Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Advisory Committee on Reactor Safeguards 582nd Meeting
Docket Number:	(n/a)
Location:	Rockville, Maryland
Date:	Friday, April 8, 2011

Work Order No.: NRC-821 Pages 1-73

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1323 Rhode Island Avenue, N.W.
Washington, D.C. 20005
(202) 234-4433

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, as reported herein, is a record of the discussions recorded at the meeting.

This transcript has not been reviewed, corrected, and edited, and it may contain inaccuracies.

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

582ND MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

OPEN SESSION

+ + + + +

FRIDAY

APRIL 8, 2011

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B3, 11545 Rockville Pike, at 10:00 a.m., Said Abdel-Khalik, Chairman, presiding.

COMMITTEE MEMBERS:

SAID ABDEL-KHALIK, Chairman

J. SAM ARMIJO, Vice Chairman

JOHN W. STETKAR, Member-at-Large

SANJOY BANERJEE, Member

DENNIS C. BLEY, Member

CHARLES H. BROWN, Member

MICHAEL L. CORRADINI, Member

DANA A. POWERS, Member

HAROLD B. RAY, Member

JOY REMPE, Member

MICHAEL T. RYAN, Member

WILLIAM J. SHACK, Member

JOHN D. SIEBER, Member

NRC STAFF PRESENT:

AMY D'AGOSTINO, RES/DRA/HFRB

DaBIN KI, RES/DRA/HFRB

SEAN E. PETERS, RES/DRA/HFRB

JING XING, RES/DRA/HFRB

HOSSEIN NOURBAKHSH, Designated Federal Official

ALSO PRESENT:

RICHARD DEEM, BNL

JIM HIGGINS, BNL

JOHN O'HARA, BNL

TABLE OF CONTENTS

P-R-O-C-E-E-D-I-N-G-S

10:14 a.m.

CHAIRMAN ABDEL-KHALIK: The meeting will now come to order. This is the second day of the 582nd meeting of the Advisory Committee on Reactor Safeguards.

During today's meeting the Committee will consider the following: (1) human factors considerations in emerging technology in nuclear power plants; (2) future ACRS activities/report of the Planning and Procedures Subcommittee; (3) reconciliation of ACRS comments and recommendations; (4) preparation for meeting with the Commission; and (5) preparation of ACRS report.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Dr. Hossein Nourbakhsh is the Designated Federal Official for the initial portion of the meeting.

We have received no written comments or requests for time to make oral statements from members of the public regarding today's sessions.

There will be a phone bridge line. To preclude interruption of the meeting, the phone will be placed in a listen-only mode during the presentations and Committee discussions.

A transcript of portions of the meeting is being kept and it is requested that the speakers use one of the microphones, identify themselves, and speak with sufficient clarity and volume so that they can be readily heard.

At this time, we will move to the next on the agenda, human factors considerations with respect to emergency technology in nuclear power plants and Dr. Bley will lead us through this.

MEMBER BLEY: Thank you, Mr. Chairman. We're pleased to have these folks here today. A number of us ran across parts of this research during the quality reviews this year and thought that some of the things we saw that really needed to come to the attention of the Full Committee, especially with the work we're doing on design certs and new reactors and small modular reactors that are coming with advanced electronics, advanced control rooms.

This work that was -- actually cropped up earlier this week in one of our other meetings is very relevant to what we're doing. Some of us who have been concerned about the possible problems that might occur through these systems, the Committee as a group went up to Cranbury, a year or two ago, and looked at two of these new control rooms. And I think you'll see there are a lot of great advantages to these systems, but the one project that really caught our eye was one on human factors under digital I&C degradation, so we asked them to come and present this to the Committee. And I think it will be of great use to us.

I'd like to turn the floor over to Sean Peters now for this presentation.

MR. PETERS: Good morning. I'm Sean Peters. I'm the Branch Chief for the Human Factors and Reliability Branch in our Division of Risk Analysis in the Office of Nuclear Regulatory Research.

Today, I'm going to give you a really brief background of our research activities and research planning associated with advanced technology control rooms. After that, we're going to have a presentation by Dr. Jing Xing on degraded digital instrumentation and control.

And based on today's Subcommittee meeting, we heard a desire to understand a little bit about what's going on in our Concepts of Operations project, so we brought in Dr. John O'Hara to talk about our ConOps project.

I'll give you a little bit of background.

We have eight years of research going into research planning for the advanced technology control rooms that are coming forth. In 2003 and 2006, we had two workshops with the NRC and international partners to discuss the emerging technology and the current state of research and regulatory guidance.

In 2006, we began a project with Brookhaven National Laboratories that culminated in a 2008 report. You guys may be a little bit familiar with that because it culminated into our NUREG/CR-6947 which did the product quality review of the 2008-2009. Based upon the research that we did and the input to the international community and international research is going on, the Working Group of Human Organizational Factors out of the Organization for Economic Cooperation and Development issued a technical opinion paper also listing the respective areas of human factors technology that needed to be researched and further technology that needed to begin.

And subsequent to that and based upon the research that we had done in 2008, we initiated a workshop with the Working Group of Human Organizational Factors again in 2010. We expect to get a report based on the current state of knowledge within the next couple of months. That should be available that we can share with the ACRS on where we think we are now in the research process versus what else is needed based upon the current state of new and advanced plans that are coming forth.

Based upon all the information that we got from 2008 through 2010, we worked with our user's offices, NRO, to prioritize the list of human factors issues and given the amount of budget that we had, we came out with user need NRO 2010-005 that dictated which types of projects and which issues we were going to look into and give information back.

So I'm just going to give you kind of a list of the current projects that we have going on. We're going to be updating NUREG-0711. NUREG-0711, I believe, was updated back around 2004 time frame. Is that correct, John? And we have gained a lot of knowledge since 2004 and we've also implemented this, the usage of this in the new reactor applications that have come forth in the Chapter 18 reviews of NUREG-0800. And a lot of information has been learned about the respective designs that are coming and a lot of user feedback on usability and gaps in the document that are needed for at least promoting efficiency of the reviews were identified. So later this year we should have a new updated NUREG-0711. And 0711 is our human factors engineering review model. This is how we implement our NUREG-0800 review criteria for Chapter 18 events.

NUREG-0700 is our human system interface design. In 2012, we will be updating NUREG-0700, based upon all the research that we have coming forth. Based upon those two being updated, we're also updating NUREG-0800 and we're creating a NUREG-0711 companion document. This basically is a technical basis document that describes in more detail what the criteria are in NUREG-0711 to give reviewers a little more background in places these can address the criterion.

Other projects that we have going on include assessment of varying levels of automation in new and advanced control rooms. We also have a project for measuring workload situation awareness and teamwork. These are inputs that people can put into a task analysis for staffing planning at nuclear power plants.

Another project that we have going on right now in wrapping up this year will be computerized procedures, looking at the varying levels of computerized procedures. If the ACRS has gone out to new or advanced plant simulators, a lot of them are using these computerized procedures systems and each one can be different in different ways.

We're also going to be looking into the integrated system validation project. We are initiating a project within the next couple of months to update the ISB guidance for once plants are constructed to do the ISB examinations and testing from the NRC staff.

And we have a major staffing project going on right now. Dr. Jing Xing is our technical expert in the staffing area and that's going to be in support of any type of per se, NuScale or mPower type requests for reduction in staffing to help develop that technical basis.

The concepts of operation, this is what John is going to talk to you about later today. We also have a human factors engineering methods and tools project which goes into the varying methods and tools. And ISB is one of these types of tools that designers of nuclear power plants use to develop their human factors review program.

And finally, based upon all that research that's coming forth, in 2013, we're going to be updating our NUREG-0711 guidance again to incorporate all that information.

The important thing about these two projects that we're going to mention next, this is the degraded I&C project and the ConOps project, these are projects that are scoping regulatory gaps. These are ones that identify what are the human factors issues and what further do we need to look into to update our guidance.

MEMBER BLEY: ConOps is the one that came up earlier this week. It looked very interesting. Is there something coming out soon on that?

DR. O'HARA: Within the next few months.

MEMBER BLEY: Okay.

MEMBER ARMIJO: What is the full terminology for ConOps for those --

DR. O'HARA: Concept of Operations.

MEMBER ARMIJO: Concept of Operations. I would never have figured that out.

DR. O'HARA: We'll talk a lot about that in a second.

MEMBER BLEY: Are you also going to talk about all the automated procedures?

DR. O'HARA: We could. It's not directly --

MEMBER BLEY: When we were visited, the obvious things that seemed advantageous of tracking your way through all the procedures and keeping track of what you're supposed to be monitoring, but one of them we looked at, a logic display, like a fault tree that tracked complex logic through the procedures which sometimes is where people go astray. I thought that was pretty neat. If you could include that later, a little of that --

DR. O'HARA: I was actually going to say a little bit about that at the end of Jing's talk.

MEMBER BLEY: Okay. I appreciate that. Thanks.

MR. RAY: I was going to ask the question, I guess I'll do it now although it may be stated later, but -- it's a good idea, obviously, anybody that's used procedures, but is there a backup to the computer? I would assume there would be.

DR. O'HARA: In fact, that's one of the things we'll talk a little bit about when we get there.

MR. RAY: Okay, fine.

MEMBER STETKAR: It is relevant because simply having a backup is one thing.

MR. RAY: And knowing how to use it.

MEMBER STETKAR: Used to actually picking it up and you know, not slicing your hands open and remembering where things are is entirely different. We've seem some evidence that although it's there on the shelf --

DR. O'HARA: There's actually some complexities on top of that because when you use these highly-automated computerized aids, when they go away and now you revert back to paper, you change the whole way the team has to work. So it's not just a matter of running to a backup system. It's a matter of changing the way you're operating, potentially to a mode that you're not used to doing.

MEMBER STETKAR: Unless occasionally you drill on that.

MEMBER BLEY: And in five or ten years, people who come into the industry at that point won't have ever used.

MR. PETERS: And so our next presentation will be Dr. Jing Xing.

DR. XING: Thanks, ladies, gentlemen --

MR. PETERS: Hold on one second. Let me get the slides up.

DR. XING: Okay. I think I can introduce myself.

(Laughter.)

DR. XING: I'm Jing. I'm a Senior Human

Performance Engineer in Sean's branch and I joined the NRC three years ago. And as soon as you mentioned the computerized procedure project because that is one project that I actually managed. And to your earlier question, the backups, the good news to let you know in the computer writes the procedure, human factors guideline developer, there is a section specific about how the backup system should be designed to allow humans to be able to pick up when the system fails.

And also in this project that I'm going to talk, you will say there's a high-level guidance taking up that issue, the backup issue.

So okay, my slides are here now. You can just look at my slides. Next, please.

Okay, so talking about digital I&C, I would like to share this email exchange I had with my colleagues in different offices a couple of weeks ago. So a couple of weeks ago I received this email from my co-worker at the NRO. He knows I work on the digital I&C. So he sent me an email, "hey, here's a digital I&C failure." Here's a car, honk if you want to stop it.

(Laughter.)

So I sent this email to a friend that works in the Division of Engineering who was working on digital I&C. So the bottom part is cut and pasted from his email. It was much longer than this. But it gave me all the reasons why he's talking about dependency. A depends on B. B depends on C. C depends on D. At the end, you never thought A and X have any relation, but it has here.

So to me, as a human factors person I say okay, I don't understand all this logic, but human factors issues in their design, why didn't you control the complexity of your system to the levels that a human can comfortably manage it.

I talked about this to our NRO counterpart who actually implemented human factors engineering into the review process. And the big point to me, well, that's not integrated system validation issue here because they should have caught this error in the integrated system validation.

So this has been going on just because this new -- and the conclusion is, okay, I'm not going to buy this car.

(Laughter.)

MEMBER BLEY: Hundred millions lines of code.

DR. XING: So that's an easy solution to that problem with the car, but we are facing bigger issue in our nuclear power plants as we are moving to the digital age. So this picture let's you say -- on the left is the traditional analog based control room and on the right is the computer-based human system interface from a PWR in Japan.

Okay, as Mr. Chairman said earlier, as we're moving to the digital stage, safety is a concern for NRC staff. So today I will use this opportunity to talk to you about the work we did in the digital I&C area for safety.

So I'm going to talk about three topics. The first are just to briefly overview the big picture of digital I&C degradation which basically is a summary of lectures I learned from our digital I&C folks. And then I will talk about human factors research in digital I&C degradation. At the end, we will briefly discuss how our human factors research fits into the bigger picture of NRC digital I&C research plan and that's what we talked in the beginning, we want to look forward what the human factors research will be there.

Next slide.

Okay, this is a high-level picture I drew above the digital I&C system in a nuclear power plant. On the top we have plant configurations. We can imagine a number of digital systems come into the communication system, surveillance system, and all those would be digitized. And then come into the control room those power plant systems. So our digital I&C staff had been working on development of inventory of all I&C systems used in nuclear power plants. Here is just a very broad description, sensors and systems in the control room. And they are actually working on developing or calculating the percentage, how much digital components are being used in various plant systems. That's a study that they are conducting which can be very informative.

And then up the system, you come with the system sending all the sensitive information and there's an interface between the system and the human there. As you see, it's an early picture. It's new program that's going to computerize the interface, like computerize the procedures and this interacts with the human. So we're looking at all this as the connection between this entire system.

Next, please.

And our digital folks are trying to understand what's the difference? The difference is between analog and the digital I&C degradation. The analog systems, it's relatively easier, because the failure modes have been well defined by now. And essentially, we're able to -- and the failure modes are -- potential failures, we are able to pre-determine them. We know what's going to fail because of the aging and from experience.

MEMBER BROWN: I don't have -- don't take this the wrong way, able to be pre-determined and traceable are interesting concepts. All I know is I've worked analog systems for 35 to 45 years now and I have found many analog type systems where number one, we were not able to pre-determine the failure modes and number two, stuff would fail, we could never find out what went wrong, but it never failed again. And so we continued operating them.

(Laughter.)

Well, it's working now. If you can't fix something, it's not broke. And so I'm not trying to pick on it, but if somebody says that's an absolute, I would have to walk away from that thought process just based on real-world experience.

