# PSAM 10

10th International Probabilistic Safety Assessment & Management Conference

**7-11 June 2010**
**Renaissance Seattle Hotel**
**Seattle, Washington**
**USA**

Conference Program Book

SCANDPOWER Risk Management
A member of the Lloyd's Register Group

CURTISS WRIGHT Flow Control Company
SCIENTECH

INL Idaho National Laboratory

CAES Center for Advanced Energy Studies

International Association for PSAM

ABS Consulting
AN ABS GROUP COMPANY

EPRI ELECTRIC POWER RESEARCH INSTITUTE

item

http://psam10.org

# Foreword

Dear Colleagues,

It's our pleasure to welcome you to PSAM10. We hope the conference provides you with ample opportunities for learning and technical discourse. Your attendance directly supports achieving the mission of IAPSAM to provide educational opportunities, and support the development and advancement of risk assessment methods helping to make the world a safer and more productive place to live. Your contributions are appreciated and valued.

This year our program includes 400 papers in 18 technical tracks covering all of the major areas of risk assessment including methods, uncertainty, space and aviation, nuclear power, human reliability and risk management just to name a few. The diversity of organizations participating in this meeting and topics that will be discussed underscore the interest and importance in the technical issues that shape our activities. We encourage you to take some time and attend a session or two outside of your area of specialty and learn about the diversity of applications of Probabilistic Safety Assessment and risk management. Build new bridges; help to broaden our fields thinking while making some new colleagues. Challenge one another, and enter into substantive dialogue!

As is our custom with this meeting, you will have a number of opportunities to renew old acquaintances and to develop new ones. We also encourage you to visit the dedicated sponsor area at the meeting to learn about new commercial products and services.

Beyond the borders of the meetings lies one of the most vibrant and unique American cities. Our local hosts and we encourage you to enjoy the Seattle area including its many restaurants and nightspots. You're never far from a bookstore or a coffee shop in this city that is known for its relaxed and eclectic atmosphere. Experience Seattle and enjoy what this fine city has to offer.

Thank you for your attendance and participation in this meeting and welcome to Seattle!

Bruce and Harold

and

**Bruce Hallbert · Idaho National Laboratory**
**Director, Nuclear Safety and Regulatory Research**
P.O. Box 1625 · Idaho Falls, ID · 83415-3855
Phone: (208) 526-9867 · Fax: (208) 526-0990 · Email: Bruce.Hallbert@inl.gov

**Harold S. Blackman, Ph.D., Director**
**Center for Advanced Energy Studies · Idaho National Laboratory**
P.O. Box 1625 · Idaho Falls, ID · 83415-3560
Phone: (208) 526- 0245 · Fax: (208) 526-8076 · Email: Harold.Blackman@inl.gov

# Acknowledgement

The PSAM 10 Conference Organizing Committee wish to express our gratitude to the many people and organizations that have contributed to ensuring the success of this conference. It is the conference participants that provide the true value and generate the most significant and lasting effects of the interactive exchanges that occur during the week of meetings. Thank you for your interest, technical contributions, and willingness to actively participate. There were numerous organizations and individuals that helped to disseminate notice of this meeting and encourage submission of technical papers. This form of support facilitated a very strong performance by the Technical Program Committee with nearly 360 papers from 32 countries in over 100 sessions will be presented and are included in the Conference Proceedings.

In addition, the conference experience has been enhanced through the financial and logistical support provided by the several contributing sponsors. The PSAM 10 Conference organizers would like to thank our sponsors, IAPSAM, Idaho National Laboratory, The Center for Advanced Energy Studies, Scandpower, and Scientech for their support.

Mrs. Hanna Shapira of Techno-Info Comprehensive Solutions (TICSs) provided the conference Web Site design and Online Software and we would also like to express our appreciation for the professionalism, technical skill and patience she has provided.

We would like to acknowledge the many efforts on behalf of IAPSAM by the Technical Program Committee for PSAM 10. In particular the conference organizers wish to acknowledge the following for their assistance, dedication and technical expertise in helping to bring about the technical program and this conference.

Tunc Aldemir
Ben Ale
George Apostolakis
Piero Baraldi
James Battles
Harold Blackman
Emanuele Bogonovo
Nattasha Freeman
Sandro Bologna
Ron Boring
Roger Boyer
Radim Bris
Mario Brito
Andreas Bye
James Chang
Simone Colombo
Wan Ki Chow
Valerio Cozzani
Vinh Dang
Homayoon Dezfuli
Enrique Lopez-Droguett
Andrew Dykes
Chester Everline
Terri Flores
Adrian Gheorghe
Ching Guey
Andrew Hale
Bruce Hallbert
Joan Harvey
Philippe Hessel
Stefan Hirschberg
Vincent Ho
Elod Hollo
Feng Hsu
Moosung Jae
David Johnson
Peter Kafka
Tsu-Mu Kao
Dana Kelly
Soli Khericha
Inn Seock Kim
James Lambert
Jeanne-Marie Lanore
Tim Leahy
James C. Lin
Antoly Lisniasky
Erasmia Lois
Gaspare Maggio
Davide Manca
Sebastian Martorell
Giuseppe Mashchio
Xie Min
Krishna Misra
Zahra Mohaghegh
Sitakanta Mohanty
Bill Nelson
Luiz Oliveira
Todd Paulos
Osvaldo Pensado
Helene Pesme
Kurt Petersen
Jerry Phillips
Luca Podofillini
Pekka Pyy
Alan Roe
Budhi Sagar
Oliver Salvi
Yoshinobu Sato
Martin Sattison
Zdenko Simic
Nathan Siu
Cornelia Spitzer
Andreas Strohm
Peter Swift
Magdy (Samy) Tawfik
Paolo Trucco
Jan Erik Vinnem
Reino Virolainen
Joon-Eon Yang
Jonathan Young
Bob Youngblood

# Previous PSAM Conferences

| | |
|---|---|
| PSAM 1 | Beverly Hills, CA, USA, February 1991<br>General and Technical Program Chair: G. E. Apostolakis |
| PSAM 2 | San Diego, CA, USA, March 1994<br>General Chair: M. G. Stamatelatos<br>Technical Program Chair: G. E. Apostolakis |
| PSAM 3 | (Held in conjunction with ESREL'96)<br>Crete, Greece, June 1996<br>General Chair: I. A. Papazoglou<br>Technical Chair: P. C. Cacciabue |
| PSAM 4 | New York, New York, USA, September 1998<br>General Chair: R. A. Bari<br>Technical Program Chair: A. Mosleh |
| PSAM 5 | Osaka, Japan, November 2000<br>Honorary Chair: H. Uchida<br>General Chair: S. Kondo<br>Technical Program Chairs: S. Kondo and K. Furuta |
| PSAM 6 | San Juan, Puerto Rico, USA, June 2002<br>General Chair: E. J. Bonano<br>Technical Program Chair: A. L. Camp<br>Technical Program C-Chair: A. Ghassemi |
| PSAM 7 | (held in conjunction with ESREL'04)<br>Berlin, Germany, June 2004<br>General Chair: C. Spitzer<br>Technical Program Chair: U. Schmocker<br>Associate General Chair: E. Zio<br>Technical Program C-Chairs: S. Chakraborty, M. Faber, and S. Hirschberg |
| PSAM 8 | New Orleans, USA, May 2006<br>General Co-Chairs: D. Johnson and L. J. Steinberg<br>Technical Program Co-Chairs: H. Blackman and M. Stamatelatos |
| PSAM 9 | Hong Kong, China, May 2008<br>General Chair: V. Ho<br>Technical Program Chair: Tsu-Mu Kao<br>Associate Technical Program Chair: E. Zio |

# Welcome

SCANDPOWER
Risk Management

Settle, June 2010

**WELCOME TO PSAM 10!**

Dear Fellow Risk Professionals,

Scandpower welcomes you to Seattle! Scandpower has been a long-time supporter of and participant in past PSAMs and is pleased to sponsor the Welcoming Reception at PSAM 10.

Scandpower has a long history of contributing to the international PSA community both as a consultancy business and as a software developer. The latter started already in 1986 when RELCON, later to merge with Scandpower in 2007, released the first PC-based software in the world for fault tree analysis. Our dedication to the development of PSA tools and applications has continued since then and today we are very proud of our achievements. Our software suite includes the flagship product RiskSpectrum® PSA - currently licensed for use at 50% of all nuclear power plants in the world.

Ever since the beginning of PSAM conferences we have enjoyed the high quality of the presentations and also had the honour to give a large number of presentations through the years. PSAM 10 is no exception - we will present more than 20 papers from applications in both the nuclear and other industries. We are looking forward to many interesting discussions this week, and to jointly contribute to the advance of the science of risk.

We also would like to encourage you to look ahead and put PSAM 11 – the Conference under the slogan of "Nordic Footprints" to be held in Helsinki in 2012 - into your calendars.

Again, a warm welcome!

Yours faithfully
Scandpower AB

Jerzy Grynblat
Nuclear Business Director

T +46 (0)8 445 21 11
M +46 (0)70 773 06 33
F +46 (0)8 445 21 01
SE-172 25 SUNDBYBERG, SWEDEN

www.scandpower.com
www.riskspectrum.com

A member of the Lloyd's Register Group

Lloyd's Register

# Welcome

CURTISS WRIGHT Flow Control Company
SCIENTECH

June 7, 2010

Dear PSAM Attendee:

As the Local Host for PSAM 10, Scientech is pleased to welcome you to this important conference and to the wonderful city of Seattle.

Sometimes the difference between ordinary and amazing is where it happens. Seattle is anything but ordinary. It's a place where bike messengers share elevators with world-renowned researchers. Where fishermen have lunch alongside top surgeons. It's a city where the extraordinary is commonplace and commonplace is anything but. And if you look closely, you just might discover that in Seattle there are amazing things happening all around you.

From a jet engine to an espresso machine to grunge rock, Seattle's world-changing events have all had a distinct sound. But the symphony doesn't end there. Your visit to Seattle may bring you the sound of an orca blowing as it surfaces, the roar of the crowd at Safeco Field or the near silence of the Olympic rainforest. While you are in Seattle we hope that you are able to take the time to listen and to hear for yourself!!!!

We consider it a great privilege to help the PSAM 10 Program team with the conference and are ready to assist in you in your stay in Seattle in any way.

Our Warmest Regards,

Daniel C. Rees — Jeffrey A. Julius

Scientech,
a business unit of Curtiss-Wright Flow Control Company

# Committees

## Technical Program Committee

Piero Baraldi
James Battles
Sandro Bologna
Ron Boring
Roger Boyer
Mario P. Brito
Wan Ki Chow
Valerio Cozzani
Vinh Dang
Adrian Gheorghe
Ching Guey
Feng Hsu
Moosung Jae
David Johnson
Tsu-Mu Kao
Soli Khericha
Tim Leahy
Anatoly Lisniansky
Erasmia Lois
Gaspare Maggio
Xie Min
Zahra Mohaghegh
Sitakanta Mohanty
Bill Nelson
Todd Paulos
Helene Pesme
Alan Roe
Budhi Sagar
Marty Sattison
Zdenko Simic
Joon-Eon Yang
Jonathan Young
Bob Youngblood

## Technical Program Committee Members At Large

Tunc Aldemir
Ben Ale
George Apostolakis
Harold Blackman
Emanuele Bogonovo
Radim Bris
Andreas Bye
James Chang
Simone Colombo
Homayoon Dezfuli
Enrique Lopez Droguett
Andrew Dykes
Chester Everline
Nattasha Freeman
Andrew Hale
Bruce Hallbert
Joan Harvey
Philippe Hessel
Stefan Hirschberg
Vincent Ho
Elod Hollo
David Johnson
Peter Kafka
Dana Kelly
Inn Seock Kim
James Lambert
Jeanne-Marie Lanore
James C. Lin
Davide Manca
Sebastian Martorell
Giuseppe Mashchio
Krishna Misra
Luiz Oliveira
Todd Paulos
Osvaldo Pensado
Kurt Petersen
Jerry Phillips
Luca Podofillini
Pekka Pyy
Oliver Salvi
Yoshinobu Sato
Nathan Siu
Cornelia Spitzer
Andreas Strohm
Peter Swift
Magdy (Samy) Tawfik
Paolo Trucco
Jan Erik Vinnem
Reino Virolainen

# General Information

## Registration

Registration is required for all attendees and presenters. Badges are required for admission to all events.

The Full Conference Registration Fee includes: Welcome Reception, Tillicum Village Dinner Excursion, Conference Luncheon, proceedings, and admittance to technical sessions.

The Student Registration Fee includes: Welcome Reception, Tillicum Village Dinner Excursion, Conference Luncheon, proceedings, and admittance to technical sessions.

Spouse/Guest: Registrants can purchase extra tickets for guests to Welcome Reception ($-50.00/ ticket) on June 7, 2010 or to the Tillicum Village Dinner Excursion ($-50.00/ ticket) on June 9, 2010

The meeting registration desk is at Courtyard Foyer

| | |
|---|---|
| Sunday | 8:00 AM – 3:00 PM |
| Monday | 7:30 AM – 4:00 PM |
| Tuesday | 7:30 AM – 4:00 PM |
| Wednesday | 7:30 AM – 4:00 PM |
| Thursday | 7:30 AM – 4:00 PM |

## Conference Proceedings

Conference Proceedings, in CD-ROM format, are included with the program book. Please check the vinyl pocket inside the back cover of the program book.

## Speaker Information

Please sign the “Speaker Sign-in Form” at the registration desk. Please be sure to bring your presentation in MicroSoft PowerPoint format. Note that the total time available for presentations (other than the plenary) varies from 18 to 25 minutes based on the number of presentations in a session. We recommend that you allow 1 to 3 minutes for questions and discussion at the end of your talk. Be alert, responsive and respectful to other speakers when the Session Chair signals you that you’ve got 5 and 2 minutes remaining in your time slot. As a presenter you will be able to use your own laptop, although one will be provided in the session room, or bring a memory stick. It is your responsibility to check with the Session Chair for file compatibility prior to the start of your session. We recommend that you seek out and meet your Session Chair prior to the time of your presentation. Please meet the Session Chair at the presentation room 15 minutes before the session begins and provide a brief biography (name, organization 2-3 line description of current work assignment). Please check the signs and handouts for further information. Please contact any of the meeting organizers if you need help or have questions.

## Session Chair Information

Please complete and return a “Session Chair Sign-in Form” to the Registration Desk the morning you are scheduled to Chair a Session(s). Please be present at your session room at least 15 minutes prior to the start of your session. This will allow you to greet and coordinate media arrangement s with the speakers, as well as collect biographical sketches. For the sake of meeting attendees, PLEASE keep the session synchronized as shown in this final program. For “no shows” simply adjourn the session at the next allotted time slot (i.e., don’t shift papers to an earlier session to fill a void). You may find it helpful to bring your own laptop and upload the speakers’ presentations prior to your session. A laptop will be provided and set-up in each of the session rooms for the daily sessions.

# Things to do in Seattle

You can't go to Paris without stopping by the Eiffel Tower. And you can't visit Seattle without checking out the view from the world-famous Space Needle. Here's a handy "must do" list for first-time visitors and those who want to be sure they've done everything (it may take more than one trip).

**The Space Needle**
Seattle Center, 400 Broad St.; 206.905.2100;
www.spaceneedle.com

A 41-second elevator ride takes you up 520 feet to the observation deck of the Space Needle, built for the 1962 World's Fair. Enjoy a meal at SkyCity, the restaurant at the top that revolves 3600 while you dine.

**Pike Place Market**
Between First Ave. and Western, from Pike to Virginia streets
www.pikeplacemarket.org

Born in 1907, Seattle's Pike Place Market is the granddaddy of farmers 'markets. Today, it's a major tourist attraction with 200 businesses operating year-round, 190 craftspeople and 120 farmer booths - plus street performers and musicians. Flowers by the bucketful, flying fish, fresh pastries and fruit, handmade cheeses, local honey, wine, an assortment of restaurants, import goods, antiques, collectibles and lots of surprises are around every corner.

**Ferries**
www.wsdot.wa.gov/ferries

Traveling by ferry is a state of mind as much as a means of transportation to some of the Puget Sound's most historic and scenic sites. Views of the Olympic and Cascade mountains, the Seattle cityscape and the green shorelines will thaw you out onto the deck to feel the salt breeze on your face. The state ferry system takes passengers and their vehicles from Seattle and nearby departure points to Vashon Island, the Kitsap Peninsula, the San Juan Islands and Canada. For privately operated ferries, see the Sightseeing & Tours (page 35) and Visitors Services/Travel & Transportation (page 120) listings in this guide.

**Seattle Aquarium Pier 59**
206.386.4300
www.seattleaquarium.org

Meet Alki, the sea otter pup born at the Aquarium. Walk under the water in a glass dome as bluntnose sixgill sharks and other Elliott Bay creatures swim all around you. Touch a sea anemone. Learn about the lives of salmon at the world's first aquarium-based salmon ladder. Marvel at the impossibly bright-colored coral reef fish. And don't forget to wave to the giant Pacific octopus.

**The Seattle Waterfront Piers 52 to 70 on Alaskan Way**
ci .seattle.wa.us/tour/water.htm

A bustling collection of attractions, restaurants and shopping, as well as starting points for ferries, cruise ships, the Victoria Clipper and Argosy boat tours are located here – Plus a new outdoor sculpture museum. Feed the seagulls at the statue of Ivar Haglund in front of Ivar's Acres of Clams, stroll by the fountains on the wooden piers of Waterfront Park, admire the view or shop for souvenirs.

**Woodland Park Zoo**
South Gate: 750 N. 50th St
206.684.4800
www.zoo.org

See more than 1 ,000 animals of 300 different species, from elephants and gorillas to piranhas and penguins, in naturalistic exhibits at the Woodland Park Zoo. Drop by at scheduled feeding times and talk with the people who care for the animals.

**Bill Speidel's Underground Tour 608 First Ave.**
206.682.4646
www.undergroundtour.com

After the Great Seattle Fire of 1889, the city was rebuilt overthe top of the ruins. This guided tour takes visitors through the hidden subterranean passages that once were the main roadways and storefronts of old downtown Seattle and tells stories of the frontier people who lived and worked there.

**The Seattle Public Library 1000 Fourth Ave.**
206.386.4636
www.spl.org

Designed by world-renowned Dutch architect Rem Koolhaas, the award-winning glass and steel structure of the new Central Library makes the building seem a little off-kilter and translucent - allowing passersby on the street to look in. It's only ½ block from our PSAM hotel.

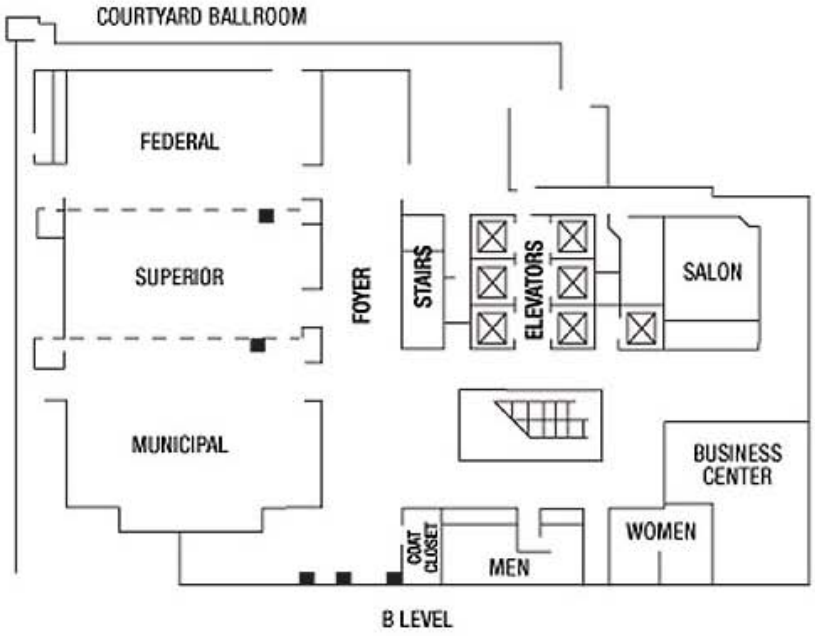
**Tillicum Village Blake Island**
206.933.8600
www.tillicumvfflage.com

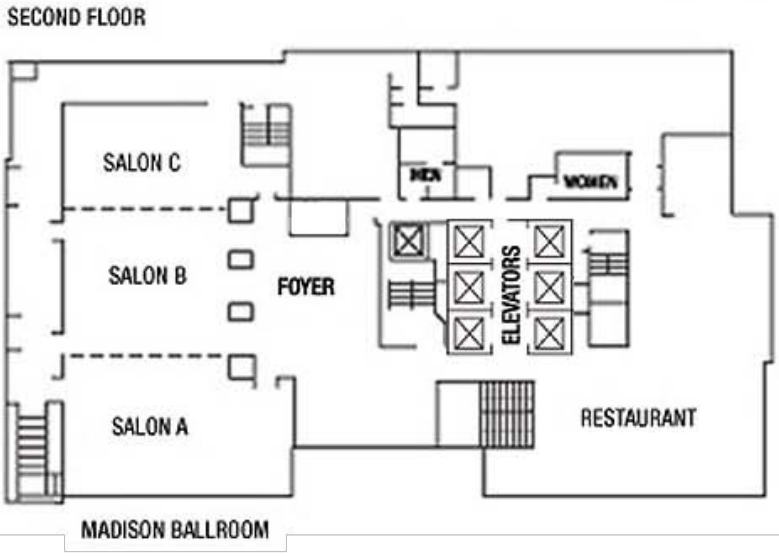
A short, narrated cruise takes you to an island village, where you'll feast on salmon cooked in the authentic Native American way. A stage show of traditional dances and stories entertains and teaches you about the people who lived in the Northwest first.

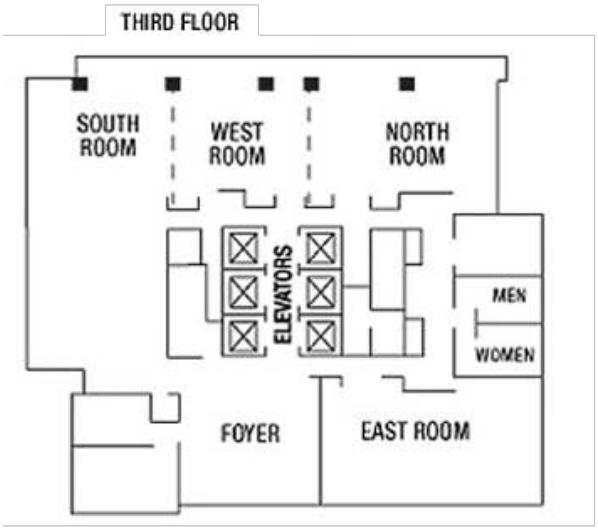
**Ride the Ducks of Seattle 516 Broad St, Seattle**
206 .441 .DUCK (3825)
www.ridetheducksofseattle.com

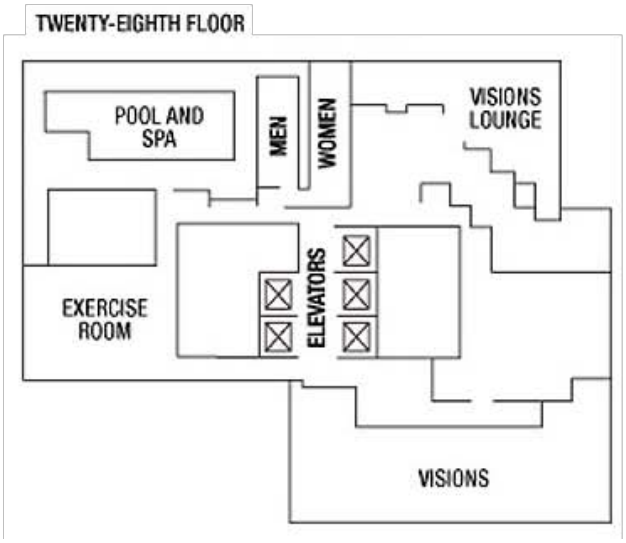
Tour Seattle by land and water on a WWII amphibious landing craft. This 90-minute adventure tour will have you "quacking up" through the streets of Seattle. You'll see the major sights of the Emerald City on land before you head out to the funky Fremont neighborhood where you'll splash into Lake Union.

# Meeting Rooms



# Meeting Highlights

| | Time | Program |
|---|---|---|
| **Sunday** | 08:00 – 15:00 | Conference Registration<br>Courtyard Foyer |
| | 08:00 – 17:00 | System Safety & Reliability: Assessment & Management Workshop<br>Salon B |
| | 08:00 – 17:00 | Special Topics for Risk Assessment in Event Evaluation Workshop<br>Salon C |
| | 08:00 – 17:00 | HRA Special Workshop, by invitation only<br>Visions |
| | 15:00 – 19:00 | IAPSAM Board Meeting<br>Salon A |
| **Monday** | 07:30 - 1600 | Conference Registration<br>Courtyard Foyer |
| | 08:30 – 10:00 | Welcome and Plenary Session |
| | 10:00 – 17:00 | Technical Sessions |
| | 18:30 – 21:00 | Welcome Reception<br>Madison Ballroom<br>Sponsored by Scandpower |
| **Tuesday** | 07:30 - 1600 | Conference Registration<br>Courtyard Foyer |
| | 08:30 – 10:00 | Plenary Session |
| | 10:00 – 17:00 | Technical Sessions |
| | 12:00 – 1:30 | Conference Luncheon<br>Madison Ballroom |
| | 17:30 – 20:30 | IAPSAM Board Meeting<br>Visions |
| **Wednesday** | 07:30 – 1600 | Conference Registration<br>Courtyard Foyer |
| | 08:30 – 10:00 | Plenary Session |
| | 10:00 – 17:00 | Technical Sessions |
| | 17:45 – 22:00 | Gala Dinner at Tillicum Village<br>Meet buses at hotel lobby at 17:45 for transport to Argosy Pier |
| **Thursday** | 07:30 – 1600 | Conference Registration<br>Courtyard Foyer |
| | 08:30 – 10:00 | Plenary Session |
| | 10:00 – 17:00 | Technical Sessions |
| **Friday** | 10:00 – 11:30 | End of Conference Meeting and Ice Cream Social |

SCANDPOWER
Risk Management

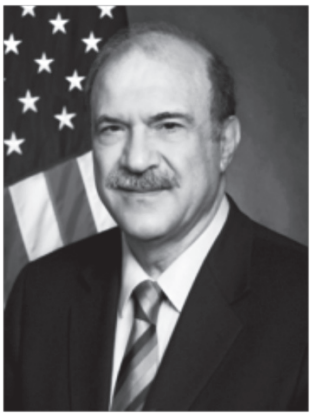
## Detailed "Meeting-At-A Glance" for Monday through Friday are provided on pages 11, 28, 45, 62, and 75

# Monday Meeting-At-A Glance

| Room Session | Salon A | Salon B | Salon C | East Room | West Room | North Room | Municipal | Federal | Superior | South Room |
|---|---|---|---|---|---|---|---|---|---|---|
| 0730 - 1600 | **Conference Registration - Courtyard Foyer** | | | | | | | | | |
| 0700 - 0830 | **Continental Breakfast - Madison, Courtyard and Compass Foyers** | | | | | | | | | |
| 0830 - 1000 | Welcome - Vincent Ho, Bruce Hallbert and Harold Blackman - Plenary Speaker - Commissioner George Apostolakis - Courtyard Ballroom | | | | | | | | | Exhibits |
| 1000 - 1030 | ***Coffee/Refreshment Break - Madison, Courtyard, and Compass Foyers*** | | | | | | | | | |
| 1030 - 1200 | Advanced Reactors 16-1: Passive Systems Reliability I | Modeling and Simulation 2-1: Phenomenological Analyses | HRA 5-1: International HRA Benchmark | PSA Applications 1-1: Loss of Offsite Power Risk | External Events 15-1: Fire: PRA I | Safety Culture 9-1: Socio-technical Modeling I | Space & Aviation 12-1: Space Shuttle PRA Applications | Decision Analysis 8-1: Methods and Fundamentals | PSA Applications 1-11: Uncertainty Analysis | |
| 1200 - 1330 | ***Lunch - on your own*** | | | | | | | | | |
| 1330 - 1500 | Advanced Reactors 16-2: Passive Systems Reliability II | Modeling and Simulation 2-2: Dynamic Systems PSA | HRA 5-2: International HRA Benchmark II | PSA Applications 1-2: Accident Precursor Analysis | External Events 15-2: Fire: PRA II | Safety Culture 9-2: Assessing Safety Culture Data | Space & Aviation 12-2: Aircraft Safety | Decision Analysis 8-2: Strategic Assessments | PSA Applications 1-12: General PSA Applications I | |
| 1500 - 1530 | ***Coffee/Refreshment Break - Madison, Courtyard, and Compass Foyers*** | | | | | | | | | |
| 1530 - 1700 | Advanced Reactors 16-3: Regulatory Perspectives | Modeling and Simulation 2-3: Nuclear Power Plant Level 2 PSA | HRA 5-3: Resolving HRA Models Differences | PSA Applications 1-3: Safety Margin Assessment | External Events 15-3: Fire: Modeling & Uncertainty Analysis | Safety Culture 9-3: Safety Culture Methodologies & Applications | Space & Aviation 12-3: Space Launch Vehicle Risk Assessments | Software Reliability 10-1: Software PRA | PSA Applications 1-13: General PSA Applications II | |
| 1830 - 2100 | ***Welcome Reception - Sponsored by Scandpower - Madison Ballroom***  SCANDPOWER Risk Management | | | | | | | | | |

# Plenary Speaker

## Commissioner George Apostolakis



The Honorable George Apostolakis was sworn in as a Commissioner of the U.S. Nuclear Regulatory Commission (NRC) on April 23, 2010, to a term ending on June 30, 2014.

Dr. Apostolakis has had a distinguished career as an engineer, professor and risk analyst. Before joining the NRC, he was the Korea Electric Power Corporation professor of Nuclear Science and Engineering and a professor of Engineering Systems at the Massachusetts Institute of Technology. He was also a member and former chairman of the statutory Advisory Committee on Reactor Safeguards of the NRC.

In 2007, Dr. Apostolakis was elected to the National Academy of Engineering for "innovations in the theory and practice of probabilistic risk assessment and risk management." He has served as the Editor-in-Chief of the International Journal Reliability Engineering and System Safety and is the founder of the International Conferences on Probabilistic Safety Assessment and Management. He received the Tommy Thompson Award for his contributions to improvement of reactor safety in 1999 and the Arthur Holly Compton Award in Education in 2005 from the American Nuclear Society.

Dr. Apostolakis has published more than 120 papers in technical journals and has made numerous presentations at national and international conferences. His research interests include the use of Probabilistic Risk Assessment (PRA) in reactor design; uncertainty analysis; decision analysis; infrastructure security; risk-informed and performance-based regulation; human reliability; and risk management involving multiple stakeholders. He has edited or co-edited eight books and conference proceedings and has participated in many PRA courses and reviews.

Dr. Apostolakis received his diploma in electrical engineering from the National Technical University in Athens, Greece in 1969. He earned a master's degree in engineering science from the California Institute of Technology in 1970 and a Ph.D. in engineering science and applied mathematics in 1973, both from the California Institute of Technology.

---

**Safety Culture: A Regulatory Perspective**

The presentation will address the commission's ongoing efforts to develop a Safety Culture (SC) policy statement that will set forth the agency's expectations for fostering a strong SC for USNRC regulated activities. The topics will include a summary of NRC efforts and what has been done thus far to reach out to a large number of NRC-regulated entities to consider a more common terminology for safety culture that will allow licensees and regulators to understand and adhere to a common policy statement. The Commission benefits from consideration of a spectrum of views in order to inform the development of a final SC policy statement, the development of a high-level SC definition, description and traits that could apply to all licensees and certificate holders. The presentation will provide a summary of the Commission's direction to staff including the draft safety culture policy statement. Other topics to be discussed include whether safety culture as applied to reactors should be strengthened, efforts to increase attention to safety culture in the nuclear materials area and considering the safety and security interfaces when developing NRC's expectations for safety culture.

# Advanced Reactors

**Monday, Salon A**

10:30 AM - Noon

## 16-1: Passive Systems Reliability I

Session Chairs: Jiejuan Tong, Nicola Pedroni

### Artificial Neural Networks and Quadratic Response Surfaces for the Functional Failure Analysis of a Thermal-Hydraulic Passive System

George Apostolakis(a), Nicola Pedroni(b), Enrico Zio(b)
*a) Massachusetts Institute of Technology, Nuclear Science and Engineering Dept., Cambridge, USA. b) Politecnico di Milano, Energy Department, Milano, Italy*

In this paper, bootstrapped Artificial Neural Network (ANN) and quadratic Response Surface (RS) empirical regression models are used as fast-running surrogates of a thermal-hydraulic (T-H) system code to reduce the computational burden associated with the estimation of the functional failure probability of a T-H passive system. The ANN and quadratic RS models are built on few data representative of the input/output nonlinear relationships underlying the T-H code. Once built, these models are used for performing, in reasonable computational time, the numerous system response calculations required for failure probability estimation. A bootstrap of the regression models is implemented for quantifying, in terms of confidence intervals, the uncertainties associated with the estimates provided by ANNs and RSs. The alternative empirical models are compared on a case study of an emergency passive decay heat removal system of a Gas-cooled Fast Reactor (GFR).

### Evaluation of the Dependencies Related to Passive System Reliability

Luciano Burgazzi
*ENEA, Bologna, Italy*

A major issue to be addressed in safety and risk studies related to advanced reactors is the reliability of the implemented passive safety features. The passive safety system operation is a quite complex process. This complexity gives rise to unpredictable failure patterns. While there are a number of well-established failure analysis (physics-of-failure) models for individual components, these models do not hold good for complex systems as their failure behaviors may be totally different. These models are based on the assumption of independent failure mechanisms, but are unable to capture the system interaction effects on failure behavior. These considerations apply to the approach to the passive system reliability assessment based on independent modes of failure. Within this methodology, the selected system critical parameters are properly modeled through the construction of probability distributions and arranged as in a series system configuration. The application of the methodology to a realistic thermal-hydraulic passive system design is illustrated. The analysis reveals that the critical parameters are not suitable to be chosen independently of each other, mainly because of the expected synergism between the different phenomena under investigation, with the potential to jeopardize the system performance. This conclusion allows the implementation of the proposed methodology, by properly capturing the interaction between various failure modes.

1:30 - 3:00 PM

## 16-2: Passive Systems Reliability II

Session Chair: Enrico Zio

### Multi-Experts Analytic Hierarchy Process for the Sensitivity Analysis of Passive Safety System

YU Yu(a), LIU Tao(a), TONG Jiejuan(a), ZHAO Jun(a), DI MAIO Francesco(b), ZIO Enrico(b), and ZHANG Aling(a)
*a) Institute of Nuclear and New Energy technology, Tsinghua University, Beijing, China. b) Department of Energy, Polytechnic of Milan, Milan, Italy*

Innovative Nuclear Power Plants (NPPs) resort to passive systems to increase their safety and reliability. However, during accidental scenarios, uncertainties affect the actual behavior of passive systems. In this paper, a systematic procedure based on the Analytic Hierarchy Process (AHP) for the identification of the uncertain parameters and the propagation of their associated uncertainties is proposed. An example of application is proposed with respect to the passive Residual Heat Removal system (RHRs) of the High Temperature Reactor-Pebble Modular (HTR-PM).

### Stochastic Analysis of Natural Circulation Decay Heat Removal of Sodium Cooled Fast Reactor based on Latin Hypercube Sampling

Takashi Takata, Tomoya Seki and Akira Yamaguchi
*Graduate School of Engineering, Osaka University, Osaka, Japan*

A stochastic analysis of uncertainty correlation between input variables and analytical result of a computational simulation has been performed in the present study. A natural circulation decay heat removal in a sodium cooled fast reactor is chosen as a target phenomenon. The Midpoint Latin Hypercube Sampling (MLHS) and the correlation ratio are used to evaluate the rank of input variables upon the phenomenon. A common uncertain factor among the input variables has also been considered in the random sampling. As a result, it is concluded that the uncertainty correlation can be evaluated with the present method even when the common uncertain factor exists in some input parameters.

### A Study on Multiple Failure States Criteria for Assessing Reliability of Passive Systems for Innovative Reactor

Seok-Jung Han And Joon-Eon Yang
*Korea Atomic Energy Research Institute, Yuseong-Gu, Daejon, Republic of Korea*

When an assessment of the reliability of passive systems (RoPS) is performed for an innovative reactor such as Very High Temperature Reactors (VHTR), it could not clearly define a state to determine the system failure (i.e., success or failure criteria of the system). Especially, this fact can be enlarged in an implementation of Probabilistic Safety Assessment (PSA). This article examined the characteristics of multiple failure states criteria (MFSC) to determine the status of a passive system based on a PSA framework. Four different types of failure criteria (single value, multiple values, single probability distribution and multiple probability distributions) were addressed. The obtained insights and discussion were described in this article.

3:30 - 5:00 PM

## 16-3: Regulartory Perspectives

Session Chair: Tim Leahy

### Use of SPAR Models for New Reactors

Donald Dube(a), Lynn Mrowca(a), Theresa Clark(a), and Christopher Fong(b)
*a) U.S. Nuclear Regulatory Commission, Washington, DC, USA. b) U.S. Nuclear Regulatory Commission, Region II, Atlanta, GA, USA*

This paper describes the use of the Standardized Plant Analysis Risk (SPAR) models by the U.S. Nuclear Regulatory Commission staff in risk-informed regulatory activities including reactor oversight. The authors discuss how SPAR models have been used for currently operating plants and how the staff expects to extend this use for evolutionary and passive light-water reactor designs. The staff has been actively exercising the AP1000 SPAR model developed by Idaho National Laboratory (INL) in 2009. Current plans are for INL to complete the development of the Advanced Boiling Water Reactor (ABWR) design model, followed by SPAR models for the Economic Simplified Boiling Water Reactor (ESBWR), United States Evolutionary Power Reactor (U.S. EPR), and United States Advanced Pressurized Water Reactor (US-APWR). Challenges related to the use of the SPAR models, including technical adequacy and configuration control, are discussed.

### Reliability Assurance Program for New Reactors and Lessons Learned and Insights Gained

Todd Hilsmeier, Lynn Mrowca, Hossein Hamzehee, and Malcolm Patterson
*U.S. Nuclear Regulatory Commission, Washington, D.C. USA*

The U.S. Nuclear Regulatory Commission reviews the reliability assurance program (RAP) for new reactor applications using NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Section 17.4, "Reliability Assurance Program." The RAP applies to those systems, structures, and components (SSCs) that are identified as being risk-significant (or significant contributors to plant safety). These SSCs are identified through probabilistic and deterministic analyses, including information obtained from the probabilistic risk assessment (PRA) and severe accident evaluations. The purposes of the RAP are to provide reasonable assurance that: • a reactor is designed, constructed, and operated consistent with the risk insights and key assumptions from probabilistic, deterministic, and other methods of analysis, • the SSCs within the scope of RAP do not degrade to an unacceptable level of reliability, availability, or condition during plant operations, • the frequency of transients that challenge these SSCs is minimized, • these SSCs function reliably when challenged. The goal of this paper is to describe the RAP process, taking into consideration the lessons learned and insights gained from RAP reviews of new reactor applications. It also identifies the most recent guidance on RAP, which incorporates these lessons

and insights.

### Implementation of Risk-Informed Applications for New Reactors

Nicholas T. Saltos, Lynn A. Mrowca, and Theodore R. Tjader
*U.S. Nuclear Regulatory Commission, Washington D.C., USA*

Probabilistic risk assessment (PRA) results have been used in the design certification and combined operation license (COL) processes to risk-inform decisions (e.g., to determine testing intervals), to the extent that this can be supported by the available PRA. However, there has been increased interest by applicants to obtain early approval (e.g., as part of the COL application) to implement risk-informed programs (e.g., risk managed technical specifications (RMTS)) when the plant transitions to operation. These programs require a detailed PRA model that incorporates "as-built, as operated" information. Several issues were identified which must be addressed before the available guidance for operating reactors can be used in this type of program for new reactors. These issues stem primarily from differences in the timing of the review and approval process for new and operating reactors, the lack of plant-specific operational experience for new reactors, and the use of different risk metrics for new reactor licensing. Although these issues impact primarily programmatic risk-informed applications (e.g., RMTS), some of these issues (e.g., risk metrics) impact also most license amendments that may be proposed after the new reactor transitions to operation. Options are being considered by the U.S. Nuclear Regulatory Commission to address these issues.

### Probabilistic Risk Assessments of Digital I&C in Nuclear Power Plant

Li Shi(a), Robert Enzinna(b), Steve Yang(c), Scot Blodgett(d)
*a) I&C Electrical System, Altran Solutions Corp. b) Risk & Reliability Engineering, AREVA NP. c) I&C V&V, AREVA NP. d) I&C Electrical System, Altran Solutions Corp*

Key issues associated with the characteristics of the digital system are discussed in this paper. These issues are: Understanding the failure modes of the digital components, the fault coverage of the digital systems (e.g., the portion of the failure rate that are selfmonitored and non self-monitored), the treatment of software (SW) reliability/ common cause failure(CCF), the hardware failure data and planning ahead for integration with the overall plant PRA. The modeling techniques corresponding to each of the issues above are discussed and summarized in this paper. These approaches are realistic and conservative. It also shows that by relying upon good engineering judgment and simplified modeling techniques, the NPP risk importance of a digital I&C system can be estimated with relative low cost. The discussed and summarized methods are suitable for estimating the probabilistic risk of digital instrumentation and control (I&C) systems in nuclear power plants (NPP) for design certification (DC) and combined operating license (COL) applications at both new plants and operating plants.

# Modeling and Simulation

**Monday, Salon B**

10:30 AM - Noon

## 2-1: Phenomenological Analyses

Session Chairs: David Johnson, Todd Paulos

### Bayesian Inference for Time Trends in Parameter Values: Case Study for the Ageing PSA Network of the European Commission

Albert Malkhasyan(a), Dana L. Kelly(b)
*a) Massachusetts Institute of Technology, Nuclear Science and Engineering Dept., a) Nuclear & Radiation Safety Center, Yerevan, Armenia. b) Idaho National Laboratory, Idaho Falls, USA*

There is a nearly ubiquitous assumption in PSA that parameter values are at least piecewise-constant in time. As a result, Bayesian inference tends to incorporate many years of plant operation, over which there have been significant changes in plant operational and maintenance practices, plant management, etc. These changes can cause significant changes in parameter values over time; however, failure to perform Bayesian inference in the proper time-dependent framework can mask these changes. Failure to question the assumption of constant parameter values, and failure to perform Bayesian inference in the proper time-dependent framework were noted as important issues in NUREG/CR-6813, performed for the U. S. Nuclear Regulatory Commission's Advisory Committee on Reactor Safeguards in 2003. That report noted that "industry lacks tools to perform time-trend analysis with Bayesian updating." This paper describes an application of time-dependent Bayesian inference methods developed for the European Commission Ageing PSA Network. These methods utilize open-source software, implementing Markov chain Monte Carlo sampling. The paper also illustrates the development of a generic prior distribution, which incorporates multiple sources of generic data via weighting factors that address differences in key influences, such as vendor, component boundaries, conditions of the operating environment, etc.

### A Systemic Use Of Coupled FMEA-PSA Tool In A Nuclear Application

Ola Bäckström and Anna Häggström
*Scandpower-Lloyd's Register, Stockholm, Sweden*

An FMEA is an excellent tool for establishing and communicating the failure modes in a system with the plant experts. For several PSA studies the FMEA has been documented using MS Excel® spreadsheets, but the use of FMEA in that way has been considered to have several drawbacks. The FMEA has for example been considered hard to keep alive, up-to-date, and to verify that the failure modes included are represented by the PSA model have added an extra documentation task. It has also been necessary to update the component failure data twice – in the FMEA and in the PSA model. Using a specially designed FMEA application could solve these issues and for a number of PSA studies the FMEA spreadsheets have been transferred to RiskSpectrum® FMEA. However, in the process of establishing an FMEA that has a one-to-one relation with the PSA model several problems have been identified that need special attention, such as how to handle components with several different mission times for the same failure mode and components with several test intervals modeled.

### A Generic Failure Modes and Effects Analysis (FMEA) Approach for Reliability Modeling of Digital Instrumentation and Control (I&C) Systems

Tsong-Lun Chu, Meng Yue, Gerardo Martinez-Guridi, John Lehner
*Brookhaven National Laboratory, Upton, NY, USA*

In this paper, a systematic failure modes and effects analysis (FMEA) approach is proposed for creating reliability models for digital instrumentation and control systems. The FMEA approach is at the level of detail where data are available or at least potentially available, i.e., at a level of generic components. The proposed FMEA approach envisions a digital system as consisting of modules, each comprising common generic components, such as an analog/digital converter or a multiplexer. The failure modes of a generic component are defined in terms of their impact on the signal(s) carried by the component, and used to evaluate their impact on the module's input and output signals based on the component's interconnection in the module, that, in turn, determines the status of the entire system. This approach was applied to a digital feedwater control system (DFWCS), consisting of several modules that perform different functions. An automated FMEA tool was created based on the source code of the software and used to propagate failures through the system to determine the system status. The proposed approach is considered a generic one that can support the reliability modeling of any digital system, and can provide a practical solution to addressing the complexity of digital systems with the aid from the automated tool. It should be noted that the implementation of the FMEA approach described in this paper did not involve detailed analysis of software; instead, two generic software failure modes were included as placeholders in the DFWCS example.

### Application of Structured Treatment of Model Uncertainty in Complex Thermal-Hydraulics System Codes

Mohammad Pourgol-Mohamad(a), Ali Mosleh(b), and Mohammad Modarres(b)
*a) FM Global, Norwood MA, USA. b) University of Maryland, College Park MD, USA*

The integrated thermal-hydraulics uncertainty analysis (IMTHUA) methodology is developed for assessment of the uncertainties for applications to "best estimate" analyses of complex thermal hydraulics (TH) system codes [2]. The goal is to develop a comprehensive method to make such codes capable of supporting the uncertainty assessment with the ability to handle important accident transients. Model uncertainty is a relatively new topic of discussion in TH code calculations by its community, despite being often the major contributor to the overall uncertainty. The IMTHUA methodology considers the TH code structural uncertainties (generally known as model uncertainty) explicitly by treating internal sub-model uncertainties, and by propagating such model uncertainties in the code calculations, including uncertainties about input parameters. This paper presents more on systematic thermal-hydraulics application of IMTHUA methodology model uncertainty portion only. The objective is to demonstrate effectiveness and practicality of the methodology on complex thermal-hydraulics system codes calculations. Special attention is given for the techniques of thermal-hydraulics model uncertainty treatment and their application on some practical examples. These codes are an assembly of models and correlations for simulation of physical phenomena and behavior of system parameters in temporal domain. In some cases, there are alternative sub-models, or several different correlations for calculation of a specific phenomenon of interest. There are also "user options" for choosing one of several models or correlations in performing a specific code computation. Dynamic characteristics of TH

calculations add more complexity to the code calculation, meaning for example, that specific code models and correlations invoked are sequence-dependent, and based certain (dynamic) conditions being satisfied. Structural uncertainty assessment (model uncertainty) for a single model will be discussed by considering "correction factor", "bias" , and also through Bayesian sub-model output updating with available experimental evidence [3]. In case of multiple alternative models, several techniques including dynamic model switching, user controlled model selection, model mixing, will be discussed. Examples from different applications are provided for greater clarification of the model uncertainty treatment techniques.

1:30 - 3:00 PM

# 2-2: Dynamic Systems PSA

Session Chairs: Nathan Siu, Todd Paulos

## From Blind to Guided Simulation: Biased Monte Carlo Based on Entropy and Zero Variance for Dynamic PSA Applications

Jinghui Li(a,b), Ali Mosleh(b), and Rui Kang(a)
*a) Beihang University, Beijing, P.R.China. b) University of Maryland, College Park, U.S.A.*

This paper views PSA from the perspective of exploring a system's event sequence space and proposes a guided simulation methodology based on zero-variance importance sampling, aiming to improve the exploration efficiency and speed up the PSA simulation. It attempts to guide the simulation in the way such that: 1) all simulated event sequences end in system failure; 2) the failure event sequences are sampled in proportion to their natural probabilities. In order to achieve that, firstly we employ an event-tree-like chart of the failure domain of the event sequence space as a map to guide the simulation (the chart or map consists of the system's failure scenarios). Secondly, a preliminary simulation is run to obtain an approximation of the natural probabilities of the failure scenarios. And this is accomplished by guiding the simulation toward the failure scenarios and exploiting the concept of Shannon entropy to allocate simulation effort among them fairly. A widely discussed example (the holdup tank) is studied to test the effectiveness of this proposed methodology.

## Discretization Sensitivity Studies for Dynamic Event Tree Analyses

Kyle Metzroth, Richard Denning, and Tunc Aldemir
*The Ohio State University, Columbus, USA*

The ADAPT (Analysis of Dynamic Accident Progression Trees) software is a tool which can generate dynamic event trees (DETs) using a system simulation tool and a user-specified set of branching rules. The DETs which are generated by ADAPT are a type of discrete DETs. Discrete DETs only branch at specific points in the system state space (i.e., specific times or specific process conditions). Under the ADAPT methodology, the cumulative probability distributions for the failure of passive components or for the occurrence of phenomena (e.g.. pipe rupture, containment failure) are discretized and the physical values corresponding to the discrete probability values are used as branching conditions. Whenever discretization of an inherently continuous process is proposed in a methodology, the question of how fine of a discretization is necessary to capture all relevant information must be addressed, particularly for non-linear processes. Exploratory work is being performed to address this issue with the ADAPT methodology. An example case is analyzed using different probability distribution discretization schemes on a set of branching conditions.

3:30 - 5:00 PM

# 2-3: Nuclear Power Plant Level 2 PSA

Session Chairs: Dana Kelly, Jim Knudsen

## Treatment of Epistemic and Aleatoric Uncertainties for the Calculation of Branch Probabilities in PSA Level 2

Gerben Dirksen(a), Axel Hoeferb, and Eva-Maria Pauli(a)
*a) AREVA NP GmbH, Erlangen, Germany, b) AREVA NP GmbH, Offenbach, Germany*

This paper demonstrates a Bayesian approach to the modeling and calculation of branch probabilities in the framework of PSA Level 2. It is demonstrated how the difference between aleatoric uncertainties, due to variability of the accident progression, and epistemic uncertainties, due to limited knowledge, is directly integrated into the method of calculating branch probabilities. Monte- Carlo programs with two levels of iteration are used to calculate the branch probabilities and the distributions thereof. Examples for the physical phenomena induced RCS rupture and hydrogen combustion are used to demonstrate the method for actual PSA Level 2.

## Uncertainty Analysis of the Severe Accident for the Ulchin Unit 3&4 Nuclear Power Plant Considering the Natural Circulation Flow Phenomenon

Gunhyo Junga(a), Jinyoung Lee(a), Kwangil Ahn(b), and Sooyong Park(b)
*a) FNC Technology Co., Ltd., Seoul, Republic of Korea. b) Korea Atomic Energy Research Institute, Daejeon, Republic of Korea*

Probabilistic Safety Assessment (PSA) technology has been widely used to measure safety levels and identify weak points of nuclear power plants. But, it was pointed out that a structuring CET with phenomenological events was difficult and there were large uncertainties due to a lack of data used in an expert judgment and an expert judgment itself. So, in order to use PSA results to design and improve NPPs, and apply PSA results to decision making in NPPs, the quality of PSA results should be improved and uncertainties lied in PSA methodologies should be eliminated. Phenomenological uncertainty analysis to reduce level 2 PSA uncertainties using the MELCOR code is off the ground. First of all, MELCOR1.8.6 model of Ulchin unit 3&4 NPPs for the phenomenological uncertainty analysis considering the natural circulation flow has been developed. Especially, analysis of the creep rupture phenomenon of the reactor coolant system by the natural circulation flow after melting of the reactor core among the various severe accident phenomena was accomplished. For the detailed uncertainty analysis, Latin Hypercube Sampling methodology was applied to generate samples of probabilities of uncertainty source variables using the MELOR uncertainty engine. A number of MELCOR calculations were performed for various uncertainty source variables using the batch MELCOR program for convenience.

## Uncertainty Evaluation of Source Terms in Seismic Level-2 PSA in BWR Plant

Susumu Sumida, Kyoko Funayama and Mitsuhiro Kajimoto)
*Japan Nuclear Energy Safety Organization (JNES), Tokyo, Japan*

Japan Nuclear Energy Safety Organization (JNES) has been developing a methodology of Probabilistic Safety Analysis (PSA) for accident sequences that control the residual risk under the severe seismic condition. In the present study, uncertainties of source terms were analyzed based on sensitivity analyses for major parameters on source terms. Probability distributions of important parameters were decided by referring many conventional models and experimental studies. Uncertainty analyses of level-2 PSA for dominant accident sequences were performed by the MELCOR1.8.5 code with mechanistic models. As the results, average values of noble gas and volatile radionuclides were in good agreement with NUREG-1150. However, average values of non-volatile radionuclides were significant smaller than those of NUREG-1150 using the XSOR code with fast running parametric models. In the present study, uncertainty bound and special feature of source terms were obtained for major accident sequences under the severe seismic condition for the typical BWR plant.

## Using PSA to Develop a Tool for Rapid Source Term Prediction Based on Bayesian Belief Networks

Michael Knochenhauer(a) and Wiktor Frid(b)
*a) Scandpower – Lloyd's Register, Stockholm, Sweden. b) SSM, Swedish Radiation Safety Authority, Stockholm, Sweden*

This paper describes the outcome from the first phase of a project dealing with the development of a computerized tool for rapid source term prediction, RASTEP (RApid Source TErm Prediction). The tool will be tailored to the needs of the Swedish Radiation Protection Agency's (SSM) emergency preparedness organisation. The project will use as a starting point the outcome of the recently performed EU project STERPS [1] (Source Term Indicator Based on Plant Status). The STERPS project was part of the European Union 5th Euroatom Framework program, and had the objective to develop for trial use a tool for rapid and early diagnosis of plant status and estimation of likely environmental releases. The methodology is based on developing a plant model using the Bayesian Belief Network (BBN) methodology, making extensive use of PSA information. In the ongoing RASTEP project, the Swedish Radiation Safety Authority (SSM) aims at developing the pilot application from the EU project into a set of fully functional BBN models for all Swedish nuclear power plants. The basic aim of the project is to develop RASTEP as a tool for rapid source term prediction for practical use in severe accident situations, including interfaces to the LENA and ARGOS off-site dose calculation tools. The tool shall consider the specific needs of the SSM emergency organisation, including definition of the necessary administrative infrastructure. This includes the development of RASTEP with required functionality, including required user and program interfaces, and development of procedures for update and maintenance of the specific plant models in RASTEP.

### Quantification of Severe Accident Scenarios in Level 2 PSA of Nuclear Power Plant with Continuous Markov Chain Model and Monte Carlo Method

Satoshi Shinzaki, Akira Yamaguchi, And Takashi Takata
*Osaka University, Suita, Japan*

In a level 2 PSA (Probabilistic Safety Assessment), ET (Event Tree) and FT (Fault Tree) analysis methods are generally used for the quantification of the risk in events developing process. However, an interdependency of events and a direct coupling with a mechanistic analysis of physical process are not appropriately taken into consideration by the ET/FT methods. Hence, in the present study, the authors have proposed a new quantification method which can reflect thermal hydraulic response characteristic of nuclear power plant using Continuous Markov Chain Model and Monte Carlo (CMMC) method. Furthermore, a fast reactor model is developed and the effectiveness of the proposed method is shown through a sample analysis of loss-of-heat-sink (PLOHS) accident. It is concluded that the new method is able to quantify scenarios of the accident and promising to improve the accuracy of quantification of level 2 PSA.

# Human Reliability Analysis

**Monday, Salon C**

10:30 AM - Noon

## 5-1: International HRA Benchmark I

Session Chairs: John Forester, Ron Boring

### Lessons Learned on Benchmarking from the International Human Reliability Analysis Empirical Study

Ronald L. Boring(a), John A. Forester(b), Andreas Bye(c), Vinh N. Dang(d), Erasmia Lois(e)
*a) Idaho National Laboratory, Idaho Falls, Idaho, USA. b) Sandia National Laboratories, Albuquerque, New Mexico, USA. c) OECD Halden Reactor Project, Halden, Norway. d) Paul Scherrer Institute, Villigen PSI, Switzerland. e) U.S. Nuclear Regulatory Commission, Washington, DC, USA*

The International Human Reliability Analysis (HRA) Empirical Study is a comparative benchmark of the prediction of HRA methods to the performance of nuclear power plant crews in a control room simulator. There are a number of unique aspects to the present study that distinguish it from previous HRA benchmarks, most notably the emphasis on a method-to-data comparison instead of a method-to-method comparison. This paper reviews seven lessons learned about HRA benchmarking from conducting the study: (1) the dual purposes of the study afforded by joining another HRA study; (2) the importance of comparing not only quantitative but also qualitative aspects of HRA; (3) consideration of both negative and positive drivers on crew performance; (4) a relatively large sample size of crews; (5) the use of multiple methods and scenarios to provide a well-rounded view of HRA performance; (6) the importance of clearly defined human failure events; and (7) the use of a common comparison language to "translate" the results of different HRA methods. These seven lessons learned highlight how the present study can serve as a useful template for future benchmarking studies.

### The International HRA Empirical Study: Simulator Results From the Loss of Feedwater Scenarios

Helena Broberg(a), Salvatore Massaiu(a), Jeffrey Julius(b), and Bertil Johansson(a)
*a) OECD Halden Reactor Project, Halden, Norway. b) Scientech, Seattle, USA*

In the International HRA Empirical Study, Human Reliability Assessment (HRA) methods' predictions were compared to crew performances obtained at the Halden Man Machine Laboratory (HAMMLAB) PWR simulator. Ten licensed nuclear operation crews handled two versions of a Loss of Feedwater (LOFW) scenario, where the analyzed Human Failure Events (HFEs) related to starting Bleed and Feed (B&F). In the complicated version the crews were faced with conflicting indications for the Steam Generator (SG) levels and with the concurrent goal of establishing condensate flow to the SGs. For the purpose of comparison, the results are represented in terms of performance of the HFEs, the driving Performance Shaping Factors, and operational stories. In the base version, all crews established B&F before the SGs were empty. In the complex version, seven of the ten crews did not start B&F before empty SGs due to high complexity and poor indications of conditions. These crews established condensate flow, and started B&F within 25 minutes after empty SGs. The crews who started B&F before dryout, were facilitated by conditions caused by previous events or actions. The empirical results show the importance of situational dynamics (operator-plant and operator-operator interactions) for HFE outcomes in complex scenarios.

