Consequence Modeling and Management

Monday 6/23/2014 10:30 Honolulu

Chair:

4 Nuclear Refugees After Large Early Radioactive Releases
Ludivine Pasucci-Cahen
Institut de Radioprotection et de Sûreté Nucléaire, Fontenay-aux-Roses, France
However improbable, large early radioactive releases from a nuclear power plant would entail major consequences for the surrounding population. In Fukushima, 80,000 people had to evacuate the most contaminated areas around the NPP for a prolonged period of time. Had they remained where they lived, they would have received doses dangerous for their health in the long run. These people have been called “nuclear refugees”.

The paper first argues that the number of nuclear refugees is a better measure of the severity of radiological consequences than the number of fatalities, although the latter is widely used to assess other catastrophic events such as earthquakes or tsunamis. It is a valuable partial indicator in the context of comprehensive studies of overall consequences.

Section 2 makes a clear distinction between long-term relocation and emergency evacuation and proposes a method to estimate the number of refugees.

Section 3 examines the distribution of nuclear refugees with respect to weather and release site. The distribution is asymmetric and fat-tailed: unfavorable weather can lead to the contamination of large areas of land; large cities have in turn a higher chance of being contaminated. Variability with respect to site is quite intuitive; however, results show that simulations are far superior to an approach based on population living within 20 or 30 km around the site.

73 Multidimensional Risk Evaluation: Assigning Priorities for Actions on a Natural Gas Pipeline
Mônica Frank Marsaro, Marcelo Hazin Alencar, Adiel Teixeira de Almeida, and Cristiano Alexandre Virgínio Cavalcante
Universidade Federal de Pernambuco, UFPE, Recife, Brazil
This paper presents a multicriteria decision model application to define actions with a view to mitigating the risks involved in this mode of transportation. Natural gas is a fossil fuel that is important for society and is transported through pipelines. It is used for different purposes in industrial and civil applications. Although pipelines are one of the safest transport systems, some accidents involving natural gas have occurred. The Multicriteria decision model described in this paper is put forward as a means to minimize such possibilities. It incorporates MAUT (Multi-attribute Utility Theory), which considers a decision maker’s preferences and some aspects of the Decision Theory approach. Three dimensions of risk, namely the human, financial and environmental ones - are targeted in the context of probabilistic consequences. As an important result, the information obtained from the model is shown to be important in order to define how resources should best be allocated and to establish maintenance policies for managing and mitigating risk.

100 Development of Accident Consequence Assessment Scheme using Accident Cost and Consideration of Decontamination Model
Kampanart Silva (a), Koji Okamoto (b), Yuki Ishiwatari (b,c) Shogo Takahara (d) and Jiraporn Promping (a)
(a) Thailand Institute of Nuclear Technology, Nakhon Nayok, Thailand, b) The University of Tokyo, Tokyo, Japan, c) Hitachi-GE Nuclear Energy, Ltd., Ibaraki, Japan, d) Japan Atomic Energy Agency, Ibaraki, Japan
Severe accident at nuclear power plants, including the Fukushima accident in March 2011, wreak various kinds of consequences, including health effects, economic, social and environmental impacts. The authors developed the scheme of the accident consequence assessment using “accident cost”, aiming for it to be an index that is as comprehensive as possible. Normalized accident costs of all accident sequences along with their breakdowns, and the breakdown of the average accident cost are presented. The radiation effect cost, the decontamination cost and the relocation cost are the three major components that dominate the accident cost. The decontamination model was reconsidered since decontamination effects were taken into account by very simple assumptions and decontamination cost was estimated by a rough calculation scheme in the former model. 99 decontamination-related parameters were selected and the model is formed. A sensitivity analysis was performed to identify parameters with large influence on accident cost calculation and large extent of interactions with other parameters. Parameters with high importance tend to have large extent of interactions with other parameters. Parameters influential to accident cost, e.g., the dose of setting decontamination target area, a number of waste management-related parameters, are identified.

118 Safety of LPG Rail Transportation: Influence of Safety Barriers
V. Busini, M. Derudi, R. Rota
Politecnico di Milano, Department of Chemistry, Materials and Chemical Engineering “G. Natta”, Piazza Leonardo da Vinci 32, 20133 Milano, Italy
The risk due to the road and rail transportation of liquefied petroleum gas (LPG) is well known. Severe scenarios were caused by road or rail accidents involving LPG pressurized tank cars. Consolidated approaches exist for the analysis, the prevention and the mitigation of risk due to the transportation of hazardous materials (HazMat) by road or rail. In Europe a specific regulation applies to the use of the transport of HazMat and specific regulations apply to the qualification of equipment used for LPG transportation. Nevertheless, on June 29th, 2009, an extremely severe transportation accident involving LPG took place in the station of Viareggio, in Italy. A train carrying 14 tank cars of LPG derailed and several railcars overturned on the shunts in the Viareggio station. A tank was punctured, releasing its entire content that ignited causing an extended and severe flash-fire. The present study focused on the study of the effect of different parameters on the heavy gas cloud dispersion resulting from the accident, such as meteorological parameters and height of safety walls. It was found that, to be effective, the mitigation barriers must be carefully designed, with particular reference to their height with respect to the height of the heavy gas cloud.

169 Determination of Target Reliability Levels Based on Value to the Customer and Warranty Budgets
Michael Bartholdt, Volker Schweizer and Bernd Bertsche
University of Stuttgart, Stuttgart, Germany
The method presented here serves to determine the system’s as well as subsystems’ target reliability levels combined. It centers the functions of the product to be achieved and known to weight requirements in line with the voice of the customer. Each subsystem’s target reliability level is defined in accordance with its quantitative contribution to fulfilling the functions as desired by the customer. Statistically inevitable failures before the targeted product lifetime are often compensated by warranty and good-will expenditures. These costs are methodologically broken down and allocated to each subsystem purposefully in order to achieve the utmost customer satisfaction. By bringing together such costs per subsystem and its importance to the customer, reliability goals are obtained aligned with the value to the customer.

In contrast to most of the existing methods to define and allocate reliability goals (typically realized by two different methods), subsystem target reliability levels are defined at first. The system’s reliability goal is then calculated by means of Boole-theory. Arbitrarily complex systems can be analyzed.
How to Integrate Correctly Hardware Common Cause Failures in Frequency Calculations?

Hervé Brunelière, Monica Rath, and Wenjie Qin
AREVA NP SAS, Paris La Défense, France

Hardware common cause failures are generally the highest contributors in the I&C systems reliability and availability studies. Comparisons of such results from calculations of frequency of spurious actuations by a safety system or frequency of failures of a control system with operation feedback of such failures show that the frequency calculations are often overestimated. This is due to the use of «classic» common cause failure parameters. This is mainly explained by the fact that, for these undesired events, failures are generally not hidden ones and are then detected within few hours. Then, for common cause failures that are not simultaneous, the first failure is often repaired before the second one appears. This over conservatism can lead to inappropriate design choices like addition of redundancies or interlocks to minimize the frequency of an undesired event based on a calculation that does not reflect the real situation. This is then a concern for a designer and for a utility to limit as far as possible the impact of this over conservatism.

One solution is to consider only independent failures in frequency calculations. In this case, the result is underestimated as simultaneous common cause failures that are possible and credible are not considered in the result. Then, the risk is not to implement some necessary measures in the design due to over optimistic results. The paper will discuss possible solutions to handle these types of failures in calculations based on real cases. Illustrations will be based on a typical architecture of an I&C system based on Teleperm XS platform similar to the ones currently implemented in nuclear power plants. The paper will also integrate discussions on relevance of the different methodologies including no consideration of CCF at all, degraded CCF factors values and possibilities of extrapolation. These methodologies will be compared based on their impact on calculation results and the consistency with operational experience.

The Basic Idea of Quantitative Model of Reactor Protection System Considering Stochastic Process

Hitohshi Muta
Tokyo City University, Tokyo, Japan

In nuclear power plants such as ABWR and the latest PWR, digital instrumentation and control system have been installed increasingly to reactor emergency shutdown system which is one of the important safety functions. However, it has been found that it is difficult to model the digital equipment reliability in probabilistic risk assessment (PRA). And some of issues such as taxonomies of failure modes have been studied in the international framework, OECD/NEA/WGRisk task group called DIGREL.

In this paper, the reactor trip actuation failure event logics and frequencies resulting from the multiple failures and the demand following the initiating event are analyzed qualitatively and quantitatively. This paper presents the example of the reliability analysis of the digital Reactor Protection System (RPS) considering stochastic process, the approach given by this paper will be applicable to establish the PRA model of digital RPS of the actual nuclear power plant.


Hai Tang, Lixuan Lu
University of Ontario Institute of Technology, Oshawa, ON, Canada

Most of today’s Safety Instrumented Systems (SIS) are hardware and software integrated systems. In these systems, failures can occur in both hardware and software. Hardware failures and their effects have been studied extensively in the literature. However, the methods and results dealing with hardware failure are not directly applicable for software reliability modeling, due to the nature of difference between hardware and software. This is especially of concern when the SIS is used for safety critical applications. In this paper, a hardware and software integrated reliability model is proposed to model the reliability of the integrated system. The requirement on software reliability is then determined based on the hardware reliability and the requirement on the Safety Integrity Level (SIL) of the integrated system. Following this, a Bayesian stopping rule is used to determine the minimal number of successful software runs, in order to provide a certain level of confidence that the reliability requirement on the software is achieved.

OEC/D/NEA WGRISK task on failure modes taxonomy for digital I&C – DIGREL

Abdallah Amri (a), Stefan Authén (b), Hervé Bruneliere (c), Gilles Deleuze (d), Gabriel Georgescu (e), Jan-Erik Holmberg (f), Man Cheol Kim (g), Keisuke Kondo (h), Ming Li (i), Ewgenij Piljugin (j), Wietse Postma (k), Jiří Sedlak (l), Carol Smidts (m), and Nguyen Thuy (n)


The OECD/NEA CSNI Working Group on Risk Assessment (WGRisk) has set up a task group called DIGREL to develop a taxonomy of failure modes of digital components for the purposes of probabilistic risk analysis (PRA). The failure modes taxonomy is based on a failure propagation model and a definition of five levels of abstraction: 1) system level, 2) division level, 3) I&C unit level, 4) I&C unit modules level, 5) basic components level. This structure corresponds to a typical reactor protection system architecture. The failure propagation model consists of the following elements: fault location, failure mode, uncovering situation, failure effect and the end effect. These concepts are applied to define the relationship between a fault in hardware or software modules (module level failure modes) and the effect on I&C units (I&C unit level failure modes). The purpose of the taxonomy is to support PRA, and therefore focuses on high level functional aspects rather than low level structural aspects. This focus allows handling of the variability of failure modes and mechanisms of I&C components. It reduces the difficulties associated with the complex structural aspects of software in redundant distributed systems.