DR. XING: Thank you. I actually agree with you on that. Like I was originally trained as an electrical engineer and for the first three years, we worked with all those analog systems. We built up from the radio -- same with the resistors, capacitors, and it didn't work. To a certain level, we can trace it down.

MEMBER BROWN: You used key words, a certain level you can -- I agree with the comparison. I mean the digital systems provide a much wider range of uncertainty and failure modes with which you have to deal and they run into the same untraceable issue also. I just didn't like the absolute nature of the two statements.

MEMBER SIEBER: Spurious things are hard to track.

MEMBER BROWN: Exactly.

DR. XING: Then like --

MEMBER BROWN: I've got tell you an example just to make sure you understand us, okay?

(Laughter.)

We were trying to get a test program going on a cruiser, nuclear cruiser in 1968 or 1969, something like that. And it was at Puget Sound and for some reason we kept tripping and having noisy source range instruments that would not allow us do a startup or would shut us down or intermediate range which would scram us.

It just kept going on for weeks. We finally, finally traced to the ferry that left

Bremerton and went to the other side of the sound, but that only happened if a cover, a big steel sheet on the main deck in the front was off from protecting environment, rain, stuff, to get in, and that ferry's radar would then funnel down the passageway and would trigger the 10^{-12} impedance -- 1-^{-12}, excuse me, very high impedance input that you had and just kept getting us nuts. We were amazed. How did we ever find it, number one. It's just an example of the funny things that can happy. I'm sorry I had to tell the story.

DR. XING: I like the story. Imagine a similar situation in the digital world. At least in the analog world you have some wires, pipes allow you to trace. In the digital world, it's more like the dealing with a program for hardware and the software which you can't --

MEMBER BROWN: Ones and zeroes.

(Laughter.)

DR. XING: I'm glad you come with a number. So actually, my boss has a concern when I put the number and limited failure modes there because like last year when we went to visit in France, and asked about their failure modes in their computerized procedure, they said ah, that's easy. It's only one mode. Software failure.

(Laughter.)

MEMBER BROWN: That's about where we are, but go ahead.

(Laughter.)

I'm sorry to interrupt.

DR. XING: Our NRC folks, they told me it's unlimited failure modes, basically because you're not able to predetermine them for software. If you can determine them, you can fix it during the software development. And often you can't trace them because they go -- they gave me a 10, 12, some number of power of possibilities. You can't trace them.

So I put this picture out basically what they told me the status of where they are. There are studies of various database about digital system failures such as a COMPSIS, a computer-based safety database. And the saying is the more you know, you feel the sense the more you don't know. So it's like the revealed failures are merely the tip part of the big iceberg.

But the good thing is digital I&C folks have identified the importance of contributing factors to the digital I&C failure such as engineer errors due to the interest in functionalities, complexity in software, interdependency amongst systems and uncertainty of verification and validation process. There's too many possibilities. You can never exhaust potential outcomes. And the faults resulting from maintenance, upgrades, and configuration changes. So these are the contributing factors.

Our engineer staff is developing guidelines to trace those factors, to try their best to reduce the possibility of failures.

In our project, we are dealing with another aspect. No matter how much you do, we know there will always be failures, data failures. So we are -- the focus of our effort is okay, we know there is failure. Then we want to understand what is the impact of the failure? And what are the treatments, like a doctor knows what's going to happen to you, give you some medicine.

So that comes to the second part of human factors research in digital I&C degradation. And this project was performed in 2007 to 2010 by Brookhaven and our branch led by Dr. John O'Hara. And the report is already out. Right now, it's the BNL report and basically about the end of this year, I promised to myself, we're going to get it published as a NUREG/CR. So if some of you haven't seen this report yet, I can send you an electronic copy.

So I will briefly summarize what we did in this project.

Next, please.

So a lot of times in the beginning when I talk to our digital I&C folks, they thought well degradation for digital I&C is an engineering job. What's the matter with human factors? Some people tend to have that kind of opinion. And the fact is plant personnel and the I&C system always work together so the operators will need to perceive basic parameters and monitor the plant's processes and just the operations as needed and the response to transients, accidents, and other failures.

So therefore, I&C degradation may significantly lower operators' ability to do their job. So that's the major objective we want to focus on this project. So break down that into three objectives.

We want to understand the impact of I&C degradations on human performance because human is a part of the whole system. And we want to develop if there's an impact there and we need to develop a technical basis for including considerations of degradation I&C, means the I&C human factors engineering activities that Sean just described earlier. And finally, we need to develop human factors review guidance on degradation I&C.

So to achieve these objectives, we first -- actually, John's team went to Oak Ridge Lab to talk to the digital folks there to find, hey, you guys have done everything we needed for this, so we can take your results for our project. Ideally, we start with when we want to have the information, the digital I&C characterization on safety and the non-safety systems. To achieve our objective, we also need to know the digital I&C failure data and the failure modes, and the data about failures on operators, on systems, and then finally on plant safety. So that's the ideal world.

Unfortunately, we were facing the reality when we found out, okay, there was no standard of digital I&C characterization. As I mentioned earlier, our digital I&C folks are still working on this. And there was limited digital I&C failure data. The modes are being studied, but haven't been developed yet. And when they went to look at the literature, there were very few studies that addressed the effect of failures on operators. Just like the email I received, most of them will tell you, hey, there's a failure, but the result is telling you how this affects the driver. But the driver case it's easy to imagine when your heart stops. But we need a solid technical basis there.

Therefore, because of this limited knowledge, we narrowed down the scope of our project to the blue part, So we take the information we know about digital I&C systems and the failures and we try to identify how they're going to impact the human system interface and how that finally impacts the crew performance. And unfortunately, at this point we haven't got enough data. We haven't really gotten into considering the grid path -- how this impact will eventually impact the system and plant safety. That's something we're thinking for the next step.

So based upon that consideration, this is the approach we take in this project. So first of all, the information was very scattered, like digital I&C people are talking one language. Our NRC operational experience event report talk in another language. And the academic research lab who may study the effect of human performance are speaking in the third language.

So we realized we need at least the first step, we need to get a generic framework to integrate this digital I&C and the human performance. So let's put everyone talking the same language, so we can collect and generalize the information. That's our first step.

The second step is develop a framework to evaluate all information available to generalize the effects of degraded I&C on human performance. And after we establish that, that's going to establish us as having the basis for regulation. Then we develop a human factors engineer review guidance.

Next, please.

So our first goal is develop a framework so as a way to link all those -- to link -- to put the I&C system HSI and human performance as an entity. The philosophy for developing this framework is we want -- because we want to develop generic guidance, so we want to keep this framework as design-independent so it does not just work for BWR or PWR or Westinghouse. So we want to identify the design-independent function element in each of those levels.

And for the specific links between these elements and between the different layers, that's going to be design specific and it's going to depend on the specific scenario, so that we cannot include in the framework.

Next, please.

So basically, the idea is the framework gives you common language, allows you to translate different information into the universal level.

So this is the framework we used. So in the I&C system, the functional element we used, DOE's very generic classification, I&C system, a sensor subsystem, monitoring system, automation control, and the communication. This is very high-level generic and in fact, this was done three years ago and our digital I&C safety for now are coming up with a much finer classification so in the future we may consider replacing the new classification.

And on the human system interfaces, luckily, Dr. John O'Hara - data division -- with the human factors community and the nuclear industry. There has been a commonly accepted classification for the human system interface which is alarm information system, operator support system such as computerized procedure and the controls and the work stations. So we already have a good classification there. And the same situation for the human side.

So what you see on the right side are the primary tasks of classification we will be using in all about human factors guidelines. The primary task as an operator is do the monitoring and detection of the system and then assess the situation and to make a response planning and implement that plan.

Besides that, there's also teamwork process with either crew and the interface management, a secondary task is managing the interface. This actually could become more an important issue with the computerized system. I think a lot of us at NRC has experienced previously use of paper to fill out travel authorization versus use of the eTravel system, how much work you have to spend on managing that interface besides your primary tasks in planning your trip.

Okay. So with that framework, we move to the next, use that to develop a technical basis. So our approach is first we use the framework to analyze the schedule information in the scientific literature, in the operational experience event. And the digital I&C failure database such as the feedwater failure database. So we use -- we take all this rote information in different areas and put them in the framework in the middle part. It belongs to this I&C system. This is part of the task that will be affected. And the functions of human performance will be affected.

So after we got this information, using

our human factors approach we can try to extract and identify --

MEMBER BLEY: Excuse me, is the -- do we have a substantial database now on degraded I&C?

DR. XING: We have some.

MEMBER BLEY: -- and operation?

DR. XING: Yes. I let John answer that question.

DR. O'HARA: Yes, the term "database" down there, basically that was a database of failure modes for a particular digital feedwater system for operating PWR. It's not a generic database of failure modes. So basically, if you look at what we did, we looked at, as it says here, the research literature, then the operating experience literature, and then we did an actual evaluation using a -- basically, we extended a failure mode in effects analysis for digital PWR -- digital feedwater system on a PWR the opposite way from the standpoint of we took the failure modes for a part of it and instead of propagating it out to see how it impacted the plant systems, we went the other way and looked at what it would show as in the human system interfaces for that feedwater system and like what kinds of conditions aren't alarmed, what would the operators know if they got that information?

So database here is referring very specifically to a particular --

MEMBER STETKAR: John, is that particular example the stuff that Louis worked on a couple of years ago?

DR. O'HARA: Yes. We used his model.

MEMBER STETKAR: Okay. We've been briefed on that, so we're familiar with that study. Calibrate the database.

DR. O'HARA: We went in the other direction is essentially what we did.

DR. XING: And also to your question, we know there is a database called the COMPSIS and maintained by IAEA on the digital failures, digitized unsafe failures in the nuclear domain. And our Division of Engineering for staff right now is working on that database, so if in the future will continue this work, that will be a good resource.

MEMBER BLEY: Did you also do something like an expert elicitation to try to generalize that? I thought you did? Am I dreaming that?

DR. O'HARA: That was part of another project.

MEMBER BLEY: Not for this.

DR. O'HARA: For not this.

MEMBER STETKAR: You said something real quick, you said IAEA. I do some work with the IAEA. What they get is at best politically filtered by about three levels of international vested interest. So I caution you using IAEA databases as if they're either data or bases.

(Laughter.)

Just past experience, honestly. The implication -- the question and it's a leading question, have you thought of reaching out to other -- there is much more experience internationally, but at the lower level people like Siemens or AREVA EDF, you know, without the -- let me just say national interest filtration you might get through the IAEA, have you thought of are you pursuing those avenues in terms of trying to compile data?

DR. XING: The answer is yes, not in specific projects, but for example, a related project in computerized procedures and we have approached Germany, and France, other countries, what kind of failures they have been experiencing so far. And also for the plants that are constructed in Finland and Sweden, other countries, we have talked, how the extended work group meeting try to exchange this information. So far, that's in a staff level information exchange, no official --

MEMBER STETKAR: I would just, you know, again, emphasize that it's easy to access information from the IAEA.

DR. XING: Definitely.

MEMBER STETKAR: The fidelity of that information is often filtered.

DR. XING: And also in the nuclear industry, we've been talking with NASAM. They have a whole bunch of database failures which could be very useful for us.

MEMBER BROWN: On the database issue, what level of data are you looking for? I mean is it -- here I've got a computing platform that's got processors on it and it's IO chips and it's filters and it's got buffers, memory, AD convertors and on and on. Is it a piece part type failure? Is it a software failure, categorized in some way based on -- I mean try and envision the types of software failures like incorrect messages or headers or footers that sent it to the wrong place or I'm just trying to get a feel. Is it hardware or you effectively said no, it's not hardware. It's not failure of processes.

DR. O'HARA: We stayed at the functional

level. This is the first time we're looking at this stuff, right? So we tried to get down to such a level, but it became very, very difficult very quickly.

MEMBER BROWN: Not surprising.

DR. O'HARA: So what we ended up doing is we backed up to a functional level.

MEMBER BROWN: Right.

DR. O'HARA: And in fact, we used the DOE Gen 4 road map piece for the I&C system and we stayed at that level, recognizing all the architectural differences that you have when you start tying these pieces together. So within each of our functional levels like sensing and monitoring, you have hardware, software. You have actually, some analog components, some digital components, but for this first pass to try to put all this information together, we stated that functional level because when we rolled -- when we look at this event that happened here and this study that EPRI did and they all use very different language. They are classifying things differently. So we use this higher level of classification to enable us to bin information together so that ultimately we can make some generalization.

MEMBER BROWN: So about functional level

-- I'm trying to connect my brain to functional level, like data that was presented incorrectly to the operator?

DR. O'HARA: Yes.

MEMBER BROWN: Or a control function where you said something was supposed to start and didn't?

DR. O'HARA: Yes, like --

MEMBER BROWN: Or stopped when it wasn't supposed to.

DR. O'HARA: Jing listed before the functional breakdown that we used. And again it's admittedly a high level functional grouping because the information we had was all over the map.

MEMBER BROWN: That's fine. You answered my questions.

DR. XING: Actually, a part of your question also can be answered in some slides that I will not go over, but is in your handout in the results section. You will see a long list of examples.

MEMBER BROWN: Okay, thank you.

DR. XING: What this data we're looking for.

Okay, so I will skip the example how we actually did the data analysis, so just let you know we did an analysis.

Okay. So after -- next slide.

Now we come to the result of the analysis. This is a very high level summary of the result. Through our analysis we established the evidence that digital I&C degradation can, in fact, affect all aspects of human performance such as what John said on the functional level, locked-up information can impact operators' situational assessment. And we also identified the human factor issues related to degraded I&C. For example, one issue you already speak of, the backup systems.

Okay, next.

I will not go over this slide, the next cover slide, but that's in answer to your question. It's detailed information, how at the functional level, the degraded I&C impact our human performance. We actually did this by breakdown into those generic functional level systems in the next four slides, impact on sensor of the degradation of sensor system.

Next.

Impacts of automation and control system failure.

Next.

Impacts of the communication system.

Next.

MEMBER STETKAR: Jing, I'm skimming through this here. I didn't notice anything that jumped out at me and perhaps because I was reading so quickly, that is uniquely associated with digital systems. In other words, sensor failures in an analog system or improper signals can result in the same -- is there anything, because of the time, is there anything in those quick things that you skimmed through that you identified as uniquely associated with the digital nature of these systems?