### Towards a Model of Procedure Following for Predictive Cognitive Task Analysis

Salvatore Massaiu
*OECD Halden Reactor Project, Halden, Norway*

Qualitative task analysis is a crucial aspect of Human Reliability Analysis (HRA). Yet, the guidance provided by most methods is not systematic and thorough enough to capture cognitive aspects of operators' response that have significant impact on performance outcomes. This paper presents initial work on a model of procedure following for characterizing the guidance system (i.e. emergency procedures, conduct of operations), its effects on crew cognition (i.e. control modes), and the expected performance difficulties. The explanatory power of the model is illustrated through an analysis of observed crew performance in an emergency scenario. The paper concludes that the modeling approach, which is inspired by notions from situated action theory and naturalistic decision making, is well suited for predictive cognitive task analysis of nuclear power plants emergency operating systems.

### Quantitative Results of the HRA Empirical Study and the Role of Quantitative Data in Benchmarking

Vinh N. Dang(a), Salvatore Massaiu(b), Andreas Bye(b), and John A. Forester(c)
*a) Paul Scherrer Institute, Villigen PSI, Switzerland. b) OECD Halden Reactor Project, Halden, Norway. c) Sandia National Laboratories, Albuquerque, USA*

In the International HRA Empirical Study, diverse Human Reliability Analysis (HRA) methods are assessed based on data from a dedicated simulator study, which examined the performance of licensed crews in nuclear power plant emergency scenarios. The HRA method assessments involve comparing the predictions obtained with the method with empirical reference data, in quantitative as well as qualitative terms. This paper discusses the assessment approach and criteria, the quantitative reference data, and the comparisons that use these data. Consistent with the expectations at the outset of the study, the statistical limitations of the data are a key issue. These limitations preclude concentrating solely on the failure counts defined by the Human Failure Event (HFE) success criteria and the failure probabilities based on these counts. In assessing quantitative predictive power, this study additionally uses a reference HFE difficulty (qualitative failure likelihood) ranking that accounts for qualitative observations in addition to the failure counts. Overall, the method assessment prioritizes qualitative comparisons, using the rich set of data collected on performance issues. Here, the quantitative predictions and data are used to determine the essential qualitative comparisons, demonstrating how quantitative and qualitative comparisons and criteria can be usefully combined in HRA method assessment.

1:30 - 3:00 PM

## 5-2: International HRA Benchmark II

Session Chairs: Vinh Dang, Helena Broberg

### Lessons Learned on Benchmarking from the International Human Reliability Analysis Empirical Study

J.A. Forester(a), E. Lois(b), V.N. Dang(c), A. Bye(d), G. Parry(b), and J. Julius(e)
*a) Sandia National Laboratories, Albuquerque, USA. b) U.S. Nuclear Regulatory Commission, Washington DC, USA. c) Paul Scherrer Institute, Villigen PSI, Switzerland. d) OECD Halden Reactor Project, Halden, Norway. e) Scientech, Seattle, USA*

In the International HRA Empirical Study, human reliability analysis (HRA) method predictions for human failure events (HFEs) in steam generator tube rupture and loss of feedwater scenarios were compared against the performance of real crews in a nuclear power plant control room simulator. The comparisons examined both the qualitative and quantitative HRA method predictions. This paper discusses some of the lessons learned about HRA methods that have been identified to date. General strengths and weaknesses of HRA methods are addressed, along with the reasons for any limitations in the predictive results produced by the methods. However, the discussions of the lessons learned in this paper must be considered a "snapshot." While most of the data has been analyzed, more detailed analysis of the results from specific HRA methods are ongoing and additional information may emerge.

### Application of ASEP/THERP in International HRA Empirical Study

Stacey M L Hendrickson(a), Y. James Chang(b), and C. R. Grantom(c)
*a) Sandia National Laboratories, Albuquerque, NM, USA. b) U.S. Nuclear Regulatory Commision, Rockville, MD, USA. c) Consultant, West Columbia, TX, USA*

A recent endeavor to study human reliability analysis (HRA) methods was undertaken to assess the strengths and weaknesses of multiple HRA methods and ultimately validate the underlying models. The International HRA Empirical Study proposed a series

of scenarios representing either a steam generator tube rupture (SGTR) or a loss of feedwater (LOFW) [1]. The human failure events (HFEs) developed to represent these situations corresponded to both nominal conditions in which the situation resembles one the crew would be expected to be well trained on and a complex condition in which the crew would be expected to struggle some in correctly interpreting the problem. One method assessed within the HRA Empirical Study was Accident Sequence Evaluation Program (ASEP) [2]. This paper presents the lessons learned from applying ASEP along with the Technique for Human Error Rate Prediction (THERP) [3] to the assessment of human error probabilities (HEPs) for the SGTR and LOFW scenarios. Although ASEP was the primary method applied, THERP was also used within the purview allowed through ASEP.

### Enhanced Bayesian THERP — Lessons learnt from HRA benchmarking

Jan-Erik Holmberg(a), Kent Bladh(b), Johanna Oxtrand(c), and Pekka Pyy(d)
*a) VTT, Espoo, Finland. b) Vattenfall Power Consultant, Malmö, Sweden. c) Ringhals AB, Väröbacka, Sweden. d) Teollisuuden Voima Oy, Helsinki, Finland*

The Enhanced Bayesian THERP (Technique for Human Reliability Analysis) method uses as its basis the time-reliability curve introduced in the Swain's human reliability analysis (HRA) handbook. It differs from the Swain's Handbook via a transparent adjustment of the time-dependent human error probabilities by use of five performance shaping factors (PSFs): (1) support from procedures, (2) support from training, (3) feedback from process, (4) need for co-ordination and communication, (5) mental load, decision burden. In order to better know the characteristics of the Enhanced Bayesian THERP from a more international perspective, the method has been subject to evaluation within the framework of the international "HRA Methods Empirical Study Using Simulator Data". Without knowledge of the crews' performances, several HRA analysis teams from different countries, using different methods, performed predictive analyses of four scenarios. This paper gives an overview of the method with major findings from the benchmarking. The empirical comparison gives confidence that the time reliability curve is a feasible and cost effective method to estimate human error probabilities when the time window is well defined and relatively short. The comparison of empirical observations with predictions was found as a useful exercise to identify areas of improvements in the HRA method.

### Lessons learned on HRA Benchmarking: the EDF point of view with MERMOS

Helene Pesme, Pierre Le Bot
*EDF R&D, Clamart, France*

EDF decided to participate in the HRA International Study launched in 2007 for two main aims: to make its MERMOS method more widely and practically understood and to learn about other Human Reliability Assessment methods. The lessons learned during this Benchmarking proved to be muchbroader. This paper presents our comments on the last phase of the Benchmark. It then focuses on the methodological developments at EDF for this last study case. It proved to be very interesting regarding the use of MERMOS without any data from simulator observations: this led us to specify more clearly the "MERMOS by delta" method which enables the use of detailed HFE analyses of EDF PSAs. Moreover, this method could be used for the future PSA of new reactors, for which no simulator data are available yet. Finally this paper will underline the lessons learned from the entire Benchmark, which proved to be a great opportunity for HRA experts to debate on relevant issues such as the models of accidents in HRA, the use of simulator data in HRA and data collection. Further exchanges are taking place within the HRA community thanks to this Benchmark.

3:30 - 5:00 PM

## 5-3: Resolving HRA Models Differences

Session Chairs: Ali Mosleh, John Forester

### A Model-Based Human Reliability Analysis Framework

Ali Mosleh(a), John A. Forester(b), Ronald L. Boring(c), Stacey M. L. Hendrickson(c), April M. Whaley(c), Song-Hua Shen(d), Dana L. Kelly(c), James Y.H. Chang(d), Vinh N. Dang(e), Johanna H. Oxstrand(f), Erasmia L. Lois(d)
*a) University of Maryland, College Park, MD, USA. b) Sandia National Laboratories, Albuquerque, NM, USA. c) Idaho National Laboratory, Idaho Falls, ID, USA. d) US Nuclear Regulatory Commission, Washington, DC, USA. e) Vinh N. Dang, Paul Scherrer Institute, Villigen PSI, Switzerland. f) Vattenfall Ringhals AB, Väröbacka, Sweden*

In response to a Staff Requirements Memorandum (SRM) to the Advisory Committee on Reactor Safeguards (ACRS), the US Nuclear Regulatory Commission (NRC) has undertaken a research effort to create a consensus approach to human reliability analysis (HRA). This paper provides an overview of the approach being developed. The approach introduces the "crew response tree" (CRT) concept, which depicts the human failure events in a manner parallel to the PRA event tree process, provides a structure for capturing the "context" associated with the human failure events under analysis, and uses the Information Processing Model as a platform to identify potential failures. It incorporates behavioral science knowledge by providing the decompositions of human failures/failure mechanisms/failure factors built from a top-down and bottom-up approach, the latter reflecting those findings from scientific papers that document theories and data of interest. The structure provides a roadmap for incorporating the phenomena with which crews would be dealing, the plant characteristics (e.g., design, indications, procedures, training), and human performance capabilities (awareness, decision, action). In terms of quantification, the approach uses the typical PRA conditional probability expression, which is delineated to a level adequate for associating the probability of a human failure event with conditional probabilities of the associated contexts, failure mechanisms, and the underlying factors (e.g., performance shaping factors). Such mathematical formulation can be used to directly estimate HEPs using various data sources (e.g., expert estimations, anchor values, simulator or historical data), or can be modified to interface with existing quantification approaches.

### Example Application of Model-Based HRA Approach

Song-Hua Shen(a), Ali Mosleh(b), Dana L. Kelly(c), Ronald L. Boring(c)
*a) US Nuclear Regulatory Commission, Washington, DC, USA. b) University of Maryland, College Park, MD, USA. c) Idaho National Laboratory, Idaho Falls, ID, USA*

In response to a Staff Requirements Memorandum (SRM) to the Advisory Committee on Reactor Safeguards (ACRS), the US Nuclear Regulatory Commission (NRC) has undertaken a research effort to create a consensus approach to human reliability analysis (HRA). The qualitative part of the approach includes a scenario-driven method of capturing possible interactions of the operating crew with the plant. At its top-layer, the method includes a Crew Response Tree (CRT) that identifies human failure events (HFEs). The potential failure mechanisms of the HFEs are explored with the aid of a mid-layer "causal model" using the Information-Diagnosis/Decision-Action (IDA) model and cognitive models from the psychological literature. The last layer of the model links relevant performance shaping factors (PSFs) to each failure mechanism. These layers together embody the results of task analysis and evaluation of context factors performed by an interdisciplinary team of analysts. In each scenario of the CRT, the mid-layer and bottom-layer models are linked together to produce the sequence of events and their causes that lead to one or several HFEs. Two companion papers in this conference proceedings describe the overall methodology and the development of the mid-layer models. This paper presents an illustrative application of the method.

### A Mid-Layer Model for Human Reliability Analysis: Understanding the Cognitive Causes of Human Failure Events

Stacey M. L. Hendrickson(a), April M. Whaley(b), Ronald L. Boring(b), James Y.H. Chang(c), Song-Hua Shen(c), Ali Mosleh(d), Johanna H. Oxstrand(e), John A. Forester(a), Dana L. Kelly(b)
*a) Sandia National Laboratories, Albuquerque, NM, USA. b) Idaho National Laboratory, Idaho Falls, ID, USA. c) US Nuclear Regulatory Commission, Washington, DC, USA. d) University of Maryland, College Park, MD, USA. e) Vattenfall Ringhals AB, Väröbacka, Sweden*

The Office of Nuclear Regulatory Research (RES) at the US Nuclear Regulatory Commission (USNRC) is sponsoring work in response to a Staff Requirements Memorandum (SRM) directing an effort to establish a single human reliability analysis (HRA) method for the agency or guidance for the use of multiple methods. As part of this effort an attempt to develop a comprehensive HRA qualitative approach is being pursued. This paper presents a draft of the method's middle layer, a part of the qualitative analysis phase that links failure mechanisms to performance shaping factors. Starting with a Crew Response Tree (CRT) that has identified human failure events, analysts identify potential failure mechanisms using the mid-layer model. The mid-layer model presented in this paper traces the identification of the failure mechanisms using the Information-Diagnosis/Decision-Action (IDA) model and cognitive models from the psychological literature. Each failure mechanism is grouped according to a phase of IDA. Under each phase of IDA, the cognitive models help identify the relevant performance shaping factors for the failure mechanism. The use of IDA and cognitive models can be traced through fault trees, which provide a detailed complement to the CRT.

### Developing a New HRA Quantification Approach from Best Methods and Practices

Vinh N. Dang(a), John A. Forester(b), Ali Mosleh(c)
*a) Paul Scherrer Institute, Villigen PSI, Switzerland. b) Sandia National Laboratories, Albuquerque, NM, USA. c) University of Maryland, College Park, MD, USA*

The Office of Nuclear Regulatory Research (RES) of the U.S. Nuclear Regulatory Commission is sponsoring work in response to a Staff Requirements Memorandum (SRM) directing an effort to establish a single human reliability analysis (HRA) method for the agency or guidance for the use of multiple methods. One motivation is the variability in Human Failure Event (HFE) probabilities estimated by different analysts

and methods. This work considers that a reduction of the variability in the HRA quantification outputs must address three sources: differences in the scope and implementation of qualitative analysis, the qualitative output-quantitative input interface, and the diversity of algorithms for estimating failure probabilities from these inputs. Two companion papers (Mosleh et al. and Hendrickson et al.) describe a proposed qualitative analysis approach The development of the corresponding quantification approach considers a number of alternatives including a module-based hybrid method and a data-driven quantification scheme. This paper presents on-going work and the views of the contributors.

# PSA Applications

**Monday, East Room**

10:30 AM - Noon

## 1-1: Loss of Offsite Power Risk

Session Chairs: Risto Himanen, Jim Chapman

### Best Practices for Treatment of LOOP in PRAs

Patrick Baranowsky, E.T. Burns, and Doug True
*ERIN Engineering and Research, Inc., Bethesda USA*

The accurate modeling of Loss of Offsite AC Power (LOOP) and possible Station Blackout (SBO) events in a probabilistic risk assessment (PRA) requires a broad and detailed treatment. Many areas of PRA are impacted. Accident sequences must be developed in a sufficiently rigorous fashion to satisfy regulatory application requirements. In addition, the ASME/ANS Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications includes a number of expectations regarding the treatment of LOOP and SBO. Due to the typically large contribution of LOOP to the risk profile, this issue was addressed as part of the Electric Power Research Institute's PRA scope and quality project. The objective was to define and provide guidance for industry best practices for the treatment of LOOP events in PRAs that conforms to the requirements of the ASME/ANS PRA standard. The best practices include: A breakdown of the accident sequence modeling areas, identification of applicable PRA standard high level and supplemental requirements, technical approaches and alternatives for satisfying the PRA standard and supporting references, and several examples and results of sensitivity analyses. This paper provides an overview and summary of some key elements of the technical analysis supporting the best practices.

### Proposed SPAR Modeling Method for Quantifying Time Dependent Station Blackout Cut Sets

John A. Schroeder, Robert F. Buell
*Idaho National Laboratory, Idaho Falls, USA*

The U.S. Nuclear Regulatory Commission's (USNRC's) Standardized Plant Analysis Risk (SPAR) models and industry risk models take similar approaches to analyzing the risk associated with loss of offsite power and station blackout (LOOP/SBO) events at nuclear reactor plants. In both SPAR models and industry models, core damage risk resulting from a LOOP/SBO event is analyzed using a combination of event trees and fault trees that produce cut sets that are, in turn, quantified to obtain a numerical estimate of the resulting core damage risk. A proposed SPAR method for quantifying the time-dependent cut sets is sometimes referred to as a convolution method. The SPAR method reflects assumptions about the timing of emergency diesel failures, the timing of subsequent attempts at emergency diesel repair, and the timing of core damage that may be different than those often used in industry models. This paper describes the proposed SPAR method.

### Simulation Model for the Frequency and Duration of LOOP: Applications in Risk Based Evaluations

Antti Tarkiainen and Risto Himanen
*Teollisuuden Voima Oyj, Eurajoki, Finland*

Loss of offsite power (LOOP) events have typically a major contribution to the estimated core damage frequencies of nuclear power plants (NPPs). Both the frequency and the duration of the LOOP events are crucial parameters for the calculation of the associated risks. This information can be estimated using statistics of occurred events, but the available database may be limited and such information is not best suited for the evaluation of the possible effects of planned modifications - both on the plant level and on the external power grid level. Therefore, the Finnish utility TVO has developed a simulation model to allow for the realistic estimation of both LOOP frequency and LOOP duration. During the past three years, this simulation model has laid the foundation for several risk based evaluations concerning plant modifications and plant maintenance, including the evaluation of recent plant modifications aimed to improve the NPP's ability to survive from undervoltage and overvoltage situations.

### Modeling the Increased Vulnerability to a Loss of Offsite Power Event

Ross C. Anderson(a), Christopher J. Sutton(b)
*a) Dominion, Richmond, VA USA, b) Dominion, Richmond, VA USA*

Switchyard maintenance is one of the activities that can increase the potential for a Loss of Offsite Power at a nuclear plant. The consequential Core Damage Frequency is also increased. Dominion has developed a method to more accurately model this vulnerability, as well as the potential vulnerability of other conditions such as grid instability or severe weather.

1:30 - 3:00 PM

## 1-2: Accident Precursor Analysis

Session Chairs: Gaspare Maggio, Frank Groen

### IRSN Accident Precursor Assessment Methodology and Examples of Application

N. Rodionova, C. Gagnier, G. Briday and J.-C. Valero
*IRSN, Fontenax-aux-Roses, France*

Having 58 PWR type reactors of standardized design in operation, ASN, the French Regulatory Authority deals with the important number of operational events reported by utility to regulator (about 70 per month). All reported events are screened and analysed by IRSN (Technical Support Organization for the French Regulatory Body) taking into account their significance to safety and risk of Nuclear Power Plant. The precursor assessment is a part of in-depth analysis process which is aimed at prioritizing the events, identifying the most important accident scenarios, which could lead to the unacceptable consequences (core damage or radioactive releases), help to define the root causes of the event and to recommend and prioritize the corrective measures. The paper presents the methodology for screening, selection and assessment of accident precursor events, as well as provides some examples of application. As an example of significant event, the precursor assessment of Blayais Unit 3 High Pressure Safety Injection System (HPSI) unavailability, dated of 25 of august 2008, is presented. During the periodical test performed before refuelling outage, the operator revealed the presence of boron plugs fully clogging needle valves on the two out of tree safety injection lines. The root cause investigation has shown several deficiencies related to HPSI motor operated valves reliability, periodical test execution and routing operational actions that resulted to boron crystallisation of injection lines for the period of four months. The estimated conditional core damage probability is 8,3 10-5. The main assumptions, quantitative results and sensitivity analysis are discussed.

### Precursor Event Program at EDF - Objectives, Method, Results and Insights

Jean Primet(a), Eddy Panato(b)
*a) Electricité de France, R&D Division, Clamart, France, b) Electricité de France, Nuclear Generation Division, St-Denis, France*

The precursor program was started by EDF in 1994. Since then, more than 600 reported operational events identified as Safety Outstanding Events have been analyzed whenever possible using probabilistic methods based on PSAs. Analysis provides an estimate of the remaining protections against core damage at the time the event occurred. Included in the frame of EDF national operating feedback process, event probabilistic analysis is mainly used to : - detect or confirm the most significant safety related operational event and help understand why they are significant; - give priorities in terms of treatment (in-depth analysis, emergency of feed-back corrective actions,); - provide indicators, among others, to assess EDF nuclear power plants operation safety level. EDF developed its own methodology starting from best international practices and taking into account some particularities. Analysis are currently limited to level 1 internal event PSA (at power and shutdown modes) and start with a selection process to screen among the numerous events occurring on EDF fleet. Main difficult methodological issues (common cause failure, human reliability assessment and partially unavailable or degraded components and systems,…) are addressed in order to achieve consistent treatment throughout all the analysis. Future methodological developments could include uncertainties treatment and PSA scope extension (fire, level 2) into the analysis method. Lessons learnt from the program are many and various. Statistical and qualitative analysis has shown that the operational safety level of EDF nuclear fleet significantly improved as far as the precursor analysis is concerned : this is mainly due to the reduction of transient and initiating events frequency and to many back-fitting measures and design improvements which were implemented on the units. Analysis of corrective measures efficiency also permitted to check that individual most significant events were treated appropriately. Additional insights concern recurrent precursors (which kind of transients or systems are involved periodically in precursor events) and enabled to identify potential generic weaknesses.

### An Accident Precursor Analysis Process Tailored for NASA Space Systems

Frank Groen, Michael Stamatelatos(a), Homayoon Dezfuli(a) and Gaspare Maggio(b)
*a) Office of Safety & Mission Assurance, NASA, Washington, D.C. USA. b) Technology Risk Management Operations, ISL, New York, NY USA*

Accident Precursor Analysis (APA) serves as the bridge between existing risk modeling activities, which are often based on historical or generic failure statistics, and system anomalies, which provide crucial information about the failure mechanisms that are actually operative in the system and which may differ in frequency or type from those in the various models. These discrepancies between the models (perceived risk) and the system (actual risk) provide the leading indication of an under-appreciated risk. This paper presents an APA process developed specifically for NASA Earth-to-Orbit space systems. The purpose of the process is to identify and characterize potential sources of system risk as evidenced by anomalous events which, although not necessarily presenting an immediate safety impact, may indicate that an unknown or insufficiently understood risk-significant condition exists in the system. Such anomalous events are considered accident precursors because they signal the potential for severe consequences that may occur in the future, due to causes that are discernible from their occurrence today. Their early identification allows them to be integrated into the overall system risk model used to inform decisions relating to safety.

### Development of NASA's Accident Precursor Analysis Process Through Application on the Space Shuttle Orbiter

Gaspare Maggio(a), Frank Groen(b), Teri Hamlin(c), Robert Youngblood(d)
*a) Technology Risk Management Operations, ISL, New York, NY. b) Office of Safety & Mission Assurance, NASA, Washington, D.C.. c) Space Shuttle Safety & Mission Assurance, NASA, Houston, TX. d) Risk, Reliability, and NRC Programs Department, Idaho National Laboratory, Idaho Falls, ID*

Accident Precursor Analysis (APA) serves as the bridge between existing risk modeling activities, which are often based on historical or generic failure statistics, and system anomalies, which provide crucial information about the failure mechanisms that are actually operative in the system. APA does more than simply track experience: it systematically evaluates experience, looking for under-appreciated risks that may warrant changes to design or operational practice. This paper presents the pilot application of the NASA APA process to Space Shuttle Orbiter systems. In this effort, the working sessions conducted at Johnson Space Center (JSC) piloted the APA process developed by Information Systems Laboratories (ISL) over the last two years under the auspices of NASA's Office of Safety & Mission Assurance, with the assistance of the Safety & Mission Assurance (S&MA) Shuttle & Exploration Analysis Branch. This process is built around facilitated working sessions involving diverse system experts. One important aspect of this particular APA process is its focus on understanding the physical mechanism responsible for an operational anomaly, followed by evaluation of the risk significance of the observed anomaly as well as consideration of generalizations of the underlying mechanism to other contexts. Model completeness will probably always be an issue, but this process tries to leverage operating experience to the extent possible in order to address completeness issues before a catastrophe occurs.

3:30 - 5:00 PM

## 1-3: Safety Margin Assessment

Session Chairs: Jeanne-Marie Lanore, Vinh Dang

### Assessing Safety Margins: The Impact of a Power Uprate on Risk from Small And Medium LOCA Scenarios

Vinh N. Dang, Tae-Wan Kim, Martin A. Zimmermann, and Annalisa Manera
*Paul Scherrer Institute, Villigen PSI, Switzerland*

The evaluation of proposed plant modifications combines deterministic safety analysis focusing on design basis accidents and Probabilistic Safety Analysis (PSA) for beyond-design basis scenarios. While deterministic acceptance criteria must be met before and after plant modifications, modifications do affect safety. This paper discusses a study performed to quantify this impact, within the frame of the Safety Margin Analysis and Application (SM2A) task. For a hypothetical 10% power uprate for a Pressurized Water Reactor, the study focuses on the Small and Medium Loss of Coolant Accident (SLOCA and MLOCA) scenarios. A reduction of bounding assumptions and the explicit treatment of uncertainties in the accident sequence thermal-hydraulic analyses are key aspects of the SM2A analyses, which use elements of ‚Äúbest estimate plus uncertainty‚Äù deterministic safety analysis. An explicit treatment of the distribution of the time to switch to recirculation mode is one of the main features of the MLOCA analysis. The results demonstrate that the SM2A methodology is capable of quantifying small changes in the core damage frequency (CDF), which the bounding approach in PSA might mask. In addition, they underscore a need to address aleatory uncertainties explicitly in some PSA accident sequence calculations.

### Impact on Safety Margins of a 10% Power Up-Rate for Zion NPP SBO Transient

F. Fouet, P. Probst, J.M. Lanore
*IRSN, Institut de Radioprotection et de Sûreté Nucléaire, Fontenay-Aux-Roses, France*

During the past years, nuclear power plants underwent some major changes in their design and operation mode to fulfil new objectives, such as power up-rate, life extension and/or increased fuel burn up. While fulfilling all the regulatory requirements, these changes ‚Äúnot necessarily and/or completely accounted for in the original design ‚Äù can challenge the plant safety margins and induce a potential increase of the risk. In order to assess the impact of such modifications on the safety margins, the Committee on the Safety of Nuclear Installations (CSNI) approved in December 2003 a Safety Margins Action Plan (SMAP) and established an international Working Group aimed at developing a new methodology to address the problem, which has been successfully done [NEA/CSNI/R(2007)9]. Then, the CSNI mandated a SM2A (Safety Margin, Assessment and Application) group to apply the SMAP methodology to a real case. A 10% power up-rate for Zion PWR has been selected as NPP modification and the increase of Core Damage Frequency (CDF) was selected as a metric for change in safety margin appraisal. A Probabilistic Safety Analysis ‚Äúbased (PSA) investigation phase, shared by the organisations participating in the group, was aimed at selecting the event trees and the main sequences, which the change could potentially affect in a significant way. It was agreed that, once the selection done, calculations had to be run to quantify the effects. The reference PSA for Zion NPP used in the exercise was performed in the framework of NUREG 1150. For the SM2A exercise it was agreed upon that the risk measure is CDF. IRSN was in charge of the LOSP event trees. In this family of events it appeared that 2 sequences correspond to the conditions (a potential effect with a non negligible probability). These 2 selected sequences were Station Black Out (SBO) scenarios: SBO with loss of Auxiliary Feed Water (AFW) and SBO with a seal Loss Of Coolant Accident (LOCA). This paper describes the PSA based sequences selection and the preparation of the input desks for CATHARE code, presents the assumptions of modelling, and discusses the numerical results for those two scenarios. The Peak Cladding Temperature (PCT) being the safety variable of interest, it appears that it is sensitive to the power increase only in the first scenario (SBO+AFW). For this case, an uncertainty analysis has been carried out, too, in order to assess the increase of CMF. Its main findings are discussed in the paper.

### Application of the Damage Domain Approach to the Calculation of Exceedance Frequencies

Javier Hortal(a), José M. Izquierdo(a), César Queral(b), And Luisa Ibañez(b)
*a) CSN (Nuclear Safety Council), Madrid, Spain. b) Technical University of Madrid (UPM), Madrid, Spain*

Exceedance frequencies of selected safety limits are used in the SMAP methodology as suitable risk indicators for the assessment of safety margins. Calculation of exceedance frequencies as proposed by SMAP is based on the consideration of the accident sequences composing the so called Risk Space, an extension of the classical PSA event trees. The contribution of each sequence to the exceedance frequency of a specified limit results from an uncertainty analysis, usually supported by the use of best estimate plant simulation codes. The Damage Domain approach is presented as an adequate method to perform the uncertainty analysis, especially suited for those sequences where some events occur at uncertain times. This approach has been proposed by CSN in the context of the application exercise SM2A and has been used to develop the analysis of selected scenarios of loss of Component Cooling and/or Service Water as a contribution of CSN to SM2A.

# External Events

**Monday, West Room**

10:30 AM - Noon

## 15-1: PRA I

Session Chairs: Ching Guey, Chris Rochon

### Fire PRA Walkdown Best Practices

Chris Rochon and Ashley Mossa
*Westinghouse Electric Company, LLC, Windsor, CT, U.S.*

There are several sets of plant walkdowns that need to be completed in support of a Fire PRA based on NUREG/CR-6850 [1] and ASME/ANS RA-Sa-2009 [2]. The purpose of this document is to support the performance of the most efficient Fire PRA

walkdowns possible. The best way to improve efficiency is to prepare far in advance, such that data supporting multiple tasks can be collected during very few walkdowns. This can help to maximize data accuracy as well as decrease the overall effort and time requirements of the walkdowns. In support of thorough walkdown planning and performance, this document also provides guidance on safety, planning (including guidelines for estimation of scheduling), preparation, the roles / responsibilities of each walkdown performer, and the walkdown process. Sample walkdown worksheets are provided. Key efficiencies and lessons include: 1) group similar walkdowns in order to complete walkdowns in fewer rounds, 2) plan to use certain items during the walkdowns which may eliminate the need for re-work (e.g., a camera, flashlight, and appropriate drawings), 3) the possible use of a portable electronic data entry device (such as a laptop computer), and 4) the collection of data in support of more detailed fire modeling.

### Development of Risk Assessment Method for Fires Caused by Earthquake (VI)

Takeshi Matsuoka(a), and Katsunori Ogura(b)
*a) Utsunomiya University, Utsunomiya City, Japan. b) Japan Nuclear Energy Safety Organization, Tokyo, Japan*

A concept and calculation formula is presented for the conditional occurrence probability of fire in case of earthquake. The median values of precursory phenomenon capacity for important components of nuclear power plants are calculated by the proposed formula and results are listed up. A method to quantify risk due to earthquake-induced fire is presented. The procedure of risk assessment for fires caused by Earthquake is explained with a flow chart. An analysis framework for the earthquake-induced fire PSA, which is now being developed, is explained.

### Fire PSA for French 1300 MWe PWR

Fabienne Nicoleau, Gabriel Georgescu, François Corenwinder
*Institute for Radiological Protection and Nuclear Safety (IRSN), Fontenay Aux Roses, France*

As part of the third decennial visit for the French 1300 MWe NPP, EDF will develop a Fire PSA. In order to dispose of its own tool, the IRSN is also developing a fire PSA for the PWR 1300 MWe. The methodology is similar with the one used for the 900 MWe Fire PSA, developed also by IRSN in the past. The study is an extension of the in-house developed 1300 MWe NPP Level 1 PSA for internal events. Several information exchanges were performed between EDF and IRSN during the development of the project. The EDF and IRSN studies are similar in scope; however the objectives and the main assumptions may be different. The IRSN study objectives are to provide an independent verification of the EDF study and also to allow the performance of further PSA applications in the frame of technical instruction of subsequent safety issues. To develop the 1300 MWe Fire PSA, IRSN also planned to do fire simulation with the SYLVIA code of IRSN (a two-zone fire model) in order to estimate the damage time of equipments and to investigate in R&D area, temperature criteria of damage of equipment and the impact of the smoke. The paper will present the ongoing fire PSA.

1:30 - 3:00 PM

## 15-2: Fire: PRA II

Session Chairs: P. Gauymer, Soli Khericha

### Using PSA to Verify Safe Shutdown Capability at Ringhals

Jonas Sevrell(a), Cilla Andersson(b), Jonas Nyström(b) and Ann Svenningsson(b)
*a) Risk Pilot AB, Malmö, Sweden. b) Ringhals AB, Varberg, Sweden*

In this paper an efficient method on how to perform a Safe Shutdown Analysis (SSA) after fire and pipe break is presented. The focus is on how to keep the SSA up to date and as an integral part of the ongoing safety analysis work at Ringhals. The starting point is a SSA performed by Westinghouse Electric at Ringhals, which has been further developed to meet the following objectives: - It should be possible to update the SSA with reasonable efforts. - The SSA should be traceable and possible to audit. - The SSA and PSA should use the same basic data. - The SSA document structure should be consistent with the PSA document structure. To reach those objectives have the following measures have been taken: - The SSA is integrated into the current PSA-model. - The electrical dependencies were mapped and modeled in the PSA-model. - The cable routes were mapped in detail. - Fault Tree (FT) Analysis Cases were implemented representing each area event.

### Fire Risk Assessment of a Large Passenger Ship using Computer Simulation

Beom Jin Park, Jin Choi, Heejin Kang, and Dongkon Lee
*Maritime & Ocean Engineering Research Institute, Daejeon, Republic of Korea*

Fire accidents tend to cause larger damage to ships than other type of accidents, despite the fact that fire accidents account for 10% of total ship accidents. Therefore, in any safety regulations, prevention and mitigation of fire accidents are considered with high emphasis. In this paper, fire risk analysis of a large passenger ship is performed. Event tree is used to model fire scenarios considering the effect of fire detection and fire suppression. Then the design fire scenarios that need further study are selected from preliminary fire simulation results using zone model fire simulation and expert review. Field model fire simulation software is used to calculate the consequence of each selected design fire scenario door, windows and ventilation systems.

### Detailed Fire Modeling Sensitivity and Uncertainty Analysis

Michael D Wright
*Jacobsen Engineering Ltd., Holmes Chapel, UK*

The purpose of this paper is to demonstrate the use of the Monte Carlo (MC) simulation code Crystal Ball© for detailed fire modeling, using a typical fire compartment as an example. The methodology is used to derive fire damage state probabilities, CDF and LERF for this compartment and to quantify the uncertainty and sensitivity of the results to uncertainties in the input parameters in accordance with Task 15 of NUREG/CR-6850. The scope of this paper is to: • describe how the Monte Carlo simulation technique can be used for detailed fire modeling, sensitivity analysis and uncertainty analysis • review and characterize the uncertainties associated with detailed fire modeling • demonstrate the application of the technique using a specific example and compare the results with point estimates • present the results of the sensitivity analysis and uncertainty analysis for this specific case

3:30 - 5:00 PM

## 15-3: Fire: Modeling and Uncertainty Analysis

Session Chairs: Steven Nowlen, J. LiPaper Number

### Methodology for Fire PSA during Design Process

Heiko Kollasko(a) and Joerg Blombach(b)
*a) AREVA NP GmbH, Erlangen, Germany. b) Consultant, Herzogenaurach, Germany*

Fire PSA is an essential part of a full scope level 1 PSA. The objective of the fire PSA is to identify fire-related event sequences relevant to safety, and to quantify their contribution to core damage frequency. This involves e.g. the identification of potential fire hazards, the identification of relevant fire areas, the assessment of fire initiating event frequencies, the characterization of fire-induced event sequences and quantification of the selected fire scenarios. Hence, the contribution of internal fires to the core damage frequency shall be determined. The scope of the probabilistic fire analysis is limited to fires that are initiated from fire sources within the plant. Internal fires are analyzed for power states and shutdown states considering all areas within the plant boundary where a fire may lead to a core damage sequence. During the design of a nuclear power plant not all information usually needed for a detailed fire PSA is available. Cable fires play an important role in fire PSA. However, especially cable routing is not yet finally planned. PSA including fire PSA shall be performed already during the design phase to provide probabilistic insights for the design. A fire PSA may be requested as well for licensing purposes. Therefore a methodology has been developed – and already been applied successfully – which makes use of the strict divisional separation of redundancies in the design of modern nuclear power plants and does not need the detailed cable routing within the divisions but uses conservative bounding assumptions that all equipment fails due a fire in the concerned division. Critical fire areas where components belonging to different division may be affected by a fire are identified and analysed. For the determination of fire frequencies a component based approach is proposed. The resulting core damage frequencies due to fire are conservative.

### Summary of GEH Authored Fire PRA Frequently Asked Questions

Dennis Henneke, Yunlong Li, and Matthew Warner
*GE Hitachi Nuclear Energy, Wilmington, NC, USA*

A number of National Fire Protection Association (NFPA) Standard 805 Frequently Asked Questions (FAQs) affecting Fire Probabilistic Risk Assessment (FPRA) have been generated and subsequently responded by GE Hitachi Nuclear Energy (GEH) FPRA personnel. These FAQs (08-43, 08-47, 08-50 through 52 and a new unnum-

bered FAQ) refine the state-of-the-art FPRA methodology in NUREG/CR-6850 and provide additional guidance for FPRA practitioners to readily apply, which greatly reduce the modeling uncertainties and result in more realistic FPRA models. FAQ 08-43 provides clarification of NUREG/CR-6850 (EPRI 1011989) guidance on the location of fires within electrical cabinets. FAQ 08-50 provides clarifying and revised guidance for the estimation of the probability of non-suppression. FAQ 08-51 recommends a method for determining hot short durations. FAQ 08-52 provides additional guidance on the fire growth rate for transient fires within the plant and the treatment of transient fires within the control room. A new unnumbered FAQ provides additional guidance on the treatment of fire propagation in electrical cabinets.

### Limitations Imposed on Fire PRA Methods as the Result of Incomplete and Uncertain Fire Event Data

Nowlen, Steven P(a) and Hyslop, J.S.(b)
*GE Hitachi Nuclear Energy, Wilmington, NC, USA*

Fire probabilistic risk assessment (PRA) methods utilize data and insights gained from actual fire events in a variety of ways. For example, fire occurrence frequencies, manual fire fighting effectiveness and timing, and the distribution of fire events by fire source and plant location are all based directly on the historical experience base. Other factors are either derived indirectly or supported qualitatively based on insights from the event data. These factors include the general nature and intensity of plant fires, insights into operator performance, and insights into fire growth and damage behaviors. This paper will discuss the potential methodology improvements that could be realized if more complete fire event reporting information were available. Areas that could benefit from more complete event reporting that will be discussed in the paper include fire event frequency analysis, analysis of fire detection and suppression system performance including incipient detection systems, analysis of manual fire fighting performance, treatment of fire growth from incipient stages to fully-involved fires, operator response to fire events, the impact of smoke on plant operations and equipment, and the impact of fire-induced cable failures on plant electrical circuits.

# Safety Culture & Organizational Factors

**Monday, North Room**

10:30 AM - Noon

## 9-1: Socio-technical Modeling I

Session Chair: Zahra Mohaghegh

### Development of an Aviation Safety Causal Model Using Socio-Technical Risk Analysis (SoTeRiA)

Zahra Mohaghegh
*Center for Risk and Reliability, University of Maryland, College Park, Maryland, USA*

In the wake of several highly-publicized aviation accidents in the past ten years, the use of Probabilistic Risk Analysis (PRA) for safety-related operational and design decisions has gained significant momentum and acceptance in civil aviation. Research studies in the field of aviation have highlighted some of the contributing factors of accidents, but there is no comprehensive model tracing the paths of influence starting from the root organizational factors up to the accidents and/or incidents. This paper uses a framework called Socio-Technical Risk Analysis (SoTeRiA), which is an extension of PRA, in order to develop a safety causal model for air carrier maintenance. The proposed aviation safety causal model covers a broad range of influencing factors including the physical and human aspects of the systems as well as their organizational and regulatory environments. This resulting model, through proper integration with models of the technical systems, will help manage risks proactively, based on leading indicators in the safety-related practices of the organization, and relevant regulatory activities and oversight.

### Bridging the Gap between Human Judgment and Automated Reasoning in Predictive Analytics

Antonio P. Sanfilippo, Roderick M. Riensche, Stephen D. Unwin, Jodi P. Amaya
*Pacific Northwest National Laboratory, Richland, WA, USA*

Events occur daily that impact the health, security and sustainable growth of our society. If we are to address the challenges that emerge from these events, anticipatory reasoning has to become an everyday activity. Strong advances have been made in using integrated modeling for analysis and decision making. However, a wider impact of predictive analytics is currently hindered by the lack of systematic methods for integrating predictive inferences from computer models with human judgment. In this paper, we present a predictive analytics approach that supports anticipatory analysis and decision-making through a concerted reasoning effort that interleaves human judgment and automated inferences. We describe a systematic methodology for integrating modeling algorithms within a serious gaming environment in which role-playing by human agents provides updates to model nodes and the ensuing model outcomes in turn influence the behavior of the human players. The approach ensures a strong functional partnership between human players and computer models while maintaining a high degree of independence and greatly facilitating the connection between model and game structures.

### Why are Organizational Risk Models so Insensitive?

Paolo Trucco(a), Chiara Leva(b)
*a) Politecnico di Milano, Milan, Italy. b) Trinity College Dublin, Ireland*

Several research projects and programs on system safety engineering and Quantitative Risk Analysis in the last 40 years offered very strong evidences of the crucial role that human and organizational factors (HOFs) play in major accidents. According to this increasing concern toward the relevance of HOFs in limiting safety performance of complex socio-technical systems, considerable research effort has been spent worldwide in the last couple of decades. This resulted in a quite rich literature covering from theoretical bases, to accident investigation methods and application to major disasters, to very sophisticated modeling approaches and techniques of HOFs in Quantitative Risk Analysis. Nevertheless, many of the models and applications described in scientific literature demonstrate very limited sensitivity of the accident event probability to the variation of single or multiple HOFs, or an “often obfuscating numerology”[1]. The paper proposes a critical review of the literature on the modeling strategies and techniques of HOFs, in order to point out major current limitations and to partially explain the argued limited sensitivity of these models. Finally, the paper explores five different critical investigation topics as likely origins of the limitations suffered, offering suggestions on additional research questions and methods able to provide further insight.

1:30 - 3:00 PM

## 9-2: Assessing Safety Culture Data

Session Chairs: Bill Nelson, Tracy Dillinger

### How Do Safety Culture Assessments Relate to Objective Operational Safety Performance?

Joan Devine and Sherry Borener
*Federal Aviation Administration, Washington, DC, USA*

Like any other instrument—an altimeter, a barometer, a radar, etc.—reliable safety measurement tools and metrics provide highly valuable input to decision makers at every level of an organization. Advances in the ability to capture and analyze operator and aircraft performance data and airspace operational information, as well as organizational and human performance information, have significantly improved our understanding of real-world operations. However, the bulk of our operational and event data, the use of which helps to identify the potential for incidents and accidents before they occur, is analyzed independently of the organizational data collected to evaluate operating norms and assess perceptions of safety climate. Our research question is, How does safety culture relate to objective operational safety outcomes? This study describes a methodology, provides results from a test case, and relates safety indicators from publicly available reports to a single safety culture intervention (i.e, a safety climate survey). The study identifies a safety culture metric, pre- and post-study baseline safety metrics, and a statistical relationship between the two measures.

### Predicting Rare Events

Romney B. Duffey
*Atomic Energy of Canada Limited, Chalk River, ON, Canada*

Rare events are widely misunderstood, as they may be previously unobserved, and are called “unknown unknowns”, “black swans”, or “fat tails”. We already know from the world’s event data that standard statistical distributions for probability and frequency of occurrence do not work for rare events (c.f. the case of “zero failures”), simply because the impact of learning, forgetting, randomness, risk exposure and experience are not properly accounted for. Accidental or seemingly random outcomes all share the human involvement, and are due in large part to human mistakes coupled with problems in system design, maintenance, and management. Rare events pose a special problem, as we may have limited or no prior data, and hence highly uncertain event, failure or outcome rates. In this paper, we provide a new means and method to predict the future (posterior) probability of such rare events based on the extreme case of insufficient learning, as expected for events that have not occurred often. We compare the predictions against data for rare events, and establish the uncertainties as an explicit function of the future risk exposure.

### Mining Behavior-Based Safety Data to Predict Safety Performance

Jeffrey C. Joe
*Idaho National Laboratory, Idaho Falls, USA*

The Idaho National Laboratory (INL) has implemented a behavior-based safety program called Safety Observations Achieve Results (SOAR). SOAR encourages employees to perform infield observations of each other's behaviors, and unlike other observation programs, emphasizes positive reinforcement for safe behaviors observed. In addition, SOAR encourages observers to correct, if needed, their co-worker's work practices and habits (i.e., behaviors). The underlying premise of correcting co-worker's "at-risk" behaviors is that more serious adverse safety events (e.g., OSHA-recordable events) are prevented from occurring because these lower level "at risk" behaviors are identified and corrected before they can propagate into culturally accepted unsafe behaviors that result in injuries or fatalities. While this premise is widely accepted across various hazardous industries, it has not been empirically evaluated thoroughly. The INL now has a significant amount of SOAR data on these lower level "at risk" behaviors. This paper describes the use of data mining and inferential statistical techniques to analyze these data to determine whether they can predict the occurrence of a more serious adverse safety event.

3:30 - 5:00 PM

## 9-3: Safety Culture Methodologies & Applications

Session Chairs: Zahra Mohaghegh

### Safety Culture Change in Two Companies

A.R. Hale(a), J. Jacobs(b) and M. Oor(c)
*a) Delft University of Technology, Delft, Netherlands & Hastam, Maldon, UK. b) Jacobs Safety Management, Veghel, Netherlands. c) Stichting Consument en Veiligheid, Amsterdam, Netherlands*

As part of an initiative of the Dutch Ministry of Social Affairs and Employment an evaluation study was undertaken in 17 companies undertaking safety interventions to improve safety performance through changes to safety culture and management. Overall results of the evaluation of all 17 interventions [2, 3] showed that dialogue with employees about safe working, top management support and a charismatic, creative and persistent coordinator of the project were characteristics of the successes when compared to the failures. One of these initiatives, in a reinforced concrete element construction company, appeared to be particularly effective according to the available outcome and intermediate measures. It had these three characteristics alongside a number of others. This paper describes the intervention, indicating how broad-ranging it was in the changes made. Its major elements involved workers and first line supervision much more in the detection, reporting and decision making about ways to remove the hazards. There was also a major emphasis on altering risk perceptions through risk awareness workshops. The performance data available for this study consisted of injury data covering the three years before and the four years after the start of the intervention, together with data from systematic observations of behaviour. The improvements in behaviour, safety climate and the decrease in injuries were highly significant. The paper contrasts this with an intervention in a fork-lift truck maker, which shows many of the same intervention elements, but has only some of the positive changes, with the main reduction of injuries occurring before the main interventions were introduced.

### Safety Culture and Safety Leadership: The Way Forward

Kathryn Mearns
*Industrial Psychology Research Centre, University of Aberdeen, Aberdeen, UK*

Despite the conceptual ambiguity surrounding both safety climate and culture, dimensions relating to 'management commitment to safety' have often emerged as the most powerful predictors of safety performance (Flin et al., 2000). Schein (2004) has argued that leaders determine the culture of an organization and leadership (both safety specific and general) shows a positive relationship with safety climate (Barling, Loughlin, & Kelloway, 2002; Zohar, 2002). The question remains as to what type of leadership is most effective and whether leaders at different levels require different styles to reinforce and encourage safety-related behaviours. Most safety research has focused on supervisory level leadership using the Transactional/Transformational model (Flin & Yule, 2004) or Leader- Member Exchange (Hofmann & Morgesen, 1999), although recent work is starting to focus on the Authentic Leadership Model (Avolio & Gardner, 2005) and how characteristics of authentic leaders can influence safety culture, climate and safety performance (Reid et al., 2008; Roger, 2009). Authentic Leadership seems to be particularly important because it reflects characteristics of trust, which Reason (1997) believed was the cornerstone of safety culture. Trust is required to create a reporting culture where employees are willing to report incidents without fear of unjustified reprisals so that the organization can learn from these incidents and prevent them from occurring again in the future. The current paper will explore the safety leadership, culture, climate, performance relationship and will debate the possible mechanisms behind this relationship.

### Development of an Aviation-Wide Safety Culture Assessment Tool

Balk, A.D., Montijn, C.
*Air Transport Safety Institute- Dutch Aerospace Laboratory, Amsterdam, Netherlands*

In order to assist organisations in the aviation industry with the assessment and management of their safety culture, the Air Transport Safety Institute has conducted a scientific review of the main existing and emerging safety culture frameworks. The findings of this review have been used to develop a safety culture framework founded on the common key elements of the various models. Based on this framework, a safety culture assessment tool has been developed: the Aviation Safety Culture Inquiry tool (ASC-IT). ASC-IT can be applied to all categories of organisations in the aviation industry. ASC-IT is applied in the form of web- or paper-based surveys to various organisational levels. Results are presented on the overall organisational level, but also on detailed level and for each target group in order to identify opportunities for improvement. ASC-IT provides a capability for benchmarking against similar organisations or other sectors within the aviation industry. Experience gained in the application of the framework in the airline, airport, maintenance and ground handling environment are summarized in the paper.

# Space and Aviation

**Monday, Municipal**

10:30 AM - Noon

## 12-1: Space Shuttle PRA Applications

Session Chairs: Roger L. Boyer, Gaspare Maggio

### Hubble Space Telescope Crew Rescue Analysis

Teri L. Hamlin(a), Michael A. Canga(a), and Grant R. Cates(b)
*a) National Aeronautics and Space Administration (NASA), Houston, USA. b) Science Applications International Corporation (SAIC), McLean, USA*

In the aftermath of the 2003 Columbia accident, NASA removed the Hubble Space Telescope (HST) Servicing Mission 4 (SM4) from the Space Shuttle manifest. Reasons cited included concerns that the risk of flying the mission would be too high. The HST SM4 was subsequently reinstated and flown as Space Transportation System (STS)-125 because of improvements in the ascent debris environment, the development of techniques for astronauts to perform on orbit repairs to damaged thermal protection, and the development of a strategy to provide a viable crew rescue capability. However, leading up to the launch of STS-125, the viability of the HST crew rescue capability was a recurring topic. For STS-125, there was a limited amount of time available to perform a crew rescue due to limited consumables (power, oxygen, etc.) available on the Orbiter. The success of crew rescue depended upon several factors, including when a problem was identified; when and what actions, such as powering down, were begun to conserve consumables; and where the Launch on Need (LON) vehicle was in its ground processing cycle. Crew rescue success also needed to be weighed against preserving the Orbiter's ability to have a landing option in case there was a problem with the LON vehicle. This paper focuses on quantifying the HST mission loss of crew rescue capability using Shuttle historical data and various power down strategies. Results from this effort supported NASA's decision to proceed with STS-125, which was successfully completed on May 24th 2009.

### 2009 Space Shuttle Probabilistic Risk Assessment Overview

Teri L. Hamlin(a), Michael A. Canga(a), Roger L. Boyer(a), and Eric B. Thigpen(b)
*a) National Aeronautics and Space Administration (NASA), Houston, USA. b) Science Applications International Corporation (SAIC), Houston, USA*

Loss of a Space Shuttle during flight has severe consequences, including loss of a significant national asset; loss of national confidence and pride; and, most importantly, loss of human life. The Shuttle Probabilistic Risk Assessment (SPRA) is used to identify risk contributors and their significance; thus, assisting management in determining how to reduce risk. In 2006, an overview of the SPRA Iteration 2.1 was presented at PSAM 8 [1]. Like all successful PRAs, the SPRA is a living PRA and has undergone revisions since PSAM 8. The latest revision to the SPRA is Iteration 3.1, and it will not be the last as the Shuttle program progresses and more is learned. This paper discusses the SPRA scope, overall methodology, and results, as well as provides risk insights. The scope, assumptions, uncertainties, and limitations of this assessment

provide riskinformed perspective to aid management's decision-making process. In addition, this paper compares the Iteration 3.1 analysis and results to the Iteration 2.1 analysis and results presented at PSAM 8.

### Extravehicular Activity Probabilistic Risk Assessment Overview for Thermal Protection System Repair on the Hubble Space Telescope Servicing Mission

Mark Bigler(a), Ed Roeschel(a), Michael Canga(a), Gary Duncan(b)
*a) National Aeronautics and Space Administration (NASA), Houston, USA. b) Science Applications International Corporation (SAIC), Houston, USA*

Following the Columbia accident in 2003, NASA developed repair techniques for the Thermal Protection System (TPS) as well as crew rescue capability to reduce risk to future flights from ascent debris and/or Micrometeoroid and Orbital debris (MMOD). For the Hubble Space Telescope (HST) Servicing Mission, the crew rescue capability was limited by the inability to safe haven on the International Space Station (ISS), resulting in a greater reliance on the repair capability. Therefore, NASA management wanted a better idea of the risk associated with repairing the TPS, since the repair would have to be conducted using Extravehicular Activity (EVA). NASA Safety and Mission Assurance (S&MA) developed an integrated EVA risk model to assess the risks associated with an EVA to support NASA management in the Space Shuttle Program (SSP) when making riskinformed decisions. This paper provides an overview of the EVA risk model that was developed to support the HST Servicing Mission in the event of TPS damage.

### Estimating the Reliability of a Soyuz Spacecraft Mission

Steven J. Farnham II(a), Warren C. Grant(a), and Michael G. Lutomski(b)
*a) ARES Corporation, Houston, TX USA. b) NASA-JSC, Houston, TX*

Once the US Space Shuttle retires in 2010, the Russian Soyuz Launcher and Soyuz Spacecraft will comprise the only means for crew transportation to and from the International Space Station (ISS). The U.S. Government and NASA have contracted for crew transportation services to the ISS with Russia. The resulting implications for the US space program including issues such as astronaut safety must be carefully considered. Are the astronauts and cosmonauts safer on the Soyuz than the Space Shuttle system? Is the Soyuz launch system more robust than the Space Shuttle? Is it safer to continue to fly the 30 year old Shuttle fleet for crew transportation and cargo resupply than the Soyuz? Should we extend the life of the Shuttle Program? How does the development of the Orion/Ares crew transportation system affect these decisions? The Soyuz launcher has been in operation for over 40 years. There have been only two loss of life incidents and two loss of mission incidents. Given that the most recent incident took place in 1983, how do we determine current reliability of the system? Do failures of unmanned Soyuz rockets impact the reliability of the currently operational man-rated launcher? Does the Soyuz exhibit characteristics that demonstrate reliability growth and how would that be reflected in future estimates of success?

1:30 - 3:00 PM

## 12-2: Aircraft Safety

Session Chairs: Curtis Smith

### Proposing Safety Performance Indicators for Helicopter Offshore on the Norwegian Continental Shelf

Ivonne A. Herrera(a), Erik Hollnagel(b) and Solfrid Håbrekke(a)
*a) SINTEF Technology and Society, Safety Research, Trondheim, Norway. b) MINES ParisTech, Sophia Antipolis, France*

Over last 10-years period there has been just one helicopter accident (with no fatalities) in the Norwegian sector of helicopter offshore operations. In this case, safety monitoring cannot be based on the absence of accidents. The main objective of this paper is to suggest a combination of leading and lagging indicators to monitor safety performance for helicopter offshore operations. An approach is described to identify indicators using different perspectives: a Risk Influence Model, the Functional Resonance Analysis Method (FRAM), and lessons learned from previous studies. The approach uses accident and incident data, as well as normal operations (when nothing goes wrong). The suggested indicators were evaluated through observations and interviews/workshop with helicopter operators, air traffic controllers, helicopter deck operators and regulators. The paper discusses the approach and proposes a set of domain specific safety performance indicators. The work was carried out under the Norwegian Helicopter Safety Study 3 (HSS-3).

### Risk Change and Contributions to Risk in Offshore Helicopter Traffic on the Norwegian Continental Shelf

Tony Kråkenes and Solfrid Håbrekke
*SINTEF Technology and Society, Safety Research, Trondheim, Norway*

The Helicopter Safety Study 3 (HSS-3) is a joint industry project funded by major oil and gas companies operating on the NCS. HSS-3 addresses risk to personnel traveling with helicopter on the Norwegian Continental Shelf (NCS). The time period studied is mainly 1999–2009, but the study also makes predictions for the coming decade (2010–2019). This paper documents main results from HSS-3 pertaining to the quantification of risk in two ways. First, we quantify risk change during and between the study periods. Second, we assess the relative contributions to the risk from three "classes" of contributors: 1) Accident categories; 2) Risk influencing Factors (RIFs) for accident frequency; 3) RIFs for accident consequence. A risk influence model based on RIFs and accident categories is described. This model has been used extensively in combination with statistical data and expert judgment to produce the study results. Results show that the estimated risk reduction during the time period 1999–2009 is 20 %, while the estimated risk reduction in the next decade (2010–2019) is 27 %.

### Modelling and Identification of Take - off Aircraft Operation

Anna Wieslawa Stelmach
*Dept. Air Transport Engineering – Faculty of Transport, Warsaw University of Technology, Warsaw, Poland*

While observing the dynamic increase in the intensity of the air traffic, the issue of constant controlling and monitoring every individual operation carried out during the flight process becomes a vital matter. One of the most significant operations in this process is the aircraft's take-off procedure. On the airports such procedures are observed quite frequently, with a rate of several dozen seconds up to few minutes. The correctness of carrying out the mentioned guidelines has a crucial impact on the traffic capacity of the runway, number of operations completed within the area of the airport and, above all, safety of the passengers. The research and analysis of these processes cannot, for obvious reasons, be done on objects in real conditions. Therefore, there is a tendency to use IT tools and methods for the purpose of the analysis of the operations which occur in the area of the airport. In order to make use of the computer simulation it is essential to have mathematical models of these operations. The take-off operation consists of the following stages: take-off run of the aircraft, take-off, acceleration and ascend. These operations are described in a special instruction (procedure)[1,2] of conduct for every stage, however their real course always differs from the required one. This is an obvious fact but in extreme cases may lead to threats in the traffic safety. The purpose of this article is to create models for particular stages of the take-off operation and to identify elementary models of these stages basing on parameters recorded by the board flight recorder. The created mathematical and computer models (for simulation research), reproducing the aircraft's real operations in the area of the airport, shall be used for automatization of the operations conducted in the airport's area. The automatization process might possibly increase the traffic capacity of the runway and, unquestionably, would contribute to the improvement of the passengers' safety.

