U.S. NUCLEAR REGULATORY COMMISSION
NOTICE OF GRANT/ASSISTANCE AWARD

1. GRANT/AGREEMENT NO.	2. MODIFICATION NO.	3. PERIOD OF PERFORMANCE	4. AUTHORITY
NRC-HQ-11-G-04-0060		FROM: 9/21/2011 TO: 11/02/2012	Pursuant to Section 31b and 141b of the Atomic Energy Act of 1954, as amended

5. TYPE OF AWARD	6. ORGANIZATION TYPE	7. RECIPIENT NAME, ADDRESS, and EMAIL ADDRESS
[X] GRANT [ ] COOPERATIVE AGREEMENT	Public State-Controlled Institution of Higher ED DUNS: 001425594 NAICS: 611310	Massachusetts Institute of Technology 77 Massachusetts Avenue E19-750 Cambridge, MA 02139-4307

8. PROJECT TITLE:

Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants

9. PROJECT WILL BE CONDUCTED	10. TECHNICAL REPORTS ARE REQUIRED	11. PRINCIPAL INVESTIGATOR(S) NAME, ADDRESS and EMAIL ADDRESS
PER GOVERNMENT'S/RECIPIENT'S PROPOSAL(S) DATED See Program Description AND APPENDIX A-PROJECT GRANT PROVISIONS	[X] PROGRESS AND FINAL [ ] FINAL ONLY [ ] OTHER (Conference Proceedings)	Nancy Leveson, Ph.D. Massachusetts Institute of Technology 77 Massachusetts Avenue Cambridge, MA 02142 Email: leveson@mit.edu, Phone: 617-258-0505

12. NRC PROGRAM OFFICE (NAME and ADDRESS)	13. ACCOUNTING and APPROPRIATION DATA	14. METHOD OF PAYMENT
NRC Attn: Robin Barnes, Robin.BarnesRES@nrc.gov Office of Regulatory Research MS: CS C6-D20, (301) 251-7401 11545 Rockville Pike Rockville, Maryland 20852 Luis Betancourt, Tech Analyst, Luis.Betancourt@nrc.gov	APPN. NO: 31X0200.160 B&R NO: 2011-60-11-6-119 JOB CODE: G6018 BOC NO: 4110 OFFICE ID NO: RFPA: RES-11-197 FAMIS: GR0018	[ ] ADVANCE BY TREASURY CHECK [ ] REIMBURSEMENT BY TREASURY CHECK [ ] LETTER OF CREDIT [X] OTHER (SPECIFY) Electronic ASAP.gov (See Remarks in Item #20 "Payment Information")

15. NRC OBLIGATION FUNDS		16. TOTAL FUNDING AGREEMENT		
THIS ACTION	$174,535.36	NRC	$174,535.36	This action provides funds for Fiscal Year in the amount of See Page Two
PREVIOUS OBLIGATION		RECIPIENT		
TOTAL	$174,535.36	TOTAL	$174,535.36	

17. NRC ISSUING OFFICE (NAME, ADDRESS and EMAIL ADDRESS)

U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: M`Lita Carr Email: MLita.Carr@NRC.GOV
Mail Stop: TWB-01-B10M
Rockville MD 20852

18.	19. NRC CONTRACTING OFFICER
Signature Not Required	Sheila Bumpass 9/21/2011 (Signature) (Date) NAME (TYPED) Sheila Bumpass TITLE Contracting Officer TELEPHONE NO. 301-492-3484

20. PAYMENT INFORMATION

Payment will be made through the Automated Standard Application for Payment (ASAP.gov) unless the recipient has failed to comply with the program objectives, award conditions, Federal reporting requirements or other conditions specified in 2 CFR 215 (OMB Circular A110).

21. Attached is a copy of the "NRC General Provisions for Grants and Cooperative Agreements Awarded to Non-Government Recipients.
Acceptance of these terms and conditions is acknowledged when Federal funds are used on this project.

22. ORDER OF PRECEDENCE
In the event of a conflict between the recipient's proposal and this award, the terms of the Award shall prevail.

23. By this award, the Recipient certifies that payment of any audit-related debt will not reduce the level of performance of any Federal Program.

SUNSI REVIEW COMPLETE

TEMPLATE - ADM001

ADM002

ATTACHMENT A - SCHEDULE

A.1 PURPOSE OF GRANT

The purpose of this Grant is to provide support to the "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants" as described in Attachment B entitled "Program Description."

A.2 PERIOD OF GRANT

1. The effective date of this Grant is September 21, 2011. The estimated completion date of this Grant is November 02, 2012.

2. Funds obligated hereunder are available for program expenditures for the estimated period: September 21, 2011 – November 02, 2012.

A. GENERAL

1. Total Estimated NRC Amount:	$174,535.36
2. Total Obligated Amount:	$174,535.36
3. Cost-Sharing Amount:	$0.00
4. Activity Title:	Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants
5. NRC Project Officer:	Robin Barnes, Luis Betancourt (TA)
6. DUNS No.:	001425594

B. SPECIFIC

RFPA No.:	RES-11-197
FAMIS:	GR0018
Job Code:	G6019
BOC:	4110
B&R Number:	2011-60-11-6-119
Appropriation #:	31X0200
Amount Obligated:	$174,535.36

A.3 BUDGET

Revisions to the budget shall be made in accordance with Revision of Grant Budget in accordance with 2 CFR 215.25.

	Year 1	Year 2
Direct Participant Cost	$ 86,592.61	$ 17,607.60
Indirect Cost	$ 58,450.02	$ 11,885.13
Yearly Total	**$145,042.63**	**$ 29,492.73**

A.4 AMOUNT OF AWARD AND PAYMENT PROCEDURES

1. The total estimated amount of this Award is $174,535.36 for the 13.5 month period.

2. NRC hereby obligates the amount of $174,535.36 for program expenditures during the period set forth above and in support of the Budget above. The Grantee will be given written notice by the Contracting Officer when additional funds will be added. NRC is not obligated to reimburse the Grantee for the expenditure of amounts in excess of the total obligated amount.

3. Payment shall be made to the Grantee in accordance with procedures set forth in the Automated Standard Application For Payments (ASAP) Procedures set forth below.

Attachment B – Program Description

PROGRAM DESCRIPTION

While all-digital reactor protection systems have been certified and are operating in France, Germany, Japan, Korea, Sweden, Switzerland, and the UK, among other countries, the U.S. has been more cautious in accepting such designs. Some individual safety systems have been upgraded to digital, including core protection calculators at Palo Verde and Waterford; load sequencers at Turkey Point; and Eagle 21 safety systems at some Westinghouse plants. Oconee will be the first complete all-digital U.S. safety system installation [NEI, 2011].

The NRC has been deliberately (and rightly) cautious regarding critical aspects of digital upgrades. Historically, the NRC has resisted reactor protection systems that are 100% digital. But the NRC is not alone in this caution. The UK required the Sizewell B plant to install a hardwired back-up to the digital I&C system and Finland's nuclear regulator, STUK, required the Olkiluoto 3 nuclear facility to install an automatic hardwired backup system in the event of complete loss of its digital I&C system [NEI, 2011]. Neither of these backup systems, however, totally solve the problem of the digital I&C system not failing but instead doing the wrong thing.

One of the challenges of reviewing licensing plans is the rapid pace of change in digital technology. One reason for using digital technology is to provide enhanced functionality, but digital technology is changing much faster than our engineering techniques can respond to these changes. New technology introduces potential unknowns into our systems and creates new paths to losses. The NRC faces challenges in trying to keep its Standard Review Plan up-to-date given the rapid pace of change in digital technology. Although digital I&C promises multiple benefits like self-checking, on-line diagnostics, improved accuracy, fault tolerance, and automated sensor calibration verification, it also presents unique challenges, from software logic errors and unanticipated system interactions to filtering and digital noise problems and trips that result from configuration changes while at power [NEI, 2011].