A Component-based Approach for Assessing Reliability of Compound Software

Monica Lind Kristiansen (a), Bent Natvig (b), and Harald Holone (c)

a) Department of Informatics, Østfold University College, Halden, Norway, b) Department of Mathematics, University of Oslo, Oslo, Norway, c) Department of Informatics, Østfold University College, Halden, Norway

Predicting the reliability of software systems based on a component approach is inherently difficult, in particular due to failure dependencies between the software components. This paper describes a component-based approach for assessing reliability of compound software, where failure dependencies between software components are explicitly addressed. This is done by finding accepted upper bounds for probabilities that pairs of software components fail simultaneously and then by including these into the reliability models. To find these accepted upper bounds, the approach applies principles of Bayesian hypothesis testing on simultaneous failure probabilities. In addition, the restrictions imposed on the simultaneous reliabilities and failure probabilities by the marginal reliabilities and failure probabilities are taken into account. To illustrate the approach, we use an example based on mobile positioning systems for backtracking. This is for instance used to help people with dementia to find their way home if they get lost.
Enterprise Risk Management

Monday 6/23/2014 10:30 Oahu
Chair: David Johnson, ABS Consulting

161 Automated Evolutionary Restructuring of Workflows to Minimise Errors Via Stochastic Model Checking
Luke Thomas Herbert (a), Zaza Nadja Lee Hansen and Peter Jacobsen (b)
a) DTU Compute, Lyngby, Denmark, b) DTU Management, Lyngby, Denmark

This paper presents a framework for the automated restructuring of workflows that allows one to minimise the impact of errors on a production workflow. The framework allows for the modelling of workflows by means of a formalised subset of the Business Process Modelling and Notation (BPMN) language, a well-established visual language for modelling workflows in a business context. The framework’s modelling language is extended to include the tracking of real-valued quantities associated with the process (such as time, cost, temperature). In addition, this language also allows for an intention preserving stochastic semantics able to model both probabilistic- or non-deterministic branching behaviour. We further extend this formalism to allow for the introduction of error states which allow for both fail-stop behaviour and continued system execution. We explore the practical utility of this approach by means of a case study from the food industry. Through this case study we explore the extent to which production faults can be reduced and the impact of these can be minimised, primarily through restructuring of the production workflows. This approach is fully automated and only the modelling of the production workflows and the expression of the goals require manual input.

384 Enterprise Risk and Opportunity Management for Nonprofit Organizations and Research Institutions
Allan Benjamin (a), Homayoon Dezfuli (b), Chris Everett (c), Julie Pollitt (d), Dev Sen (c)
a) Independent Consultant, Albuquerque, NM, USA, b) Office of Safety & Mission Assurance, NASA Headquarters, Washington, DC, USA, c) Information Systems Laboratories, Inc., Rockville, MD, USA

Enterprise risk and opportunity management (EROM) concerns the means by which organizations develop and implement their strategic goals through a portfolio of programs, projects, institutional assets, and activities. The overall objective of EROM is to reach an optimal balance between minimizing the potential for loss (risk) while maximizing the potential for gain (opportunity). The focus of this paper is on the development of guiding principles and an overall approach that serves the interests of technically oriented nonprofit organizations and research institutions. These interests tend to place emphasis on performing services and achieving technical gains more than on achieving specific financial goals, which is the province of commercial enterprises. In addition, the objectives of nonprofit organizations may extend to institutional development and maintenance, financial health, legal and reputational protection, education and partnerships, and mandated milestone achievements. This paper discusses the philosophical underpinnings of EROM in the context of nonprofit organizations, the integration of EROM with existing management processes, and the nature of the activities that are performed to implement EROM within this context.

589 Programmatic Assessment of RG-MOX Utilization Following Participation in the DOE Surplus Plutonium Disposition Program
David H. Johnson, Andrew A. Dykes (a), Andrew G. Sowder, and Albert J. Machiels (b)
a) ABSG Consulting, Irvine, CA, USA, b) Electric Power Research Institute (EPRI), Charlotte, NC, USA

EPRI is building a suite of tools for assessing nuclear fuel cycle options based on a platform of software, simplified relationships, and explicit decision-making and evaluation guidelines. This paper summarizes an example of an assessment from a utility perspective regarding continuing MOX utilization with commercial reactor-grade mixed-oxide fuel (RG-MOX) following successful utilization participation in the DOE Surplus Plutonium Disposition Program. This assessment reflects potential opportunities and problems based on topic familiarity and the perspective embedded in the scenario definition, as follows: (1) economic considerations will represent a primary driver for utilities operating in the U.S. commercial environment, and (2) back-end management issues must be flagged due to the number and magnitude of constraints in used-fuel management at U.S. nuclear plants for both wet and dry storage (and the important interface between them). While economic considerations are seen as the primary utility decision drivers with respect to RG-MOX use under the stylized conditions defined here, this assessment also showed that technical waste management issues could be showstoppers if not adequately resolved.

358 A Jointly Optimization of Production, Delivery and Maintenance Planning for Multi-Warehouse/ Multi-Delivery Problem
Hajej Zied, Turki Sadok, and Rezg Nidhal
LGIPM-University of Lorraine, Metz, France

This paper develops a jointly optimization problem in order to establish an optimal production, delivery and maintenance strategy for a manufacturing system subjected to a random failure. The problem consists on several warehouses allow to satisfy random demands during a finite horizon, under service level. In order to assure an economical objective, we have determined the optimal production/maintenance plan and the economically delivery quantities plan considering the delivery time for each warehouse. The aim of the proposed approach is to show a jointly production/maintenance/delivery optimization, with a constrained stochastic production-delivery-maintenance planning problem under hypotheses of service level, delivery time for each warehouse and failure rate, which minimizes the total production, inventory, delivery and maintenance costs. A numerical example confirms the analytical results.

135 Investigating the Role of Statistical Models in Water Distribution Asset Management: A Semi-structured Interview Approach
Vikram M. Rao, and Roayce A. Francis
The George Washington University, Washington DC, USA

A robust asset management plan needs to be in place for water utilities to effectively manage their distribution systems. Of concern to utilities are broken pipes, which can lead to bacteria entering the water system and causing illness to consumers. Typically, water utilities allocate a portion of funds every year for renewal of pipes and valves. However, pipe renewal is largely based on replacing current broken pipes, and long-term asset management planning to replace pipes is not a priority for water utilities. Water utilities are beginning to use probabilistic break models and other statistical tools to predict pipe failures. These models incorporate variables such as pipe length, diameter, age, and material. These models are emerging in the water industry; however, their direct impact on long term asset planning remains to be seen. In addition, the effectiveness of these models is questionable, as there is currently little research done to evaluate the ability of these models to assist in asset management planning. This paper discusses the role of probabilistic pipe break models in structuring long-term asset management decisions. We determine that there are many factors that are needed to contribute to the feasibility of statistical models in a water asset management program, including data availability, funds, and shared information.
**Environmental Modeling**

**Monday 6/23/2014 10:30 Waialua**

Chair: Stefan Hirschberg, Paul Scherrer Institut

189 **Modeling of Pollutant Dispersion in Street Canyon by Means of CFD**

Davide Meschini, Valentina Busini (a), Sjoerd W. van Ratingen (b), Renato Rota (a)

*a) Department of Chemistry, Materials and Chemical Engineering “G. Natta”, Politecnico di Milano, Italy, b) TNO, Utrecht, Netherlands*

Nowadays, pollution from traffic remains one of the major sources for contamination in urban areas and it is widely known that substances emitted by vehicles represent a serious hazard to human health; some traffic-related pollutants, such as NO, NOx and CO are responsible for both acute and chronic effects on human health. This is often the case near busy traffic axis in city centers or street canyons. Purpose of this work is to validate the CFD model predictions against the field measurements of pollutants dispersion in an actual urban environment: Göttinger Strasse, Hanover, Germany. In the location, the population exposure to traffic-related pollution is expected to be high. Steady-state simulations have been performed for 18 different wind directions, with an increment of 20°, in order to cover the whole wind rose. A grid and a Schmidt number sensitivity analysis have been carried out in order to determine both the most suitable resolution of the computational geometry and the most suitable parameter to model the turbulence conditions in the street canyon. All CFD simulations have been performed for neutral atmospheric conditions and have been carried out with the CFD code FLUENT 12.1.

221 **Consideration on the Assessment of the Environmental Consequences and Impacts During Transport of Radioactive Materials (RAM)-A Safety Case**

Gheorghe Vieru

AREN, Bucharest, ROMANIA

The transport of Dangerous Goods-Class #7 Radioactive Material (RAM), is an important part of the Romanian Radioactive Material Management. The overall aim of this activity is for enhancing operational safety and security measures during the transport of the radioactive materials, in order to ensure the protection of the people and the environment. The paper will present an overall of the safety and security measures recommended and implemented during transportation of RAM in Romania. Some aspects on the potential threat environment will be also approached with special referring to the low level radioactive material (waste) and NORM transportation either by road or by rail. A special attention is given to the assessment and evaluation of the possible radiological consequences due to RAM transportation. The paper is a part of the IAEA’s Vienna Scientific Research Contract on the State Management of Nuclear Security Regime (Framework) concluded with the Institute for Nuclear Research, Romania, where the author is the CSI (Chief Scientific Investigator).

546 **Health Effects of Technologies for Power Generation: Contributions from Normal Operation, Severe Accidents and Terrorist Threat**

S. Hirschberg, C. Bauer, P. Burgherr (a), E. Cazzoli (b), T. Heck, M. Spada and K. Treyer (a)

*a) Paul Scherrer Institute, Laboratory for Energy Systems Analysis, Villigen, Switzerland, b) Cazzoli Consulting, Villigen, Switzerland*

As a part of comprehensive analysis of current and future energy systems we carried out numerous analyses of health effects of a wide spectrum of electricity supply technologies including advanced ones, operating in various countries under different conditions. The scope of the analysis covers full energy chains, i.e. fossil, nuclear and renewable power plants and the various stages of fuel cycles. State-of-the-art methods are used for the estimation of health effects. This paper addresses health effects in terms of reduced life expectancy in the context of normal operation as well as fatalities resulting from severe accidents and potential terrorist attacks. Based on the numerical results and identified patterns a comparative perspective on health effects associated with various electricity generation technologies and fuel cycles is provided. In particular the estimates of health risks from normal operation can be compared with those resulting from severe accidents and hypothetical terrorist attacks. A novel approach to the analysis of terrorist threat against energy infrastructure was developed, implemented and applied to selected energy facilities in various locations. Finally, major limitations of the current approach are identified and recommendations for further work are given.