3:30 - 5:00 PM

## 12-3: Space Launch Vehicle Risk Assessments

Session Chairs: Gaspare Maggio

### Physical Drivers in Launch Vehicle Failures

Rosalind Beckwith(a), Susie Go(b), and Donovan Mathias(b)
*a) Eloret Corporation, USA. b) NASA Ames Research Center, Moffet Field, USA*

This paper presents a summary of root causes and cascades leading to launch vehicle failures. Historical trends motivate the need to develop more sophisticated models for relevant system failure interactions rather than relying on baseline component reliability analysis. Launch vehicle failures from 1958 have been categorized, first by briefly examining failure cascades from initiating to manifesting subsystem. This exposes how failures transfer from one subsystem to another until final failure. Failures are also categorized by physical driver: design, process or weather. Failures stemming from design choices are of particular interest because they are brought about through system behaviors that could have been exposed or prevented through more rigorous testing and analysis. Examples from each type of specific physical trigger for both design and process failures are presented in summary form.

### Sensitivity Analysis of Launch Vehicle Debris Risk Model

Ken Geea and Scott L. Lawrence
*NASA Ames Research Center, Moffett Field, CA, USA*

As part of an analysis of the loss of crew risk associated with an ascent abort system for a manned launch vehicle, a model was developed to predict the impact risk of the debris resulting from an explosion of the launch vehicle on the crew module. The model consisted of a debris catalog describing the number, size and imparted velocity of each piece of debris, a method to compute the trajectories of the debris and a method to calculate the impact risk given the abort trajectory of the crew module. The model provided a point estimate of the strike probability as a function of the debris catalog, the time of abort and the delay time between the abort and destruction of the launch vehicle. A study was conducted to determine the sensitivity of the strike probability to the various model input parameters and to develop a response surface model for use in the sensitivity analysis of the overall ascent abort risk model. The results of the sensitivity analysis and the response surface model are presented in this paper.

### Role of Simulation Assisted Risk Assessment in Abort Trigger Recommendations

T. Manning(a), S. Lawrence(a), D. Mathias(a), H. Nejad(b), K. Geea, B. Ramamurthy(c), and P. Gage(d)
*a) NASA Ames Research Center, Moffett Field, California, USA. b) Eloret Corporation, Sunnyvale, California, USA. c) Valador Inc., Palo Alto, California, USA. d) Neerim Corporation, Palo Alto, California, USA*

A physics-based, simulation-assisted risk assessment of a crewed launch vehicle is used to evaluate the efficacy of failure detection mechanisms and response logic—known collectively as “abort triggers”— with respect to crew safety in the event of a vehicle failure during ascent to low earth orbit. Loss-of-crew risk is evaluated against three configurations of abort triggers, representing progressively broader and deeper sub-system coverage. An effort to propose new abort triggers beyond a limited baseline set is described. Given the rapidity and energy with which the most dangerous failures progress in launch systems, available warning time and failure mitigation effect are chief factors in determining an abort trigger’s contribution to crew safety. Loss-of-crew effect is determined for the subset of proposed triggers for which warning time and failure mitigation data are available, while the upper bound on loss-of-crew reduction potential is determined through coverage analysis for all of the proposed triggers. The importance of the baseline set of abort triggers is also established, particularly for a “last resort” trigger that detects vehicle structural breakup. Finally, the considerations used in the final abort trigger selection are discussed.

### Probabilistic Design Analysis (PDA) Approach to Determine the Probability of Cross-System Failures for a Space Launch Vehicle

Ann T. Shih(a), Yunnhon Lo(b), Natalie C. Ward(c)
*a) National Aeronautics and Space Administration (NASA), Langley Research Center, Hampton, VA, USA. b) Bastion Technologies, Inc., NASA Marshall Space Flight Center, Huntsville, AL, USA. c) Jacobs ESTS Group/ APL, NASA Marshall Space Flight Center, Huntsville, AL, USA*

Quantifying the probability of significant launch vehicle failure scenarios for a given design, while still in the design process, is critical to mission success and to the safety of the astronauts. Probabilistic risk assessment (PRA) is chosen from many system safety and reliability tools to verify the loss of mission (LOM) and loss of crew (LOC) requirements set by the NASA Program Office. To support the integrated vehicle PRA, probabilistic design analysis (PDA) models are developed by using vehicle design and operation data to better quantify failure probabilities and to better understand the characteristics of a failure and its outcome. This PDA approach uses a physics-based model to describe the system behavior and response for a given failure scenario. Each driving parameter in the model is treated as a random variable with a distribution function. Monte Carlo simulation is used to perform probabilistic calculations to statistically obtain the failure probability. Sensitivity analyses are performed to show how input parameters affect the predicted failure probability, providing insight for potential design improvements to mitigate the risk. The paper discusses the application of the PDA approach in determining the probability of failure for two scenarios from the NASA Ares I project.

# Decision Analysis

**Monday, Federal**

10:30 AM - Noon

## 8-1: Methods and Fundementals

Session Chairs: Robert Youngblood, Homayoon Dezfuli

### A Decision Analysis Framework for the U.S. Nuclear Fuel Cycle

Lara Pierpoint
*Massachusetts Institute of Technology, Cambridge, U.S.A.*

A decision analysis framework is presented for aiding decision makers in evolving the U.S. nuclear fuel cycle. A system dynamics model is used to calculate the impacts of deploying advanced burner reactors in the U.S., and these impacts are synthesized in a decision tree with multi-attribute payoffs. Two one-period versions of the decision tree are explored, each including a single decision node at 2040 where Advanced Burner Reactors (ABRs) are deployed along with Light Water Reactors (LWRs), or LWRs only are built for the remainder of the century. Preliminary results track with intuition, indicating that ABRs should only be built if their costs are low, if reducing waste is preferable to minimizing costs, and/or if nuclear power growth is high. The correspondence of the results to basic logic indicates this methodology may be useful for more complex fuel cycle decisions, where a high number of decision variables and uncertainties preclude an easy understanding of the tradeoffs and desirable pathways.

### Methodology of Selecting Useful Activities for Risk-Informed Decision Making

Yoshiyuki Narumiya
*The Kansai Electric Power Co., Ltd., Osaka, Japan*

It is necessary to select an useful case by ascertaining the realities of the safety activities of an own plant, considering the regulatory requirement, selecting the risk metric that the risk of changing can be exactly understood, and using the judgment standard provided by reasonable grounds to achieve “real risk-informed decision making.” In the first of steps for risk information application “Surveying”, activity is integrated hierarchized to items at a detailed level, and four aspects of each item of a) Aspect of absolute value, b) Aspect of change in risk metric, c) Aspect of dominant factor, and d) Aspect of time trend, are distributed in step 1. On the other hand, an appropriate risk metric is chosen from four characteristics of (1) the absolute value, (2) the amount of the change (or change ratio), (3) the importance measures, and (4) the time trend. As mentioned above, the clear risk informed decision making becomes possible to do by analyzing, understanding the characteristic of the changed activity enough, and choosing the adequate risk metrics:

### Analysis of Robustness of Statistical Survival Estimates via Multiple Objective Optimization

M. P. Brito and G. Griffiths
*National Oceanography Centre, Southampton, UK*

The decision supporting the deployment of expensive and complex technology in extreme environments is usually based on formal risk assessment. In the context of underwater vehicles deployment, a mission is authorized if and only if the estimated risk does not exceed an acceptable level. The typical rationale is to devise risk mitigation activities that make sure that the predictable risk equals the acceptable risk. This may be considered a good solution because it reduces the workload on the team. However by having the actual risk equal to the acceptable risk one is stating that the tolerance to future faults is zero. Faults do inevitably take place during campaigns and new faults will inevitably change the risk profile. It becomes imperative to quantify the robustness of the probability of survival estimate to faults that might take place during missions. This paper proposes the use of multiple objective genetic algorithms for estimating the robustness of a survival estimate. The proposed framework in which the method is applied is presented and two test cases illustrating the application of the approach using Autosub3 autonomous underwater vehicle survival data are discussed in detail.

1:30 - 3:00 PM

## 8-2: Strategic Assessments

Session Chair: Adrian Gheorge

### Modelling of Problems Taking Decisions in Low Density Traffic Lines Cases

Andrzej Chudzikiewicz
*Faculty of Transport, Warsaw University of Technology, Warsaw, Poland*

In all EU countries including Poland new technical and organizational solutions for the rail transport are continuously researched. Those new solutions would lead to a significant decrease in financial outlays related to the exploitation of the User – Railway – Vehicle system (URV). One of the research elements is discussions regarding the rail transport organization in Poland on subjects such as shutting down some rail connections, while on opening some new ones; on fees for using traffic lines; on local governments' subsidies and so on. Such discussions cover various aspects, not only technical condition, economic legitimacy, social factors and safety, but also in particular legal regulations referring to these issues. The dilemma specifically concerns lines with low density of traffic, so called Low Density Traffic Lines, which are considered to be a generator of expenditures and, at the same time, cause nothing but problems to the infrastructure's administrator. In many cases, the basis for decisions on the rail transport organization of these lines rests upon considerations and evaluations based only on the grounds of the decision-makers' intuition, without thorough technical and economic analyses. The reason behind is the length of time necessary to gather vital data essential to built rail line models where all the above mentioned aspects, necessary simulations and drawing up suitable forecasts (economic in particular) are included. In this field, there is the absence of tools, including IT tools, which could be used by the decision- makers (local governments, operators) in the decision-making process as a support instrument to their actions. The aim of this article will be to present the issues of creating such tools, in particular of creating a model for LDTL, which would later form a basis to built a simulation tool that would support the process of analysis while taking a decision on shutting down, opening or modernizing a low density traffic line.

### RAMS Engineering in the Development of Sustainable Energy Production Systems

Lijuan Dai(a), Marvin Rausand(b), and Ingrid Bouwer Utne(a)
*a) Department of Marine Technology. b) Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway*

For sustainable energy production systems, reliability, availability, maintainability, and safety (RAMS) are very important attributes. They ensure energy efficiency in three dimensions (environmental, economic, and social) of sustainability, and play a decisive role in achieving the success of the system. This paper presents a new approach to integrate RAMS engineering in the development of a sustainable energy production system. The offshore wind energy conversion system (OWECS) is chosen as an example. The new approach covers all phases of the system development process. Analytical methods that should be used in the various phases are identified.

# Software Reliability

**Monday, Federal**

3:30 - 5:00 PM

## 10-1: Software PRA

Session Chairs: Roger Boyer, Alan Nikora

### Establishing a Philosophical Basis for Probabilistic Modeling of Software Failures

Tsong-Lun Chu(a), Gerardo Martinez-Guridi(a), Meng Yue(a),Pranab Samanta(a), Gopika Vinod(b), and John Lehner(a)
*a) Brookhaven National Laboratory, Upton, NY, USA. b) Bhabha Atomic Research Center, Mumbai, India*

An important research topic is the fundamental philosophical aspects of software failures and their use in developing a probabilistic model of a digital system that integrates hardware and software failures. Accordingly, an expert panel meeting (workshop) was held in May 2009, with the goal of establishing the basic technical principles upon which software failures can be accounted for in a probabilistic risk assessment (PRA) of a nuclear power plant. Experts were invited from three types of stakeholders to ensure that they were represented in the discussions: experts with knowledge of software reliability and/or PRA, one representative from the U.S. Nuclear Regulatory Commission, and one representative from the nuclear industry. The workshop addressed the most fundamental questions raised on modeling these failures probabilistically, on including them in PRAs, and on methods for quantifying software failure rates and probabilities. This paper summarizes the approach for organizing the workshop, the discussions associated with the workshop, and the conclusions reached. Among the main conclusions, the panelists unanimously agreed that: software fails, the occurrence of software failures can be treated probabilistically, it is meaningful to use software failure rates and probabilities, and they can be included in reliability models of digital systems.

### A Framework for Software Reliability Management Based on the Software Development Profile Model

Arya Khoshkhou(a,b), Michel Cukier(a,c), Ali Mosleh(a)
*a) Center for Risk and Reliability University of Maryland College Park, MD USA. b) Lockheed Martin Corporation 7615 Ora Glen Drive Greenbelt, MD USA. c) The Institute for Systems Research University of Maryland College Park, MD USA*

This paper describes the Software Development Profile Model (SDPM) as a framework for estimating the reliability of software constructs based on the software change history. Recent empirical studies show a strong correlation between the change history of a file and its fault-proneness. Statistical data analysis techniques such as regression analysis have been applied to validate this finding and tools have been developed to predict the probable fault-prone files based on the software change history. Our model describes the relationship between the reliability of software constructs based on their change history and software development process. SDPM is independent of the type of construct, which can be a module, class, function point, line of code (LOC), source statement (SS), or other types of software unit for which data has been collected. The proposed model is based on the assumption that anytime a software construct is touched, it has a chance to become defective. Under this assumption, the model estimates the reliability of software constructs based on the change history and software development activities. The reliability estimate of software constructs are then used to estimate the level of defect proneness of various software artifacts such as source files or software modules.

### A PSA Model Developed for the Digital Reactor Protection System of the Latest PWR in Japan

Keisuke Kondo, Haruo Fujimoto and Masahiro Yamashita
*Japan Nuclear Energy Safety Organization (JNES), Tokyo, Japan*

A PSA model has been developed for the digital reactor safety protection system of the latest three-loop PWR in Japan. This plant adopts digital reactor safety protection and control system from the construction stage as one of the major fundamental design features and has started commercial operation in December 2009. The digital reactor protection system (RPS) of this plant consists of the digital primary system and the analogue backup subsystem. The primary system consists of four channels of sensors, reactor trip processors and channel trip processors as well as eight sets of reactor trip breakers. Reactor trip is accomplished by at least two partial reactor trip signals out of four channel trip processors. The backup subsystem, so-called 'anti-CCF measure,' receives the sensor signal from the primary subsystem and generates an alternative reactor trip signal to open the dedicated breakers attached to the CRDM M-G set power distributor boards. A PSA model was developed for this Reactor Protection System (RPS) as well as Engineered Safety Features Actuation System (ESFAS) and quantified. As a result of the review by the NISA and JNES, it is shown that the digital system has higher reliability relative to the conventional system for both RPS and ESFAS.

### Application of Context-based Software Risk Model (CSRM) to Assess Software Risk Contribution in Constellation Project PRAs

Michael Yau, and Sergio Guarro
*ASCA, Inc., Redondo Beach, USA*

A traditional space mission Probabilistic Risk Assessment (PRA) does not usually include in its scope the modeling and assessment of software contributions to system risk. This paper presents an approach adopted by the Constellation program for augmenting a PRA that was originally derived in this manner. This approach includes scenarios and logic models developed according to the Context-based Software Risk Model (CSRM) to assess software related mission risk. CSRM can be applied at different levels of detail, to match the available system and software design information at a particular stage of development. For practical purposes, two basic stages and forms of CSRM application are defined, the Specification-Level CSRM and the Design-Level CSRM.

# PSA Applications

**Monday, Superior**

10:30 AM - Noon

## 1-11: Uncertainty Analysis

Session Chairs: Kaisa Simola, Kurt Vedros

### Impact of Uncertainty on Calculations for Recovery from Loss of Offsite Power

Dana L. Kelly
*Idaho National Laboratory, Idaho Falls, USA*

Uncertainty, both aleatory and epistemic, can have a significant impact on estimated probabilities of recovering from loss of offsite power within a specified time window, and such probabilities are an input to risk-informed decisions regarding the significance of inspection findings in the U.S. Nuclear Regulatory Commission's Reactor Oversight Process. In particular, the choice of aleatory model for offsite power recovery time can have a significant impact on the estimated nonrecovery probability, especially if epistemic uncertainty regarding parameters in the aleatory model is accounted for properly. In past and current analyses, such uncertainty has largely been ignored. This paper examines the impact of both aleatory and epistemic uncertainty on the results, using modern open-source Bayesian inference software, which implements Markov chain Monte Carlo sampling. It includes examples of time-dependent convolution calculations to show the impact that uncertainty can have on this increasingly frequent type of calculation, also. The results show that the "point estimate" result, which is an input to risk-informed decisions, can easily be uncertain by a factor of 10 if both aleatory and epistemic uncertainties are considered. The paper also illustrates the use of Bayesian model selection criteria to aid in the choice of aleatory model.

### Determination of success criteria of an accident sequence based on uncertainty analysis in a PSA model

Ho-Gon Lim(a), Joon-Eon Yang(a), and Un-Chul Lee(b)
*a) Korea Atomic Energy Research Institute, Daejeon, Korea. b) Seoul National University, Seoul, Korea*

We propose new success criteria determination methodology in an accident sequence in a PSA model. Best-estimate (BE) T-H analysis method is introduced to quantify a failure/success probability of an accident sequence by considering the effect of parameters which can influence the accident progression but are not included in the ET. The processes are composed of three step, (1) parameter selection based on their significance on the accident progression, (2) T/H analysis by Monte-Carlo sampling of the parameters based on their statistical distribution characteristics, and (3) conditional failure/success probability quantification in a accident sequences.

### Experimentation of Sensitivity Study Based on Beta Factors to Assess the Impact of I&C In PSA

Gilles Deleuze(a), Thuy Nguyen(b), Richard Quatrain(a), Franck Jouanet(a)
*a) EDF R&D, Clamart, France. b) EDF R&D, Chatou, France*

This article proposes an approach, still under investigation at EDF R&D, to improve the representation of digital I&C in Probabilistic Safety Assessment (PSA), while keeping the models simple and usable. The approach relies on the combined use of a particular representation of I&C effects, the "Compact Model", and a sensitivity analysis based on "Beta Factors" representing potential dependencies due to hardware, software or human actions. It considers the different failure mechanisms and common cause failure mechanisms (random mechanisms, systematic mechanisms, and human factors), that are evaluated by a combination of probabilistic and deterministic approaches.

### Uncertainty Propagation Method for CCF Basic Events

Yunlong Li(a), Michael Lloyd(b), and Dennis Henneke(a)
*a) GE Hitachi Nuclear Energy, Wilmington, NC, USA. b) Risk Informed Solutions Consulting Services, Inc., Russellville, AR, USA*

Common Cause Failure (CCF) basic events are generally important contributions to nuclear power plant (NPP) risk. This fact requires their inclusion in NPP Probabilistic Risk Assessment (PRA) models and, subsequently, requires the treatment of their uncertainties. Typically, NPP PRA models treat CCF uncertainties simplistically and without rigorous basis. Given the relative importance of CCF, the treatment of CCF uncertainty should be both realistic and rigorous. This paper explains an analytical method to calculate CCF basic events uncertainties, which account for the uncertainty propagation from both the independent failure basic event and the CCF parameters. Two examples are provided to demonstrate the application of this analytical method, which simulate a simplified four-train system model. The analytical results are compared to the results from a Monte Carlo simulation code. The differences between the two methods are found to be 1% and 3% for the two examples. Additional sensitivity cases have been developed to reflect the current methods used in the industry for CCF uncertainty propagation. The sensitivity results demonstrate the necessity to further the rigor of the CCF uncertainty calculation processes, which has been demonstrated by this paper with the application of the analytical method.

1:30 - 3:00 PM

## 1-12: General PSA Applications I

Session Chairs: Jean Primet, Robert Buell

### Use of PSA in a Modernization Program. Findings and Results from the Ringhals 1 PSA

Anders Olsson(a), Peter Jacobsson(b), Stefan Authén(c) and Stefan Eriksson(d)
*a) Scandpower-Lloyd's Register, Malmo, Sweden. b) Systecon AB, Malmo, Sweden. c) Risk Pilot, Stockholm, Sweden. d) Vattenfall AB, Varobacka, Sweden*

This paper will present how the PSA study for Ringhals 1 has been used as a tool for the large modernization project at Ringhals 1. The paper will give the background for the modernization of the plant, the background of the PSA study, modeling and results of the PSA.

### Developing A Methodology for Identifying Correlations Between LERF and Early Fatality

Kyungmin Kang(a,b), Moosung Jae(a), Kwang Il Ahn(b)
*a) Department of Nuclear Engineering, Hanyang University, Sungdong-Gu, Seoul, Korea. b) Korea Atomic Energy Research Institute (KAERI), Yuseong, Daejeon, Korea*

The correlations between Large Early Release Frequency (LERF) and Early Fatality need to be investigated for risk-informed application and regulation. In RG-1.174, there are decision-making criteria using the measures of CDF and LERF, while there are no specific criteria on LERF. Since there are both huge uncertainty and large cost need in off-site consequence calculation, a LERF assessment methodology need to be developed and its correlation factor needs to be identified for riskinformed decision-making. This regards, the robust method for estimating off-site consequence has been performed for assessing health effects caused by radioisotopes released from severe accidents of nuclear power plants. And also, MACCS2 code are used for validating source term quantitatively regarding health effects depending on release characteristics of radioisotopes during severe accidents has been performed. This study developed a method for identifying correlations between LERF and Early Fatality and validates the results of the model using MACCS2 code. The results of this study may contribute to defining LERF and finding a measure for risk-informed regulations and riskinformed decision-making.

### Development and Application of a Risk Monitor for Nuclear Power Plant

Y. Wu(a,b), Y. Li(a,b), L. Hu(a,b), Y. Luo(b,c), X. Gu(a,b), J. Q. Wang(a,b), F. Wang(a,b), J. Wang(a,b), T. Chen(c), J. Qi(c)
*a) School of Nuclear Science and Technology, University of Science and Technology, Hefei, China. b) Institute of Plasma Physics, Chinese Academy of Sciences, Hefei, China. c) Hefei University of Technology, Hefei, China*

Risk monitor, which has been widely used in the progress of RID (Risk Informed Decision) in a NPP (Nuclear Power Plant), is a plant specific real-time analysis tool to determine the instantaneous risk based on actual plant configuration. Based on wide investigation of challenges and technical issues during the development of a risk monitor, a prototype named Risk Angel has been designed by FDS Team in collaboration with several institutes and universities. An overview of the architecture and main functions of Risk Angel were introduced in this paper, as well as the quantitative approach, the calculating engine and the model development. Risk Angel has been applied in a nuclear power plant in P.R. China

### Results of the Updated Level 1 PSA Model of the NPP Doel 3

Erik Bourdiaudhy(a), Françoise Dassy(b)
*a) Electrabel, NPP Doel, Belgium. b) Tractebel Engineering, Brussels, Belgium*

Electrabel which is part of the group GDF SUEZ owns and operates 7 nuclear power plants (type PWR) in Belgium. The total installed capacity is about 8000 MW. For NPP Doel 3 which is a 900 MW PWR Framatome design, a first PSA model was developed by Tractebel Engineering in co-operation with the operator Electrabel. The model was validated by Regulatory Body in 2000. As a result of this PSA, improvements of the plant have been performed. The major modifications were: - upgrading reliability of seal injection primary pumps - modification of procedures in cold shutdown conditions - changes in reactor protections at midloop condition - opening the pressurizer manhole at midloop condition In the framework of the Periodic Safety Review (PSR) of 2009 the model has been updated taking into account new regulations. The new model has a better performance and is more detailed. Following changes can be noted: - Methodologies (HRA, OEF) - Plant modifications - Specific demands of Regulatory Body - New Initiating Events (IE) The following changes in the new Level1 model will be discussed: - Covering of all plant operating modes by extension of Plant Operating States (POS) - All IE, considered in the scope of PSR update, are treated in all the applicable POS - Systematic modeling of supporting systems as compressed air, cooling diesels, ventilation - More detailed modeling of IE Loss Of Offsite Power (LOOP) - Taking into account frequency of tests, outline failures - Changes of Human Reliability Analysis (HRA) Their specific impact on the global CDF will be examined in detail. Global CDF will be discussed and details presented by Plant Operating State (POS). Strengths and weaknesses are spotted in order to upgrade the reliability of the NPP.

3:30 - 5:00 PM

## 1-13: General PSA Applications II

Session Chairs: Jim Chapman, Kevin Coyne

### NPSAG/NKS: Evaluation of the Technical Specification Criteria – Development of a Guidance Document

Anna Häggström(a), Ola Bäckström(a), and Ilkka Männistö(b)
*a) Scandpower-Lloyd's Register, Stockholm, Sweden. b) VTT, Helsinki, Finland*

A nuclear power plant's Technical Specifications (TS) define the limits and conditions for plant operation to secure the validity of the assessment performed in the SAR. As the probabilistic safety assessment (PSA) has developed over the years, it has demonstrated to constitute a useful tool for evaluating many aspects of the TS from a risk point of view. No guidance for risk-informed development and assessment of TS has however been available in the Nordic countries. In a joint project between the Nordic PSA Group (NPSAG) and Nordic nuclear safety research (NKS) a guidance document therefore has been developed. The guidance provides both general and detailed requirements on methods and acceptance criteria and on how risk-informed methodologies are to be used to change or specify new demands in the TS for both allowed outage times (AOTs) and surveillance test intervals (STIs).

### Using of the PSA During the Third Periodic Safety Visit of 900 MWe Power Reactors in France

F. Corenwinder, G. Georgescu and A. Laborde
*Institute for Radiological Protection and Nuclear Safety (IRSN), Fontenay aux Roses, France*

The periodic safety review procedure, applicable to existing reactors, is a periodic process implemented for a given reactor series, which incorporates the analysis of recent operating experience and updated knowledge. PSAs are used during the periodic safety review mainly to assess the core damage frequency and its change compared with the assessment made on completion of the previous review, including an analysis of the changes in system characteristics (equipment reliability, for example) and in operating practices. The identification of the main contributions to the core damage frequency highlights any weak points for which design and operation changes can be studied, or even judged necessary. During the period 2005-2009, the third periodic review for the 900 MWe nuclear power reactors was performed. In this frame, a particularly deep verification of the PSA developed by the EDF was performed by IRSN. In this context the PSAs developed by IRSN (Level 1, Level 2 and Fire PSA) were used to asses the EDF studies. The Level 1 PSA helped to identify the need for an important safety design modification (mitigation of the main pumps thermal barrier rupture) and the need to perform further deterministic studies for an important phenomena (boron dilution by the rupture of the main pump seal leak heat exchanger tubes).

### An Approach to Classify the Risk of Operating Nuclear Power Plants – Case Study: Neckarwestheim Unit 1 and Unit 2

A. Strohm(a), L. Ehlkes(a), W. Schwarz(a), M. Khatib-Rahbar(b), M. Zavisca(b), and D. Rittig(c)
*a) EnBW Kernkraft GmbH, Kernkraftwerk Neckarwestheim, Germany. b) Energy Research, Inc., Rockville, Maryland, USA. c) ISaR GmbH, Garching, Germany*

A level-2 Probabilistic Safety Assessment (PSA) is an integrated approach to investigate the progression of severe accidents up to containment failure and release of radionuclides into the environment. The results of a standard level-2 PSA include the frequencies associated with various containment failure modes (release categories) along with the environmental release quantities for various radioisotopes (source terms). The extended level-2 PSA approach discussed in this paper merges the standard level-2 PSA results into an integral metric for risk assessment by estimating the integral risk of activity of radiological release to the immediate vicinity of the plant. Risk is defined as a product of the released activity and the release-category frequency, integrated over all possible release categories. This approach was recently used to assess the risk of severe accidents for the Neckarwestheim Unit 1 (3-loops, 840 MWe) and the Neckarwestheim Unit 2 (4-loops, 1400 MWe) nuclear power plants, which entered commercial operation in 1976 and 1989, respectively. The results have demonstrated that neither the core damage frequency nor the core damage profile necessarily is an adequate indicator of plant risk. Furthermore, neither the absolute frequencies of release categories nor the relative proportions of the release category frequencies necessarily provide a balanced picture of severe accident risk as represented by the integral activity of release.

# Tuesday Meeting-At-A Glance

| Room Session | Salon A | Salon B | Salon C | East Room | West Room | North Room | Municipal | Federal | Superior | South Room |
|---|---|---|---|---|---|---|---|---|---|---|
| 0730 - 1600 | **Conference Registration - Courtyard Foyer** | | | | | | | | | |
| 0700 - 0830 | **Continental Breakfast - Madison, Courtyard, and Compass Foyers** | | | | | | | | | |
| 0830 - 1000 | Plenary Speaker - Dr. Douglas Hubbard - Madison Ballroom | | | | | | | | | Exhibits |
| 1000 - 1030 | ***Coffee/Refreshment Break*** | | | | | | | | | |
| 1030 - 1200 | Advanced Reactors 16-5: PRA In Design - Risk Management (Panel) | Modeling and Simulation 2-4: Systems Modeling | HRA 5-4: Resilience and Use of Data | PSA Applications 1-4: Test and Research Reactor PSA Applications | External Events 15-4: Fire: Risk and consequence Analysis I | Safety Culture 9-4: Socio-technical Modeling II | Space & Aviation 12-4: Lunar Exploration Risk Assessments | Software Reliability 10-2: Software Design and Failure Analysis | PSA Applications 1-14: Specific PSA Applications I | |
| 1200 -1330 | ***Conference Luncheon - Madison Ballroom and Municipal Room if needed*** | | | | | | | | | |
| 1330 - 1500 | Advanced Reactors 16-4: Safety Issues and Methodology | Modeling and Simulation 2-5: Uncertainty and Importance | HRA 5-5: Human Behavior and Disaster Response I | PSA Applications 1-5: Unique Risk Contexts Design and Shutdown | External Events 15-5: Fire: Risk and consequence Analysis II | Safety Culture 9-5: Safety Culture in Practice | Space & Aviation 12-5: Mars Exploration Risk Assessments | Special Session 19-1: Importance Measures | PSA Applications 1-15: Specific PSA Applications II | |
| 1500 - 1530 | ***Coffee/Refreshment Break - Madison, Courtyard, and Compass Foyers*** | | | | | | | | | |
| 1530 - 1700 | Risk Management 4-1: Special Session - ESREDA-ESRA Maintenance Modeling | Modeling and Simulation 2-6: PSA Quantification | HRA 5-6: Dynamic Approaches | PSA Applications 1-6: Level 2 PSA | External Events 15-6: Fire Data Analysis | Safety Culture 9-6: Nuclear Safety Culture and Regulatory Oversight | Space & Aviation 12-6: Methods | Security Infrastructure 14-1: Vulnerability of Critical Infrastructures | PSA Applications 1-16: Methods | |
| 1730 - 2030 | IAPSAM Board Meeting and Dinner - Visions | | | | | | | | | Exhibits |

# Plenary Speaker

## Douglas W. Hubbard

Mr. Hubbard is the inventor of the powerful Applied Information Economics (AIE) method. He is the author of the #1 bestseller in Amazon's math for business category titled How to Measure Anything: Finding the Value of Intangibles in Business (Wiley 2007). His latest book is titled The Failure of Risk Management: Why It's Broken and How to Fix It (Wiley 2009).

His career has focused on the application of AIE to solve current business issues facing today's corporations. Mr. Hubbard has completed over 60 risk/return analyses of large, critical projects, investments and other management decisions in the last 16 years. AIE is the practical application of several fields of quantitative analysis including Bayesian analysis, Modern Portfolio Theory, Monte Carlo Simulations and many others. Mr. Hubbard's consulting experience totals over 20 years and spans many industries including insurance, banking, utilities, federal and state government, entertainment media, military logistics and manufacturing.

In addition to his books, Mr. Hubbard is published in CIO Magazine, Information Week, DBMS Magazine, Architecture Boston, OR/MS Today and Analytics Magazine. His AIE methodology has received critical praise from The Gartner Group, The Giga Information Group, and Forrester Research. He is a popular speaker at IT Metrics & Economics conferences all over the world.

Prior to specializing in Applied Information Economics, his experiences include data and process modeling at all levels as well as strategic planning and technical design of systems.

---

**The Failure of Risk Management**

Douglas W. Hubbard, President, Hubbard Decision Research and author of The Failure of Risk Management: Why It's Broken and How to Fix It (2009) and How to Measure Anything: Finding the Value of "Intangibles" in Business (2007).

What is your organization's greatest risk? Chances are, it's that your risk analysis – and therefore your risk management – has some serious flaws and may not be improving decisions at all. Even the most quantitative analysis methods have been found to have systemic – but avoidable – biases and errors. For example,

- While most quantitative models have at least some subjective estimates, research shows that experts are consistently overconfident in their assessments of their own uncertainty.
- Empirical analysis is vastly underutilized in quantitative risk assessments and when it is applied, it tends to be applied to the wrong problem.
- Research shows that there is a strong placebo effect in the use of "structured" methods causing decision maker to feel more confident in their choices, even when the decisions and forecasts were measurably worse
- A proliferation of new "soft" risk assessment methods will cause far more problems than they (claim to) solve.

The speaker, Douglas Hubbard, will review all of these problems and how to avoid them. His talk will show research collected from a variety of fields that show that 1) quantitative methods work best, 2) but even quantitative methods have avoidable problems and 3) the growing popularity of "qualitative" methods will make us feel better about decisions without actually improving them (or even making them worse).

# Advanced Reactors

**Tuesday, Salon A**

10:30 AM - Noon

## 16-5: Probabilistic Risk Assessment in Design -PANEL Disscussion

Session Chair: Robert Youngblood - Panelists to be determined

### PRA In Design: Increasing Confidence in Pre-operational Assessments of Risks (Results of a Joint NASA/ NRC Workshop)

Robert Youngblood(a), Nathan Siu(b), and Homayoon Dezfuli(c)
*a) Idaho National Laboratory, Idaho Falls, Idaho, USA . b) US Nuclear Regulatory Commission, Washington, DC, USA. c) National Aeronautics and Space Administration (NASA), Washington, DC, USA*

In late 2009, the National Aeronautics and Space Administration (NASA) and the U.S. Nuclear Regulatory Commission (NRC) jointly organized a workshop to discuss technical issues associated with application of risk assessments to early phases of system design. The workshop, which was coordinated by the Idaho National Laboratory, involved invited presentations from a number of PRA experts in the aerospace and nuclear fields and subsequent discussion to address the following questions: (a) What technical issues limit decision-makers' confidence in PRA results, especially at a pre-operational phase of the system life cycle? (b) What is being done to address these issues? (c) What more can be done? The workshop resulted in participant observations and suggestions on several technical issues, including the pursuit of non-traditional approaches to risk assessment and the verification and validation of risk models. The workshop participants also identified several important non-technical issues, including risk communication with decision makers, and the integration of PRA into the overall design process.

### Design Requirements for PBMR Reactor Building for the Next Generation Nuclear Plant

Karl N. Fleming, Fred A. Silady, Alfred Torri, Lori Mascaro, and David A. Dilling
*Technology Insights, San Diego, U.S.A*

This paper summarizes a recent study that develops technical and functional requirements (T&FRs) for the PBMR being designed for the Next Generation Nuclear Plant (NGNP) Reactor Building (RB), including considerations of the role of the reactor building to support reactor safety functions and alternative reactor building design strategies to achieve each safety function that has been defined during the pre-conceptual design. A comprehensive set of technical and functional requirements for the NGNP Reactor Building was developed in this study for use in the Conceptual Design Phase to follow. These requirements were developed in a top down fashion starting with the NGNP Top Level Requirements identified in the Preconceptual Design Report for the NGNP and the following considerations: Role of the Reactor Building (RB) in the Pebble Bed Modular Reactor (PBMR) NGNP safety design approach. A key result of this study was the evaluation of alternative Reactor Building concepts for the satisfaction of the building safety functions involving pressure relief for helium pressure boundary (HPB) leaks and breaks, retention of radioactive material that may be released from the fuel and the HPB, and limiting of the potential for air ingress following large HPB breaks.

1:30 - 3:00 PM

## 16-4: Safety Issues and Methodology

Session Chair: Rick Grantom

### Scenario Aggregation and Analysis via Mean-Shift Methodology

Diego Mandelli(a), Alper Yilmaz(b), Tunc Aldemir(a), Richard Denning(a)
*a) The Ohio State University, Nuclear Eng. Program; Columbus (OH), USA. b) The Ohio State University, Civil, Environmental Eng. and Geodetic Sciences; Columbus (OH), USA*

A challenging aspect of dynamic methodologies, such as the Dynamic Event Tree (DET) methodology, is the large number of scenarios generated for a single initiating event. Such large amounts of information can be difficult to organize in order to extract useful information. The scenario dataset is composed of scenarios which contain information on the system components and the system process variables, such as values of pressures and temperatures for the reactor coolant system and the containment throughout the time period of the transient. In order to facilitate analysis, it can be fruitful to accomplish two tasks: i) identify the scenarios that have a "similar" behavior (i.e. identify the most evident classes), and, ii) decide, for each event sequence, to which class it belongs (i.e., classification). It is shown how it is possible to accomplish these two tasks using the Mean-Shift Methodology. The Mean-Shift methodology is a kernel-based, non-parametric density estimation technique that is used to find the modes of an unknown distribution, which corresponds to regions with highest data density. The methodology is illustrated by applying it to the DET analysis of a simple level controller.

### An Integrated Safety Assessment Methodology for Generation IV Nuclear Systems

Timothy J. Leahy(a), Gian-Luigi Fiorini(b)
*a) Idaho National Laboratory, Idaho Falls, ID, USA. b) Commissariat Energie Atomique, Cadarache, FRANCE*

The Generation IV International Forum (GIF) Risk and Safety Working Group (RSWG) was created to develop an effective approach for the safety of Generation IV advanced nuclear energy systems. Early work of the RSWG focused on defining a safety philosophy founded on lessons learned from current and prior generations of nuclear technologies, and on identifying technology characteristics that may help achieve Generation IV safety goals. More recent RSWG work has focused on the definition of an integrated safety assessment methodology for evaluating the safety of Generation IV systems. The methodology, tentatively called ISAM, is an integrated "toolkit" consisting of analytical techniques that are available and matched to appropriate stages of Generation IV system concept development. The integrated methodology is intended to yield safety-related insights that help actively drive the evolving design throughout the technology development cycle, potentially resulting in enhanced safety, reduced costs, and shortened development time.

### Sodium Metal Fires and Advanced Reactor Safety

Tara J. Olivier, John C. Hewson, Thomas K. Blanchat, Steven P. Nowlen
*Sandia National Laboratories, Albuquerque, NM, USA*

Using liquid metal coolant in fast reactors introduces unique safety risks; namely, metal fires. Sandia National Laboratories (SNL) current research goals include adding metal fire phenomenology to the existing fire models, specifically metal surface reaction capability, and performing discovery experiments to support model validation. The development of the computational models will attempt to include the ability to estimate the heat release rate of sodium spray and pool fires. This will consist of extending existing spray and pool-surface combustion models to include surface reactions. The discovery experiments will be performed to assess the understanding provided by the current computational fire models. This paper will focus on the initial experimental results for both the sodium spray and pool fire experiments performed at SNL. Some of the initial program research will be discussed including the literature review, phenomenon identification and ranking table exercise, and background information about the rational for the sodium pool fire experiments.

# Risk Assessment

**Tuesday, Salon A**

3:30 - 5:00 PM

## 4-1: Special Session ESREDA-ESRA Maintenance Modeling

Session Chairs: Enrico Zio, Adrian Gheorghe

### Imperfect Maintenance Models: A Review

Inma T. Castro
*Department of Mathematics, University of Extremadura, Cáceres, Spain*

Imperfect maintenance models have been extensively used in the reliability literature. This paper shows some methods used to model the imperfect maintenance.

### Condition-based Maintenance and Non-Observable Deteriorating Systems

Phuong Khanh Nguyen Thi(a), Mitra Fouladirad(b), Christophe Bárenguer(b)
*a) Ecole des mines de Nantes, Nantes, France. b) Universit´e de Technologie de Troyes, Institut Charles Delaunay, FRE CNRS, Troyes, France*

The aim of this paper is to discuss the problem of optimisation of condition-based maintenance policies for a deteriorating system where the deterioration state is not directly observable. The deterioration process is assumed to be a time-homogenous

Markov chain with finite state space. The deterioration process is modeled by a doubly stochastic process known as Hidden Markov Models. In the framework of the system under consideration, appropriate inspection/ replacement policies which minimize the expected average maintenance cost are derived. The average cost of different maintenance policies are analyzed through simulation experiments to compare the policies performances. Keyword: Condition-based maintenance, Hidden Markov Model, Deteriorating systems, Expected long run average cost, Adaptive maintenance policy, Preventive replacements.

### From Living PSA to Living Probabilistic Asset Management

Sipke E. van Manen and Johan van den Bogaard
*Rijkswaterstaat, Ministry of Transport, Public Works and Water Management, The Netherlands*

In order to guarantee performance of complex safety related systems, a commonly used approach is the so-called Probabilistic Safety Analysis (PSA). In the nuclear industry PSA is successfully used in a large number of plants around the world over many years. The maturity of and experience with PSA makes it a powerful tool in the safety decision-making process, which is routinely applied by both plant operators and Regulatory Authorities, see for instance [1]. The PSA approach focuses on safety critical systems. However, the approach can be broadened to e.g. performance critical systems To include these assets in the performance assessments PSA as such does not suffice and adjustments in the approach are necessary. This paper introduces an adjusted PSA approach that is applicable for other assets and is called Probabilistic Asset Management (PAM). PAM considers all relevant life cycle stages and related activitites affecting performance characteristics, such as design, building/ construction, maintenance and operation of the asset. This means understanding the system ans specific asset behavior, both at regular operating conditions and in faulty and degraded conditions. A clear definition of operating conditions and unacceptable deviations (resulting in fault conditions) for the complete asset is necessary, including contributions from auxiliary safety systems, external power and communication lines, human intervention (operation, maintenance, recovery), software and so on. Applying a life cycle approach performance characteristics of specific assets and even systems may change (e.g. due to aging) significantly or may have to change (e.g. changing user requirements). To remain in control of the system perfomance over time, these time effects are taken into account in the PAM approach. This paper shows how the well-known Deming Circle is applied to Probabilistic Asset Management which makes it a living PAM, in accordance with a living PSA. It is shown that with Living PAM the decision making process in asset management is supported by an extremely powerful tool.

# Modeling and Simulation

**Tuesday, Salon B**

10:30 AM - Noon

## 2-4: Systems Modeling

Session Chairs: Olivier Nusbaumer, Ho-gon Lim

### Analysis of Logical Loops in Boolean System Models

Takeshi Matsuoka
*Utsunomiya University, Utsunomiya City, Tochigi, Japan*

Discussions are made for operation of typical engineering systems with loop structure. It is revealed that components are necessary to be classified into three types, Self sustained type (SS-type), Generative type (G-type) and Transmitter type (T-type). For a system that has logical loop structure(s), the Boolean relations have to be described with unknown element(s). The procedure for solving Boolean equations with unknown element(s) is described. Establishment of loop operation is discussed in time-dependent behavior for a fundamental structure. This process is expressed by Boolean relations and indefinite elements are identified by comparing to engineering behavior. A generalized procedure is proposed for solving Boolean equations that represent logical loop structure(s).

### Epistemic Uncertainty Reduction in the PSA of Nuclear Power Plant using Bayesian Approach and Information Entropy

Akira Yamaguchi, Masa-aki Kato, and Takashi Takata
*Osaka University, Suita, Japan*

It is a great concern how effectively the epistemic uncertainty can be reduced in the probabilistic safety assessment (PSA) as the safety research advances and new knowledge is obtained. The only way to reduce the epistemic uncertainty seems to be to extend our knowledge concerning the uncertain phenomena or parameters. If we have new experimental data, the evidence may suggest improvement or modification in the model and the database for the safety analysis. It is reasonable and effective to collect the seismic fragility data concerning the risk-dominant contributors. On the other hand, if the importance of the information is small, we would take little notice of the data. The issue is how to design the new experiment so that we can effectively improve the model and the database. In the present study, the authors propose a new methodology to measure the reduction in the epistemic uncertainty on the basis of the information entropy concept. The prior and the posterior seismic fragility is updated from experimental data using the Bayesian method. We can determine the experimental conditions that enhance our knowledge on the phenomena in the most effective and economical way. As a result, the uncertainty of the seismic PSA results is reduced on the basis of metrics expressed as the information entropy.

### A Treatment of Not Logic in Fault Tree and Event Tree Analysis

Ola Bäckström and Daniel Ying
*Scandpower-Lloyd's Register, Stockholm, Sweden*

Not logic in fault trees and event trees can be introduced for a number of reasons. One reason to use not logic is when modeling event trees. In the underlying fault tree, the success branches will be represented as negated gates with their inputs underneath. Another use of not logic is to exclude unwanted or impossible combinations of fault events. In this case it is not obvious how the treatment should occur, since it may depend on the point of view in the analysis. This paper will discuss a method of treating this type of not logic. The inclusion of not logic in a model usually makes the model much more complex and leads to longer run-times and more memory consumption. In fact, large real-life PSA models is in many cases impossible to solve using complete not logic treatment. In other cases, the user may not be willing to pay the price in terms of long run times that come with the treatment of "semi-complete" not logic. There is no reason to actually cover all the possible combinations of not logic structures that can occur in a fault tree, since these cases do not model real life fault events. One can always argue that an algorithm should solve these cases too, but the result of them would have no real life meaning. Therefore, it is necessary to use a set of rules for modeling not logic in a fault tree in order to prevent these situations. In cases where they do exist, this should be alerted to the user that there may be errors in the solution due to the modeling of the not logic structure in the fault tree.

### Model Uncertainty via Mixed Bayesian Networks

Paulo Renato Alves Firmino(a), Enrique López Droguett(b)
*a) Rural Federal University of Pernambuco, Recife, Brazil. b) Federal University of Pernambuco, Recife, Brazil*

Model uncertainty (MU) is among the most important issues for statistical inference. It aims at measuring uncertainty about the structure of the model instead of working on the specification of the parameters underlying such a structure (parameter uncertainty). This characteristic is useful, for instance, for inferring about a given quantity based on a set of models, allowing for aggregated estimates. In a Bayesian perspective, models' estimates are viewed as evidences in order to infer about the target quantity. The main purpose of the present paper is to encapsulate recent MU frameworks into Bayesian networks (BN) in order to facilitate their comprehension and to improve both the quality of the resulting Bayesian model as well as to make use of existing algorithms directed to manipulate mixed BN (networks involving categorical and non-categorical variables). By means of case studies, the sensitiveness of the MU Bayesian models to their underlying conditional distributions is evaluated. Furthermore, the performance of known methods for BN manipulation is studied and compared with an alternative approach developed by the authors into the context of MU Bayesian models.

### Large Scale Nuclear Sensor Monitoring and Diagnostics by Means of an Ensemble of Regression Models Based on Evolving Clustering Methods

Giulio Gola(a), Davide Roverso(a), Mario Hoffmann(a), Piero Baraldi(b), Enrico Zio(b)
*a) Institute for Energy Technology, Halden, Norway. b) Polytechnic of Milan, Milan, Italy*

On-line sensor monitoring systems aim at detecting anomalies in sensors and reconstructing their correct signals during operation. Auto-associative regression models are usually adopted to perform the signal reconstruction task. In full scale implementations however, the number of sensors to be monitored is very large and cannot be handled effectively by a single reconstruction model. This paper tackles this issue by resorting to an ensemble of reconstruction models in which each model handles a small group of signals. In this view, firstly a procedure for generating the signal groups must be set. Then, a corresponding number of signal reconstruction models must be built on the bases of the groups and, finally, the outcomes of the reconstruction models must be aggregated. In this paper, three different signal grouping approaches are devised for comparison: pure-random, random-filter and random-wrapper. Signals are then reconstructed by Evolving Clustering Method (ECM) models. The median of the outcomes distribution is here retained as the ensemble aggregate. The ensemble approach is applied to a real case study concerning the validation and reconstruction of 792 signals measured at the Swedish boiling water reactor located in Oskarshamn.

1:30 - 3:00 PM

# 2-5: Uncertainty and Importance

Session Chairs: David Johnson, Curtis Smith

### A Comparison of Polynomial Response Surfaces and Gaussian Processes as Metamodels for Uncertainty Analysis with Long-Running Computer Codes

Dustin R. Langewisch, George E. Apostolakis
*Department of Nuclear Science and Engineering, Massachusetts Institute of Technology, Cambridge, MA, USA*

We discuss some of the findings of a recently completed extensive review of the literature concerning methods for approximating the input-output behavior of complex computer codes (i.e., metamodeling). This review has been motivated by a need in the nuclear safety community to perform uncertainty analysis (UA) for long-running (e.g., several hours or days per simulation), mechanistic computer models, a task that has often proven prohibitively expensive due to the need to perform hundreds or thousands of simulations. We focus on the use of polynomial response surfaces (RS) and Gaussian processes (GP) as metamodels. RSs, though simple, efficient, and often quite useful, have been criticized by several authors who have raised numerous objections to their use as metamodels for deterministic codes, and we summarize these objections. GPs offer several advantages over RSs, particularly with regards to these criticisms, but do so at the expense of some simplicity and efficiency. Finally, we present the results of a case study involving the failure probability estimation of a passive nuclear safety system. The results of this case study suggest that GPs are superior when data are limited, but that both RSs and GPs perform comparably when many data are available.

### The Design Process Under the Focus of the Lateo

Fabio Ferreira da Costa Campos, Walter Franklin Marques Correia, Andre Menezes Marques das Neves
*Universidade Federal de Pernambuco – Department of Design, Recife, Brazil*

The field of subjective uncertainty is currently in an area of knowledge where an epistemology is not well established. This work will be shown the direction of an epistemology of subjective uncertainty, with their respective premises, and a way to check them through models. If a system fails to model all the assumptions of the subjective uncertainty will not be able to model the subjective uncertainty in a general way. This is what happens, for example, the rules of combination so far used the Dempster-Shafer theory, one of the formal models that deal with subjective uncertainty. This paper presents a method to model the three premises of subjective uncertainty (the lack of explicit knowledge, the conflict between the evidence and the non-uniqueness of the assignment of belief and their relative division among the hypotheses chosen), extending the Dempster-Shafer theory, correcting their behavior counter-intuitive, and allowing its use in a wide range of situations, demonstrated by the application in the design area as example.

### On Influence of the Structure of a Networked System on its Performances

Stefano La Rovere(a), Paolo Vestrucci(b)
*a) NIER Ingegneria, Bologna, Italy. b) Facoltà di Ingegneria - DIENCA Bologna, Italy*

We consider a Networked system made up of unfaultable “source” and “user” nodes and directed edges, subjected to failure and repair events. The influences of the Structure of the Network on its performances are investigated by adopting additive measures for the ranking of edges; these measures super-impose a ranking of the (unfaultable) user node. During the PSAM9 we defined the Partial and Global Risks of a Networked system and we proposed the ranking of the system’s elements by means of the Differential Importance Measure (DIM) [3], correctly referred to the Global Risk [12], [13]. In this paper, a so called “Hybrid measure” is introduced on the basis of the Normalized partial derivatives [7], [9]. It is defined with respect to the decomposition of the variance associated with the Global Risk, by including the correlations among the Partial Risks due to the Structure of the Network. It can be estimated without further information than ones used for the computation of DIM. The comparison between the two Measures clarifies the different meanings of Importance and Sensitivity ranking of edges and user nodes in the analysis of the Structure of a Networked system. Analytical evidences and an applicative case are provided.

3:30 - 5:00 PM

# 2-6: PSA Quantification

Session Chairs: David Johnson, Jim Knudsen

### BDD Application to the Calculation of Probability and Importance Measures of Minimal Cutsets

Woo Sik Jung(a), Jeff Riley(b), Ken Canavan(b)
*a) Korea Atomic Energy Research Institute. b) Electric Power Research Institute*

In order to calculate more accurate top event probabilities from cutsets, the ACUBE software was developed. ACUBE calculates a top event probability and importance measures from cutsets by (1) dividing cutsets into two groups, (2) calculating the major group (the higher cutset probability group) exactly, (3) calculating the minor group (the lower cutset probability group) with an approximate method such as Min Cut Upper Bound (MCUB), and (4) combining the two results. By applying the ACUBE algorithm to the PSA, the accuracy of a top event probability and importance measures can be significantly improved.

### An Approach to Evaluate Quantification Errors in PSAs

Jongsoo Choi
*Korea Institute of Nuclear Safety, Daejeon, Korea*

Probabilistic Safety Assessment (PSA) is increasingly being used to assess the level of safety of Nuclear Power Plants (NPPs). NPP PSA analyzes accident scenarios by event tree and fault tree techniques. However these techniques are not the only ones used in the PSA quantification. The NPP PSA quantification is a complicated process and always has the following two limitations: (1) approximation errors in quantifying Minimal Cut Sets (MCSs) and (2) truncation errors in deleting low-probability cut sets. In practice it is extremely difficult to exactly quantify PSA results without the approximation error and the truncation error. This paper proposes an approach to exactly quantify the risk measures of NPP PSAs using the proposed exact MCS quantification method applicable to largesized MCS problems and the iterative process of demonstrating that the convergence of risk measures can be considered sufficient. This paper also shows that the proposed approach is successfully applied to NPP PSAs.

### Estimating the Probabilities of Overlapping End States

Todd Paulos
*Alejo Engineering, Inc., Huntington Beach, CA, USA*

A practice commonly employed in Probabilistic Risk Assessments (PRAs) is to define mutually exclusive adverse end states. A difficulty sometimes encountered when quantifying such end states is that they cannot be uniquely defined by cut sets restricted solely to basic event failures, i.e., there will be basic events that contribute to both end states. As an example, consider a robotic mission with two critical science instruments. If the success criterion for the mission is that both critical instruments are necessary for satisfying science objectives, then failure of either or both instruments precludes a successful mission. Failure of both critical instruments leads to loss of mission, while failure of just one of the instruments results in an intermediate end state where some, but not all science objectives are satisfied. Quantification of such end states can be challenging in full scope PRAs where conventional, fault tree cut set software programs are used. This paper will demonstrate a methodology to solve for the quantitative values of overlapping end states from fault tree cut set PRA codes.

### The Model of Resilience in Situation (MRS) as an Idealistic Organization of At-Risks Systems to be Ultra Safe

Pierre Le Bot
*Electricité de France (EDF R&D), Clamart, France*

It is known that the safety of at-risks systems as Nuclear Power Plants can be improved by several competing approaches. The traditional safety engineering approach focuses on technical aspects of safety. The adverse events occurrence are prevented and their consequences limited by technical measures as the reliability of the components, material and organizational barriers as the procedures …The Human Factors approach focuses on the added value of human operation. It leads to improve the human machine interaction to optimize human activity in order to limit errors and inadequate operation. The safety management organizes the operation and its quality at the best and guarantees the professionalism of teams and individuals regarding safety by selecting, training, developing safety culture etc. For ultra safe at-risks systems, a traditional problem is the dilemma of operators for choosing between the strict application of the prescriptions and the optimization of the operation from their experience with their understanding of the situation in real time. Traditionally the answers of the cited approaches are opposite: technically the solution is to anticipate more by improving the procedures and by asking the operators to apply them strictly. At the opposite, human centered approaches will prone to trust the actors and to ask them to be aware of the situation and to use their adaptability, skills and competencies. We argue that this point is the keypoint of Human Reliability: by using an adequate model, Human Reliability can take into account both technical and human approaches. We have built such a model from an adaptation of Jean Daniel Reynaud’s Theory of Social Regulation. The two main characteristics of that model are a dynamic description of the system functioning and the necessary use of two opposite rationalities, the anticipating technical rationality on one hand, the flexible rationality of human collective on the other hand. The dynamic functioning of the team is based on the succession of phases of reconfiguration, where the system chooses rules to cope with the situation, and phases of stabilization where the system applies its rules.

# Human Reliability Analysis

**Tuesday, Salon C**

10:30 AM - Noon

## 5-4: Resilience and Use of Data

Session Chair: Helene Pesme

### The Method for Estimation of Human Error Probability

Kenji Yoshimura, Kenjiro Hikida, Hiroko Itoh, Chihiro Nishizaki, and Nobuo Mitomo
*National Maritime Research Institute, Tokyo, Japan*

Estimation of a Human Error Probability (HEP) is an essential element to assess risks. Our target in this research is establishing a systematized technique to obtain necessary information to estimate HEP. We aim at developing a systematic approach to human factors with the simulator and experiment scenarios designed rationally by examining into about 6,860 maritime accidents. Those scenarios designed are set after due deliberation on reports of maritime accidents in Japanese waters, which had been investigated by the Maritime Accident Inquiry Agency of Japan from 1990 to 2007. We created a database in which position, time, type of ships, ships movement, and cognitive condition are itemized at each accident. All accidents are then classified into cases by the cognitive condition. In each case, typical and critical items were chosen to contribute to experiment scenarios. Factors which might complicate scenarios were eliminated rationally by this process. This paper outlines the development of the experiment and the experimental outcome. Experienced navigation officers participated in the experiments as subjects and they took duties as usual in the simulator. We will present details of the experiment scenarios and HEP obtained from experiments done by the simulator, as a result of this research.

### Bridging Resilience Engineering and Human Reliability Analysis

Ronald L. Boring
*Idaho National Laboratory, Idaho Falls, Idaho, USA*

There has been strong interest in the new and emerging field called resilience engineering. This field has been quick to align itself with many existing safety disciplines, but it has also distanced itself from the field of human reliability analysis. To date, the discussion has been somewhat onesided, with much discussion about the new insights afforded by resilience engineering. This paper presents an attempt to address resilience engineering from the perspective of human reliability analysis (HRA). It is argued that HRA shares much in common with resilience engineering and that, in fact, it can help strengthen nascent ideas in resilience engineering. This paper seeks to clarify and ultimately refute the arguments that have served to divide HRA and resilience engineering.

### Development of a Questionnaire for Characterization of an Emergency Operation System: Application to Emergency Operating Procedures

Jonghyun Kim(a), Luca Podofillini(a), and Pierre Le Bot(b)
*a) Paul Scherrer Institute, 5232, Villigen, Switzerland. b) EDF R&D, Industrial Risk Management Department, 1 avenue du General de Gaulle, Clamart,France*

This paper presents recent efforts to characterize emergency operation systems (EOSs) of nuclear power plants, carried out in a collaboration between Électricité de France (EDF) and the Paul Scherrer Institute (PSI), Switzerland. The term EOS broadly refers to the system consisting of personnel, human-machine interface (including its automated/computerized aspects), procedures, and to the way the interactions among these elements are organized to prevent and respond to incidents and accidents. This paper presents 1) a high-level characterization questionnaire for the overall EOS, based on EDF's Model of Resilience in Situation and 2) a detailed questionnaire specific for emergency operating procedures. An application to the Emergency Operating Procedures of a Boiling Water Reactor plant is presented. Examples of situations are given that may stress the EOS and reveal potential EOS strengths and weaknesses, based on the identification of key procedure features.