A major concern in approving digital I&C systems is the potential for common cause failure in I&C software. Because identical software is used in the redundant channels of safety-related systems, a bug inadvertently designed or implemented into the software (rather than resulting from degradation over time) could cause the same inaccuracies or misbehaviors in all the channels. The NRC has written that "experience with digital I&C systems to date has shown that reliance upon quality assurance processes alone has not been adequately effective at preventing common cause failures even in high-integrity digital systems" [NRC, 2010].

Finally, challenges also exist in demonstrating the ability of digital systems to meet NRC regulations requiring security against intentional external cyber attacks. As Mario Gareri, in the Office of New Reactors, explained in NRC testimony in 2008, "If you look at the

2. NRC hereby obligates the amount of $164,536.41for program expenditures during the period set forth above and in support of the Budget above. The Grantee will be given written notice by the Contracting Officer when additional funds will be added. NRC is not obligated to reimburse the Grantee for the expenditure of amounts in excess of the total obligated amount.

3. Payment shall be made to the Grantee in accordance with procedures set forth in the Automated Standard Application For Payments (ASAP) Procedures set forth below.

Attachment B – Program Description

PROGRAM DESCRIPTION

While all-digital reactor protection systems have been certified and are operating in France, Germany, Japan, Korea, Sweden, Switzerland, and the UK, among other countries, the U.S. has been more cautious in accepting such designs. Some individual safety systems have been upgraded to digital, including core protection calculators at Palo Verde and Waterford; load sequencers at Turkey Point; and Eagle 21 safety systems at some Westinghouse plants. Oconee will be the first complete all-digital U.S. safety system installation [NEI, 2011].

The NRC has been deliberately (and rightly) cautious regarding critical aspects of digital upgrades. Historically, the NRC has resisted reactor protection systems that are 100% digital. But the NRC is not alone in this caution. The UK required the Sizewell B plant to install a hardwired back-up to the digital I&C system and Finland's nuclear regulator, STUK, required the Olkiluoto 3 nuclear facility to install an automatic hardwired backup system in the event of complete loss of its digital I&C system [NEI, 2011]. Neither of these backup systems, however, totally solve the problem of the digital I&C system not failing but instead doing the wrong thing.

One of the challenges of reviewing licensing plans is the rapid pace of change in digital technology. One reason for using digital technology is to provide enhanced functionality, but digital technology is changing much faster than our engineering techniques can respond to these changes. New technology introduces potential unknowns into our systems and creates new paths to losses. The NRC faces challenges in trying to keep its Standard Review Plan up-to-date given the rapid pace of change in digital technology. Although digital I&C promises multiple benefits like self-checking, on-line diagnostics, improved accuracy, fault tolerance, and automated sensor calibration verification, it also presents unique challenges, from software logic errors and unanticipated system interactions to filtering and digital noise problems and trips that result from configuration changes while at power [NEI, 2011].

A major concern in approving digital I&C systems is the potential for common cause failure in I&C software. Because identical software is used in the redundant channels of safety-related systems, a bug inadvertently designed or implemented into the software (rather than resulting from degradation over time) could cause the same inaccuracies or misbehaviors in all the channels. The NRC has written that "experience with digital I&C systems to date has shown that reliance upon quality assurance processes alone has not been adequately effective at preventing common cause failures even in high-integrity digital systems" [NRC, 2010].

Finally, challenges also exist in demonstrating the ability of digital systems to meet NRC regulations requiring security against intentional external cyber attacks. As Mario Gareri, in the Office of New Reactors, explained in NRC testimony in 2008, "If you look at the

design aspect, we're trying to prevent possible bugs or back doors being put into the software life cycle while we're developing the software. And if you look at the programmatic approach, we're trying to prevent attackers from the outside getting into the systems through a cyber attack, [or] the internet" [NRC, 2008].

The Problem

The NRC has strong and effective methods for assurance of safety in traditional electromechanical safety systems. Unfortunately, many of the assumptions underlying these traditional NPP assurance methods do not apply to software.

First, software does not fail randomly like hardware: software is pure design without any physical realization of that design—it contains only systematic design defects. Software can be thought of as *design abstracted away from its physical representation*, that is, it is pure design without any physical realization of that design. While this abstraction reduces physical limits in design and thus allows exciting new features and functions to be incorporated in system design, it also greatly increases potential complexity and changes the types of failures modes. Essentially there are two means for "failure" of digital systems. The hardware on which the software executes can fail in the same way that analog hardware does and the protection against these types of computer hardware failures, like redundancy, are similar. In addition to the computer hardware failing, however, the software (which embodies the system functional design) can be incorrect or include behaviors that are unsafe in the encompassing system. Because the potential problems are always pure design defects, redundancy (which simply duplicates the design errors) is not effective. Knight and Leveson showed, back in the mid-1980's, that making multiple versions of the software using different teams does not solve the problem either [Knight and Leveson, 1986]. Others tried to replicate the Knight and Leveson experiments to try to demonstrate they were wrong, but simply replicated the results [Knight and Leveson, 1990]. People make mistakes on the hard cases in the input space; they do not make mistakes in a random fashion: Therefore, independently developed software is very likely to contain common cause failure modes.

In fact, almost all serious accidents caused by software have involved errors in the requirements, not in the implementation of those requirements in software code (computer instructions) [Leveson, 1995]. In most accidents, the software requirements have had missing cases or incorrect assumptions about the behavior of the system in which the software is operating. Often there is a misunderstanding by the engineers of the requirements for safe behavior, such as an omission of what to do in particular circumstances that are not anticipated or considered. The software may be "correct" in the sense that it successfully implements its requirements, but the requirements may be unsafe in terms of the specified behavior in the surrounding system, the requirements may be incomplete, or the software may exhibit unintended (and unsafe) behavior beyond what is specified in the requirements. Redundancy or multiple versions of the implementations of the requirements does not help in these cases.

Hardware, of course, can also contain requirements and design defects, but hardware can usually be exhaustively tested and the defects discovered and removed before the system is used. In addition, most hardware designs are not revolutionary, but use or build on standard designs used for decades. Software, on the other hand, cannot be exhaustively tested or even come close to that goal. For example, a software implemented

collision avoidance system required on all commercial aircraft in the U.S. (called TCAS II) has been calculated to contain 1020 states. Continuity, which allows infinite state hardware systems to be tested by using interpolation between the test inputs, does not apply to discrete-state digital systems.

In addition, most software represents a new design—it is used to introduce efficiencies or functions that were not in previous hardware designs. Even reuse of old software does not seem to solve the problem [Joyce, 2002; Leveson, 2011]: almost all the software-related spacecraft losses in the past few decades involved reused software from past spacecraft [Leveson, 2004]. These results may stem partly from complacency created by successful use in previous systems and because undocumented assumptions made during the original development may be inappropriate for the new use.

Even if the functionality being provided by software is the same as that of the hardware being replaced, the software-related system failure modes can be and usually are very different than the hardware-based system it is replacing. For example, when an analog mode annunciator in a nuclear power plant control room fails, the screens will go blank and the operators will detect this right away. When a digital box performing the same function fails, the screens will tend to simply freeze, which may take longer to detect. More generally, software tends to "fail" (i.e., not satisfy its requirements) by doing the wrong thing, not by stopping.

Not only do the old reliability enhancing design techniques not work for software, but software is creating new types of accidents and new accident causes that are unrelated to the reliability of the individual components. Accidents in systems with software components are increasingly caused by unsafe interactions among operational (nonfailed) components [Leveson, 2011]. These *component interaction accidents* cannot be controlled using the standard redundancy and overdesign (safety margins) effective against hardware component failures. Industries that have been more aggressive about introducing digital technology are experiencing these new types of accident causes. The nuclear power community, which has been more conservative about the use of digital technology, is approaching the level of system complexity where component interaction accidents will increasingly occur.