249 **Metal Remediation of Acid Mine Drainage Using a Hybrid System of Microalgae Reactor**

Young-Tae Park, Hongkyun Lee, Hyun-Shik Yun, Jaeyoung Choi

Korea Institute of Science and Technology- Gangneung Institute, Gangneung, South Korea

Acid mine drainage (AMD) contains high concentrations of heavy metals and has become a serious environmental problem. A pipes inserted microalgae reactor (PIMR) was constructed to cultivate microalgae and purify AMD. The effects of metal concentration, pH and sulfate after pretreatment on the removal of iron and microalgae growth were investigated. Batch studies showed that PIMR and microalgae can adsorb iron with an uptake of 63.21 ± 9.8 mg/L iron. Microalgae growth was measured by optical density (OD) and dry cell weight (DCW); OD and DCW were 3.96 and 1.54 g/L respectively. Continuous studies also proved that PIMR can be used for metal remediation and microalgae cultivation.

**Fire Modeling and Simulation**

**Monday 6/23/2014 10:30 Waianae**

Chair:  

155 **Experiences from Developing and Implementing Shutdown Fire PRA at Forsmark NPP**

Erik Cederhorn, Maria Frisk

Risk Pilot AB, Stockholm, Sweden

The cold shutdown mode has earlier been considered as a safe mode without a significant risk for a major accident. However during the last few decades knowledge has improved regarding risks during shutdown mode. Many activities are on-going during this period and the risk of fire occurrence may be affected. Due to an increased number of plant activities the integrity of the fire compartments may not be intact and this could lead to more extensive fire spreading. At the same time important barriers may be unavailable due to maintenance and a fire event could become critical. Time available for recoveries before fuel is exposed in the reactor pressure vessel after an initiating event i.e. fire event, which results in loss of residual heat removal, is in many cases significantly longer than 24 hours. Area event analyses for shutdown mode generally tend to produce quite conservative results, which is why efforts have been made to increase realism in the analyses by using of improved methods. In order to increase realism dependencies between plant risk and maintenance activities, i.e. different combinations of safety system alignments, during the shutdown period have been studied in detail. This has had an impact on the estimation of both fire ignition frequencies and probabilities for fire spreading between different compartments.

This paper will discuss the methodology applied to the fire PRA at Forsmark NPP during the cold shutdown period, with focus on fire frequency analysis and fire scenario analysis. The implementation of fire analysis in the PRA and lessons learned from this will also be addressed.
Modeling and Quantification of Team Performance in Human Reliability Analysis for Probabilistic Risk Assessment

Jeffrey C. Joe and Ronald L. Boring
Idaho National Laboratory, Idaho Falls, USA

Probabilistic Risk Assessment (PRA) and Human Reliability Analysis (HRA) are important technical contributions to the United States (U.S.) Nuclear Regulatory Commission’s (NRC) risk informed and performance based approach to regulating U.S. commercial nuclear activities. Furthermore, all currently operating commercial nuclear power plants (NPPs) in the U.S. are required by federal regulation to be staffed with crews of operators. Yet, aspects of team performance are underspecified in most HRA methods that are widely used in the nuclear industry. Furthermore, there are a variety of “emergent” team cognition and teamwork errors (e.g., communication errors) that are 1) distinct from individual human errors, and 2) important to understand from a PRA perspective. The lack of robust models or quantification of team performance is an issue that affects the accuracy and validity of HRA methods and models, leading to significant uncertainty in estimating human error probabilities (HEPs). This paper describes research that has the objective to model and quantify team dynamics and teamwork within NPP control room crews for risk informed applications, thereby improving the technical basis of HRA, which improves the risk-informed approach the NRC uses to regulate the U.S. commercial nuclear industry.
97 Study on Analysis Method of Operator’s Errors of Situation Awareness in Digitized Main Control Rooms of Nuclear Power Plants
Pengcheng Li (a), Li Zhang (a,b), Licao Dai, Jianjun Jiang, and Difan Luo (a)
a) Human Factor Institute, University of south China, Hengyang, People’s Republic of China, b) Hunan Institute of Technology, Hengyang, People’s Republic of China

Situation awareness (SA) is a key element that impacts operator’s decision-making and performance in nuclear power plants (NPPs). The subsequent complex cognitive activities can not be correctly completed due to errors of situation awareness (ESA), which will lead to disastrous consequences. In order to investigate and analyze operator’s situation awareness error in digitized main control room (DMCR) of the nuclear power plants, the model of ESA is established, the classification system of SAE is developed based on the built SAE model, and the method of ESA is also constructed on the basis of the observation of simulator and operator surveys. Finally, a case study is provided to illustrate the concrete application of the method. It provides a theoretical and practical support for the operator’s SAE analysis in the digitized main control room of nuclear power plants.

136 Study on Human Errors in DCS of a Nuclear Power Plant
Licao Dai (a), Li Zhang (b), Pengcheng Li (a), Hong Hu (b) Yanhua Zou (b)
a) Human Factor Institute, University of South China, Hengyang, P.R.China, b) Hunan Institute of Technology, Hengyang, P.R.China China

More and more main control rooms in advanced nuclear power plants (NPP) use computer-based displays and controls, which are called digital control systems (DCS). DCS changes some technological aspects in a NPP control room, including information display systems, alarm systems, controllers and components and computer-based procedure systems. These changes on man-machine interface (MMI) alter the ways of operators acquiring information and controlling the system and thus give rise to new human error issue. In order to investigate the impact of the new MMI on human reliability, the researchers conducted a study in a reference plant with DCS. The practical operation data as well as the experimental data were acquired to study the causes, effects and recovery factors of the new human errors. The research makes an effort on providing a foundation for human error prevention in a DCS and human reliability analysis.

167 Experience Feedback from Fukushima towards Human Reliability Analysis for Level 2 Probabilistic Safety Assessments
V. Fauchille, H. Bonneville, J.Y. Maguer
Institut de Radioprotection et de Sûreté Nucléaire, Fontenay-aux-Roses Cedex, FRANCE

In the years 2000, the IRSN developed its first level 2 Probabilistic Safety Assessment (PSA) for the 900 MWe French PWRs. It was an ambitious project and one of the important tasks was to build a Human Reliability Analysis (HRA) model able to model the human actions to be implemented after the core melted. These actions are performed by operators in the main control room or by field operators outside but most of the decisions are taken, on the basis of the Severe Accident Management Guide (SAMG), by the crisis organization. A Human and Organizational Reliability Analysis in Accident Management (HORAAM) model is born from this enterprise. It is based on the “Decision Tree method”. HORAAM has been developed from the observation of the nuclear crisis exercises that are regularly practiced in France. Several influence factors which particularly affect human and organizational reliability in such a situation were identified. Currently HORAAM is used at IRSN but it has never been compared to the experience feedback of a real accident. After the Fukushima accident, IRSN conducted a study to confront HORAAM with the difficulties encountered to implement actions after the core meltdown. The purpose of this article is to present the main conclusions drawn from this study.

M07 Industrial Safety and Accident Analysis I

Monday 6/23/2014 10:30 Kona
Chair: Thor Myklebust, SINTEF

8 The Impacts of Supervisor Attributes and Supervision-Related Policies on Safety and Environmental Outcomes and Reporting Behavior
Christopher J. Jablonowski (a), John J. Tolle (b)
a) Shell Exploration and Production Company, Houston, TX, U.S.A, b) Value Discovery LLC, Houston, TX, U.S.A

This paper specifies detection-controlled regression models to investigate the drivers of health, safety, and environmental (HSE) performance and reporting behavior. The analysis confirms some results from previous research and also tests new hypotheses, with emphasis on supervision-related practices and policies. Most of the results are general and thus applicable to other regions, to other operators, and very likely to other industrial sectors. The results can be used to drive decisions regarding operating practices and HSE management system policy.

17 Change Impact Analysis as Required by Safety Standards, What to Do?
Thor Myklebust (a), Tor Stålhane (b), Geir Kjetil Hanssen, and Børge Haugset (a)
a) SINTEF ICT, b) ILI NTNU

Change Impact Analysis related to safety of products and systems is used by companies in many industries and is required by several standards. The International Electrotechnical Commission (IEC) has issued several standards with requirements and guidelines for the establishment of analysis like FMECA (IEC 60812), FTA (IEC 61025), Design review (IEC 61160), HAZOP (IEC 61882), Markov (IEC 61615) and RBD (IEC 61078) but no standard for Change Impact Analysis. Based on the aforementioned standards, a literature study and experience from several projects, this paper proposes a Change Impact Analysis Report adapted to the specific characteristics of the Railway and Process industry domains. The purpose of this paper is to serve as a tool to aid manufacturers in performing a Change Impact Analysis at the appropriate level which will be approved by assessors and certification bodies. This is important since the Change Impact Analysis report is one of the main inputs to the assessor/certification body.

The paper starts by presenting and clarifying relevant terms and definitions, as these differ from standard to standard. The main part of the paper structures and describes the relevant topics for a Change Impact analysis report. Using the described approach will save time and cost and reduce the risk of having to re-issue the Change Impact analysis, thus ending up with a product having hidden defects. Using the mindset from SafeScrum - a method that introduces elements from agile into safety-related software development, will result in further savings.

This work is part of a series of Railway and IEC 61508 certification projects and the SUSS2 Research projects.
The two methods, namely STEP and CAST, are based on different assumptions of accident causation and highlights different mechanisms that contributed to the evolving risk of the plant. Our understanding of the underlying mechanisms for the degradation of systems, although far from perfect, is improving with time. The identification of unanticipated degradation mechanisms. A case study is described involving a potential bypass accident sequence involving the progression of flow-related failures. Surveillance data is used to guide the plant’s preventative maintenance and surveillance programs. In general, however, these data are not used to characterize the evolving risk of the plant. Our understanding of the underlying mechanisms for the degradation of systems, although far from perfect, is improving with time. The possibility of developing a condition-dependent PRA is explored that would take a first principles approach to modeling the progression of degradation mechanisms, periodically adapting the model to account for surveillance results, and using the model as a basis for a time-dependent characterization of plant-specific risk. Because surveillance data would be used to periodically assess the consistency of the observed behavior with model predictions, it might be possible to provide early identification of unanticipated degradation mechanisms. A case study is described involving a potential bypass accident sequence involving the progression of flow-accelerated corrosion in a secondary system piping and stress corrosion cracking of steam generator tubes.
Risk-Informed Safety Margin Characterization Case Study: Use of Prevention Analysis in the Selection of Electrical Equipment to Be Subjected to Environmental Qualification

D. P. Blanchard (a) and R. W. Youngblood (b)

a) Applied Reliability Engineering, Inc. (AREI), San Francisco, California USA, b) Idaho National Laboratory (INL), Idaho Falls, Idaho, USA

Age-related degradation of electrical equipment is cited in numerous discussions of extended nuclear power plant operation as an important issue. Which SSCs matter? For which SSCs do we need ongoing assurance of performance? Replacement of all components and cables is a daunting prospect. Being able to focus on a subset of SSCs from an environmental qualification (EQ) perspective, while still maintaining plant-level safety and efficiency even if the other components and cables degrade, would be worthwhile.

