RiskSpectrum Magazine

2014

PSAM 12
Welcome to Honolulu

Risk sharing
in a globalised economy

RiskWatcher Web
sees the light

RiskSpectrum PSA
BDD & other tools

Lloyd's Register Consulting

In this issue:

Johan Sörman
Editor-in-Chief
Lloyd's Register Consulting
johan.sorman@lr.org

Hannah Häggström
Consultant Editor
hannah@underhuset.com

RISK SPECTRUM

RiskSpectrum Magazine is published by Lloyd's Register Consulting and distributed to some 3,000 subscribers in 72 countries.

Contact us:
Lloyd's Register Consulting
P.O. Box 1288,
S-172 25 Sundbyberg,
Sweden
sales.riskspectrum@lr.org

For a free subscription email sales.riskspectrum@lr.org

Associate editors and design — Inge Alme, Helle Gjønnes Møller
Language consultant — Victoria Coleman
Printing — Pipeline Nordic AB

"Nuclear has never been safer; however, we are still in the process of phasing out."

Where are we heading?

Dear readers,

In the article "Forging new alliances for nuclear power", Dr Hans-Holger Rogner points out that nuclear energy is considered non-competitive given the current gas prices in the USA. At the same time, the Fifth Assessment Report of the Intergovernmental Panel on Climate Change (IPCC) addresses the need to reduce CO_2 emissions and mentions nuclear energy as a possible alternative energy source in this context.

Focus on safety is steadily increasing in most energy disciplines, with new methods being developed and substantial effort being invested. The integrated DSA and PSA approach is one example of how the work has evolved. Both DSA and PSA are good, sound methods. An article in this magazine looks at their combined role and the historical "rivalry" between them. Instantaneous risk evaluations of blowout preventers (BOP) on drilling rigs are another example of improvements and are discussed in a separate article.

Given the international target of 1 accident in 10,000 reactor years and taking into account that there are some 400 stations around the world, we should expect one major accident every 25 years. We have been producing nuclear energy commercially since around 1960, or for roughly 65 years. In the course of these 65 years we have had three major accidents, one of which is discussed in this magazine. We could of course argue about whether the containment meets expectations or not in the event of a core melt. But considering that we have not had the same number of reactors in operation at all times:

The number of major accidents is not too far off the estimate!

I would go so far as to state that nuclear has never been safer; however, we are still in the process of phasing out. Although one could claim that we are only phasing out nuclear in a few countries, the decision not to invest in new nuclear will in practice mean the phasing out of ageing plants. In 10–20 years, the current "old fleet" will not be in operation any more. There are several reasons for this, and the economy is a very strong driver.

The new reactors and reactor types pose a much lower risk. How can we communicate this? Or is risk really the problem? Are we good enough at communicating the results of risk analysis to the public? Dr Todd Paulos makes an important statement in his article, pointing out that "society has become more risk aware and knowledgeable". In light of this, are we providing the right results? Should we focus on providing decision-makers and the public at large with PSA Level 3 analyses including environmental and health aspects and relevant measures that are comparable to those for other societal risks, such as environmental economic risk?

The picture is fragmented, and I doubt that we risk analysts are helping to make it any clearer. ■

Ola Bäckström
Software Manager and Vice President
Lloyd's Register Consulting
ola.backstrom@lr.org

PSAM 12

A family event?

I am very happy to present this special issue of RiskSpectrum Magazine for PSAM 12. I hope the magazine will serve as a source of information about PSAM 12 and Hawaii as well as a source of insight into technically advanced topics for RiskSpectrum and PSA professionals.

PSAM 12 is an important event for Lloyd's Register Consulting, as it gives us the opportunity to meet you, the conference participants. This year's location is particularly interesting for me because I wouldn't normally travel to Hawaii for business or pleasure. Not because it doesn't appeal to me, but because I live so far away, in Sweden.

I have brought family along to PSAM, as I know many of you have, too, and I welcome the PSAM 12 organisers' efforts to make it easier for our families to accompany us. Many in the industry have to travel for work, and one way of combining our job with our family life is to bring our family to work.

In the 2010 issue of RiskSpectrum Magazine for the PSAM 10 conference in Seattle, I wrote that the development of RiskWatcher Web was about to start. At that time, an agreement had just been signed between China Nuclear Power Engineering Company (CNPE) and Scandpower (now Lloyd's Register Consulting) for the development of RiskWatcher Web for two NPPs in China.

Today, we can pronounce the development project a success: RiskWatcher Web has now been installed at Tianwan and Qinshan Phase II. Read more about it in a separate article in this magazine.

Don't miss the Welcome Reception at 7:00 pm on Monday. Lloyd's Register Consulting is sponsoring the event, and I hope many of you can join us.

I wish you all a successful conference – and don't forget to have fun! ■

Johan Sörman
johan.sorman@lr.org

Lloyd's Register Consulting is presenting a number of papers at PSAM 12. Please take the opportunity to come and listen.

Paper title and schedule:

#368: Monday, 1:30 pm, Waialua: "Component Reliability in the T-Book – The New Approach"

#473: Monday, 3:30 pm, Kahuku: "Time Dependent Analysis with Common Cause Failure Events in RiskSpectrum"

#459: Tuesday, 3:30 pm, Oahu: "Method for Analysing Extreme Events"

#456: Wednesday, 10:30 am, Kahuku: "Quantification of MCS with BDD, Accuracy and Inclusion of Success in the Calculation – the RiskSpectrum MCS BDD Algorithm"

#216: Wednesday, 1:30 pm, Waianae: "Development of Feed Water Line & Main Steam Line Break Initiating Event Frequencies for Ringhals Pressurized Water Reactors"

#458: Wednesday, 3:30 pm, Waialua: "Quantification of Reactor Protection System Software Reliability Based on Indirect and Direct Evidence"

#165: Thursday, 10:30 am, Waialua: "BOP Risk Model Development and Applications"

#217: Thursday, 3:30 pm, Oahu: "Addressing Off-site Consequence Criteria Using PSA Level 3 – Enhanced Scoping Study"

Aloha! Welcome to Honolulu!

There's no doubt that you will have busy days during the PSAM 12 conference, but if you have some time to spare, Honolulu has a lot to offer. Like numerous travel sites say: Honolulu has it all.