The violation of these basic causal assumptions about accidents when using software means that many of the traditional techniques for safety assurance do not apply to the digital components of systems. The problem then is how can we improve our ability to provide software assurance for safety-critical applications and how can these techniques be combined with traditional design and assurance techniques to provide a more effective means of designing and certifying or licensing mixed analog and digital instrumentation in NPPs.

A Potential Solution

To include software in our safety assurance techniques, we need to include the new types of accident causes that software introduces in our conception of how accidents occur. This goal can be accomplished by extending the models of causation currently used. Leveson has created a new accident causality model, called STAMP (System-Theoretic Accident Model and Processes), which is based on system theory.
In STAMP, safety is reformulated as a control problem rather than simply a reliability (or availability) problem. Component failure (and unreliability of the system components) is

still included, but more generally accidents are considered to occur when component failures, external disturbances, or unsafe interactions among system components are not adequately handled, i.e., controlled, resulting in unsafe system behavior. Unsafe system behavior is defined in terms of required behavioral safety constraints not being met. For example, a typical system safety constraint for a nuclear power plant is that the reactor protection system must always insert neutron absorbing material into the core when a reactivity excursion is feared or cooling is inadequate. Failure to enforce that constraint could, under certain circumstances, lead to an unacceptable release of radioactivity into the environment.

To prevent accidents, the system design must enforce the safety constraints on system behavior. The actual process that may lead to the lack of control (or accident) can be very complex and may involve indirect, non-linear, and feedback relationships among the events and the system components.

Safety constraints specify those relationships among system variables or components that constitute the non-hazardous or safe system states—for example, the power must never be on when the access door to the high-power source is open; two aircraft must never violate minimum separation requirements; pilots in a combat zone must be able to identify targets as hostile or friendly; and the public health system must prevent the exposure of the public to contaminated water and food products. In nuclear power plants, common system-level safety constraints are that control rods must be inserted into the core when core reactivity is out of control or when core cooling is insufficient, the reactor core must be provided with sufficient cooling to evacuate heat and prevent damage to the core, fuel cladding must prevent leakage of radioactivity, etc. These high-level behavioral constraints can be refined into more specific constraints on the behavior of each of the system components, which together will ensure the system-level safety constraints. Accidents result from individual component behavior that violates its safety constraints and from interactions among system components that violate the systemlevel safety constraints—in other words, from a lack of appropriate constraints on component and system behavior.

Besides safety constraints, one other important concept is needed in formulating safety as a control problem. In basic systems and control theory, in order to provide effective control, the controller must have an accurate model of the process it is controlling (Figure 1). For human controllers, this model is commonly called the mental model. For both automated and human controllers, the process model or mental model is used to determine what control actions are necessary to keep the system operating effectively.

The process model includes assumptions about how the controlled process operates and about the current state of the controlled process. Accidents in complex systems, particularly those related to software, often result from inconsistencies between the model of the process used by the controller and the actual process state which leads to the controller providing inadequate control. Usually, these models of the controlled system become incorrect due to missing or inadequate feedback and communication channels. In the Mars Polar Lander loss, for example, the software thought the spacecraft was on the surface of the planet and issued an instruction to cut off the descent engines. At the time, however, the spacecraft was still 40 meters above the planet surface. As another example, the autopilot software may think the aircraft is climbing when it really is descending and apply the wrong control law or the pilot may think a friendly aircraft is hostile and shoot a missile at it.

A large number of accidents involving software can be explained by inaccurate process models. Software is often used to control system components or behavior. The same is true for accidents related to human errors. STAMP provides a much more effective way of designing to reduce human error than does treating human error like machine failure.

Part of the challenge in designing effective safety controls is providing the feedback and inputs necessary to keep the controller's model consistent with the actual state of the process. An important component in understanding accidents and losses involves determining how and why the controller was ineffective; often this is because the process model used by the controller was incorrect or inadequate in some way. Designing for safety or analyzing an existing design for safety involves creating and analyzing the controls used to enforce the safety constraints (safe behavior) to ensure that they will be effective in ensuring the safety constraints will be enforced by the system design.

Using these concepts, we have created a new hazard analysis technique called STPA (System Theoretic Process Analysis) [Leveson, 2011]. STPA can be used to identify the physical constraints that must be enforced and to ensure that the system design adequately enforces them. It also identifies the required process model (mental model if the controller is a human) that the controller needs in order to provide adequate control and thus the information required in that process or mental model. If that information gets lost or corrupted, accidents can occur.

STPA is basically a rigorous method for examining the control loops in the safety control structure to find potential flaws and the potential for (and causes of) inadequate control. Because the STAMP framework extends current accident models and thus includes component failure accidents, STPA not only identifies the hazard scenarios identified by fault trees, event trees, and other traditional hazard analysis methods, but it also includes those factors not included or poorly handled in these traditional methods such as software requirements errors, component interaction accidents, complex human decision-making errors, inadequate coordination among multiple controllers, and management and regulatory decision making. Figure 2 shows some of the types of flaws considered in an STPA analysis. Some, such as inadequate coordination of multiple controllers, are not shown. The analysis is performed on a control structure specification of the system and the black box behavior (transfer function) of the components. The transfer function may be specified in a formal specification language.

STPA first assists in identifying the safety control requirements. There are four types of inadequate control that can lead to accidents:

1. A required control action is not provided or not followed.
2. An incorrect or unsafe control action *is* provided.
3. A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence.
4. A control action required for safety is stopped too soon.

We use a table to record the results of this part of the analysis. Some entries in the table signal incorrect behavior but not a safety problem. When the table is filled for each of the identified system hazards, the identified hazardous behaviors can be translated into safety constraints (requirements) on system component behavior. This partially solves the problem of inadequate requirements leading to software-related accidents.

The next step in STPA is to determine how these unsafe control actions could occur, that is the scenarios that can lead to a hazardous system state or accident. Like HAZOP, but unlike fault trees, STPA works on a system model (the functional control structure) and guidance is provided by STPA on what to look for so that omissions of scenarios or causes are less likely to occur.

Flaws in the safety control structure identified by STPA can be used to redesign or reengineer the safety controls. In turn, the model and analysis techniques can be used to evaluate proposed changes. Changes may involve adding or strengthening communication and feedback channels in order to ensure accurate process models and thus improved decision making. Other changes may involve redistributing responsibilities, coordinating or consolidating oversight, or simply clarifying the assumptions and rules under which the system operates.

The important question, of course, is whether this works. Few formal comparisons have been made yet between STPA and traditional techniques such as fault tree analysis, but what has been done shows STPA to be very promising. Two real-world examples of using STPA are the most relevant: the use on the new U.S. Missile Defense System and the use by the Japanese Space Agency (JAXA) on the Japanese HTV (unmanned spacecraft to take cargo to the International Space Station).

For the ballistic missile defense system (BDMS), STPA was used right before the system was to be deployed and field tested. So many potential paths to inadvertent launch were identified that had not been found by previous extensive analyses on the system and on the individual system components using traditional techniques, such as fault tree analysis, that deployment and testing had to be delayed for six months to eliminate the previously unidentified scenarios. While the scenarios identified by STPA included those caused by potential component failures, as expected, new scenarios were also identified that involved unsafe interactions among the components without any component failure—each operated according to its specified requirements, but the interactions could lead to hazardous system states. These new scenarios included problems such as missing cases in the software logic of the launch control system and obscure timing relationships in the communication of signals between the system components.