This paper summarizes a case study that examines SSC aging for components within a PWR large dry containment. The case study illustrates how an understanding of SSC margin can be characterized given the overall integrated plant design, and was developed to demonstrate a method for deciding on which SSCs to focus, which SSCs are not so important from an environmental qualification margin standpoint.

The method chosen for selection of SSCs important to aging and environmental challenges is known as Top Event Prevention (TEP) or Prevention Analysis. TEP is a Boolean method for optimal selection of SSCs (that is, those combinations of SSCs both necessary and sufficient to meet a predetermined selection criterion) and allows demonstration that plant-level safety can be maintained by the collection of selected SSCs alone.

Risk-informed Prioritization of Modernization Activities Using Ageing PSA Model

Shahen Poghosyan and Armen Amirjanjan

Nuclear and Radiation Safety Center, Yerevan, Armenia

Nuclear Power Plant modernization is a continuous process, which is aimed to reduce risk as low as reasonably achievable. Modernization process is especially important for old design NPPs to keep them in compliance with current safety standards. In addition, modernization process is important for plants where age is becoming more and more significant factor in regard with equipment reliability. Development of modernization program requires not only listing the issues to be addressed, but also to come up with common understanding of importance of proposed measures and their priority. Traditionally prioritization of modernizations is mainly done using deterministic considerations. Meanwhile parallel application of PSA models allow to come up with numerically justified and optimal solutions.

Incorporation of ageing aspects in PSA model provide additional information for modernization prioritization in regard with plant’s components ageing perspective. This paper describes a feasibility study aimed to use integrated risk-informed decision-making principles for prioritization of modernizations. Paper discusses proposed approach for prioritization, which implies combination of probabilistic and deterministic indicators. In addition, paper discusses comparative analysis of results obtained using base case PSA model and ageing PSA model.

The Reliability Effects of Transient-Induced Degradation on the Performance of Large Power Transformers

Brittany L. Guyer (a), Carl R. Grantom (b), and Michael W. Golay (a)

a) Massachusetts Institute of Technology, Cambridge, MA, USA, b) CRG LLC, West Columbia, TX, USA

Increased knowledge of the effects of severe operational transients on component reliability, in combination with currently used mechanistic component degradation models, could augment the predictive capability of reliability modeling. A new component reliability model has been developed that considers the effects of both types of degradation. An application of the new model was sought in order to provide insight into both the sources and consequences of severe component transients and how these considerations can be formulated into a new framework for component aging management supporting component reliability programs. The large power transformer was selected for demonstration of this new reliability model. This component was selected as it is a component that has failed prematurely, has experienced strong transients during its operational lifetime, data are available about the important effects that the occurrence of strong transients have had on this component, and the transients experienced have resulted in effects that are not readily repairable (i.e., requiring component replacement). In this work, a strategy is proposed for the development of a physics-of-failure model of large power transformers that could be implemented in order to make more realistic performance predictions, supporting improved long-term plant asset management.
Model of Improvement of Maintenance Policies for Electrical Substations

Cristiano Cavalcante, Marcelo Alencar, Adiel Almeida, Ana Paula Costa, Rodrigo Ferreira (a), Maxwell Luna, Rogério Sá, Alison Ferreira and Adilson Vieira (b)

We observe that in electrical substation, issues often arise that directly influence the requirements for maintenance actions to be adequate. Maintenance policies are sometimes inappropriate because the aging of assets has been incorrectly evaluated, because technological upgrades are not properly reflected in maintenance plans, or because the operational regime is not taken into account. Thus, once the need for adjustments because of the presence of one or more of the issues mentioned above has been identified, it is essential that a different systematic be implemented to achieve the expected performance of the affected substation. Accordingly, this article proposes a model for establishing adequate maintenance policies to produce more effective results, taking into account not only the possible consequences of failure to which the system under study is subject but also the various specific concerns associated with the performance indices of the electricity system. A real electrical substation is used as a pilot system.

A Stochastic Production Planning Optimization for Multi Parallel Machine under Leasing Contract

Medhioub Fatma, Hajie Zied, and Rezg Nidhal

In this paper, we aim at optimizing the production planning. The problem consists on a several identical machines mounted in parallel and which are leased depending on a fluctuating demand over a finite time horizon under given service level. The objective of the production plan is to determine the best combination of leased machines numbers, production time (or level) and inventory levels, by developing a mathematical model, that minimize the average total costs over the finite time horizon. The contribution and newness of this work is that it treats this approach under new constraints related especially to leasing techniques and consequently we assume that the number of workstations varies from a production period to another. This characteristic is due to the leasing principle as well as to the fluctuating demand that we have to take into account. A numerical example confirms the analytical study.

Review of the Preventive Maintenance Requirements for the Safety Systems of the Mochovice NPP

Zoltan Kovacs, Robert Spenlinge

A requirement to optimize the Preventative Maintenance (PM) tasks assigned to specified safety systems has been identified at Mochovice Nuclear Power Plant (NPP). RELKO Ltd. has been tasked with optimising the PM tasks via application of the Reliability-Centered Maintenance (RCM) and PSA methodology. This paper details the results of the RCM analysis performed on the Core Cooling Systems. It is concluded that the PM tasks assigned to the Core Cooling Systems were, in the main, based upon the original equipment manufacturers’ (OEM) recommendations. Following the accumulation of about ten years of operating and maintenance experience it was concluded that many of the current task types and task frequencies required major revision in order to maintain the optimum levels of both reliability and availability of the Core Cooling Systems. It is also concluded that in several cases, specific components within the Core Cooling Systems will benefit from a shift in maintenance strategy from fixed interval invasive routines to a predictive maintenance (PdM) based strategy. Such a strategy will ensure close monitoring of system and component performance without compromising nuclear safety or availability. It is recommended that the Mochovice NPP replaces the current maintenance catalogue assigned to the Core Cooling Systems with new PM tasks detailed in the paper. In addition, the paper presents the impact of changes on CDF and LERF after implementation of the new PM tasks.

An Integrated Management for Occupational Safety and Health throughout the Plant-Lifecycle

Yukiyasu Shimada (a), Teiji Kitajima (b), Tetsuo Fuchino (c), and Kazuhiro Takeda (d)

The main purposes of occupational safety and health (OSH) management are to assure safe and healthful working conditions for working men and women and to prevent industrial accidents by the establishment of process safety management (PSM) system in the company level as well as the improvement of safety engineering techniques. Business process model has been developed to systematize the engineering activities and information flow throughout a plant-lifecycle (i.e. from research and development through process/plant design, construction and active manufacturing period, including production and maintenance) of chemical processes. This paper proposes an integrated approach for OSH management based on the business process model of engineering activities. This approach consists of three level hierarchical PSM; 1) PSM framework at enterprise-level, 2) HSE (Occupational Health, Process Safety, and Work Environment Protection) management activities at middle-management-level, and 3) SQDC-conscious tasks at manufacturing-site-level. Hierarchical integration of the PSM at each level makes it possible to realize the consistent and collaborative OSH management.

End User Involvement in the Development of Procedures and Safety Management Systems

Thomas Wold and Karin Laumann

IT-based Safety Management Systems contains procedures, safety standards, checklists and descriptions on how different tasks should be performed, and are usually designed at an executive level in the organization, and then communicated to the lower level in the organization where they are being applied. This paper presents data collected from qualitative interviews with executives and operators from two companies in the gas and petroleum industry. The executives generally regard Safety Management Systems as important tools for all work in hazardous environments, while the operators weren’t that enthusiastic. How can end user involvement in the development phase of procedures and Safety Management System improve use? A central argument is that Human Factors must be involved as early as possible in the development phase, and that operators need to understand the purpose of the management system in order to use it as intended. The informants that had been involved in the development of the procedures at least to some extent, felt an ownership to the management system, while the ones who hadn’t been involved at all felt no ownership to the management system, and did not see the purpose of it.
Identifying Requirements for Effective Human-Automation Teamwork
Jeffrey C. Joe (a), John O’Hara (b), Heather D. Medema and Johanna H. Oxstrand (a)
a) Idaho National Laboratory, Idaho Falls, ID, USA, b) Brookhaven National Laboratory, Upton, NY, USA

Previous studies have shown that poorly designed human-automation collaboration, such as poorly designed communication protocols, often leads to problems for the human operators, such as: lack of vigilance, complacency, and loss of skills. These problems often lead to suboptimal system performance. To address this situation, a considerable amount of research has been conducted to improve human-automation collaboration and to make automation function better as a “team player.” Much of this research is based on an understanding of what it means to be a good team player from the perspective of a human team. However, the research is often based on a simplified view of human teams and teamwork. In this study, we sought to better understand the capabilities and limitations of automation from the standpoint of human teams. We first examined human teams to identify the principles for effective teamwork. We next reviewed the research on integrating automation agents and human agents into mixed agent teams to identify the limitations of automation agents to conform to teamwork principles. This research resulted in insights that can lead to more effective human-automation collaboration by enabling a more realistic set of requirements to be developed based on the strengths and limitations of all agents.

Characterization of Resilience in Nuclear Power Plants
Florah Kamanja (a), and Kim Jonghyun (b)
a) Kenya Electricity Generating Company, Nairobi, Kenya, b) KEPCO International Nuclear Graduate School, Ulsan, South Korea

An emergency operation system in a nuclear power plant consist of operators, human-machine interface, procedures, and the interactions among these elements working together to respond to incidents. The complexity of dynamic systems such as nuclear power plants poses a challenge for safety as it can be a source of deviations from normal behavior during system operation. NPP control rooms consist of many elements that result in complex interactions between them. Resilience is the ability of a system to recover from a disturbance, so that it can sustain required operations under both expected and unexpected conditions. Nuclear power plants must anticipate the operating risks caused by either the hardware, human, or organizational failures in order to be resilient. The ability of NPPs to monitor the current status of the system, anticipate possible problems, react appropriately to events, and learn from past incidents is a measure of success hence the resilience. Although the significance of resilience has been stressed in the literature, there is a lack of adequate literature attempting to analyze system resilience. To achieve a practical and insightful understanding of the EOS resilience complexity, this paper aims at characterizing resilience attributes based on the existing literature.

Operational Experience and Data Analysis
Monday 6/23/2014 1:30 Waialua
Chair:

Recent Insights from the International Common Cause Failure Data Exchange (ICDE) Project
Albert Kreuser (a), Gunnar Johanson (b)
a) Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Cologne, GERMANY, b) ES konsult, Solna, SWEDEN

Common-cause failure (CCF) events can significantly impact the availability of safety systems of nuclear power plants. In recognition of this, the international CCF data exchange (ICDE) project was initiated in 1994. The objectives of the ICDE project are: to provide a framework for a multinational co-operation; to collect and analyze CCF events over the long term so as to better understand such events, their causes, and their prevention; to generate qualitative insights into the root causes of CCF events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences; to establish a mechanism for the efficient feedback of experience gained in connection with CCF phenomena, including the development of defenses against their occurrence, such as indicators for risk based inspections; and to record event attributes to facilitate quantification of CCF frequencies when so decided by the member countries of the Project. Until January 2014, 1346 ICDE events had been analyzed and reported in public OECD/NEA reports. This paper presents recent activities and lessons learnt from data collection on Control Rod Drive Assemblies and Heat Exchangers and on cross-component analysis on events which were due to external factors.