DR. XING: I mean that's a very good point. I may not put that in this list, but there are a number of them in this report.

MEMBER STETKAR: Okay.

DR. XING: So next time I will remember. The reason there was a mixture was because we were dealing at the functional level. And this system still is a combination of hardware and software so they don't look so --

MEMBER BLEY: We have that report, by the way.

DR. O'HARA: If I could just add one thing to John's question? A digital I&C system has, as you well know, analog and digital components. And we're looking at it as essentially a system. So you may have a failure in a sensor, right? Which is an analog component, but when it propagates up into a graphics display now you're dealing with the digital processing of that signal and the integration of that signal with lots of other information and we found a lot of effects along those lines.

MEMBER STETKAR: That's a bit more of what I was going, because the information is processed and displayed perhaps differently than real time.

DR. O'HARA: And in fact, a lot of our report sort of speaks to those differences, but in these systems, it's hard to rule out completely a sensor.

MEMBER STETKAR: Oh yes, certainly. That's a fact. I was just looking for something --

DR. O'HARA: -- took the sensors out. So we looked at that functional level, recognizing that a digital system does have analog components to it.

MEMBER STETKAR: Okay, thanks.

DR. XING: Okay, so --

MEMBER BROWN: As part of this -- I skimmed through also, so I wanted to ask this question before you finished it. One of the things we dealt with when we started putting this stuff into our shifts was the actual transition from certain types of displays, the graphics and everything, vastly improve the operators' general picture of what's going on in the plant if you can combine sensors and it puts it into a picture for you, whether its bar graphs, up and down things, or little lines or whatever.

One of the things we've found is that now you've got this screen which is taking bunches of data, integrating it and giving you this picture. If it fails. you have to transition to now I've got all my data again. I've got individual pieces of data and if the -- so we had to start making decisions. Where did we want generalized graphics which would be useful and how did we present it? And if we lost it, how did we maintain the operators' proficiency with taking and integrating the four pressure instruments instead of having a choice being made and sometimes we just decided we weren't going to -- we're going to show them all, even on the graphics display because we didn't want them to lose track of these things vary and they're not a precise number.

Is that a part? I didn't see that, the transition of what the operator perceives, his understanding of the varying parameters of the -- the same parameter being presented from a number of channels. Is that part of this overall?

DR. XING: Yes, and actually, we can -- you're just asking the next part of the presentation, the human effects.

I'm going to skip over all and basically we developed the guidelines we wanted to address in the design process, take what you just said into consideration. And number two, the guideline goes to, okay, when we design the interface exactly as you said, how the information should be presented? Should we present all, too much for operator or too late, they can't understand the whole logic? So we develop guidelines to address this. The design process and the HSI design for this particular. And the more detailed information you can find in our computerized procedural guidelines which talks more specifically the point you just mentioned, how the backup format should be consistent or compatible with computerized graphic display. So there's more information there.

Okay, I think I will try to wrap up the whole thing in the next three minutes for the next 15 slides.

Let's do some quick forward. Move forward. Forward.

This is just some examples of guidelines we have.

Move forward. And look at the examples of the guidelines. HSI design is the second one. It's HSI should support operators in determining the steps for failure recovery and the backup action. This is a very high level, general response to the question you've raised. As I say, the details will be in the computerized procedure.

Okay, next. To summarize, our data were first cut in this important area. Establish the technical basis for regulation and develop the human factor review guidance. So next, we want to have briefly -- we want to take a look where -- next.

We want to look at where we stand in the NRC's entire digital I&C research, what human factors research. So I just bring up a copy the NRC's 2010 to 2014 digital I&C research plan. I was told everybody here is an expert on this.

MEMBER BROWN: Not everybody.

(Laughter.)

DR. XING: So here at the tasks those four elements in the research plan and what we did in the analysis, analyzed which tasks because there's a human factor -- is the human factor aspect is explicitly called up such as those two in the red line. And those that are implicitly embedded. And the ones that we haven't fully analyzed and don't know, for example, like 3.1.7, diagnostics and prognosis. We know there are human factors issues there, but it's not clearly described in the project, program yet.

MEMBER BLEY: I've got a question. Is it expected, and if it is, how would it be implemented that the key issues you're identifying somehow get related to NRO, NRR, and industry and is it expected that they -- that examination for I'll call it coping mechanisms with these problems somehow gets integrated into the inspection plans for the new reactors as they come forward? We'll be past the licensing process and when they have the inspections and is it anticipated how this works its way under those procedures?

DR. XING: Yes. I will give a high-level answer to that and let John actually tell you how --

MEMBER BLEY: We should probably be asking NRO, but since you're here.

DR. XING: Actually, John is also representing NRO.

(Laughter.)

There are two phases of the implementation of the computerized first stage aspect of the human factor aspects. So high-level answer is okay, we developed this review guidance. And NRO will do the design review to make sure okay, like the guideline we develop will make sure in the design process you have considered this task analysis. When you design something, you need to do task analysis. You're not just analyzing what the operator is going to do in the normal situation. You need to analyze if there's a degradation in the system. So we'll make sure they take that into consideration.

MEMBER BLEY: But this is not reflected now, I don't think, in 711 which is what's guiding the reviews of the designs right now.

MEMBER STETKAR: And in fact, some of the designs have already been reviewed.

MEMBER BLEY: Quite a few of them.

MEMBER STETKAR: Yes, and they're out. The train has left the station. So that, for example, the thought process that might come out of this indeed is now folding over, as Dennis mentioned, into the inspection world, not a design review, but the inspection world. So I think that was the genesis of the question when you're working in that environment.

DR. XING: What's interesting is that because just yesterday when we had our human factors workshop with our users, we were talking about how to

-- we know this project, our other project has been focused on how to implement the human factor principles in the design process. However, at this point, to us, it's not completely clear how this is going to be implemented in the inspection because we keep hearing about ITAAC, ITAAC, and how the human factors aspect of this guideline would develop here. We don't know at this stage how to integrate it in there. I hope to hear direction from this Committee to direct us in that.

DR. O'HARA: May I add just one? Both NUREG-0711, the two principal guidance documents, NUREG-0711 and NUREG-0709 both already recognize I&C failure as something to be looked at. It's like broad brush -- if you think our guidance here is general, that's even more general, but we do ask about it.

So for instance, and let me just give you a very quick example because I know we're running out of time, but quick example of how this research has already informed a review process. We always ask about failures of the operator support systems as part of design certification review.

And typically, they're treated as wholesale failures. So we would ask about the computerized procedure system and it would be explained to us and shown to us how a system-like computerized procedure system, how they address its failure.

And the failures that are considered is loss of the computerized procedure system. And I'm heavily involved with those reviews and when we started to get into this, when we saw the nuances and complexities of it, we were doing an audit, on-site audit of a computerized procedure system. I won't mention whose it is, but a particular system and they were showing us yes, see, if it fails, this is what we do.

And I started to ask just because of this stuff, basically, I started to ask some questions about well, have you looked at like the effects of sensor drift or some of the key inputs that are being monitored by this procedure? Have you looked at if they fail, what happens at the interface. Or suppose your data highway is really jammed up and now we slow things down, events at nuclear plants have already happened because of that. So -- and basically, they kind of caucused together and they said, no, we haven't looked at that, but we have to. So they made a commitment to take a look at what kinds of I&C conditions such as what we're talking about here, how they might impact a crew's use of a computerized procedure system.

MEMBER STETKAR: That's great. And I think what Dennis was asking is there work in place to expand that? I hate to use the word formalize, but at least get that thought process not what is evolving into inspection guidelines rather than -- and into review, but trying to get it up front.

MEMBER BLEY: In case you get run over by a truck.

MEMBER STETKAR: That's right.

MEMBER BLEY: God forbid.

DR. O'HARA: But you guys know the way this rolls out, right? So we do this, we get some results. We have guidance that asks these very questions. That guidance gets rolled into NUREG-0711 and NUREG-0700 as they are revised. Inspection plans, I don't know. Because as far as I know the inspection plans are going to be based on the ITAAC and --

MEMBER BLEY: There's still some interpretation down there and you might find a way.

DR. O'HARA: You all probably know much better than we do, but there's some difficulty in getting new findings into those plans.

MEMBER BLEY: We asked for this as an

information briefing. We did not intend to write a letter on this. I'm starting to wonder if that was the right thing to do. But let's go ahead.

Had you guys thought about that? You weren't expecting a letter from us?

MR. PETERS: No, we weren't expecting a letter. It was purely an informational briefing, but I mean we're looking into like I said our ISV projects and looking and forming inspection procedures as they come forth. We're just in the initial planning stages of that right now with the staff, so taking these ideas back, I think it's a very good thing for us to do on the path forward.

MEMBER STETKAR: In terms of planning, I mean honestly, depending on the time scales you look at for the new designs coming in, there may be timing issues and reorganization of priorities as far as your activities that could be affected by that type of consideration.

DR. XING: Talking about time lines, another implementation other than computerized procedure, we have NRR user need to ask us to locate how the failure of automation in general would impact operator's performance. That is an on-going effort.

MEMBER BROWN: I got the impression, based on your example when you said the computerized procedures hadn't taken into account other than the gross failure of the screen went dark and you have to go to paper, I presume that's what you do, the effect of individual say center drift or whatever, is there a plant parameter data input into these computers to automatically select what procedure somebody will go to as opposed to the operator taking data and selecting the procedure?

DR. O'HARA: As guidance. Operator is always in control. The triggering conditions for the procedures in some systems, the triggering conditions alert the operator to the need for a particular procedure.

MEMBER BLEY: We've seen some of that. We can talk about that later.

MEMBER BROWN: I just wanted to make sure I understood.

DR. O'HARA: You visited one of the designs that does that.

MEMBER BROWN: And I understand that.

CHAIRMAN ABDEL-KHALIK: We have a third presentation, I believe.

DR. XING: Okay, so you know our name and the number. Any time if you are interested in a particular failure or you have heard of an interesting failure, let us know.

(Laughter.)

Thank you.

MR. PETERS: So next will be Dr. John O'Hara.

DR. O'HARA: I'm going to be presenting the next presentation. Let me apologize ahead of time. This is very late on the agenda. I think Dennis will vouch for me for that. So if this presentation is a little rough around the edges, it was developed yesterday.

(Laughter.)

We didn't have a lot of time for wordsmithing.

MR. PETERS: This is based on a request Tuesday.

DR. O'HARA: But basically we have some on-going work looking at trying to get a heads up on some of the issues that might be arising for the licensing reviews of the small modular reactors and so we're going to give you a briefing of that project. It's not over. So it's on-going and I'll try to point out what parts of it are done and what parts are still ongoing.

Next slide.

The team for this project is at the NRC side Amy who is sitting right over there. She promised to answer all the difficult questions. And DaBin who is sitting back there. And Jing was our project manager originally and she's graduated, moved on to other projects.

The BNL team is shown as well.

Next slide.

We're going to organize this around the topics you see here, basically to give you a picture of the background, what we were trying to -- what our objectives were, what approaches we're taking and then some of the preliminary results as they're coming out. And then what we're doing to move forward.

Okay, as you all know very well, the world and the United States is working on developing new and advanced reactor concepts. One concept is the small modular reactor. They're somewhat different than the traditional plants we're used to in the sense that they're very small, typically. We use the -- IAEA uses 350 megawatts electric. We expanded that a little bit to include some other designs. They're all under 400 megawatts.

The idea is they're scalable. You can add modules at a later date. You can buy as many modules as you want to suit your needs. If your needs change, you get additional modules. It's not that easy, but okay.

(Laughter.)

That's the marketing strategy. And these reactors are based on a diversity of technologies, light waters, heavy metals, liquid metals, and high temperature gas cooled reactors.

So what we're really setting out to do is to begin to look at this to see whether anything about this, any aspects to the design and operation of these plants that we ought to start sort of thinking about from the human factors perspective and research and initiate a project to do that.

Next slide, please.

As I said, we try and identify what the human factors aspects of these new kinds of reactors are and we also wanted to, based on what we're learning about those reactors, assess the current NRC regulations and guidance and see do any of those have to change or be modified in any way or improved in order to set the stage for the licensing reviews of those plants.

So the methodology was broken down to a

number of different areas. Our first was to figure out what questions we should be asking. As you know, most of these designs, they're in preliminary stages of design. They're not fully developed. A lot of the vendors don't have a really concrete idea or fully developed idea as to how they'll be operated. So we wanted to come up with a way of asking the right questions.

So we developed a module of a Concept of Operations and that was developed to help guide us to ask basically to ask the kinds of questions we think we need to ask to understand the human role in these systems. And I'll define that development in a few minutes.

We use that model to develop essentially a list of questions for each of the aspects of Concept of Operations and we use that throughout the project to look at the various designs and to do some other things that I'll describe.

Next we took that model in hand and we went and sought to find out what these issues might be. Issues here, we're talking about things that might be novel about these designs that we just don't really have enough information about now or things that might be part of the designs that might give us some cause of concern now based on information that we have.

To do that, we went to two principal sources of information. One is design information about small modular reactors, that is, whatever we could get about NuScale, mPower, a variety of these designs, we got that information and analyzed it. We also looked at a lot of the general literature that's coming out now. As you all well know, the Commission has had briefings with industry and there's been working groups at DOE. So we tried to get information from those sources because they've also been identifying things like technical issues. So we got that information, too.

Second source of information we went to given that we knew going into this that we weren't going to have a tremendous amount of information about the human factors aspect, the SMRs designs at this stage of the game because of the state of their design development. So we went to what we call surrogate systems. These were other industrial domains where some of the human performance challenges might be similar, that is, where operators, for instance, manage or control multiple units of something. We thought by looking at those kinds of systems we might learn something about the operation of these multiple SMR units in the nuclear industry.

Next slide.

As I mentioned before, we looked at the existing guidance and did an evaluation, based on some of the results we were getting to identify areas that might need improvements. And we have a task, this one I'll say up front, we're just starting now, but to look at the issues that we identify how might they be addressed in HRA or PRA. Are there any implications for doing risk analyses for these plants that come out of some of the issues we identified.

And then lastly, to develop insights about how to proceed with this information both in terms of future research as well as regulatory activity.