### Calibration of PROCOS using Bayesian Networks

Massimiliano De Ambroggi, and Paolo Trucco
*Politecnico di Milano, Department of Management, Economics and Industrial Engineering, Milan, Italy*

PROCOS [9] is a probabilistic cognitive simulator aiming at supporting human reliability analysis in complex operational contexts. The paper proposes the development of a new calibration procedure in order to better use field data for shaping the relationship function between Performance Shaping Factors (PSFs) and HEP for each operator's cognitive process. In particular, the use of Bayesian Belief Networks (BBNs) is investigated. Starting from the HERA dataset, the number of occurrences has been expanded in a consistent way in order to have a larger quasi-real database. The trial application of the novel procedure to the calibration of five decision blocks of the PROCOS cognitive model showed a good approximation with a logistic function, in accordance with previous literature on the matter [2]. The research methodology allowed for tuning and qualitatively validating the new calibration procedure even though the final results of the entire simulation process are biased by the use of quasi-real data. When, in the near future, a more populated and consistent incident reporting database might be available, a complete validation of the method and the assessment of its accuracy will be also possible.

1:30 - 3:00 PM

## 5-5: Human Behavior and Disaster Response I

Session Chairs: Jeff Julius, Susan Cooper

### Overview of the Joint EPRI/NRC-RES Fire Human Reliability Analysis Guidelines Project

Susan Cooper(a), Kendra Hill(a), Stacey Hendrickson(b), John Forester(b), Jeffrey A. Julius(c), Jan Grobbelaar(c), Kaydee Kohlhepp(c), Bill Hannaman(d), Erin Collins(d), Bijan Najafi(d), and Stuart R. Lewis(e)
*a) U.S. Nuclear Regulatory Commission, Rockville, MD, USA. b) Sandia National Laboratories, Albuquerque, NM, USA. c) Scientech, a Business Unit of Curtiss-Wright Flow Control Company, Tukwila, WA, USA. d) SAIC, Campbell, CA, USA. e) Electric Power Research Institute, Charlotte, NC, USA*

In 2007, the Electric Power Research Institute (EPRI) and the U.S. Nuclear Regulatory Commission's (NRC's) Office of Nuclear Regulatory Research (RES) embarked upon a cooperative project to develop explicit guidance for estimating probabilities for human failure events under fire-generated conditions. This collaborative project produced draft NUREG-1921, "EPRI/NRC-RES Fire Human Reliability Analysis Guidelines." The guidance presented in this report is intended to be both an improvement upon and an expansion of the initial guidance provided in a previous collaborative effort, NUREG/CR-6850 (EPRI 101989) [1], "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities." This paper summarizes the fire human reliability analysis (HRA) guidance developed through this project, which addresses fire-specific influences on crew performance (e.g., use of fire procedures; misleading indications due to fire-induced instrument failures, electrical spurious actuations; smoke, heat and other fire-induced hazards). The guidance includes: 1) process steps for performing HRA, 2) discussion and tools for performing qualitative HRA tasks, and 3) a three tiered, progressive approach for fire HRA quantification. The three quantification approaches consist of: a screening approach per NUREG/CR- 6850 guidance, a scoping approach, and detailed quantification using either EPRI's Cause-Based Decision Tree (CBDT) and Human cognitive Reliability/Operator Reliability Experiment (HCR/ORE) [7] or NRC's A Technique for Human Event ANAlysis (ATHEANA) [8] approach with modifications to account for fire effects. This paper is one of four PSAM 10 papers providing an overview and insights into the recently published draft EPRI/NRC Fire HRA guidelines. The second paper provides additional details into the new scoping method developed by the NUREG. The final two papers provide insights and lessons learned from the application of the new Fire HRA methods in developing Fire PRA models undergoing transition of their fire protection program to NFPA-805.

### EPRI/NRC Fire HRA Guidelines: Introduction to Fire HRA Scoping Quantification

Stacey M. L. Hendrickson(a), John Forester(a), Susan Cooper(b), Kendra Hill(b), Jeffrey A. Julius(c), Jan Grobbelaar(c), Kaydee Kohlhepp(c), Bill Hannaman(d), Erin Collins(d), and Bijan Najafi(d)
*a) Sandia National Laboratories, Albuquerque, NM, USA. b) U.S. Nuclear Regulatory Commission, Rockville, MD, USA. c) Scientech, Tukwila, WA, USA. d) SAIC, Campbell, CA, USA*

The fire human reliability analysis (HRA) guidelines [1] developed jointly by the Electric Power Research Institute (EPRI) and the U.S. Nuclear Regulatory Commission (NRC) are intended as explicit guidance for identifying, modeling and quantifying human failure events under fire-generated conditions. A three tiered approach to quantification is offered including a screening level similar to that presented in NUREG/CR-6850 [2], a new scoping fire HRA quantification approach, and two detailed HRA quantification approaches. This paper introduces the new scoping fire HRA quantification method. This new scoping approach offers a mid-level quantification option that is less resource intensive than a full, detailed analysis and offers less conservative human error probabilities (HEPs) compared to the screening approach. The scoping fire HRA quantification approach is based on the use of flowcharts directing the analyst to the correct HEPs based on assessment of key performance shaping factors. The process includes a demonstration of feasibility and an assessment of the available time margin for completing the action(s) in question. This paper is one of four PSAM 10 papers providing an overview and insights into the recently published draft EPRI/NRC Fire

HRA guidelines.

### Lessons Learned from Fire HRA Applications

Erin P. Collins(a), Pierre Macheret(b), Paul Amico(c), and G. William Hannaman(d)
*a) SAIC, New York, NY, USA. b) SAIC, Las Vegas, NV, USA. c) SAIC, Abingdon, MD, USA. d)SAIC, San Diego, CA, USA*

This paper discusses the insights gained from the application of the EPRI/NRC Fire HRA Guidelines to recent Fire PRA/HRA projects and the consideration of issues specific to NFPA 805 transition projects that include Fire PRA/HRA.

### EPRI/NRC Fire HRA Guidelines: Lessons Learned During Applications

Jeffrey A. Julius, Jan Grobbelaar, and Kaydee Kohlhepp
*Scientech, a Business Unit of Curtiss-Wright Flow Control Company, Tukwila, WA, USA*

The fire human reliability analysis (HRA) guidelines [1] developed jointly by the Electric Power Research Institute (EPRI) and the U.S. Nuclear Regulatory Commission (NRC) are intended as explicit guidance for identifying, modeling and quantifying human failure events under fire-generated conditions. A three tiered approach to quantification is offered including a screening approach similar to that presented in NUREG/CR-6850 [2], a new scoping fire HRA quantification approach, and two detailed HRA quantification approaches based on existing methods [3, 4]. This paper discusses the lessons learned and insights gained from the development of the draft EPRI/NRC Fire HRA Guidelines and the subsequent application of these guidelines to recent Fire PRA/HRA projects, including the consideration of issues specific to NFPA 805 transition projects that include Fire PRA/HRA. This paper is one of four PSAM 10 papers providing an overview and insights into the recently published draft EPRI/NRC Fire HRA Guidelines. The first two papers provide a general overview of the Fire HRA Guidelines project and additional details describing the new scoping method developed by the NUREG. The final two papers provide insights and lessons learned from the application of the new Fire HRA methods in developing Fire PRA models undergoing transition of their fire protection program to NFPA-805.

3:30 - 5:00 PM

## 5-6: Dynamic Approaches

Session Chairs: James Chang, Dana Kelly

### Dynamic Probabilistic Risk Assessment Model Calibration and Validation Using Simulator Data - Another Application of HRA Empirical Study Data

Kevin Coyne(a) and Ali Mosleh(b)
*a) U.S. Nuclear Regulatory Commission, Washington D.C., USA. b) University of Maryland Center for Risk and Reliability, College Park, MD, USA*

The recent International Human Reliability Analysis (HRA) Empirical Study has provided an excellent opportunity to calibrate and validate a number of probabilistic risk assessment tools and methods (PRA). In particular, the unique combination of detailed plant thermal-hydraulic data and human performance information arising from this simulator-based empirical study has proved to be very useful for the calibration and initial validation of the Accident Dynamics Simulator paired with the Information, Decision, and Action in a Crew context cognitive model (ADS-IDAC) dynamic PRA method. The ADS-IDAC environment couples a thermal-hydraulic model with a crew cognitive model to permit the dynamic simulation of operator performance during nuclear power plant accidents. ADS-IDAC generates a discrete dynamic event tree using simple branching rules to model variations in crew responses. This paper describes the recent validation efforts used to demonstrate the utility of ADS-IDAC for the analysis of human performance issues during nuclear power plant accidents. A general approach for modeling sources of crew-to-crew variabilities for postulated accident scenarios is described. This general method is applied to the loss of feedwater (LOFW) HRA empirical study scenarios in order to predict potential human error events. A comparison of the ADSIDAC predictions to the actual empirical study results is presented, along with insights regarding recalibration of the dynamic model. This process has not only resulted in significant improvements in the capabilities of the ADS-IDAC model but also demonstrated methods for capturing the rich data obtained from empirical simulator-based studies.

### Dynamic Human Reliability Method in Seismic PSA for Multi-Unit-Site

Tadakuni Hakata(a), Keiko Hasegawa(b), Akihiko Endo(c) and Sadanori Aoi(c)
*a) TH Consulting, 6-17-4 Matsubara Setagaya-ku Tokyo 156-0043, Japan. b) Mitsubiishi Heavy Industries, LTD., 2-16-5 Konan Minato-ku Tokyo 108-8215, Japan. c) MHI Nuclear Engineering Company. LTD., 3-1 Minatomirai 3-Chome, Nishi-ku,Yokohama 220-8401, Japan*

This paper presents a new dynamic HRA method for operators' human error probability (HEP) to be used in seismic PSA for nuclear power plants. The model consist of a base-line HEP as a function of accelerations of earthquakes as the general effects and an additional terms which take into consideration the various effects on HEPs depending on various divert reactor plant status, such as the number of initiating events occurred and number of important mitigating safety system failures, and the effects of simultaneous occurrence of accidents in the other units in the same site. The effects on HEPs are determined at each sampling run in PSA by Monte Carlo method. HEPs are assigned using the SPAR-H HRA method, which uses performance shaping factors (PSF) for diagnosis and operator actions due to allowable time, stress, complexity, work process, etc. Trial sample PSAs of Level-1 and Level 1.5 (containment failure modes assessment) for a typical four PWR plants site were conducted using a Monte Carlo seismic PSA code, CORAL-reef, in which the proposed HEP model is included. This study will contribute to refinement of HRA for seismic event PSA.

### Use of Dynamic Event Trees to Model Variability in Crew Time Performance

D. Mercurio and V.N. Dang
*Paul Scherrer Institut, Villigen PSI, Switzerland*

One motivation for the joint operator-plant simulation of complex systems is to be able to analyze the impact of the variability in the time performance of tasks on the evolution of accident sequences. In addition, such simulations may also support Human Reliability Analysis by providing information on the plant indications seen by the operators over time, which in turns depends on when the tasks are performed. This paper deals with the modeling of crew time performance variability within Dynamic Event Tree simulations. An analysis of a set of time performance data from a simulator study confirms that there is some correlation among the performances of a series of tasks, as could be expected. The paper describes an approach for treating this correlation by grouping the performances in terms of tendencies. The results show that this approach based on crew tendencies is able to accurately reproduce the probabilities of the outlier time performances for the overall task. These are the lower-probability responses that may be particularly relevant for safety. An application of this approach to a scenario using the Accident Dynamic Simulator (ADS) dynamic event tree model is also shown.

# PSA Applications

**Tuesday, East Room**

10:30 AM - Noon

## 1-4: Test and Research Reactor PSA Applications

Session Chairs: Martin Sattison, Bentley Harwood

### Feasibility Study to Develop a PSA Study for the Jules Horowoitz Research Reactor

A. Laborde, G. Georgescu, F. Cocheme and JM. Lanore
*Institute for Radiological Protection and Nuclear Safety (IRSN), Fontenay aux Roses, France*

In France a new research reactor is under construction at the Cadarache site. The Jules Horowitz Reactor (RJH) will be a major infrastructure of European interest in the fission sphere, open to international collaboration. Today a PSA is not requested for the licensing of the RJH, but IRSN, as the ASN (French Safety Authority) technical support, is interested in developing such study as a complementary safety assessment tool. Past experience has shown that the development and the use of PSA during the design stage, even with incomplete data, is beneficial and sometimes can be mandatory to have a well balanced design. Furthermore, a PSA could be a useful tool to make the dialogue easier amongst the different organizations involved in the RJH project. In this context, IRSN developed, as a preliminary step, a feasibility study for a Level 1 PSA of research reactors, and particularly for RJH.

### Advanced Test Reactor Probabilistic Risk Assessment Upgrade and Modeling – INL/CON-09-16803

Bentley Harwood and Richard Yorg
*Idaho National Laboratory, Idaho Falls, United States*

This paper describes the Probabilistic Risk Assessment (PRA) upgrade activities associated with the Advanced Test Reactor (ATR). The ATR, located at the Idaho National Laboratory (INL), is a low pressure, low temperature, 250 MWth pressurized water reactor using aluminum clad fuel in a serpentine arrangement. The reactor con-

tains several types of experiment facilities in flux traps and in the reflector region. The serpentine fuel element layout creates nine flux traps, five of which house an experiment loop that is capable of simulating commercial power reactor conditions. Digital distributed control systems are used to monitor and control plant and equipment parameters. Reactivity and shutdown of the ATR are controlled through safety rods, automatic regulating rods, neck shim rods, and outer control cylinders. These features also allow core power to be high in one lobe and low in another lobe. Power sources on some equipment are selectable from commercial to diesel power. The ATR PRA was originally developed in the late 1980s through the early 1990s. The ATR PRA upgrade activities were initiated in 2006 to incorporate various completed plant modifications into the PRA model. Early in the upgrade it was determined to be most cost effective and efficient to develop a fresh PRA model using the existing model as a basis where appropriate. The upgrade effort used several analysts in various locations. The resulting twenty-two independent primary and support system models (which are maintained for future updates) are then combined to form the ATR PRA. Combining the system models requires the use of external data files to facilitate merging, and these files also allow consistent maintenance of model as reactor operating states and other initial conditions change. Hence, the current reactor configuration can be quickly applied and reanalyzed at any time. The upgraded PRA, when completed, will be able to model the plant in any configuration during any operating state. The resulting model will support real-time operational risk monitoring, risk informed maintenance, inspections, and other reliability studies. Recent results of the PRA have caused heavy load drop calculations to be re-evaluated. The results of these calculations will streamline load handling activities during all plant operating states and will likely allow postulating less plant damage for each load drop event. PRA input is expected to be used in the authorization process for performance of on-line maintenance activities.

### Probabilistic Safety Assessment of Esfahan HWZPR

Sepanloo Kamran(a), Ziyarati Davood(b)
*a) Iran Nuclear Regulatory Authority, Tehran,Iran. b) Islamic Azad University,Tehran,Iran*

Nowadays, Probabilistic Safety Analysis (PSA) is used for most of 370 nuclear power plants and 300 research reactors around the world. PSA is a complete and well-structured method for determination of accident scenarios and quantitative estimation of the risk of reactors. By providing corrective safety measures based on the PSA results the operational safety is considerably improved. In the present paper, the results of application of PSA method to Heavy Water Zero Power Reactor (HWZPR) which is a research reactor located in Esfahan, Iran, are presented. The model developed is calculated using computer code SAPHIRE. The core damage frequency is about 1.625E-7. Operator error is recognized as the most important factor in the overall core damage causes. The calculation results are compared with the similar analysis results for Tehran Research Reactor. The analysis is performed according to International Atomic Energy Agency (IAEA) procedures.

1:30 - 3:00 PM

## 1-5: Unique Risk Contexts: Design and Shutdown

Session Chairs: Ari Julin, Peter Swift

### Use of Risk Informed Approach in Design, Construction and Commissioning of OL3 EPR

Ari Julin, Jouko Marttila, Reino Virolainen and Lasse Reiman
*Radiation and Nuclear Safety Authority (STUK), Helsinki, Finland*

The risk informed approach has been applied in several areas during the design and construction of OL3, e.g. supporting the detailed design of SSCs, definition of pre-service and inservice inspection programs, evaluation of the safety classification of SSCs, development of procedures, training and in definition of risk informed technical specifications, periodic testing and online preventive maintenance programs. Risk insights have led to several modifications to the original EPR design. In addition to the internal events PRA, internal and external hazard analyses provided useful insights to ensure that the site specific concerns and environmental conditions are adequately taken into account in the design. The results of various OL3 PRA applications are presented and main insights are briefly discussed. In OL3 project, risk informed approach has been applied in a large scale for the first time in the design, construction and commissioning of a new NPP unit. Experiences from OL3 licensing have been utilized in the further development of risk informed requirements in Finland.

### Improvement of Shutdown PSA Model and Examination of New Practical Application of Risk Monitor

Hiroshi Abe, Issei Hidaka, Suguru Kobayashi, Naoki Hirokawa, Mitsuru Yoneyama
*TEPCO SYSTEMS CORPORATION, Tokyo, Japan*

This paper describes the improvement of shutdown PSA model in order to assess core damage frequency (CDF) of various plant configurations during refueling outage schedule. Additionally, as a part of application of risk information, risk monitors have been sequentially introduced into some Japanese nuclear power stations and are utilized to improve decision-making for operation and maintenance management. Since it is expected that risk monitor will afford the key to expanding the application of risk information in Japanese nuclear power plants, new practical application of risk monitor were examined in this paper.

### Development of Probabilistic Risk Assessment Model for BWR Shutdown Modes 4 and 5 Integrated in SPAR Model

S. Khericha(a), S. Sancaktar(b), J. Mitman(b), J. Wood(b)
*a) Idaho National Laboratory, Idaho Falls, ID, USA. b) U.S. Nuclear Regulatory Commission, Washington DC, USA*

Nuclear plant operating experience and several studies show that the risk from shutdown operation during modes 4, 5, and 6 can be significant in commercial light water reactors. This paper describes development of the standard template risk evaluation models for shutdown modes 4 and 5 for commercial boiling water nuclear power plants (BWR). The shutdown probabilistic risk assessment model uses full power Nuclear Regulatory Commission's (NRC's) Standardized Plant Analysis Risk (SPAR) model as the starting point for development. The shutdown PRA models are integrated with their respective internal events at-power SPAR model. This is accomplished by combining the modified system fault trees from SPAR full power model with shutdown event tree logic. For human reliability analysis (HRA), the SPAR HRA (SPAR-H) method is used which requires the analysts to perform a task analysis and complete worksheet to assign the performance shaping factors (PSFs). The results are then used to estimate HEP of interest. The preliminary results indicate the risk is dominated by the operator's ability to diagnose the events and provide long term cooling.

### Probabilistic Risk Assessment of NuScale Reactor During the Design Phase

Kent B. Welter(a), Ross Snuggerud(a), Jason Pottorf(a), Mohammad Modarres(b), Inn S. Kim(c)
*a) NuScale Power, Inc., Corvallis, OR, USA. b) University of Maryland, College Park, MD, USA. c) International System Safety Analysis Technology, Inc., Germantown, MD, USA*

In this study, a probabilistic risk assessment (PRA) for the NuScale scalable modular reactor (SMR) has been performed to risk-inform the design and as a part of the effort for the preapplication licensing of this design. NuScale is a modular, scalable 45-MWe Light Water Reactor. Each NuScale module has its own combined high-pressure containment vessel and reactor steam supply system, and its own designated turbine-generator set. NuScale power plants are scalable, allowing for a single facility to have just one or up to 24 units. In a multi-module plant, one unit can be taken out of service without affecting the operation of the others. The NuScale PRA is supporting the design process by offering insights on the basis of the module and facility risk profile. The current PRA effort is preliminary and will help to inform the development of the more complete PRA analysis and documentation that will be required for a planned U.S. Design Certification. The initial PRA was performed for an at-power, Level-1 PRA for internal events, low power and shutdown, as well as internal fire and flood. To accomplish the evaluation, a reasonably complete Level-1 PRA model of a single model as well as risk significance of a multi-module plant was developed. The use of PRA in the early stages of the design process has led to the identification of severe accident events and appropriate design and performance features to enhance prevention and mitigation of the associated challenges. As a result, the total core damage frequency for the NuScale design has been estimated as 2.8×10−8 per year (excluding seismic risk).

### Probabilistic Risk Assessments for Nuclear Power Plants in Design: A Limited-Scope Literature Review

J. Wood, B. Wagner, K. Coyne, N. Siu
*U.S. Nuclear Regulatory Commission, Washington DC, USA*

A number of the technical challenges associated with pre-operational PRAs are quite clear to PRA analysts and users. In order to develop consensus standards requirements for pre-operational PRAs, or technical guidance to support these consensus standards, it is useful to review whether and how these challenges have been dealt with in past studies. This paper discusses the results of a limited-scope literature review performed to survey whether and how past, pre-operational PRAs for NPPs have addressed these challenges, and what additional challenges they have identified that may need to be addressed in future standards requirements and supporting guidance.

3:30 - 5:00 PM

## 1-6: Level 2 PSA

Session Chairs: Estelle Sauvage, Mike Calley

### Ringhals PWR PSA Level 2; A Description of Modifications in the Structure, Why and How

Ola Bäckström(a) and Cilla Andersson(b)
*a) Scandpower-Lloyd's Register, Stockholm, Sweden. b) Ringhals AB, Väröbacka, Sweden*

At Ringhals plant specific PSA level 2 models, that cover all plant operating modes, were developed for the PWRs several years ago. The structure has been built around the defined four phases, with at least one event tree – but often several – within each phase. The complexity with regard to the level 2 PSA is therefore high, and it has been found hard to review and quality assure the PSA model and its inputs. This paper is about a change in modelling strategy. The project also covered inclusion of the newly installed PAR units at Ringhals.

### Historical Perspectives and Insights on Nuclear Reactor Consequence Analyses

Hossein P. Nourbakhsh
*Office of Advisory Committee on Reactor Safeguards (ACRS), Nuclear Regulatory Commission, Washington, DC, USA*

The paper begins with an overview of major contributions to consequence assessment to provide historical perspectives and insights on previous state-of-the-art analyses of the consequences of severe reactor accidents. It then discusses how the results and insights from the NUREG-1150 study, together with recent advances in understanding of severe accident phenomenology and containment failure mechanisms, could be used to update the results of such earlier Level-3 PRAs for comparison with aspects of State-Of-the-Art Reactor Consequence Analyses (SOARCA) results.

### Generic Accident Progression Event Tree for Belgian Level 2 PSA

J. Van Dingenen, P. Dejardin, L. Oury, and L. Sallus
*Tractebel Engineering S.A., Brussels, Belgium*

Within the framework of the Western European Nuclear Regulators Association (WENRA) reference levels and the periodic safety review process an updated level 2 PSA study is performed by Tractebel Engineering S.A. (GDF SUEZ) (TE) for the seven Belgian Nuclear Power Plants (NPP), which are all of Pressurized Water Reactor type. Therefore a generic Accident Progression Event Tree (APET) is developed divided into two successive parts treating respectively the Containment Performance (CP-APET) and the source term or the release of fission products (FP-APET) for a representative range of severe accidents. The main improvements compared to previous level 2 PSA studies are the development of a generic APET instead of a specific one for each plant, including both power states and shutdown states in one APET and taking into account accident management actions, namely the Emergency Operating Procedures and the Severe Accident Management Guidelines. Additionally, the FP-APET consists of eight general user functions, which are modified volume-based XSOR-algorithms, each evaluating the amount and timing of the release of one of the radionuclides" classes from NUREG-1465, resulting in a schematic approach and an increased number of sequences evaluated during ST assessment.

# External Events

**Tuesday, West Room**

10:30 AM - Noon

## 15-4: Fire: Risk and Consequence Analysis 1

Session Chair: J. Hyslop

### Improved Treatment of Manual Suppression in Fire Probabilistic Risk Assessment

J. S. Hyslop(a), Steven P. Nowlen(b)
*a) U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Rockville, MD, USA. b) Sandia National Laboratories, Albuquerque, NM, USA*

The U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Reactor Regulation implemented a frequently asked questions (FAQs) program[1] to address issues related to the transition of pilot plants to the risk-informed, performance-based rule 10 CFR 50.48(c) partially endorsing National Fire Protection Association Standard 805. In this program, the NRC and industry are resolving questions related to both prescriptive fire protection and fire probabilistic risk assessment (PRA). These fire PRA FAQs span much of the field, addressing fire ignition frequencies and the counting of components, aspects of fire damage assessments from high-energy bus duct faults and large oil fires in main feedwater pumps, manual suppression, and electrical circuit hot short evaluations. This paper will focus on the interim solution of the fire PRA FAQ on manual suppression[2]. This FAQ modifies the approach put forth in NUREG/CR-6850 (EPRI 1011989) by allowing greater credit to early suppression by nuclear power plant personnel, beyond the full fire brigade credited in NUREG/CR-6850.

### Fire-Induced Failure Mode Testing for DC-Powered Control Circuits

Steven P. Nowlen(a), Gabriel Taylor(b), Jason Brown(a)
*a) Sandia National Laboratories, Albuquerque NM, USA. b) U.S. NRC Office of Nuclear Regulatory Research, Washington DC, USA*

The U.S. Nuclear Regulatory Commission, in concert with industry, continues to explore the effects of fire on electrical cable and control circuit performance. The latest efforts, which are currently underway, are exploring issues related to fire-induced cable failure modes and effects for direct current (dc) powered electrical control circuits. An extensive series of small and intermediate scale fire tests has been performed. Each test induced electrical failure in copper conductor cables of various types typical of those used by the U.S. commercial nuclear power industry. The cables in each test were connected to one of several surrogate dc control circuits designed to monitor and detect cable electrical failure modes and effects. The tested dc control circuits included two sets of reversing dc motor starters typical of those used in motor-operated valve (MOV) circuits, two small solenoidoperated valves (SOV), one intermediate size (1-inch (25.4mm) diameter) SOV, a very large directacting valve coil, and a switchgear/breaker unit. Also included was a specialized test circuit designed specifically to monitor for electrical shorts between two cables (inter-cable shorting). Each of these circuits was powered from a nominal 125V battery bank comprised of 60 individual battery cells (nominal 2V lead-acid type cells with plates made from a lead-cadmium alloy). The total available short circuit current at the terminals of the battery bank was estimated at 13,000A. All of the planned tests have been completed with the data analysis and reporting currently being completed. This paper will briefly describe the test program, some of the preliminary test insights, and planned follow-on activities.

### Development of a 3D Risk Analysis Technique for Fire Disaster and Its Application on Accident Simulation of a Public Site

Yet-Pole I and Yi-Hao Huang
*Department of Safety, Health and Environmental Engineering, National Yunlin University of Science and Technology, Douliou, Taiwan*

This research constructs a three-dimensional fire risk analysis technique (3D-FRAT) for common building fires. In order to demonstrate its effect, the 3D-FRAT employed a self-developed 3D risk-calculating module in combination with the FDS software to simulate the Welcome Restaurant accident happened in Taiwan. Different firefighting facilities that comply with the related building and fire-preventive laws have been used in the simulations to test their mitigating effectiveness on the accident. The study applied the parameters of temperature, CO, and O2 concentration simulated by FDS to calculate the personal death probability and individual risk. The results were shown by-animation, 3D pictures, and sliced pictures to facilitate the researchers' understanding of human hazards caused by thermal radiation or smoke in a specific fire accident. The minimal personnel-escaping times for different hazardous factors were estimated; various firefighting designs that can reduce loss of human life and property were also discussed. According to the simulation results, the individual risk values in Welcome Restaurant were between 3.108×10-9 to 2.719×10-5 (persons/year). It is foreseeable that the 3D-FRAT can provide the related organizations a useful tool for choosing a better fireproofed building or fire-fighting equipment in the future.

1:30 - 3:00 PM

## 15-5: Fire: Risk and Consequence Analysis 2

Session Chair: Ray Gallucci

### Burn-down Risk of Historical Buildings in Kyoto Under an Expected Post-Earthquake Fire Scenario

Keisuke Himoto, Tomoki Yukimoto, and Takeyoshi Tanaka
*Kyoto University, Uji, Japan*

Burn-down risk of historical buildings in Kyoto city under an expected post-earthquake fire scenario was evaluated. The scenario assumes fire to be initiated in the vicinity of a historical building soon after the seismic motion. Following this, the fire spreads

through the urban area and may reach to the target historical building depending on the city structure of the neighborhood. In this study, shift of "Hanaore Fault" laid in the north-eastern part of the city area was assumed as the cause of earthquake. Probability of outbreaks of fire was estimated by a correlation obtained from the record of 1995 Kobe Earthquake. Simulation of fire spread following the outbreak was conducted by a physics-based model formerly developed by the authors. As a result of the analysis, burn-down risks of designated "Important Cultural Properties – Buildings and Structures" at 63 sites in Kyoto city were obtained.

### Gentilly-2 CANDU Nuclear Power Plant level 1 Fire and Flood PSA – Insights on a Work in Progress

K. Joober(a), C. Selman(a), J-F. Bolduc(a), A. Nava Dominguez(a) , A. Bellil(a), T. Houasnia(b), R.Vaillancourt(b)
*a) GENIVAR LP, Montréal, Québec, Canada. b) Hydro-Québec, Montréal, Québec, Canada*

The objective of this report is to present a summary of work performed to date on the Level 1 Internal Fire and Flood PSA for the Hydro-Québec Gentilly-2 CANDU Nuclear Power Plant. The overview will present findings, observations, challenges, and solutions that have been developed to supplement the NUREG/CR-6850 and EPRI-1019194 methodologies.

### Smoke-Induced Failure, with Potential Effect of Temperature and Humidity, of Electrical Devices for Consideration in Fire Probabilistic Risk Assessment

Raymond H.V. Gallucci
*U.S. Nuclear Regulatory Commission (USNRC), MS O-10C15, Washington, D.C. USA*

With the issuance of 10CFR50.48(c), the USNRC opened the door for nuclear power plant licensees to transition their traditional, deterministic fire protection programs to ones that are risk-informed and performance based. To date, half the commercial fleet have committed to this transition, which includes updates to existing fire PRAs using the latest technologies, which continue to evolve. While there have been technical advances in fire PRA modeling, predicting the likelihood of damage to electrical components due to smoke effects has remained essentially dormant for 20 years since the original research in the 1980s by NASA, followed USNRC-sponsored testing in the early 1990s. Even today, the prediction of smoke-induced damage to electronic equipment relies on a probabilistic failure model developed in a 1990 doctoral thesis, which is still cited in Volume II, "Fire Protection," of DOE HDBK-1062-96. In an effort to resurrect examination of this phenomenon, this paper combines the limited quantitative information available into a preliminary, simplistic model for the probability of failure of a solid state electrical device due to smoke exposure, with an option to incorporate the potential synergistic effects of temperature and humidity. Results are preliminary and likely conservative, so it is recommended that any such considerations in fire PRA applications be limited to sensitivity analyses.

3:30 - 5:00 PM

## 15-6: Fire: Data Analysis

Session Chairs: Patrick Baranowsky, Marina Roewekamp

### The OECD Fire Database and its Applicability in Fire PSA

Marina Röwekamp(a), Wolfgang Werner(b), and Alejandro Huerta(c)
*a) Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, Germany. b) Safety Assessment Consulting (SAC), Breitbrunn, Germany. c) OECD/NEA, Paris, France*

The objectives of the OECD FIRE Project include the establishment of a database containing information supportive to fire risk assessment. From the Database insights can be obtained into the root causes of fire events which can then be used to develop approaches or mechanisms for their prevention or mitigation of their consequences. The Project exchanges fire events data covering all operational modes, including construction and decommissioning, of commercially operated nuclear power plants. Currently, the OECD FIRE Database contains 365 fire events. Review of the Database fire events indicates that fires are most likely to occur in the turbine building and in process rooms. This is consistent with observations from IRS and INES databases. A large majority of fires could be confirmed within a few minutes. In more than 85 % of the events, manual fire fighting means were involved in fire suppression. Only one fire was suppressed by automatically actuated fixed systems alone. The percentage of self-extinguished fires and fires terminated by fire source isolation is significant. The positive effects of human intervention on fire extinguishing are demonstrated. The OECD FIRE Database is becoming large enough to estimate room or component based fire initiator frequencies. Also, event trees derived from the collected data are presented and a proposal is made for estimating component based fire initiator frequencies from information in the OECD FIRE database.

### Database for a Comprehensive Fire PSA

Marina Röwekamp(a), Michael Türschmann(b), Michael Schwarz(c), and Heinz Peter Berg(d)
*a) Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, Germany. b) Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Berlin, Germany. c) EnBW Kernkraftwerk GmbH, Kernkraftwerk Philippsburg, Philippsburg, Germany. d) Bundesamt für Strahlenschutz, Salzgitter, Germany*

To perform a state-of-the-art Fire PSA it is essential to establish and apply a comprehensive database in a well structured and easily traceable manner. A thoroughly investigated database is able to assist by means of its implemented functions data examination, preparation, analysis and application as well as the review of a Fire PSA. For performing Fire PSA for full power plant operational states (FP) as well as for low power and shutdown states (LP/SD) different needs have to be fulfilled by the database. This requires either two separate databases or a common more complex one. The methodology for performing systematically a Fire PSA is subdivided into the following tasks: In a first step, a meaningful plant partitioning in compartments (plant compartmentation) is necessary. This is followed by the compartment related evaluation steps, including determination of fire occurrence frequencies, quantification of fire damage probabilities and evaluation of fire induced core damage frequencies. For each task it has to be analyzed where additional information is needed to be implemented in the database for performing a Fire PSA LP/SD compared with a Fire PSA FP. As a suitable example, the database having been developed in the frame of the Fire PSA performed for a German nuclear power plant with BWR is used.

### Insights from Using the Fire Modeling Database in Fire PRAs

Francisco Joglar, Guy Ragan, Mark Graham, Brian Downey, Josh Fox
*SAIC, Reston, U.S.A.*

A relational database application, the Fire Modeling Database (FMDB), has been developed to support fire analysis and quantification tasks for fire probabilistic risk assessment (FPRA). Supported tasks include plant partitioning, estimation of fire ignition frequencies, scoping fire modeling, detailed fire modeling, and risk quantification. The database stores and maintains an FPRA equipment list, a list of ignition sources, detection/suppression information, fire scenarios with associated targets, etc. The database can generate formatted reports, e.g., severity-factor analysis for documenting scoping fire modeling tasks. It also produces output data for fire damage and frequency at the compartment and scenario levels for input to CAFTA/FRANX or other FPRA quantification tools. The purpose of this paper is to summarize insights gained in the use and maintenance of the FMDB in an FPRA. This paper addresses efficient compilation of data and population of the FMDB and provides insights on using and modifying the database gained by use of the FMDB in a specific plant FPRA.

### Enhanced Fire Events Database to Support Fire PRA

Patrick Baranowsky(a), Ken Canavan(b), and Shawn St. Germain(c)
*a) ERIN Engineering and Research, Inc., Bethesda, USA. b) Electric Power Research Institute, Charlotte, USA. c) Idaho National Laboratory, Idaho Falls, USA*

This paper provides a description of the updated and enhanced Fire Events Data Base (FEDB) developed by the Electric Power Research Institute (EPRI) in cooperation with the U.S. Nuclear Regulatory Commission (NRC). The FEDB is the principal source of fire incident operational data for use in fire PRAs. It provides a comprehensive and consolidated source of fire incident information for nuclear power plants operating in the U.S. The database classification scheme identifies important attributes of fire incidents to characterize their nature, causal factors, and severity consistent with available data. The database provides sufficient detail to delineate important plant specific attributes of the incidents to the extent practical. A significant enhancement to the updated FEDB is the reorganization and refinement of the database structure and data fields and fire characterization details added to more rigorously capture the nature and magnitude of the fire and damage to the ignition source and nearby equipment and structures.

# Safety Culture & Organizational Factors

**Tuesday, North Room**

10:30 AM - Noon

## 9-4: Socio-technical Modeling II

Session Chair: Zahra Mohaghegh

### The Highly Reliable Resilient Organization Methodology: Incorporating Organizational and Managerial Factors in the Assessment of Organizational Vulnerability

Joseph F. Gifun, Dimitrios M. Karydas
*Eindhoven University of Technology, Eindhoven, The Netherlands*

The intent of this paper is to present to leaders of organizations and other decision makers within organizations a methodology to assist in understanding the vulnerability their organizations face each day and provide the means to eliminate or mitigate these vulnerabilities in a consistent, systematic, and most importantly, a preemptive manner. The Highly Reliable Resilient Organization (HRRO) methodology was developed for this purpose and it specifically focuses on assessing the aspects of an organization that provide the foundation for the organization's core function; its culture, its ability to manage risk, and its governing processes. The HRRO methodology is a multi-attribute analytic-deliberative process that provides the means to 1) assess vulnerability preemptively as a way to determine the proposed effect of the implementation of a proposed mitigation project or initiative under consideration, 2) assess vulnerability correctively, i.e. post impact to determine its effect on the organization, 3) prioritize proposed mitigation projects or initiatives using criteria determined by the organization's stakeholders, and; 4) include the cost of risk avoidance with non-monetary criteria in benefit-to-cost analyses The HRRO methodology can be applied to any organization; however, as the criteria, criteria definitions, constructed scales, and weights are specific to an organization customization is necessary.

### Integrating System Dynamics and Bayesian Networks with Application to Counter-IED Scenarios

KD Jarman, AJ Brothers, PD Whitney, J Young, DA Niesen
*Pacific Northwest National Laboratory, Richland, WA, USA*

The practice of choosing a single modeling paradigm for predictive analysis can limit the scope and relevance of predictions and their utility to decision-making processes. Considering multiple modeling methods simultaneously may improve this situation, but a better solution provides a framework for directly integrating different, potentially complementary modeling paradigms to enable more comprehensive modeling and predictions, and thus better-informed decisions. The primary challenges of this kind of model integration are to bridge language and conceptual gaps between modeling paradigms, and to determine whether natural and useful linkages can be made in a formal mathematical manner. To address these challenges in the context of two specific modeling paradigms, we explore mathematical and computational options for linking System Dynamics (SD) and Bayesian network (BN) models and incorporating data into the integrated models. We demonstrate that integrated SD/BN models can naturally be described as either state space equations or Dynamic Bayes Nets, which enables the use of many existing computational methods for simulation and data integration. To demonstrate, we apply our model integration approach to technosocial models of insurgent-led attacks and security force counter-measures centered on improvised explosive devices.

### A Paired Comparison Approach to Quantify Management Influences on Risk (II)

Pei-Hui Lin, A.R. Hale, B.J.M. Ale
*Safety Science Group, Delft University of Technology, The Netherlands*

In a previous research, we developed a quantification method to eliminate some deficiencies of current quantification techniques used for safety management. The approach used paired comparison expert judgments to differentiate a set of management influences to reduce human or technical failure, and quantify the size of different management influences on risk by combining it with BBN, Fault tree (FT), and Event Sequence Diagram (ESD). However, the human or technical factors in the previous research are generally formulated with measurable units for quantification purpose. In this paper, we discuss whether we can model a relatively "soft" human factor in the BBN and demonstrate the management influences on it.

1:30 - 3:00 PM

## 9-5: Safety Culture in Practice

Session Chairs: Susan Brissette, Tracy Dillinger

### Best Practice Framework for Safety Culture Improvement Programs

Torkel Soma, Berit Bergslid Salvesen, and Sondre Øie
*DNV, Oslo, Norway*

Over the last decades there have been extensive developments in the strategies for improved operational safety. At the same time more and more stakeholders demonstrates zero tolerance for accidental losses. Accidents and injuries may have a dramatic impact on a company's reputation and potential in loss of business opportunities, in addition to substantial economic consequence. An excellent safety track record is therefore a prerequisite for a healthy and sustainable business. As a result, many companies in various high risk industries are increasingly concerned with achieving and demonstrating sound safety performance in order to stay in business.

### Review of Legal System of Occupational Safety and Health in Mainland China

Y.G. Cao(a), Q. Chen(a), W.K. Chow(b), Gigi C.H. Lui(b) and Xu Dong Wang(c)
*a) College of Safety and Environment Engineering, Capital University of Economics and Business, Beijing, China. b)Research Centre for Fire Engineering, Department of Building Services Engineering, Area of Strength: Fire Safety Engineering, The Hong Kong Polytechnic University, Hong Kong, China. c) Beijing YiQing Enterprises Group Co., Ltd., Beijing, China*

The practice of occupational safety and health (OSH) management is a good indication of economical development in the urban areas to some extent. With the rapid social and economical development in China, OSH has become more concerned by the local government. Professionals in all disciplines are paying more attention to OSH. The legal system of OSH is becoming more a basis for the improvement of OSH management. Now, OSH is not only watched carefully by the Authority Having Jurisdiction (AHJ). In recent years, health and safety at work is taken as an important subject by employers and employees in enterprises of all scale. In addition to prescriptive regulations which might not be applicable to new subject disciplines, broad knowledge is required in safety engineering, industrial hygiene and medicine, ergonomics, and psychology. Through many years of development, the OSH regulatory system in China is expanding gradually, and implemented in the society as a fundamental requirement. The current situation of OSH in China is reviewed in the paper. This would give more insights into the present status of the supervisory organization, legal system and the major legislations concerned in Mainland China.

### Measuring Safety Culture in European Air Traffic Management

Barry Kirwan(a), Kathryn Mearns(b), Jeanette Winter(b), Tom Reader(b), Marinella Leone(a), Andrew Kilner(a), Anna Wennenberg(a), Eve Grace-Kelly(a)
*a) Eurocontrol Experimental Centre, Bretigny-sur-Orge, Paris, France. 2) Industrial Psychology Research Centre, School of Psychology, University of Aberdeen, Aberdeen, UK*

The concept of safety culture originated in the nuclear industry but since then has been applied in other industries including the energy sector, construction and more recently, healthcare. There is a prolific literature on the nature and consequences of safety culture, although valid and reliable measurement of this multi-faceted construct has proved challenging. Without appropriate measurement it is difficult to know how to manage safety culture yet many organizations are trying to implement both cultural and behavioural approaches to improve their safety performance (DeJoy, 2005). The current study outlines the development of a Safety Culture Measurement Tool (SCMT) for Air Traffic Management (ATM) across Europe, using a mixed methods approach (Guldenmund, 2007) and discusses how this approach can lead to improvements in safety culture within this type of organization. The paper describes the process of developing the SCMT and how it is implemented. Items for a questionnaire were developed through a literature review of safety culture and associated constructs (e.g. safety climate) and 52 interviews with air traffic controllers (ATCOs) and engineers, followed by tests of face and content validity with domain experts. The questionnaire was then implemented in two phases across nine European Air Navigation Service Providers (ANSPs) and the construct and discriminant validity tested using exploratory (EFA) and confirmatory analysis (CFA). Preliminary model testing with CFA suggests a good model fit for only one ANSP (n=310, $\chi 2$=532.29, df=391, GFI=.898, CFI=.931, RMSEA=.034), based on 30 items out of the original 59 item questionnaire, however, this could have been a reflection of sample size since the other ANSPs returned less than n=300, which precludes adequate testing using factor-analytic methods. The model suggests five sub-factors (Commitment; Responsibility; Involvement; Team Working; Reporting and Learning) mapping onto three higher-order factors – 'How safety is prioritised'; 'How people are involved in safety' and 'How we learn'. Further confirmation of the model with larger samples from other ANSPs is required before the construct validity of the measure can be determined.

### Safety attitudes of caregivers: the case of healthcare organizations in Mexico

Daniel Velazquez-Martínez, Jaime Santos-Reyes, and Tatiana Gouzeva
*Grupo: "Seguridad, Análisis de Riesgos, Accidentes y Confiabilidad de Sistemas" (SARACS), SEPI-ESIME, IPN, Mexico City, Mexico*

The treatment of patients may be regarded as a complex process involving, inter alia, sophisticated technology, medicine, diverse patients, multiple work process, and various professional disciplines. On the other hand, based on previous experiences of other industries such as, the nuclear, aviation, oil and gas the healthcare system is susceptible to failure. Systems failures may include sound alike drugs, poorly designed devices and equipment, poor team work and communication, human error, etc. Given this, patient safety has become a priority recently. The paper presents some discussion about the ongoing research project intended to assess the safety attitudes of caregivers of four healthcare systems in Mexico. The approach has been the adop-

tion of the "Safety Attitude Questionnaire" (SAQ) has been developed by the University of Texas, Center of Excellence for patient Safety research and Practice. The SAQ have been applied to four healthcare systems. The analysis of the questionnaires is being conducted. Currently, a larger healthcare organization than the four reported here is being considered for the application of the SAQ.

3:30 - 5:00 PM

## 9-6: Nuclear Safety Culture and Regulatory Oversight

Session Chairs: Zahra Mohaghegh, Bill Nelson

### Methodology for Detection and Assessment of the Impact of Informal Processes on Organizational Output

Lesa M Ross and Ali Mosleh
*University of Maryland, College Park, USA*

Informal processes exist, and can impact an organization's output, including safety. Informal processes cannot be eliminated (nor should they necessarily be). The question becomes how can we identify the informal processes and assess their impact on our system's safety? The methodology for the detection and assessment of informal processes requires the completion of six objectives: modelling of the organization from a process perspective, modelling of the processes, development of process taxonomy, determination of causes of informal processes, detection of the informal processes - using an indirect detection method (questionnaire that can be completed by a management representative which takes a small amount of time with minimal cost) and a direct detection method (process audit), and a methodology for the assessment of the impact of informal processes on an organization's risk. It has been determined that when informal processes that are beneficial to an organization are brought into the formal system, or detrimental informal processes are eliminated, the probability of the output failure decreases. The ability to assess the impact of the informal processes and to manage their occurrence within an organization will allow an organization to more effectively manage their risk.

### Building and Assessing an Effective Safety and Performance Culture

William R. Nelson
*DetNorske Veritas (USA) Inc., Houston, TX USA*

In order to reach maximum levels of performance and safety for complex installations such as nuclear power plants and oil refineries, technical and organizational risk factors should be integrated so that the full spectrum of risk information can be utilized and communicated. Current approaches typically separate technical and organizational perspectives due to the diverse engineering and social sciences perspectives of the two disciplines. Both safety and performance issues require balanced treatment to enable maximum business performance. DNV has developed an approach combining bow tie diagrams (from the oil and gas and process industries) and defense in depth objective trees (from the nuclear power industry) to address these needs. The approach has been applied to the study of supply chain risk for Lockheed Martin, focusing on three complex risk issues: environmental compliance, information systems for supporting organizational situation awareness, and incentives and motivation across a community of suppliers. The results of this application show promise for designing safety management systems and a "safety and performance culture" to enable operations excellence for high risk installations such as nuclear power plants, oil refineries, and offshore oil platforms. The approach is now being applied to the assessment of risk informed safety culture for a nuclear power station in Canada.

### Managing Safety of Industrial Hazardous Installations with Emphasis on the Control Systems, Interfaces and Human Factors

Przemysław Kacprzak, Kazimierz T. Kosmowski
*Gdansk University of Technology, Gdansk, Poland*

In the paper a procedure for the layer of protection analysis (LOPA) as a tool to evaluate the risk of accident scenarios occurrence in hazardous installations is outlined. In such installations several protection layers exist. Human operator performance in each layer is unavoidable, but the role and tasks are different and depend on the context of situation. Based on suggestions form literature (EEMUA, CREAM) and own proposals the slightly modified LOPA procedure, containing probabilistic modeling of accident scenarios including the human operator performance within human reliability analysis (HRA) is presented. Also a procedure for selecting, appropriate to situation considered and designed solution of human machine interface (HMI), a HRA methodology is proposed. Selected aspects of the alarm system (AS) designing, crucial in order to provide its required functionality and reliability are also discussed. Mentioned issues are illustrated on an example of HRA analysis with utilization of SPAR – H technique for the case of the control and protection system of a high pressure container.

# Space and Aviation

**Tuesday, Municipal**

10:30 AM - Noon

## 12-4: Lunar Exploration Risk Assessments

Session Chair: Adrian Gheroghe

### Constellation Probabilistic Risk Assessment (PRA): Design Consideration for the Crew Exploration Vehicle

Peter G. Prassinos(a), Michael G. Stamatelatos(a), Jonathan Young(b), Curtis Smith(c)
*a) National Aeronautics and Space Administration, Washington DC, USA. b) Pacific Northwest National Laboratory, Hanford, WA, USA. c) Idaho National Laboratory, Idaho Falls, ID, USA*

Managed by NASA's Office of Safety and Mission Assurance, a pilot probabilistic risk analysis (PRA) of the NASA Crew Exploration Vehicle (CEV) was performed in early 2006. The PRA methods used follow the general guidance provided in the NASA PRA Procedures Guide for NASA Managers and Practitioners. Phased-mission based event trees and fault trees are used to model a lunar sortie mission of the CEV – involving the following phases: launch of a cargo vessel and a crew vessel; rendezvous of these two vessels in low Earth orbit; transit to the moon; lunar surface activities; ascension from the lunar surface; and return to Earth. The analysis is based upon assumptions, preliminary system diagrams, and failure data that may involve large uncertainties or may lack formal validation. Furthermore, some of the data used were based upon expert judgment or extrapolated from similar components/systems. This paper includes a discussion of the system-level models and provides an overview of the analysis results used to identify insights into CEV risk drivers, and trade and sensitivity studies. Lastly, the PRA model was used to determine changes in risk as the system configurations or key parameters are modified.

### Lunar Landing Operational Risk Model

Chris Mattenberger(a), Blake Putney(a), Randy Rust(b), Brian Derkowski(b)
*a) Valador, Inc. Palo Alto, CA, USA. b) NASA Johnson Space Center, Houston, TX, USA*

Characterizing the risk of spacecraft goes beyond simply modeling equipment reliability. Some portions of the mission require complex interactions between system elements that can lead to failure without an actual hardware fault. Landing risk is currently the least characterized aspect of the Altair lunar lander and appears to result from complex temporal interactions between pilot, sensors, surface characteristics and vehicle capabilities rather than hardware failures. The Lunar Landing Operational Risk Model (LLORM) seeks to provide rapid and flexible quantitative insight into the risks driving the landing event and to gauge sensitivities of the vehicle to changes in system configuration and mission operations. The LLORM takes a Monte Carlo based approach to estimate the operational risk of the Lunar Landing Event and calculates estimates of the risk of Loss of Mission (LOM) – Abort Required and is Successful, Loss of Crew (LOC) – Vehicle Crashes or Cannot Reach Orbit, and Success. The LLORM is meant to be used during the conceptual design phase to inform decision makers transparently of the reliability impacts of design decisions, to identify areas of the design which may require additional robustness, and to aid in the development and flow-down of requirements.

### Functional Risk Modeling for Lunar Surface Systems

Fraser Thomson(a), Donovan Mathias(b), Susie Go(b), and Hamed Nejad(a)
*a) Eloret Corporation, NASA Ames Research Center, Moffett Field, USA. b) NASA Ames Research Center, Moffett Field, USA*

We introduce an approach to risk modeling that we call 'functional modeling,' which we have developed to estimate the capabilities and robustness of a lunar base. The functional model tracks the availability of key services and resources provided by systems, and the operational state of those systems' constituent strings. By tracking functions, we are able to identify cases where identical needs can be fulfilled by multiple elements (rovers, habitats, etc.) that are connected together on the lunar surface. For those cases we credit functional diversity, which enables us to compute more realistic estimates of operational mode availabilities.

### Mass-Constrained Availability for Lunar Exploration

Susie Go(a), Donovan L. Mathias(a), Fraser Thomson(b), and Balachandar Ramamurthy(c)
*a) NASA Ames Research Center, Moffett Field, CA, USA. b) ELORET Corp., Sunnyvale, CA, USA. c) Valador, Inc., Palo Alto, CA, USA*

This paper explores the definition and calculation of availability metrics for an example lunar outpost concept and the study of how different logistical supply capabilities would impact its functionality over time. First, some definitions of outpost availability are introduced to provide a metric that can be used to evaluate functionality. A Monte Carlo simulation model is used to integrate the functions of various lunar surface system elements and run their nominally-scheduled operations in a time-dependent manner. Using the definitions for availability, the impact of system failures can be tracked through time to observe the number of lunar outpost availability days that are actually achieved with respect to the planned outpost days. A series of simulation runs is performed using different mass levels to limit the ability to restore element functionality and, ultimately, the availability of the integrated system of outpost elements. The sensitivity analysis provides a mechanism for understanding how well the space transportation mass delivery capabilities align with the needs of the outpost.

1:30 - 3:00 PM

## 12-5: Mars Exploration Risk Assessments

Session Chair: Adrian Gheroghe

### Risk Requirements for a Mars Base

B. Ramamurthy(a), D. L. Mathias(b), B. J. Franzini(c), B. F. Putney(a),J. R. Fragola(c)
*a) Valador, Inc., Palo Alto, CA, USA. b) NASA Ames Research Center, Moffett Field, CA, USA. c) Valador, Inc., Rockville Centre, NY, USA*

This paper discusses the methodology involved in allocating quantitative risk requirements for future human space exploration programs. The establishment and maintenance of a long term, human habitable base or outpost on Mars is considered to be the ultimate exploration goal for the human space program in the analysis presented in this paper. The capability to perform exploration activities of interest requires a robust surface system architecture that can provide life support functions over the long durations of surface stay in Conjunction class reference mission architectures for Mars. The elements of a baseline transportation model are adopted, and within this context, the risk associated with transportation, set up and return from the Mars base is determined as a function of sustaining life functions on the surface. The point where the individual influences of these characteristic risks balance is sought out. The risk at this point is sub-allocated from the architecture level down to the surface elements that comprise the design architecture. The requirements on the different systems in the architecture are scoped down based on the combined availability of life support functions as a function of time.

### Risk Based Precursor Design Supporting a Crewed Mars Mission

B.J. Franzini(a), B. Ramamurthy(b), E. L. Morse(c), B. F. Putney(b), J. R. Fragola(a), D. L. Mathias(d)
*a) Valador, Inc., Rockville Centre, NY, USA. b) Valador, Inc., Palo Alto, CA, USA. c) Valador, Inc., Herndon, VA, USA. d) NASA Ames Research Center, Moffett Field, CA, USA*

The optimization of an integrated space exploration campaign requires balancing of multiple parameters including performance, cost, schedule and risk. This is particularly true of ambitious human exploration missions involving engineering elements and logistics of the scale that will be required for a crewed Mars mission. A clear definition of the campaign objective and an understanding of the design space with respect to these interdependent parameters are required to focus development activities. Objective-free trade studies may generate insights that are only indirectly useful, and real progress towards programmatic decisions and commitments can only be made if these trade studies are tied to the integrated analysis of the end objective. The use of a risk based design methodology where long term exploration campaign objectives flow down in the form of near term project requirements will be discussed here using a crewed mission to Mars as the high-level exploration campaign objective. The methodology involves identifying critical path (flagship) technologies required to support a Mars mission. Technology Readiness Levels (TRL) based uncertainty and reliability growth models, represent a means of assessing test and precursor effectiveness in terms of achieving the mission objective.

### Considering a Cost Constrained Risk Informed Design Paradigm for NASA

B. F. Putney(a), B. Ramamurthy(a), E. L. Morse(b), B. J. Franzini(c), J. R. Fragola(c), D. L. Mathias(d)
*a) Valador, Inc., Palo Alto, CA, USA. b) Valador, Inc., Herndon, VA, USA. c) Valador, Inc., Rockville Centre, NY, USA. d) NASA Ames Research Center, Moffett Field, CA, USA*

This paper discusses the application of a cost constrained risk informed design paradigm to developing a crewed Mars exploration program. Parameters that are studied in the planning and optimization of a space program typically include the cost, schedule, risk and performance. The measure of success of a given space program architecture depends on the ability to meet certain predefined criteria with respect to these interdependent parameters. Large programs tend to be beset with cost overruns and schedule delays arising from technical risks. A notional model of integrated mission risk, taking into account the transient trends of hardware maturation is discussed. The total time taken to accomplish the first complete mission- from the start of the campaign to the safe return of crew to the Earth is considered as a metric. This model is used to investigate how risks associated with hardware, stemming from as yet unresolved or unrealized technical issues or defects in the design, impact the schedule risk. The mission end date distribution generated by this model and the sensitivity of the solution to different levels of initial maturity for the key hardware elements is discussed. Observations regarding strategic risk mitigation are provided on the basis of this analysis.

### Engineering Risk Assessment of Ares I

D. L. Mathias, S. L. Lawrence, S. Go, and M. J. Werkheiser
*NASA Ames Research Center, Moffett Field, CA USA*

Risk awareness has been a key aspect of the design of NASA's next generation Ares I crew launch vehicle. An Engineering Risk Assessment approach has been incorporated as a way of addressing the system's risk drivers and fulfilling analysis needs as the teams —design outll risks. The approach is scalable with the changing needs of the design teams and Project as a whole. The current paper describes the Engineering Risk Assessment approach incorporated in the Ares I process, and presents examples to illustrate how the approach evolves with Project phase.

3:30 - 5:00 PM

## 12-6: Methods

Session Chair: Adrian Gheroghe

### The Integration of Probabilistic Risk Assessment and Game Theory Analysis in Support of Next Generation Spacecraft Designs

Clayton Smith, Tara Anderson, Eric Greenberg, Sanae Kubota, and Leopoldo Mayoral
*Johns Hopkins University Applied Physics Laboratory, Laurel, MD, USA*

Reliability analyses of space systems are not new. These analyses tend to be deterministic representations of an inherently stochastic failure and operational processes. They provide value to the engineering design community in identifying weak points in the design early which can be remedied by various means. When addressing threats to operational spacecraft, this paradigm is not sufficient. The uncertainties in threat initiators, impacts, and system responses need to be accounted for as does the adaptive nature of the threats. This paper describes a methodology used in a spacecraft vulnerability analysis that merges probabilistic risk assessment techniques with application of Game Theory. The analysis results highlighted potential vulnerabilities and mitigations which are used to support system trades to enhance development of the design. PRA is a powerful tool that starts with a view of risk comprising various operational and failure scenarios, the consequence states for the scenarios, and the probabilities (including the associated uncertainty) for ending in those states. Utility functions were derived from the resultant data sets for both a potential adversary and the spacecraft design team. The Game Theory analysis determined the most rational strategy for each to take in the presence of uncertainty. Design teams can then use the risk-based prioritized list of mitigations to increase the robustness of their designs in a cost effective manner.