You will find everything from historic landmarks and monuments to shopping, arts and culture. And don't forget to go to the beach, the famous Waikiki beach. Since the conference is being held at the Sheraton Waikiki, the Waikiki will be there waiting for you every day.

What will the weather be like? Probably very sunny, warm and agreeable.
The average temperature in June is 81 °F (27 °C). The average water temperature in June is 79 °F (26 °C).

Need-to-know words

Would you like to learn to say more than just aloha? According to the Huffington Post, there are 27 Hawaiian words that you need to know before exploring the 50th state of the USA.

1. Aloha – used as a greeting or parting.
2. Mahalo – thank you.
3. Kokua – help.
4. 'Ono – delicious.
5. Malasda – a Portuguese donut.
6. Mauka – towards the mountain.
7. Makai – towards the ocean.
8. Poke – a dish made of raw seafood mixed with sauce and onion.
9. Windward – the side of an island that is exposed to the prevailing wind and is the wetter side.
10. Leeward – the side that is protected from the prevailing wind and is typically the drier side.
11. Vog – volcanic smog.
12. Pau – done or finished. As in pauhana, or "after work", to mean happy hour.
13. Wahine – women.
14. Kane – men.

Curious about the remaining 13 words? Visit www.huffingtonpost.com to learn them all. Type "27 words" in the search column.

Highlights in Honolulu according to the official tourist site gohawaii.com

These are of course just a few of the recommendations you will find at gohawaii.com. Visit the site to find out more about what Honolulu and Oahu have to offer.

- Aloha Tower, a historic Honolulu landmark and home to an outdoor shopping and dining marketplace.
- Kapahulu, a small neighbourhood next to Waikiki with unique shops and some of Honolulu's best local food.
- Hanauma Bay Nature Preserve, one of Oahu's most popular snorkelling destinations.
- Leahi (Diamond Head). Hike to the top of the Diamond Head State Monument for panoramic views of Waikiki and Honolulu.
- Downtown Honolulu and Chinatown, Oahu's historic centres for government, business and the arts.
- National Memorial Cemetery of the Pacific, one of the nation's prominent national cemeteries
- Kawaiahao Church, the first Christian Church built on Oahu in 1842.
- Honolulu Museum of Art, Hawaii's largest fine-arts museum.
- Shangri La, one of Hawaii's most architecturally significant homes.

The biggest PSAM Conference yet

RiskSpectrum Magazine took the opportunity to ask the General Chair, Dr Todd Paulos, about his expectations for the upcoming PSAM.

What are the most important issues for PSAM 12?
As an organization, the most important issue for us is to capture the level of interest of the first-time attendees and increase their future participation. I feel as a society we have stagnated the past few years, but we have many first-time attendees from many different countries and new industries coming to Honolulu, and it is the participation of these new IAPSAM members that will carry the organization forward.

It has always been our charter to spread our influence into new industries and geographical areas, and areas such as Oceania, Eastern Europe and Latin America have had little participation in the past. We hope to grow the participation in these areas, as well as others, in the next decade. We appear to be headed for a PSAM Topical Meeting in Brazil in 2015, which is fantastic for this organization. With every conference, we are trying to increase the participation of various industries, such as I have with this conference to encourage more participation from the medical and finance industries. I am sure everyone will find these plenary sessions to be interesting and fresh.

Is there any question that you think will receive special attention?
There is no singular question or topic that will receive special attention. We have tried to bring together a diverse set of plenary speakers from nuclear, environmental, medical and financial areas to compare notes and learn from each other. I do expect more than 50% of the papers to have a nuclear "flavor", but there are many areas in which research from one industry applies to one or more other areas. This is the point of the conference.

PSAM 11 was held in Helsinki 2012. What has happened in the past two years?
Sadly, in the last two years I have put on 10 kg and added gray hair, while my Co-Chair consistently looks better with age. As a society, the past two years have certainly been interesting, with the increasing need for risk assessment in many new fields – at least that seems the case if you read the news. I seem to see the word "risk" more and more in headline news stories encompassing oil and gas, space and space travel, war, finance, business, medical, sports and activities, weather, acts of God, aviation, and the socio-political climate of today's current events.

I think we have finally reached that turning point as a society where the application of risk and risk management methods is clearly not a nuclear industry-only term, and every industry needs to understand these topics to succeed in day-to-day business. I rarely hear anyone say "no risk is acceptable" any more, as even society has become more risk aware and knowledgeable.

"My expectations are to have the biggest PSAM conference yet. We have had larger conferences with ESREL, but this should be our largest PSAM-only endeavor with 500–550 attendees."

Will the participants have any chance to see more of Hawaii and Honolulu or will the days be fully booked during the conference?
We hope that the participants will take the opportunity to spend time before or after the conference to see more of Honolulu and perhaps Hawaii (but not during!). We have tried to infuse the Hawaiian atmosphere and flavor into the conference as best that we can, to give everyone a taste of Hawaii during the conference, such as at our conference dinner which is a Hawaiian luau, but obviously extra time would be needed to travel to other islands.

There are plenty of things to do and see in Honolulu and even on the island of Oahu, but we would suggest to the attendees to use the special rates we have secured with Starwood Resorts to go to other islands before or after the conference. We have always pitched the statement "come for a conference and stay for a vacation", but we are sure the participants will not want to miss the technical program as we have some new industries represented at the conference. ■

Hannah Häggström
hannah@underhuset.com

Todd Paulos, Ph.D.

Todd Paulos has over 20 years of experience in the field of reliability engineering, systems engineering and probabilistic risk assessment. He is currently working in the commercial and military aviation industry as the reliability engineering manager at Parker Hannifin's customer support operations, providing support to aircraft manufacturers, operators and air forces worldwide. Prior to that, Dr Paulos was involved in a number of NASA programs and worked at the Lockheed Martin Skunk Works. He has worked on the development of over 30 aircraft and spacecraft in the course of his career.

Dr Paulos has been involved with the IAPSAM organization and the PSAM conferences since the very first conference was held in Beverly Hills, California, in 1991. He has been a supporter and organizer of the conference for many years, and has only missed one. He hopes to find newer career engineers and scientists to carry the organization forward.

Dr Paulos holds a Bachelor of Science in Engineering from Harvey Mudd College, and an M.S. and a Ph.D. in Mechanical Engineering from the University of California at Los Angeles. His current research revolves around understanding real world aviation data, repair forecasting simulations for maintenance repair and overhaul (MRO) environments, and sanity checks for risk and reliability software programs.