Next slide.

So the first step was to try to figure out what questions we should be asking. As many of you probably know, particularly those of you that are designers, it's become somewhat fashionable these days to talk about concepts of operations. Most large procurements by the government these days for systems through DoD, DOT, DHS, all these require a Concept of Operations document for new systems. And in addition to that, a lot of the industry standards have sort of hooked up on this and said you know, in the early stages of a systems development, you should come up with a concept of operations that helps lay out all your assumptions, everything you expect this new system to be and then the engineering flows from that.

I just grabbed one of many systems engineering V diagrams. This is one from a DOT document and it shows Concept of Operations sort of being the very initial step. So we thought that was probably a good idea. I mean a lot of that SMR designs, although some of the Legacy designs have been around for a while, the development of these into module or commercial reactors that will be scalable is in the relatively early stages of development.

So we thought a Concept of Operations approach might be a good place to start.

Next slide.

So we went to the literature. We looked at the standards that are out there now and again, DoD has them. There are a number of them out there. We started to look at those standards to see what kinds of information they're pointing to that would be reflected in these documents.

Generally speaking, most of the ConOps

look at the ConOps being sort of almost a top-down process, a document that will be continued to be developed over the course of the project's life span. And it starts at the very top with what are the goals of this system, maybe even before anything is designed yet, what are its goals, what are its missions, what do we expect it to do, right down to the detailed design of the control rooms and the procedures and things like that.

Next slide.

Now ConOps is not new to our review process. In NUREG-0711, we do look at ConOps. But we don't look at it in this sort of broad, comprehensive way. If you look at ConOps right now, you'll see ConOps is in the human system interface design area where we're talking about the sort of Concept of Operations for putting a crew in a control room and staffing responsibilities and things like that. So we thought for this work we wanted to expand that to better reflect some of the more current concepts of -- Concept of Operations. And we developed basically a six-dimensional model. That is, we broke the Concept of Operations down into six topical areas that are shown in this graphic right here. The plant missions being sort of at the center of everything and then looking at all the various aspects of the design.

So let me just quickly step through these different dimensions. Okay, plant missions. Now this may seem to be something that you would think geez, don't we know what the plant missions are? It produces electricity. Well, for the small modular reactors, as a for instance, a lot of them have identified secondary missions, so like hydrogen production or use of industrial steam. So we wanted to identify all of the sort of going in missions that these designs are attempting to achieve.

Now at that high level you also look at goals and objectives of the design, what some of the high-level functions are that are going to be needed to accomplish those goals. Constraints are very important. Designers enter a project with certain sort of constraints like we might say -- this is a big one in DoD. We want to reduce the staffing. We want fewer people on the new destroyer. We want to operate with a lean crew and so how do we achieve that? And the SMR designers have similar goals in mind. Not all of them, but many of them, to look at staffing profiles, for instance, that are lower than what would take to operate current plans. So that's the plant mission.

Next, please.

Next, roles and responsibilities of all agents. To accomplish the goals, we've got high-level functions that need to be accomplished, well, who is going to do them or what's the breakdown going to be between automation and the crews?

MEMBER BLEY: So agents are both people and equipment?

DR. O'HARA: Yes, yes. In highly automated systems, people tend to talk about their agent base. Things can be done by agents or entities that do things. It can be automation. It can be the people. More often than not, these days, it's a combination of the automation and the people since most industries have recognized extremely high automation can cause lots of problems for operators. So a lot of work in automation now is how do we better work in people with the automations so that they can perform their role better.

So looking at the relative relationship between people and automation is the roles and responsibilities. And oftentimes, as I said, this is a design goal somewhat heading in. We want to have more automation or it might be the result of another assumption you make, want fewer people. Now fewer people, I need more automation.

Staffing qualifications and training, describing the approach towards staffing the plant, the positions, allocation of responsibilities, what kinds of qualifications are needed, training needed to support those positions.

Next, a management of normal operations. This was the day to day, everyday thing. How will a plant be managed by its agents, humans and automation to go through its normal operations. And how will plant personnel interact with plant systems and functions to accomplish those things. Once I know that, how do I design the support systems for the crews in terms of control rooms and procedures and things for them to perform their roles to meet the functions.

Next slide.

Management of off-normal conditions is essentially the same considerations, but now we're dealing with the not normal events, but things that come up that have to be addressed including, based on our last project, things like the graded conditions all the way through equipment failures, loss of systems, all the way to emergencies. What's the concept of dealing with these things is what we're asking early on and as the design proceeds, we look at the details.

Management of maintenance and modifications. What's the notion of how this plant will be upgraded? How will it be maintained? What the approach is.

MEMBER STETKAR: John, let me sneak in a quick question. In the automotive business, I've run into some people worrying that as automation tends to come in there, the concept of shared control, between the driver and the car is a dangerous one. On the other hand, I don't see there's an option and I would -- I'm just hypothesizing, but I think the key is that you have to train the people to understand how to interact with a shared mode with the control systems.

Can you say anything about that? Any of you?

DR. O'HARA: I mean I think the implementation of automation now is reflecting some of these concerns. So if you look at just to use your vehicle analogy, there's a lot of shared control that currently goes on in a vehicle. If you have anti-lock brakes or power-assisted brakes, you give the command to brake and then there's a lot of low-level automation that handles the keeping the wheels in position and things like that. Automatic transitions are an example of shared automation. You decide how fast you want to go, the automatic transmission decides what gears should be used and manages to transition between those gears. And that thinking is creeping into the process control industry.

And I want to talk a little bit about our very interesting experiences with aerial vehicles and the use of automation of aerial vehicles where they're being driven towards more interactive automation because if they don't, operators lose complete sense of what the individual vehicles are doing.

MEMBER BLEY: And that's coming up.

DR. O'HARA: And that trend away from just -- automate everything you can possibly automate to what parts of this should I automate and what roles should I allow or allocate to the humans so that together they operate in the most effective way and can manage degradations which are, of course, very serious in highly automated systems.

MEMBER BLEY: Have you also talked to the commercial airlines because it is a big issue with pilots and commercial airlines.

DR. O'HARA: We actually did --

MEMBER BLEY: Fly by wire stuff.

DR. O'HARA: Absolutely, and we actually did that in not this project because we already had a project prior to this one on automation.

MEMBER BLEY: Okay.

DR. O'HARA: We had a lot of information that went into this one and a lot of our information came from aviation industry.

MEMBER BLEY: Because they've struggled with that for a decade.

DR. O'HARA: That industry is actually the industry that initiated this whole notion of levels of automation because they recognize you just can't fully automate everything, so they looked at various levels and we actually adopted for the nuclear industry a model that originally was based on the aviation -- but that's not another project.

DR. D'AGOSTINO: I'm just going to supplement answers. Dr. Amy D'Agostino. I just wanted to say that Sean presented in the very beginning, so I'm the technical monitor on this project and Sean presented in the beginning that we also have other concurrent automation projects going on that are actually addressing those specific issues where we're looking at functional allocation and when the tasks are allocated in different ways to different agents, what we're seeing as far as the human performance effects. So there are some other projects going on that's addressing that and we're trying to tie that work together.

MEMBER STETKAR: Good.

DR. O'HARA: So we developed this model. We then use it to develop a set of questions that then we could take with us and ask of the literature and ask of the designers -- ask some of our designers, we had an opportunity to interact with and to ask of the surrogate systems and that gave us sort of a common framework of information.

Next slide.

Okay, in terms of SMRs, the information sources we used were general publications out there, relative to the SMRs. But really we had three key reports that were very detailed, assembled, who NROs work with the laboratory consortium that you're probably familiar with. And NRO tasked the laboratory consortium to come up with very detailed descriptions of the various SMR designs and we utilized that as input to our project because it was very detailed information and it assembled, it sort of does a lot of legwork of trying to go out and assess that information.

We also had site visits with one of the vendors and discussions with a couple of others regarding these ConOps dimensions. And we took advantage of the industry meetings that have been going on, the Commission being the focal points of those meetings and DOE being another one. And we essentially looked at a sampling of the reactors in various classes and if you're wondering why we picked those, some of them probably would be obvious, but when we started out this project, these were the designs the NRC was most interested in. So we selected them.

As you know, they were probably over 50 SMR designs, if you look world wide. And so we focused on those of most interest to the NRC.

Next slide.

In terms of surrogate systems, we looked at a few and we basically got our information about them from general publications, site visits. We had an opportunity to visit some of these sites and interviews with people working on these systems. So it's a broad array of information. And again, we used our ConOps set of questions as our information gathering tool.

So the systems we looked at, two of them here and two of them are on the next slide, but we met with the Nuclear Navy people in terms of the operation of reactors aboard naval vessels.

MEMBER BLEY: And they were sharing information?

DR. O'HARA: Can't talk about it, because it's classified.

(Laughter.)

We got some information. We're trying to figure out how we can use it. And also about future developments of Navy vessels.

Refineries, as many of you probably well know, many refineries operate as multiple units. So we went to one where basically four units of a refinery operated from the single control room by the same crew.

Next slide.

Okay, another was remote or tele-intensive care units. And before you get upset, and think what the heck were you going to a place like that for, that was a target of opportunity we had. It didn't cost the NRC a penny. We had an opportunity to visit one of these centers because some informal discussions with a physician who worked at one of these systems led to him saying you know, we do the same thing. We monitor patients at multiple locations. We have to deal with the differences between those locations. We have central control room where we do this. And so we said hey, we'll take a night, go to one of these things in the wee hours and see what they do and talk to their staff with our ConOps questionnaire in hand. And it was very interesting.

And the guy that designed the tele-intensive care unit we went to went on to tell us how to design control rooms for nuclear plants, too.

(Laughter.)

So we got some added benefit from that visit. It actually was fascinating and it did hold some lessons learned for us and they're in the report. But my favorite, my very personal favorite is the unmanned vehicles. Now the reason it's my favorite is because in 2005, DoD published a road map for the future of unmanned aerial systems. They've been pretty successful, as you know, as used in the Persian Gulf and in the Middle East. They've been used for Katrina and an aerial vehicle has been used now at Fukushima to get into -- go to places where you don't want the human crews to be sitting.

Anyway, in 2005, they developed a road map. The vehicle you see here, the Predator, is actually operated by two guys. One handles the flight controls and navigation. The other guys handles the payload and mission aspects. DoD decided they don't want that. It's too manpower intensive. They want one guy to be able to control multiple vehicles. Not only that, they want to be able to control heterogeneous vehicles, vehicles of different types. So that's a goal. It's a long-range road map.

In 2009, DoD published another plan to extend that to all unmanned vehicles, not just aerial vehicles because there's ground resources, marine resources, and air resources. And we thought it was especially interesting because they're in a sense setting out to do -- to some degree what a small modular reactor, some of them are intending to do and also they're in the development phase, just like we are, in a sense. They're in the stage where they're saying okay, what technology do we need to make this happen? What do we need to do?

MEMBER BLEY: And right now, they're flying these things as they would if they were manned aircraft, same crewing arrangement?

DR. O'HARA: Yes, they are. And I should --

MEMBER BROWN: Now all of the fighters are two-man. The F18s are two. This replicates that approach. The F16s and F15s, I don't think are two people.

DR. O'HARA: I should probably also add, not all the unmanned vehicles or two people, the Predator is. And there are different staffing arrangements, but it's not many vehicles to one operator. And that's what they want to get to. So I think it's really interesting because they're along a development path not unlike what the SMR vendors want to do and therefore, there's lessons to be learned from them.

MEMBER BLEY: Are they further along?

DR. O'HARA: Actually, they've encountered a lot of difficulties which provide lessons learned as well.

DR. XING: Actually, I can -- just to brief -- the latest news I learned from Air Force on this, the original agenda set up over ten years ago as John said, one operator operating multiple vehicles. The current status as they end up is the three or four operators operating one vehicle because with the fact that you lose all your sensation, your 3D vision, all those -- you need three or four people behind this single person to provide all those different missions here. I think that's a very good lesson learned to think about small modular reactor operations.

DR. O'HARA: This is really interesting and what's nice about the DoD work they funded a lot of studies so they produced a real literature database. Of course, it's not a nuclear plant. It's a moving vehicle. So it's not exactly the same, but a lot of the human challenges are similar.

Next slide.

Okay, results. Results, we're kind of assembling the results now. What we are currently doing as we speak, if I was not sitting here, I'd be back in my office working on the issues and getting them all together.

But just to give you a snapshot of sort of what we're seeing here. In terms of plant missions, there's new goals and new things that designers want to do with these plants beyond what our current fleet of nuclear plants do. This is the NGNP vision of the -- NGNP feeding lots of industrial applications and maybe even being a big piece of the hydrogen economy eventually. But that's a NGNP figure that's on that slide.

Another thing that's somewhat different in terms of just looking based at how we classified information in terms of plant mission, but unlike even the new reactors now, they're based on much less, not that there's none, but much less predecessor plant experience and operating experience. They're not in that like very slow, evolving pathway that like the AP1000 and the ABWR are. They're making a little bit of a bigger jump. And so that's something that we have to treat, look at in the future.

Roles and responsibilities. Very high degree of automation. The concept is you automate everything. In other words, all -- not just safety systems, but all the normal ops, operations would be automated. So we do recognize through past research, high automation, other industries, that there are definitely tradeoffs with high automation. You need the high automation if you're going to ask one guy to let's say monitor four plants, but by providing that high degree of automation, you make it a bit more difficult for him to stay integrated with everything.

Function allocation and processes. Jing mentioned the NRC's current look at this, but automation is getting implemented in a lot more complex ways. It's not you just automate or you do it manually. Dennis, you mentioned shared automation. But shared automation is one step along this pathway.

There's automation by consent. Automation by exception. There's a number of different ways automation is implemented, but the reality is we don't really have a good basis to decide which of these levels should we pick for a particular function. So that's very important work.

Staffing and qualifications, you're all well aware of the staffing exemptions that most of these folks require. Again, reason being that there's way fewer staff than there will be reactors. There will be new positions, positions that are somewhat new to us in the control room to handle secondary functions and novel operations like moving a module from one place in the pool to another. The NuScale concept of refueling and maintenance is you unplug the module from where it operates normally and you move it through the bay that they all sit in to a special zone where you do the maintenance activity and they'll sell the utilities an extra module so while that one is being worked on, you move a fresh module in and you plug it in.