Internal Flooding According to EPRI Guidelines – Detailed Electrical Mapping at Ringhals
Per Nyström, Carl Sundén (a), and Cilla Andersson (b)
a) Risk Pilot, Gothenburg, Sweden, b) Ringhals AB, Varberg, Sweden

Eleven different tasks should be executed according to the EPRI guidelines for performing internal flooding PSA. Task 2 deals with identification of flood sources/mechanisms as well as with Systems, Structures and Components (SSCs). In this task it is briefly mentioned that not only the main components such as pumps and valves can be affected by flooding but also associated components such as circuit breaker, junction boxes and instrumentation and control circuitry are affected. It is fairly easy to locate the main components as well as the impact of flooding on these components. However it is more difficult to make a detailed mapping of the cable routing and the electrical dependencies (at Ringhals called electrical mapping) for the main components. This paper describes how this type of work is being executed and documented at Ringhals NPP in Sweden.

NRC Reactor Operating Experience Data
Shawn Walter St. Germain
Idaho National Laboratory, Idaho Falls, USA

Idaho National Laboratory (INL) has been providing technical assistance to the U.S. Nuclear Regulatory Commission Division of Risk Analysis in the Office of Nuclear Regulatory Research in the areas of data collection and reliability and risk calculation. INL collects, codes, assures the quality of, and maintains all reactor operating experience data necessary to support the Industry Trends Program and various risk-associated NRC studies requiring reactor operating experience data. The types of data collected under this effort include initiating event data, system reliability data, loss of offsite power data, common cause failure data, fire event data, and shutdown initiating event data. The data sources for this effort primarily consists of Licensee Event Reports (LERs), Event Notifications, and equipment failure reports provided by the Institute for Nuclear Power Operations (INPO). This data is analyzed and results published annually on the NRC website. The data is primarily used to support the NRC’s standardized plant analysis risk (SPAR) models but also provides generic industry average values for use by the industry in their individual PSA models. This paper characterizes the types of data collected, the various uses of this data, and the methods of collection, storage and retrieval.
Component Reliability in the T-Book – The New Approach
Anders Olsson, Erik Persson Sunde, and Magnus Gudmundsson
a) Lloyd’s Register Consulting, Stockholm, Sweden. b) TUD Office, Vattenfall, Stockholm, Sweden

T-Book is a world-famous, high-level data handbook for use in Nuclear PSAs (Probabilistic Safety Assessments). Due to its ambitious scope, high level of detail, and high QA standard, it has become world-famous, and is frequently used even outside the nuclear field. Since 2008, Lloyd’s Register Consulting, on behalf of the Nordic PSA Group (NPSAG) and TUD (the editor of T-Book), has performed a series of projects to enhance and consolidate the process, right from the classification and sampling of data, through parameter assessment, PSA modeling, and up to the final interpretation of results. Two aspects have proven to be of particular interest. Firstly, providing more homogeneous groups of T-Book components, which will have positive impact on PSA in terms of less conservative and more precise parameters, as well as increased consistency in the entire modeling process. Secondly, the benefits of said homogenization need to be weighed against the use of the multi-parametric model for standby components, because these two aspects are not fully compatible. A comprehensive approach, addressing both these aspects, is presented for selected components: pumps, batteries, diesel generators, and motor operated control valves. In this paper, the background and motives for the proposed strategy will be outlined, as well as the "tool box" to put it into practice. The presentation will also include what has been accomplished during 2013, and what is going to be introduced in the new version of the T-Book.

Phenomena Modeling

Preparation of Implementation Standard Concerning Severe Accident Management in Nuclear Power Plants
Shinya Kamata (a), Koji Okamoto (b), and Tomoyuki Sugiyama (c)
a) Japan Nuclear Safety Institute, Minato-ku, Tokyo, Japan. b) The University of Tokyo, Tokai-mura, Naka-gun, Ibaraki, Japan. c) Japan Atomic Energy Agency, Tokai-mura, Naka-gun, Ibaraki, Japan

The Great East Japan Earthquake with a magnitude of 9.0 (The 2011 off the Pacific coast of Tohoku Earthquake) occurred on March 11, 2011, and the accident was the result of the tsunami descended on the Fukushima Daiichi Nuclear Power Plant by the earthquake. Eventually, the core cooling systems of the units 1, 2 and 3 could not cope with the high pressure; this led to a severe accident. Hydrogen explosions were triggered in the reactor buildings of units 1, 2, and 3. In the light of these circumstances, Atomic Energy Society of Japan (AESJ) decided to establish a standard that consolidates the concept of maintaining and improving severe accident management. The standard also provides technical requirements for renovation and addition of the equipment, the formulation of procedures, and strategies. All these items enable the minimization of risks so as to prevent severe accidents, or otherwise enable the mitigation of impacts of severe accidents once occurred.

David L. Luxat, Donald A. Dube, Andrew S. Dercher (a), Richard Wachowiak, Rosa Yang (b), and Jeff R. Gabor (a)
a) ERIN Engineering and Research, Inc., West Chester, PA, USA. b) Electric Power Research Institute, Palo Alto, CA, USA

This paper presents initial results from the investigations of flammable gas transport from the Units 1, 2, and 3 containments into their respective reactor buildings. This study is being conducted as part of the Phase 2 effort of the EPRI Fukushima Technical Evaluation, which is an extension of Phase 1 evaluation (Reference [3]). It builds upon the existing event evaluations conducted by TEPCO (References [1] and [2]) and Sandia (Reference [4]). The analyses are conducted using EPRI's Modular Accident Analysis Program (MAAP), version 5.01. The analyses identify the potential for high temperature conditions in the drywell head region of Units 2 and 3 to contribute to the onset of leakage from each drywell—drywell pressures below twice design. It is not likely that high temperatures in the drywell head region developed at Unit 1 prior to the onset of leakage from the drywell head flange (at about twice design pressure). The leakage at all units through the drywell head flange has been found to enhance the build-up of flammable gases on the refuel floor. Unit 1 may have experienced flammable conditions on its refuel floor for 10 hours prior to the combusion event. Unit 2 likely did not develop flammable conditions on its refuel floor due to the open blowout panel. At Unit 3, leakage from the pipe vent into the Standby Gas Treatment System soft ducting may have allowed hydrogen to build-up at lower elevations—this could have contributed to more damage to the reactor building structure.
PSAM12 - Probabilistic Safety Assessment and Management

503 Cost-Effectiveness of Vehicle Barriers and Setback Distance for Protecting Buildings from Vehicle Bomb Attack
Nathaniel Heatwole
University of Southern California, Los Angeles, USA

Decision-making regarding implementing measures to protect buildings from vehicle bomb attack is often undertaken using highly judgment-based risk processes. This paper presents a quantitative risk-cost model for using vehicle barriers to set back distance around a new office building. The model explicitly considers both the attack probability, and the damages in the event of an attack (both target building and collateral), as well as how both of these might change as mitigation measures are implemented. The attack damages are assessed using a new empirical blast model, which adapts the estimation methods used by the U.S. Geological Survey for earthquake damages, and is based on data from three well-studied vehicle bomb attacks. Monte Carlo simulation is used to carry the uncertainty in the inputs through to the final results. The model outputs are the mitigation costs, the attack damages, the "break even" attack probability (at which the benefits of the mitigation justify its costs), and the cost per statistical life saved (assuming an attack). The results suggest that this mitigation option is cost-effective only when the attack probability (for the case without the mitigation measures present) is rather high.

M16 Policy Making and Legislative Issues
Monday 6/23/2014 1:30 Ewa
Chair:

41 From Prescriptive Arrival Times to Performance Based Fire Service Delivery – Parallels of Fire Service Planning and Fire Engineering
Adrian Ridder, Uli Barth
University of Wuppertal, Wuppertal, Germany

The fire safety design process of buildings underwent a substantial shift in the last roughly two decades, switching from prescriptive building codes to performance-based, fire-engineered designs. A similar process can be observed with Strategic Fire Service Planning which defines "how much fire service" is necessary per municipality. The methods used there become more and more sophisticated as well. However, with increasing complexity it becomes harder to explain and interpret results to the decision-makers, which applies both to fire engineering and fire service planning. The need for further research is made clear as the major outcome of this paper.

409 Issues in Incorporating Probabilistic Safety Assessment (PSA) in the Design and Licensing Stages of Generation IV Reactors
Ibrahim A. Alrammah
School of Mechanical, Aerospace and Civil Engineering (MACE), University of Manchester, Manchester, United Kingdom

Probabilistic approaches have been used and are also highly recommended to be used from the very early stage of the reactor design process. So far, Probabilistic Safety Assessment (PSA) approach is increasingly being utilized in the demonstration of safety in combination with deterministic approaches (e.g. to justify the classification of situations, to determine the sequences of sophisticated failures) and used also to verify the systems and components reliability in order to satisfy safety targets. However, epistemic problems such as uncertainties due to lack of design information, unknown phenomena, plant-specific hazards, data, etc., are larger than that from existing reactors, and will impose a significant challenge to the decision makers. This paper will discuss some technical issues related to applying PSA in the design and licensing stages of Generation IV reactors. These aspects include: initiating events, passive systems modeling, reliability data, common cause failure (CCF), modeling of novel design features, modeling of preventive maintenance, technical specifications, human reliability analysis (HRA), systems interdependencies, modeling of instrumentation and control (I&C), external hazards, continuous design risk monitoring, supporting studies, interpretation of PSA results for new plants.

501 Need for PRA in the Oil and Gas Industry
Matt Johnson, Nicholas Lovelace (a), and Michael Lloyd (b)
a) Hughes Associates, Inc., Lincoln, NE, USA, b) Risk Informed Solutions Consulting Services, Ball Ground, GA, USA

Probabilistic Risk Assessment (PRA) is widely used in the nuclear industry to assess the risk from hazards to nuclear power plants. This paper discusses the application of PRA methods to the oil and gas industry, and, specifically, to assessing production platform safety and optimizing levels of hydrocarbon production. Oil and gas platform safety can be analyzed with a focus on potential loss of life to platform workers from internal hazards such as uncontrolled liquid or gas hydrocarbon releases with subsequent ignition. Additionally, platform production capabilities can be analyzed with a focus on reducing production downtimes. PRA methods can be effectively utilized to identify both safety and operating issues for typical platform alignments, maintenance and testing frequencies, and prioritization of enhancements to platform operation.