Todd is a native of Seal Beach, California, where he resides with his wife Cindy and their three children, Victoria, Nicholas and Alexander.

Todd would like to thank Parker Hannifin for its support of this and past PSAM conferences, and also extends his thanks to the many other people, organizations and universities that have given their support as well.

Forging new alliances for nuclear power

Globalised economy opens up for risk sharing

Nowadays, countries can get financing for nuclear power plants from abroad, offering state guarantees to pay for them in the longer term using revenues from power generation. What challenges does this offer?

In the peak era of the nuclear industry (1970s and 1980s), nuclear power plants were usually financed by governments and/or national companies. Some of the nuclear power plants that are now being planned are financed by multinational companies whose majority owner is in some cases a government.

RiskSpectrum Magazine asked Dr Hans-Holger Rogner, an expert in the application of systems analysis to long-term energy demand and supply issues, to share his knowledge and insights with regard to this development.

Today some 45 countries are considering embarking on a peaceful nuclear programme. Some of these countries will be dependent on financing from other countries and governments for building the nuclear power plants. Is this a new trend, and do you see any challenges in this?
It is in a way a new trend in the nuclear industry. Early on, in the pioneering era of large-scale nuclear power plants, most were state financed or built with public money, like in France and Germany. We were simply not a globalised economy at the time. In regulated markets where one could pass on risks to consumers there was no need for cross-border finance (=risk sharing). As well as national pride, competition for civil nuclear leadership, etc. made nuclear power a matter of home priority.

In the USA, nuclear power has been financed by companies and consortiums operating in regulated electricity markets with electricity rates set by the regulator on a "cost plus" basis. Risks of cost overruns or inefficient operations were thus borne by the rate payers, i.e. consumers. After the TMI accident in 1979 all new builds were stopped in the USA. This was mainly due to uncertainty in the new safety regulations. It was judged that requirements could change, causing revisions in the designs even for plants already under construction. Due to the regulatory uncertainty it became a too risky business to invest in, especially at a time of excess generating capacity and cheaper fossil alternatives after the oil price collapse of 1986. Many projects were cancelled and those continued experienced enormous completion delays and cost overruns.

"In regulated markets where one could pass on risks to consumers there was no need for cross-border finance (=risk sharing)."

Today we have a mix of liberalised and competitive markets. In deregulated electricity markets, however, investing in capital-intensive nuclear power represents a much higher financial risk than before, as cost-plus rate-setting is history. Therefore the finance structure is very different today. Recognising that risks should be allocated to those who can best manage them, different entities assume risks for different phases during a nuclear power plant project. The risk of each phase is also spread over several partners that only take a risk during their part of the construction or operational phase. Usually both the technology vendors and buyers assume a certain share of the risk. Because of the size of investment, there is no single company that by itself can take on such a big investment. On a per kW basis, investing in natural gas-fired combined-cycle plants is only a fifth to a fourth of the capital required for a nuclear plant. As gas plants are also of smaller unit sizes, the financial risk exposure is further reduced – nuclear fell out of favour with utilities and investors.

Still, in the USA there are five nuclear power plants under construction today. Four of these projects were started last year, at a time of low gas prices which are expected to prevail for a long time into the future. At 2013 gas prices, nuclear is generally considered non-competitive. Still, nuclear power is considered a sound investment as its fuel prices are not as volatile as the price of gas, and it protects against future climate legislation as it hardly

emits any carbon dioxide. Moreover, all new builds are located in states with regulated electricity markets and at least two units have made use of billions of dollars of government loan guarantees – all of which reduces financial risks.

As regards large-scale vendor finance, ROSATOM, Russia, appears to be unique. They will soon be building and operating new nuclear power plants in Turkey and will provide financing based on 15-year fixed-price power purchasing agreement with the Turkish Electricity Trading and Contracting Company (TETAS).

Of course, a country's political stability and past track record in serving loans for large infrastructure projects are factored into the risk assessment of a cross-border investment project.

What would you say are the driving forces for the interest shown by countries that currently do not have nuclear power in starting national nuclear power programmes?

Economic development is closely linked to access to reliable and affordable electricity. There is a huge demand for power in many developing countries and all electricity generating options are needed. Oil, coal and gas prices are volatile and high. Infrastructure investments are needed for importing and distributing fossil fuels. Renewables are growing fast but are still expensive and do not provide dispatchable electricity. Energy security is very important for a sound development of business and economy in a country and having nuclear power adds to energy security.

What is the driving force for countries to invest in power generating stations in foreign countries? Why not build nuclear power plants in their own country and export the power?

Nuclear power plants are built by the nuclear industry, which may or may not be state-owned. Regardless of ownership, a nuclear deal is always a political deal. Electricity demand in most industrialised countries (the nuclear technology holders) is flat compared to the demand growth in developing countries. Hence in the near-term there will be little demand for new builds other than the replacement of retired plants. In addition, many countries are implementing renewable directives which further reduce demand for non-renewable capacity. So the nuclear industry focuses on growth markets abroad.

Building at home and wheeling electricity to neighbouring countries is a consideration of some potential nuclear projects in Eastern Europe but this faces a certain risk with regard to demand as mentioned earlier. This could be partially mitigated by assuming interests in downstream operations, i.e. transmission and distribution which extend the exporters' potential value chain.

What role will the nuclear fuel supply play in the future?

The future of nuclear energy will depend on numerous factors ranging from electricity demand, economic performance of non-nuclear alternatives and market structures to finance, government policy and socio-political preferences. Having analysed these factors globally, there is a future for the technology. Stable government policy support of the technology is key ("Yes, nuclear power is part of the country's long-term energy mix"), especially for private sector involvement and finance. How much nuclear and when, etc., should be left to the market. In addition, the industry has to continue to innovate towards better economic and improved safety.

Are there already examples of cross-border infrastructure investments from other industries that we can learn from?

The Aswan Dam in Egypt was built in the 1960s and had a significant impact on the economy and culture of Egypt. The Soviet Union provided funding as well as technicians and heavy machinery for the dam project. This was finally agreed after a long period of negotiations involving the USA, the UK and others, and also included arms for the Egyptian army.