MEMBER BLEY: John, I hate to do this, but our time is evaporating and we have other things on the agenda, so if you can push through real quickly to a conclusion.

DR. O'HARA: These slides, what you'll see is just some of the high points of where -- within our framework of ConOps, I'm not going to go over them, they're just things that come up that are different with these designs than some of the others.

MEMBER CORRADINI: Can I ask one question now that you're finished, which is who from the utilities have you involved from the get-go so you get reality into module units? Are you using anybody from essentially combined cycle natural gas plants which have multi-modules or somebody from fossil units or somebody who's planning to do a module reactor?

DR. O'HARA: Yes, no, yes, yes.

(Laughter.)

As I said, we went to a refinery. We went to -- because we interacted with an engineering consulting company that's been involved in a lot of not just refineries, but other process control units to integrate disparate control rooms into central control rooms leading to these multi-unit operations, that was bevel engineering.

MEMBER CORRADINI: A CCGT will have two, three or four on a site with a common control room, so that's one that would pop up as a power plant.

DR. O'HARA: We did go to -- again, we

discussed it with the folks for the refineries and went to one, saw their operations, interviewed the crew, etcetera. That's all we did in that area. With the vendors, we have had interactions with three of the SMR vendors and one of them we actually visited and sat down and went through all of our -- we're trying to get -- we didn't go to all of them, but we went to -- we had interactions with three of them.

MEMBER BLEY: And when you did they have operators on their staff working with their designs or not?

DR. O'HARA: No.

MEMBER BLEY: That's too bad.

DR. O'HARA: We won't go there this moment.

MEMBER BLEY: Okay.

DR. O'HARA: Basically, this is where we are now. We've compiled these issues. We're looking at them, massaging them. Some of them come from the surrogate system, so we're trying to better understand what they mean, SMRs. And that's the sort of snapshot of where we are now.

Go to the next slide. The last one.

Here's what we still have to do, compile sort of this integrated final list of issues from all the different SMR designs and the sources of information. We're working now and asking questions, what does all this mean for HRA?

And finally, our last task was to look at our results and look at how it impacts future research and guidance. That's it.

MEMBER BLEY: Thank you. We were pleased to hear earlier this week from some of the SMR folks that they're actually looking to this work, to help them forward. John, Jing, and Sean, thank you very much. We appreciate your presentation.

Mr. Chairman, back to you. Given our late start, almost on time.

CHAIRMAN ABDEL-KHALIK: Perfect. We are off the record.

(Whereupon, the above-entitled matter went off the record at 11:48 a.m.)

Advanced Control Room Human Factors Research

Sean E. Peters, Chief
Human Factors & Reliability Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research
April 8, 2011

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Overview

- Background – Sean Peters
- Effects of Degraded I&C on HSIs and HP– Jing Xing
- HF Aspects of CONOPs of SMRs – John O’Hara (BNL)

Background

- HP research issues associated with emerging technologies
  - 2003 - OECD/NEA Workshop
  - 2006 - CSNI/SEGHOF/HRP Workshop – Future control station designs and human performance issues in NPPs
  - 2008 - BNL Tech Report No. 79947-2008 - HF considerations with respect to emerging technology in nuclear power plants: Detailed analysis
  - 2008 - NUREG/CR-6947 – HF considerations with respect to emerging technology in nuclear power plants: Summary
  - 2009 - CSNI/WGHOF Technical Opinion Paper – Research program topics on HP in new nuclear plant technology
  - 2010 - CSNI/WGHOF/NRC Workshop - Research on HF for the design and operation of new nuclear plant technology
  - 2010 – User Need – NRO-2010-005

Current Projects

•Update NUREG-0711 (2011)
• NUREG-0700
• Update NUREG-0800
• Develop NUREG-0711 Companion Document
• Impact of Automation on CR Design
• Methods for Measuring Workload, SA and Teamwork
• Computerized Procedures
• Integrated Systems Validation
• Staffing Verification & Evaluation for Advanced CR Designs
• HF Aspects in CONOPS of Modular Design
• HFE Methods and Tools
•Update NUREG-0711 (2013)

Human Factors Aspects of Operating Small Modular Reactors

NRC RES Project JCN N-6862

ACRS Meeting
April 8, 2011

BROOKHAVEN NATIONAL LABORATORY
a passion for discovery

Office of Science
U.S. DEPARTMENT OF ENERGY

The Team

- U.S. Nuclear Regulatory Commission

  Amy D'Agostino and DaBin Ki

  Jing Xing, Team member Emeritus

- Brookhaven National Laboratory

  John O’Hara , Jim Higgins, and Richard Deem

Topics

- Background
- Objectives
- Methodology
- Concept of Operations Model
- Preliminary SMR Issues
- Summary of Current Status
- Path Forward

Background

- Advanced reactors and advanced reactor technology are being developed and implemented
- Small modular reactors (SMRs) are one of the options
  - 400 megawatts electric (MWe) or less (our definition)
  - scalable, may be operated in groups to obtained desired output
  - diversity of reactor technologies (LWRs, LMRs, HTGRs)
- Research is needed to provide a better understanding of the human performance implications of SMRs
- The U.S. Nuclear Regulatory Commission (NRC) initiated work to examine the human factors engineering (HFE) and ConOps aspects of SMRs

Objective

- To identify the human factors aspects associated with the monitoring and control of multi-unit SMRs
- Assess where NRC guidance documents need to be enhanced for review of modular design

Methodology

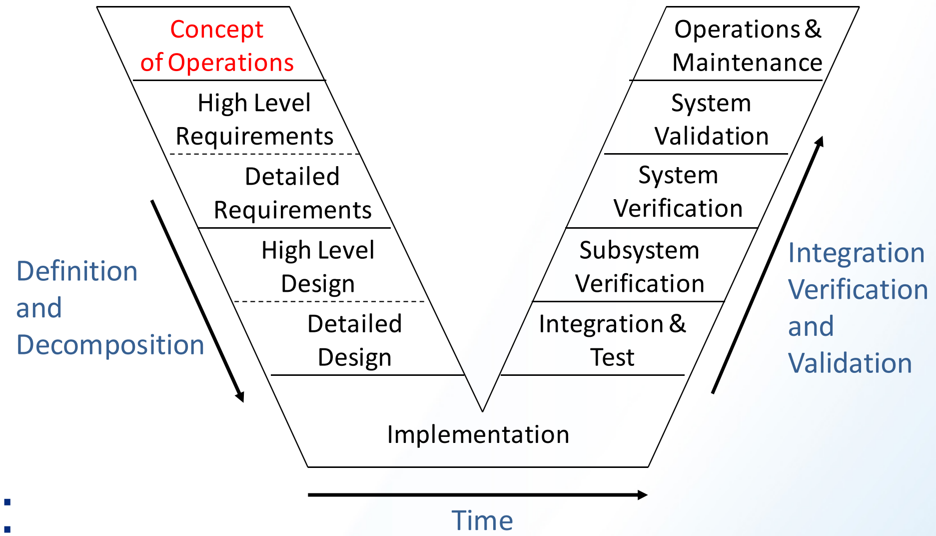
- Develop a Concept of Operations (ConOps) model addressing the HFE aspects of a design
  - to identify the needed information and structure its organization
  - to develop a ConOps questionnaire to guide subsequent tasks
- Identify issues related to SMR operations
  - an issue is defined as an aspect of SMR design or operations that are novel and may indicate a need for enhanced review guidance to better support SMR HFE Reviews
  - staff review of information about SMR design and operations from documentation and site visits to identify the human-performance issues
  - obtained information about the operations of "surrogate systems," i.e., systems whose operations pose similar human performance demands related to multi-module operations

Methodology

- Evaluate current NRC regulations and review guidance
  - is the guidance suitable to address issues of human performance in SMRs
  - what aspects of the regulations and guidance may need to be enhanced for review of modular design
- Identify the implications of SMR human performance issues for human reliability analysis
- Develop insights for the use of the research results for future research and review activities

ConOps Model Development

- Vision of what plant operation should be like
- Integral to the systems engineering process
- IEEE Standard 1362 (IEEE, 2007) states that a ConOps:



(adapted from DOT, 2009)

… describes system characteristics of the to-be-delivered system from the user's viewpoint. The ConOps document is used to communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements (e.g., training, facilities, staffing, and maintenance). It describes the user organization(s), mission(s), and organizational objectives from an integrated systems point of view. (p. 1)

ConOps Model Development

- A ConOps reflects top-down and bottom up considerations
  - from the top, the concept reflects the high-level goals for system operations
  - from the bottom, the technological infrastructure needed to support the ConOps

High-level mission and goals

Define functions necessary to achieve the goals

Allocate functions to human and system resources

Decompose functions into tasks

Analyze tasks to define performance requirements

Design detailed HSI, procedures, and training

ConOps Model Development

- ConOps is considered in the NRC HFE review process, per NUREG-0711
- A more detailed model of ConOps to support information collection and organization for SMRs was developed
- Six ConOps dimensions were defined

CONOPS Dimensions

- Plant's Missions
  - the high-level goals the plant expectedly will achieve
  - can be described in terms of
    - goals and objectives, e.g., electrical generation, other production goals, and safe performance
    - high-level functions – the functions that must be undertaken (regardless of the performing agent) to achieve the plant's goals
    - boundary conditions – the operating envelope of the design
    - constraints – an aspect of the design, such as a specific staffing plan or the use of specific technology, that are design drivers

CONOPS Dimensions

- Roles and Responsibilities of All Agents
  - addresses the relative roles and responsibilities of personnel and plant automation and their relationship
  - definition of human roles and responsibilities in a system is the first step toward human-system integration
  - usually specified to some level before design work begins and is refined using a variety of evaluation techniques, such as operating experience review, function and task analysis, and testing

- Staffing, Qualifications, and Training
  - addresses approaches to staffing the plant, including staffing levels and personnel qualifications, and training
  - the ways in which shift teams will be structured and the types of interactions between team members and other people

CONOPS Dimensions

- Management of Normal Operations
  - addresses concepts for how the plant will be operated by personnel to manage its normal evolutions, such as start-up, low power, full power, and shutdown
  - how personnel will interact with plant functions, systems, and components to accomplish their main tasks of monitoring and controlling the plant through these normal evolutions
  - how control room (and other) resources are designed to support their activities, e.g., the HSIs, procedures, and supporting infrastructure

CONOPS Dimensions

- Management of Off-Normal Conditions and Emergencies
  - addresses concepts for how degraded conditions, disturbances and emergencies will be handled, and how responses to such situations will be determined
  - considerations include
    - degraded I&C and HSI conditions (such as a faulty sensor, loss of an aspect of automation, or of electronic communication, or a workstation)
    - failed equipment, such as pumps and valves
    - loss of plant systems that must be compensated for, such as the failure of cooling water
    - emergencies that may impact safety, such as a loss of coolant accident (LOCA)
- Management of Maintenance and Modifications
  - addresses concepts for system maintenance, installing upgrades, and configuration management

Identify SMR Issues

- SMR Information sources
  - general publications addressing the operational and HFE aspects of SMR designs (including key NRO reports)
  - industry SMR meetings by DOE, NRC, and vendors
  - site visits and interviews
- Data collections structured by ConOps questionnaire
- Three classes of SMRs were examined

Reactor	MWe	Vendor
Integral PWRs (iPWRs)		
International Reactor Innovative and Secure (IRIS)	335	Westinghouse Electric Corp
NuScale	45	NuScale Power, Inc.
mPower	125	Babcock & Wilcox
Gas-cooled Reactors		
Gas Turbine-Modular Helium Reactor (GT-MHR)*	285	General Atomics
Pebble Bed Modular Reactor (PBMR)*	175	Westinghouse Electric Corp.
Liquid-metal Reactors (LMRs)		
Super-Safe, Small and Simple (4S)	10	Toshiba Corp.
Hyperion Power Module (HPM)	25	Hyperion Power Generation, Inc.
Power Reactor Innovative Small Module (PRISM)	311	GE Hitachi Nuclear Energy

Identify SMR Issues

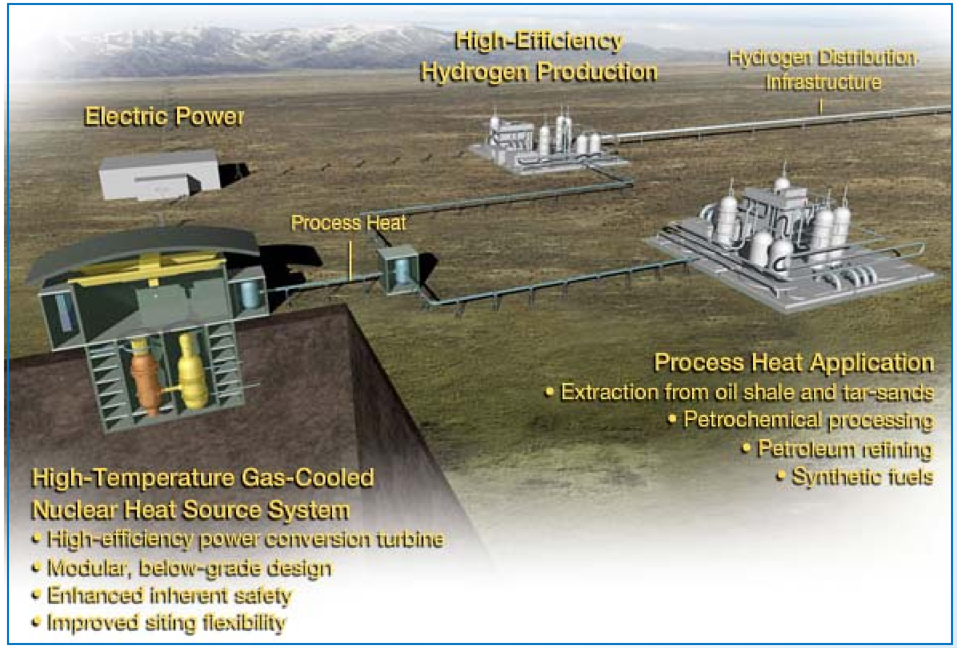
- Surrogate system information sources
  - general publications
  - site visits and interviews
- Data collections structured by ConOps questionnaire
- Surrogate systems
  - nuclear naval vessels
  - refineries
  - continued on next slide