564 Learning how to Learn from Failures: The Case of Fukushima Nuclear Disaster
Ashraf Labib
University of Portsmouth, Portsmouth, United Kingdom

In this work, it is argued that learning from failures and safety competence should be an important part of the curriculum of Engineering and Management students. The case of Fukushima will be used to illustrate how to learn about learning from failures using multi-models inspired by reliability and risk analysis in order to investigate disasters. This type of analysis can offer richness to our understanding of the root causes and provide insight into policy making and support decisions for resource allocations for prevention of such disasters. The analysis is based on a workshop related to learning from failures where students and practitioners were first given a brief about the related theory of reliability analysis and decision science, followed by introduction of the analytical techniques that can be used (such as FTA, RBD and AHP). They were then given a brief in the form of a narrative of the accident from investigation reports, and they were then divided into small groups with the task to perform an analysis of the disaster followed by presentation of recommendations in the form of a written report and an oral presentation. Finally, a set of generic lessons and recommendations are provided in order to prevent future system failure.
### Low-power and Shutdown

**Monday 6/23/2014 1:30 Kona**

**Chair:**

**45 A methodology for determining of Plant Operating States of Low Power Shutdown Probabilistic Safety Assessment for the Next-Generation Nuclear Power Plants**

Jae Gab Kim (a), Kwang Nam Lee (b), Hak Kyu Lim (a)

*a* KEPCO-ENC, Integrated Engineering Department, Korea, *b* KEPCO-ENC, Power Engineering Research Institute, Korea

This paper outlines the Low Power Shutdown (LPSD) Probabilistic Safety Assessment (PSA) portion of a methodology for the determination of the Plant Operating States (POSs). This is to determine how best to characterize them for inclusion into the LPSD PSA. The characterization of POSs will begin with a review of available shutdown PSA studies for current generation plants. The next-generation Nuclear Power Plants (NPPs) provide useful references for POS development. Several sets of current and next-generation NPPs including NUREG/CR-6144 of Surry Unit 1 shutdown PSAs have been reviewed to identify potential POSs. The POS set defined for the next-generation NPS PSA must represent all conditions that can occur over the course of a fuel cycle. This paper considers all plant conditions except full power operation which is addressed with the internal events PSA. The development of POSs can lead to group plant states that require similar equipment, timing, and operator action to respond to an upset condition. POS Grouping is based on Technical Specifications (TS) requirement as well as key factors associated with the main shutdown risk contributors like RCS temperature, RCS pressure, RCS inventory, State of RCS pressure boundary, and Decay heat levels.

**255 Shutdown PSA for Ringhals NPP Unit 1. Insights, Overview and Results**

Stefan Eriksson, Marie Gryte (a), and Erik Cederhorn (b)

*a* Ringhals AB, Väröbacka, SWEDEN, *b* Risk Pilot, Stockholm, SWEDEN

During 2011, 2012 and 2013 a Shutdown PSA (SPSA) has been developed for Ringhals NPP unit 1. Ringhals 1 is a Boiling Water Reactor (BWR) made by ASEA-Atom situated at the West coast of Sweden. The SPSA supplement the existing PSA Level 1 and 2 for Ringhals 1 and the final outcome will give a complete risk profile for the unit, providing support for verification of plant safety and upgrades. This paper gives an overview of the level 1 SPSA. A description is made of the basic conditions for identification of Plant Operating States (POSs), analysis of initiating events, sequence analysis and system analysis. The result for level 1 SPSA of R1 is briefly discussed.

**554 Developing a Low Power/Shutdown PRA for a Small Modular Reactor**

Nathan Wahlgren

NuScale Power, LLC, Corvallis, OR, USA

A growing area of interest in the field of nuclear risk analysis is the application of PRA techniques to low power and shutdown configurations when the availability of systems and components may differ significantly from normal operation. Many operating plants have performed (or are in the process of performing) a PRA for low power operations, and new reactor designs are required to be complete one as part of the design certification process. NuScale Power is developing a natural-circulation small modular reactor, and certain features of the design require refueling and maintenance procedures different from any in the industry. This uniqueness eliminates some sources of risk traditionally addressed in a shutdown PRA, but also introduces entirely new areas of risk. One major challenge is that all modules in the plant share a common refueling area, so each module must be lifted and moved from its operating location with fuel in the core. The module is completely disconnected and most systems credited in the full power PRA are unavailable when the module is in transit. This paper will give an overview of NuScale’s design and refueling process and discuss some of the challenges involved with developing a shutdown PRA for a reactor that is designed to be moved with fuel assemblies in place. Special attention is paid to determining a failure probability for a singlefailurer- proof crane with little directly applicable publicly available data.

**99 Risk-Informed Design Changes of an Advanced Reactor in Low Power and Shutdown Operation**

Ji-Yong Oh, Ho-Rim Moon, Han-Gon Kim and Myung-Ki Kim

Korea Hydro and Nuclear Power Co. Ltd, Central Research Institute, Daegu, Korea

APR+ has been developed in Korea since 2007. APR+ adopts various advanced safety features including passive auxiliary feedwater system, four emergency diesel generators. Through the implementation of the advanced designs, APR+ increased the safety to the world best level of evolutionary reactors. The full power core damage frequency or containment failure frequency decreased significantly comparing to APR1400 that is base model of APR+. However, low-power shutdown risk has not been improved substantially. This paper suggests several design changes that optimize low-power shutdown risk. Based on the design alternatives, this paper discusses risk effectiveness of the proposed design including various factors, e.g. equipment reliability, human error, training, procedure and so on.

**548 An Implementation Strategy of Low Power Shutdown PSA for KHNP NPPs**

Jang-Hwan Na, Seok-Won Hwang, Ho-Jun Jeon

Central Research Institute of Korea Hydro & Nuclear Power Co., Ltd., Daegu, Korea

Rightly after the Fukushima accidents, the Korean Regulatory Agency with the support from a group of academic and research experts evaluated the safety of Korean nuclear power plants including plants on construction. The expert group particularly focused on any possible design vulnerabilities in view of ultimate heat sinks and power sources considering external hazards such as seismic, flood or complex initiated events. They identified several common or plant-wise improvement factors and elicited 49 post-action items as near term Fukushima accident measures. One of the measures is to develop SAMG (Severe Accident Management Guideline) during LPSD (Low Power and Shutdown) operation in addition to the existing SAMG on the full power operation. At first, KHNP (Korea Hydro & Nuclear Power) decided to develop the LPSD PSA (Probabilistic Safety Assessment) models to increase the quality of LPSD SAMG. To get a technical adequacy, KHNP decided to revise the full spectrum of existing PSA models including full power, external or level 2 PSA incorporating up-to-date reliability data and methodologies. This paper presents an implementation strategy of developing LPSD PSA models including the status of upgrading full power PSA models at the end of 2013.
Reliability Analysis and Risk Assessment Methods I

Monday 6/23/2014  3:30 PM  Honolulu

Chair: Kaushik Chatterjee, FM Global

Yiliu Liu, Marvin Rausand
Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

Some dangerous failures of safety-instrumented systems (SISs) are detected almost immediately by diagnostic self-testing, whereas other dangerous failures can only be detected by proof-testing. The first type is called dangerous detected (DD) failures and the second type is called dangerous undetected (DU) failures. Proof tests are usually carried out at constant time intervals. DD-failures are repaired almost immediately whereas a DU-failure will persist until the item is proof-tested. Many items can have a DU- and a DD-failure at the same time. After the repair of a DD-failure is completed, the maintenance team has two options: to perform an "insert" proof test for DU-failure or not. If an insert proof test is performed, it is necessary to decide whether the next scheduled proof test should be postponed or performed at the scheduled time. This paper uses Petri nets to model the proof test strategies after DD-failures and to analyze the effects of the different strategies on the SIS performance. It is shown that insert proof tests reduce the unavailability of the system, whereas the adjustment (or not) of the test schedule does not have any significant long term effect.

47  A New Interfacing Approach between Level 1 and Level 2 PSA
Nicolas Dufflot, Nadia Rahni, Thomas Durin, Yves Guiguenu and Emmanuel Raimond
IRSN, Fontenay aux Roses, France

IRSN (TSO of the French Nuclear Safety Authority) has been developing L2 PSAs for many years, using its own probabilistic tool, KANT (probabilistic event trees software) associated to a very fast-running source term code (MER). Since the IRSN L1PSAs event trees are developed with one other dedicated software, the L1-L2 PSA interface methodology is a key and difficult point of the IRSN PSA methodology.

In the previous versions of the IRSN PSAs, L1-L2 PSA interface was a mostly manual process, resulting in significant resources allocation. To cope with such a difficulty, a new interfacing approach, allowing computerized generation of plant damage states (PDSs), has been developed. This approach is based on the introduction of flag events (basic events with a probability of one) into the L1PSA minimal cut sets (MCSs) in order to transfer information related to front lines systems (needed for accident management) status and operators actions. Afterwards, the MCSs are filtered to identify automatically the different PDSs of the L1-L2 PSA interface using a new dedicated tool. The automatic PDS generation allows implementing a very detailed L1-L2PSA interface easy to update. Since this new IRSN interfacing approach is based on fault trees only, it can be implemented with most of the level 1 PSA tools.

48  An Approach to Ensure the Availability of Complex Systems
Kaushik Chatterjee, Kumar Bhimavaramu, Robert Kasinski, and William Doerr
FM Global, Norwood, MA, USA

Availability of a system depends on: (1) the components' reliabilities; and (2) the Inspection, Testing and Maintenance (ITM) characteristics (i.e., inspection/testing frequency, repair/replacement duration, and maintenance restoration factor). Complex systems typically have several sub-systems and components with complicated interactions and dependencies. In order to ensure a desired availability of a safety-critical complex system such as a fire protection system throughout its lifetime, it is necessary to: (1) ensure the needed reliability of the critical components through carefully planned durability/life tests; and (2) perform ITM actions at appropriate intervals (or frequencies).

This paper presents a comprehensive approach to: (1) establish the reliability targets and the ITM frequencies for the critical components based on the desired availability of the system; and (2) estimate durability/life test duration and sample size requirements based on the established reliability targets for these critical components. The steps of the comprehensive approach have been demonstrated using a typical foam-water sprinkler protection system. The comprehensive approach, when applied to a safety-critical complex system, would help achieve the desired availabilities of the critical components, which in turn would ensure the desired availability of the system throughout its lifetime.