There are other examples such as pipeline projects (the Russian Federation and Germany), or the numerous infrastructure projects China has embarked on, building roads, bridges and railways in Africa. Of course, these cross-border projects are not acts of altruism – it is all politics and strategy or as in the case of China investing in Africa, access to energy sources. ■

Johan Sörman
johan.sorman@lr.org

Hans-Holger Rogner, Ph.D.

Dr Rogner holds an MSc in industrial engineering (1975) and a PhD in energy economics (1981). For most of his career he has been engaged in comprehensive energy system analysis, energy modelling and integrated resource planning.

Until his retirement from the International Atomic Energy Agency (IAEA) in 2012, he directed the IAEA programme on Capacity Building and Nuclear Knowledge Maintenance for Sustainable Energy Development.

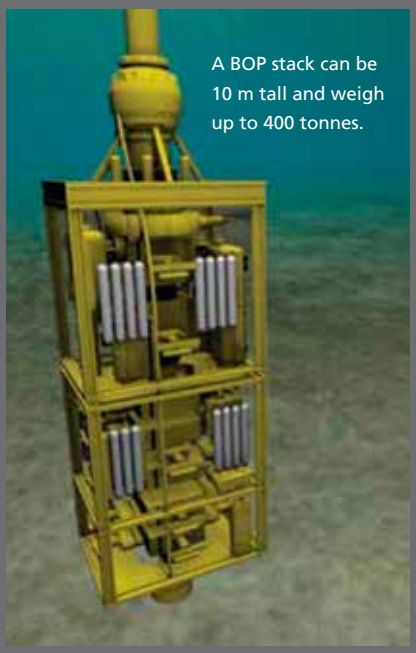
Dr Rogner holds positions of Affiliate Professor at the Royal Institute of Technology (KTH), Stockholm, Sweden, and Guest Scholar at the International Institute for Applied Systems Analysis (IIASA) in Laxenburg, Austria.

Facts

Today there are 72 new nuclear plants under construction in 15 countries and another 45 countries are considering embarking on a peaceful nuclear programme.

Safeguarding the BOP

The Lloyd's Register BOP Risk Model allows owners and operators to model the risk of their blowout preventer (BOP) – a critically important component in any hydrocarbon drilling operation – for component failure, helping to determine whether to pull the BOP to the surface for inspection and repair or not.



A BOP stack can be 10 m tall and weigh up to 400 tonnes.

The results received from the BOP Risk Model significantly reduce risk and non-productive time, both of which can prove costly to the industry and society at large. The model is a key technical and innovative first step towards risk-informed and transparent decision-making for safer drilling, as well as towards immediate and consistent communication with all stakeholders in the event of a subsea BOP equipment failure.

The BOP Risk Model is an innovative response to the Deepwater Horizon disaster, combining the LR Consulting and LR Drilling teams' extensive risk analysis experience, in-depth knowledge of the drilling industry and software applications.

The BOP Risk Model consists of a fault tree model realised in RiskSpectrum PSA and then compiled for use in RiskSpectrum RiskWatcher, a tool developed to support online risk monitoring. RiskSpectrum RiskWatcher comes in both a standard desktop version and a web version.

"As the industry looks to implement new, best-in-class offshore drilling operations, we believe we have a great deal to contribute," says Duco De Haan, SVP, Lloyd's Register Energy – Drilling. "The Energy business is breaking new ground in assessing risk by developing technology such as the BOP Risk Model. What makes this product so valuable is the quality of the data used to carry out the assessments. The ability to define the operational risk level of a BOP, including the risk effect of faulty components, is already proving to be of great benefit to the industry and society as a whole."

"The Energy business is breaking new ground in assessing risk by developing technology such as the BOP Risk Model."

Duco De Haan, SVP, Lloyd's Register Energy – Drilling

The final line of defence

A BOP is a large, specialised valve used to seal, control and monitor an oil or gas well. It can be the size of a double-decker bus and, in the case of the Macondo (Deepwater Horizon) BOP, can weigh up to 400 tonnes. It is there to prevent the uncontrolled release of oil or gas, and it is critical to the safety of the crew, the rig and the environment.

Although BOP failures are uncommon, they are far from unknown, and may be the result of electrical, hydraulic or mechanical issues. Whatever the cause, failure in such a complex system – that can control 250–375 tonnes of ram force in waters more than 2700 metres deep – may have extremely serious consequences.

Building the BOP Risk Model

The modelling of the BOP in a risk and reliability model for use in RiskWatcher BOP software includes the following steps:

1. Identify the key functions carried out by the BOP.
2. Establish the block diagrams describing the logic path identifying each main component necessary for the function to work. This is further broken down all the way until each main, minor and subcomponent needed for the function has been identified.
3. Carry out an FMEA to identify possible failures of the components and the consequences of the failures. These are then used as inputs to the BOP Risk Model.
4. Establish fault trees based on the logic block diagrams and the FMEA. The fault trees are built in RiskSpectrum PSA software. The systems, subsystems, components and failure modes are also added in RiskSpectrum PSA.
5. Compile the BOP Risk Model in RiskSpectrum PSA in a format that can be opened in RiskWatcher BOP software. The BOP risk levels can then be assessed in RiskWatcher by comparing the remaining available redundancy of the BOP capabilities with the minimum requirements in the company policy, industry standards and regulatory regulations. The minimum requirements are identified and verified by experienced BOP experts. These requirements form the basis for the "Pull" or "No Pull" signals from the BOP Risk Model.

For drilling rigs operating in the Gulf of Mexico, it is essential to comply with the following regulatory and industry requirements:

- CFR 250
- API 16D
- API Standard 53

In addition to the overall status of the BOP, the status of each of the functions and sub-functions is represented by a status bar.

Four colours are displayed in RiskWatcher software to indicate the different risk levels based on the applicable requirements and the "real-time" BOP status.

Below are examples of what the colours mean:

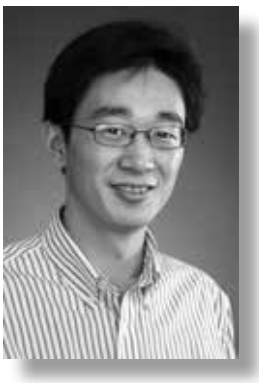
- RED: Red at the top level means that critical functions cannot be operated and that the BOP is under the minimum requirements. Critical functionality is less than 100%.
- ORANGE: Orange means loss of redundancy. A detailed risk assessment of the failure taking into account the actual risk of the drilling operation must be performed.
- YELLOW: Yellow means that at least one component in the BOP has failed. Maintenance is needed at the next available opportunity.
- GREEN: Green means everything is fine, no problems. This must be the colour when deploying the stack and after landing.