Identify SMR Issues

- Surrogate systems (continued)
  - tele-intensive care units
  - unmanned vehicles

Results: Preliminary SMR Issues

- Plant's missions
  - New Goals, Objectives, and Functions
  - Limited Predecessor Plants and Operating Experience
- Roles and responsibilities of all agents
  - High Degree of Automation for All Operations
  - Function Allocation to Support Automation Decisions

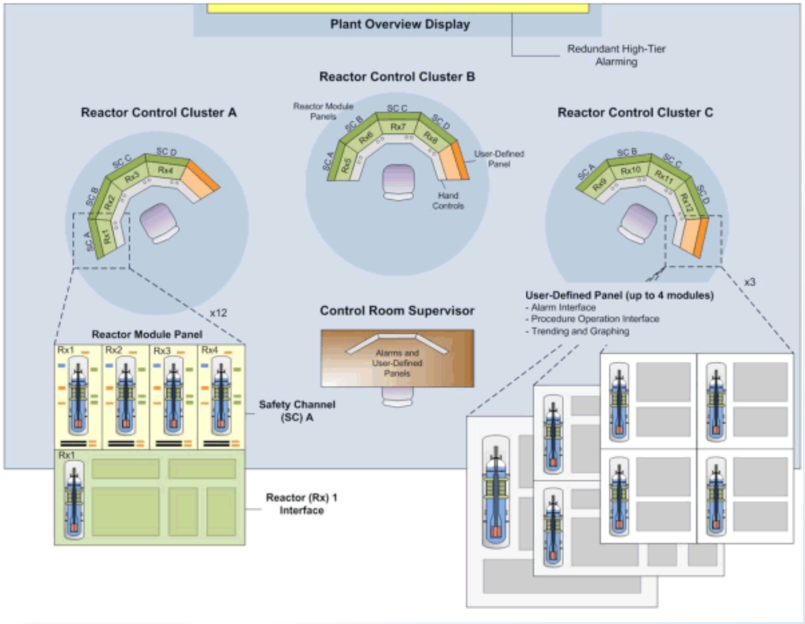


- Staffing, qualifications, and training
  - Staffing Levels (10 CFR 50.54m exemption)
  - New Positions (for secondary functions and other novel operations such as module transfer)

Results: Preliminary SMR Issues

- Management of Normal Operations
  - Non-LWR Processes
  - Impact of Adding Modules During the Operation of Other Modules
  - Refueling Strategies
  - Module/unit Differences in Surrogate Systems
  - Multi-unit Situation Awareness
  - Control Room Configuration and Workstation Design for Multi-Modular Teams
  - HSI Design for Multi-module Monitoring and Control
  - HSIs for Secondary Functions

Preliminary NuScale MCR Concept



Results: Preliminary SMR Issues

- Management of Off-Normal Conditions and Emergencies
  - Operational Team Organizational Transitions to Manage Off-Normal Units in Surrogate Systems
  - New Hazards associated with Non-LWR design (e.g., higher operating temperatures and sodium coolant)
  - Potential Impacts of Unplanned Shutdowns or Degraded Conditions of One Module on Other Modules
  - Identification of Risk-Important Human Actions (RIHAs) when One Operator/Crew is Managing Multiple SMRs

- Management of Maintenance and Modifications
  - Modular Construction
  - New Maintenance Practices

Summary of Current Status

- A ConOps model was developed and has provided a useful tool for obtaining information about SMRs and surrogate systems
- Information about the design and operations of SMRs has been obtained
  - ConOps of SMRs not fully developed at this point
- Information from surrogate systems has been obtained
- Preliminary issues were identified in each of the ConOps dimensions examined

Path Forward

- Finalize the list of issues identified from all information sources
- Determine HRA implications of SMR ConOps
- Develop insights for use of the results

Human Factors and Digital I&C Degradation

Brookhaven National Lab

Human Factors and Reliability Branch, DRA/RES/NRC

United States Nuclear Regulatory Commission
Protecting People and the Environment

Honk if you want to stop your VW Jetta

NEW YORK (CNNMoney) -- Volkswagen of America is recalling about 71,000 of the German automaker's new 2011 Jetta sedans for a wiring problem that could cause the car to turn off when the horn is used.

- “Power is ON” may be viewed as a pre-condition in the logic.
- Inadvertently, the implicit dependencies are not tracked (i.e., no deterministic procedure in place)
- Horn short circuit can disable “Converter Box.”
- Converter box” has to be enabled, functional, and turned ON to supply power (and enable) engine controller.
- “Engine controller” has to be operational for controlled motion of vehicle.
- If “Engine controller” is OFF and vehicle is in motion, “vehicle motion control” is in an unknown state (i.e., controllability cannot be assured).

Digital age in NPP

Control Room with Analog HSIs

Control Room with Computer-based HSIs

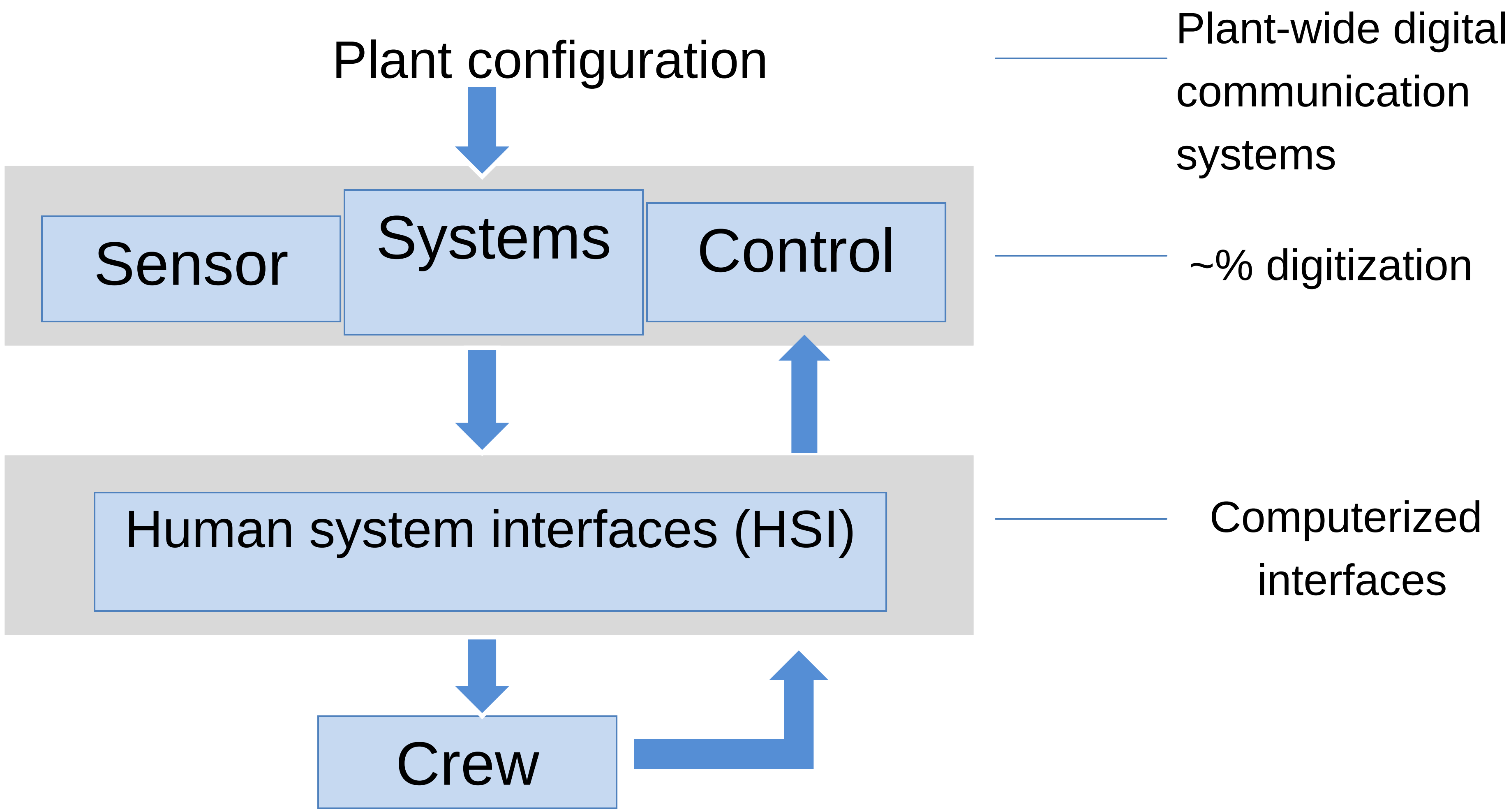
Outline

I. Digital I&C degradation/failures

II. Human factors (HF) research in digital I&C degradation

III. HF in the NRC's Digital I&C research

Digital I&C in NPP



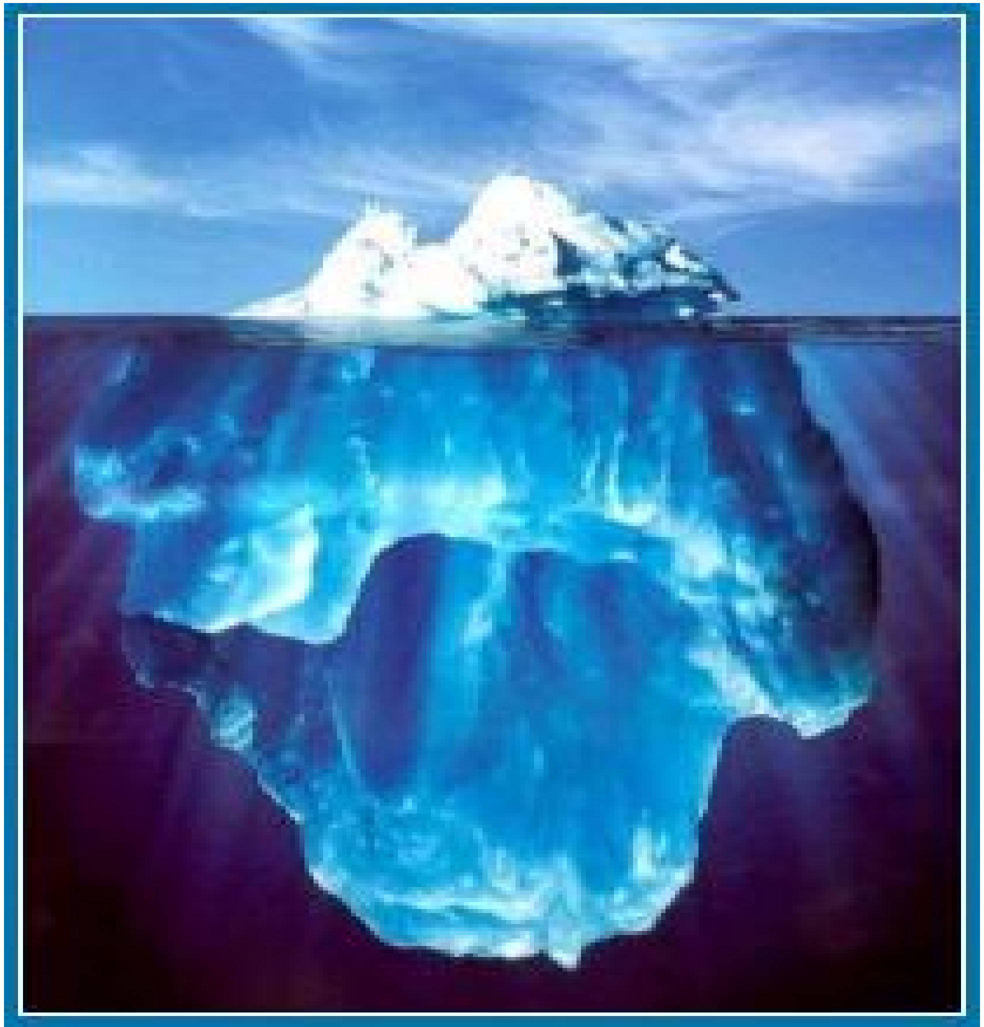
Differences in analog and digital I&C degradation

Analog - hardware degradation	Digital - programmable hardware and software faults
•Limited failure modes	•Unlimited failure modes
•Able to be pre-determined	•Not able to be pre-determined
•Traceable	•Often untraceable

Current efforts in identifying digital I&C failure modes

There are digital I&C failure databases such as COMPSIS.

The revealed failures are merely the tip of the iceberg.