101  Reliability/Availability Methods for Subsea Risers and Deepwater Systems Design and Optimization
Annamaria Di Padova (a), Fabio Castello (b), Fabrizio Tallone (a), Michele Piccini (b)
(a) Saipem S.p.A., Fano, Italy, (b) RAM&SE S.R.L., Turin, Italy

The restriction of construction licenses for onshore oil/gas treatment plants and regasification units along with energy demand growth has increased the development of offshore installations. Furthermore the discovery of new offshore deep water fields enhance the engineering efforts towards the development of engineering of submarine systems and plants. Due to the complexity of these submarine systems, the severe environment where they operate and the difficulty or the impossibility to repair a component, a high system availability is becoming a key requirement. In this framework, to have a system architecture verified also from the reliability and availability point of view, the RAM analysis are becoming an essential part of the design. This paper describes the application of reliability/availability methods (RBD, Monte Carlo method, FMEA risk assessment) to support the design of subsea deep water systems. In particular, two case studies are presented, the first aiming at the definition of the optimum configuration of retrievable and permanent deep water modules, the second addressing the verification of design configurations and the suggestion of tests and inspection plans to guarantee system integrity along operating life. Moreover the paper summarizes also difficulties to find subsea equipment reliability data and proposes solutions for reliability components characterization.

Dependent Failure Modeling I

Monday 6/23/2014  3:30 PM  Kahuku

Chair: Andrew O'Connor, Acuitas Reliability Pty Ltd

56  Statistical Analysis of Common Cause Failure Events Using ICDE Data
S. Yu, M.D. Pandey (a), S. Yalaoui and Y. Akl (b)
a) University of Waterloo, Waterloo, Canada, b) Canadian Nuclear Safety Commission, Ottawa, Canada

Analysis of Common Cause Failures (CCF) is an important element of the Probabilistic Safety Assessment (PSA) of systems important to safety in a nuclear power plant. Based on the conceptualization of the CCF event, many probabilistic models have been developed in the literature. This paper utilizes a modern method, called “General Multiple Failure Rate Model”, for the probabilistic modeling of CCF events. To estimate the parameters of the GMFR model, the Empirical Bayes (EB) method is adopted. A detailed case study is presented using CCF data for Motor Operated Valves (MOVs).
Extending the Alpha Factor Model for Cause Based Treatment of Common Cause Failure Events in PRA and Event Assessment

Andrew O'Connor, Ali Mosleh  
Center for Risk and Reliability, University of Maryland, College Park, United States

Common Cause Failure modeling for Probability Safety Assessments has become standard practice in many industries. Of the numerous models proposed to include common cause, one of the most widely adopted has been the Alpha Factor Model, which is supported by the US Nuclear Regulatory Commission CCF database and software tools. The Alpha Factor Model (AFM) uses an empirical ratio between the independent failures and CCF failures to quantify the model parameters. While this has been advantageous in allowing the prediction of system reliability with little or no data, it has been limiting in other applications such as modeling the characteristics of a system design or including the characteristics of failure when assessing the risk significance of a failure or degraded performance event (known as an event assessment).

This paper proposes a new CCF model called the Partial Alpha Factor Model (PAFM), which extends the AFM to allow the explicit modeling of coupling factors between components such as shared maintenance, or shared location. Using this more explicit modeling allows the model to be tailored depending on how far the system design defends against such dependencies. By using the principles of the AFM as the basis for this new model, its implementation may be feasible without modification to existing PRA software or significant changes in data collection requirements.

Estimating Common Cause Failure Probabilities for a PRA Taking into Account Different Detection Methods

Kalle E. Jänkälä  
Fortum Power and Heat Oy, Espoo, Finland

The methodology to estimate residual parametric common cause failure (CCF) probabilities consists of the selection of the data source, source plants, source systems and component type, failure mode, assessment of the impact vectors, determination of equivalent observations, calculation of CCF rates of different multiplicities with uncertainties using an empirical Bayes estimation method and finally determining explicit CCF basic events and their probabilities to be used in the probabilistic safety assessment model. The CCF probabilities are obtained as the result of unavailability estimation accounting for different detection methods and corresponding outage times. Typically CCF events of safety system components are detected by tests during plant operation or during annual overhaul. In CCF quantification this is often regarded as the only way of detection. This leads into CCF unavailability quantification in which the CCF rate is based on all kinds of CCF events and the corresponding outage time is always determined by the test interval and testing scheme. This approach might be overly conservative or sometimes optimistic. This paper improves CCF unavailability estimation by taking into account monitoring and different kinds of tests and outage times and considering failure modes in the failure rate estimation.

Time Dependent Analysis with Common Cause Failure Events in RiskSpectrum

Pavel Krcal (a,b) and Ola Bäckström (a)  
a) Lloyd's Register Consulting, Stockholm, Sweden, b) Uppsala University, Uppsala, Sweden

Testing of components with common cause failure presents a challenge to a realistic analysis of failure probabilities. In reality, the most commonly used testing scheme is staggered testing. Common Cause Failure (CCF) models in Probabilistic Safety Assessment (PSA) studies often assume a sequential testing scheme. This might be overly conservative if the actual testing scheme is staggered. Some software tools, e.g., RiskSpectrum, offer time dependent analysis where one can model testing of components in time explicitly. This paper deals with effects of different testing schemes on the quantification of CCF events in time dependent analysis. Determining which formulae shall be used by software tools in time dependent analysis requires an in-depth understanding of how to model effects of tests on the common cause parts of failures. We analyze assumptions which lie behind different ways of modeling tests of common cause failure events.

Risk and Hazard Analyses I

Monday 6/23/2014 3:30 PM Oahu

A State of the Practice Investigation Guiding the Development of Visualizations for Minimal Cut Set Analysis

Yasmin I. Al-Zokari, Liliana Guzman (a), Barboros Can Conar (b), Dirk Zeckzer (c), Hans Hagen (a)  
a) TU Kaiserslautern, Kaiserslautern, Germany, b) University of Applied Sciences, Kaiserslautern, Germany, c) Leipzig University, Leipzig, Germany

Minimal Cut Set (MCS) analysis is used for the qualitative and quantitative safety and reliability analysis of systems. While many studies concerning MCS computation in the safety domain are found, no study gives a complete and detailed description of the tasks performed by practitioners during MCS analysis. The goals of this study are (1) to elicit the context (including the tasks) of MCS analysis; (2) to obtain the requirements and needs of the safety analysts, and the tools used; (3) and to assess the quality of the tools from the point of view of the safety engineers regarding their (3a) representation, (3b) interaction, (3c) performance, and (3d) usability. We found that the main purpose is improving improvements to increase the hazard's safety. The main tasks are identifying critical basic events, the related system components, and single points of failure. The stakeholders are mainly decision makers and system engineers. The main requirements are understanding single points of failure, determining MCS order, and finding basic events with high failure probability and related components. The results show that the usability of the tools is accepted but their information presentation can be improved by providing overviews and the missing interactions.

Risk Analysis and Decision Theory: An Extended Summary

E. Borgonovo, V. Cappelli, F. Maccheroni, M. Marinacci (a), and C. Smith (b)  
a) Department of Decision Sciences and IGIER, Università Bocconi, Milan, Italy, b) Idaho National Laboratory, Idaho Falls, Idaho, USA

We reconcile Kaplan and Garrick's seminal definition of risk with classical subjective expected utility, filling in the relevant gaps and providing a framework that is ready-to-use in applications. We show that Kaplan and Garrick's "frequency" format can be set in one-to-one correspondence with [26]'s utility theory. Kaplan and Garrick's "probability" format corresponds to the framework of [22] in which epistemic uncertainty is captured by a subjective probability over uncertain events. Finally, Kaplan and Garrick's "probability of frequency" format, the most general one, corresponds to the recently proposed framework of [13], which distinguishes aleatory and epistemic uncertainty in a Bayesian perspective. The classic Kaplan and Garrick's risk triplets are then cast in the powerful setting of axiomatic Decision Theory, with its solid behavioral foundations, allowing one to make explicit the often implicit decisions of a Risk Analysis.
In the early days of safety, together with his famous diagram, Farmer introduced a form of risk aversion. The first objective of the paper is to propose a general formulation of risk aversion along Farmer’s thinking. This theoretical framework is particularly well suited when accident severity cannot be mitigated and prevention efforts are aimed at reducing probabilities, as is the case with nuclear safety. This is shown to go beyond the expected utility theory. The second part of the paper reports on an attempt at estimating Farmer’s risk aversion as perceived by a panel of nuclear safety professionals. This tends to confirm Farmer’s views.

This paper aims to shed light on the concept of ambiguity in engineering risk assessment. The objectives are to 1) Clarify the meaning of ambiguity in risk assessment; 2) Describe sources and manifestations of ambiguity in preassessment, risk analysis, and risk evaluation/decision-making; and 3) Outline a procedure for approaching ambiguity in practice. To address these objectives, we first review existing definitions of ambiguity, which are argued to be of limited relevance to engineering risk assessment. We then propose a new overall definition of ambiguity as a challenge in risk-informed decision-making, and define linguistic, contextual, and normative ambiguity as distinct categories of ambiguity that have different implications for risk assessment. Based on this, we list concrete sources and manifestations of ambiguity in risk assessment in a set of tables that can be used as a checklist for identifying ambiguity in the assessment process. We finally outline a stepwise procedure for approaching ambiguity in risk assessment, in order to provide practical guidance and stimulate further research on ambiguity in risk-informed decision-making.

How is Capability Assessment Related to Risk Assessment? - Evaluating Existing Research and Current Application from a Design Science Perspective

Several countries use capability assessments as a part of their efforts to manage risk. However, it is unclear how such assessments are connected to other risk management activities (e.g. risk assessment). Therefore, the aim of the present paper is to present a study of how capability assessment is related to risk assessment. Capability assessment methods were identified through a scoping study and the Swedish capability assessment method was investigated through interviews with Swedish public actors and analysis of legislative documents. The data was analysed using a design science perspective. The results of the analysis show that the purposes presented for some capability assessment methods are the same or similar to purposes common to risk assessment methods, and the actual form of some of the methods is similar to existing risk assessment methods. Nevertheless, the relationship between capability assessment and risk assessment is unclear. We conclude that if capability assessments are going to continue to be an important part of risk management activities more research is needed to better establish the relationship between risk assessment and capability assessment.
Analyses of AP1000® Expanded Event Tree Sequences Based on Best-Estimate Calculations

J. Montero-Mayorga, C. Queral, J. Gonzalez-Cadelo and G. Jimenez
Universidad Politecnica de Madrid, Madrid, Spain

The Westinghouse AP1000® reactor is an advanced design whose safety systems are based on natural mechanisms such as gravity or natural circulation, namely, they are passive safety systems. Because of the passive nature of the safety related systems and its dependency on small changes on certain variables (e.g. pressure), it is necessary to confirm that when core cooling is achieved, uncertainties are bounded. The thermal-hydraulic (T/H) uncertainty evaluation process performed by Westinghouse Electric Company (WEC) identified a set of low T/H margin by expanding probabilistic risk assessment (PRA) event trees. Expanded event trees contain more branches than classic event trees, including all possibilities for system actuation. Then detailed conservative computer codes were applied in order to analyze the bounding sequences that were significant to the core damage frequency and demonstrating that the T/H uncertainty was bounded. The UPM group has analyzed the low-margin sequences obtained by WEC with the best estimate computer code TRACE in order to verify the previous results and also to study the phenomenology of such sequences through a best estimate code. This paper presents the results obtained for the DVI line break case confirming that it does not exist damage in the bounding sequence selected for that case.