Further development – BOP Risk Model web version

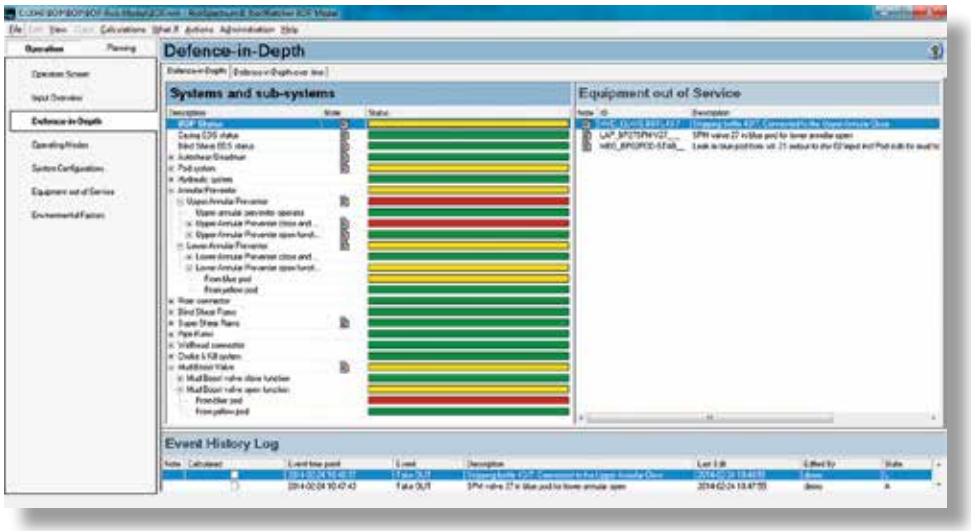
A web version of RiskWatcher software for the BOP Risk Model has been developed to enable the model to be opened via a web browser. All users with an authorised user name and password can open the model within the company intranet.

All the modelling information and event history, including the out-of-service equipment, restoration, etc., is saved on the server and made available to all users. Multiple users can open the same model and check the up-to-date BOP status.

The obvious next step is of course to include quantitative measures in the reliability model to be able to evaluate e.g. compliance with SIL levels and conditional probabilities for dropping to the next risk level (Defence-in-Depth). ■



Dr Xuhong He
Principal Consultant, LR Consulting
Xuhong.he@lr.org



BOP RiskWatcher desk-top interface. The overall BOP status in a particular configuration is yellow in the BOP Risk Model; thus drilling can be continued without pulling the BOP.

BOP Risk Model wins prestigious awards

FROM LEFT: The Rt Hon Lord Howell of Guildford; Will Greenwood MBE (former English rugby union player); Meindert Sturm, Global Business Development Manager for the LR Drilling business; and Xuhong He, Principal Consultant for the LR Consulting business.

"Our BOP Risk Model is an excellent demonstration of our deep competencies in using the world-leading risk assessment software RiskSpectrum. The recognition of the EIC award is a great encouragement to continue to improve the BOP Risk Model product and, more importantly, to apply the same technology to many other safety-critical systems across the energy supply chain," says Dr Xuhong He, Principal Consultant, Lloyd's Register Consulting.

Lloyd's Register won the EIC Award for Supply Chain Excellence 2013 for its work on Blow-Out Preventer (BOP) risk modelling for safer, better-performing deepwater drilling operations. The award was presented to Lloyd's Register at the annual Energy Industries Council (EIC) award summit, held at the Natural History Museum in London, UK, on 10 October 2013.

The EIC award recognises companies in the energy industry that have demonstrated superiority within the supply chain. Only one winner is chosen each year. Lloyd's Register received the award for its BOP Risk Model.

Lloyd's Register was also recognised at the annual Offshore Technology Conference (OTC) on 5 May 2014 by Hart Energy's E&P magazine for outstanding new technology. The BOP Risk Model earned the company a Special Meritorious Engineering Award (MEA) in the drilling category.

The MEAs are the industry's oldest and most widely respected awards annually honouring the world's best new tools and techniques for finding, developing and producing hydrocarbons. MEA entries are judged on their game-changing significance, both technically and economically, by an independent panel of experts comprising engineers and engineering managers from operating and consulting companies worldwide. ■

Celebrating 30 years in the business of safety

"We now employ the creators and developers of the two most successful PRA software programs, namely RiskSpectrum and RiskMan."

It feels like just yesterday that I wrote an article about the 25th anniversary of our operation. While the content of the article is obviously still valid, it needs to be supplemented with events from the last five years.

During this period one event dominates all the others: Lloyd's Register – a UK-based enterprise with an over 250-year history – acquired Scandpower in its entirety, including the Swedish operation Relcon Scandpower. From one day to the next we became a member of a global organisation with operations in some 200 countries and around 8,000 employees. Becoming a member of Lloyd's Register has opened up new opportunities for our operation, while at the same time creating new challenges.

Woody Epstein, 1984 edition

We have become much more international, particularly in consultancy – our software business has been international for decades. Our consultants are now active all over the world. Our base of consultants has increased considerably through the acquisition of a PRA-oriented company in India. Our nuclear consultants there are now active in Switzerland and Belgium, while at the same time expanding the India business into new areas, especially oil and gas.