In a paper written by the engineers performing the analysis [Pereira *et.al.*, 2006], two other advantages were noted:

1. The effort was bounded and predictable and assisted the engineers in scoping the efforts. Once all the defined control actions are examined, the assessment is complete.
2. As the control structure was developed and the potential inadequate control actions were identified, they were able to prioritize required changes according to which control actions have the greatest role in keeping the system from transitioning to a hazardous state.

The paper concluded:
"The STPA safety assessment methodology ... provided an orderly, organized fashion in which to conduct the analysis. The effort successfully assessed safety risks arising from the integration of the elements. The assessment provided the information necessary to characterize the residual safety risk of hazard associated with the system. The analysis and supporting data provided management a sound

basis on which to make risk acceptance decisions. Lastly, the assessment results were also used to plan mitigations for open safety risks. As changes are made to the system, the differences are assessed by updating the control structure diagrams and assessment analysis templates" [Pereira *et.al.*, 2006].

A more careful evaluation of STPA was made by JAXA for the HTV unmanned spacecraft [Ishimatsu, 2010]. Because human life on the International Space Station is involved, rigorous NASA hazard analysis standards using fault trees and other analysis methods had been employed and reviewed by NASA experts. Later, STPA was experimentally applied to the same system in an evaluation of the new technique for potential use at JAXA. All the hazard causal factors identified in the fault tree analysis were identified by STPA. But, as with the BMDS comparison, additional causal factors were identified by STPA alone. Those additional causal factors again involved those related to more subtle types of errors beyond simple component failures and those related to software defects and human errors.

Research Goal

The research goal is to demonstrate the applicability, feasibility, and relative efficacy of using STPA in the assurance to nuclear power plants. STPA has the potential to augment the existing NRC review and certification or licensing regime with the aim of not only providing means to assess hazards associated with the introduction of digital technology in nuclear power plants, but also tools to evaluate the extent to which these hazards are adequately mitigated by the encompassing system architecture and to generate recommendations for safety-driven improvements when they are needed. This research will identify if the current evaluation framework can be made more efficient and more effective by the use of STPA and which aspects of the current framework might benefit. It will also demonstrate how STPA can fit within the existing NRC regulatory framework for validating retrofit of old plants and certification or licensing of new reactor designs that include safety-related digital systems. We expect that STPA could be an effective method (at the "guidance" level) to meet the requirements set by NRC regulation, but this needs to be demonstrated.

Research Plan:

To accomplish the goal, we plan to apply STPA to a digital platform and one of the associated safety-related applications. Performing this analysis and comparing its results to the supporting evidence provided by the license applicant for safety assurance will enable us to judge whether STPA has the potential to better inform the safety evaluation of digital systems than currently used design and hazard assessment methodologies. For example, we want to determine whether STPA provides additional information of relevance to decision making than can be provided by the current technologies.

Selection of the test bed to be used in the research will be based on the availability of design information for it and the topical usefulness of its evaluation. From our preliminary investigations, it appears that the description made available by Areva and the NRC for the US EPR I&C digital platform (previously certified by the NRC) and the description that is provided of its Reactor Protective System (RPS) application are likely to meet both these goals.

Oconee's I&C digital upgrade offers an example of the design of such a digital system,

including Areva's Teleperm XS RPS and the Engineered Safeguards Protection System1 (ESPS) [NEI, 2011]. This system design has four redundant protection channels that monitor safety-related plant parameters and generate reactor trip signals to protect the fuel and fuel cladding, the reactor coolant system and the reactor building from damage when any of the monitored parameters exceed their trip set points. The digital ESPS consists of two subsystems, each of which consists of three instrument input channels. Each pair of channels shares process variable sensors and contains the signal processing, conditioning and isolation equipment for each plant variable and control signal monitored, power supplies, and equipment for analyzing the plant variables to determine if a protective action is required. When power is lost, the RPS fails to the tripped state, and the ESPS fails to the non-actuated state.

Oconee's new digital RPS features redundant sensors, measuring channels, logic, and actuation devices. The RPS initiates a reactor trip when any two of these four channels detects an exceeded safety limit. Each of these four protective layers is physically separated from the others and runs on a separate power source. Similarly, the ESPS initiates an output signal when any two of its three protective channels (also physically and electrically isolated from each other) detect an exceeded safety limit.
Not only are the physical aspects of the system unique compared to traditional technology in similar systems, but human operator requirements also change, such as the assumption that the additional engineered safeguard channels and online monitoring (OLM) and diagnostic capabilities will reduce periodic operator checks of system performance [NEI, 2011].

Areva has argued that Teleperm XS (TXS) achieves functional diversity by "dividing the... system into independent subsystems which... execute different I&C functions for handling one and the same event." Areva also pointed to such TXS features as asynchronous operation, the absence of process-driven interrupts, 'watchdog monitoring,' clearly defined rules for use of the software functional blocks including exception handling, and fail-safe operation when a software error is detected. We will demonstrate how to evaluate these assertions.
The other major problem with digital systems of concern to the NRC is cyber security. STPA has not yet been applied to this problem, but we believe it has potential. We plan to create additions to STPA to evaluate cyber security risks and demonstrate them on Oconee's cyber security design protections.

To achieve these goals, we plan to

1. Review the existing regulatory framework and analysis methods used to perform safety analysis and certification of digital systems in
a. The US nuclear industry
b. Abroad (esp. Canada and France)
c. In other industries (e.g. civil aviation), comparing the technical and regulatory practices in these industries to the procedures and problems in the nuclear power industry
2. Perform STPA on the US EPR reactor protective system's digital control system
3. Compare the results of the STPA analysis with Areva's safety analysis as it was submitted to the NRC
4. If our results show improvement of the safety assessment, propose modification of NRC guidance to include the STPA framework as a means to identify hazards and ensure safe design.

5. Investigate the applicability and feasibility of using STAMP for cyber security in nuclear power plants.

The deliverable will be a report and Ph.D. dissertation presenting the results of the five research steps listed above.

Attachment C – Standard Terms and Conditions

The Nuclear Regulatory Commission's
Standard Terms and Conditions for U.S. Nongovernmental Grantees

Preface

This award is based on the application submitted to, and as approved by, the Nuclear Regulatory Commission (NRC) under the authorization 42 USC 2051(b) pursuant to section 31b and 141b of the Atomic Energy Act of 1954, as amended, and is subject to the terms and conditions incorporated either directly or by reference in the following:

- Grant program legislation and program regulation cited in this Notice of Grant Award.
- Restrictions on the expenditure of Federal funds in appropriation acts, to the extent those restrictions are pertinent to the award.
- Code of Federal Regulations/Regulatory Requirements - 2 CFR 215 Uniform Administrative Requirements For Grants And Agreements With Institutions Of Higher Education, Hospitals, And Other Non-Profit Organizations (OMB Circulars), as applicable.

To assist with finding additional guidance for selected items of cost as required in 2 CRF 220, 2 CFR 225, and 2 CFR 230 this URL to the Office of Management and Budget Cost Circulars is included for reference to:
A-21 (now 2 CFR 220)
A-87 (now 2 CFR 225)
A-122 (now 2 CFR 230
A-102:

http://www.whitehouse.gov/omb/circulars_index-ffm

Any inconsistency or conflict in terms and conditions specified in the award will be resolved according to the following order of precedence: public laws, regulations, applicable notices published in the Federal Register, Executive Orders (EOs), Office of Management and Budget (OMB) Circulars, the Nuclear Regulatory Commission's (NRC) Mandatory Standard Provisions, special award conditions, and standard award conditions.

Certifications and Representations: These terms incorporate the certifications and representations required by statute, executive order, or regulation that were submitted with the SF424B application through Grants.gov.

I. Mandatory General Requirements
The order of these requirements does not make one requirement more important than any other requirement.