### Treatment of Uncertainties in the Comparison of Design Option Safety Attributes

Frank Groen, and Bill Vesely
*NASA, Washington DC, USA*

The comparison of design alternatives based on their safety attributes often involves the comparison of levels of safety based on figures of merit such as the Loss of Crew (LOC) likelihood. Uncertainty associated with the estimates of such measures complicates may cause differences between options to be considered insignificant by decision makers even when there is a good engineering argument to be made for one option compared to others. A direct representation of the uncertainty about the differ-

ence between options are more informative in such cases. Dependencies between estimates, due to similarities between the design alternatives, must be considered in such comparisons.

### Common Cause Failure Modeling: Aerospace vs. Nuclear

James E. Stott(a), Paul T. Britton(b), Robert W. Ring(b), Frank Hark(b), and G. Spencer Hatfield(b)
*a) NASA Marshall Space Flight Center, AL, USA. b) Bastion Technologies MSFC, AL, USA*

Aggregate nuclear plant failure data is used to produce generic common-cause factors that are specifically for use in the common-cause failure models of NUREG/CR-5485. Furthermore, the models presented in NUREG/CR-5485 are specifically designed to incorporate two significantly distinct assumptions about the methods of surveillance testing from whence this aggregate failure data came. What are the implications of using these NUREG generic factors to model the common-cause failures of aerospace systems? Herein, the implications of using the NUREG generic factors in the modeling of aerospace systems are investigated in detail and strong recommendations for modeling the common-cause failures of aerospace systems are given.

# Software Reliability

**Tuesday, Federal**

10:30 AM - Noon

## 10-2: Software Design and Failure Analysis

Session Chairs: Mario Brito, Gaspare Maggio

### Probabilistic Assessment of Effectiveness of Software Testing for Safety-Critical Systems

William Alton Ballance, William Jenkins, and Sergiy Vilkomir
*East Carolina University, Greenville, NC, USA*

This paper provides the results of experimental evaluation of effectiveness of pair-wise testing. We consider a non-traditional area of pair-wise testing application, namely using pair-wise approach for testing logical expressions. A tool has been developed for experimental numerical investigation. This tool generates faults of various specific types and applies the previously derived test sets to determine if the testing method detected those faults. The user can see how effective a particular test case was at discovering a particular fault type. We investigate fault detection for five various types of faults in 20 different logical expressions which contain from 5 to 14 logical variables each. Three different pair-wise test sets, generated by two different tools, are applied for each logical expression and each generated fault. The program calculates probabilities of faults revealed over single expressions, the entire test set, and between fault types. We compare our results with results by other researchers and provide recommendation for practical testing. The tool has been used for analysis of pair-wise testing, however, it can be also used to analyze other testing criteria.

### Software Fault-Failure and Error Propagation Analysis Using the Unified Modeling Language

Chetan Mutha, Manuel Rodriguez, and Carol Smidts
*The Ohio State University, Columbus, USA*

A framework for fault-failure and error propagation through different UML diagrams is introduced. The method is formalized by defining rules for fault propagation across different UML diagrams and also within a particular diagram. A study of the propagation of faults through each diagram highlights various structural and behavioral aspects of the software failure. This method will allow the designers to proactively analyze the functionality of the systems early in the design process, understand functional and other failures and their propagation paths, overall impact on the system, and redundancies and safeguards that should be added. The main advantage of the method is that it permits the analysis of the failure and fault propagation at a highly abstract level before any potentially high-cost design commitments are made thereby supporting decision making early in the design process, providing guidance to the designers to allow elimination of failures through exploration of system components and their functionality, and facilitating the development of more reliable system configurations. This method is discussed using an example and results are given for the Helium tank sub-system of the Space Shuttle's Reaction Control System (RCS).

### EDF CCF Benchmark on CCF Methodologies for CCF Groups of Size 4

Jean Dewailly(a), Anne-Marie Bonnevialle(a), and Thi Thuy Linh Nguyen(b)
*a) EDF R&D, Clamart, France, b) UTT, Troyes, France*

Common Cause Events are dependent failures in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause. As Common Cause Failures (CCFs) are known as a major contributor to risk, their quantification is very important in the context of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants. Several methodologies exist to quantify CCF. In this paper, the objective is to quantify, then to compare the results of the CCF estimation for three CCF groups of size 4. Each of them is quantified in three different contexts (1) update of a previous set of CCF parameters, (2) use of the "recent" data only and (3) estimation based on the overall defence of the system against CCFs at the time of the design stage.

### Multi-threads Software Reliability Estimation Based on Test Results and Software Structure

Yaguang Yang and Russell Sydnor
*United States Nuclear Regulatory Commission, Rockville, MD, USA*

This paper extends a single-thread software reliability model to a multi-thread software reliability model. This probabilistic model is based on software structure and software test results. The software structure is represented by nodes and edges in graph theory. Each node is either a logic branch point or a logic converge point. Each edge is a piece of the code which does not include any logic branch. These edges are either parallel or serially connected. The reliability of each piece of software (edge) is determined by software test result. The reliability of the entire software is estimated by using the reliabilities of edges and the structure of the software.

# Special Session

**Tuesday, Federal**

1:30 - 3:00 PM

## 19-1: Importance Measures

Session Chairs: Emanuele Borgonovo, Dr. Curtis Smith

### The Limit Exceedance Factor Applied to the Technology Neutral Framework

B.C. Johnson and G.E. Apostolakis
*Department of Nuclear Science and Engineering, Massachusetts Institute of Technology, Cambridge, MA, USA*

There are importance measures commonly used in Probabilistic Risk Assessments and risk-informed regulation for structures, systems, and components . When designing a conceptual reactor with a safety goal in mind, these importance measures are quite extreme. For example, the Risk Achievement Worth is defined such that a component is always in the failed state; however, a designer may not be looking to remove a system but to simplify it to improve economics. These traditional importance measures are also not well suited to the Technology Neutral Framework (TNF) proposed by the NRC staff. The Limit Exceedance Factor (LEF) has been developed as a more informative importance measure when there is a goal in mind. It is defined as the factor by which the failure probability of a component may be multiplied such that the end state (e.g., dose, core damage) frequency exceeds a limit. It allows a designer to know how much room there is for possible simplification in redundant systems. Alternatively, in the case where a system does not meet the frequency limit it can show which systems might be ideal targets for improvement to reach the limit. The TNF replaces the traditional design basis accidents by a set of Licensing Basis Events (LBEs) whose frequency and dose must satisfy certain limits. We constructed LBEs for a sodium-cooled fast reactor using functional event trees and generic release categories. When applied to these LBEs, LEF gives useful information while traditional importance measures do not.

### Determining Interactions in PSA models: Application to a Space PSA

C. Smith(a) and E. Borgonovo(b)
*a) Idaho National Laboratory, Idaho Falls, Idaho, USA. b) ELEUSI research center, Bocconi University, Milan, Italy*

This paper addresses use of an importance measure interaction study of a probabilistic risk analysis (PSA) performed for a hypothetical aerospace lunar mission. The PSA methods used in this study follow the general guidance provided in the NASA Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. For

the PSA portion, we used phased-based event tree and fault tree logic structures are used to model a lunar mission, including multiple phases (from launch to return to the Earth surface) and multiple critical systems. Details of the analysis results are not provided in this paper – instead specific basic events are denoted by number (e.g., the first event is 1, the second is 2, and so on). However, in the model, we used approximately 150 fault trees and over 800 basic events. Following analysis and truncation of cut sets, we were left with about 400 basic events to evaluate. We used this model to explore interactions between different basic events and systems. These sensitivity studies provide high-level insights into features of the PSA for the hypothetical lunar mission.

### An Extreme-Value Approach to Anomaly Vulnerability Identification

Chris Everett(a), Gaspare Maggio(a), and Frank Groen(b)
*a) Technology Risk Management Operations, ISL, New York, NY. b) Office of Safety & Mission Assurance, NASA, Washington, D.C.*

The objective of this paper is to present a method for importance analysis in parametric probabilistic modeling where the result of interest is the identification of potential engineering vulnerabilities associated with postulated anomalies in system behavior. In the context of Accident Precursor Analysis (APA), under which this method has been developed, these vulnerabilities, designated as anomaly vulnerabilities, are conditions that produce high risk in the presence of anomalous system behavior. The method defines a parameter-specific Parameter Vulnerability Importance measure (PVI), which identifies anomaly risk-model parameter values that indicate the potential presence of anomaly vulnerabilities, and allows them to be prioritized for further investigation. This entails analyzing each uncertain risk-model parameter over its credible range of values to determine where it produces the maximum risk. A parameter that produces high system risk for a particular range of values suggests that the system is vulnerable to the modeled anomalous conditions, if indeed the true parameter value lies in that range. Thus, PVI analysis provides a means of identifying and prioritizing anomaly-related engineering issues that at the very least warrant improved understanding to reduce uncertainty, such that true vulnerabilities may be identified and proper corrective actions taken.

### Total Order Reliability in PSA: Importance of Basic Events and Systems

E. Borgonovo(a) and C. Smith(b)
*a) ELEUSI research center, Bocconi University, Milan, Italy. b) INL, Idaho National Laboratory, Idaho Falls, Idaho, USA*

The purpose of this work is twofold. First, to formalize the properties of the total order reliability importance measure for PSA models. Second, to extend the definition of the total order importance measure to groups of basic events. This allows one to obtain the importance of systems and to address the relevance of interactions among systems.

# Security / Infrastructure

**Tuesday, Federal**

3:30 - 5:00 PM

## 14-1: Vulnerability of Critical Infrastructures

Session Chair: Enrico Zio

### Combining Particle Swarm Optimization and Support Vector Regression for Reliability Prediction

Márcio das Chagas Moura(a), Isis Didier Lins(a), Enrico Zio(b) and Enrique López Droguett(a)
*a) Department of Production Engineering, Center for Risk Analysis and Environmental Modeling, Federal University of Pernambuco, Recife-PE, Brazil. b) Department of Energy, Polytechnic of Milan, Milan, Italy*

Support Vector Machines (SVMs) constitute an interesting alternative for regressing component reliability behavior over time, based on time series data. However, similarly to all empirical regression modeling paradigms, their performance depends on the setting of a number of parameters that influence the effectiveness of the training stage during which the SVMs are constructed. The problem of choosing the most suitable values for the SVM parameters can be framed in terms of an optimization problem aimed at minimizing the regression error. In this work, this problem is solved by Particle Swarm Optimization (PSO), a probabilistic approach based on an analogy with the co-operative motion of biological organisms, such as schools of fishes and flocks of birds. SVM in liaison with PSO is applied to tackle a benchmark reliability prediction problem of literature; comparison of the results obtained with other time series modeling paradigms such as Artificial Neural Networks indicate that the PSO-SVM model is able to provide reliability predictions with comparable or superior accuracy.

### QoS of a SCADA System Versus QoS of a Power Distribution Grid

E. Ciancamerla, S. Di Blasi, C. Foglietta, D. Lefevre, M. Minichino(a), L. Lev and Y. Shneck(b)
*a) ENEA, Rome, Italy. b) IEC, Haifa, Israel*

The main objective of a SCADA system of a Power distribution grid is to assist utility companies in supplying power to customers, according to Quality of Service (QoS) indicators established by a National Electric Authority. SCADA performs real time measurements and commands to improve operations on its Power grid by means of Remote Terminal Units that are connected to a SCADA control Centre throughout a dedicated or even a public Telco network. In the paper, indicators of QoS of Fault Isolation and System Restoration (FISR) service, delivered by SCADA system are computed, discussed and correlated to quality indicators of power supplied to customers. In delivering FISR service (and many other services), SCADA system, Telco network and Power grid act as a whole heterogeneous network. While SCADA system and Telco network can be well represented by means of discrete event simulators, to represent a Power grid a continuous simulator is typically required. Here, limited to FISR service, SCADA system, Telco network and power grid have been represented by using a unique discrete event simulator.

# PSA Applications

**Tuesday, Superior**

10:30 AM - Noon

## 1-14: Specific PSA Applications I

Session Chairs: Marko Cepin, Jim Knudsen

### Assessment of Switchyard Reliability with the Fault Tree Analysis

Marko Cepin
*Faculty of Electrical Engineering, Ljubljana, Slovenia*

Reliability of power systems largely depends on the switchyards reliability. Switchyard reliability is defined as the inability of the switchyard to support the delivery of electrical power supply to any of its related loads. The method is developed based on the fault tree analysis, which enables qualitative and quantitative evaluation. The method enables definition of different success criteria related to the number and to the capacity of the related loads. The results show the switchyard reliability as a representative curve of reliability versus the capacity of electric power supply not delivered. The main benefit of the method is its extension from consideration of independent failures to consideration of independent and common cause failures.

### Evaluation of Fuel Damage Frequency Resulting from Loss of Spent Fuel Pool Cooling

Masaru Yamanaka(a), Kaoru Sakata(a), Satoru Fukuyama(b), Shigeyuki Nakanishi(b)
*a) Genden Information System Company, Tokyo, Japan. b) The Japan Atomic Power Company, Tokyo, Japan*

The spent fuel irradiated in the reactor core is kept and cooled in the Spent Fuel Pool (SFP). So there is some risk of the spent fuel damage in the SFP as well as that of the reactor core damage when abnormal events such as loss of cooling accident occur. It is thought that the risk of spent fuel damage in the SFP is lower than that of reactor core, because the decay heat level generated by the spent fuel in the SFP is lower than that of reactor core. However, there is a possibility that the fuel damage risk of the SFP cannot be ignored in comparison with the core damage during the refueling outage, because the fuel that has high decay heat level is transferred to the SFP during the exchange of fuel and the mitigation system for the SFP is limited in comparison with the reactor core. Therefore, in this study, risk monitor to evaluate the SFP fuel damage risk during the plant shutdown conditions was constructed for a BWR plant, and the SFP fuel damage frequency was evaluated. By utilizing the risk monitor, the useful risk information for the safety management activity can be supplied during the refueling outage.

### Using Risk Assessment for Graded Quality Assurancein Nuclear Power Plants

Robert J. Lutz, Jr.
*Westinghouse Electric Co., Monroeville, USA*

The 50.69 rule was published by the Nuclear Regulatory Commission (NRC) in 2004 for voluntary implementation by plant owners to categorize structures, systems, and components in nuclear power plants according to their safety significance. This was one of the showcase initiatives for risk-informed regulation and a significant effort was expended by both the industry and the NRC to develop the rule and the guidance for implementation. While the provisions of the new rule focus on safety, reduce regulatory burden and reduce plant operating and maintenance costs, in the six years since the rule was approved for use no plant owners have implemented the rule. There are sound reasons why the benefits of the rule have not been realized by plant operators, including limited resources and an uncertain regulatory environment. These barriers are examined in detail in this technical paper. While the barriers are slowly being removed, the uncertain regulatory environment remains the most substantial. Publication of a draft and final inspection guideline by the NRC in 2010 should reduce the uncertainty. If the inspection guideline is found to be consistent with the original intent of the 50.69 rule, the implementation of a 50.69 program will enjoy a higher priority among plant operators and resources will be made available. Thus, 2010 is a pivotal year in determining the future of this significant risk-informed initiative and the future of performance based risk-informed regulation as a whole.

### PSA Based Selection of Transients Susceptible to Pressurized Thermal Shock at NPP Paks

Zoltán Karsa(a), József Elter(b), and Attila Bareith(a)
*a) NUBIKI Nuclear Safety Research Institute, Budapest, Hungary. b) Paks Nuclear Power Plant, Paks, Hungary*

The paper discusses the most important features of PSA based selection of Pressurized Thermal Shock (PTS) transients for the Paks NPP. The applied analysis methods, data and tools are briefly described and the results of PSA quantification are presented. Use of the analysis results in the overall re-evaluation of reactor pressure vessel integrity in relation to pressurized thermal shock is summarized. Finally, some follow-on activities are highlighted.

1:30 - 3:00 PM

## 1-15: Specific PSA Applications II

Session Chairs: Robert Buell, Peter Swift

### Lessons Learned in Risk Evaluation for Extended Power Uprate

Ching Guey
*Florida Power and Light, Juno Beach, FL, USA*

Significant resources have been spent in improving PRA models to meet the requirements of Reg. Guide 1.200 Revision 1. A risk evaluation to support the extended power uprate has been performed for three plants. Although extended power uprate license amendment request is not a risk-informed submittal, the conformance of Reg. Guide 1.200 requirements introduced unexpected iterations in the PSA (scope and level of detail) to support the risk evaluation of EPU. This paper provides lessons learned of three different plants with different risk profiles.

### PRA Modeling of Debris-Induced Failure of Long Term Core Cooling via Recirculation Sumps

David S. Teolis, Robert J. Lutz, Jr., and Heather L. Detar
*Westinghouse Electric Company LLC, Monroeville, USA*

Generic Safety Issue GSI-191 identified that the methodology used for assessing containment sump screen debris loading at Pressurized Water Reactor (PWR) nuclear power plants may not be conservative. All PWR licensees have been required to reassess their design basis for long term core cooling (LTCC) and make necessary modifications. NEI 04-07 provided a conservative methodology for assessing PWR sump screen performance and the impact on LTCC. This methodology was based on analytical and experimental studies of debris generation, transport and head loss on sump screens. These studies were acceptable for conservative design basis assessments; however, a probabilistic risk assessment (PRA) model was necessary to enable utilities to model the potential for debris-induced failure of LTCC and to determine the risk significance of any non-conformances to their licensing basis. A probabilistic risk assessment model for debris-induced LTCC was developed, as reported in WCAP-16882, based on the conservatisms, margins and uncertainties in the licensing basis methodology and provides implementation guidance. Changes to the PRA are recommended prior to implementation of the debris-induced LTCC model to permit development of a model that more realistically represents the potential for failure of LTCC due to debris generation. An implementation example is also provided.

### The Case for Subdividing the Large Break LOCA Category in the PRA for PWR Nuclear Power Plants

Heather L. Detar, Robert J. Lutz, Jr., and David S. Teolis
*Westinghouse Electric Co., Pittsburgh PA, USA*

The loss of coolant accident (LOCA) categories in the PRA for nuclear power plants have traditionally been defined on a functional basis. Large break LOCAs were defined as those events that only require low pressure emergency core cooling (ECC) recirculation for successful core cooling. As a result, the large break LOCA category typically encompasses all pipe breaks from about 6 inch equivalent diameter up to at double ended guillotine rupture of the reactor coolant system (RCS) loop piping. Although this is a wide size range, the large break LOCAs typically contributes 1% or less to the overall core damage frequency. Thus there has not been an urgent need to be more finely derive the large LOCA classes. Several recent developments point to the need to consider splitting the traditional large LOCA class into two separate categories. One driver is the significance determination process for non-conformances in the licensing basis for containment sump blockages. The licensing basis for containment sump screen performance is very complex and it is quite likely that a plant may experience a non-conformance. Breaking the LOCA class into two categories can help assure that the risk significance of many types of non-conformances will be negligible. Another driver is the need for ECC hot leg recirculation to prevent the buildup of boric acid in the reactor vessel to levels that could result in blockages due to precipitation of the boric acid. Analyses show that hot leg recirculation may only be required for break sizes in which the reactor coolant loops cannot be refilled to provide full loop circulation. A third driver is the need to maintain all of the ECC system accumulators in-service.

### Analysis of RHR Pump's Operability during Loss of Room Cooling for Probabilistic Risk Assessment in Korea

Jinhee Park, C.Yoon, H.G. Lim, S.H. Han(a), C.J. Lee(b)
*a) Korea Atomic Energy Research Institute, Yuseong, Daejeon, KOREA. b) Korea Institute of Nuclear Safety, Yuseong, Daejeon, KOREA*

In PRA analysis, the HVAC (Heating, Ventilation and Air Condition) system for room cooling is essential for the vital mitigation safety systems operation during mission time. In the PRA models in Korea, upon Loss of Room Cooling, the operability of equipment in the room is assumed to immediately be failed conservatively or a simple recovery action (door opening in the equipment room by operator) for the equipment operation has been applied optimistically based on expert judgment. This was seen as an unrealistic assumption. To address this issue, KAERI (Korea Atomic Energy Research Institute) has performed the room heat-up calculation for various rooms in that the vital mitigation systems located using the CFD (Computational Fluid Dynamics) Code during Loss of Room Cooling. The results of those room heat-up calculations showed that the ambient temperature increasing of the room did not exceed over the design temperature within mission time upon Loss of Room Cooling accident. To verify these results, the CFD code calculation, we performed the real room hest-up test at a safety pump room in a Korean nuclear power plant. From this test, the room temperature did not exceed over the design temperature but the surface temperature of pump body was increased much more than we expected. To apply this result to the PRA, an analysis for predicting the temperature of pump motor internal parts has been performed.

3:30 - 5:00 PM

## 1-16: Methods

Session Chairs: Robert Youngblood, Kurt Vedros

### SSM research project on Defense-in-Depth PSA – Assessing Defense-in- Depth Levels with PSA Methods

Per Hellström(a), Michael Knochenhauer(a), Ralph Nyman(b)
*a) Scandpower, Solna, Sweden. b) SSM (Swedish Radiation Safety Authority), Solna, Sweden*

One of the basic requirements for nuclear safety is to maintain and to develop the Defensein- Depth (DiD). The overall aim is to prevent deviations from normal operation from occurring and, if prevention fails, to detect and limit their consequences, and to prevent any escalation to more serious conditions. Swedish regulation in SSM FS 2008.1, requires that the Defense-in-Depth is analyzed with deterministic and probabilistic methods. PSA studies are to be performed for all operating modes, as realistic as possible. In principle, the PSA can be used to investigate the application of DiD. A PSA addresses the frequency of initiating events that challenge nuclear safety (DiD Levels 1 and 2), the conditional probability of failure of safety systems and the frequency of core damage (DiD Level 3), the conditional probability of bypass or failure of the containment and the frequency of a large (early) release (DiD Level 4) and effectiveness of the off-site emergency response measures and the frequency of social and economic consequences (DiD Level 5) DiD levels are evaluated by the licensees with PSA, however, the results are seldom referred to in terms of weaknesses and strengths of the DiD levels The SSM research project has made an inventory of the potential and possible methods for using PSA in evaluating and ranking the system structures and

components (SSCs) being part of the different DiD levels. The project has identified and described current use of PSA results and the possibility for extended use of PSA results in evaluating a plants current DiD levels, the impact on DiD levels due to plant changes and the importance of plant events reported in the Licensee Event Reports (LERs) for the SSCs belonging to each DiD level. The different pieces making up a PSA (initiating events, sequences, consequences in level 1 and level 2 etc) and DiD (definitions of DiD levels etc) are elaborated and a new extended framework for the different elements of DiD and PSA and their relations is outlined. Modeling features, PSA results and their presentation in support of providing a deeper insight in the Defense-in-Depth characteristics are presented, and provide a further basis for improved use of PSA and risk results in the evaluation of a plant´s Defense-in-Depth.

## The Application of Probabilistic Safety Assessment in CPR1000 Severe Accident Prevention and Mitigation Analysis

Liu Pingping, Zhang Ning
*China Nuclear Power Technology Institute, Shenzhen, China*

Authors discuss the relationship between Probabilistic Safety Assessment (PSA) and severe accident study and also introduce on how to apply PSA in severe accident prevention and mitigation. PSA could find the plant vulnerabilities on severe accidents prevention and mitigation. Some modifications or improvement focusing on these vulnerabilities can be found. PSA also can assess the efficiency of these actions for decision-making. According to CPR1000 unit severe accident analysis, this article shows an example for the process and method on how to use PSA to enhance the ability on severe accident prevention and mitigation.

## User-Friendliness and Transparency in PSA Modelling

Cilla Andersson(a), Stefan Authén(b) and Jan-Erik Holmberg(c)
*a) Ringhals AB, Väröbacka, Sweden. b) Risk Pilot AB, Stockholm, Sweden. c) VTT, Espoo, Finland*

Most of the probabilistic safety assessments (PSA) for Nuclear Power Plants were originally created to make conservative estimates of the core damage frequencies for internal events, which might occur during power operation. The PSA models have then been expanded to replace conservative estimates with more realistic assumptions and to include other types of initiating events, modes of operation and end states. The development has resulted in very large and detailed models, which are hard to understand completely, even for an experienced PSA engineer. Today, the trend to increase the level of detail and the scope of the PSA models continues as a consequence of regulatory requirements. Hence the Nordic PSA Group (NPSAG) has initiated a project with the aim of identifying methods to reduce the complexity of the PSA models. This paper presents and discusses the results of the first part of the project in which areas of importance for the user-friendliness and transparency of a PSA are identified..

# Wednesday Meeting-At-A Glance

| Room Session | Salon A | Salon B | Salon C | East Room | West Room | North Room | Municipal | Federal | Superior | South Room |
|---|---|---|---|---|---|---|---|---|---|---|
| 0730 - 1600 | **Conference Registration - Courtyard Foyer** | | | | | | | | | |
| 0730 - 0830 | **Continental Breakfast - Madison, Courtyard, and Compass Foyers** | | | | | | | | | |
| 0830 - 1000 | Plenary Speaker - Dr. Elizabeth Pate–Cornell Madison Ballroom | | | | | | | | | Exhibits |
| 1000 - 1030 | ***Coffee/Refreshment Break*** | | | | | | | | | |
| 1030 - 1200 | Risk Management 4-2: Safety Goals | Modeling and Simulation 2-7: Expert Judgment | HRA 5-7: HRA Qualitative Analysis | PSA Applications 1-7: Data & Aging | External Events 15-7: Seismic: Hazards and Response Analysis | Safety Culture 9-7: Safety Management | Industrial Safety 6-1: QRA on Industrial Application | Security Infrastructure 14-2: Methods for Managing Vulnerabilities | Environmental Risk 3-1: Climate Change Challenges | |
| 1200 - 1330 | ***Lunch - on your own*** | | | | | | | | | |
| 1330 -1500 | Risk Management 4-3: Risk Informed Decision Making I | Modeling and Simulation 2-8: Explosive and Fire | HRA 5-8: Improving Safety and Reliability Through HRA Applications | PSA Applications 1-8: Instrumentation & Control I | External Events 15-8: Seismic: PRA | Safety Culture 9-8: Safety Management and Knowledge Management | Industrial Safety 6-2: Risk/Reliability Analysis | Security / Infrastructure 14-3: Facility Security Assessment | Environmental Risk 3-2: Geological Carbon Capture & Sequestration I | |
| 1500 - 1530 | ***Coffee/Refreshment Break- Madison, Courtyard, and Compass Foyers*** | | | | | | | | | |
| 1530 - 1700 | Risk Management 4-4: Risk Informed Decision Making II | Modeling and Simulation 2-9: Bayesian Methods and Binary Decision Programs | HRA 5-9: Applications, Tools, and Comparisons | PSA Applications 1-9: Instrumentation & Control II | External Events 15-9: Wind, Hurricane and Lightening | Safety Culture 9-9: Pushing the Envelope in Safety Management | Industrial Safety 6-3: Accident Analysis I | Security / Infrastructure 14-4: Area-Level Risk Management | | |
| 1745 - 2200 | ***Gala Dinner at Tillicum Village - meet buses in front of lobby at 1745 for transport to Argosy Cruise Pier*** | | | | | | | | | |

# Plenary Speaker

## Dr. M. Elisabeth Paté-Cornell

Professor and Chair
Department of Management Science and Engineering
Stanford University

Terman Engineering Building, Room 340
Stanford, CA 94305
Tel: (650) 723 3823
Fax: (650) 736 1945
e-mail: mep@stanford.edu
Web page: http://www.stanford.edu/dept/MSandE/people/faculty/mep/

Elisabeth Paté-Cornell is the Burt and Deedee McMurtry Professor in the School of Engineering and has been chair of the Department of Management Science and Engineering at Stanford University since its creation in January 2000. She has been a member of National Academy of Engineering since 1995. Her primary areas of teaching and research are engineering risk analysis, risk management, and decision analysis.

**Risks and games: three models and illustrations**

Recent developments in risk analysis have included elements of game analysis. These games and the resulting risks can be analyzed in several ways (e.g., a principal agent model, or simulation of an alternate game between two parties.) I will present three cases. The first case involves modeling and simulation of a game between a manager and an agent to assess the risk of system failure associated with some management decisions. The illustration represents a project's development under tight resource constraints, in which the agent may cut corners, thus increasing the probability of technical failure risk in operations. The result is an optimal incentive strategy, balancing costs and benefits to the managers, and the probability of technical failures as a result of the constraints.

The second case in that of an alternate "game" between a government and insurgents. A balanced counter-insurgency strategy includes allocation of resources between the short term to reduce the immediate risk of insurgents' attacks, and the long term to address the fundamental problems that fuel the insurgency. At the end of the simulation period, the model allows estimation of the probability that a particular attribute of the government's utility function (e.g., political stability) is below a given threshold.

The third case is an analysis of different US nuclear counter-proliferation strategies (economic, diplomatic and military) focusing on a particular country. The probability that the country acquires nuclear weapons in a given time frame depends on its intent and capabilities. The development of nuclear weapons is described as a semi-Markov process with transitions among four states: nuclear-weapon free, latent nuclear weapons, nuclear weapons infancy and nuclear weapons arsenal. The model includes an analysis the country's decisions in each time period, and of different US strategies over a determined number of time units using a genetic algorithm. The result is the probability of a nuclear attack on the US in that time frame.

# Risk Management

**Wednesday, Salon A**

10:30 AM - Noon

## 4-2: Safety Goals

Session Chairs: Yolande Akl, Jeanne-Marie Lanore

### Guidance for the Definition and Application of Probabilistic Safety Criteria

Michael Knochenhauer(a) and Jan Erik Holmberg(b)
*a) Scandpower – Lloyd's Register, Stockholm, Sweden. b) VTT Technical Research Centre of Finland, Espoo, Finland*

A guidance document has been developed as part of a four-year Nordic project dealing with the use of probabilistic safety criteria for nuclear power plants. The Guidance sums up, on the basis of the work performed throughout the project, issues to consider when defining and applying probabilistic safety criteria. The Guidance describes the terminology and concepts involved, levels of probabilistic safety criteria and relations between these, how to define a criterion, how to apply a criterion, on what to apply the criterion, and how to interpret the result of the application. It specifically deals with what makes up a probabilistic safety criterion, i.e., the risk metric, the frequency criterion, the PSA used for assessing compliance, and the application procedure for the criterion. It will also discuss the concept of subsidiary criteria, i.e., different levels of safety goals, their relation to defense in depth and to a primary safety goal in terms of health effects or other off-site consequences.

### Status and Experience with the Technical Basis and Use of Probabilistic Risk Criteria for Nuclear Power Plants

Philippe Hessel(a), Jan-Erik Holmberg(b), Michael Knochenhauer(c) and Abdallah Amri(d)
*a) Canadian Nuclear Safety Commission, Ottawa, Canada. b) VTT, Espoo, Finland. c) Relcon Scandpower, Solna, Sweden. d) OECD Nuclear Energy Agency, Paris, France*

Probabilistic safety criteria, including safety goals, have been progressively introduced by regulatory bodies and utilities. They range from high level qualitative statements to technical criteria. They have been published in different ways, from legal documents to internal guides. They can be applied as legal limits down to "orientation values". The OECD/NEA Working Group on Risk (WGRISK) prepared a questionnaire on the probabilistic risk criteria for nuclear power plants. Answers were received from 13 nuclear safety organizations and 6 utilities. The reported probabilistic risk criteria can be grouped into 4 categories, in relation with the tools to be used for assessing compliance: core damage frequency, releases frequency, frequency of doses and criteria on containment failure. Introduction of probabilistic safety criteria is generally considered to result in safety improvements. Opinion is widespread on the benefits of using probabilistic safety criteria for communication with the public, ranging from bad to good experiences. The responses to the questionnaire suggested that more work should be considered in the definition of releases frequencies: some regulators include a time range (generally 24 hours) in the criterion while others do not limit the time to be considered. It is suggested that, in the first case, the existing PSAs should be revisited to assess if long development accident sequences were considered.

### Comparison of Risk Criteria in Safety-Critical Industries

Michael Knochenhauer and Anders Persson(a), Jan Erik Holmberg(b), and Xuhong He(c)
*a) Scandpower – Lloyd's Register, Stockholm, Sweden. b) VTT Technical Research Centre of Finland, Espoo, Finland. c) Scandpower – Lloyd's Register, Beijing, PR China*

The paper describes the results from a sub-project within a Nordic research project dealing with probabilistic risk criteria for nuclear power plants (NPP). In order to provide perspective on the project's detailed treatment of probabilistic risk criteria for NPP:s, and to make it possible to relate these to risk criteria defined and applied in other safety-critical industries, criteria defined and used within the European railway and offshore oil and gas industries have been discussed in some detail and compared to NPP criteria.

1:30 - 3:30 PM

## 4-3: Risk Informed Decision Making I

Session Chairs: Reno Vinolainen, Marina Rowekamp

### Blending Deterministic and Probabilistic Arguments in the Regulatory Decision-Making – The Canadian Approach

Philippe Hessel
*Canadian Nuclear Safety Commission, Ottawa, Canada*

A safety assessment is a systematic process to verify that applicable safety requirements are met in all phases of the life cycle of a Class I nuclear facility. Safety analysis is a key component of a safety assessment. Safety analysis incorporates both probabilistic and deterministic approaches, which complement each other. Deterministic safety analysis is the principal means of demonstrating that the dose acceptance criteria and safety goals are met with a high degree of confidence for all accidents within the design basis. Probabilistic safety analysis is the principal means of demonstrating that the safety goals are met for potential accidents both within and beyond the design basis. It identifies vulnerabilities not necessarily accessible through deterministic safety analysis alone. With the development of probabilistic analysis techniques, nuclear facilities licensees and applicants have introduced probabilistic arguments in support of applications for a licence to operate as well as submissions aimed at obtaining approval for facility modifications, for closure of action items, or for temporary licence exemptions. The document described in this paper defines the process the CNSC staff should use to assess submissions that use both deterministic and probabilistic arguments and to reach a decision.

### Is a Risk Assessment Always Feasible? A Case Study

Stanley H. Levinson
*AREVA NP Inc., Lynchburg, VA, USA*

Risk assessments in the nuclear power industry (and many others) have proven to be a very effective tool to aid a decision-maker. Licensees and the Nuclear Regulatory Commission routinely use insights from risk assessments to make daily operational decisions, to permit on-line maintenance, to determine the scope and rigor of inspections, to change Technical Specifications, etc. In fact, there are few issues where the question, "how does this impact the risk" is not routinely asked. But, should a risk assessment automatically be performed? Could the lack of information (and data), or lack of an analytical model create a situation where a risk assessment could generate confusion and uncertainty rather than valuable insights for the decision-maker? This paper examines the process to determine if a viable risk assessment to evaluate the failure frequency of a Babcock & Wilcox-designed plants' upper and lower core barrel internals bolts is possible. A risk assessment that can not support the decision-making process is of little value. In this case study, it was concluded that the risk assessment was not feasible to perform.

### Risk Analysis of Escape Time in Buildings of Hong Kong

L. T. Wong and N. K. Fong
*Department of Building Services Engineering, The Hong Kong Polytechnic University, Hong Kong, China*

Fire safety of some buildings is examined from the perspective of the risk of evacuees, who would be unable to escape from an unprotected space through the designated exits in the period of time allowed. This paper, taking account of exit design, occupant load and its variations using the door carrying capacity approach, presents a simple method to determine the probable risk to evacuees in buildings of Hong Kong. The probable risk of evacuees in example residential, institutional and office buildings of Hong Kong was evaluated for certain exit dimensions with the door carrying capacity, with considerations of the uncertainties of the probable occupant loads and the specific flow rates at the exit. The results show that the building occupant load, occupant-load ratio, total exit width and specific flow rate at the exit significantly affect the risk to evacuees. The result would be useful in the risk assessment for safe egress design of buildings.

### Combining Probability Distributions in Operational Risk Management

Dr.ir. Louis Goossens(a), Dr.ing. Jürgen van Grinsven(b)
*a) Safety Science Group, Delft University of Technology, Delft, The Netherlands. b) Nyenrode University, Breukelen, The Netherlands*

The major difficulties and challenges which financial institutions face are closely related to the estimation of their level of exposure to operational risk. In their efforts to estimate this level, they construct a probability distribution using expert judgment. In financial institutions however, no common method exists to combine probability distributions which are derived from multiple experts. Current methods are often considered to

be too complex, time consuming and lack to address problems such as effectiveness, efficiency and satisfaction. Moreover, handling large volumes of data requires a great deal of coordination, especially when derived from multiple expert judgments. In this paper we propose a method for combining probability distributions which are derived from multiple experts. First, we discuss relevant background literature on operational risk and expert judgment. Next, we propose a method to elicit and combine probability distributions which are derived from multiple expert judgments in operational risk management. We applied this method to two case studies in a large Dutch Financial Institution and present our research results. The results indicate that this method is more effective, efficient and leads to more satisfaction when implemented in practice. Finally, the main research issues as well as future developments are discussed.

3:30 - 5:00 PM

## 4-4: Risk Informed Decision Making II

Session Chair: Jon-Erik Holmberg

### Risk Informed In-Service-Inspection Activities within the European Network for Inspection and Qualification

Kaisa Simola(a) and Luca Gandossi(b)
*a) VTT Technical research Centre of Finland, Espoo, Finland. b) European Commission Joint Research Centre, Petten, The Netherlands*

The European Network for Inspection Qualification (ENIQ) was established in 1992 in response to increasing recognition of the importance of qualification of non-destructive inspection systems used in in-service inspection programs for nuclear power plants. ENIQ has established a Task Group on Risk (TGR) to work towards developing best practice for risk-informed in-service inspection methodologies, with the objective of increasing the safety of European nuclear power plants. In March 2005 TGR published a European framework document for risk-informed in-service inspection. More recently, TGR has been working at producing more detailed recommended practices and discussion documents on several RI-ISI related issues. TGR has published reports on following topics: The role of ISI within the philosophy of defense-in-depth; The verification and validation of structural reliability models to be used in RI-ISI programs; The use of expert panels in RI-ISI; The applicability of RI-ISI to the reactor pressure vessel; and RI-ISI updating. Work is ongoing to develop documents on other RI-ISI related issues. In addition, TGR has been active in initiating international projects, such as the JRC-OECD/NEA coordinated RI-ISI benchmark exercise (RISMET), and a project on the relationship between inspection qualification and RI-ISI. This paper describes the activities and publications of TGR to date.

### New Approach to Integrating Various Risk Types Throughout a Development Project

Clayton Smith(a), and Ali Mosleh(b)
*a) Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland, USA. b) University of Maryland, College Park, Maryland, USA*

Project risk management is currently used in several industries and mandated by government acquisition agencies around the world resulting in many guidance documents and standards. Common practice results in the creation of a list of risk items and placing them in a location of a matrix based on an assigned probability and consequence scales. Project teams are then tasked to “move” the items to an acceptable place on the matrix by implementing action plans and contingency procedures. The determination of probability and consequence is often accomplished by committee usually focusing on cost and schedule consequences. Several authors have noted deficiencies in these structures. This paper examines casting the risk management process into a Probabilistic Risk Assessment framework to tie project risk to system risk. Within this structure the definition of risk is consistent with that held by PRA analysts and augmented to address the deviations from an accepted plan. The benefits of such an approach leads to a system where the scenarios tracing risk items to many possible consequences are explicitly understood; the interaction between the cost model, schedule model and system model drive the analysis; probabilities for overruns, delays, increased system hazards are determined directly, and finally a set of importance measure are calculated for risk items, causes, and decision points.

### Application of Risk-Informed Evaluation on the Selected Changes in NPP Dukovany

Stanislav Hustak, Vladislav Pistora
*Nuclear Research Institute Rez plc., Rez, Czech Republic*

Nuclear Research Institute in Rez near Prague, Czech Republic, maintains Living Probabilistic Safety Assessment (Living PSA) program for Nuclear Power Plant Dukovany, a VVER type plant in the Czech Republic. This project has been established as a framework for activities that are related to risk assessment and support for risk-informed decision making. Continuously updated PSA model for all plant operational modes is extensively used for various PSA applications, typically for configuration management using risk monitor during shutdown states or for evaluation of Technical Specifications (TS) changes associated with allowed outage time. Recently, PSA model has been also used to evaluate acceptability of other types of proposed TS changes. Assessment of the possibility to change conditions for pressure hydrotest of primary circuit is an example. Living PSA model is properly refined to reflect information and outputs from deterministic analyses and then used to calculate the risk impact of the given change. Effectiveness of compensatory measures is taken into account as well. Such risk-informed evaluations are typically used as a support for plant licensing submittal to the Czech Regulatory Authority (SUJB). At present time, they are done in accordance with proposed SUJB guideline for risk-informed decision making.

### A Study of Risk-Based Verification for Offshore Engineering Systems

J. Wang(a), J. Phipps(b), and D.B. Matellini(a)
*a) Liverpool John Moores University, Liverpool, UK, b) ABS Consulting Ltd, Warrington, UK*

Risk based verification provides a cost-effective approach for maintaining necessary safety levels for the life cycle of offshore installations. Following a literature review of the topic area and the identification of the research needs, a general risk-based verification framework is proposed with appropriate risk assessment contents incorporated into it. The risk management software THESIS® (The Health, Environment and Safety Information System) is used to implement the framework with the aim of providing the reader with a flavour of how safety data can be managed. The study concludes by highlighting both benefits and limitations of risk-based verification for offshore applications.

# Modeling and Simulation

**Wendesday, Salon B**

10:30 AM - Noon

## 2-7: Expert Judgment

Session Chairs: Ali Mosleh, Nathan Siu

### Is the Expert Judgment Better Than Random Numbers?

Daniela Hanea, Ellen Jagtman and Ben Ale
*Safety Science Group, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands*

Expert judgment method is very often used in risk analysis of complex systems to fill in quantitative data. Although it has been proven that it is reliable source of information when no data is available, many times it raises questions related to the choice of experts and the choice of seed questions used to measure the experts’ performance. Especially with the very complex systems, covering more domains, the right expertise of the assessors is questionable. However, when no data is available but the quantification is necessary, experts with partial knowledge of the problem are better than nothing. But on the other hand, the question is whether they are better than random choices. This paper compares the assessment of three groups of conscious assessors with different levels of field and statistical knowledge with a group of random assessors. The comparison is made based on their calibration and information scores and ranks computed for a set of seed questions. The analysis extends also on the type of questions for which it is expected, that the random assessors and the conscious assessors perform clearly different.

### Treatment of Epistemic Uncertainties with Non-Probabilistic Approaches in Applications of Probabilistic Risk Assessment

Tu Duong Le Duy(a,b), Dominique Vasseur(a), Laurence Dieulle(b), Christophe Bérenguer(b), Mathieu Couplet(a)
*a) Risk Management Department , Electricity of France R&D, Clamart cedex, France. b) Troyes University of Technology- Institut Charles Delaunay/LM2S & STMR UMR 6279, CNRS-Troyes - France*

In Nuclear Power Plants, Probabilistic Risk Assessment (PRA) insights contribute to achieve a safe design and operation. In that context, decision making process must be robust and uncertainties must be taken into account. In the current approach of PRA, parameter uncertainty due to a lack of knowledge is generally represented by a log-normal distribution. However, resorting to a specific probability distribution for PRA parameter uncertainty representation seems to be questionable and could lead to ambiguous results in decision making in some cases. More recently, other mathematical frameworks have been proposed to represent parameter uncertainty in a more appropriate manner. In this paper, we will discuss some important issues in parameter uncertainty representation and study two non-probabilistic frameworks which have been recently proposed to be used in risk assessment: a hybrid (i.e. probabilistic-possibilistic) framework and the Dempster-Shafer theory of evidence. The Dempster-

Shafer theory of evidence framework is recognized in this paper as the most attractive framework with regard to hybrid framework and traditional probability framework in the context of PRA. A unified Dempster-Shafer representation for parameter uncertainty is proposed to deal with current issues and this representation is studied in some PRA practical examples.

### Study on the Effectiveness Evaluation of Crime Prevention System Based on Fuzzy Theory and Risk Entropy

Xi Guo(a), Ruimin Hu(b)
*a) School of Computer Science Wuhan University, Wuhan China. b) National Engineering Research Center For Multimedia Software , Wuhan China*

With the rapid development of industrialization, security situation becomes more and more serious in China. Many cities have established crime prevention systems in order to maintain social stability. With the number of crime prevention system increasing, we need to assess their effectiveness in a scientific and objective manner. In this paper, we first introduce the effectiveness evaluation model based on the concept of risk entropy (the origin of the idea) in crime prevention system. We then apply the Analytic Hierarchy Process and Fuzzy Comprehensive Evaluation methods in the model analysis. We not only solve the problem of interference on subject factors in traditional qualitative method for crime prevention system, but also improve the assessment objectively. In the next stage, we conduct the simulation experiment according to the specific examples of crime prevention system. The case study shows that the assessment results are consistent with the reality and this method can be reasonably used for the effectiveness evaluation of crime prevention system. We believe this work contributes to the theoretical framework guiding the design, development, and deployment of the crime prevention system.

### Numerical Scales for Pairwise Comparisons

Michael A. Elliott
*Department of Nuclear Science and Engineering, Massachusetts Institute of Technology, Cambridge, MA, USA*

It is often desirable in decision analysis problems to elicit from an individual the ranking of a population of attributes according to the individual's preference and to understand the degree to which each attribute is preferred to the others. A common method for obtaining this information involves the use of pairwise comparisons, which allows an analyst to convert subjective expressions of preference between two attributes into numerical values indicating preferences across an entire population of attributes. Key to the use of pairwise comparisons is the underlying numerical scale that is used to convert subjective preferences into numerical values. This scale represents the psychological manner in which individuals perceive increments of preference among abstract attributes and it has important implications about the distribution and consistency of an individual's preferences. Three popular scales, the traditional integer scale, a balanced scale and a power scale are examined. Results of a study of 64 individuals show that none of these scales can accurately capture the preferences of all individuals. It is concluded that applications of pairwise comparisons might benefit from permitting participants to choose the scale that best models their own particular way of thinking about the relative preference of attributes.

### Expert Panel Size vs. Accuracy of Aggregated Estimates: An Empirical Study

Calvin H. Shirazi, Ali Mosleh
*Center for Risk and Reliability, University of Maryland, College Park, Maryland, USA*

Historically, decision-makers have used expert opinion to supplement insufficient data. Expert opinion, however, is applied with much caution. This is because judgment is subjective and contains some degree of uncertainty. Because expert opinion may contain error, it seems logical to consult multiple experts in an attempt to have a more inclusive database. Speculations about the positive correlation between the prediction accuracy and the number of experts, assert that the more experts are elicited, the higher the accuracy of the combined estimate. Question still remains whether empirical data actually support this assertion, and if so, to what extend this link has an impact on practical cases. To answer this question, collected expert judgments empirical data are aggregated in a Bayesian framework using a developed domain independent or 'generic' likelihood functions. Total number of estimates with reduced errors is depicted against the corresponding expert panel size. The objective is to determine the correlation between the number of experts and the accuracy of the combined estimate to recommend an expert panel size.

1:30 - 3:00 PM

## 2-8: Explosions and Fire

Session Chair: Ralph Nyman

### Use of Computational Fluid Dynamics, CFD, for Defining Design Accidental Loads and Optimizing Risk Mitigating Measures

Bjørn Inge Bakken, Joar Dalheim, Ulf Danielsen and Bjørn Hekkelstrand
*Scandpower – Lloyd`s Register, Kjeller, Norway*

Over the past 15 years CFD and FEM methods have been increasingly used in Quantitative Risk Assessments (QRA) and practical safety engineering for the oil & gas industry. Advanced modeling of fire and explosion loads, supported by large scale experiments to validate the tools, has improved the understanding of fire and explosion phenomena. Due to the nature of these accident scenarios a probabilistic approach is required since design for worst case scenarios often is prohibitive. A key question is hence to enable definition of the maximum credible accidental loads, e.g. the 1E-4 explosion load. A method for probabilistic analysis of explosion loads has been developed and is now widely used and accepted in the oil & gas industry. Optimized design of fire protection of pressurized equipment is another element in this context and involves use of passive fire protection, material selection and optimized depressurization systems. A "Guideline for protection of pressurized systems exposed to fire" has been developed. The principles of the guideline are currently being adopted by industry standards like API, ISO and Norsok. The aim of the guideline is to ensure adequate and cost effective fire protection with focus on minimizing the risk of accident escalation.

### A Dynamic Risk Analysis Model for an Offshore Platform

Jan K. Lund
*Scandpower-Lloyd´s Register, Kjeller, Norway*

The RiskSpectrum PSA tool has been successfully used to establish a total risk model for an offshore platform. In order to meet the requirements to a detailed and diversified risk picture for an offshore operator an extra consequence assessment module (RSCM) was developed. A RS/RSCM model of a platform can produce a nuanced risk picture and adjustments to the barriers, changes in activity, reduced or increased manning can be reflected to estimate the risk picture at future points in time. The dynamic risk model identifies trends in the risk parameters that may impair the limits set by the operator´s risk acceptance criteria and hence proactive risk reduction effort can be implemented as part of future modification projects.

3:30 - 5:00 PM

## 2-9: Bayesian Methods and Binary Decision Programs

Session Chair: Don Wakefield

### Minimally Informative Prior Distributions for PSA

Dana L. Kelly, Robert W. Youngblood, and Kurt G. Vedros
*Idaho National Laboratory, Idaho Falls, ID USA*

A salient feature of Bayesian inference is its ability to incorporate information from a variety of sources into the inference model, via the prior distribution (hereafter simply "the prior"). However, over-reliance on old information can lead to priors that dominate new data. Some analysts seek to avoid this by trying to work with a minimally informative prior distribution. Another reason for choosing a minimally informative prior is to avoid the often-voiced criticism of subjectivity in the choice of prior. Minimally informative priors fall into two broad classes: 1) so-called noninformative priors, which attempt to be completely objective, in that the posterior distribution is determined as completely as possible by the observed data, the most well known example in this class being the Jeffreys prior, and 2) priors that are diffuse over the region where the likelihood function is nonnegligible, but that incorporate some information about the parameters being estimated, such as a mean value. In this paper, we compare four approaches in the second class, with respect to their practical implications for Bayesian inference in Probabilistic Safety Assessment (PSA). The most commonly used such prior, the so-called constrained noninformative prior, is a special case of the maximum entropy prior. This is formulated as a conjugate distribution for the most commonly encountered aleatory models in PSA, and is correspondingly mathematically convenient; however, it has a relatively light tail and this can cause the posterior mean to be overly influenced by the prior in updates with sparse data. A more informative prior that is capable, in principle, of dealing more effectively with sparse data is a mixture of conjugate priors. A particular diffuse nonconjugate prior, the logistic-normal, is shown to behave similarly for some purposes. Finally, we review the so-called robust prior. Rather than relying on the mathematical abstraction of entropy, as does the

constrained noninformative prior, the robust prior places a heavy-tailed Cauchy prior on the canonical parameter of the aleatory model.

### Analytical Solutions of Large Fault Tree Models using BDD: New Techniques and Applications

Olivier Nusbaumer(a), Wolfgang Kröger(b), and Enrico Zio(c)
*a) Leibstadt Nuclear Power Plant, Leibstadt, Switzerland. b) Swiss Federal Institute of Technology, Zürich, Switzerland. c) Polytechnic of Milan, Milan, Italy*

Most tools available for quantifying large linked Fault Tree models as used in Probabilistic Safety Assessment (PSA) are unable to produce analytically exact results. The algorithms of such quantifiers are designed to neglect sequences when their likelihood decreases below a predefined truncation limit. In addition, the rare event approximation is typically implemented to the first order, ignoring success paths. In the last decade, new quantification algorithms using the mathematical concept of Binary Decision Diagram (BDD) have been proposed to overcome these deficiencies. Since a BDD analytically encodes Boolean expressions, exact failure probabilities can be deduced without approximation or truncation. However, extended effort is required when converting a given Fault Tree to its BDD form; this turns out to be an optimization problem of NP-complete complexity. Several innovative optimization techniques are developed and investigated as a case study on the fullscope PSA model of the Leibstadt Nuclear Power Plant. We succeeded in converting the Leibstadt PSA model into a BDD with more than 1'500'000 nodes, for a total of 3650 basic events. The BDD covers a complete Event Tree sequence that includes reactor shutdown and cooling with all Emergency Core Cooling Systems and support systems, enabling objective comparisons between quantification tools.

### A Comparison of Two Different Methods of Solving a Fault Tree using Binary Decision Diagrams

Ola Bäckström, Wang Wei and Daniel Ying
*Scandpower-Lloyd's Register, Stockholm, Sweden*

Different methods for solving PSA models are being developed, among these methods Minimal Cutsets (MCS) and Binary Decision Diagrams (BDD) are the most relevant. The MCS method is fairly quick but its disadvantage is that it is an approximation of the solution. The BDD method is an exact solution, but instead takes a serious amount of computer resources and will in many cases lead to too large calculation models with unreasonable calculation time on normal computers. The BDD method should not be overseen though since there are possible shortcuts that make the solutions more obtainable. This paper will discuss two different methods of solving a fault tree using BDD; one using a Shannon Decomposition Algorithm and one using a Pivotal Propagation Algorithm. There are several techniques for solving fault trees using BDDs and one issue to consider is modularization. This can be done while preprocessing the fault tree before the actual BDD is built or it can also be done on the fly while the BDD is being built. One of the difficulties of building a BDD is to get a sensible variable ordering. It is well known that changing the order of the variables can cause the number of nodes to increase in the resulting BDD. This is a main issue in creating a good ordering of the variables. Different techniques of performing this will also be discussed. It is also important to develop some sort of truncation technique that can be applied in the case when the BDD becomes too large. A good BDD algorithm should also be able to work on any types of fault trees. Therefore it is essential that the algorithm can handle not logic structures. The two methods handles not logic in different ways, in the pivotal propagation algorithm, the not logic is handled naturally by the construction of the algorithm, where as in the Shannon decomposition method requires some more work. Finally we will discuss some different ways of quantifying the final BDD.

### Importance Measures for Hybrid Causal Logic Models

Chengdong Wang, Ali Mosleh
*Center for Risk and Reliability, University of Maryland, College Park, MD, USA*

Hybrid Causal Logic (HCL) is a multi-layered modeling technique, combining Bayesian belief networks (BBN) with conventional Probabilistic Risk Assessment (PRA) framework. The method and a PRA software platform for modeling and analysis based on HCL methodology has been applied in a few major risk applications in civil aviation, and oil sectors. Since HCL is a hybrid of binary logic and BBN, many of the conventional algorithms needed for risk assessment and risk management activities (such as uncertainty propagation, and risk importance measures) could no longer be used. This paper described the way that some of the more popular risk importance measures (Risk Achievement Worth and Vesely-Fussell) can be applied in HCL context. A simple example is provided to illustrate the process.

# Human Reliability Analysis

**Wendesday, Salon C**

10:30 AM - Noon

## 5-7: HRA Qualitative Analysis

Session Chairs: Helena Broberg, Jan-Erik Holmberg

### Qualitative Analysis Makes Simple HRA Methods a Competitive Alternative

Johanna Oxstrand(a), Kent Bladh(b), and Stephen Glen Collier(c)
*a) Vattenfall Ringhals AB, Varobacka, Sweden. b) Vattenfall Power Consultant, Malmo, Sweden. c) Institue for Energy Technology, Halden, Norway*

This paper intends to illustrate how a well-conducted qualitative analysis reduces the importance of choosing a specific human reliability analysis method. This conclusion is motivated by the results of the research project International HRA Empirical Study where several human reliability analysis (HRA) methods were implemented and their individual results compared to empirical data. This paper focuses on the implementation of the HEART method within this study as conducted by the authors. HEART obtained highly competitive results, especially considering the traditional view of HEART as a "quick-and-dirty" approach. This paper explains how the competitive results are due to the underlying qualitative analysis conducted before HEART was applied. The competitive results for HEART illustrate how even a simplified method can get credible results when combined with good qualitative insights.

### A Performance Shaping Factors Causal Model for Nuclear Power Plant Human Reliability Analysis

Katrina Groth and Ali Mosleh
*University of Maryland, College Park, MD, USA*

Many current Human Reliability Analysis (HRA) methods calculate human error probability (HEP) based on the state of various PSFs. There is no standard set of PSFs used in HRA, rather each method uses a unique set of PSFs, with varying degrees of interdependency among the PSFs. In calculating HEPs, interdependency is generally ignored or addressed through varying parameters in linear or loglinear formulas. These dependencies could be more accurately represented by a causal model of PSF relationships. This paper introduces a methodology to develop a data-informed Bayesian Belief Network (BBN) that can be used to refine HEP prediction by reducing overlap among PSFs. The BBN framework was selected because it has the ability to incorporate available data and supplement it with expert judgment. The methodology allows the initial models to be updated as additional data becomes available. This paper presents a draft model based on currently available data from human error events in nuclear power plants. The resulting network model of interdependent PSFs is intended to replace linear calculations for HEPs.

### How Many Performance Shaping Factors are Necessary for Human Reliability Analysis?

Ronald L. Boring
*Idaho National Laboratory, Idaho Falls, Idaho, USA*

It has been argued that human reliability analysis (HRA) has expended considerable energy on creating detailed representations of human performance through an increasingly long list of performance shaping factors (PSFs). It is not clear, however, to what extent this refinement and expansion of PSFs has enhanced the quality of HRA. Indeed, there is considerable range in the number of PSFs provided by individual HRA methods, ranging from single factor models such as timereliability curves, up to 50 or more PSFs in some current HRA models. The US Nuclear Regulatory Commission advocates 15 PSFs in its HRA Good Practices (NUREG-1792), while its SPAR-H method (NUREG/CR-6883) espouses the use of eight PSFs and its ATHEANA method (NUREG- 1624) features an open-ended number of PSFs. The apparent differences in the optimal number of PSFs can be explained in terms of the diverse functions of PSFs in HRA. The purpose of this paper is to explore the role of PSFs across different stages of HRA, including identification of potential human errors, modeling of these errors into an overall probabilistic risk assessment, quantifying errors, and preventing errors.