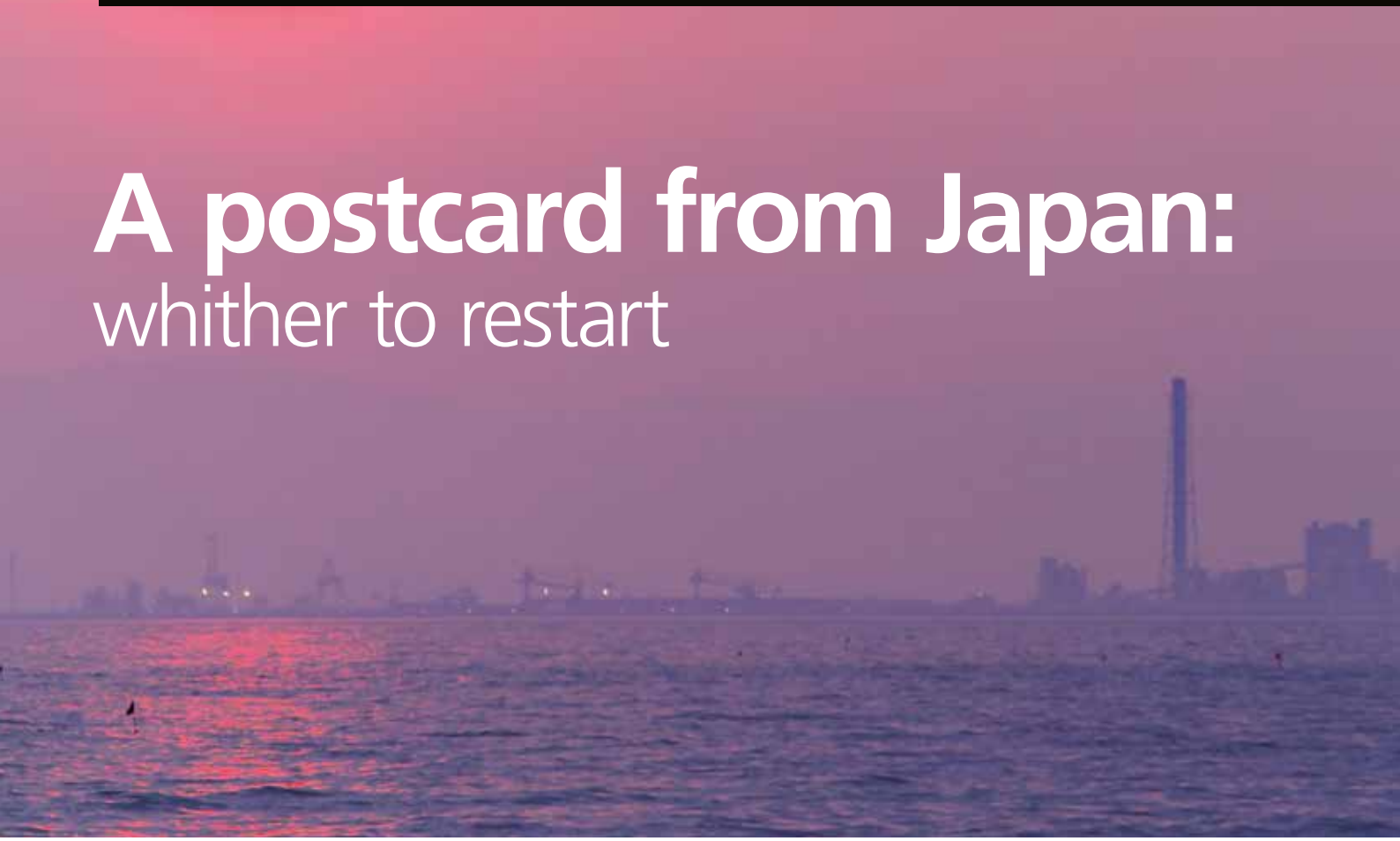
Our operation in Japan is led by Steve "Woody" Epstein, with considerable success in both software and consultancy. It is interesting to note that with Woody in our organisation we now employ the creators and developers of the two most successful PRA software programs, namely RiskSpectrum and RiskMan. The first versions of both software were released in 1986. Woody claims that RiskMan was released just a few weeks before RELTREE (the predecessor of RiskSpectrum); however, we know that it was the other way around. In the photo you can see a young Woody working hard at developing RiskMan software.

In Japan we have been involved in a number of post-Fukushima activities, targeting seismic evaluation of safety at closed NPPs as part of the restart process. We were one of the first experts admitted to affected plants in order to evaluate the consequences of the earthquake and following tsunami. Our evaluation indicated that the plant withstood the earthquake without any noticeable damage to the safety-related systems and structures, which is quite interesting given the very powerful magnitude of the earthquake.

In other articles in this issue you can read about new RiskSpectrum products, in particular the BOP Risk Monitor for oil and gas operations and the web-based version of RiskSpectrum RiskWatcher, which was developed in close cooperation with our partners in China and is already in use there.

As you can see, the past five years have been quite intensive and eventful. It is my hope that the coming 30 years will be just as successful and interesting. ■

Jerzy Grynblat
Nuclear Business Director, Lloyd´s Register
jerzy.grynblat@lr.org



A postcard from Japan: whither to restart

In February 2011, Lloyd's Register Consulting (LR Consulting) began operations in Japan. No sooner had our business plans for the year been completed, than the Great Eastern Japan Earthquake and Tsunami occurred and the subsequent disaster at Fukushima began to unfold.

As the nuclear power industry worldwide waited, a distinct lack of information was forthcoming from Japan in those early days of the crisis. One of our customers, EdF Energy UK, commissioned the LR Consulting Japan office to write a confidential report on the events at Fukushima Daiichi. The report, entitled "Research and Analysis behind the Events in Japan, 11 March 2011: The Fukushima Daiichi Nuclear Accident", was delivered to EdF Energy in June 2011. The 28,000 word report was heavily researched including interviews with leading nuclear experts in Japan, prominent members of the world media, and workers who had been at Fukushima Daiichi. Even though several books and reports have been written in the three years since the accident, the LR Consulting report has proven to be extremely accurate in its analysis.

The first year after the accident proved to be a difficult time for nuclear business in Japan. The Japanese Prime Minister, Naoto Kan, requested Chubu Electric to voluntarily close the Hamaoka NPS since reports indicated the significant likelihood of another magnitude 9 earthquake occurring elsewhere in Japan, this time on the Nankai Trough facing the Hamaoka plant. The reports stated that if a 9.0 earthquake occurred on the Nankai Trough, the effects would be serious. The earthquake itself would likely kill thousands, and a series of 34-meter tsunamis would impact areas from the Kanto Region to Kyushu, adding thousands to the death toll, and destroying areas with large populations. Moreover, it would severely impact the Hamaoka NPS. Chubu Electric complied with the Prime Minister's request.

All plants shut down

Prime Minister Kan, and his successor Prime Minister Noda, instituted stress tests which were required by all nuclear power plants. As plants went offline for

"Even though several books and reports have been written in the three years since the accident, the LR Consulting report has proven to be extremely accurate in its analysis."