Contributing factors to digital I&C failures

- Engineering errors due to increasing functionality
- Complexity in software and control logic
- Interdependency among systems
- Uncertainty in V&V process
- Faults resulting from maintenance, upgrades, and configuration changes

Outline

I. Digital I&C degradation/failures

II. Human factors (HF) research in digital I&C degradation

III. HF research in the NRC's Digital I&C research

N-6526: Human Factors Aspects of Operations Under Conditions of Degraded I&C

Performance period: 2007-2010

Deliverable: Technical Report BNL-91047-2010

The Effects of Degraded Digital Instrumentation and Control Systems on Human-system Interfaces and Operator Performance: HFE Review Guidance and Technical Basis

John O'Hara, Bill Gunther, and Gerardo Martinez-Guridi

Brookhaven National Laboratory

Degraded I&C and human performance

Plant personnel and the I&C system work together to:

- perceive basic parameters
- monitor the plant's processes, performance, and various barriers that prevent release of radioactive material
- adjust operations as needed
- respond to transients, accidents, and other failures

I&C degradation may significantly lower the operator's ability to monitor systems and take control actions

Project Objectives

1. Understand the impact of I&C degradations on human performance

2. Develop technical basis for including considerations of degraded I&C in the NRC’s human factors engineering (HFE) activities

3. Develop HFE review guidance on degraded digital I&C

What we know about digital I&C: Ideal vs. Reality

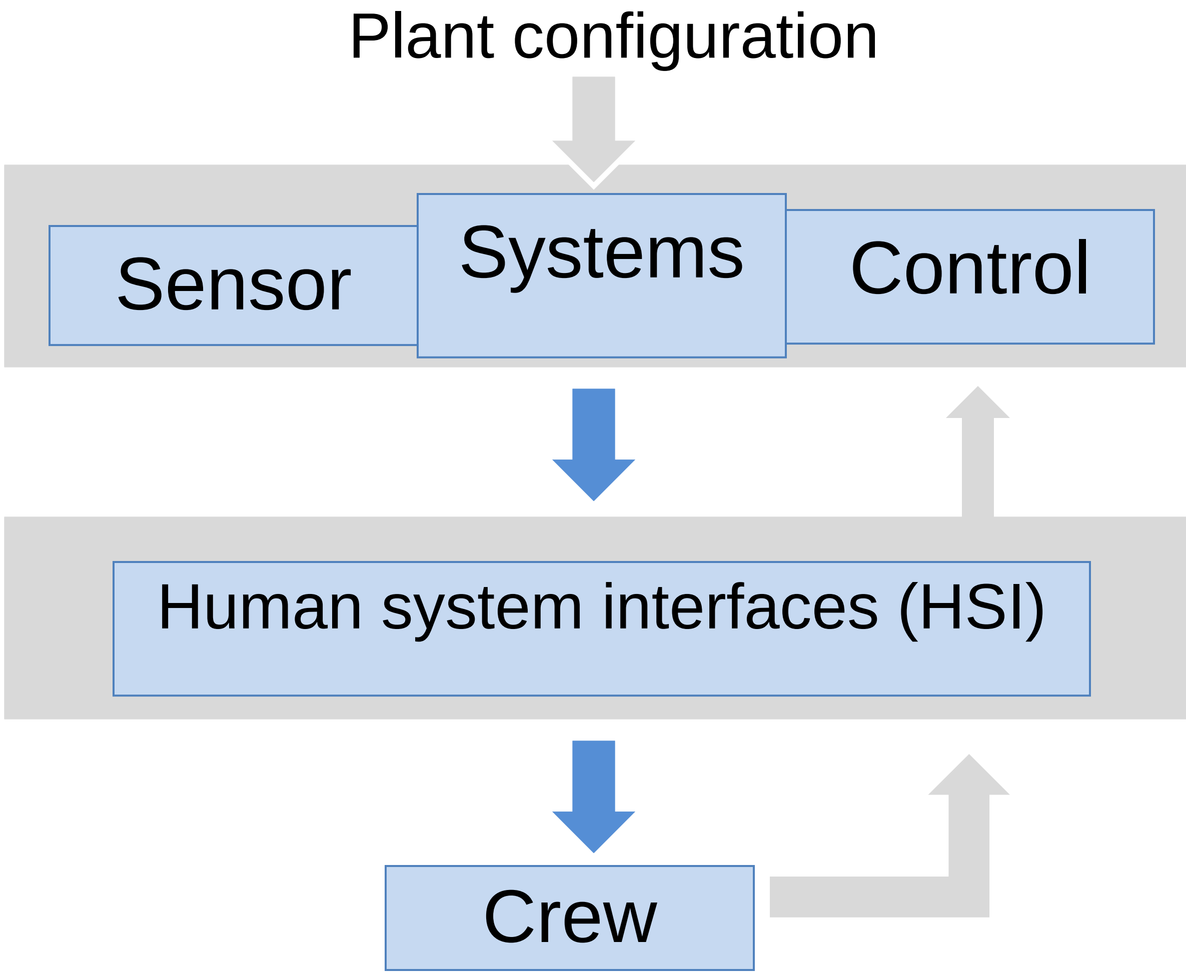
Ideal

- Digital I&C characterization of safety and non-safety systems
- Digital I&C failure data and failure modes
- Data about failures on operators, systems, and the plant safety

Reality

- No standard Digital I&C characterization
- Limited Digital I&C failure data and modes are being studied
- Few studies address the effects of failures on operators

Scope of the project



Technical Approach

1. Develop a generic framework integrating digital I&C system and human performance

2. Use the framework to evaluate available information to generalize the effects of degraded I&C on human performance

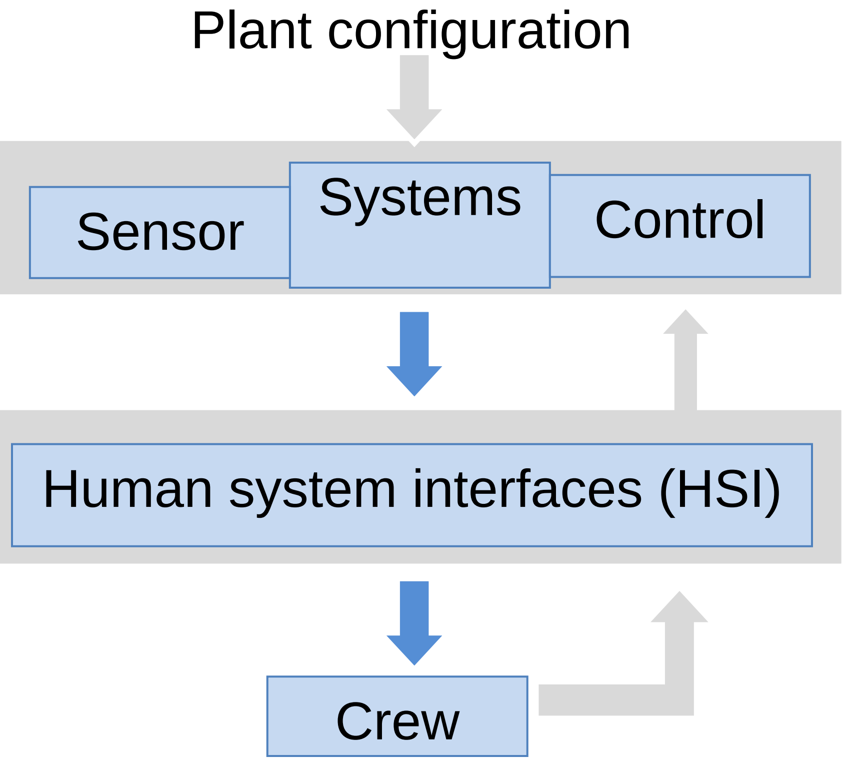
3. Develop HFE review guidance

Goal: Digital I&C – HSI - human performance framework

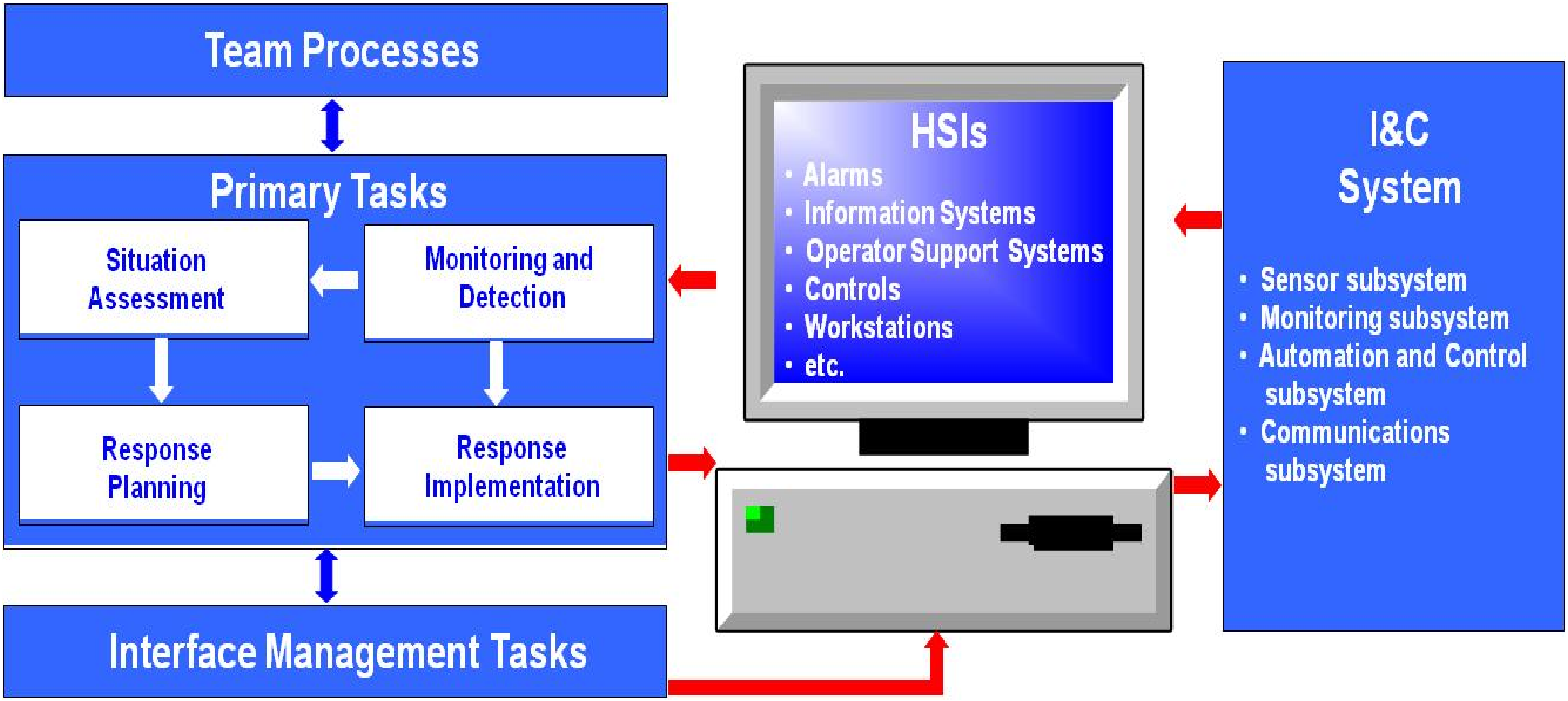
Available information about digital I&C failures are not associated with operator performance. So, we need a generic framework to consider I&C systems, HSI, and human performance as an entity.

Development of the framework:

- Identify design-independent functional elements within each level
- Links between the elements are design-specific.



Digital I&C - Human Performance Framework



Goal: Develop the technical basis for human performance effects under degraded I&C

Approach:

- Use the framework to analyze available information and generalize information about the impacts of degraded I&C on human performance
- Extract and identify HF issues
- Apply HF principles to address the issues -> review guidance

- Literature
- Operational experience
- Digital I&C failure database

IC subsystems

HSI systems

Human performance functions

HF issues

Analysis of Operating Experience Example

NRC IN 2009-03: Spurious Safety Injection with Failure to Reset

– Failed zener diode resulted in logic problems

Human Performance					
Monitoring & Detection	Situation Assessment	Response Planning	**Response Implementation**	Interface Mgt.	Team Processes

Human-System Interface Subsystem					
Alarms	Information System	COSSs	**Controls**	Communication Systems	Workstations

I&C Subsystems			
Sensor Subsystem	Monitoring Subsystem	Automation/Control Subsystems	**Communication Subsystem**

Human factors issues:

- Required several local manual actions to recover
- Operations and I&C personnel awareness limitations
- Procedural guidance less than adequate

Results of analysis

1. Established evidence that digital I&C degradation can affect all aspects of human performance.
   - Example-delayed or locked-up information impacts operators' situational assessment
   - A single failure can misguide operators' understanding of plant status.

2. Identified HF issues related to degraded I&C
   - Example-Personnel detection of digital system degradation
   - Transition to back-up systems (when and how)

Results:
Impacts of degraded I&C on human performance

- I&C degradations can impact the HSIs that operators use to monitor and control the plant and, therefore, operator performance

- A single failure can mislead operators about the plant's state
  - the problem is more complex when the control system uses different information than the operators; it may appear to be malfunctioning to operators in view of their information and understanding of the situation; operators may take inappropriate actions based on the erroneous information

- Important degradation of the digital system may not be alarmed nor communicated to operators in a timely way, potentially causing a delayed response

- Degraded conditions may not immediately affect the system's functionality and may not be communicated to the operators creating latent failures and, subsequently, more serious events, should there be additional failures or changes in conditions

Impacts of degraded sensor & monitoring subsystems

- Poor situation awareness associated with degradations of the sensor and monitoring subsystems

- Sensor degradations can make displays difficult to understand
  – graphical displays that integrate information appear more subject to the effects of sensor degradation than simpler displays

- Operators may have difficulty distinguishing between process and sensor failures

- Operators’ task performance worsens as the magnitude of sensor noise increases

Impacts of degraded automation and control subsystem

- Poor situation awareness and response planning associated with degradations of automatic systems
- Automation degradations are often difficult to detect
- When automation fails, operators may be challenged to assess the current status of the tasks that automation was performing and the systems it was controlling
- When automation fails teamwork is affected when operators have to manually perform automation’s tasks, thereby changing the roles and responsibilities of crew members
- Factors contributing to this difficulty include over reliance on automation and poor HSI design for monitoring automation

Impacts of degraded communication subsystem

- As time lags increase, the operator’s control performance decreases
- The operator’s closed-loop control (control based on feedback) becomes increasingly unstable
- Operators shift control strategies becoming increasingly open-loop (control based on prediction rather than feedback)

Goal: Develop the NRC's HF review guidance

10 CFR 50.34(f)(2)(iii):

Control room design [shall] reflect state-of-art human factors principles.

- NRC's Standard Review Plan (NUREG-0800, Ch.18) describes the staff's review activities to verify that accepted HF engineering principles are incorporated during an NPP design process.

- NRC's Human Factors Engineering Review Model (NUREG-0711) provides guidance for detailed review of design process.