Application of Web-based Risk Monitor in Tianwan Nuclear Power Plant

Hao Zheng (a), Wei Wang (b), Xiaohui Gu, Yong Qu, Zhenli Bao (c), Xuhong He (b)
a) Lloyd's Register Consulting, Beijing, China, b) Lloyd's Register Consulting, Stockholm, Sweden, c) Jiangsu Nuclear Power Co., Lianyungang, China

As one of the specific applications of Living PSA, Risk Monitor, which is a real-time analysis tool used to determine the instantaneous risk based on actual plant configuration, has been widely used in risk-informed decision-making process during plant operation. A web-based Risk Monitor application for Tianwan nuclear power plant (NPP) is currently being used onsite to improve the PSA applications, popularize the concept of risk-informed management, and then enhance the whole risk management level in Tianwan NPP. Compared with the traditional windows based tools, this web-based Risk Monitor application is a natural multi-user program with great advantages. It has good interface with plant’s existing information system and can automatically update the risk information upon changes of component configuration, has been widely used in risk-informed decision-making process during plant operation. A web-based Risk Monitor application for Tianwan nuclear power plant (NPP) is currently being used onsite to improve the PSA applications, popularize the concept of risk-informed management, and then enhance the whole risk management level in Tianwan NPP. Compared with the traditional windows based tools, this web-based Risk Monitor application is a natural multi-user program with great advantages. It has good interface with plant’s existing information system and can automatically update the risk information upon changes of component status/configurations.

This paper presents the overview of the Risk Monitor application used in Tianwan NPP, including challenges and experience of implementing Web-based Risk Monitor, and major feature improvements which facilitate the application of Risk Monitor. Example PSA applications implemented in Tianwan NPP will also be presented together with future plan and challenges.

Analyzing System Changes with Importance Measure Pairs: Risk Increase Factor and Fussell-Vesely Compared to Birnbaum and Failure Probability

Janne Laitonen, Ilkka Niemelä

Radiation and Nuclear Safety Authority (STUK), Helsinki, Finland

Importance measures are used to rank components of a system according to a selected criterion depending on the decision problem. Sometimes, more than one importance measure may be used. In risk-informed decision making, a component that is critical to safety is usually prioritized higher in allocating activities, e.g. maintenance or inspection. One desired effect of this prioritization is to improve the reliability of the critical components. Changes in the system or component reliability affect their importance measures. If these feedbacks are taken into account, new ranking for the components may be obtained.

This paper examines the properties of risk importance measure pairs in analyzing system changes with fault tree analysis. A common approach is to use risk increase factor (or risk achievement worth) and Fussell-Vesely importance measure. This approach is compared to an alternative method which utilizes Birnbaum importance measure and the failure probability of a basic event. It is shown that the first approach may lead to difficulties in understanding the effect of system changes whereas the latter seems to provide simpler and more robust alternative. The paper includes examples to show and compare the differences between the two methods. The key advantages of the alternative method are that it reflects the absolute instead of relative change, the variables are independent, and that the interpretation of the importance measures is straightforward, reflecting risk in terms of safety margin and failure probability.

Energy Loss Optimization in Basic T-Shaped Water Supply Piping Networks for Probabilistic Demands

KW Mui, LT Wong, and CT Cheung
Department of Building Service Engineering, The Hong Kong Polytechnic University, Hong Kong, China

Minimization of energy loss of water supply networks is a major concern of pump power reduction for sustainable water systems in buildings. This paper presents a mathematical model for energy loss optimization in a common basic T-shaped water supply piping network that serves infinite probabilistic demands. Optimized designs based on proper network pipe sizes are analyzed. Optimal pipe radius ratios (2 1/7 to 2 3/7) and their corresponding energy implications in the network are also discussed. The results show that existing piping designs are not optimized for probabilistic demands and there is potential for energy loss reduction.
In several countries, the requirements for probabilistic risk assessments have increased beyond a Level 1 internal events PRA to add or address spatial and external hazards. In a growing number of countries the requirements have further increased to address all Level 1 hazards in all plant operating modes. Sciensite developed its first shutdown probabilistic risk assessment (PRA) in the early 1990s for a European nuclear power plant. Since then several additional low power and shutdown PRA models were developed in the United States following the same approach. The original shutdown PRA model was expanded to evaluate hazards challenging fuel in the reactor vessel and fuel in the spent fuel pool; modeling Level 1 core damage for all hazards in all plant operating modes, with corresponding Level 2 (release) and Level 3 (consequence) models. This complete PRA of all hazards and all modes was incorporated into the European plant’s licensing basis, and in 2010 a peer review was conducted.

In the last three years, the shutdown PRA model was updated and a follow-on peer review conducted. Plant operational state definitions were revised to better agree with technical specifications governing the plant operating modes. Additional initiating events were modeled for the fuel pool plant operational states as well as the refueling plant operational states. Initiating event frequencies have been updated to reflect recent operating experience. Success criteria and accident sequence development were revised based on insights from new thermal-hydraulic analyses. New shutdown procedures and “FLEX” strategies were considered in the accident sequence development. New operator actions were credited and human reliability analyses were performed. During the same period, additional model changes and refinements were developed on the USA shutdown PRA models.

This paper presents the insights and improvements made in the PRA models of low power and shutdown states, and also presents a summary of insights and benefits that the plant obtained during the development and updates of the underlying shutdown PRA models.
Finally the interpretation of the results and deduction of general issues and recommendations regarding to the design of prototype test procedures are presented. Variables are analyzed. Furthermore a method for the comparison of qualitative and quantitative characteristics and their impact on the door system is described.

The overall objective of the Working Group on Risk Assessment (WGRISK) of the OECD Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) is to advance the understanding of Probabilistic Safety Assessment (PSA) and to facilitate its utilization for enhancing the safety of nuclear installations. To accomplish this mission, WGRISK continuously performs a variety of activities to exchange information on PSA between member countries. This paper presents a brief overview on the actually on-going WGRISK activities and perspectives. In addition to on-going tasks covering more traditional PSA challenges (e.g. tasks relating to human reliability analysis (HRA) and digital instrumentation and control (I&C)), new challenges for PSA have arisen from the recent nuclear power plant operating experiences and the insights from the post-Fukushima stress tests. In response to these new challenges, WGRISK conducted an international workshop on "PSA of Natural External Hazards Including Earthquakes" in June 2013. This workshop revealed valuable insights on challenges associated with external events such as scope consideration for PSA, the need to consider combinations of external hazards, and multi-unit impacts. Another ongoing WGRISK activity is the second follow-up workshop on "Fire PRA" to be held in April 2014. The Fire PRA workshop will address many of the technical challenges associated with including fire hazards, which typically provide a non-negligible contribution to the overall core or fuel damage frequency, in PSA. WGRISK recently initiated a task focused on obtaining insights from PSA related to the loss of electrical power sources. This task will collect examples of PSA insights related to a loss of electrical power sources, including those insights identified as a result follow-up activities to the Fukushima Dai-ichi reactor accidents. It is expected that this task will also highlight the capabilities of PSA as a tool for providing insights related to the potential consequences of the loss of a safety function, such as core damage frequencies or frequencies of radioactive releases. The use of PSA in this manner may provide a measure of defense-in-depth in case of loss of a safety function, which will augment more traditional analysis approaches that emphasize identification of failures that can lead to loss of system function.

**Automotive Engineering**

**Monday 6/23/2014 3:30 PM Kona**

Chair: Stefan Bracke, University of Wuppertal

146 RAPP: Method for Risk Prognosis on Complex Failure Behaviour in Automobile Fleets Within the Use Phase

Stefan Bracke and Sebastian Sochacki
University of Wuppertal, Chair of Safety Engineering and Risk Management, Wuppertal, Germany

The increasing complexity of product functionality and manufacturing process parameters often leads to complex failure modes during the product life cycle. These field information are the basis for risk analyses and damage case prognosis with the goal of an early risk detection and leads to the possibility of nearby interactions e.g. product and manufacturing optimisation or recall action. This paper outlines the essential procedure of the new developed method "Risk Analysis and Prognosis of complex Products (RAPP)". The main focus of the RAPP method is the detection, visualisation and prognosis of risks and damage cases depending on their life span variables regarding to a product fleet - based on a risky production batch - in field. The RAPP method contains multiple steps: First steps include the mapping/prognosis of the failure behaviour and the mapping of product field load profiles. Next step is focusing on the estimation of the critical area regarding the life span variable (e.g. critical kilometer range). Based on these steps, it is possible to perform the risk analysis and risk prognosis regarding the product fleet. Finally, the last step of the RAPP method is the verification of risk analysis and prognosis. The theory and application of the RAPP method is explained within an automotive case study oil tube leakage.

168 Stress-Dependent Weibull Shape Parameter Based on Field Data

Jochen Juskowiak and Bernd Bertsche
University of Stuttgart, Stuttgart, Germany

The Weibull shape parameter is often assumed to be constant, with no dependency on stress. However, some cases exist, in which it is a function of stress. If the stress-dependency is not considered, vague assumptions about the Weibull shape parameter may lead to inaccurate results, e.g. for reliability prediction or demonstration testing purposes. Drawbacks in choosing an adequate parameter are e.g. extensive testing at a specific stress level, or insufficiently established mathematical descriptions. This paper presents an approach which allows a stress-dependent derivation of the Weibull shape parameter based on field data. In order to do so, simulations of the customer behavior and additional information from the customers themselves are used. Linking the occurred failure with the corresponding stress-level is thus possible.

314 APTA Approach: Analysis of Accelerated Prototype Test Data Based on Small Data Volumes Within a Car Door System Case Study

Marcin Hinz, Philipp Temminghoff, and Stefan Bracke
University of Wuppertal, Chair of Safety Engineering and Risk Management, Wuppertal, Germany

Knowledge of failure behavior and failure modes regarding the component’s complete life cycle is fundamental within the early development phases of technical and complex products. Here, an overview of the design of prototype test procedures as well as the transformation of expected field failure behavior in prototype test characteristics is described. This provides the required knowledge for the understanding of accelerated testing and is the basis for understanding of the developed “Accelerated Prototype Test data Analysis” (APTA) approach. The APTA approach is demonstrated with the help of a case study with regard to a car door system. The analysis of the design principles, expected impacts in the usage phase and car door prototype test procedure is discussed. With the use of nonparametric as well as parametric statistical methods, the wearing and ageing of specific door mechanism characteristics (e.g. forces or displacements) in relation to life span variables are analyzed. Furthermore a method for the comparison of qualitative and quantitative characteristics and their impact on the door system is described. Finally the interpretation of the results and deduction of general issues and recommendations regarding to the design of prototype test procedures are presented.