1:30 - 3:00 PM

# 5-8: Improving Safety and Reliability Through HRA Applications

Session Chairs: Pierre Le Bot, Pamela Nelson

### What place for Human Reliability Assessment in the Reliability approach and in Human Factors Approaches?

Helene Pesme, Pierre Le Bot
*EDF R&D, Clamart, France*

Human Reliability is a discipline found at the intersection of two fields, Reliability and Human Sciences, for the study of high-risk socio-technical systems. This discipline has its own area of expertise but ultimately remains somewhat disconnected from, and indeed little-known in the two fields from which it comes, at least in France. It deserves a higher profile. This article proposes to highlight the characteristics of human reliability and its findings and development prospects, in the spheres of both reliability and the human factor alike, from the EDF viewpoint. Promoting human reliability both in the field of reliability and in the field of human factors is fundamental. The establishment of an Association for Human Reliability is proposed in order to achieve this objective, following the model of existing associations in the fields of reliability or ergonomics. The PSAM 10 Conference and pre-workshop could be a first milestone for this ambitious but essential objective.

### Human System Simulation in Support of Human Performance Technical Basis at NPPs

David I Gertman, Jeffrey Joe, Alan Mecham, William Phoenix, Katya Le Blanc and Samy Tawfik
*Human Factors, Controls, and Statistics Department, Idaho National Laboratory (INL), Idaho Falls, ID*

This paper focuses on strategies and progress toward establishing the Idaho National Laboratory's (INL's) Human Systems Simulator Laboratory at the Center for Advanced Energy Studies (CAES), a consortium of Idaho State Universities. The INL is one of the National Laboratories of the US Department of Energy. One of the first planned applications for the Human Systems Simulator Laboratory is implementation of a dynamic nuclear power plant simulation (NPP) where studies of operator workload, situation awareness, performance and preference will be carried out in simulated control rooms including nuclear power plant control rooms. Simulation offers a means by which to review operational concepts, improve design practices and provide a technical basis for licensing decisions. In preparation for the next generation power plant and current government and industry efforts in support of light water reactor sustainability, human operators will be attached to a suite of physiological measurement instruments and, in combination with traditional Human Factors Measurement techniques, carry out control room tasks in simulated advanced digital and hybrid analog/digital control rooms. The current focus of the Human Systems Simulator Laboratory is building core competence in quantitative and qualitative measurements of situation awareness and workload. Of particular interest is whether introduction of digital systems including automated procedures has the potential to reduce workload and enhance safety while improving situation awareness or whether workload is merely shifted and situation awareness is modified in yet to be determined ways. Data analysis is carried out by engineers and scientists and includes measures of the physical and neurological correlates of human performance. The current approach supports a user-centered design philosophy (see ISO 13407 "Human Centered Design Process for Interactive Systems, 1999) wherein the context for task performance along with the requirements of the end-user are taken into account during the design process and the validity of design is determined through testing of real end users.

### Improving Safety With Dynamic Probabilistic Risk Assessment – ADS-IDAC as a Human Reliability Analysis Tool

Kevin Coyne(a) and Ali Mosleh(b)
*a) U.S. Nuclear Regulatory Commission, Washington D.C., USA. b) University of Maryland Center for Risk and Reliability, College Park, MD, USA*

State-of-the-art dynamic simulation probabilistic risk assessment (PRA) approaches offer significant advantages for the analysis of nuclear power plant crew behaviors during off-normal and accident conditions. For example, dynamic simulation probabilistic risk assessment methods that integrate nuclear plant thermal-hydraulic information with an operator behavior model can improve the identification and quantification of human error events. Furthermore, dynamic simulation methods can provide a more realistic prediction of the consequences of human error events than the conventional fault tree/event tree static PRA framework. As dynamic methods reach an increased level of maturity, they can contribute to human reliability analysis (HRA) in a number of important ways, including assessment of plant procedures; identification of potential human error events (including errors of commission); evaluation of the consequences arising from operator errors; and human performance data collection and analysis. This paper describes several potential applications for the ADS-IDAC dynamic simulation approach. For example, the detailed operating procedure model used in ADS-IDAC can support the evaluation and assessment of plant emergency operating procedures, particularly procedure branching requirements that rely on thermal-hydraulic plant conditions. The knowledge-based operator behavior model provides improved capabilities for identifying situational contexts that may lead to improper operator actions (e.g., the use of normally useful rules during inappropriate circumstances). Because dynamic simulation methods explicitly model the plant thermal-hydraulic response to operator actions, they can provide a more realistic assessment of the consequences from error events. Finally, because ADS-IDAC attempts to capture underlying cognitive processes that drive crew behaviors, it provides an efficient framework for capturing actual operator performance data such as timing of operator actions, mental models, and decision-making activities.

3:30 - 5:00 PM

# 5-9: Applications, Tools, and Comparisons

Session Chairs: Johanna Oxstrand, Salvatore Massaiu

### Application of the ATHEANA Methodology for the HRA of a PSA Scenario for a BWR Nuclear Power Plant

Teresa Ruiz-Sánchez, Pamela F. Nelson
*Universidad Nacional Autónoma de México, Jiutepec, Morelos, México*

ATHEANA is a second generation methodology that directs a multidisciplinary group to use guide words to search for deviations that are random variations of the nominal context usually evaluated in the Human Reliability Analysis (HRA) methods. This paper presents an application of this method for one scenario of loss of Balance of Plant in a Boiling Water Reactor (BWR) nuclear power plant. The Human Failure Event (HFE) identified was the failure to perform the emergency depressurization given the failure to align the booster pumps (the system that injects coolant into the pressure vessel at an intermediate pressure). The findings included the fact that these types of plant deviations are often included in the training scenarios in plant simulators, especially when the instructors are very knowledgable Senior Reactor Operators who have experienced similar ocurrences in their operating days. In order to quantify the Human Error Probability (HEP) for each unsafe action, a hybrid method was used; that is, that the quantification was performed using The CBDTM (Cause Based Decision Tree Method) and THERP (Technique for Human Error Rate Prediction), instead of the ATHEANA quantification approach.

### Consideration of Success Path in PRA Accident Sequences for Identification of Human Interaction Dependencies

Alexander Trifanov
*Kinectrics Inc., Toronto, Canada*

It is recognized that dependent failures are often significant risk contributors. Probabilistic Risk Assessments traditionally search for dependencies between operator actions within accident sequences by reviewing cutsets containing multiple human errors. It is evident that this approach identifies only dependencies between failed operator actions in the same accident sequence. However, combinations including both successful and failed actions in the same accident sequence are quite common and may be missing from the dependency analysis. Although existing PRAs are able to identify most of risk-significant dependencies, some unfeasible sequences of operator actions may still be credited, vulnerabilities in accident mitigation strategies may be overlooked, and contribution of some accident sequences to the core damage frequency may be unrealistic. This paper demonstrates the described deficiency in traditional methods and proposes approaches how to identify complete sequences of human interactions for human error dependency analysis.

### A Tool for PANAME HRA Method

V. Fauchille, J.Y. Maguer
*Institut de Radioprotection et de Sûreté Nucléaire, Fontenay-aux-Roses Cedex, France*

PANAME is the HRA method implemented at the IRSN for the level 1 PSA models. PANAME is a first generation HRA method and in this case the time available for the operators to implement a safety significant action is a sensitive parameter. Previous applications of PANAME highlighted a user's effect in evaluating the durations of operator's paths through the procedures. To cope with this difficulty, the IRSN developed "the Additional Calculation Tool" (ACT). This tool supports the analysts in calculating the necessary duration for an average speed operator to path through an instruction up to a point. It was designed from the observation that an emergency operating procedure is a succession of basic elements: tests, required information exchanges, controls and actions. On the basis of experience feedback from operational events and

simulation runs, a mean duration was allocated to each of the basic elements. Finally a calculation sheet was implemented on a spreadsheet to computerize the process. Calibration of the tool is still ongoing. From now on, this tool was used to produce the HRA data of a level 1 PSA study and results are satisfactory.

# PSA Applications

**Wendesday, East Room**

10:30 AM - Noon

## 1-7: Data and Aging

Session Chairs: Yet Pole, Pat Baranowsky

### Supporting Preliminary Design Decision Making with A Risk Data Base

Joseph R. Fragola
*Valador Inc, Rockville Centre, NY, USA*

Attribute identification, class assignment, and the development of correspondences of classes of attributes to ranges of reliability measures are critical to the proper development and application of reliability data. The proper assignment of attribute classes can allow for the establishment of reasonable estimates of the credible range to be expected for reliability measures for devices even if they are not yet existent, or for devices whose reliability measures are unknown to the analyst as long as their attributes can be brought into correspondence with known device attribute classes. Proper class structuring of a database allows reliability measures to be applied, albeit within a range of uncertainty, so as to be useful during the preliminary design stages where the elements of the design are necessarily conceptual and reliability measures provide significant value needed to the designer. This paper addresses design as a decision making process and discusses the manner in which the designer might “logically” proceed in this decision making considering the apparent lack of historical precedent for truly “new” designs. It also discusses the characteristics of a database, which might be useful to support decision making at the preliminary stages of the design process, how such a database might be developed, and how it might be employed to support the development of viable preliminary designs.

### PRA Database Update Process Concepts

Erin P. Collins(a), Cindy A. Williams(b), and Pierre Macheret(c)
*a) SAIC, New York, NY, USA. b) First Energy Nuclear Operating Company, Akron, OH, USA. c) SAIC, Las Vegas, NV, USA*

This paper discusses the information cross-over that exists between Probabilistic Risk Assessment (PRA), Reactor Oversight Program (ROP) Mitigating System Performance Index (MSPI) program and Maintenance Rule activities, and how to collect, categorize and apply the data in a manner consistent with the ASME/ANS RA-Sa–2009 Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications sections on Data Analysis high level and supporting requirements. In addition, guidance will be provided on documentation of PRA updates consistent with Regulatory Guide 1.200.

### When the Details Matter – Sensitivities in PRA Calculations That Could Affect Risk-Informed Decision-Making

Dana L. Kelly
*Idaho National Laboratory, Idaho Falls, USA*

As the U.S. nuclear industry continues its efforts to increase its use of risk information in decision making, the detailed, quantitative results of probabilistic risk assessment (PRA) calculations are coming under increased scrutiny. Where once analysts and users were not overly concerned with figure of merit variations that were less than an order of magnitude, now factors of two or even less can spark heated debate regarding modeling approaches and assumptions. The philosophical and policy-related aspects of this situation seem to be well-recognized by the PRA community. On the other hand, the technical implications for PRA methods and modeling have not been as widely discussed. This paper illustrates the potential numerical effects of choices as to the details of models and methods for parameter estimation with four examples: 1) issues related to component boundary and failure mode definitions; 2) the selection of the time period data for parameter estimation; 3) the selection of alternative diffuse prior distributions, including the constrained non-informative prior distribution, in Bayesian parameter estimation; and 4) the impact of uncertainty in calculations for recovery of offsite power.

### Standards, Guidance and Practices for Improved Data Quality

Martin B. Sattison
*Idaho National Laboratory*

Since the mid 1980s, the Idaho National Laboratory (INL) has been involved with numerous projects to collect operational reactor data, develop data tools, and trend and analyze that data for the U.S. Nuclear Regulatory Commission (NRC). Because the data are used in subsequent risk analyses, the NRC must have confidence in the quality of the data delivered. The NRC tasked the INL to establish a comprehensive data quality assurance program. A key element of that effort was to establish a set of requirements based on industry and government standards, guidance and good practices. This paper discusses where these were found, the process of extracting the requirements and recommendations from the source materials, and the consolidation of them into a concise set of 22 standards, guidance and practices for technical data quality. While this set was created specifically for the data programs within the NRC"s Office of Research, they have broad application to many high-technology industries.

1:30 - 3:00 PM

## 1-8: Instrumentation & Control I

Session Chairs: Hui-Wen Hunag, Martin Sattison

### International Experience with Modeling Digital Systems in PSAs

Tsong-Lun Chu(a), Gerardo Martinez-Gurdi(a), Alan Kuritzky(b), and Abdallah Amri(c)
*a) Brookhaven National Laboratory, Upton, NY, USA. b) U.S. Nuclear Regulatory Commission Washington, DC, USA. c) Nuclear Energy Agency, Paris, France*

This paper summarizes the discussions and recommendations from an international technical meeting focused on current experiences with reliability modeling and quantification of digital systems in the context of probabilistic safety assessments of nuclear power plants. The meeting was organized by the Working Group on Risk Assessment of the Committee on the Safety of Nuclear Installations of the Nuclear Energy Agency of the Organization for Economic Co-operation and Development, and was held in Paris, France during October 2008.

### Integrated Functional Safety And Security Analysis Of The Process Control And Protection Systems With Regard To Uncertainty Issue

Tomasz Barnert, Kazimierz T. Kosmowski, and Marcin Śliwiński
*Gdansk University Of Technology, Gdansk, Poland*

This Paper Discusses An Attempt To Integrate Safety And Security Issues With Respect To Functional Safety Analysis. Taking Into Account Distributed Control And Protection Systems The Issue Of Integrating Functional Safety With Security Analysis Appears. This Integration Is Connected With Some Classification Of Communication Channels Used In The System As Well As Occurrence Of The Scada (Supervisory Control And Data Acquisition) Solution. Both Mentioned Aspects Should Be Included In The Security Vulnerability Assessment Carried Out For Such Kind Of Systems. Another Difficulty Is The Fact That Both Safety And Security Aspects Consist Of Two Different Groups Of Functional Requirements For The Control And Protection Systems. In The Paper It Is Proposed That The Security Aspect Should Be Considered As A Risk Parameter Taken Into Account In The Functional Safety Analysis As Well As Its Influence On Uncertainty Of Results. On The Other Hand There Is A Verification Issue Of Required Sil For Designed Safety-Related System, Which Implements A Safety Function. In This Case The Result Of Security Analysis Is Affecting Uncertainty Of Probabilistic Model Parameters. Thus, The Security Analysis Is Some Kind Of Bridge Connecting Determining Of Required Sil (Safety Integrity Level) And Its Verification In The Process Of Functional Safety Analysis.

### Risk-Informed Safety Classification in Plant Automation Modifications of Loviisa NPP

Kalle Jänkälä
*Fortum Power Division / Nuclear Safety, Espoo, Finland*

The original analogue automation of Loviisa NPP in Finland will be replaced with digital automation with expected completion in year 2016. The automation renewal is implemented in overlapping stages for the two VVER-440 units commissioned in 1977 and 1980. A proposal for a safety class shall be submitted to the Finnish Nuclear Safety Authority (STUK) in conjunction with the preliminary inspection document of a system change. In conjunction with extensive changes concerning whole systems the safety classification shall be assessed by Probabilistic Risk Assessment (PRA). The assessment shall be used to demonstrate that the quality management system required by the safety classification of each component is adequate compared with the risk importance of the component. Some safety classification proposals and their risk-informed

assessments have already been submitted to STUK. The methodology and reasoning is presented in this paper with examples indicating that PRA importance measures can be used to valuate a safety significance of a system for safety classification in spite of the difficulties in estimating the reliability of digital automation.

3:30 - 5:00 PM

## 1-9: Instrumentation & Control II

Session Chairs: Jan-Erik Holmberg, Mike Calley

### Development of the Ringhals 1 PSA with Regard to the Implementation of a Digital Reactor Protection System

Stefan Authén(a), Erik Wallgren(a) and Stefan Eriksson(b)
*a) Risk Pilot AB, Stockholm, Sweden. b) Ringhals NPP, Väröbacka, Sweden*

This paper presents the implemented process for assessment and modification of the PSA study of the Swedish NPP Ringhals 1 due to the ongoing safety enhancement program regarding Digital Reactor Protection System (RPS) connected with improvements of safety functions. The chosen technical RPS concept is based on the addition of a new diversified and digital protection function (a "backpack" called the Diversified Plant Section, DPS) while maintaining the existing relay-based RPS. The purpose is to be able to handle events requiring separation (mainly external events, e.g. fire), that the existing RPS cannot handle with regard to enhanced authority requirements. The major part of the existing equipment within the RPS will hence be retained. This paper focus on the challenges in achieving a realistic model of a software based Reactor Protection Systems with traditional fault tree technique and the integration into existing PSA-models. Issues such as level of detail in modeling, critical failure modes, failure data, continuous monitoring, complex validation of input parameters and safety functions, complex dependencies and fault tree structures are addressed. Importance analyses and lessons learned are presented together with Ringhals conclusions.

### Risk Insights Associated with Digital Upgrades

David Blanchard, Ray Torok
*a) Applied Reliability Engineering, Inc., San Francisco, CA, USA. b) Electric Power Research Institute, Palo Alto, CA, USA*

Nuclear power plants are considering upgrades to existing instrumentation and control systems (I&C) to address equipment obsolescence issues and to take advantage of reliability and safety benefits that can be achieved with digital technologies. It is recognized, however, that when implementing a digital upgrade, there is potential for introducing new common-cause failure modes (CCF) associated with the digital equipment including its software. This paper presents the results of research performed with a full scope, Level 1, internal events PRA for a PWR to assess the impact of varied levels of reliability and diversity in the upgrading of plant I&C systems to digital equipment. The focus of the analysis was to • determine for what accident sequences in a PRA digital common-cause failures could have a significant effect on safety and, if possible, • establish what level of diversity and defensive measures in the I&C could limit this effect were it to be found to be significant. The results of this research demonstrate that plant risk can be made insensitive to postulated digital CCF by ensuring digital systems are implemented with defense-in-depth and diversity levels consistent with those of the plant mitigating systems which they are to control.

### Field Programmable Gate Arrays (FPGA) Application for Diverse Backup System

Hui-Wen Huang(a), Mao-Sheng Tseng(a), Chunkuan Shih(b), Kai-Lan Chang(b) and Tsu-Mu Kao(a)
*a) Institute of Nuclear Energy Research (INER), Taoyuan County, Taiwan (R.O.C.). b) Institute of Nuclear Engineering and Science, National Tsing Hua University, Hsinchu, Taiwan (R.O.C.)*

The digitalized Instrumentation and Control (I&C) system of nuclear power plants (NPP) could provide operator easily Human-Machine Interface (HMI) and more powerful overall operation capability. However, some software errors may cause a kind of Common Cause Failure (CCF). As a consequence, the event of Anticipated Transients Without Scram (ATWS) will occur. In order to assure that the plant can be shutdown safely and to follow the requirements of 10CFR50.62, the utility builds up various ATWS mitigation features in NPP. The features include Fine Motion Control Rod Drive Run In, Alternate Rod Insertion, Standby Liquid Control System, Reactor Internal Pump Trip or Runback, Feedwater Flow Runback and Inhibition of Automatic Depressurization System. This research developed an evaluation method of diverse back-up means for computerized I&C system. A diverse back-up of digital I&C system is the most important means to defend against CCF and un-detectable software faults. Institute of Nuclear Energy Research (INER) is developing a computerized I&C test facility, which is incorporated a commercial grade I&C systems with Personal Computer Transient Analyzer (PCTran)/Advanced Boiling Water Reactor (ABWR), a NPP simulation computer code. By taking the technology of Field Programmable Gate Array (FPGA) to implement the methods of ATWS mitigation, the research built up a diverse back-up of digital I&C system to expect to defend against CCF and un-detectable software faults. According to the testing and evaluation, the work can be achieved the analysis of Diversity and Defense-in-Depth (D3).

# External Events

**Wendesday, West Room**

10:30 AM - Noon

## 15-7: Seismic: Hazards and Response Analysis

Session Chairs: Khaled Joober, Payam Ashtari

### Continuous Combinatorial Critical Excitation for S.D.O.F Structures

P. Ashtari and S.H. Ghasemi
*Civil Engineering Department of Zanjan University, Zanjan, Iran*

Earthquake is an uncertain and random phenomenon. Therefore, it is so much important to find an excitation which can create the highest crisis in a structure under some specific constraints of the earthquake such as earthquake intensity and amplitude limit of power spectral density (PSD). The critical excitation proposed here, in this paper, is introduced in the frequency domain and the objective function is the maximization of the mean square of story drift. The proposed critical excitation has the capability to cover the frequency range of power spectral density function and to have maximum responses. For this purpose, effort is made to adapt a linear combination of $F(\omega)$ and Kanai-Tajimi equation as the critical excitation, where $F(\omega)$ represents critical response of the structure and Kanai- Tajimi equation is PSD of the past natural earthquakes. These excitations are referred to as continuous critical excitation. Also, single degree of freedom structures are investigated in the stationary sate. Finally, the proposed method is compared with the other's method of finding critical excitation.

### Implementation Guidance for SSHAC Level 3 and 4 Processes

Kevin J Coppersmith(a), Julian J Bommer(b), Ann Marie Kammerer(c) and Jon Ake(c)
*a) Coppersmith Consulting Inc, Walnut Creek, CA, USA. b) Imperial College London, London, UK. c) US Nuclear Regulatory Commission, Washington DC, USA*

Risk analysis for critical facilities requires a probabilistic assessment of the hazards that could affect the installation. The complexity of the processes that generate geological hazards such as seismic ground shaking and volcanic events is such that there is inevitably large uncertainty associated in the hazard assessment. This uncertainty is reflected in the range of legitimate technical interpretations made by informed technical experts based on the available data. Procedures to develop multiple expert assessments for seismic hazards in a structured process have been established in the SSHAC (Senior Seismic Hazard Analysis Committee) guidelines. The objective of the present paper is to capture and clarify the insights gained from performing a number of detailed assessments using the SSHAC approach over the past 10-15 years. Unlike classical expert elicitation, which attempts to extract information from independent experts, the SSHAC process encourages interaction amongst experts and fosters learning by the experts throughout the process, with the ultimate objective of capturing the full community distribution of technical interpretations. The SSHAC guidelines, written largely in abstract, have now been implemented in practice several times. In these studies valuable lessons have been learned, which are now being distilled into a new U.S. Nuclear Regulatory Commission NUREG-series report to provide practical guidance on implementing SSHAC processes for hazard assessments. A key lesson from these studies is that higher level SSHAC processes (Levels 3 and 4) which specify the use of a Participatory Peer Review Panel (PPRP), provide a higher degree of regulatory assurance and stability for the initial development of hazard models for safety-critical installations. Also, significant technically-informed participation by project sponsors and regulators throughout the process enhances the likelihood of regulatory acceptance.

### Seismic Fragility Evaluation of an Electrical Transmission Substation System in Korea by using a Fault Tree Method

Min Kyu Kim, Young-Sun Choun, and In-Kil Choi
*Korea Atomic Energy Research Institute, Daejeon, Korea*

In this study, a seismic fragility analysis was performed for an electrical transmission substation system in Korea. For the evaluation of the seismic fragility function of the electrical transmission substation system, a fragility analysis about each type of equipment and facility was performed and finally a fragility analysis about the whole electri-

cal transmission substation by using a Fault-tree analysis was performed because the electrical transmission electrical transmission substation system consists of several equipment and facilities. The target equipment in the GIS type electrical transmission electrical transmission substation was selected as the transformer systems and the insulated bushings based on previous earthquake hazard records. The failure mode of a transformer is considered as a sliding, overturning and the failure of a bushing. The failure criteria for sliding and overturning were determined by considering the friction resistance and moment resistance. The failure criteria for the bushing failure estimated the maximum acceleration response at the connection points of a bushing and a transformer body. The failure mode of the insulated bushing was also determined by the maximum acceleration response at the connection points of a bushing and a steel structure. To evaluate the probability of a failure for a whole electrical transmission electrical transmission substation system, a fault tree by considering a 4 bank system electrical transmission electrical transmission substation was constructed. For the evaluation of the probability of a failure for a one bank system, a fault tree was constructed. Finally, the seismic fragility was evaluated for the Transmission systems in Korea.

### Gentilly-2 CANDU Nuclear Power Plant level 1 Fire and Flood PSA – Insights on a Work in Progress

K. Joober(a), C. Selman(a), J-F. Bolduc(a), A. Nava Dominguez(a) , A. Bellil(a), T. Houasnia(b), R.Vaillancourt(b)
*a) GENIVAR LP, Montréal, Québec, Canada. b) Hydro-Québec, Montréal, Québec, Canada*

The objective of this report is to present a summary of work performed to date on the Level 1 Internal Fire and Flood PSA for the Hydro-Québec Gentilly-2 CANDU Nuclear Power Plant. The overview will present findings, observations, challenges, and solutions that have been developed to supplement the NUREG/CR-6850 and EPRI-1019194 methodologies.

1:30 - 3:00 PM

## 15-8: Seismic: PRA

Session Chairs: Soli Khericha, Ching Guey

### AOT Study Using Seismic PSA and Associated Issues

Haruo Fujimoto and Keisuke Kondo
*Japan Nuclear Energy Safety Organization (JNES), Tokyo, Japan*

Using a 4-loop PWR seismic PSA model, a trial study on AOTs was made. Specifically, CDF and ICCDP were calculated for HPIS, LPIS, AFWS, DGs and SWS, assuming one of their trains being out of service, respectively. In addition, sensitivity studies on SWS operation mode and the correlation model of failures due to seismic were performed. According to the results, ICCDPs satisfied the criterion of 5x10-7 except SWS. On the other hand, ICCDP of SWS met this requirement if the train separation of SWS and CCWS was assumed not to do when ECCS operation mode was changed. The perfect correlation model of equipment failures due to seismic, commonly used in seismic PSA models, leads conservative results of CDF. However this assumption is not appropriate to evaluate ICCDP. According to the results of sensitivity studies, the perfect correlation model provided the smallest ICCDP as expected. However, the relationship between CDF and ICCDP for the different correlation models did not show a downward-sloping tendency as expected. Investigation using a simplified model revealed that errors originated from the upper-bound approximation used in quantification would be one of the causes of this deficiency especially when the probabilities of basic events become large.

### Insights Gained from the Beznau Seismic PSA

Martin Richner(a), Sener Tinic(c), Dirk Proske(a), Mayasandra Ravindra(b), Robert Campbell(b), Farzin Beigi(b) and Alejandro Asfura(c)
*a) Axpo AG, Nuclear Power Plant Beznau, Doettingen, Switzerland. b) ABS Consulting, 300 Commerce Drive, Irvine, CA USA. c) APA Consulting, 181 Rudgear Drive, Walnut Creek, CA, USA*

The most recent results and insights gained from Seismic Level 2 PSA study of the Beznau NPP are shown. Beznau is the oldest operating PWR worldwide. The plant was extensively backfitted during the last years, especially with respect to seismic events. The paper shows the recent results of the probabilistic seismic hazard study performed for the four NPPs in Switzerland. This so called PEGASOS study was performed according to the SSHAC procedures (NUREG/CR-6372) at the highest elaborated Level 4.. Switzerland is an area of low to moderate seismicity and the PEGASOS study was the first one of that kind performed for a NPP at that high level. The paper also presents the methods, results and conclusions of the Beznau Seismic PSA. Some examples illustrate how plant safety was improved based on the results of the seismic PSA. The paper discusses the role of the seismic capacity of the containment with respect to the large early release frequency (LERF). In addition, the calculated results indicate that seismic events are important contributors to the core damage frequency (CDF) and to the LERF even in areas of low to moderate seismicity. Based on the PEGASOS seismic hazard results, an outlook is given on the reactor building seismic capacity required for Advanced Light Water Reactors (ALWRs).

### Study on Effects of Correlative Degree of Component Damages on Seismic PSA during Component Outage

Y. Katagiri(b), Y. Narumiya(a), T. Ohya(a), T. Kuramoto(b), K. Toyoshima(b), T. Higashiyama(b)
*a) Kansai Electric Power Company (KANSAI). b) Nuclear Engineering, Ltd. (NEL)*

For the purpose of risk-informed decision making about plant safety management activities, all risks from internal and external events that affect those activities should be evaluated. In Japan, seismic effects are particularly important in this respect. In this study, to confirm the effects on increase in seismically-initiated risks during component outage, which are caused by the difference of correlative degrees of component damages and the difference of component which is set out of service, the core damage frequency (CDF) attributable to an earthquake during component outage and the increase ratio of CDF which is defined as the ratio of CDF without component outage to CDF with component outage (hereinafter this ratio is called RAW.) are evaluated. This study shows that a conservative evaluation of seismically-initiated effect during component outage can be performed by assuming the completely dependent correlation of component damages for CDF and the completely independent correlation for RAW. These trends do not change depending on the component which is set out of service and these indexes become higher as effects for other systems due to component outage become larger. It is also confirmed that RAW of Seismic PSA is excessively larger than that of internal event PSA.

3:30 - 5:00 PM

## 15-9: Wind, Hurricane and Lightning

Session Chair: James Lin

### Statistical Modeling of Power Outage Duration Times in the Event of Hurricane Landfalls in the USA

Roshanak Nateghi(a), Seth D. Guikema(a), and Steven M. Quiring(b)
*a) Johns Hopkins University, Baltimore, MD, U.S.A. b) Texas A&M University, College Station, TX, USA*

This paper compares statistical methods for modeling power outage durations during hurricanes and examines the predictive accuracy of these methods. Being able to make accurate predictions of power outage durations is valuable because the information can be used by utility companies to plan their restorations efforts more efficiently. This information can also help inform customers and public agencies of the expected outage times, enabling better collective response planning and coordination of restoration efforts for other critical infrastructures that depend on electricity. We compare the out-of-sample predictive accuracy of five distinct statistical models for estimating power outage duration times in the event of a hurricane land-fall in the U.S. The methods compared include both regression models (accelerated failure time and Cox proportional hazard models) and data mining techniques (regression trees, Bayesian additive regression trees and multivariate additive regression splines). Our results indicate that Bayesian additive regression trees yield the best prediction accuracy.

### Estimation of Uncertainty Distributions for Internal Flood Initiators Using Parametric Sensitivity Study

Robert J. Wolfgang
*ERIN Engineering and Research, Inc., West Chester, PA, USA*

Appendix A of EPRI Technical Report 1013141 lists the failure rate uncertainty distributions of the various flooding modes obtained from industry data for the various piping systems that were used in calculating initiating event frequencies for various PRA internal flood scenarios. To help understand the effect on the uncertainty associated with the initiating frequency for an internal flood scenario based on contributions from various water systems, a parametric study was performed in which each of the system piping failure rates was fitted to a cumulative distribution based on the reported 5th, 50th, and 95th percentiles. An additional source of uncertainty was the estimate of pipe diameters and lengths for those recorded water sources obtained during plant walkdowns. A distribution of values was then assigned to these parameters to help bound the estimated uncertainty associated with obtaining this type of data in the field. A parametric analysis was then able to be performed using @RISK, which is an iterative risk analysis tool used with Microsoft Excel. The modeled uncertainty distributions were used as the input for the @RISK sampling algorithm to determine the resultant distribution results for each modeled internal flood initiator, accounting for uncertainty associated with both industry data and estimates of the piping geometry and configuration obtained from the field.

### Assessment of the Probability of Structural Damage due to Lightning Impact on Process Equipment in the Chemical and Process Industry

Elisabetta Renni(a,c), Mario Paolone(b), Alberto Borghetti(b), Calo Alberto Nucci(b), Elisabeth Krausmann(a), Valerio Cozzani(c)

*a) European Commission – Joint Research Centre, Institute for the Protection and Security of the Citizen, Ispra (VA), Italy. b) Dipartimento di Ingegneria Elettrica, Alma Mater Studiorum - Università di Bologna, Bologna, Italy. c)Dipartimento di Ingegneria Chimica, Mineraria e delle Tecnologie Ambientali, Alma Mater Studiorum - Università di Bologna, Bologna, Italy*

A detailed analysis of past accidents evidenced that lightning strikes on storage or process vessels containing flammable materials may cause severe accidents at refineries, storage sites, processing sites and other industrial facilities where hazardous materials are stored or processed. Although the hazard due to lightning is well known and is usually considered in the safety analysis of chemical and process plants, well accepted quantitative procedures to assess the contribution of accidents triggered by lightning to industrial risk are still lacking. In particular, the approaches to the assessment of lightning strike probability, damage caused by lightning strike and intensity of loss of containment (LOC) caused by lightning are mostly based on expert judgment and not on up-to-date models that take into account the relevant progress made in the last years in the analysis of the lightning phenomenon. In the present paper an innovative procedure for the quantitative assessment of the industrial risk due to LOC of hazardous substances triggered by lightning is introduced. The study was focused on the development of models for lightning impact probability and for damage probability. In particular, a Monte Carlo approach was developed to calculate the probability of lightning impact on the basis of the geometry of the structure and of lightning intensity and frequency data.

### Insights from the Assessment of Safety Risk of Lightning Events at LNG Facilities

James C. Lin
*ABSG Consulting Inc., Irvine, USA*

The risks from lightning events at LNG facilities may arise from potential arcing or burnthrough of the pressure boundary for the hydrocarbon containment and the subsequent ignition that may result from the lightning attachment. The critical targets for lightning attachment and lightning strike-induced burnthrough or arcing include the exposed containing equipment (e.g., pipes, valves, pumps, vaporizers, tanks/vessels, etc.) of hydrocarbon products (LNG/NG). The greatest risk of release of LNG/NG at LNG terminals during the lightning events is likely from the burnthrough effect associated with direct strikes to the LNG/NG containing pipes, since such other equipment as tanks/vessels, valves, etc. is designed with greater wall thickness. Because of the grounding system design, sideflash due to potential difference is unlikely. Only pipes with a wall thickness less than 4 mm can be punctured by the lightning burnthrough effect. At some LNG terminals, only LNG/NG pipes with a diameter of 8" or less are susceptible to lightning burnthrough puncture. Because of the piping service class design, most of the high pressure LNG and NG pipe segments are not susceptible to lightning puncture. The hole size that may be produced by the lightning direct-strike burnthrough is usually all less than 9 mm, based on a very conservative charge transfer of 350 coulombs. The largest hole sizes may result from the smaller LNG/NG pipes.

# Safety Culture & Organizational Factors

**Wendesday, North Room**

10:30 AM - Noon

## 9-7: Safety Management

Session Chairs: Tracy Dillinger, Susan Brissette

### Safety Intelligence: Senior Executive Managers and Organizational Safety Performance

Fruhen, L.S.(a), Mearns, K.J.(a), Kirwan, B.(b) and Flin, R.(a)
*a) Industrial Psychology Research Centre, University of Aberdeen, United Kingdom. b) EUROCONTROL, Bretigny Sur Orge, France*

The present study investigates what traits, skills and knowledge of senior executive managers are believed to affect safety outcomes in air traffic management. The impact of senior executive managers on safety outcomes has frequently been highlighted by the academic literature and practitioners, but it has not been fully investigated how these managers exert their impact. To clarify what traits and skills are relevant in this relationship, a sample of senior executive managers participated in interviews (n=8). A range of skills and traits including social competence, safety knowledge, motivation, personality, safety prioritization and leadership style are identified as relevant by the present sample. Based on this, the authors make suggestions regarding future research and possible applications.

### Assessing the Safety Impact due to Organizational Change

Ulf Kahlbom
*Risk Pilot AB, Stockholm, Sweden*

Organizational change is periodically performed in several safety critical industries such as for example nuclear power. The reasons for change are many, but among the most important are generation change, and harder economical pressure, partially due to tax increases and deregulation. In all organizations, and particularly the safety critical, it is of course important that the changes don't fail. But at the same time experiences from other industries shows that in more than 70% the changes fail to live up to the goals that were set for the organizational change [2]. In several countries, i.e. Sweden and Great Britain, the regulators therefore demands that an assessment of the safety consequences due to an organizational change is made before the implementation of the change. The safety assessment is also a vital contribution in the CEO's decision making process regarding the proposed organizational change. A method for assessing the above aspects were developed and applied in organizational changes made in two different organizations. The method considers the design of the changes and also the three different phases of the change, the design, implementation and post-implementation phase. This means that for example plans for the change, employee involvement, employee attitudes, follow up plans, as well as the structural aspects of the change should be addressed in the safety assessment. Several important experiences were made when developing and applying the method, and the paper briefly touch upon for example; the process for organizational change, employee attitudes and motivation, structural change and potential consequences for safety, follow up plans and some problems and challenges when performing a safety assessment of organizational change.

### Safety Culture and SMS: How Shaping Organizational Safety Culture Ensures the Successful Implementation of a Safety Management System

Kenneth P. Neubauer
*Futron Corporation*

Organizations that perform at the highest levels of their professions understand that ensuring the safety of their personnel and the preservation of the assets used in the execution of their missions and strategies are vital elements of their success. These organizations also realize that high levels of safety performance and the effective management of risk are not products of chance. Achieving the highest levels of safety requires leadership, constant awareness, and a systematic approach to accident prevention. For a growing number of organizations, the systematic approach is safety is achieved through the implementation of a set of tools and processes known as a Safety Management System or SMS. Those organizations implementing an SMS and achieving high levels of safety performance understand that an effective Safety Management System is built upon and operates within a strong, positive safety culture. This is particularly true of organizations that engage in high risk activities such as nuclear power, medicine, and aviation. "Each nuclear (power) station, because of the special characteristics and unique hazards of the technology—radioactive byproducts, concentration of energy in the reactor core, and decay heat—needs a strong safety culture."1 In the medical field, ". . . it is well recognized that safety culture is pivotal for quality in medicine."2 Within Aviation, safety culture is a concept that has ". . . become broadly accepted . . . to describe the context in which safety practices are fostered within an organization. How line management deals with day-to-day activities is fundamental to a generative organizational culture for the management of safety."3

1:30 - 3:00 PM

## 9-8: Safety Management and Knowledge Management

Session Chairs: Susan Brissette, Bill Nelson

### Performance Indicators as Cultural Artifact: Stories of Applied Organizational Change

W. E. Carnes(a), M. Dexter Ray(b), Larry Supina, MPA(c)
*a) U.S. Department of Energy, Washington,. D.C.. b) SRR Savannah River Site, Savannah River, South Carolina. c) B&W Pantex, Amarillo, Texas*

This paper discusses changes in thinking about performance indicators at two U.S. Department of Energy (DOE) sites through the stories that the key participants tell. The paper represents stories in progress, not complete, and with the journeys' goals articulated more as value expressions than as end states. The stories suggest culture shifts from a management-centric compliance focus to more of a work-centric learning focus. How performance indicators have changed in content and use are integral to discussions of this shift. In short, this paper views indicators as artifacts, and the conversations that occur around those artifacts reveal insights about the organizations' cultures. The stories are about alignment or non-alignment of espoused values, local work practices, and deep assumptions revealed by what "everyone knows" about

indicators and how they are used.

### Confidential Communication for Reliable Information and Knowledge Exchange

Vladimir Iliev(a) and Gueorgui Petkov(b)
*a) International Institute for Social Communication and Behavior, Pleven, Bulgaria. b) Technical University, Sofia, Bulgaria*

The paper examines the cases when the confidential communication can give rise to operator's errors. The psychological description of confidential communication gives opportunity to incorporate into context quantification by the performance evaluation of teamwork method not only cognition and execution but affection as well. By communication operators develop specific interpersonal relations or mask their omissions and violations. The understanding of confidential communication is especially important for modeling these circumventions that resonance human error. Some specific and general counter-measures and error reduction recommendations could be determined. Practitioners can use them for reliable information and knowledge exchange in order to minimize bias in the decision-making.

### Bringing SMS in Aviation to Life by Human Integration: Building on the ICAO SMS and Transitioning Away from a Static Regulatory Approach

Floor Koornneef(a), Simon Stewart(b), and Roland Akselsson(c)
*a) TU Delft, Delft, The Netherlands. b) easyJet Plc, Luton, United Kingdom. c) Lund University, Lund, Sweden*

The ICAO approach to risk management is essentially a technical model based on an engineering process viewpoint and is more applicable in concept to stable systems, such as chemical and nuclear industries. If airlines are to manage risk in a proactive manner they need to apply risk detection tools that provide real time and continuous systems oversight. This paper describes briefly the systems approach applied to the development and implementation of a dynamic Safety Management System (SMS) in a major airline in Europe with a focus on management of operational risks. This work has been realized as a part of the in the FP6 HILAS project. The SMS principally consists of a Risk Management System (RMS) and a Safety Assurance process. Principles of Organizational Learning and Resilient Safety Culture have been adhered to throughout this development. As a result, the RMS is conceived as an aspect system with functions, actors, supporting processes and connecting data streams. The work in progress demonstrates that integrating humans in processes of risk management leads to bridging expertise domains, enables improved business controls and efficiencies, as well as safety risks.

3:30 - 5:00 PM

## 9-9: Pushing the Envelope in Safety Management

Session Chairs: Bill Nelson, Tracy Dillinger

### Identifying the Typcial Biases and their Significance in the Current Safety Management Approaches

Teemu Reiman(a) and Carl Rollenhagen(b)
*a) VTT, Espoo, Finland. b) KTH, Stockholm, Sweden*

The aim of the article is to describe a set of biases in safety management practices and their possible consequences for safety. We will outline main biases of safety management in four thematic areas: beliefs about individual behavior, beliefs about organizations, safety models and safety management methods. A common theme underlying the biases is a lack of systems view on safety. A systemic safety management takes into account people, technology and organization and their interaction in equal terms. Furthermore, such an approach can shift focus from people to technology to organizational aspects depending on their current safety significance.

### Through the Looking Glass: Developing Organizational Ability to Understand Work as Imagined versus Work as Done

W. E. Carnes(a), Richard Hartley(b), Kim Leffew(b), Brian Harkins(c), Shane Bush(d), William Rigot(e)
*a) U.S. Department o f Energy, Washington, D.C. USA. b) B&W Pantex. c) DOE Oak Ridge Laboratory, Oak Ridge Tennessee, USA. d) Idaho National Laboratory, Idaho, USA. e) Savannah River Nuclear Solutions, Savannah River, SC, USA*

This paper focuses on approaches to understand "work-as-done" at three different Department of Energy (DOE) operations. Each effort was independently initiated as result of the sponsoring organizations' experiences in integrating high reliability thinking within the context of the DOE Integrated Safety Management framework. The paper represents "works in progress" and places the three efforts within a context of high reliability literature. As the efforts progress, they will be examined through the lenses of related research, including ethnographic observational studies and work process design studies. Additional comparative analysis will examine the three project approaches in comparison with prevailing observation-based evaluative practices used in the U.S. commercial nuclear power industry, with particular reference to recent research by Reiman and Oedewald.

### Images of Organisational Safety Culture

Frank W. Guldenmunda
*Safety Science Group, Delft University of Technology, Delft, Netherlands*

The study of safety culture is as popular as ever. In this paper various approaches towards the study of safety culture are presented accompanied by a metaphorical image. Successively, the net, the castle in the air, the porcupine, the mirror, the thing and the piece of art are discussed. None of the approaches can provide the final word on safety culture; personal preference as well as various research issues will determine the choice for an approach. A combination of approaches is nevertheless recommended.

# Industrial Safety

**Wendesday, Municipal**

10:30 AM - Noon

## 6-1: QRA on Industrial Application

Session Chairs: Tsu-Mu Kao, Yet-Pole I

### Risk Influence Factors Related to Helicopter Operations in the North Sea

Jon Espen Skogdalen and Jan Erik Vinnem
*University of Stavanger, Stavanger, Norway*

The project Risk Modeling – Integration of Organizational, Human and Technical factors is developing a method for quantifying risk and barrier performance reflecting technical, human, organizational and operational factors (OMT-method). The OMT-method is combined with conducted research related to helicopter safety. Identification and modeling of risk influence factors (RIF) and safety barriers are central. Offshore helicopter flying involves highly technical machines, well qualified personnel and detailed international regulations. The RIFs are very much the same as found in other operations with the potential for major accidents, but for helicopter operations there are few safety barriers that separate an initiating event and an accident.

### Quantitative Risk Assessment on Taiwan's Liquefied Natural Gas Tanks System with External Events

Tsu-Mu Kao and Chun-Sheng Weng
*Institute of Nuclear Energy Research, Taoyuan County, Taiwan (R.O.C.)*

According to the Taiwan's regulation, "Safety Inspection Rules for Dangerous Machines and Equipments", the Liquefied Natural Gas (LNG) tank is a specific facility for the storage of high-pressure gas and an internal inspection should be implemented by the end of a 15 year period. The three first-phase LNG tanks in Taiwan in operation from 1990 till 2006 have exceeded the time limit for an internal inspection as required by law. The Taiwan's regulation encourages utilities to implement QRA on LNG tank systems as an alternative to the required internal surveillance inspection. The Taiwan's regulation body granted the Chinese Petroleum Corp. (CPC), Taiwan with 2 additional years of extension in March 2007, depending on the final results of the QRA of the first-phase LNG tank systems in our previous study. Taiwan's LNG plant is located in the high threat area of earthquake, typhoon, and lightning. The additional risk impact of QRA on LNG receive terminal with external events assessment of operating the LNG facility is evaluated. The individual risk and societal risk of LNG receive terminal caused by external events is minor. Based on results of this study, the Taiwan's Council of Labor Affairs (TCLA) granted the CPC, Taiwan exemption for internal inspection of LNG tanks with 4 additional years in March 2010.

1:30 - 3:00 PM

## 6-2: Risk/Reliability Analysis

Session Chairs: Paolo Trucco, Min Xie

### The Results of Final Application from PROTEGER - Model for Implementation of Work Safety Management Systems Based on OHSAS and Checkland

Walter F. M. Correia(a), Denise D. de Medeiros(b), Marina de L. N. Barros(a), Fabio Campos(a), Mariana Pereira Bezerra(a)
*a) Universidade Federal de Pernambuco – Department of Design, Recife, Brazil. b) Universidade Federal de Pernambuco – Department of Production Engineering, Recife, Brazil*

This article aims to make a short explanation of the final results of applying the model PROTEGER, whose development was designed to contribute in the implementation of MSWS - Management Systems in Work Safety, directed to industry in general, based on unique features observable inside each organization. The model was developed based on data collected also in Brazil and Portugal, where the study was done. The developed tool intends, by using analytical indicators, improve the quality of life of workers, optimize the time of implementation of these systems, and generate a larger awareness about the importance into the scope of work safety.

### Understanding and Modeling Operational Risks: A Multi Context Application

Amerigo Silvestri(a), Enrico Cagno(b), and Paolo Trucco(b)
*a) SAIPEM SpA (ENI Group), Internal Audit Dept. and PhD Candidate at Politecnico di Milano, Milan, Italy. b) Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy*

The enhancement of Enterprise Wide Risk Management process needs to be founded on coherent definition and related model of Operational Risk (OR) [1]. A new OR model is proposed that aims to improve the risk analysis phase, enlarging the traditional description of cause-effect mechanisms (called “pathology”-based risk analysis) with some “inherent” characteristics of operational risk factors that could impact on the organizations core capabilities (called “anatomy”- based risk analysis). The paper shows the use of the new OR model to perform risk analysis of three operational conditions related to very different business contexts. The objective is to demonstrate, through a qualitative analysis, how the anatomy-based approach allows organizations either to have a wider range of risk management options and to exploit their link with the business management activities.

### Sensitive Incorporation of Ageing Effects into the PSA Model

Emil Stefanov(a,b) and Gueorgui Petkov(b,a)
*a) Kozloduy Nuclear Power Plant, Kozloduy, Bulgaria. b) Technical University of Sofia, Bulgaria*

The paper presents the results of a case study on sensitive incorporation of ageing effects into the PSA model of the Russian PWR - WWER-1000. The possible impact of age-related degradation on the component unreliability, safety system unavailability and on the plant risk profile is demonstrated. The discussion on the sensitive use of PSA to evaluate the structures, systems and components ageing effects on the overall plant safety is provided using the WWER-1000 large LOCA PSA model as an example. Based on the comparison of generic and specific ageing reliability databases used in case study some practical insights, recommendations and limitations for sensitive incorporation of the ageing effects into the PSA model are also discussed. The set of “virtual” reliability data was prepared on the basis of the results of case study and available generic data sources. The data includes time-dependent reliability models for certain mechanical, electrical and instrumentation & control components of the high pressure injection system, accumulator’s injection system and low pressure injection & residual heat removal system. The study was carried out within the framework of the EC-JRC Ageing PSA Network Task 7.

3:30 - 5:00 PM

## 6-3: Accident Analysis

Session Chairs: Kurt Petersen, Valerio Cozzani

### Risk Informed Insights from Transformer Fires at NPPs

Matti Lehto, Jouko Marttila, and Reino Virolainen
*Radiation and Nuclear Safety Authority (STUK), Helsinki, Finland*

In 1984, a severe transformer fire occurred in a transforming station in Finland. Extinguishing of the developed transformer oil fire was extremely difficult and the fire incident initiated assessment of severe transformer fires at Finnish NPPs. The assessment pointed out important modifications to be performed in Loviisa NPP, where the start-up transformer was located closed to the main and auxiliary transformers. First, the start-up transformer was relocated and barriers of the main transformer bunkers were enhanced. Later on, the main and auxiliary transformers at Loviisa NPP were equipped with fixed automatic water extinguishing system. Transformer fire tests were performed to ensure extinguishing system’s design performance. In the early 1980’s, some generic statistics were available, but almost no public statistics existed on transformer fires at NPPs. Nowadays, fire frequency for transformers has been estimated based on the US NPP operation experience. Certain OECD countries have collected NPP fire event data since 2003 and the data is mature enough to be utilized for comparison with the US data and producing risk informed insights.

### Classifying Underlying Causes of Fatalities: The Case of Construction

Andrew Hale(a), Helen Bolt(b), and Damian Walker(c)
*a) Delft University of Technology, Safety Science Group, Delft, Netherlands & HASTAM, Maldon, UK. b) Consultant supporting the Health and Safety Executive, Construction Division, London, UK. c) HM Inspector, Health and Safety Executive, Human Factors and Ergonomics, Corporate Specialists, Division, Plymouth, UK*

As part of an Inquiry set up by the Secretary of State for Work and Pensions in the UK alongside a research review and extensive interviews with system actors, a deeper analysis was made of a sample of recent construction fatalities. The sample of 26 accidents (28 fatalities) was drawn from the 211 fatalities in the years 2005/6 to 2007/8, to be broadly illustrative of a range of accident characteristics. The accidents were analysed on the basis of available inspectorate reports and interviewing the investigating inspectors. A standard method of classification was developed, based on the HFACS classification of errors and task level factors, with additional categories covering the organisational and regulatory/market levels of the system. The results showed a concentration of underlying factors associated with inadequacies in planning and risk assessment; competence assurance; hardware design, purchase and installation; and contracting strategy. This paper describes the development and testing of the classification method and provides a summary of the findings and their comparison with results from an initial analysis of another sample of 50 fatalities analysed earlier by the Health & Safety Executive (HSE) to examine the potential vulnerability of migrant workers.

### Learning from Accident Investigations - A Cross-country Comparison

Alexander Cedergren, Kurt Petersen
*LUCRAM, Lund University, Sweden*

This paper compares all accident investigation reports covering railway accidents issued by the national investigation boards in Sweden, Norway and Denmark during a two-year period (2008- 2009). By using content analysis, units of text describing attributed causes have been selected and categorized as belonging to one of three hierarchical levels; the micro level (technical malfunctioning and human actions), meso level (organizational actions and factors in the physical environment), and macro level (inter-organizational and regulatory factors). In addition, attributed causes on each level have been further categorized as belonging to different ‘types’ of causes. In a similar manner the recommendations described in all studied reports have been divided into different classes. The results show that the majority of attributed causes in all three countries belong to the micro level, and about half of all recommendations aim at human factors aspects. Furthermore, the diversity in different ‘types’ of causes differs between the countries. The analysis has been followed up by interviews with the investigation boards. Based on these interviews, it can be concluded that the structure, mandate and traditions of the investigation boards influences the outcome of the investigations in such way that a broader mandate gives rise to a higher potential for accidents to be examined from multiple perspectives.

### A preliminary Analysis of the ‘News Divine’ Incident by Applying the MORT Technique

Jaime Santos-Reyes, and Samuel Olmos-Peña
*Grupo: “Seguridad, Análisis de Riesgos, Accidentes y Confiabilidad de Sistemas” (SARACS), SEPI-ESIME, IPN, Mexico City, Mexico*

The paper presents the results of the analysis of the “News Divine” stampede incident which took place on 20th June 2008. The fatal incident occurred when the police raid a packed nightclub to check reports that drugs and alcohol were being sold to underage. The approach has been the application of the Management Oversight Risk Tree (MORT) technique. The MORT is intended to look at various organizations failures that have led to the incident. The MORT consists of a large tree with several branches that are required to look at when assessing the incident. Some preliminary results of the analysis of what happened during the undesirable event have been presented. More work is needed in order to identify any management elements on the why branch of the MORT tree that contributed to the particular problems identified in the present analysis. Moreover, other accident analysis approaches may be used for the present case. It is hoped that by conducting such analysis lessons can be learnt so that similar events can be prevented in the future.

# Security / Infrastructure

**Wendesday, Federal**

10:30 AM - Noon

## 14-2: Methods for Managing Vulnerabilities

Session Chair: Felicia Duran

### Energy Security of Military and Industrial Facilities: A Scenario-Based Multiple Criteria Decision Analysis to Identify Threats and Opportunities

James H. Lambert(a), Christopher W. Karvetski(a), Igor Linkov(b), Tarek Abdallah(b)
*a) University of Virginia, Charlottesville, Virginia, USA. b) Engineer Research and Development Center, US Army Corps of Engineers*

Energy security is the capacity to avoid adverse impact of disruptions from natural, accidental, or intentional events affecting energy and utility supply and distributions systems [1]. The integration of multiple fuel sources, use of regional renewable energies, consideration of cultural acceptance, defined criteria and metrics, and appropriate research and development all constitute a plan for achieving energy security [2]. When evaluating alternative investment strategies in energy security for military and industrial facilities, it is important to consider future scenarios of the energy environment. Some scenarios may be evidence-based projections derived from geographic, regulatory, geopolitical, and other driving forces. Other scenarios could reflect the advocacy positions of various stakeholders in a large-scale infrastructure or military/ industrial system. This paper reflects a philosophy to incorporate uncertain scenarios to update a scoring function of a multiple criteria decision analysis (MCDA). The approach identifies what scenarios most affect the prioritization of investment portfolios, and what portfolios are most opportunistic or vulnerable across the scenarios. The approach efficiently adjusts the scoring function and is therefore suitable for considering a potentially large set of scenarios in stakeholder negotiation, group decision making, and brainstorming.

### A Method for Optimal Allocation of Defensive Alternatives: Analysis of a Strategic Interaction with a Multi-objective Approach

Carlos Renato dos Santos(a), Isis Didier Lins(b), Paulo Renato Alves Firmino(b,c), Márcio das Chagas Moura(b,d) and Enrique López Droguett(b)
*a) Departamento de Matemática, UFPI, Parnaíba-PI, Brazil. b) CEERMA, Departmento de Engenharia de Produção, UFPE, Recife-PE, Brazil. c) Departamento de Estatística e Informática, UFRPE, Recife-PE, Brazil. d) Núcleo de Tecnologia, Centro Acadêmico do Agreste, UFPE, Caruaru-PE, Brazil*

Compelled by recent astonishing and catastrophic events, academic community and society as a whole have paid attention at methods that aid stakeholders in making decisions regarding investments in more effective defense systems. This paper aims at providing a method devised to support decision makers who are interested in allocating investments in security systems that may be subjected to purposeful attacks. Thus, it considers the strategic interactions between two rational agents: (i) a defender who wants to protect critical parts of the main system (e.g. power transmission lines, oil tankers, banks, museums, among others) via a security structure and (ii) an attacker who is interested in shutting the defense system down so as to obtain free access to the main system. The methodology proposed in this article uses Game and Reliability Theories and Multi-objective Genetic Algorithm (MOGA) to model this strategic interaction, which is analyzed in terms of a sequential game in the scenarios of complete/ perfect and incomplete/imperfect information. An application example involving data from a real power system line is provided.

### Vulnerability Assessment of Hazardous Materials Transportation Systems

Adrian V. Gheorghe(a), Bogdan Vamanu(b)
*a) Old Dominion University, Norfolk, Virginia, USA. b) EC – JRC, Institute Security and Protection of Citizen, Ispra, Italy*

The risk assessment methodology mainly covers the aspects related with the minimization of the impact an abnormal behavior of a system (in particular the ‚hazmat transportation' system) may have on the surrounding environment. However, at a closer look, one may see that the risk assessment takes into account the systemic internal characteristics of the analyzed process. Thus, the risk is seen as function of (i) the probability / frequency of the abnormal event occurrence (e.g. the loss of containment resulting accident following an initial disrupting event such as ‚flat tire' or ‚collision when entering the crossing'), (ii) the consequences' level of the abnormal event (depending on the physical and chemical characteristics of the transported substance(s), the confinement type, etc.), and (iii) the health and environmental impact of the event. Global developments, the social and economical facts, as well as recent events, both natural and man-made (the WTC and Madrid terrorist attacks, Katrina hurricane) led to a major change of perspective with respect to system analysis. Thus, at least three emergent coordinates in system safety analysis may be pointed out: the complex systems' interconnection, their interdependency, and the ‚intentional' factor.

### Design of Networks Considering Vulnerability: A Multi-objective Approach

Claudio M. Rocco S.(a), J. E. Ramirez-Marquez(b), Daniel E. Salazar A(a,c) and Ivan Hernandez(a)
*a) Universidad Central de Venezuela, Caracas, Venezuela. b) Stevens Institute of Technology, Hoboken, USA. c) CEANI-SIANI, Universidad Las Palmas de Gran Canaria, Spain*

The traditional approach for designing and evaluating critical infrastructures in complex networks is based on two steps. The first step is to design the system and the second step is to evaluate the design under special circumstances, such as a failure or an attack. In this paper a framework for designing and evaluating networks in just one step is proposed. The approach is based on the use of Multi-Objective optimization, the selection of proper network measures and Multiple Objective Evolutionary Algorithms (MOEAs). An example related to an electric power system illustrates the approach.

1:30 - 3:00 PM

## 14-3: Facility Security Assessment

Session Chair: Michele Minichino

### Elements of Criminal Liability as a Basis for the Design of Security Barriers and Risk Modeling

Coen van Gulijk, Marieke Kluin, Hinke Andriessen, and Ben Ale
*Delft University of Technology, Delft, The Netherlands*

In this paper the potential is explored of using the scientific principles of safety science and criminology to design protection strategies in security. The paper introduces the MMO concept which is a generic concept for the design of security barriers and their evaluation by quantitative risk analysis. It is based on a simplification of the basic elements for proving criminal liability of a defendant in US criminal law: motive, means and opportunity. These three elements form the preconditions that are needed to let an ill meaning person to develop into a hazard or threat to a system that is vulnerable to crime. The MMO concept also forms the key to the development of successful barriers against the completion of the criminal act. Taking one of these three away renders the hazard ineffective. This enables the development of a systematic strategy for protection against security threats along similar lines as safety threats are dealt with and opens the possibility the use of similar qualitative and quantitative analysis techniques.