The D1 shatter zone excavation at the Tsuruga NPS.

periodic maintenance, they would not be allowed to go back online until they passed the stress tests. By the summer of 2011, almost all nuclear power plants in Japan, including those affected by the earthquake and tsunami, were shut down, with the few remaining facing indefinite closure when they, too, went offline for maintenance.

Stress tests and approval before restart

Under the two-phase stress tests, utilities were required to examine the safety margin of important pieces of equipment in accordance with guidelines set by the Nuclear and Industrial Safety Agency (NISA) and the Nuclear Safety Commission (NSC). Based on the results of these initial tests, carried out while the units were shut down, the government would decide whether a reactor can or cannot resume operation. Even with a go-ahead from NISA, utilities would still require approval from local prefectural governments. Although not a legal requirement, the deference traditionally shown by utilities to local officials is socially mandatory.

Kansai Electric's Ohi unit 3 was the first Japanese nuclear power plant to complete the first step of the mandatory stress tests in October 2011. In February 2012, NISA endorsed the results of the stress tests at two nuclear power reactors, Ohi 3 and 4, clearing the way for their possible restart. They would be the first, and only, reactors to restart following stress test inspections when they received both national and local government approval.

And then the game changed again

The Nuclear Regulation Authority (NRA) was formed to take the place of the NSC, which was under the authority of the Prime Minister's office, and NISA, which was under the Ministry of Economy, Trade and Industry (METI). After the Fukushima nuclear disaster the government's safety measures were seen as inadequate. Also, NISA being under the umbrella of METI, which was responsible for promoting the use of nuclear power as well, was seen as a conflict of interest. As a consequence, the NRA was established on September 19, 2012 under the Ministry of the Environment and according to the new establishing law, the task of working out new nuclear safety rules would have to be completed by the summer of 2013.

The stress tests disappeared as a criterion for restart. As the Ohi units 3 and 4 reached their time for periodic maintenance, they, too, were once again shut down. By New Year's Day 2014, Japan was again left without nuclear power.

▷

Lloyd´s Register supports Japan

During the last three years since the accident at Fukushima Daiichi, LR Consulting has not been idle. We have been doing our best to help both the people of Japan and the country's nuclear industry.

The F3 fault excavation at the Higashidori NPS.

Our parent company, Lloyd's Register, has had several employees regularly volunteer in the Tohoku area. I have been volunteering in the village of Watari in Tohoku helping children in evacuation centers and in the village of Minami-soma, just some 25 km north of Fukushima Daiichi. Lloyd's Register donated USD 50,000 to the village of Minami-soma after the tsunami to help with reconstruction.

Lloyd's Register also partially funded the IAEA Mission to the Onagawa NPP with USD 250,000 to cover the time and expenses of our five experts who took part in the earthquake and tsunami walk down.

As one would expect, natural hazard risk assessment is one of the primary concerns of Japanese nuclear power plant operators. LR Consulting has been actively involved with earthquake issues in Japan. In 2013, we brought experts from several countries to make independent third party investigations at Japan Atomic Power Company's Tsuruga NPS and Tohoku EPCo's Higashidori NPS concerning the possible activity of identified faulting. We are now beginning, with our partner, Paul Rizzo Associates, probabilistic fault displacement hazard analyses (PFDHA) with clients in Japan.

Japan has also begun to embrace probabilistic risk assessment (PRA) as an important method to analyze the safety of the plants seeking permission to restart. This year, two important meetings took place focusing on PRA: the USA-Japan PRA Roundtable and the Japan Nuclear Safety Institute's Annual Meeting. I was a member of the US delegation to the Roundtable and speaker at JANSI meeting.

RiskSpectrum user group is growing

And the RiskSpectrum® family of software has now become the PRA tool of choice in Japan. Our users include Hokkaido Electric Power Company, Tohoku EPCo, TEPCO, Kansai Electric Power Company, Shikoku Electric Power Company, Kyushu Power Company, and the Japan Nuclear Fuel, Ltd. reprocessing facility.

We have now also created a new software tool, the Extreme Event Analyzer (see also PSAM 12 paper #459 "Method for Analysing Extreme Events"), which aids analysts in quantifying the impact of extreme external events on facilities.

We hope that we can continue to help Japan, and the world, in safe and responsible use of nuclear power. ■

Woody Epstein
woody.epstein@lr.org

Nuclear outlook in Japan

Since the new regulations have come into effect, eight power firms have requested safety inspections to allow the restart of 17 reactors at 10 power stations. Two of Kyushu Electric's reactors at the Sendai NPP have been fast-tracked for restart by the NRA and a decision is expected sometime this summer.

Of Japan's remaining 48 reactors, 14 will probably be restarted at some point, a further 17 are uncertain and 17 may never be switched back on, if one takes into account the age of the plants, nearby possibly active seismic faults, additional work needed to address safety concerns, evacuation plans, and local political opposition.

As a result, nuclear energy may make up less than 10% of Japan's power supply without new builds.

RiskSpectrum MCS BDD

A sign of the times

Classic MCS quantification methods like MCUB and 1st, 2nd, 3rd approximation are effective and efficient, but they also have obvious drawbacks, such as overestimation of the top results, especially in connection with high probability events. Another problem is the treatment of success in sequence and consequence analysis.

The MCS BDD algorithm has therefore been developed as part of the RiskSpectrum software suite to improve quantification of the top results in the MCS list.

A binary decision diagram (BDD) is a data structure that is used to represent a Boolean function.

Source: Wikipedia

Why an MCS BDD?

Now I'm sure you're asking yourself, "Why do I need a fifth way of calculating my CDF?!"

This is basically a very sound reaction, and in most situations you will not need better accuracy in the quantification of the results, especially consequence results. However, there are situations that may call for higher accuracy in the calculations.

There are basically two reasons why you would want higher accuracy:
a) If the results include a lot of high probability events.
b) If the success paths in the event tree sequences have an impact on the result.

These days, with more and more emphasis on seismic analysis, Level 2, fire analysis, etc., your PSA model is producing more high probability events in the MCS list. In most cases these are treated very accurately by the MCUB calculation. However, if there are many high probability events, the results may be conservative. One example here is seismic analysis at high PGA, where a lot of equipment may have a high failure probability. Using MCS BDD will also address potential problems when calculating RIF for a group of events (with regard to high probabilities).