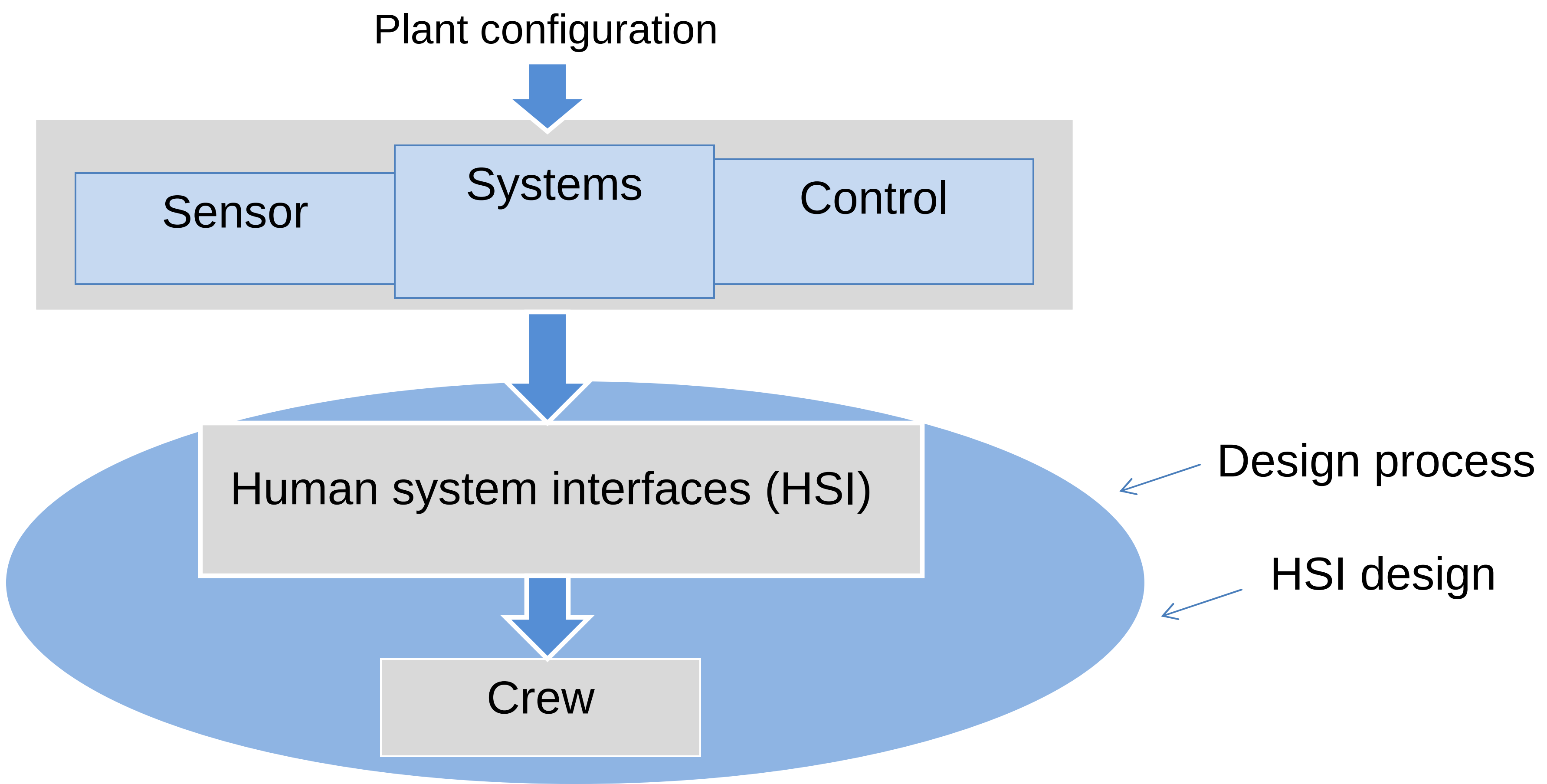
- Human-System-Interface (HSI) Design (NUREG-0700)

Digital I&C degradation guidance needs enhancement

HFE Review Guidance

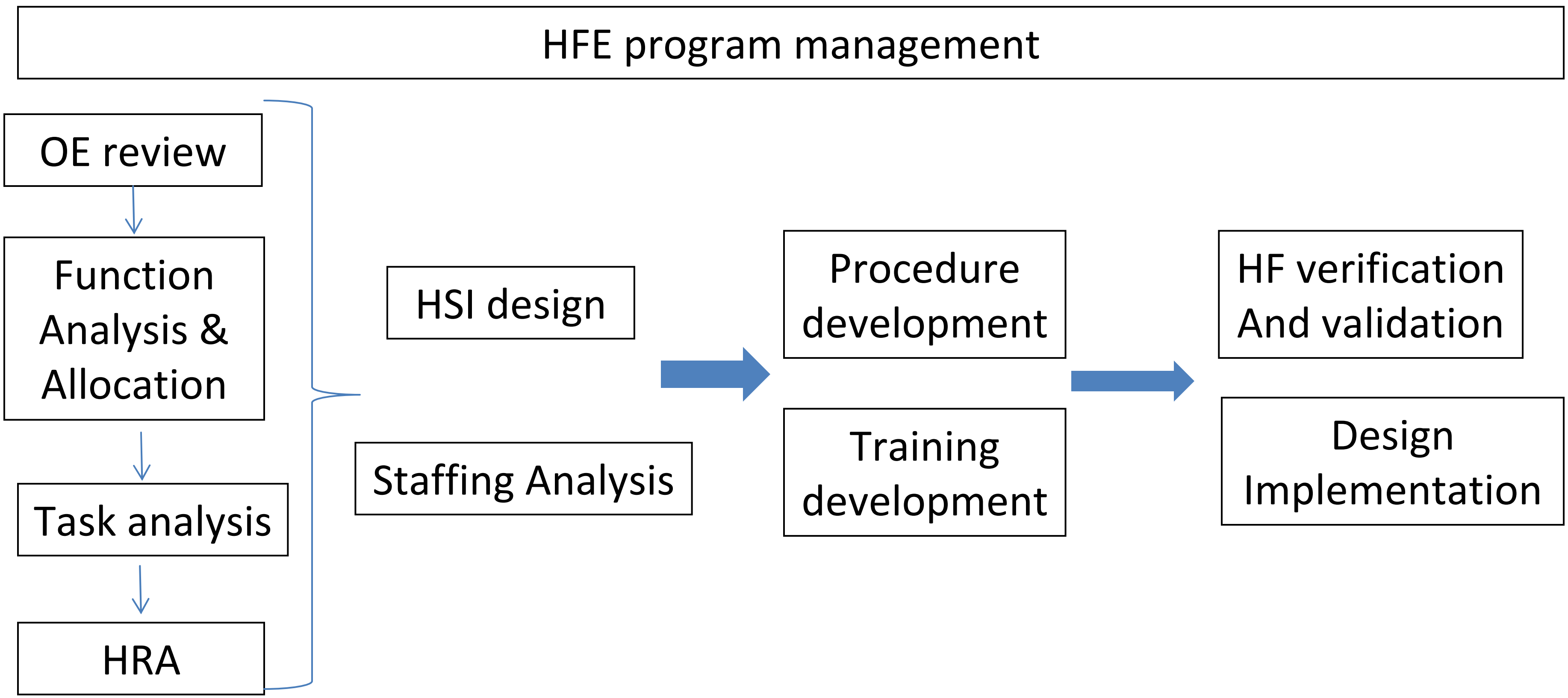
1. Analyze the impacts of I&C degradations on HSIs and operator performance during the design development process

2. Improve the HSIs so that they support operators in monitoring the I&C system and in detecting and managing degraded I&C conditions



HFE review guidance for degraded I&C

Guidance for design process: Addressing degraded I&C at every HFE elements of the design process



Examples of guidelines for design process

Operational experience review:

- Applicants should review operating experience to identify the effects of failure modes and degraded conditions of the HSI and I&C subsystem on personnel performance.

Task analysis:

- The applicant’s task analysis should identify the task requirements for managing HFE-significant I&C degradations so that risk-important tasks can be performed.

Guidance for HSI design

Total 11 guidelines for HSI design in three categories:

1. HSIs for Monitoring I&C System Conditions
   - The HSI should provide information about each I&C subsystem's status and performance parameters needed to monitor the HFE-significant aspects of the system and detect I&C degradations.

2. HSI Response to I&C System Changes
   - The HSI should support operators in determining the steps for failure recovery or back-up actions

3. Information source and quality

Summary of the project

1. Analyzed and generalized the impacts of degraded I&C on human performance

2. Established a technical basis that degraded I&C impacts human performance

3. Developed HF review guidance to improve operators' ability to monitor digital I&C systems and detect and manage degradations.

Research Challenges

- Further analysis using a more fine-grained I&C system characterization
- Effects of sensor degradations on different types of display formats
- Identification of the effect of maintenance on I&C system degradation
- Analyze methods to identify HFE-significant I&C degradations

Outline

I. Digital I&C degradation/failures

II. Human factors (HF) research in digital I&C degradation

III. HF in the NRC's Digital I&C research

The NRC's Digital I&C Research Plan

Safety aspects of digital system	Security aspects	Advanced NPP concepts	Knowledge management

3.1.1 Communications among plant-wide systems

3.1.2 Safety assessment of tool automated processes

3.1.3 Development of benchmark and reliability data

3.1.4 Integrated plant and DI&C system modeling

3.1.5 Analytic assessment of DI&C systems

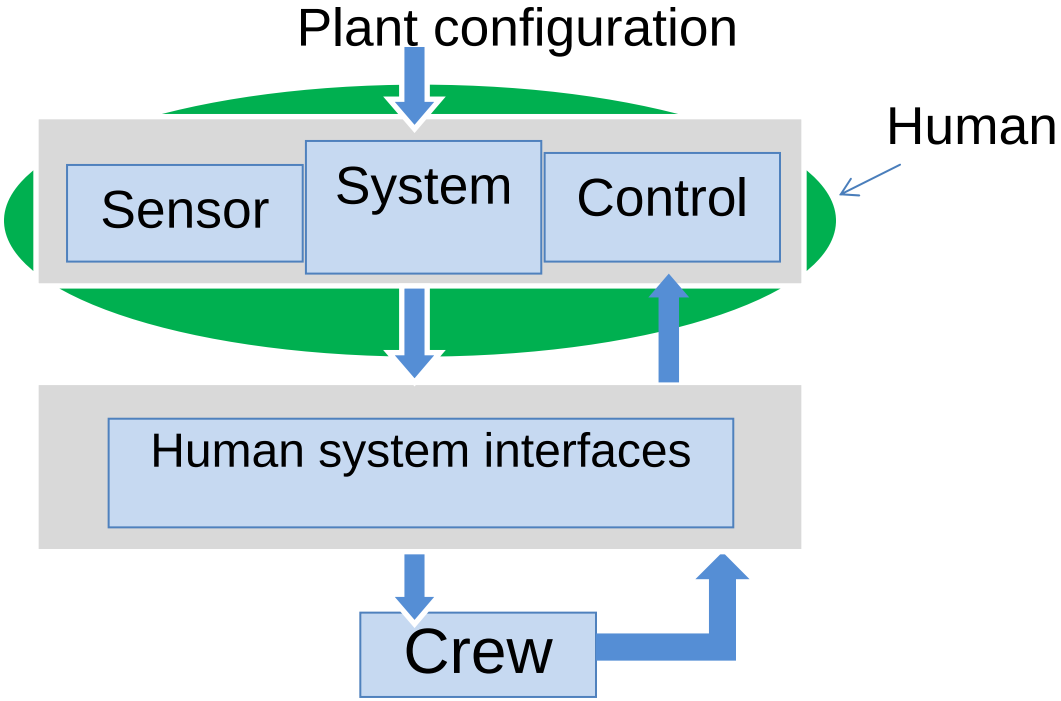
3.1.6 Digital system PRA

3.1.7 Diagnostics and prognosis

3.1.5 Analytic assessment of DI&C systems

This research will develop an NRC capability for effective and efficient assessment of digital instrumentation and control (DI&C) systematic failures during the system lifecycle. The developed knowledge base will evolve iteratively.

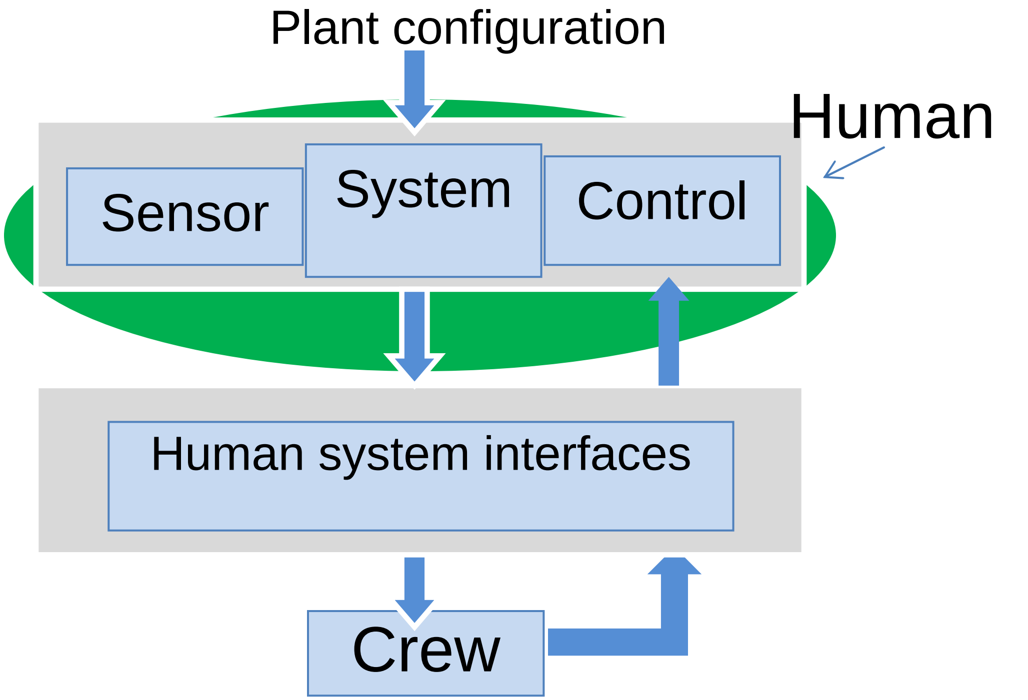
- Identify credible failure modes typical of software-intensive DI&C systems and determine the interaction of these failure modes with the rest of the systems, operating crew, and the plant by developing fault/failure models.



3.1.6 Digital System PRA

This research is to identify and develop methods, analytical tools, and regulatory guidance to support (1) NPP licensing decisions using information on the risks of digital systems and (2) including models of digital systems into NPP PRAs.

- Identify failure modes of digital systems and determine the effects on systems
- Methods for HRA associated with digital systems
  - Human errors related to HSIs.
- Human errors during upgrade of hardware and software



Future HF Research in Digital I&C