1. Applicability of 2 CFR Part 215

a. All provisions of 2 CFR Part 215 and all Standard Provisions attached to this grant/cooperative agreement are applicable to the Grantee and to sub-recipients which meet the definition of "Grantee" in Part 215, unless a section specifically excludes a sub-recipient from coverage. The Grantee and any sub-recipients must, in addition to the assurances made as part of the application, comply and require each of its sub-awardees employed in the completion of the project to comply with Subpart C of 2 CFR 215 and include this term in lower-tier (subaward) covered transactions.

b. Grantees must comply with monitoring procedures and audit requirements in accordance with OMB Circular A-133. < http://www.whitehouse.gov/omb/circulars/a133_compliance/08/08toc.aspx >

2. Award Package

§ 215.41 Grantee responsibilities.
The Grantee is obligated to conduct such project oversight as may be appropriate, to manage the funds with prudence, and to comply with the provisions outlined in 2 CFR 215.41 Within this framework, the Principal Investigator (PI) named on the award face page, Block 11, is responsible for the scientific or technical direction of the project and for preparation of the project performance reports. This award is funded on a cost reimbursement basis not to exceed the amount awarded as indicated on the face page, Block 16., and is subject to a refund of unexpended funds to NRC.

The standards contained in this section do not relieve the Grantee of the contractual responsibilities arising under its contract(s). The Grantee is the responsible authority, without recourse to the NRC, regarding the settlement and satisfaction of all contractual and administrative issues arising out of procurements entered into in support of an award or other agreement. This includes disputes, claims, protests of award, source evaluation or other matters of a contractual nature. Matters concerning violation of statute are to be referred to such Federal, State or local authority as may have proper jurisdiction.

Subgrants
Appendix A to Part 215—Contract Provisions

Sub-recipients, sub-awardees, and contractors have no relationship with NRC under the terms of this grant/cooperative agreement. All required NRC approvals must be directed through the Grantee to NRC. See 2 CFR 215 and 215.41.

Nondiscrimination
(This provision is applicable when work under the grant/cooperative agreement is performed in the U.S. or when employees are recruited in the U.S.)

No U.S. citizen or legal resident shall be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity funded by this award on the basis of race, color, national origin, age, religion, handicap, or sex. The Grantee agrees to comply with the non-discrimination requirements below:

Title VI of the Civil Rights Act of 1964 (42 USC §§ 2000d et seq)
Title IX of the Education Amendments of 1972 (20 USC §§ 1681 et seq)
Section 504 of the Rehabilitation Act of 1973,as amended (29 USC § 794)
The Age Discrimination Act of 1975, as amended (42 USC §§ 6101 et seq)

The Americans with Disabilities Act of 1990 (42 USC §§ 12101 et seq)
Parts II and III of EO 11246 as amended by EO 11375 and 12086.
EO 13166, "Improving Access to Services for Persons with Limited English Proficiency."
Any other applicable non-discrimination law(s).

Generally, Title VI of the Civil Rights Act of 1964, 42 USC § 2000e et seq, provides that it shall be an unlawful employment practice for an employer to discharge any individual or otherwise to discriminate against an individual with respect to compensation, terms, conditions, or privileges of employment because of such individual's race, color, religion, sex, or national origin. However, Title VI, 42 USC § 2000e-1(a), expressly exempts from the prohibition against discrimination on the basis of religion, a religious corporation, association, educational institution, or society with respect to the employment of individuals of a particular religion to perform work connected with the carrying on by such corporation, association, educational institution, or society of its activities.

Modifications/Prior Approval
NRC's prior written approval may be required before a Grantee makes certain budget modifications or undertakes particular activities. If NRC approval is required for changes in the grant or cooperative agreement, it must be requested of, and obtained from, the NRC Grants Officer in advance of the change or obligation of funds. All requests for NRC prior approval should be made, in writing (which includes submission by e-mail), to the designated Grants Specialist and Program Office no later than 30 days before the proposed change. The request must be signed by both the PI and the authorized organizational official. Failure to obtain prior approval, when required, from the NRC Grants Officer may result in the disallowance of costs, or other enforcement action within NRC's authority.

Lobbying Restrictions
The Grantee will comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

The Grantee shall comply with provisions of 31 USC § 1352. This provision generally prohibits the use of Federal funds for lobbying in the Executive or Legislative Branches of the Federal Government in connection with the award, and requires disclosure of the use of non-Federal funds for lobbying.

The Grantee receiving in excess of $100,000 in Federal funding shall submit a completed Standard Form (SF) LLL, "Disclosure of Lobbying Activities," regarding the use of non-Federal funds for lobbying within 30 days following the end of the calendar quarter in which there occurs any event that requires disclosure or that materially affects the accuracy of the information contained in any disclosure form previously filed. The Grantee must submit the SF-LLL, including those received from sub-recipients, contractors, and subcontractors, to the Grants Officer.

§ 215.13 Debarment And Suspension.
The Grantee agrees to notify the Grants Officer immediately upon learning that it or any of its principals:

(1) Are presently excluded or disqualified from covered transactions by any Federal department or agency;

(2) Have been convicted within the preceding three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, receiving stolen property, making false claims, or obstruction of justice; commission of any other offense indicating a lack of business integrity or business honesty that seriously and directly affects your present responsibility;

(3) Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with commission of any of the offenses enumerated in paragraph (1)(b); and

(4) Have had one or more public transactions (Federal, State, or local) terminated for cause or default within the preceding three years.

b. The Grantee agrees that, unless authorized by the Grants Officer, it will not knowingly enter into any subgrant or contracts under this grant/cooperative agreement with a person or entity that is included on the Excluded Parties List System (http://epls.arnet.gov).

The Grantee further agrees to include the following provision in any subgrant or contracts entered into under this award:

'Debarment, Suspension, Ineligibility, and Voluntary Exclusion

The Grantee certifies that neither it nor its principals is presently excluded or disqualified from participation in this transaction by any Federal department or agency. The policies and procedures applicable to debarment, suspension, and ineligibility under NRC-financed transactions are set forth in 2 CFR Part 180.'

Drug-Free Workplace
The Grantee must be in compliance with The Federal Drug Free Workplace Act of 1988. The policies and procedures applicable to violations of these requirements are set forth in 41 USC 702.

Implementation of E.O. 13224 -- Executive Order On Terrorist Financing
The Grantee is reminded that U.S. Executive Orders and U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. It is the legal responsibility of the Grantee to ensure compliance with these Executive Orders and laws. This provision must be included in all contracts/sub-awards issued under this grant/cooperative agreement.

Award Grantees must comply with Executive Order 13224, Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism. Information about this Executive Order can be found at: www.fas.org/irp/offdocs/eo/eo-13224.htm.

Procurement Standards. § 215.40-48
Sections 215.41 through 215.48 set forth standards for use by Grantees in establishing procedures for the procurement of supplies and other expendable property, equipment, real property and other services with Federal funds. These standards are furnished to ensure that

such materials and services are obtained in an effective manner and in compliance with the provisions of applicable Federal statutes and executive orders. No additional procurement standards or requirements shall be imposed by the Federal awarding agencies upon Grantees, unless specifically required by Federal statute or executive order or approved by OMB.

Travel
Travel must be in accordance with the Grantee's Travel Regulations or the US Government Travel Policy and Regulations at: www.gsa.gov/federaltravelregulation and the per diem rates set forth at: www.gsa.gov/perdiem, absent Grantee's travel regulation. Travel costs for the grant must be consistent with provisions as established in Appendix A to 2 CFR 220 (J.53). All other travel, domestic or international, must not increase the total estimated award amount.

Domestic Travel:
Domestic travel is an appropriate charge to this award and prior authorization for specific trips are not required, if the trip is identified in the Grantee's approved program description and approved budget. Domestic trips not stated in the approved budget require the written prior approval of the Grants Officer, and must not increase the total estimated award amount.