### Coping with Vulnerabilities of Interconnected Critical Infrastructures

Wolfgang Kröger, Patrick Probst
*Laboratory for Safety Analysis, ETH Zurich, Switzerland*

Critical infrastructures (CI) are exposed to a multiple set of hazards and threats and may even be misused to cause significant harm to the public. The incapacity of a single CI can snowball into others depending on their degree of interconnectedness. To understand CI behavior and identify vulnerabilities and interdependencies is the aim of the project introduced here that assists the Swiss Federal Office for Civil Protection (FOCP) in defining a national strategy for CI protection. Based on a criticality parameter evaluation, five infrastructures have been selected for analysis according to a tailored framework. In a screening analysis to start with, an adequate system understanding has to be set up and techniques (incl. network theory) have to be applied suitable to identify obvious vulnerabilities within a well defined system boundary. An in-depth analysis may be necessary to model complex interactions and to trace hidden vulnerabilities making use of more sophisticated, well selected methods (e.g. object oriented modeling/MC simulation) following a “systemof- systems” approach. Current focus is on systems for supply of electricity, information and communication (internet), urban drinking water and transportation by rail including their interdependencies, which may be physical, functional or given by a host technology. First results have proven the decisive role of human and contextual factors and of digital industrial controls systems (i.e. SCADA, potential risks of cyber attacks). Further substantiated insights with regard to susceptibility and resilience of the investigated CI are presented and experience gained by application of various methodological approaches discussed.

### Risk-Based Cost-Benefit Analysis for Security Assessment Problems

Gregory D. Wyss(a), John P. Hinton(b), Katherine Dunphy-Guzman(b), John Clem(a), John Darby(a), Consuelo Silva(a), and Kim Mitchiner(a)
*a) Sandia National Laboratories, Albuquerque, New Mexico, USA. b) Sandia National Laboratories, Livermore, California, USA*

Critical infrastructures (CI) are exposed to a multiple set of hazards and threats and may even be misused to cause significant harm to the public. The incapacity of a Decision-makers want to perform risk-based cost-benefit prioritization of security investments. However, strong nonlinearities in the most common performance metric for physical security systems make it difficult to use as the basis for cost-benefit analysis. This paper extends the definition of risk for security applications and embodies this definition in a new but related security risk metric based on the degree of difficulty an adversary will encounter to successfully execute the most advantageous attack scenario. This metric is compatible with traditional cost-benefit optimization algorithms, and can lead to an objective risk-based cost-benefit method for security investment option prioritization. It also enables decision-makers to more effectively communicate the justification for their investment decisions with stakeholders and funding authorities.

### Process and Software to Efficiently Manage Security in a Restricted Area

Julien Piwowar, Eric Châtelet and Patrick Laclémence
*University of Technology of Troyes, Troyes, France*

The increase of technologies and knowledges have broken almost all the frontiers (material or virtual) between the citizens of our Planet. We are now living in a global World in which each of us is a global player[1]. This new way of life appears exciting with even more possibilities but also new threats which have arisen associated to those improvements. Each system we use frequently (public transports, shopping areas, stadiums, etc.) is included in a larger one, itself linked to others as an endless network. So, it is more and more difficult to delimit a system. Thus today, the exponential move around systems is a catalysis factor of new threats: less predictive and more fluent. In the last years, we have identified a lack of methods to manage security taking into account risk assessment but also the different kind of aggressions procedures. To clearly assess these new risks, we have built a methodological process with an associated software to efficiently manage security in a restricted area. It permits, after an exhaustive systemic analysis, to simulate various aggressions according to several evoluting paramaters in order to improve a dispositive of security with a final aim: to anticipate acts of malevolence.

3:30 - 5:00 PM

## 14-4: Area-Level Risk Management

Session Chair: Ben Ale

### Power System Reliability Assessment Incorporating Ageing Based on Fault Tree Analysis and AC Power Flow Model

Duško Kančev(a), Marko Čepin(b)
*a) Jožef Stefan Institute, Ljubljana, Slovenia. b) Faculty for Electrical Engineering, University of Ljubljana, Ljubljana, Slovenia*

Reliability of a power system is a general term that refers to the probability of its satisfactory operation in the long term. It is a function of the time-average performance of a power system, in different loading situations, after different faults, during different outages. Additionally, equipment ageing has gradually become a major concern in many utilities since more and more system components are approaching their wear-out stage. Traditionally, only repairable failures have been considered and ageing failures have been excluded in most of power system reliability evaluation methods. Ignoring the ageing failures will most likely result in underestimation of power system unreliability, particularly for an aged system. Therefore, the ageing failure mode of components should be incorporated in reliability evaluation when the components approach to end-of-life. This paper describes how ageing characteristics of components may impact the power system reliability evaluation. A simplified version of the Macedonian power system was used as a case study.

### The introduction of Safety Integrated Urban Design

Shahid Suddle(a,b)
*a) Delft University of Technology, Delft, The Netherlands. b) SSCM – Suddle Safety Consultancy & Management, Schiedam, The Netherlands*

In the Netherlands no standards or design criteria are formulated by the government or the legislator for the realization of buildings adjacent to the infrastructure with transport of hazardous materials or chemical installations. In regard to external safety there is even also no judicial base for example the functional design of land-use planning for such locations. This paper presents a framework of design parameters for realizing projects in the neighbour of hazardous locations. The framework is set-up from an urban planning point of view, in which the effect related safety measures and design parameters for urban planning are extensively analyzed on the macro (city), meso (urban plan) and micro (building) scale level. Subsequently, design parameters are derived from the characteristics of relevant scenarios which may take place with hazardous materials. Also design parameters are investigated in relation to the safety chain enabling to integrate the measures of emergency response. Finally, the analysis is combined with each other, resulting in the framework of safety integrated urban design on different scale levels of land use. The main advantage of such a framework is that different disciplines and design parameters can be integrated at an early possible design stage in urban development, e.g. fire safety engineering, relief, loss prevention and risk analysis, through which external safety becomes communicable particularly for urban planners.

### The Use of GIS for Presenting the Group Risk for Land Use Planning

Shahid Suddle(a,b, Robert Geerts(a,c), and Claudia Basta(a)
*a) Delft University of Technology, Delft, The Netherlands. b) SSCM – Suddle Safety Consultancy & Management, Schiedam, The Netherlands. c) AVIV, Enschede, The Netherlands*

In the Netherlands, regulations for land-use planning in the vicinity of major industrial hazards or transport routes of hazardous materials are explicitly risk-based, in which the risks are visualized in two ways: Individual Risk (IR) and Group Risk (GR). IR is visualized on a geographical map presenting iso-risk contours. This is an understandable way of communicating risk with (non- )experts. However, such a straightforward approach is not appropriate for presenting the GR, through which the communication between the (non-)experts and decision makers becomes rather hard. GR is usually represented as a graph in which the cumulative probability of more than n fatalities is given as a function of N, the number of people killed. This graph is called the fN curve, almost a noncommunicable risk presentation for land use planners and decision makers. Land use planners are used to communicate in maps and drawings, while the risk analysts communicate the GR in fN-curves. Moreover, the risk acceptance criterion for the GR is difficult to apply as well. In this regard, a methodology to present the GR in a Geographical Information System (GIS) is proposed in this paper, through which the visualization and motivation of the GR becomes communicable for both land use planners and decision makers.

### Modelling Interdependencies by Applying the SSMS Model

Jaime Santos-Reyes
*"Seguridad, Análisis de Riesgos, Accidentes y Confiabilidad de Sistemas" (SARACS),SEPI-ESIME, IPN, Mexico City, Mexico*

'Critical infrastructures' came to the public domain in recent years. Moreover, it may be argued that modern society is exceedingly complex and highly interdependent. As a consequence of this, any disruption of 'critical infrastructures' can have severe consequences, as some recent events have shown. The paper presents a way to model such interdependencies. The approach has been the application of a Systemic Safety Management System (SSMS) model. Three oil and gas fields have been used to illustrate the modelling process by using the model. The model has shown that these facilities have 'horizontal' and 'vertical' interdependencies. However, more research is needed in order to explore the full potentiality of the model. For example, to apply it to other 'critical' infrastructures, such as transportation, communication, emergency services, etc. It is hoped that by conducting such analyses the model can help to gain a better understanding of the interdependence of 'critical infrastructures'.

# Environmental Risk

**Wendesday, Seuperior**

10:30 AM - Noon

## 3-1: Climate Change Challanges

Session Chairs: Zdenko Simic, Takeshi Matsuoka

### Sea Surface Temperature Prediction via Support Vector Machines Combined with Particle Swarm Optimization

Isis Didier Lins(a), Márcio das Chagas Moura(a,b), Marcus André Silva(a), Enrique López Droguett(a), Dóris Veleda(a), Moacyr Araújo(a) and Carlos Magno Jacinto(c)
*a) Center of Risk Analysis and Environmental Modeling, Federal University of Pernambuco, Recife-PE, Brazil. b) Núcleo de Tecnologia, Centro Acadêmico do Agreste, Federal University of Pernambuco, Caruaru- PE, Brazil. c) CENPES, PETROBRAS, Rio de Janeiro-RJ, Brazil*

The prediction of Sea Surface Temperature (SST) is of great importance since it is an indicator of extreme climate phenomena that have occurred in South America. The use of sophisticated ocean-meteorological models to forecast environmental metrics such as SST may demand increasing computational effort and time. In this context, learning methods like Support Vector Machines (SVMs) emerge as an alternative prediction tool. SVMs are based on input/output data and do not require the previous knowledge about the process that maps input into output. Their performance is influenced by a set of parameters which rise from the related learning problem. In order to choose appropriate values for them, SVMs are here combined with a Particle Swarm Optimization (PSO) algorithm. Therefore, PSO-optimized SVM is applied to predict SST in the Northeastern Brazilian coast with data provided by Prediction and Research Moored Array in the Tropical Atlantic (PIRATA) observation system. The obtained results indicate that PSO+SVM is a valuable SST prediction method, as it may give important contributions to the comprehension of the climate dynamics in the considered region.

### Sea Level Prediction by Support Vector Machines Combined with Particle Swarm Optimization

Márcio das Chagas Moura(b,a), Isis Didier Lins(a), Dóris Veleda(a), Enrique López Droguett(a) and Moacyr Araújo(a)
*a) Center of Risk Analysis and Environmental Modeling, Federal University of Pernambuco, Recife-PE, Brazil. b) Núcleo de Tecnologia, Centro Acadêmico do Agreste, Federal University of Pernambuco, Caruaru-PE, Brazil*

Sea level rise is reported by the Intergovernmental Panel on Climate Change (IPCC) as one of the main aftermaths of global warming. Besides that, the shortage of altimetry data in coastal zones renders the evaluation and comprehension of climate behavior burdensome in those areas. In this way, the forecast of sea level is of great importance and a Support Vector Machines (SVMs) prediction model is here used. SVMs are a learning method based on input/output data and do not demand previous knowledge about the process that maps input into output. Their performance is dependent on some parameters that appear in the related learning problem. A Particle Swarm Optimization (PSO) algorithm will be here adopted for selecting suitable values to these parameters. Therefore, this work applies a PSO-optimized SVM to forecast sea level measurements from the Brazilian coast. The obtained results show that PSO+SVM is a promising prediction method in the environmental field.

### Climate Change Impacts on Renewable Energy Sources in Croatia

Robert Pašičko(a), Zdenko Šimić(b), and Slavica Robić(b)
*a) UNDP, Zagreb, Croatia. b) University of Zagreb, Zagreb, Croatia*

Even though climate change has recently been getting enormous attention, there is very limited number of analyses performed on climate change impacts on power system planning. However, it seems very important to understand these influences as power system planning deals with a very long time span, and it is certainly affected in multiple ways with potential climate change. Power plants are facing number of risks related to the long term operation performances. The most significant sources of risk are related to the regulation, economy and technology. Technology related risks seem especially important for renewable energy sources because they are strongly influenced by the weather conditions, which might be significantly changed because of ongoing climate changes. This paper focuses on the initial evaluation of climate change impacts on renewable energy sources in Croatia - namely photovoltaic, wind and hydro energy. Key factors influencing energy generation from photovoltaics are temperature change, expected number of days under snow cover, change in global radiation and impacts of meteorological extreme events to cope with in the future. Wind generation will mostly be influenced by the change of average wind speed, wind direction and maximal wind speed expected due to meteorological extreme events. Hydro generation will be influenced by the change of precipitation and the change in temperature (due to less rain and higher evaporation). Without estimate of related uncertainty it is still not possible to estimate how important climate change influence on the future renewable energy power generation is.

1:30 - 3:00 PM

## 3-2: Area-Geological Carbon Capture and Sequestration I

Session Chair: James H. Lambert / Ditakanta Mohanty, Andreas Strohm / Geoff Freeze

### The CO2QUALSTORE Guideline for Safety and Risk Management of CO2 Geological Storage Sites

Mike Carpenter(a), Jørg Aarnes(a), David Coleman(b) and Bryce Levett(b)
*a) DNV, Høvik, Norway. b) DNV, Houston, USA*

The CO2QUALSTORE guideline has been developed by DNV in collaboration with industrial partners and with input from a number of national regulators. The guideline is globally applicable and adopts a risk-based approach to the selection, characterization and qualification of sites and projects for geological storage of CO2. This article summarizes the guideline and describes how the document promotes safety and risk management throughout a CO2 storage project lifecycle using risk assessments, predictive modeling, performance targets and tailored monitoring. The guideline is also designed to assist project developers in passing project management milestones while simultaneously demonstrating compliance with regulations and stakeholder expectations.

### The Effect of New Information on Expert Perception of Risk in Carbon Capture and Storage

Debbie Polson(a), Andrew Curtis(a) and Claudia Vivalda(b)
*a) University of Edinburgh, School of GeoSciences, Edinburgh, UK. b) Schlumberger Ltd, Paris, France*

This paper describes the evolving perception of risk during a carbon capture and storage project. Carbon capture and storage (CCS) is potentially an important technology for reducing emissions of CO2, one of the key greenhouse gases. In CCS the CO2 generated by large point-source emitters (e.g. power stations) is captured and transported to a storage site where it is injected into the Earth's subsurface and stored in the pore space of rock. A complete simulation of the capture, transport and storage of CO2, from a coal fired power station to saline reservoir storage site was carried out over the course of a project. Throughout the process, a project specific risk register is used to track the experts' perception of risk. The results show that the experts' perception of risk changed in the short term due to this information, but that their perception of risk did not necessarily change permanently. In some cases, over time it seemed to return to levels perceived prior to seeing the new information. Overall, uncertainty was the key factor in influencing perception of risk, and reducing uncertainty is required if the perception of risk is to decrease also.

### Risk Assessment Framework for Geologic Carbon Sequestration Sites

Curtis M. Oldenburg(a), Preston Jordan(a), Yingqi Zhang(a), Jean-Philippe Nicot(c), and Steven L. Bryant(b)
*a) Earth Sciences Division, Lawrence Berkeley National Laboratory, Berkeley CA. b) Department of Petroleum and Geosystems Engineering, The University of Texas at Austin, Austin, TX . c) Bureau of Economic Geology, Jackson School of Geosciences, The University of Texas at Austin, Austin, Texas*

We have developed a simple and transparent approach for assessing CO2 and brine leakage risk associated with CO2 injection at geologic carbon sequestration (GCS) sites. The approach, called the Certification Framework (CF), is based on the concept of effective trapping, which takes into account both the probability of leakage from the storage formation and impacts of leakage. The effective trapping concept acknowledges that GCS can be safe and effective even if some CO2 and brine were to escape from the storage formation provided the impact of such leakage is below agreed-upon limits. The CF uses deterministic process models to calculate expected well- and fault-related leakage fluxes and concentrations. These in turn quantify the impacts under a given leakage scenario to so-called "compartments," which comprise collections of vulnerable entities. The probabilistic part of the calculated risk comes from the likelihood of (1) the intersections of injected CO2 and related pressure perturbations with well or fault leakage pathways, and (2) intersections of leakage pathways with compartments. Two innovative approaches for predicting leakage likelihood, namely (1) fault statistics, and (2) fuzzy rules for fault and fracture intersection probability, are highlighted here.

## CO2 Geological Storage Safety Assessment: Methodological Developments

O. Bouc(a), G. Bellenfant(a), D. Dubois(b), D. Guyonnet(a), J. Rohmer(a), M. Gastine(a), F. Wertz(a), H. Fabri(a)
*a) BRGM, Orléans, France. b) IRIT, Université Paul Sabatier, Toulouse, France*

Carbon dioxide capture and geological storage is seen as a promising technology to mitigate greenhouse gas atmospheric emissions. Its wide-scale implementation necessitates demonstrating its safety for humans and the environment. We have developed a generic approach to provide references for safety assessment of CO2 storage. It is composed of a series of simple tools for identifying risk scenarios, modelling risk events and exposure. It incorporates a rigorous management of uncertainty, distinguishing between variability and knowledge incompleteness. We applied this approach on a case study in the Paris Basin. This demonstrates how it delivers conditions mixing qualitative and quantitative elements for guaranteeing safety. This approach is flexible; it can be used for various sites and with various amounts of data. It can be carried out in a time-efficient manner at various stages of a project. In particular, it provides an operator or an authority with safety indicators in an early phase or for reviewing a risk assessment. Though not a complete risk assessment workflow, it thus partly compensates for the current lack of commonly acknowledged assessment methods or safety standards for CO2 geological storage.

# Thursday Meeting-At-A Glance

| Room Session | Salon A | Salon B | Salon C | East Room | West Room | North Room | Municipal | Federal | Superior | South Room |
|---|---|---|---|---|---|---|---|---|---|---|
| 0730 - 1600 | **Conference Registration – Courtyard Foyer** | | | | | | | | | |
| 0700 - 0830 | **Continental Breakfast – Madison, Courtyard, and Compass Foyers** | | | | | | | | | |
| 0830 - 1000 | Plenary Speaker - Dr. Steven Herring - Madison Ballroom | | | | | | | | | Exhibits |
| 1000 - 1030 | ***Coffee/Refreshment Break - Madison, Courtyard, and Compass Foyers*** | | | | | | | | | |
| 1030 - 1200 | Risk Management 4-5: Risk Informed - Going On | Modeling & Simulation 2-10: Reactor Systems | HRA 5-10: HRA Applications | PSA Applications 1-10: Common Cause Failure Analysis | RAM Methodology 7-1: Aging Management | Safety Culture 9-10: Cross-Cultural Issues | Industrial Safety 6-4: Occupational Safety | Security / Infrastructure 14-5: Security Systems | Waste Management 18-1: Radioactive Waste Management I | |
| 1200 - 1330 | ***Lunch - on your own*** | | | | | | | | | |
| 1330 - 1500 | Risk Management 4-6: Risk Management | | HRA 5-11: Human Behavior and Disaster Response II | | RAM Methodology 7-2: Health Monitoring | Transportation 17-1: Transportation Risk Assessment and Management | Industrial Safety 6-5: Hazard Prevention | Medical 13-1: Risk Assessment of Ambulatory Care | Waste Management 18-2: Radioactive Waste Management II | |
| 1500 - 1530 | ***Coffee/Refreshment Break - Madison, Courtyard, and Compass Foyers*** | | | | | | | | | |
| 1530 - 1700 | | | | Structural Reliability 11-1: Structural Reliability | RAM Methodology 7-3: Quantitative Methods in RAM Analysis | | | Medical 13-2: PSA Applications to Healthcare | | Exhibits tear-down in the evening |

# Plenary Speaker

## Dr. J. Stephen Herring

Dr. J. Stephen Herring is an Idaho National Laboratory Fellow and the Technical Lead for High Temperature Electrolysis in the DOE Office of Nuclear Energy Next Generation Nuclear Plant. He is responsible for the development of solid oxide cells for the efficient production of hydrogen and synthetic fuels using the heat and electricity from advanced nuclear reactors. He has been active in the reactor physics analyses of nuclear fuels for the consumption of long-lived wastes and development of other advanced energy sources at the INL since 1979.

Steve holds BS degrees in mechanical and electrical engineering from Iowa State University (1971), and earned a PhD in nuclear engineering from the Massachusetts Institute of Technology in 1979. He was also a Rotary Foundation Fellow at the Eidgenössische Technische Hochschule in Zürich, 1974-75, and a Visiting Scientist at the Kernforschungszentrum Karlsruhe in 1987.

Contact Information:

Dr. Steve Herring
Idaho National Laboratory
P.O. Box 1625 MS 3860
Idaho Falls, Idaho 83415-3860

e-mail: j.herring@inl.gov
phone: 208-526-9497

---

**The Production of Fuels for Transportation using Nuclear Energy**

J. Stephen Herring, Carl M. Stoots, James E. O'Brien
Idaho National Laboratory

Abstract

For the last fifty years, the commercial use of nuclear energy has been almost exclusively for the generation of electricity. As we look into the future, however, we see that the twin issues of energy security and CO2 emissions will require that non-fossil sources be used for the production of gasoline, diesel and jet fuel. In the longer term, nuclear energy may also be applied to recharge batteries and to produce hydrogen for automotive and aviation use.

The nuclear production of transportation fuels will require technologies for splitting water or steam into hydrogen and oxygen. The Idaho National Laboratory, in collaboration with several other laboratories, universities and industrial firms, has been developing solid oxide electrolysers for use at 800°-850° C. These electrolysers can also be used for the conversion of CO2 and steam into synthesis gas (CO + 2 H2), which in turn can be catalytically formed into liquid fuels. The requirements for modularity, reliability and proximity between the nuclear and hydrogen/synfuels plants will require the application of probabilistic assessments of both the nuclear and chemical plants.

# Risk Management

**Thursday, Salon A**

10:30 AM - Noon

## 4-5: Risk Informed – Going on

Session Chair: Gabriel Georgescu

### Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making (NUREG-1855)

Mary Drouin(a), Gary DeMoss(a), Donnie Harrison(a), John Lehner(b), Jeffrey LaChance(c), Timothy Wheeler(c)
*a) US Nuclear Regulatory Commission, Washington DC USA. b) Brookhaven National Laboratory, Upton, NY US. c) Sandia National Laboratories, Albuquerque, NM*

In its safety philosophy, the U.S. Nuclear Regulatory Commission (NRC) has always recognized the importance of addressing uncertainties as an integral part of its decision making. With the increased use of probabilistic risk assessment (PRA) in the NRC's risk-informed decision making, the uncertainties associated with the PRA need to be considered. These uncertainties, and their potential impact on the comparison of PRA results with acceptance guidelines, need to be understood so that informed decisions are made. Guidance (NUREG-1855) has been developed on how to treat uncertainties associated with PRA in risk-informed decision making. The objectives of this guidance include fostering an understanding of the uncertainties associated with PRA and their impact on the results of the PRA, and providing a detailed approach to both the applicant and the regulator for addressing these uncertainties in the context of the decision making. The guidance in NUREG-1855 is currently focused on those sources of uncertainty associated with PRAs assessing core damage frequency (CDF) and large early release frequency for at-power light water reactors (LWRs) considering internal events and internal floods. The guidance is being revised to address internal fires and external hazards. The current guidance, however, is generally applicable to sources of uncertainties associated with full-scope PRAs.

### Estimating Performance Criteria for the Maintenance Rule

Ross C. Anderson(a), Thomas P. John(b)
*a) Virginia Commonwealth University, Richmond, VA USA. b) Dominion, Richmond, VA USA*

This paper documents a method for developing 10 CFR 50.65(a)(1) "Maintenance Rule" Performance Criteria that are based upon the 1E-6 Core Damage Probability criterion used in several other regulatory applications.

### Making a Robust Safety Case for Future Nuclear Plant Designs

Inn Seock Kim(a), Sang Kyu Ahn(b), and Kyu Myung Oh(b)
*a) ISSA Technology, Germantown, MD, USA . b) Korea Institute of Nuclear Safety, Yuseong, Daejeon, Republic of Korea*

A critical review was made of various methodological approaches that were used or have been proposed to assure the design safety of nuclear power plants, existing or future. Our findings and insights from a critical review of these design safety analysis approaches, some being deterministic while others risk-informed, are then presented so that they could help make a robust safety case for future nuclear plant designs including Generation-IV reactors. Our concerns are also addressed with respect to the increasing trend toward adopting 'risk-based', as opposed to 'risk-oriented', regulatory concepts or establishing risk-based regulatory acceptance criteria in the midst of large uncertainties especially in connection with the design-specific PSA for future/advanced reactors.

1:30 - 3:00 PM

## 4-6: Risk Management

Session Chair: Cornelia Sfetzer

### Environmental and Safety Violations, an Alternative Indicator for Process Safety?

Marieke Kluin(a), Ben Ale(a), Wim Huisman(b) and Coen van Gulijk(a)
*a) Safety Science Group, Delft University of Technology, The Netherlands. b) Faculty of law, VU University of Amsterdam, The Netherlands*

From various studies in the criminology it is known that white collar crime is a serious problem. Not only for the industry, it also endangers the safety of workers, and has an impact on public health and the environment. Incidents like Piper Alpha and BP Texas City Refinery, and similar incidents are considered as white collar crime. What was wrong with the precautions, rules and regulations regarding the safety of the people, environment or nature? Did the company break the rules or regulations? It is difficult to get a conviction for behavior which people don't expect to be treated as criminal. Was it an accident or an unwanted side effect or the result of a criminal negligence? This is a component of the second part of a PhD research and is an empirical study on occupational safety and health and environmental regulations of chemical corporations. We hypothesize that corporations who tend to be less safe have a criminal record or some other form of registration. This paper presents the initial results by doing participant observations at chemical corporations. We observed the inspection and the team judged and found minor offences, which were interesting results. We planned more participant observations at other chemical corporations to validate our first results.

### Use of Terminology in Risk-Informed Decision Making

Mary Drouin(a), Michelle Gonzalez(a), Sandra Lai(a), Gary DeMoss(a), John Lehner(b), Jeffrey LaChance(c), Timothy Wheeler(c)
*a) US Nuclear Regulatory Commission, Washington DC USA. b) Brookhaven National Laboratory, Upton, NY USA. c) Sandia National Laboratories, Albuquerque, NM USA*

The Policy Statement on the Use of Probabilistic Risk Assessment (PRA) Methods in Nuclear Regulatory Activities [1] expressed the Commission"s belief that the use of PRA technology in U.S. Nuclear Regulatory Commission (NRC) regulatory activities should be increased. Consequently, numerous risk-informed activities were carried out in all areas of NRC regulation. With increased risk-informed activities came the recognition that regulatory stability and efficiency would be enhanced if the many potential applications of risk-information are implemented in a consistent and predictable manner. An essential part of consistent and predictable implementation is the use of consistent terminology to assure accurate communication and transfer of information. Further, it is recognized that some risk related terms have been used in ambiguous ways by practitioners, the increased development of guidance documents, regulations, procedures, etc., related to risk-informed activities makes the fundamental understanding of these risk related terms more imperative. Consistent terminology is essential to the appropriate implementation of risk-informed activities and the communication between NRC and its stakeholders. It allows practitioners to eliminate communication issues and avoid unnecessary discussions that may have been erroneously perceived as technical issues. Therefore, a glossary with agreed-upon definitions of risk-informed related terms is an essential tool for future risk-informed activities.

### Risk-informed Decision Making in the Context of NASA Risk Management

Homayoon Dezfuli(a), Michael Stamatelatos(a), Gaspare Maggio(b) and Christopher Everett(b)
*a) Office of Safety & Mission Assurance, NASA Headquarters, Washington, D.C.. b) Technology Risk Management Operations, ISL, New York, NY*

NASA NPR 8000.4A, Agency Risk Management Procedural Requirements, defines Risk Management (RM) in terms of two complementary processes: Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM). The RIDM process is intended to inform decision making through better use of risk and uncertainty information in selecting alternatives and establishing baseline performance requirements. The CRM process is used to manage risk associated with the implementation of the baseline performance requirements. The RIDM process consists of the following three parts: Formulating Performance Measures and Identification of Alternatives – In this part, mission objectives are decomposed into measurable performance objectives and associated performance measures, and the set of decision alternatives to analyze is compiled. Risk Analysis of Alternatives – In this part, the performance measures of each alternative are quantified, taking into account uncertainties that stand between the decision to implement the alternative and the accomplishment of the objectives. Risk-Informed Alternative Selection – In this part, the merits of each alternative are deliberated in the context of performance commitments, i.e., the performance values that correspond to uniform levels of risk tolerance. The performance commitments of the selected alternative are input to the requirements development process as the levels of performance to be pursued.

# Modeling and Simulation

**Thursday, Salon B**

10:30 AM - Noon

## 2-10: Reactor Systems

Session Chair: Pekka Pyy

### Critical Analysis of MAAP Feed and Bleed Success Criteria

Sarah L. Chisholm, P. Doug Paul, and Bryan C. Carroll
*Duke Energy Corporation, Charlotte, USA*

Historically in the PRA model as well as in the conservative methods used by the Duke Energy design basis Safety Analysis group, a minimum of two high pressure injection pumps were required for successful implementation of feed and bleed. Using MAAP 4.0.6 and the current plant parameters, new feed and bleed success criteria of only one high pressure injection pump were developed. Given that these new success criteria are less restrictive than both the historical PRA results and the deterministic results, a critical analysis of MAAP input parameters impacting feed and bleed was performed. Additionally, several sensitivity studies were developed to verify that the new feed and bleed success criteria did not under predict the high pressure injection requirements. This critical analysis of the feed and bleed success criteria was later used to support an NRC Significance Determination Process (SDP) analyzing the impact of air entrainment in the line connecting the borated water storage tank and the high pressure injection system. The air entrainment could have led to the loss of one high pressure injection pump during safety injection. Using the new success criteria of a minimum of one high pressure injection pump required for feed and bleed assisted in bringing the results of the SDP analysis from a potential greater than Green finding to a Green finding. This paper will describe in depth the critical analysis of MAAP input parameters for plant heat sources, heat sinks, and phenomena and modeling related to feed and bleed. The paper will also describe the positive impacts of reducing the minimum success criteria to the PRA feed and bleed model and how these positive impacts affected the Duke Energy assessment of the SDP analysis.

### An Evaluation of Operator's Action Time Using the MARS Code in a Small Break LOCA

Yeonkyoung Bae(a), Jonghyun Kim(b), Changhwan Park(c)
*a) Korea Hydro & Nuclear Power Co., Ltd., Daejeon, Korea. b) Paul Scherrer Institut, 5232 Villigen PSI, Switzerland. c) Future & Challenges Technology Co., Ltd., Kwanak-Gu, Seoul, Korea*

To estimate the success criteria of operator action time, MAAP4 code which is more conservative than the best-estimate code has been used in the probabilistic safety assessment (PSA) of the reference plant. This paper presents the MARS code analysis to estimate the time windows for two operator actions of a small break LOCA, i.e., feed and bleed and core cooling recovery. For a realistic analysis, emergency operating procedures were considered. Four break sizes were simulated to obtain the most severe case for the actions. The impact of the analysis on human error probabilities and core damage frequency was also investigated, and results were compared with the previous PSA for the reference plant. In conclusion, the MARS analysis provides larger time windows for each operator action than the MAAP4 analysis, but gave a slight difference of core damage frequency (CDF) due to the difference in the break size.

### EPR Flamanville 3 Level 2 Probabilistic Safety Assessment

Body Guillaume
*EDF, Villeurbanne, France*

Probabilistic safety analysis plays an essential role in the nuclear regulation processes. As such, the EPR Level 2 PSA, allowing evaluation of the nature, the magnitude and the frequency of radioactive releases outside the containment boundary, is an essential part of EPR safety and design considerations. However, while attempting to closely model a nuclear installation, country-specific safety requirements may significantly influence the structure of a Level 2 PSA. This paper illustrates this influence, while considering US and Flamanville 3 EPRs. The Flamanville 3 Level 2 PSA is based on the US EPR Level 2 PSA submitted to the US NRC in support of the Design Certification. However, significant evolutions were made to the study for Flamanville 3. Major changes were necessary to address the differences in terms of safety design objectives between US and Flamanville 3 EPRs. These include additional system analysis, new radiological release categories and some more modifications related to the integration of Flamanville 3 Operating Strategies for Severe Accidents (OSSA).

# Human Reliability Analysis

**Thursday, Salon C**

10:30 AM - Noon

## 5-10: HRA Applications

Session Chairs: April Whaley, Katrina Groth

### Pilot Application of the EPRI/NRC Fire HRA Guidance

Barbara Baron(a), Ashley Mossa(b), and David McCoy(b)
*a) Westinghouse Electric Company LLC, Monroeville, USA. b) Westinghouse Electric Company LLC, Windsor, USA*

Fire Human Reliability Analysis (HRA) is used to determine the probability of an operator failing to perform action(s), as defined by plant specific procedures, guidance, and training, following a fire-induced initiating event. Fire Human Error Probabilities (HEPs) are included in a fire Probabilistic Risk Assessment (PRA) to reflect the as-operated plant. This paper presents the results and insights of the Pressurized Water Reactor Owners Group (PWROG) pilot application of the draft Electric Power Research Institute (EPRI) / Nuclear Regulatory Commission (NRC) Fire HRA Guidelines [1], referred to as the Guidelines herein. WCAP-17189-NP [2] documents the pilot application. The pilot plant is a Westinghouse designed plant with four Nuclear Steam Supply System loops. Specific information from the pilot plant, such as procedures, drawings, training documentation, and operator interviews, is used to develop fire HEPs. Feedback has been provided to the Guidelines writing team. The preliminary results show that substantial expertise is required to independently apply the Guidelines. It is recommended that further clarifications be provided on the practical application of the Guidelines for addressing the HRA supporting requirements to meet Capability Category (CC) II of ASME/ANS RA-Sa-2009 [3]. It is also recommended that additional guidance on several areas, such as the availability of communications, operator stress levels, and actions that are performed in response to spurious instrument indications be provided.

### Qualitative Human Reliability Analysis-Informed Insights on Cask Drops

Jeffrey D. Brewer(a), Stacey M. L. Hendrickson(a), Ronald L. Boring(a), and Susan E. Cooper(b)
*a) Sandia National Laboratories, Albuquerque, NM, USA. b) United States Nuclear Regulatory Commission, Washington, DC, USA*

Human Reliability Analysis (HRA) methods have been developed primarily to provide information for use in probabilistic risk assessments analyzing nuclear power plant (NPP) operations. Despite this historical focus on the control room, there has been growing interest in applying HRA methods to other NPP activities such as dry cask storage operations (DCSOs) in which spent fuel is transferred into dry cask storage systems. This paper describes a successful application of aspects of the "A Technique for Human Event Analysis" (ATHEANA) HRA approach [1, 2] in performing qualitative HRA activities that generated insights on the potential for dropping a spent fuel cask during DCSOs. This paper provides a description of the process followed during the analysis, a description of the human failure event (HFE) scenario groupings, discussion of inferred human performance vulnerabilities, a detailed examination of one HFE scenario and illustrative approaches for avoiding or mitigating human performance vulnerabilities that may contribute to dropping a spent fuel cask.

### Utilisation of HRA Key Insights for LPS Operating Procedures: Example for an Implementation put in Practice

Cornelia Spitzer
*TÜV SÜD Energietechnik GmbH Baden-Württemberg, Mannheim, Germany*

Probabilistic Safety Assessments (PSAs) in Germany have essentially been conducted in the framework of recurrent Safety Reviews. Moreover, this type of analysis has been utilised in the usual regulatory procedures in order to benefit from the diverse approach with respect to different safety relevant insights which can be obtained. Significant safety relevant insights have e. g. been gained from the Human Reliability Assessment (HRA) in the context of Low Power and Shutdown (LPS) PSAs whose performance has been launched by the regulatory body. In this paper major insights and results together with the implementation put in practice particularly from Human Factor (HF) points of view are described. Thereby, selected key issues on HRA as well as some substantial insights and conclusions derived from LPS HRAs will be addressed. Further, a specific example with respect to the design and review of a complete set of operating procedures specifically dedicated to the shutdown operation is illustrated by outlining the general approach as well as the overall outcome achieved. Finally, some conclusions will be drawn regarding the relevance of probabilistic investigations, the appropriateness of a symptom oriented proceeding related to shutdown operation and the potential of utilising an advanced HF methodology.

### Human Reliability Analysis for EPR™ NPP PSA Level 2

Estelle Sauvage, Paul Duncan-Whiteman, and Alexandre Ezzidi
*AREVA NP SAS, Paris, France*

For plants that have implemented Severe Accident Management Guidelines (SAMGs), human actions performed during a severe accident should be taken into account in a Probabilistic Safety Assessment (PSA) Level 2. The detailed, full-scope PSA Level 2 developed and performed for EPR™ Nuclear Power Plants (NPPs) by AREVA includes the modeling of these human actions and provides a new approach to the Human Reliability Analysis (HRA) associated with this modeling. In order to accurately model severe accident human actions in a PSA Level 2, a technique of HRA is proposed that accounts for the complex chain of the emergency response personnel involved, and the responsibility divided between different emergency organizations. An approach which was selected for the PSA Level 1 may not be applicable for such complex interactions. The standard HRA techniques would then have to be adapted to model severe accident human actions. In the approach presented here, Operating Strategies for Severe Accident (OSSA) actions are broken down into several individual tasks performed by each member of the emergency organization. The individual tasks are then combined to obtain the Human Error Probability (HEP) for the modeled action. Dependency between the different actors of the emergency organization is accounted for when combining the tasks into the final action.

1:30 - 3:00 PM

## 5-11: Human Behavior and Disaster Response II

Session Chairs: Valerie Barnes, Jeffrey Joe

### Self-reliance and Advanced Warning Technology: How to Support the Human in Danger?

S. Sillem and H.M. Jagtman
*Delft University of Technology, Safety Science Group, Delft, the Netherlands*

In case of disasters, warning technologies are used to alarm the population in danger. Warning systems are especially of importance in those cases where it is impossible to rescue all individuals in danger by a professional rescue organization. In such cases, we need to rely on the selfreliance of individuals. The warning method that is currently used in many countries (the siren) is unable to provide people with the information they need to decide about the danger they are in, in an emergency. This paper will discuss a model that incorporates the knowledge there is about increasing citizens' self-reliance in emergencies by using new methods of warning and informing people in an emergency.

### Longitudinal Study to Determine Long-term Experience of Cell Broadcast for Citizens' Alarming

H.M. Jagtman and drs. S. Sillem
*Safety Science Group. Faculty of Technology Policy and Management. Delft University of Technology. The Netherlands*

In this paper we discuss the long-term experience of citizens who participated in multiple of the Dutch trials with cell broadcast for citizens' alarming. In a longitudinal study we address both the penetration of this group (based on the responses to warning messages) and the acceptance of the technology. The analysis should give insight in if and how their experiences have changed over time. As a base-line the citizens who participated only once are used. For the penetration it is questioned if the group who participated to multiple trails is reached different (responded more or less) than the group who participated once. For the acceptance, the opinion about the technology for citizens' alarming purposes is compared between the groups. In the end, we discus if the acceptance of the warning technology has changed over time during the trials and if so, how we should consider the long-term experience: are these citizens the potential front-runners after cell broadcast is implemented or are these disillusioned participants.

### Evacuation Behavior of Over 1,000,000 Residents in a Post-earthquake Fire Scenario in Kyoto City

T.Nishino(a), S.Tsuburaya(b), K.Himoto(a), Aand T.Tanaka(a)
*a) Disaster Prevention Research Institute, Kyoto University, Japan. b) Mitsubishi Heavy Industries, Kobe, Japan*

In this paper, the evacuation behavior of residents in a post-earthquake fire scenario in Kyoto City was simulated. It is conceivable that a tremendous number of evacuees may wander around in urban area escaping from hazards due to urban fires following a large earthquake in Japan. It is essential to implement effective evacuation measures in the regional disaster prevention plan for ensuring residents' safety. We have been developing a simulation model for the evacuation behavior of residents in a post-earthquake fire. The evacuation behavior of the residents in Tokyo City in the Kanto Earthquake Fire in 1923 was simulated for validating the model. The obtained results showed that the distribution of fatalities calculated by the model was qualitatively similar to that reported by the survey. In this paper, by using this model, the evacuation behavior of residents was simulated in expected post-earthquake fire scenarios in Kyoto City. The results were discussed in terms of the number and locations of fatalities.

# PSA Applications

**Thursday, East Room**

10:30 AM - Noon

## 1-10: Common Cause Failure Analysis

Session Chairs: Albert Kreuser, Jim Knudsen

### Development of Methods for Risk Follow-up and Handling of CCF Events in PSA Applications

Jan-Erik Holmberg(a), and Per Hellström(b)
*a) VTT, Espoo, Finland. b)Scandpower AB, Solna, Sweden*

Risk follow-up aims at analysis of operational events from their risk point of view using probabilistic safety assessment (PSA) as the basis. Risk follow-up provides additional insight to operational experience feedback compared to deterministic event analysis. Even though this application of PSA is internationally widely spread and tried out for more than a decade at many nuclear power plants, there are several problematic issues in the performance of a retrospective risk analysis as well as in the interpretation of the results. An R&D project sponsored by the Nordic PSA group (NPSAG) has focused on selected issues in this topic. The main development needs were seen in the handling of CCF and the reference levels for result presentation. CCF events can be difficult to assess due to possibilities to interpret the event differently. Therefore a sensitivity study with varying assumptions is recommended as a general approach. Reference levels for indicators are proposed based on the survey of criteria used internationally. The paper summarizes the results.

### Common-Cause Failure Analysis – Recent Developments in Germany

A. Kreuser and C. Verstegen
*Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Cologne, Germany*

A couple of activities on Common Cause Failures (CCF) are currently carried out by GRS in Germany. In one of these projects the existing CCF event data pool used for the calculation of CCF probabilities in Germany is updated with younger German operating experience. The aim of two other projects is to use the in Germany available national and international operating experience with common cause failures for improving plant safety. To reach this goal the known CFF phenomena and mechanisms are described and communicated in a comprehensive and structured way with the intention to support the review of the existing CCF prevention measures in the plants. In order to be able to handle large data sets consistently and in a traceable way GRS is developing an integrated program system for combining the different steps in the CCF evaluation and calculation process. The new tool will also provide a qualified documentation of the parameters used for the calculation of CCF probabilities. In another project, the coupling model which is used in Germany for the calculation of CCF probabilities in PSA is further developed.

### Common-Cause Failure Treatment in Event Assessment: Basis for a Proposed New Model

Dana Kelly(a), Song-Hua Shen(b), Gary DeMoss(b), Kevin Coyne(b), and Don Marksberry(b)
*a) Idaho National Laboratory, Idaho Falls, USA . b) U.S. Nuclear Regulatory Commission, Washington, DC, USA*

Event assessment is an application of probabilistic risk assessment in which observed equipment failures and outages are mapped into the risk model to obtain a numerical estimate of the event's risk significance. In this paper, we focus on retrospective assessments to estimate the risk significance of degraded conditions such as equipment failure accompanied by a deficiency in a process such as maintenance practices. In modeling such events, the basic events in the risk model that are associated with observed failures and other off-normal situations are typically configured to be failed, while those associated with observed successes and unchallenged components are assumed capable of failing, typically with their baseline probabilities. This is referred to as the failure memory approach to event assessment. The conditioning of common-cause failure probabilities for the common cause component group associated with the observed component failure is particularly important, as it is insufficient to simply leave these probabilities at their baseline values, and doing so may result in a significant un-

derestimate of risk significance for the event. Past work in this area has focused on the mathematics of the adjustment. In this paper, we review the Basic Parameter Model for common-cause failure, which underlies most current risk modelling, discuss the limitations of this model with respect to event assessment, and introduce a proposed new framework for common-cause failure, which uses a Bayesian network to model underlying causes of failure, and which has the potential to overcome the limitations of the Basic Parameter Model with respect to event assessment.

### Evaluation Between Existing and Improved CCF Modeling Using the NRC SPAR Models

James K. Knudsen
*Idaho Nation Laboratory, Idaho Falls, Idaho USA*

The NRC SPAR models currently employ the alpha factor common cause failure (CCF) parameterization and represent CCF for a group of redundant components as a single "rolled-up" basic event in the system fault trees. These SPAR models will be updated to employ a more precise but computationally intensive approach that expands the CCF basic events for all active components to include all terms that appear in the Basic Parameter Model (BPM). A discussion is provided to detail the differences between the rolled-up common cause component group (CCCG) and expanded BPM adjustment concepts based on differences in core damage frequency and individual component importance measures. Lastly, a hypothetical event is evaluated with a SPAR model to show the difference in results between the current method (rolled-up CCF events) and the newer method employing all of the expanded terms in the BPM. The evaluation of the event with the SPAR model employing the expanded CCF terms will be solved using both the Graphical Evaluation Module (GEM) within SAPHIRE, and SAPHIRE itself for the conditional probability calculation discussed in Reference 1.

# Structural Reliability

**Thursday, East Room**

3:30 -5:00 PM

## 11-1: Structural Reliability

Session Chair: Andy Dykes

### Reliability Data Handbook for Piping Components in Nordic Nuclear Power Plants – Part III

Anders Olsson(a), Vidar Hedtjärn Swaling(b), and Bengt Lydell(c)
*a) Scandpower-Lloyd's Register, Malmö, Sweden. b) Scandpower-Lloyd's Register, Stockholm, Sweden. c) Scandpower-Lloyd's Register, Houston, U.S.*

The PSAM 8 and 9 conferences included presentations of an ongoing Nordic R&D project concerned with piping reliability parameter estimation using service experience data. The PSAM 8 paper (No. 0063) addressed a pilot project which purpose was to define the prerequisites for producing a Reliability Data handbook for Piping Components ("R-Book") using the database developed by the OECD Pipe Failure Data Exchange Project (OPDE), www.nea.fr/html/jointproj/opde.html). The PSAM 9 paper (No. 0097) dealt with the methodology and issues with respect to different damage and degradation mechanisms. The current paper presents the methodology for deriving application-specific failure event populations and corresponding exposure terms. The paper also includes a demonstration of the data that is presented in the R-Book and example of insights from the results.

# RAM Methodology

**Thursday, West Room**

10:30 - Noon

## 7-1: Aging Management

Session Chair: Homayoon Dezfuli

### A New Class of Risk-Importance Measures to Support Reactor Aging Management and the Prioritization of Materials Degradation Research

Stephen D. Unwin, Peter P. Lowry, and Michael Y. Toyooka
*Pacific Northwest National Laboratory, Richland, Washington, USA*

As the US fleet of light water reactors ages, the risks of operation might be expected to increase. Although probabilistic risk assessment has proven an important resource in risk-informed regulatory decision-making, limitations in current methods and models have constrained their prospective value in reactor aging management. These limitations stem principally from the use of static component failure rate models (which do not allow the impact of component aging on failure rates to be represented) and a limited treatment of passive components (which would be expected to have an increasingly significant risk contribution in an aging system). Yet, a PRA captures a substantial knowledge base that could be of significant value in addressing plant aging. In this paper we will describe a methodology and a new class of risk importance measures that allow the use of an existing PRA model to support the management of plant aging, the prioritization of improvements to non-destructive examination and monitoring techniques, and the establishment of research emphases in materials science. This methodology makes use of data resources generated under the USNRC Proactive Management of Materials Degradation program which addresses the anticipated effects of various aging degradation mechanisms on a wide variety of component types.

### Optimal Block Replacement Policy for a System Operating under a Random Time Horizon

A. Khatab(a), N.Rez(b), D. Ait-Kadi(c)
*a) Laboratory of Industrial Engineering and Production of Metz (LGIPM), Ecole Nationale d'Ingénieurs de Metz. Metz, France. b) Laboratory of Industrial Engineering and Production of Metz (LGIPM) Université Paul-Verlaine. Metz, France. c) Mechanical Engineering Department, Faculty of Science and Engineering, Interuniversity Research Center on Entreprise Networks, Logistics and Transportation (CIRRELT). Université Laval, Quebec (Qc) Canada*

In this paper we consider the block replacement policy (BRP) for a system operating over a random time horizon. Under such a policy, a system is replaced by a new one either at failure or at a given time interval. The optimality criterion is the expected total replacements cost. Conditions under which an optimal replacement period exits are given. It is shown that BRP over an infinite time horizon is obtained as a particular case of the present work. A numerical example is given to illustrate the proposed replacement model.

### Optimal Inspection Planning with Time-Dependent Reliability Analysis. Application to Rubble-Mound Breakwaters

Nguyen Dai Viet, P.H.A.J.M van Gelder, H.J. Verhagen and J.K. Vrijling
*Delft University of Technology, Delft, The Netherlands*

In order to avoid failure in its lifetime, a breakwater system has to be inspected and, if necessary, has to be repaired. In this paper, a comprehensive maintenance strategy with optimal inspection planning is formulated. Rational maintenance decision-making approaches are discussed. The proposed maintenance strategy combines time-dependent and condition-dependent maintenance with event-dependent inspection. Optimal inspection planning is obtained by cost optimization with a safety constraint. In practical cases, it is possible to achieve an optimal inspection plan when relevant parameters of strength and load are existing and available.

### A Case Study On VVER-440 Component Age-Dependent Reliability Data Assessment

Shahen Poghosyan(a), Albert Malkhasyan(a) and Andrei Rodionov(b,c)
*a) Nuclear and Radiation Safety Center (NRSC), Yerevan, Armenia. b) EC JRC Institute for Energy, Petten, Netherlands. c) Institut de Radioprotection et de Sûreté Nucléaire (IRSN), Fontenay aux Roses, France*

The paper presents the results of a case study on "VVER-440 component age-de-

pendent reliability data assessment" performed in the frame of European Commission Joint Research Center (EC JRC) Ageing PSA (APSA) Network activities. The study is aimed to demonstrate the feasibility to apply the methods and approaches developed within APSA Network for assessment of ageing trends and elaboration of time-dependent reliability models for the case of VVER-440 generic component reliability data. These approaches are presented in the special data analysis guideline produced within APSA Network. The Guidelines mostly oriented to active safety components supposing that the reliability data are collected for the large statistical samples during the long period of time. The conditions regarding the sample size and duration of data collection period are very difficult to satisfy in case of only one plantspecific data collection. This is the case of VVER-440 reactors operated in Europe. For all of them the reliability data were collected in the frame of PSA development on the plant specific basis. The case study treats the statistical data provided by APSA Network participants for three components types: diesel generators, main feedwater pumps and 6.0kV breakers. The results of the study discuss the pulling procedure and time-dependent models construction.

### Development of Aging Risk Assessment Method with Incorporation of Aging and Maintenance Effects into System Reliability Models

Nobuo Mitomo(a), Tadatsugi Okazaki(b), Hiroshi Matsui(a), Yoh-ichi Kawagoe(a), Fumi Yakabe(a)
*a) National Maritime Research Institute, Tokyo, Japan. b) Tokyo University of Marine Science and Technology, Tokyo, Japan*

In Japan, nuclear power plant has been building since 1966. As mentioned in our previous report [1] ~ [3], we have been studying about the incorporation of aging and maintenance effects into system reliability models. Purpose of this study is to confirm the risk assessment method for aging effects that we have developed, by the assessment of a sample plant. This study is a part of the project to establish the risk assessment method for aging effects, which was started in 2005 for three years and we settled three tasks as follows, 1. Incorporation of aging and maintenance effects into system reliability models. 2. Development of the code for aging risk assessment with the code developed in task 1. 3. Assessment of a sample plant. In this report, details of the task 2 and 3 are explained. Task 3 is to verify that the code developed in task 1, 2 is very useful. This project officially finished in 2007, and we are still continuing analyses about aging effects for next step.

1:30 - 3:00 PM

## 7-2: Health Monitoring

Session Chair: Robert Youngblood

### Real-time System Risk Assessment using Asynchronous Multivariate Condition Monitoring Data

Jian Sun, Dan Zhang, and Haitao Liao
*Department of Nuclear Engineering, University of Tennessee, Knoxville, USA*

To perform real-time risk assessment for a multi-component system like the steam turbine in a nuclear power plant, the risk of the system must be predicted by taking into account multiple degradation processes and the relevant condition monitoring data. In many situations, multivariate condition monitoring data are collected asynchronously due to different sampling rates and/or variable condition monitoring schemes used in sensor networks. This raises a challenging problem in probabilistic risk assessment for such complex systems. In this paper, a Functional Principal Component Analysis (FPCA) method is developed to overcome this challenge. This method enables the prediction of remaining useful life of each component in the system and the prediction of real-time system risk based on multivariate asynchronous condition monitoring data. A numerical example is provided to demonstrate the application of the proposed method.

### Qualification for Supplied Electrical Motors: A Comparative Analysis of the Reliability of Electrical Motors from Different Suppliers

Mohammad Pourgol-Mohammad
*Goodman Manufacturing Inc., Houston, USA*

It is a critical decision for an industry to replace the supplier of an existing part, e.g., an electrical motor used in its systems for long periods of time (abundance of field/test data and information), with a new supplier (lack of sufficient data) for cost-saving reasons. The replacement should be made only after a full battery of testing and analysis to make sure the reliability/quality will not be sacrificed in favor of the cost savings benefit. This is often the case with the emergence of enormous overseas and Asian suppliers, not as well known as other companies, but which have attractive offers. Such a dilemma requires a comprehensive plan for testing in a relatively short period of time, in order to estimate failure rates and reliability with acceptable confidence. To ensure that new suppliers meet the reliability requirements, a well-designed reliability test plan is necessary. The test results are combined with available field data (mostly from warranties) to qualify the electrical motors. The reliability test plan should address all areas of concern, including corrosion, vibration, load stress, and so on. The focus of this research is limited to the design of a reliability test plan for load stress. It is based on the comparative analysis of existing and new counterpart electrical motors from two different suppliers. The comparison requires consideration of consistent loads on the electrical motors; otherwise, the results will not be conclusive. Load is interdependent with other motor parameters, such as torque, voltage, current, and input power. With several experiments resulting in unbalanced current load and temperature rises on the motors with torque-controlled stresses, the test was modified to balance the load on voltage and current, as well as on torque load. TOP of the motors is bypassed to achieve higher temperatures. The result of the test will be combined with available field data to estimate the new motor failure rate and reliability. Statistical data analysis (Weibull) is conducted for the accelerated testing results to estimate life parameters. A model is proposed to estimate Weibull parameters for new supplier motor life, based on analytical results from test and warranty data (available on existing supplied motors only).

### Improving Availability and Safety of Control Systems by Cooperation Between Intelligent Transmitters

Florent Brissaud(a,b), Anne Barros(b), and Christophe Bérenguer(b)
*a) Institut National de l'Environement Industriel et des Risques (INERIS), Verneuil-en-Halatte, France. b) Université de Technologie de Troyes (UTT), ICD, FRE CNRS 2848, Troyes, France*

"Intelligent transmitters" taking part in distributed and networked control systems are considered. Such sensor systems are able to perform internal data processing, advanced functionalities (e.g. self-diagnoses, online reconfiguration), and to exchange information. A control system made up of cooperating transmitters is therefore presented, using procedures which aim to improve system availability and safety. Taking advantage of the information exchanged between transmitters, two algorithms are proposed in order to i) retain the most confident values for transmitter processing, and ii) perform diagnoses by result comparisons. The control system is modelled by stochastic and coloured Petri nets, and dependability evaluations are performed by Monte Carlo simulations. Availability and safety can be put in balance through the use of the proposed algorithms, and both criteria can be improved under some conditions, notably according to diagnostic coverage of failures.

### Structural Fatigue-Induced Degradation: Prognostics and Health Monitoring Using Acoustic Emission

Masoud Rabiei(a), Mohammad Modarres(a), and Paul Hoffman(b)
*a) University of Maryland, College Park, USA. b) NAVAIR 4.3.3 Structures Division, Patuxent River, USA*

In the past few years, a research effort has been in progress at University of Maryland to develop a Bayesian framework based on Physics of Failure (PoF) for risk assessment and fleet management of aging aircraft. The ultimate goal of this effort is to develop an integrated probabilistic framework for utilizing all of the available information to come up with enhanced (less uncertain) predictions for structural health of the aircraft in future missions. Such information includes material level fatigue models and test data, health monitoring measurements and inspection field data. Despite significant achievements in modeling of crack growth behavior using fracture mechanics, it is still of great interest to find practical techniques for monitoring the crack growth instances using nondestructive inspection and to integrate such inspection results with the fracture mechanics models to improve the predictions. In the work presented in this paper, a probabilistic damage-tolerance model based on acoustic emission (AE) monitoring is proposed to enhance the reliability and risk prediction for structures subject to fatigue cracking.

3:30 - 5:00 PM

## 7-3: Quantitative Methods in RAM Analysis

Session Chairs: Harold Blackman, Soli Khericha

### Estimating and Presenting Transient Risk for On-Line Maintenance Using the STP Balance of Plant Model

Ernie Kee, Fatma Yilmaz
*South Texas Project Nuclear Operating Company, Wadsworth, Texas USA*

RAsCal, a CRMP application used by the STP plant Work Control and Operations groups relies on data from the Balance of Plant model to help manage risk while the plant is operating on-line, producing electricity on the Texas ERCOT grid. The STP Balance of Plant model produces estimates of risk in terms of availability and frequency for events such as plant trip and various levels of non-trip production loss. Until recently, RAsCal only presented risk of plant trip to the users (Operations and Work Control). The users have asked the STP Risk Management team to add the capability to present the risk of non-trip transients to RAsCal. This study presents the way the transient risk will be included in the RAsCal application.

### Availability and Reliability of General Multistate Node Networks Modeled by UGF and Taking into Account Connectivity Uncertainty

Mazen El Falou, Eric Châtelet
*Université de Technologie, Institut Charles Delaunay, Troyes, France*

Availability assessment of nowadays telecommunication systems (as Metropolitan Area Networks, Ad-Hoc and Sensor networks, Mobile networks…) is a major performance factor in the design phase. To ensure the availability, many designers introduce redundancy into the network architecture to achieve a quality of service (QoS) over a required threshold. The universal generating function (UGF) method has proved to be very effective in the availability estimation of multistate node networks (MNN) and it does not require a great computational effort. But this method doesn't take into account the uncertainty due to environment interference, nodes degradation and signal attenuation. The proposed work introduces a method incorporating uncertainty about the connectivity in order to assess the availability of MNN. The uncertainty is modeled by probabilistic approach and is propagated into the UGF model using Monte Carlo simulation. Uncertainty analysis is applied to estimate the worst condition by comparing the output availability with the required one. The objective is to optimize and to secure the designed network architecture, and consequently to attempt the client availability requirements. In addition, the proposed method allows designers to identify critical nodes that should be redundant and frequently monitored. This permits to calibrate the designed network, to increase its availability and to reduce the budget.

