronic copy)	bjbonin@sandia.gov

1	MS0899	RIM-Reports Management	09532 (electronic copy)

Sandia National Laboratories