All common carrier travel reimbursable hereunder shall be via the least expensive class rates consistent with achieving the objective of the travel and in accordance with the Grantee's policies and practices. Travel by first-class travel is not authorized unless prior approval is obtained from the Grants Officer.

International Travel:
International travel requires PRIOR written approval by the Project Officer and the Grants Officer, even if the international travel is stated in the approved program description and the approved budget.

The Grantee shall comply with the provisions of the Fly American Act (49 USC 40118) as implemented through 41 CFR 301-10.131 through 301-10.143.

Property and Equipment Management Standards
Property and equipment standards of this award shall follow provisions as established in 2 CFR 215.30-37.

Procurement Standards
Procurement standards of this award shall follow provisions as established in 2 CFR 215.40-48

Intangible and Intellectual Property
Intangible and intellectual property of this award shall generally follow provisions established in 2 CFR 215.36.

Inventions Report - The Bayh-Dole Act (P.L. 96-517) affords Grantees the right to elect and retain title to inventions they develop with funding under an NRC grant award ("subject inventions"). In accepting an award, the Grantee agrees to comply with applicable NRC policies, the Bayh-Dole Act, and its Government-wide implementing regulations found at Title 37, Code of Federal Regulations (CFR) Part 401. A significant part of the regulations require that the Grantee report all subject inventions to the awarding agency (NRC) as well as include an acknowledgement of federal support in any patents. NRC participates in the trans-government Interagency Edison system (http://www.iedison.gov) and expects NRC funding Grantees to use this system to comply with Bayh-Dole and related intellectual property reporting

requirements. The system allows for Grantees to submit reports electronically via the Internet. In addition, the invention must be reported in continuation applications (competing or non-competing).

Patent Notification Procedures- Pursuant to EO 12889, NRC is required to notify the owner of any valid patent covering technology whenever the NRC or its financial assistance Grantees, without making a patent search, knows (or has demonstrable reasonable grounds to know) that technology covered by a valid United States patent has been or will be used without a license from the owner. To ensure proper notification, if the Grantee uses or has used patented technology under this award without license or permission from the owner, the Grantee must notify the Grants Officer. This notice does not necessarily mean that the Government authorizes and consents to any copyright or patent infringement occurring under the financial assistance.

Data, Databases, and Software - The rights to any work produced or purchased under a NRC federal financial assistance award are determined by 2 CFR 215.36. Such works may include data, databases or software. The Grantee owns any work produced or purchased under a NRC federal financial assistance award subject to NRC's right to obtain, reproduce, publish or otherwise use the work or authorize others to receive, reproduce, publish or otherwise use the data for Government purposes.

Copyright - The Grantee may copyright any work produced under a NRC federal financial assistance award subject to NRC's royalty-free nonexclusive and irrevocable right to reproduce, publish or otherwise use the work or authorize others to do so for Government purposes. Works jointly authored by NRC and Grantee employees may be copyrighted but only the part authored by the Grantee is protected because, under 17 USC § 105, works produced by Government employees are not copyrightable in the United States. On occasion, NRC may ask the Grantee to transfer to NRC its copyright in a particular work when NRC is undertaking the primary dissemination of the work. Ownership of copyright by the Government through assignment is permitted under 17 USC § 105.

Records Retention and Access Requirements for records of the Grantee shall follow established provisions in 2 CFR 215.53.

Organizational Prior Approval System
In order to carry out its responsibilities for monitoring project performance and for adhering to award terms and conditions, each Grantee organization shall have a system to ensure that appropriate authorized officials provide necessary organizational reviews and approvals in advance of any action that would result in either the performance or modification of an NRC supported activity where prior approvals are required, including the obligation or expenditure of funds where the governing cost principles either prescribe conditions or require approvals.

The Grantee shall designate an appropriate official or officials to review and approve the actions requiring NRC prior approval. Preferably, the authorized official(s) should be the same official(s) who sign(s) or countersign(s) those types of requests that require prior approval by NRC. The authorized organization official(s) shall not be the principal investigator or any official having direct responsibility for the actual conduct of the project, or a subordinate of such individual.

Conflict Of Interest Standards for this award shall follow OCOI requirements set forth in Section 170A of the Atomic Energy Act of 1954, as amended, and provisions set forth at 2 CFR 215.42 Codes of Conduct.

Dispute Review Procedures

a. Any request for review of a notice of termination or other adverse decision should be addressed to the Grants Officer. It must be postmarked or transmitted electronically no later than 30 days after the postmarked date of such termination or adverse decision from the Grants Officer.

b. The request for review must contain a full statement of the Grantee's position and the pertinent facts and reasons in support of such position.

c. The Grants Officer will promptly acknowledge receipt of the request for review and shall forward it to the Director, Office of Administration, who shall appoint an intra-agency Appeal Board to review a grantee appeal of an agency action, if required, which will consist of the program office director, the Deputy Director of Office of Administration, and the Office of General Counsel.

d. Pending resolution of the request for review, the NRC may withhold or defer payments under the award during the review proceedings.

e. The review committee will request the Grants Officer who issued the notice of termination or adverse action to provide copies of all relevant background materials and documents. The committee may, at its discretion, invite representatives of the Grantee and the NRC program office to discuss pertinent issues and to submit such additional information as it deems appropriate. The chairman of the review committee will insure that all review activities or proceedings are adequately documented.

f. Based on its review, the committee will prepare its recommendation to the Director, Office of Administration, who will advise the parties concerned of his/her decision.

Termination and Enforcement. Termination of this award by default or by mutual consent shall follow provisions as established in 2 CFR 215.60-62.

Monitoring and Reporting § 215.50-53

a. Grantee Financial Management systems must comply with the established provisions in 2 CFR 215.21

- Payment – 2 CFR 215.22
- Cost Share – 2 CFR 215.23
- Program Income – 2 CFR 215.24
    - Earned program income, if any, shall be added to funds committed to the project by the NRC and Grantee and used to further eligible project or program objectives or deducted from the total project cost allowable cost as directed by the Grants Officer or the terms and conditions of award.
- Budget Revision – 2 CFR 215.25

- The Grantee is required to report deviations from the approved budget and program descriptions in accordance with 2 CFR 215.25,and request prior written approval from the Program Officer and the Grants Officer.
- The Grantee is not authorized to rebudget between direct costs and indirect costs without written approval of the Grants Officer.
- The Grantee is authorized to transfer funds among direct cost categories up to a cumulative 10 percent of the total approved budget. The Grantee is not allowed to transfer funds if the transfer would cause any Federal appropriation to be used for purposes other than those consistent with the original intent of the appropriation.
- Allowable Costs – 2 CFR 215.27

b. **Federal Financial Reports**

The Grantee shall submit a "Federal Financial Report" (SF-425) on a quarterly basis for the periods ending March 31, June 30, September 30, and December 31, or any portion thereof, unless otherwise specified in a special award condition. Reports are due no later than 30 days following the end of each reporting period. A final SF-425 is due within 90 days after expiration of the award. The report should be submitted electronically to: Grants_FFR@NRC.GOV. ***(NOTE: There is an underscore between Grants and FFR).***

Period of Availability of Funds 2 CFR § 215.28

a. Where a funding period is specified, a Grantee may charge to the grant only allowable costs resulting from obligations incurred during the funding period and any pre-award costs authorized by the NRC.

b. Unless otherwise authorized in 2 CFR 215.25(e)(2) or a special award condition, any extension of the award period can only be authorized by the Grants Officer in writing. Verbal or written assurances of funding from other than the Grants Officer shall not constitute authority to obligate funds for programmatic activities beyond the expiration date.

c. The NRC has no obligation to provide any additional prospective or incremental funding. Any modification of the award to increase funding and to extend the period of performance is at the sole discretion of the NRC.

d. Requests for extensions to the period of performance should be sent to the Grants Officer at least 30 days prior to the grant/cooperative agreement expiration date. Any request for extension after the expiration date may not be honored.