# Safety Culture & Organizational Factors

**Thursday, North Room**

10:30 - Noon

## 9-10: Cross-Cultural Issues

Session Chair: Joan Harvey

### Cultural Differences in Design Perceptions of Consumer Products: A Kansei Engineering Approach

K Pearce, J Harvey & R Jamieson
*Newcastle University, Newcastle upon Tyne, United Kingdom*

National cross-cultural differences can be linked to organisational and manufacturing success or failure; additionally they have been shown to influence design perception, which in turn can impact on product acceptability and marketability in different countries. Participants in Austria, China, India and the United Kingdom completed Kansei Engineering questionnaires to measure affective responses to and perceptions of 8 light dimmer switches. Following univariable and multivariable statistical analysis, both gender and nationality differences were found in single emotional measures and in clusters; these are interpreted in terms of product design attributes that provoke specific emotion. The findings are considered in light of existing knowledge about national cultures and emotions.

### Risks and Engineering Design Across Cultures

Joan Harvey, Kim Pearce and Ron Jamieson
*Newcastle University, Newcastle upon Tyne, United Kingdom*

Many international joint ventures or collaborative assignments have poor success rates, often because of culture clashes. Whatever problems there may be in working with people from other cultures, these cannot be helped when the working may involve rarely or never meeting the others in person, and when the individuals involved have no understand of the cultural niceties of those with whom they are working. This research involves engineers working collaboratively on design projects with other engineers, from China, the UK, Austria and Germany. Following interviews with Chinese and UK engineers, a questionnaire was compiled to investigate attitudes to deadlines, long hours, obligation to work, relationships, and trust and specific interpretations of words relating to deadlines, such as 'soon' and 'urgent'. Several cultural differences were found and are discussed in light of prevailing theory and knowledge.

### Driver Boredom: Does it Differ Across Cultures, and Why?

J. Harvey(a), N. Thorpe(a) , S Heslop(a) and C. Mulley(b)
*a) Newcastle University, United Kingdom. b) University of Sydney, Sydney, Australia*

Driver boredom is an area of driver behaviour that has received little attention. This study utilises a factor structure underlying driver boredom in order to investigate cross-cultural, age and gender differences in the experience of driver boredom and preferred driving speeds using a self-report questionnaire. The existing structure based on 49 items included four dimensions: responses to under-stimulation, enthusiasm/flow, lapse and error proneness and anxiety. Data for UK and US respondents were compared on the four factors and also on the relationships between these factors and personality variables, allowing for age and gender. Differences were found between two main country groups and some gender differences were also found. These findings are considered in terms of cognitive capacity required for driving, self-reported cognitive failure and errorproneness and the implications for drivers maintaining safety margins when bored.

# Transportation

**Thursday, North Room**

1:30 - 3:00 PM

## 17-1: Transportation Risk Assessment and Management

Session Chair: Alan Rao

### Use of PSA Technique for Risk Assessment of Hydrogen Energy Application in Road Transport

Andrei Rodionov(a,b), Heinz Wilkening(a) and Pietro Moretto(a)
*a) EC JRC Institute for Energy, Petten, Netherlands. b) Institut de Radioprotection et de Sûreté Nucléaire, Fontenay aux Roses, France*

One of the possible applications of hydrogen energy is private and public road transport. The transport application itself consists of several technological stages, such as hydrogen production, storage, distribution and utilization in a car as a fuel. Each of these technological stages represents a certain risk for public and individual. The aim of the present study is to identify and quantify the additional risks related to hydrogen explosions during the operation of a hydrogen driven car. In a first attempt the accidents or failures of a simple one-tank hydrogen storage system has been studied as a main source of risk. Three types of initiators are taken into account: crash accidents, fire accidents without crash (no other cars are involved) and hydrogen leakages in normal situation with following ignition. The consequences of hydrogen ignition and/or explosion depend strongly on environmental conditions (geometry, wind, etc.), therefore the different configurations of operational and environmental conditions are specified. Then Event Tree / Fault Tree methods are applied for the risk assessment. The results of quantification permit to draw conclusions about the overall added risk of hydrogen technology as well as about the main contributors to the risk. Recommendations concern the applicability of proposed harm and risk acceptance criteria, as well as sensitivity of final results to the postulated assumptions and limitations. Results of this work will eventually contribute to the on-going pre-normative research in the field of hydrogen safety.

### Certification of Rail Signalling Constituent and Subsystems

Thor Myklebust
*SINTEF ICT, Trondheim, Norway*

Since the European interoperability directives came into force in 1996, a European approval system for rail signalling systems and other railway systems has been put into practice. This paper describes how certification of signalling systems can be performed in practice and how NB-Rail (Notified Bodies) contributes to this process. International certification schemes and acceptance of products are evaluated and solutions for how this can be used internationally for rail are discussed.

### The Cost-Effectiveness of a Steel Tube or a Buffer Zone for Mitigating Blast Effects on a Building Spanning an Underpass with Transport of LPG

S.I. Suddle(a,b), J. Weerheijm(a,c), A.C. van den Berg(c)
*a) Delft University of Technology, Delft, The Netherlands. b) SSCM – Suddle Safety Consultancy & Management, Schiedam, The Netherlands. c) TNO Defence, Security and Safety, Rijswijk, The Netherlands*

The use of space is being intensified near and above transport routes of hazardous materials. In The Netherlands, some buildings are even realized above infrastructure with transport of hazardous materials like LPG. An accident with an LPG-tank may result in a BLEVE, causing injuries and large structural damage to the spanning building and the vicinity. Fortunately, such disasters are scarce up to now. However, one should be aware of that such accidents may occur and escalation from accident to disaster should be prevented. On one hand, this paper presents the modelling and the analysis of the explosion effects and the dynamic response of the structural elements. On the other, an analysis of structural measures to control the consequences for the spanning building when the explosion occurs in the underpass is given: two mitigating measures to minimize the effects of a gas explosion or a BLEVE are analyzed, i.e. a steel tube for packing the infrastructure in which the LPG is transported or a buffer zone by adding two extra stories to the building, in which the first two lower floors are designed to be severely damaged under explosive loading forming a buffer zone between the infrastructure and the building above. Subsequently, the cost-effectiveness of these safety measures is determined.

# Industrial Safety

**Thursday, Municipal**

10:30 - Noon

## 6-4: Occupational Safety

Session Chairs: Davide Manca / Wan Ki Chow, Severino Zanelli / Nattasha Freeman

### Human Error: Anatomy of Accidents

Anthony J Spurgin
*Independent Consultant, San Diego, California, USA*

The paper examines various industrial accidents and lists the lessons that can be learned from their study. These insights can be used in a number of ways, such as improving an understanding of the causes of human errors and impact the modeling of human errors, selection of human reliability assessment methods and models. Accident analysis can also be used to identify how the structure of Probabilistic Risk Assessments (PRAs) could be improved by incorporating ideas derived from these investigations.

### Manual Handling Risk Assessment: The Case of Lifting and Carrying Operations in the Construction Industry

Armando Búrciaga-Ortega, and Jaime Santos-Reyes
*Grupo: "Seguridad, Análisis de Riesgos, Accidentes y Confiabilidad de Sistemas" (SARACS), SEPI-ESIME, IPN, Mexico City, Mexico*

According to the ILO organization, every year more than 2 million people die from occupational accidents or work related diseases. Musculoskeletal disorders (MSD) constitute the largest category of work related illness in developed and developing countries. The papers presents the results of a case study of a manual handling risk assessment for the case of lifting and carry operations in the construction industry. The approach has been the application of the Manual Handling Assessment Charts (MAC) tool. The MAC tool has been developed by the HSE; the tool is intended to assess the risk factors in lifting, carrying and team handling operations. The present case study only assessed the individual lifting and carrying operations in the construction industry. The results have shown that the workers performed poorly when assessed by the application of the MAC tool. More case studies are being conducted in other construction sites and other types of industries such as, manufacturing. It is hoped that by applying tools such as the MAC can help to assess the risks and prevent MSDs.

### Applying Nuclear PRA to a Nuclear Fuel Facility Integrated Safety Analysis

Matthew Warner, Jim Young
*GE Hitachi Nuclear Energy, Wilmington, NC, USA*

Nuclear fuel processing facilities are required to conduct an integrated safety analysis (ISA) as part of the licensing process. An ISA identifies potential accident sequences, designates items relied on for safety (IROFS), and describes management measures to provide reasonable assurance of IROFS availability and reliability. IROFS are intended to either prevent initiating events or mitigate accident consequences to an acceptable level. The ISA process also identifies and evaluates all internal initiating events (e.g., explosions, spills, and fires); and external initiating events (flooding, high winds, earthquakes, and external fires) that could result in facility-induced consequences to workers, the public, or the environment. Nuclear PRA methodology can be utilized for an ISA at a nuclear fuel processing facility. Applying the knowledge base that exists in the nuclear PRA industry to a fuel facility ISA can improve the quality and efficiency of the ISA. To do this, the training and oversight of the non-risk professionals on the ISA team is vital. Key areas to emphasize are precise definitions of initiators and IROFS, the multiple manifestations of dependency, and the use of quantitatively based data.

### Accident Modeling: No More Cheese Please

John Stoop
*Delft University of Technology, Delft, the Netherlands*

A series of surveys on existing accident investigation models demonstrate the existence of a wide variety of models, in particular in the human aspects domain. Such surveys however also indicate consecutive generations of models, a poor methodological basis, absence of a systems approach and a focus on the application of models by lay people. The majority proves to be a derivate from the James Reason's Swiss Cheese model and the Rasmussen model on systems hierarchy. Application of these models outside the process industry, such as in aviation, has demonstrated their conceptual limitations, leading to numerous interpretations and simplifications in accident investigation practices. Simplification of these models also degrades the intervention potential of the models. Intervention are restricted to changing isolated factors and aspects within a given design envelope. Such linearization does not longer comply with the needs of change in complex, dynamic systems design strategies. In order to intervene in complex dynamic systems, a redesign and prototyping approach is required in designing safer solutions. Such systems redesign incorporates higher systems levels, various systems states and testing of prototypes in a virtual environment by exposure to critical accident scenarios.

1:30 - 3:00 PM

## 6-5: Hazard Prevention

Session Chairs: Ivonne Andreade Herrera, Kaisa Simola

### Living Buildings in Land Use Planning with External Safety

Shahid Suddle(a,b) and Hennes de Ridder(a)
*a) Delft University of Technology, Delft, The Netherlands. b) SSCM – Suddle Safety Consultancy & Management, Schiedam, The Netherlands*

Due to a shortage of space, large urban development projects are realized adjacent or above transport routes of hazardous materials, causing external safety risks for people present (living or working) in such an environment. In The Netherlands, the decision making on land use planning regarding safety is traditionally based on a risk acceptance, and safety is in this respect not more than a test tool. However, no design standards for land-use planning in multiple and intensive used areas are given by the legislator. This paper presents a new look on coping with risks. One of the main purposes of the paper is to consider safety as a design parameter at an as early as possible stage in the development of urban locations, in stead of a test tool, resulting in safety measures taken within the project budget. The design tool should also be used at different scale levels: urban level, area level and building level. By doing this, safety integrated design and engineering is introduced in development of complex projects, which are currently confronted with the continuous changing demands of the users and legislators. Resulting from these changing demands, flexibility and clear insight in the lifecycle processes with a focus on design is very important. In this regard, we discovered that the Living Building Concept (LBC) can be used as a tool regarding safety integrated design and engineering, through which the relation between urban/land-use planning, civil engineering, environmental engineering and risk and crisis management can be strengthened.

### Development of Early Warning Indicators based on Resilience Engineering

K. Øien(a), S. Massaiu(b), R. K. Tinmannsvik(a) and F. Størseth(a)
*a) SINTEF Technology and Society, Safety Research, Trondheim, Norway. b) Institute for Energy Technology, Halden, Norway*

This paper describes a new method for the development of early warning indicators based on resilience and Resilience Engineering. This resilience based early warning indicator (REWI) method consists of three main parts. The first part is a set of contributing success factors being attributes of resilience, the second part is general issues for each of the contributing success factors ensuring that the goal of each contributing success factor is fulfilled, and the third part is the indicators established for each general issue, i.e., the way of measuring the general issues. This research has shown that it is possible to develop 'an indicator system' based on resilience engineering theory from which early warning indicators can be established. It may be used as a stand-alone system, or indicators established by other approaches may be included for the final selection of indicators. Further work is necessary in order to investigate to what degree these resilience based indicators are complementary to other safety performance indicators, for instance whether they provide a more appropriate measure of the ability to 'cope with the unexpected'.

### The Value of Disaster Prevention

Patrick Momal
*IRSN, Fontenay-aux-Roses, France*

What is the best combination of safety modifications to be chosen within a set of proposed modifications aimed at reducing (severe) accident probabilities? Can one rely on a safety-efficiency index dp/c where dp is the reduction in probability and c the cost of modifications? The answer is negative. Optimizing the selection process does mainly imply ranking modifications according to their efficiency (with exceptions). However, the efficiency index formula for a given modification should be based on μxdp/c, not dp/c. It is of course based on the reduction in probability but through the gain in expected loss (xdp if x is the accident cost) this benefit being multiplied by a factor μ (μ ≥ 1) which represents the decision-maker's risk aversion (classical economic terminology) or value of disaster prevention or willigness to prevent −terms which could be closer to preventionists' concerns. This total benefit μxdp is then allocated to cost c. Thus, optimizing safety requires teamwork with data from engineers (the probability gains dp and the accident scenarios), data provided by economists (the accident costs x) and data elicited by decision theory specialists (the multipliers μ). That is the solution in principle. In practice, it implies considering not only the most likely accident cases, but also unfavorable scenarios which imply higher costs and, especially, a higher value of disaster prevention (μ).

# Security / Infrastructure

**Thursday, Federal**

10:30 - Noon

## 14-5: Security Systems

Session Chair: Greg Wyss

### Applying Human Reliability Analysis Models as a Probabilistic Basis for an Integrated Evaluation of Safeguards and Security Systems

Felicia A. Durán(a,b) and Gregory D. Wyss(a)
*a) Sandia National Laboratories, Albuquerque, NM, USA. b) The University of Texas, Austin, TX, USA*

Material control and accounting (MC&A) safeguards operations that track and account for critical assets at nuclear facilities provide a key protection approach for defeating insider adversaries. These activities, however, have been difficult to characterize in ways that are compatible with the probabilistic path analysis methods that are used to systematically evaluate the effectiveness of a site's physical protection (security) system (PPS). MC&A activities have many similar characteristics to operator procedures performed in a nuclear power plant (NPP) to check for anomalous conditions. This work applies human reliability analysis (HRA) methods and models for human performance of NPP operations to develop detection probabilities for MC&A activities. This has enabled the development of an extended probabilistic path analysis methodology in which MC&A protections can be combined with traditional sensor data in the calculation of PPS effectiveness. The extended path analysis methodology provides an integrated evaluation of a safeguards and security system that addresses its effectiveness for attacks by both outside and inside adversaries.

### Vulnerability of Critical Infrastructure Systems: A Physical Analogy for Modeling Complex Hysteresis Behavior

Adrian V. Gheorghe(a), Dan V. Vamanu(b)
*a) Old Dominion University, Department Engineering Management and Systems Engineering, Norfolk, VA, USA. b) "Horia Hulubei" National Institute of Physics and Nuclear Engineering, Bucharest, Romania*

Systems consisting of parts – which may be seen as atomic (indivisible) components that usually come in large numbers, are couple with each other with a strength expressed as coupling "energy", and respond to external stress – were often shown to share behavioral features largely indifferent to the nature of the system. Taking advantage, the paper employs the Physics concept of hysteresis as a derivative of a co-operative behavior, to show that systems" observed tendency to resist stress and maintain their state and performance level against the driving stress applied is ubiquous and, especially off-Physics, highly meaningful. In the context of the developed model, the concepts of resiliency and vulnerability of highly interdependent critical infrastructure systems are introduced and experimented within a "serious gaming" simulation framework.

### Investigating the Impact of Humans in Information Technology Security: A Case Study at the University of Maryland

Danielle Chrun(a), Michel Cukier(a,b), Ali Mosleh(a), and Gerry Sneeringer(c)
*a) Center for Risk and Reliability, Department of Mechanical Engineering, University of Maryland, College Park, Maryland, USA. b) The Institute for Systems Research University of Maryland, College Park, Maryland, USA. c) Office of Information Technology University of Maryland, College Park, Maryland, USA*

With the increase of the number of attacks and their diversification, a main concern for organizations is to protect their network. To do so, decision makers need to decide what security strategy to implement to best protect their network. However, tools are lacking to help them decide how to invest in security. In this paper, we propose a causal model for managing information security that includes the human element involved in information security. The model is based on months of discussions with the Director of Security at the University of Maryland. It includes 1) the three stakeholders involved in security (attacker, user and organization) and the organization's assets, 2) characteristics for each stakeholder and the organization's assets (characteristics consist in attributes of each stakeholder and the organization's assets that have an influence on increasing or decreasing security), and 3) influences between the different characteristics. We will show how the qualitative model can be used to reason about security at several levels: assess organizational security, decide how to invest in security, and identify causes of security issues.

# Medical

**Thursday, Federal**

1:30 - 3:00 PM

## 13-1: Risk Assessment of Ambulatory Care

Session Chair: Jim Battles

### Approaches to Reduce Risk to Patients in U.S. Ambulatory Health Care

Robert J. Borotkanics(a), James M. Levett(b), Donna Woods(c), Virginia Moyer(d)
*a) Agency for Healthcare Research and Quality, Rockville, MD, USA. b) Physicians' Clinic of Iowa, Cedar Rapids, Iowa, USA. c) Northwestern University, Chicago, IL, USA. d) Baylor College of Medicine and Texas Children's Hospital, Houston, TX, USA*

Ambulatory health care is complex, and the scope of practice has increased over the past several decades. In parallel, the National Academies report, Building a Better Delivery System: A New Engineering/Health Care Partnership, has gained the interest of health care professionals. Use of risk assessments is increasing. Although ambulatory care may be technologically less complex than inpatient care and seemingly less complex than other industries, it is logistically more complex. This increases the risk of potential harm to patients. These factors are substantially influenced not only by the structure of the primary care, but also by the supporting infrastructure and cohesion of the health care community at the regional level. This paper provides a summary of the major, risk-informed quality improvement strategies used in ambulatory care and discusses the community-level factors that positively influence the type and rigor of an ambulatory-level health care quality improvement.

### The Future of Ambulatory Health Care: A Risk-Informed Model

Robert J. Borotkanics
*Agency for Healthcare Research and Quality, Center for Quality Improvement and Patient Safety, Rockville, MD, USA*

Health care provided in ambulatory settings, is complex, with intricate processes, involving the deliberate coordination of many people, often across multiple organizational boundaries. With the ever expanding scope of ambulatory care, it is increasingly important to remove or mediate potential risks and harms to patients before they occur. While the use of adverse event reports and chart review identifies risks and harms retrospectively, it is important to also look forward and eliminate or reduce potential risks to patients before they occur. The framework laid out in this paper, which is grounded in risk analysis, is an emerging model to improve patient safety and reduce the probability that harmful events will occur. Each aspect of the model is critically important. Risk analyses identify aspects of the care process with greater potential likelihood and significance of harm. Diverse teams of professionals come together to evaluate and troubleshoot potential and actual hazards. Critically important is consistent, leadership backing. Boundary maintenance provides a means for ambulatory centers to maintain their identity and work effectively with other organizations. Finally, quality improvement interventions need to be engineered into ambulatory care where possible, so that quality of care and prevention of patient harm are normal parts of the work day. The U.S. Agency for Healthcare Research and Quality's (AHRQ's) Risk-Informed Intervention program is an important step forward in demonstrating the value of this model. Geographically distributed throughout the United States, these AHRQ teams conduct risk assessments and are now implementing important and potentially self-sustaining interventions that cross multiple organizational boundaries.

### Ambulatory Care Patient Safety Proactive Risk Assessment, a Necessary First Step

James B. Battles
*US Agency for Healthcare Research and Quality, Rockville, Maryland, USA*

Much of the health care in the United States and around the world is delivered in ambulatory settings. Most medical and surgical procedures that were once provided only in hospitals are now routinely performed in ambulatory settings. However much of the focus on patient safety has been in the in patient setting. There is insufficient information on risks, hazards, and their consequences in ambulatory care. Unlike in the hospital setting there are no identified safe practices that should be implemented in the ambulatory setting. Evidence based safe practices in ambulatory care are yet to be identified. Using proven proactive risk assessment/modeling methods it is possible to begin to move to risks informed design and intervention. AHRQ has funded 20 risk assessment projects using a variety of methods and approaches to identifying risk and hazards in ambulatory setting. Clearly identifying risks and hazards is an essential first step in improving the quality and safety of ambulatory care. Proactive risk assessment is a vital first step in the design and development of interventions and safe practices. The use of established proactive risk assessment is a essential aspect of an going patient safety activities.

3:30 - 5:00 PM

## 13-2: PSA Applications to Healthcare

Session Chair: Robert Borotkanics

### Transmission of Antibiotics Resistance from Food: a Probabilistic Risk Analysis

Robert J. Borotkanics(a), Matthew Samore(b)
*a) Johns Hopkins School of Medicine, Division of Health Sciences Informatics, Baltimore, MD, USA. b) University of Utah, School of Medicine, Division of Clinical Epidemiology, Salt Lake City, Utah, USA*

Use of antibiotics has resulted in the emergence of antibiotic resistant Escherichia coli. Resistant strains may be acquired via prescription use, food consumption and household transmission. The goals of this study were to, 1) clarify the role of food exposures' contribution to the emergence of antibiotic-resistant E. coli colonization in the gut; 2) refine a simulation model to estimate the expected number of antibiotic-resistant colonized cases resulting from food exposures.
The study was carried out in a rural Idaho community, as a nested cohort of the larger Inter-Mountain Project on Antimicrobial Resistance and Therapy Study. Adjusted Monte Carlo simulation models suggest that food is an important contributor to resistant strain colonization. Bayesian inference found chicken to be substantial source of antibiotic resistant E. coli. Grocery store sampling of food samples is a reliable surrogate to household collection of food samples in epidemiological studies of antibiotic resistance. Antibiotics used in human, health care have entered the food system and are actively being re-transmitted. Antibiotics used in agriculture could also result in antibiotic resistant E. coli colonization. Our interpretations are suggestive and require further study, particularly on food production and their potential impact on clinical medicine.

### Risk Informed Evaluation

James B. Battles
*US Agency for Healthcare Research and Quality, Rockville, Maryland, USA*

Proactive risk assessment and risk modeling is becoming an increasingly important tool in health care The US Agency for Healthcare Research and Quality (AHRQ) has and is supporting risk assessment projects in the area of patient safety using PRA and ST-PRA. AHRQ has also linked the use of risk assessment and risk modeling to the design of new patient safety practices, particularly in the area of ambulatory care. It is now time to take the lessons that we have learned in the development and use of risk models not only in the design of safe practice and safety systems but to evaluation and assessment of these new safety interventions. We need to create a risk informed approach to evaluation of safety and quality improvement efforts. Using the risk models that were created for risk informed design that identify the risks associated with adverse outcomes these risk models can be used to focus attention on which processes are related to the elimination or mitigation of the risks associated with the adverse or undesirable outcomes.

### Using Risk Models to Improve Safety with Dispensing High-Alert Medications in Community Pharmacies

Michael R. Cohen(a), Judy L. Smetzer(a), John E. Westphal(b), Sharon Conrow Comden(b), Donna M. Horn(a), Thomas P. Lawlor(c)
*a) Institute for Safe Medication Practices, Horsham, PA, USA. b) Outcome Engineering, LLC, Plano, TX, USA. c) Independent Consultant, Deerfield, IL, USA*

Purpose: Determine if socio-technical probabilistic risk assessment (ST-PRA) can create detailed risk models that predict the incidence of preventable adverse drug events (PADEs) with high-alert medications dispensed in community pharmacies. Scope: This study involves PADEs associated with warfarin, methotrexate, fentanyl patches, and insulin analogs dispensed from a sample of 12,000 community pharmacies. Methods: A model-building team was used to build 10 fault trees to estimate the incidence of PADEs for the four targeted medications. The fault trees were populated with team estimates of human error, failed capture opportunities, and at-risk behaviors, validated and analyzed to determine unique risk pathways, and evaluated to determine the impact of recommended interventions on incidence rates. Results: PADEs with the highest incidence included: dispensing the wrong dose/strength of warfarin due to a data entry error (1.83/1,000 prescriptions); dispensing warfarin to the wrong patient (1.22/1,000 prescriptions); and dispensing an inappropriate fentanyl patch dose due to a prescribing error (7.30/10,000 prescriptions). PADEs with the lowest incidence included: dispensing the wrong drug when filling a warfarin prescription (9.43/1 billion prescriptions). Increasing patient counseling, conducting a second data entry verification process during product verification, bar-coding technology, and hard computer alerts that can't be bypassed easily provided the largest quantifiable reductions in risk. Key Words: Socio-technical probabilistic risk assessment (ST-PRA), preventable adverse drug event (PADE), fault tree, risk models.

### A PRA-Based Evaluation of Alternative White Boards in an ED Setting

John Wreathall(a), Robert L. Wears(b), and Shawna J. Perry(c)
*a) John Wreathall & Co., Inc., Dublin OH, USA. b) Shands Jacksonville Medical Center, University of Florida, Jacksonville, FL, USA. c) Virginia Commonwealth University Health Systems, Richmond, VA, USA*

There is a generally promoted view in healthcare that information technology (IT) will be a panacea for the various crises in that industry, from improving patient safety to reducing costs and expanding availability of care. This study was based in a busy emergency department (ED) in a large urban area in the USA and describes a PRA-based assessment of the relative risks to patient safety from using existing physical white boards as patient status tracking devices vs. IT-based devices intended to perform the same function. While both types appear to be work satisfactorily under nominal (routine) conditions, those times when the ED becomes a high-tempo stressed environment tends to lead to greater problems with the IT-based system. This is because it is less malleable than the physical system and therefore less readily adaptable to the complexities of work that arise in the high-tempo periods. Additionally, under these conditions, it had failure modes that were not anticipated before its implementation. These are seen as potentially important lessons for healthcare in its move to IT-based "solutions" in other areas.

# Waste Management

**Thursday, Superior**

10:30 AM - Noon

## 18-1: Radioactive Waste Management I

Session Chairs: Enrico Zio / Sitakanta Mohanty, Budhi Sagar

### Potential Impacts of Alternative Waste Forms on Long-Term Performance of Geological Repositories for Radioactive Waste

Peter N. Swift, Clifford W. Hansen, Ernest Hardin, Robert J. MacKinnon, David Sassani, S. David Sevougian
*Sandia National Laboratories, Albuquerque, New Mexico, USA*

Published results of performance assessments for deep geologic disposal of high-level radioactive waste and spent nuclear fuel in the United States, Sweden, France, Switzerland, and other nations provide insight into those aspects of the waste form that are potentially important to the long-term performance of the repository system. Hypothetical modifications to the wastes, such as might result from new technologies for processing spent fuel and advances in nuclear reactor design and waste forms have the potential to impact long-term performance. This paper reviews relevant results of existing performance assessments for a range of disposal concepts and provides observations about how hypothetical modifications to waste characteristics (e.g., changes in radionuclide inventory, thermal loading, and durability of waste forms) might impact results of performance assessment models. Disposal concepts considered include geologic repositories in both saturated and unsaturated environments.

### Conceptual Structure of Performance Assessments for the Geologic Disposal of Radioactive Waste

Jon C. Helton, Clifford W. Hansen, Cedric J. Sallaberry
*Sandia National Laboratories, Albuquerque, NM USA*

A conceptual structure for performance assessments (PAs) for radioactive waste disposal facilities and other complex engineered facilities based on the following three basic conceptual entities is described: EN1, a probability space that characterizes aleatory uncertainty; EN2, a function that predicts consequences for individual elements of the sample space for aleatory uncertainty; and EN3, a probability space that characterizes epistemic uncertainty. The implementation of this structure is illustrated with results from PAs for the Waste Isolation Pilot Plant and the proposed Yucca Mountain repository for high-level radioactive waste.

### Preliminary Performance Assessment of Deep Borehole Disposal of Radioactive Waste

Bill W. Arnold, Geoff Freeze, Peter N. Swift, Patrick V. Brady, and Stephen J. Bauer
*Sandia National Laboratories, Albuquerque, NM, USA*

Long-term disposal of high-level radioactive waste (HLW) and spent nuclear fuel (SNF) in deep (3 to 5 km) boreholes has the potential to achieve long-term safety performance at costs competitive with mined repositories. Low permeability, high salinity, and geochemically reducing conditions at many locations in the deep crystalline basement rock limit significant fluid flow and radionuclide transport. For a preliminary performance assessment analysis, 400 spent fuel assemblies were assumed to be vertically stacked inside the lower 2 km segment of 5 km deep borehole. The radionuclide release scenario was assumed to be (1) up the sealed borehole for 1 km in the crystalline basement rock, (2) into the overlying sediments, and (3) eventual capture by a hypothetical water withdrawal well. Coupled thermal-hydrologic analyses indicate that thermal expansion of groundwater would produce an upward pulse of flow. The preliminary performance assessment included the effects of radionuclide solubility, transport up the sealed borehole, sorption, radionuclide decay, and pumping from the withdrawal well, to calculate the dose to a human receptor. The performance assessment calculations indicated a negligible dose to the human receptor. The dose was due solely to the contributions of a single radionuclide (Iodine-129). The negligible long-term dose from a single deep borehole predicted by the preliminary performance assessment underscores the potential viability of deep borehole disposal of radioactive waste.

### The Performance of Deep-Burn TRISO Spent Fuel in a Geological Repository

Bret Patrick van den Akker and Joonhong Ahn
*Department of Nuclear Engineering, University of California at Berkeley, Berkeley, USA*

The use of a Deep Burn Reactor to recycle Commercial Spent Nuclear Fuel (CSNF) offers remarkable benefits including the extraction of additional electricity, added proliferation resistance, and a reduction of the radiotoxicity of the spent fuel. Two central components of the Deep Burn Reactor are the TRISO fuel particles, and the all graphite core. The TRISO coatings not only allow for extremely high burnups, but their corrosion resistance to groundwater attack makes them ideally suited for geologic disposal. Our analysis of the performance of the TRISO particles under attack from groundwater corrosion indicate that the overall failure rate of the TRISO particles will likely be below 0.1% for between 3,000 – 100,000yrs depending on the rate of dissolution of the SiC layer. The all graphite core design for the Deep Burn reactor is attractive from a repository perspective because of the slow corrosion of graphite in both air and water. Calculations of the lifetime of the graphite waste form in a flooded geological repository are in the range of 10^8 – 10^9 years. This remarkable resistance to groundwater corrosion makes this graphite waste form a near ideal engineered barrier against the release of radionuclides from a geological repository.

### Comparison Study of Radionuclide Transport Model for ILW and HLW Repositories between Advanced Nuclear Fuel Cycle Concept (KIEP – 21) and Reference Spent Fuel Disposal System (KRS) of Korea

Jihae Yoon and Joonhong Ahn
*Department of Nuclear Engineering, University of California, Berkeley, Berkeley, California USA*

We have evaluated the mass release rates of radionuclides at various locations in the engineered and natural barrier systems, and compared those between the case of direct disposal of spent PWR fuels in the KRS concept and that of wastes from the KIEP-21 pyroprocessing system in the A-KRS concept to investigate the potential radiological and environmental impacts. In both cases, most actinides and their daughters remain in the vicinity of waste packages as precipitates because of assumed low solubility. The total mass release rate of radionuclides from direct disposal concept is similar to those from the pyroprocessing disposal concept. While the mass release rates for most radionuclides would decrease to negligible levels without assuming any dilution or dispersal mechanisms due to radioactive decay, significant mass release rates for 129I, 79Se, and 36Cl, are observed at the 1,000-m location in the host rock. The effects of the waste-form alteration rate on the release of radionuclides were significant at the engineered barriers region, especially for congruently released radionuclides. The package failure time factor could handle containment and delay in the release of the radionuclides. The footprint of repository for the KIEP-21 system is about one tenth of those for the direct disposal:

1:30 - 3:00 PM

## 18-2: Radioactive Waste Management II

Session Chair: Enrico Zio / Sitakanta Mohanty, Budhi Sagar

### Performance Assessment for Radioactive Waste Management at Sandia National Laboratories: A 30-year History

Bonano, E.J., Kessel, D., Marietta, M., Swift, P., and Dotson, L.
*Sandia National Laboratories, Albuquerque, New Mexico, USA*

Over the past three decades, Sandia National Laboratories has developed and applied a performance assessment (PA) methodology that has informed key decisions concerning radioactive waste management. This experience includes not only the WIPP and Yucca Mountain projects, but also the initial development and demonstration of the U.S. Nuclear Regulatory Commission's initial PA capabilities for both high-level and low-level wastes, the subseabed disposal program, PAs for wastes stored at the Idaho National Engineering Laboratory, and PAs for greater confinement disposal (GCD) boreholes at the Nevada Test Site, as well as multiple international collaborations. These efforts have produced a generic PA methodology for the evaluation of total waste management systems that has gained wide acceptance within the international community. More importantly, this methodology has been used as an effective management tool to evaluate different disposal designs and sites; inform development of regulatory requirements; identify, prioritize and guide research aimed at reducing uncertainties for objective estimations of risk; and support safety assessments. This PA methodology could be adapted to evaluate analyses of different strategies and options that might be proposed to manage the back-end of the nuclear fuel cycle.

## Overview of Performance Assessment for the Waste Isolation Pilot Plant

Daniel J. Clayton, R. Chris Camphouse, Sean C. Dunagan, James W. Garner, Ahmed E. Ismail, Thomas B. Kirchner, Kristopher L. Kuhlman, Jennifer L. Long and Martin B. Nemer
*Sandia National Laboratories, Carlsbad, NM, USA*

The Waste Isolation Pilot Plant (WIPP) has been developed by the U.S. Department of Energy for the geologic (deep underground) disposal of transuranic waste. Compliance with the containment requirements is demonstrated by means of performance assessment (PA). The term PA signifies an analysis that 1) identifies the features, processes and events (FEPs) that might affect the disposal system; 2) examines the effects of these FEPs on the performance of the disposal system; 3) estimates the cumulative releases of radionuclides caused by all significant FEPs; and 4) accounts for uncertainty in the parameters of the PA models. Modifying the WIPP PA is a reoccurring process, which ensures confidence in the PA results. The updated WIPP PA demonstrates that the results continue to lie entirely below the specified limits and the WIPP therefore continues to be in compliance with the containment requirements. Analysis of the results shows that the total releases are dominated by radionuclide releases that could occur during an inadvertent penetration of the repository by a future drilling operation. The natural and engineered barrier systems of the WIPP provide robust and effective containment of transuranic waste even if the repository is penetrated by multiple borehole intrusions.

## Summary of the Total System Performance Assessment for the Yucca Mountain License Application

Clifford W. Hansen, M. Kathryn Knowles, Robert J. MacKinnon, Jerry A. McNeish, S. David Sevougian, Peter N. Swift
*Sandia National Laboratories, Albuquerque, New Mexico, USA*

The Department of Energy's 2008 Yucca Mountain Performance Assessment represents the culmination of more than two decades of analyses of post-closure repository performance in support of programmatic decision making for the proposed Yucca Mountain repository. The 2008 performance assessment summarizes the estimated long-term risks to the health and safety of the public resulting from disposal of spent nuclear fuel and high-level radioactive waste in the proposed Yucca Mountain repository. The standards at 10 CFR Part 63 request several numerical estimates quantifying performance of the repository over time. This paper summarizes the key quantitative results from the performance assessment and presents uncertainty and sensitivity analyses for these results.

## A Monte Carlo Simulation Model for Radionuclide Migration at the Repository Scale

F. Cadini(a), J. De Sanctis(a), T. Girotti(a) and E. Zio(a), A. Luce(b), A. Taglioni(b)
*a) Dipartimento di Energia - Politecnico di Milano, I-20133 Milan, Italy. b) ENEA CR Saluggia, Saluggia (VC), Italy*

The paper illustrates a Monte Carlo simulation-based compartment model in which detailed, local-scale modeling feeds a global-scale analysis of the repository, at reasonable computational expenses. An application to a realistic case study is presented to verify the feasibility of the approach. This work has been funded by the Ente per le Nuove Tecnologie, L'Energia e l'Ambiente (ENEA) within the Framework Program Agreement with the Italian Ministry of Economic Development for the research area N. 5.2.5.8 "NUOVO NUCLEARE DA FISSIONE".

## Comprehensive Consideration of Features, Events, and Processes (FEPs) for Repository Performance Assessments

Geoff Freeze and Peter Swift
*Sandia National Laboratories, Albuquerque, NM, USA*

The analysis of features, events, and processes (FEPs) is a common activity associated with the development of performance assessment (PA) models of radioactive waste repositories. FEP analysis supports: (1) the identification of a comprehensive list of potentially relevant FEPs, and (2) the screening of those potentially relevant FEPs to ensure that all important phenomena are implemented in the PA model analysis. FEP analysis is predicated on the assumption that the list of potentially relevant FEPs is truly comprehensive (i.e., have we thought of everything?). However, the comprehensiveness of a FEP list cannot be proven with absolute certainty. This paper describes a formal FEP analysis methodology of iterative and integrated FEP identification, FEP categorization, and review that be applied to provide confidence in, and support the demonstration of, comprehensiveness of a FEP list. A specific example from the Yucca Mountain Project (YMP) is presented to demonstrate the methodology.

# Friday Meeting-At-A Glance

| Room Session | Salon A | Salon B | Salon C | East Room | West Room | North Room | Municipal | Federal | Superior | South Room |
|---|---|---|---|---|---|---|---|---|---|---|
| 0730 - 0830 | **Continental Breakfast – Madison, Courtyard, and Compass Foyers** | | | | | | | | | **Exhibits tear-down throughout the day** |
| 0830 - 1000 | | | | | | | Medical 13-3: Risk Related Studies in Healthcare | Commercial 20-1: PSA Software | Commercial 20-2: PSA Tools | |
| 1000 - 1030 | ***End of Conference Meeting – Madison Ballroom*** | | | | | | | | | |
| 1030 - 1130 | ***Ice Cream Social – Madison Ballroom and Foyer*** | | | | | | | | | |
| Adjourn | | | | | | | | | | |

# Medical

**Friday, Municipal**

8:30 - 10:00 AM

## 13-3: Risk Related Studies in Healthcare

Session Chair: Robert Borotkanics

### What Can We Learn About Risks in Healthcare from an Aggregate Analysis of Multiple Risk Assessments?

Donna M. Woods(a), Jonathan Young(b), Jane L. Holl(a,c), Sally Reynolds(c), Robert Wears(d), Ellen Schwalenstocker(e), Jennifer Oelerich(b), Olivia Ross(a), Anna Torricelli(a)
*a) Institute for Healthcare Studies, Feinberg School of Medicine, Northwestern University; Chicago, IL; USA. b) Battelle Northwest Pacific Laboratory; Seattle, WA; USA. c) Children's Memorial Hospital; Chicago, IL; USA. d) University of Florida Shands Health System; Jacksonville, FL; USA. e) National Organization of Children's Hospitals and Related Institutions; Alexandria, VA USA*

Identification of specific paths for medical care risks is a challenge to patient safety improvement. Frequently safety vulnerabilities and risks that exist at one institution also exist at other institutions. These represent systemic fault-lines in the safety of healthcare. The objective of this study was to collect risk results were collected from across institutions and to identify generic healthcare risks to target for substantive patient safety improvement. The LEARN method was developed and applied to review (conduct a meta-analysis) of aggregated risk assessment results from multiple FMEA studies. Sixteen risk assessments were collected from different institutions across the United States. Over 400 failpoints are described. Of these, 296 had a risk priority number designating them as medium to high risk. High risk fail points (127) included: Communication, specimen collection and management, adequate clinical resources, patient identification. Clinician communication in the course of the provision of healthcare represented the largest pool of high-risk failure modes. Of the 212 failure modes causes described, four causes represent over 50%: Human error (17%); busy, distracted (16%); Inadequate procedures (9%); Lack of data/info (9%). The identified failure modes and failure mode causes from this analysis can become topics for attention for development of risk informed interventions and safe practice implementation.

### The State Of Risk Assessment in Healthcare

Donna M. Woods(a), Robin Sullivan(b), Jonathan Young(b), Jane L. Holl(c), Sally Reynolds(c), Robert Wears(d), Ellen Schwalenstocker(e), Jennifer Oelerich(b), Olivia Ross(a), Anna Torricelli(a)
*a) Institute for Healthcare Studies, Feinberg School of Medicine, Northwestern University; Chicago, IL; USA. b) Battelle Northwest Pacific Laboratory; Seattle, WA; USA. c) Children's Memorial Hospital; Chicago, IL; USA. d) University of Florida Shands Health System; Jacksonville, FL; USA. e) National Organization of Children's Hospitals and Related Institutions; Alexandria, VA; USA*

The Failure Mode Effects Analysis (FMEA) has experienced broad adoption in healthcare. Sixteen healthcare FMEA risk assessments were collected from institutions across the country. Criteria to assess these risk results was developed: Inclusion of a multi-disciplinary team; process flow, identified failure-modes, consequences, causes, controls/safeguards; consideration of more than one fail-point, cause, consequence including both omissions and commissions; cross study comparison of elements; frequency/consequence assessment validated with data. Numerous risks have been identified using FMEAs, however, the analyses of similar processes by different teams produced very different results. Failure-modes and causes described in one FMEA study may be overlooked or unspecified in another study of the same topic. Conducting a review across FMEAs not only captured common risks across the studies but provided a more comprehensive assessment of the pool of existing risks. In comparison with other high risk industries, healthcare is teeming with low and high impact risks - this is true for both the frequency and volume of potential failure modes. Still, at this stage in the use of FMEAs, there is evidence of truncation of inquiry in the specification of potential failures and causes. The criteria developed through this study can also be used prospectively in the form of a checklist to improve risk assessment results.

### On Modeling Risk of Adverse Events In Complex Healthcare Settings

Reza Kazemi(a), Ali Mosleh(a), and Meghan Dierks(c)
*a) University of Maryland College Park, MD. b) Harvard Medical School, Cambridge, MA*

Reports from various sources indicate that a substantial number of hospitalized patients suffer treatment caused injuries, while in the hospital. While risk can not be entirely eliminated from healthcare activities, our goal is to develop effective and durable mitigation strategies to render the system 'safer'. In order to do this, though, we must develop models that comprehensively and realistically characterize the risk. Despite the magnitude of the problem, current analysis of adverse events in healthcare settings continues emphasis on individual case studies. Efforts to understand the nature of aggregate risk through formal methods have been limited. This paper will report on results of a research aimed at developing and applying a generic methodology for assessing adverse event risk in acute care hospitals as s function of organizational factors non-organizational factors, using a combination of modeling formalisms. First, a system dynamics (SD) framework will be used to capture changes in the level of risk as a function of duration of hospital stay, complexity of the patient's condition, and constraints imposed by external agencies (e.g., insurers and regulatory/certification authorities) on operational decisions. Second, Bayesian Belief Networks (BBN) are applied to provide input to some of the 'soft' variable nodes, including organizational factors, human decision making and idiosyncratic patient responses to interventions.

### Method for the Elicitation of Cognitive Competencies for Disaster Nursing

Taro Kanno(a), Kimiko Hayano(b), Chie Ishida(c), Kayoko Kawahara(b), Chikako Kawahara(d), Mariko Ohara(e), Kazumi Sato(f) and Yuko Kuroda(g)
*a) The University of Tokyo, Tokyo, Japan. b) Tokyo Metropolitan University, Tokyo, Japan. c) Showa University, Kanagawa, Japan. d) Tokyo Medical University, Tokyo, Japan. e) The Japanese Red Cross College for Nursing, Japan. f) Ojiya General Hospital, Japan. g) NPO Hanshin Supporting Organization for Senior Citizen and the Disabled Person, Japan*

This paper proposes and examines a method to elicit cognitive competencies for disaster nursing based on the results of a content analysis of interview data. One aspect of the method focuses on cognitive process in terms of the transitions among the three primitive cognitive steps: "information (perception)", "decision", and "action". The other aspect uses a natural language processing technique and focuses on the targets of perception in disaster situations. This method was applied to the results of a content analysis of interviews with nurses who exhibited high performance in actual earthquake disasters. It was found that there were different cognitive patterns depending on the nursing tasks, but there were also some common characteristics found with respect to the objects of attention and concern among good performers. Cognitive competencies for the disaster nursing activities obtained in this study are summarized.

# Commercial

**Friday, Federal**

8:30 - 10:00 AM

## 20-1: PSA Software

Session Chairs: Woo-sik Jung

### Exchange of PSA Data and Models

Johan Sörman, Lars Lundstedt, and Pavel Krcal
*Scandpower – Lloyd´s Register, Stockholm, Sweden*

Most PSA software includes a text based export and import format that in most cases is unique for the software. There are also other formats that have ambitions of being universal for exchanging data and models between PSA tools. For what purposes are PSA models exported and imported to and from PSA software? For what applications are PSA data and models exported? What are the special considerations that have to be made when designing an import and export tool for PSA models? SETS and FTAP are text formats defined back in the eighties. They are still used, but mainly for benchmarking software solving fault tree models. These formats can be used for exporting and importing PSA model data to and from PSA software. They include data for basic events, gates, house events, reliability data, component data, etc. They also include information about fault tree logic. Under the IMdR (Institute pour la Maîtrise de Risque) Open PSA initiative a new format called The Open PSA Model Exchange Format (OPSAMEF) is being developed. The OPSAMEF is an XML format. The ambition is to have one format that the PSA community world-wide can agree upon. One initial idea has been that the OPSAMEF will include all data and logic in models stored in any of the major PSA tools available today. This will of course add new possibilities for the users, but it will also add significant problems with respect to quality assurance (error handling etc). What is an appropriate level of detail for an import format? When does the format itself become more important than the use of it?

### Standardized Models for Documenting, Reporting and Presenting Results in PSA

Johan Sörman, Ola Bäckström
*Scandpower-Lloyd's Register, Stockholm, Sweden*

Nuclear installation inspectorates and regulatory authorities responsible for overseeing and approving license for operation of nuclear installations require reports based on information from the Probabilistic Safety Assessment (PSA) in general and PSA result in particular. While some standards for reporting are less specific and does not give indications on the way the properties and results from the PSA should be reported in more detail, the interest for templates for filling out critical and essential information that could simplify and allow for more frequent reporting is increasing. Are we moving into an era with more standardised models for documenting, reporting and presenting results also in PSA? An example is the Swiss Federal Nuclear Safety inspectorate (ENSI) regulatory guidelines, ENSI-A05/e, issued March 2009. This guideline explains very clearly what is expected to be reported with regard to quantification and presentation of Level 1 and level 2 PSA results. A set of tables with predefined headers are listed. This makes it easier for utilities and regulator to report and review properties and results from the PSA. Some may argue that the PSA is very different for different type plants and therefore it is not possible to standardise the reporting format. Such an example is the requirements for the performance of PRAs for new non-Light Water Reactors and that there is a need for a technology neutral approach with regard to standards to address diverse non-LWR designs such as liquid metal and gas-cooled reactors. But the use of common formats for result presentation may be a key player in the strive of getting more comparable models and to harmonize the models and documentation of them. A standardized presentation could therefore be an advantage in the documentation. Standardized formats can also be an advantage from production point of view, since this will increase the use of tools for result documentation generation. In this paper one such tool, RiskSpectrum Doc, presents how the results required by HSK can be presented.

### RISKMAN®, Celebrating 20+ Years of Excellence!

Donald Wakefield, Steven Epstein, Yongjie Xiong, Kamyar Nouri
*ABS Consulting, Irvine, CA, USA*

RISKMAN® is a PC-based, general purpose, integrated tool for quantitative risk analysis. Initiated with software programs first developed for main frames, and with development supported by a user's group spanning three continents, the PC version of RISKMAN® now celebrates more than 20 years of risk-based applications. While mostly used in the nuclear power industry and related government organizations, RISKMAN® is also used in the offshore oil industry, marine industry, aerospace, and for specialty applications such as for assessing the risks associated with the excavation and destruction of abandoned chemical weapons.

### Software Tool-Based Human Reliability Analysis

Xuhong He(a), Hao Zheng(a), Johan Sörman(b) and Ola Bäckström(b)
*a) Scandpower Inc., Beijing, China. b) Scandpower AB, Stockholm, Sweden*

The practice of Human Reliability Analysis (HRA) shows that it can bring big uncertainties in risk quantification. A well-designed software tool could facilitate the HRA team to achieve good quality HRA with efficient resources. These advantages could not be achieved automatically from the software tool, rather good HRA practice coming from a qualified HRA team using a systematic process. This paper discusses what kind of roles a HRA software tool could play to assist the HRA analysis to meet the requirements, e.g. those from the ASME PSA Standards. This paper also introduces a HRA software tool called RiskSpectrum HRA developed by Scandpower. RiskSpectrum HRA is a standalone HRA program interfacing with RiskSpectrum PSA. It is hoped that by using RiskSpectrum HRA, HRA analysts can consistently conduct the proposed HRA analysis with good traceability and documentation.

# Commercial

**Friday, Superior**

8:30 - 10:00 AM

## 20-2: PSA Tools

Session Chair: James Knudsen

### Quantification of Conditional Probability for Triggering Events Using Fault Tree Approach

Shuwen (Eric) Wang(a), Ernie Kee(b), and Fatma Yilmaz(b)
*a) ABSG Consulting Inc. (ABS Consulting)Irvine, California USA. b) South Texas Project Nuclear Operating Company, Wadsworth, Texas USA*

The objective of this work is to develop a general method for quantifying the conditional probability that the plant is in any power reduction state (e.g., TRIP, 50% down power, etc.) given any triggering event. We developed an algorithm that utilizes the existing BOPPP model fault trees to quantify the conditional power reduction probabilities.

### Use of result processing, presentation of ideas behind RiskSpectrum Consequence Matrix

Ola Bäckström, Johan Sörman and Lars Lundstedt
*Scandpower-Lloyd's Register, Stockholm, Sweden*

If result and result treatment in the oil and gas industry is compared to the corresponding in the nuclear business it can be concluded that the oil and gas industry do more of result processing. This paper discusses how processing of the results within the PSA software could improve the useability of results within a PSA study, simplify and enhance ways of working and simplify updates of the documentation. The paper also discusses how the results from a PSA (or availability analysis) could be used for other purposes, like economic evaluation or third party impact. In a PSA you are obviously interested in the frequency for the unwanted state, e.g. when it comes to verification that the core damage frequency fulfills the requirement. But also in these cases you might want to process the information before graphs etc. are being compiled. Other types of applications are for example economic evaluations. And especially when the quantification is done in several steps and need several results from the PSA. This paper presents the background and the idea behind the design of RiskSpectrum Consequence Matrix.

### Validation Project for the Open-PSA Model Exchange Using RiskSpectrum® and CAFTA®

Steven Epstein(a), F. Mark Reinhart(b), and Antoine Rauzy(c)
*a) ABS Consulting, Yokohama, Japan. b) Vienna, Ausstria. c) Dassault Systemes, Paris, France*

Under the sponsorship of the Institut pour la Maîtrise des Risques (IMdR), and supported financially and technically by more than ten European and US organizations (see section 4), this validation project has been successfully completed with both RiskSpectrum®, from Relcon Scandpower and CAFTA®, from EPRI.

### A Declarative Approach for Risk Outage Management

Mohamed Hibti and Dominique Vasseur
*EDF R&D, Clamart, France*

In this paper, we present a declarative programming approach to deal with the problem of planning verification of maintenance operations in a Nuclear Power Plant. The idea is to avoid Fault Tree modeling which is not a very user-friendly model in terms of understanding and reviewing. An alternative is proposed based on a declarative approach, a better robustness and, consistency and interpretation of results. The safety (degradation) levels are computed using interactions between the impact of maintenance operations on the plant systems and the technical specifications requirements modeled as a set of relations between the components and the Safety Functions.

# Notes

# Notes

# Notes

# PSAM 10 Program/Proceedings CD-ROM

**About this CD-ROM**
The material in this CD-ROM was published using Adobe© technology.
Included on the CD-ROM are versions of Acrobat Reader for Microsoft© Windows™, Apple© Macintosh™ (Mac OS X), and Unix©

**Installation**
To view files on this CD-ROM you must have Adobe Reader installed on your hard drive. Installation instructions can be found in the README.TXT file.

**Getting Started**
Windows users: Software included in this CD-ROM should automatically launch the proceedings. You can always start viewing the content by opening the Start.pdf file provided Adobe Reader has been installed on your hard drive.
MacOS X and Unix users: To start open the Start.pdf file.

# PSAM 11
## ESREL 2012

www.psam11.org

11th International
Probabilistic Safety Assessment and
Management Conference

25–29 June 2012, Scandic Marina Congress Center
Helsinki, Finland

First announcement


**Conference Venue**
PSAM 11 & ESREL 2012 will be held at the Scandic Marina Congress Center by the seaside in downtown Helsinki. A number of hotel rooms will be available in the Scandic Grand Marina Hotel neighbouring the venue. Other affordable hotels will be available as well.

**Conference Secretariat**
CONGREX / Blue & White Conferences Oy
P.O. Box 81, FI-00371 Helsinki, Finland
Phone: +358 9 5607 500, fax: +358 9 5607 5020
Email: psam11@congrex.fi
Conference website: www.psam11.org

**Important Dates**

| | |
|---|---|
| Abstracts Submission Deadline | 17 June 2011 |
| Notification to Authors | 30 September 2011 |
| Full Paper Submission Deadline | 30 January 2012 |
| Early Registration Deadline | 30 March 2012 |
| Conference Dates | 25–29 June 2012 |

**Previous Conferences**

| | | |
|---|---|---|
| PSAM 1 | Beverly Hills, USA | 1991 |
| PSAM 2 | San Diego, USA | 1994 |
| PSAM 3 & ESREL '96 | Crete, Greece | 1996 |
| PSAM 4 | New York, USA | 1998 |
| PSAM 5 | Osaka, Japan | 2000 |
| PSAM 6 | San Juan, Puerto Rico | 2002 |
| PSAM 7 & ESREL '04 | Berlin, Germany | 2004 |
| PSAM 8 | New Orleans, USA | 2006 |
| PSAM 9 | Hong Kong, China | 2008 |
| PSAM 10 | Seattle, USA | 2010 |

Helsinki – Friendly. Northern. Compact. Surrounded by sea. The exotic East meets Scandinavian Simplicity. See you in Helsinki, World Design Capital 2012! More information on the sights, museums, restaurants etc. www.visithelsinki.fi

PHOTOS: Helsingin kaupungin kuvapankki / Paul Williams, Helsingin kaupungin kuvapankki / Comma Image Oy

## Welcome to the Conference

PSAM 11 will be the major international event in Probabilistic Safety Assessment in 2012. The Conference brings together experts from various industries, research organisations, regulatory authorities and universities. It offers a platform for contacts between different fields from nuclear, process and chemical industries, off-shore and marine, space and aviation, IT and telecommunications, bio and medical technology, civil engineering and financial management. The multidisciplinary Conference is aimed to ensure the cross-fertilization of methods, technologies and ideas.

The PSAM 11 program is a perfect blend of ESREL–PSAM traditions and Nordic Footprints in the safety assessment including a special emphasis of non-nuclear technologies.

Additional information on the conference website **www.psam11.org**

## Contact Information

**Conference General Chair**
Reino Virolainen
Radiation and Nuclear Safety Authority (STUK)
P.O. Box 14, FI-00881 Helsinki, Finland
Phone: +358 9 75988 362
Email: psam11@stuk.fi

**Program Committee Chair**
Terje Aven
University of Stavanger
N-4036 Stavanger, Norway
Phone: +47 51 83 22 67
Email: terje.aven@uis.no

**Local Organizing Committee**
Reino Virolainen (STUK)
Kalle Jänkälä (Fortum)
Risto Himanen (TVO)
Jan-Erik Holmberg (VTT)
Ari Julin (STUK)
Pekka Pyy (TVO)
Veikko Rouhiainen (VTT)
Ilkka Niemelä (STUK)
Matti Lehto (STUK)
Kaisa Simola (VTT)
Ahti Salo (Aalto University)
Harri Koskinen (Finnair)

## Technical Disciplines

- Consequence Modeling and Management
- Digital I&C and Software Reliability
- Enterprise risk management
- Environmental Impact Assessment
- Fire Simulation and Analysis
- Human Reliability Analysis
- Industrial Safety and Accident Analysis
- Lifetime and Ageing Management
- Maintenance Modelling and Optimisation
- Non-probabilistic/soft methods in reliability analysis
- Occupational Safety
- Operational Experience and Data Analysis
- Phenomena Modeling
- Policy Making and Legislative Issues
- Reliability Analysis and Risk Assessment Methods
- Risk and Hazard Analyses
- Risk Governance and societal safety
- Risk Informed Applications
- Risk Informed Licensing and Regulation
- Risk Management in Large Projects
- Risk Perception and Communication
- Safety Assessment Software and Tools
- Safety Culture and Human & Organizational Factors
- Safety integrity level (SIL)
- Safety Management and Decision Making
- Structural Reliability Analysis Methods
- Uncertainty and Sensitivity Analysis, Bayesian methods

## Industrial & Service Sector

- Automotive Engineering
- Aviation and Space
- Biotechnology and Food Industry
- Chemical and Processing Industry
- Civil Engineering
- Crisis and Emergency Management
- Electrical and Electronic Engineering
- Energy Production and Distribution
- Environment and Sustainable Development
- External Hazards and Climate Risks
- Health and Medicine
- Information Security
- Infrastructures
- Insurance and Finance
- IT and Telecommunications
- Manufacturing and Mechanical Systems
- Marine Engineering
- Nanotechnology
- Nuclear Engineering
- Offshore Oil and Gas
- Public Planning and Policy Decisions
- Security and Defense
- Training and Education
- Transportation
- Waste Management