Automated Standard Application For Payments (ASAP) Procedures

Unless otherwise provided for in the award document, payments under this award will be made using the Department of Treasury's Automated Standard Application for Payment (ASAP) system < http://www.fms.treas.gov/asap/ >. Under the ASAP system, payments are made through preauthorized electronic funds transfers, in accordance with the requirements of the Debt Collection Improvement Act of 1996. In order to receive payments under ASAP, Grantees are required to enroll with the Department of Treasury, Financial Management Service, and Regional Financial Centers, which allows them to use the on-line method of withdrawing funds from their ASAP established accounts. The following information will be required to make withdrawals under ASAP: (1) ASAP account number – the award number found on the cover sheet of the award; (2) Agency Location Code (ALC) – 31000001; and Region Code. Grantees

enrolled in the ASAP system do not need to submit a "Request for Advance or Reimbursement" (SF-270), for payments relating to their award.

Audit Requirements

Organization-wide or program-specific audits shall be performed in accordance with the Single Audit Act Amendments of 1996, as implemented by OMB Circular A-133, "Audits of States, Local Governments, and Non-Profit Organizations." http://www.whitehouse.gov/omb/circulars/a133/a133.html Grantees are subject to the provisions of OMB Circular A-133 if they expend $500,000 or more in a year in Federal awards.

The Form SF-SAC and the Single Audit Reporting packages for fiscal periods ending on or after January 1, 2008 must be submitted online.

1. Create your online report ID at http://harvester.census.gov/fac/collect/ddeindex.html
2. Complete the Form SF-SAC
3. Upload the Single Audit
4. Certify the Submission
5. Click "Submit."

Organizations expending less than $500,000 a year are not required to have an annual audit for that year but must make their grant-related records available to NRC or other designated officials for review or audit.

III. Programmatic Requirements

Performance (Technical) Reports

a. The Grantee shall submit performance (technical) reports electronically to the NRC Project Officer and Grants Officer on a quarterly basis unless otherwise authorized by the Grants Officer. Performance reports should be sent to the Program Officer and Technical Analyst at the email address indicated in Block 12 of the Notice of Award, and to the Grants Officer at: Grants_PPR.Resource@NRC.GOV. ***(NOTE: There is an underscore between Grants and PPR).***

b. Unless otherwise specified in the award provisions, performance (technical) reports shall contain brief information as prescribed in the applicable uniform administrative requirements 2 CFR §215.51 which are incorporated in the award.

c. The Office of Regulatory Research requires the submission of progress reports on the SF-RPPR on a quarterly basis for the periods ending March 31, June 30, September 30, and December 31, or any portion thereof, unless otherwise specified in a special award condition. Reports are due no later than 30 days following the end of each reporting period.

Unsatisfactory Performance

Failure to perform the work in accordance with the terms of the award and maintain at least a satisfactory performance rating or equivalent evaluation may result in designation of the Grantee as high risk and assignment of special award conditions or other further action as specified in the standard term and condition entitled "Termination."

Failure to comply with any or all of the provisions of the award may have a negative impact on future funding by NRC and may be considered grounds for any or all of the following actions:

Failure to comply with any or all of the provisions of the award may have a negative impact on future funding by NRC and may be considered grounds for any or all of the following actions: establishment of an accounts receivable, withholding of payments under any NRC award, changing the method of payment from advance to reimbursement only, or the imposition of other special award conditions, suspension of any NRC active awards, and termination of any NRC award.

Other Federal Awards With Similar Programmatic Activities
The Grantee shall immediately provide written notification to the NRC Project Officer and the Grants Officer in the event that, subsequent to receipt of the NRC award, other financial assistance is received to support or fund any portion of the program description incorporated into the NRC award. NRC will not pay for costs that are funded by other sources.

Prohibition Against Assignment By The Grantee
The Grantee shall not transfer, pledge, mortgage, or otherwise assign the award, or any interest therein, or any claim arising thereunder, to any party or parties, banks, trust companies, or other financing or financial institutions without the express written approval of the Grants Officer.

Site Visits
The NRC, through authorized representatives, has the right, at all reasonable times, to make site visits to review project accomplishments and management control systems and to provide such technical assistance as may be required. If any site visit is made by the NRC on the premises of the Grantee or contractor under an award, the Grantee shall provide and shall require his/her contractors to provide all reasonable facilities and assistance for the safety and convenience of the Government representative in the performance of their duties. All site visits and evaluations shall be performed in such a manner as will not unduly delay the work.

IV. Miscellaneous Requirements

Criminal and Prohibited Activities
a. The Program Fraud Civil Remedies Act (31 USC §§ 3801-3812), provides for the imposition of civil penalties against persons who make false, fictitious, or fraudulent claims to the Federal government for money (including money representing grant/cooperative agreements, loans, or other benefits.)

b. False statements (18 USC § 287), provides that whoever makes or presents any false, fictitious, or fraudulent statements, representations, or claims against the United States shall be subject to imprisonment of not more than five years and shall be subject to a fine in the amount provided by 18 USC § 287.

c. False Claims Act (31 USC 3729 et seq), provides that suits under this Act can be brought by the government, or a person on behalf of the government, for false claims under federal assistance programs.

d. Copeland "Anti-Kickback" Act (18 USC § 874), prohibits a person or organization engaged in a federally supported project from enticing an employee working on the project from giving up a part of his compensation under an employment contract.

American-Made Equipment And Products
Grantees are herby notified that they are encouraged, to the greatest extent practicable, to purchase American-made equipment and products with funding provided under this award.

Increasing Seat Belt Use in the United States
Pursuant to EO 13043, Grantees should encourage employees and contractors to enforce on-the-job seat belt policies and programs when operating company-owned, rented or personally-owned vehicle.

Federal Leadership of Reducing Text Messaging While Driving
Pursuant to EO 13513, Grantees should encourage employees, sub-awardees, and contractors to adopt and enforce policies that ban text messaging while driving company-owned, rented vehicles or privately owned vehicles when on official Government business or when performing any work for or on behalf of the Federal Government.

Federal Employee Expenses
Federal agencies are generally barred from accepting funds from a Grantee to pay transportation, travel, or other expenses for any Federal employee unless specifically approved in the terms of the award. Use of award funds (Federal or non-Federal) or the Grantee's provision of in-kind goods or services, for the purposes of transportation, travel, or any other expenses for any Federal employee may raise appropriation augmentation issues. In addition, NRC policy prohibits the acceptance of gifts, including travel payments for Federal employees, from Grantees or applicants regardless of the source.

Minority Serving Institutions (MSIs) Initiative
Pursuant to EOs 13256, 13230, and 13270, NRC is strongly committed to broadening the participation of MSIs in its financial assistance program. NRC's goals include achieving full participation of MSIs in order to advance the development of human potential, strengthen the Nation's capacity to provide high-quality education, and increase opportunities for MSIs to participate in and benefit form Federal financial assistance programs. NRC encourages all applicants and Grantees to include meaningful participations of MSIs. Institutions eligible to be considered MSIs are listed on the Department of Education website: http://www.ed.gov/about/offices/list/ocr/edlite-minorityinst.html

Research Misconduct
Scientific or research misconduct refers to the fabrication, falsification, or plagiarism in proposing, performing, or reviewing research, or in reporting research results. It does not include honest errors or differences of opinions. The Grantee organization has the primary responsibility to investigate allegations and provide reports to the Federal Government. Funds expended on an activity that is determined to be invalid or unreliable because of scientific misconduct may result in a disallowance of costs for which the institution may be liable for repayment to the awarding agency. The Office of Science and Technology Policy at the White House published in the Federal Register on December 6, 2000, a final policy that addressed research misconduct. The policy was developed by the National Science and Technology Council (65 FR 76260). The NRC requires that any allegation be submitted to the Grants Officer, who will also notify the OIG of such allegation. Generally, the Grantee organization shall investigate the allegation and submit its findings to the Grants Officer. The NRC may accept the Grantee's findings or proceed with its own investigation. The Grants Officer shall inform the Grantee of the NRC's final determination.

Publications, Videos, and Acknowledgment of Sponsorship
Publication of the results or findings of a research project in appropriate professional journals and production of video or other media is encouraged as an important method of recording and reporting scientific information. It is also a constructive means to expand access to federally

funded research. The Grantee is required to submit a copy to the NRC and when releasing information related to a funded project include a statement that the project or effort undertaken was or is sponsored by the NRC. The Grantee is also responsible for assuring that every publication of material (including Internet sites and videos) based on or developed under an award, except scientific articles or papers appearing in scientific, technical or professional journals, contains the following disclaimer:

> "This [report/video] was prepared by [Grantee name] under award [number] from [name of operating unit], Nuclear Regulatory Commission. The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the view of the [name of operating unit] or the US Nuclear Regulatory Commission."

Trafficking In Victims Protection Act Of 2000 (as amended by the Trafficking Victims Protection Reauthorization Act of 2003)

Section 106(g) of the Trafficking In Victims Protection Act Of 2000 (as amended as amended, directs on a government-wide basis that:

"any grant, contract, or cooperative agreement provided or entered into by a Federal department or agency under which funds are to be provided to a private entity, in whole or in part, shall include a condition that authorizes the department or agency to terminate the grant, contract, or cooperative agreement, without penalty, if the grantee or any subgrantee, or the contractor or any subcontractor (i) engages in severe forms of trafficking in persons or has procured a commercial sex act during the period of time that the grant, contract, or cooperative agreement is in effect, or (ii) uses forced labor in the performance of the grant, contract, or cooperative agreement." (22 U.S.C. § 7104(g)).

Award Term

2 CFR 170.220 directs agencies to include the following text to each grant award to a non-federal entity if the total funding is $25,000 or more in Federal funding.

Reporting Subawards and Executive Compensation.

a. *Reporting of first-tier subawards.*

1. *Applicability.* Unless you are exempt as provided in paragraph d. of this award term, you must report each action that obligates $25,000 or more in Federal funds that does not include Recovery funds (as defined in section 1512(a)(2) of the American Recovery and Reinvestment Act of 2009, Pub. L. 111–5) for a subaward to an entity (see definitions in paragraph e. of this award term).

2. *Where and when to report.*

i. You must report each obligating action described in paragraph a.1. of this award term to *http://www.fsrs.gov.*

ii. For subaward information, report no later than the end of the month following the month in which the obligation was made. (For example, if the obligation was made on November 7, 2010, the obligation must be reported by no later than December 31, 2010.)

3. *What to report.* You must report the information about each obligating action that the submission instructions posted at *http://www.fsrs.gov specify.*

b. *Reporting Total Compensation of Recipient Executives.*

1. *Applicability and what to report.* You must report total compensation for each of your five most highly compensated executives for the preceding completed fiscal year, if—

i. the total Federal funding authorized to date under this award is $25,000 or more;

ii. in the preceding fiscal year, you received—

(A) 80 percent or more of your annual gross revenues from Federal procurement contracts (and subcontracts) and Federal financial assistance subject to the Transparency Act, as defined at 2 CFR 170.320 (and subawards); and

(B) $25,000,000 or more in annual gross revenues from Federal procurement contracts (and subcontracts) and Federal financial assistance subject to the Transparency Act, as defined at 2 CFR 170.320 (and subawards); and

iii. The public does not have access to information about the compensation of the executives through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986. (To determine if the public has access to the compensation information, see the U.S. Security and Exchange Commission total compensation filings at *http://www.sec.gov/answers/execomp.htm.*)

2. *Where and when to report.* You must report executive total compensation described in paragraph b.1. of this award term:

i. As part of your registration profile at *http://www.ccr.gov.*

ii. By the end of the month following the month in which this award is made, and annually thereafter.

c. *Reporting of Total Compensation of Subrecipient Executives.*

1. *Applicability and what to report.* Unless you are exempt as provided in paragraph d. of this award term, for each first-tier subrecipient under this award, you shall report the names and total compensation of each of the subrecipient's five most highly compensated executives for the subrecipient's preceding completed fiscal year, if—

i. in the subrecipient's preceding fiscal year, the subrecipient received—

(A) 80 percent or more of its annual gross revenues from Federal procurement contracts (and subcontracts) and Federal financial assistance subject to the Transparency Act, as defined at 2 CFR 170.320 (and subawards); and

(B) $25,000,000 or more in annual gross revenues from Federal procurement contracts (and subcontracts), and Federal financial assistance subject to the Transparency Act (and subawards); and

ii. The public does not have access to information about the compensation of the executives through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986. (To determine if the public has access to the compensation information, see the U.S. Security and Exchange Commission total compensation filings at *http://www.sec.gov/answers/execomp.htm.*)

2. *Where and when to report.* You must report subrecipient executive total compensation described in paragraph c.1. of this award term:

i. To the recipient.

ii. By the end of the month following the month during which you make the subaward. For example, if a subaward is obligated on any date during the month of October of a given year (*i.e.,* between October 1 and 31), you must report any required compensation information of the subrecipient by November 30 of that year.

d. *Exemptions*

If, in the previous tax year, you had gross income, from all sources, under $300,000, you are exempt from the requirements to report:

i. Subawards,

and

ii. The total compensation of the five most highly compensated executives of any subrecipient.

e. *Definitions.* For purposes of this award term:

1. *Entity* means all of the following, as defined in 2 CFR part 25:

i. A Governmental organization, which is a State, local government, or Indian tribe;

ii. A foreign public entity;

iii. A domestic or foreign nonprofit organization;

iv. A domestic or foreign for-profit organization;

v. A Federal agency, but only as a subrecipient under an award or subaward to a non-Federal entity.

2. *Executive* means officers, managing partners, or any other employees in management positions.

3. *Subaward:*

i. This term means a legal instrument to provide support for the performance of any portion of the substantive project or program for which you received this award and that you as the recipient award to an eligible subrecipient.

ii. The term does not include your procurement of property and services needed to carry out the project or program (for further explanation, see Sec. __ .210 of the attachment to OMB Circular A–133, "Audits of States, Local Governments, and Non-Profit Organizations").

iii. A subaward may be provided through any legal agreement, including an agreement that you or a subrecipient considers a contract.

4. *Subrecipient* means an entity that:

i. Receives a subaward from you (the recipient) under this award; and

ii. Is accountable to you for the use of the Federal funds provided by the subaward.

5. *Total compensation* means the cash and noncash dollar value earned by the executive during the recipient's or subrecipient's preceding fiscal year and includes the following (for more information see 17 CFR 229.402(c)(2)):

i. *Salary and bonus.*

ii. *Awards of stock, stock options, and stock appreciation rights.* Use the dollar amount recognized for financial statement reporting purposes with respect to the fiscal year in accordance with the Statement of Financial Accounting Standards No. 123 (Revised 2004) (FAS 123R), Shared Based Payments.

iii. *Earnings for services under non-equity incentive plans.* This does not include group life, health, hospitalization or medical reimbursement plans that do not discriminate in favor of executives, and are available generally to all salaried employees.

iv. *Change in pension value.* This is the change in present value of defined benefit and actuarial pension plans.

v. *Above-market earnings on deferred compensation which is not tax-qualified.*

vi. Other compensation, if the aggregate value of all such other compensation (e.g. severance, termination payments, value of life insurance paid on behalf of the employee, perquisites or property) for the executive exceeds $10,000.