Studying success paths in the event trees may be relevant when the failure probability for a top event (function event) is significant, particularly when the sequence path is important. Such situations may be relevant in, for example, a PSA Level 2, where you are actually interested in all the sequences – not just the failure sequences. It is also relevant for seismic analysis that is transferred into PSA Level 2. RiskSpectrum PSA already offers the possibility to perform "simple quantitative" treatment of success paths. This method may, however, be too conservative if it is applied generally, for two main reasons:

- The simple success module introduces new high probability events.
- The simple quantification of success paths may be insufficient if there are significant dependencies between failure and success paths.

The quantification within the MCS BDD solves both of these issues, as it handles the high probability issue and ensures that the quantification of the success path is correct (no longer quantified separate to the quantification of the failure path). The success path is actually merged with the BDD representing the failure path.

So, the answer to your initial question is: You won't normally need this possibility, but there may be situations in which you want to make sure that you don't need it or situations in which you would benefit from using it. ■

Ola Bäckström
ola.backstrom@lr.org

How is the BDD built?

So I have my MCS list and now I want to use the RiskSpectrum MCS BDD. How does it work, Pavel?
Here is how a MCS list can be quantified using a BDD. First you have to pick a pivotal element.

What is that?
A pivotal element is a basic event that you can find in the MCS list. Let's take basic event A. This event is then assumed to be TRUE and the MCS list is re-minimised. Next, you assume that A is FALSE and re-minimise the MCS list again. Now you have two MCS lists, one with A=TRUE and the other with A=FALSE. Then you pick a new pivotal element, e.g. basic event B, and set it first to TRUE in the two MCS lists and then to FALSE. Now you have four MCS lists with combinations of A and B set to TRUE and FALSE. Then you just continue to pick new pivotal elements and set them to TRUE and FALSE until you end up with an MCS that is either TRUE or FALSE.

So let´s say I have a fault tree that generates the MCS:
AB
AC
CD
How would this look in a BDD?

Pavel continues: Have a look at Figure 1. The first pivot element chosen is basic event A. It has been added in node 1 (n1). If we choose to move along the left line from A, we assume that A=TRUE, and if we move to the right, we assume that A=FALSE.

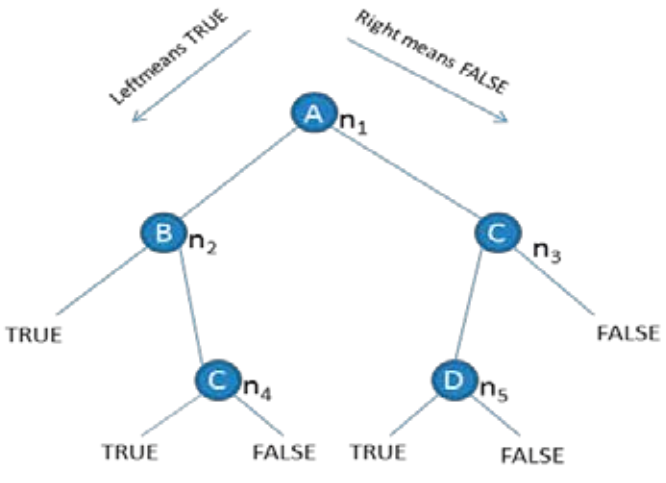


Figure 1. An example of basic events inserted in nodes in a binary decision diagram (BDD).

In Table 1 below you can see the MCS lists that are saved in the nodes.

MCS	n1	n2 A=TRUE	n3 A=FALSE	n4 A=TRUE B=FALSE	n5 A=FALSE C=TRUE
	AB	B	CD	C	D
	AC	C			
	CD				

Well, this seems easy enough. How is the BDD used for calculating the top event frequency or probability?
The calculation is done using a recursive algorithm that looks like this:

P(n1) = P(A) * P(n2) + (1- P(A)) * P(n3)
P(n2) = P(B) * TRUE + (1- P(B)) * P(n4)
P(n3) = P(C) * P(n5) + (1- P(C)) * FALSE
P(n4) = P(C) * TRUE + (1- P(C)) * FALSE
P(n5) = P(D) * TRUE + (1- P(D)) * FALSE

This yields:
P(n1) = P(A)* P(B)+P(A)* (1- P(B)) * P(C)+ (1- P(A))* P(C)*P(D)
And this formula is used for calculating the top event for the MCS list that you have created. ■

Pavel Krcal
Senior Software Developer
Pavel.krcal@lr.org

How is the MCS BDD implemented in RiskSpectrum?

RiskSpectrum Magazine asked Wang Wei, project manager of the MCS BDD development project, how the MCS BDD is implemented in the software.

When we release the RiskSpectrum MCS BDD you will find an option to include BDD generation and calculation in the Analysis Case in RiskSpectrum PSA.

The algorithm in RiskSpectrum MCS BDD uses a pivotal decomposition method to build the BDD structure from an MCS list the way Pavel explained. By continually picking pivotal elements from the MCS list both failure and success branches are further developed. When all the branches have reached a fixed state, the complete BDD structure is generated. The key process of building the BDD structure is to select the pivotal element from the remaining MCS list and append it to the branch of the current pivotal node under construction.

Backtracking has to be performed before selecting the next pivotal element in order to get all the pivotal elements along the backward path. Then the MCS list can be minimised against the state of these elements.

But the development does not stop here. We also have more things to consider when generating a BDD from an MCS.

In order to reduce the amount of computation to a practical scale, we have made it possible to define a threshold in the MCS list so that the part of the cutsets below the threshold can be evaluated with an ordinary MCS quantification, e.g. MCUB. The algorithm to create the BDD is focused on the part of the MCS list above the threshold in order to quantify the result precisely. The results of the two parts are then summed up with the MCUB method to ensure a conservative top result.

Frequency events, usually as initiating events, and success modules are considered mutually exclusive. Success modules are combinations of events that represent successful paths in an event tree. It is possible to split the MCS list into different, mutually exclusive groups and solve each group individually. This can greatly reduce the scale of the problem, as the top result can be calculated by a direct accumulation of the results of each separate group.

Instead of building a complete BDD for the whole sequence, we can build one main BDD structure for the sequence MCS list without success modules, as well as another BDD for the success module itself. At a later stage, the success module BDD can be appended to and merged with the main BDD to get a full representation of the logic of the sequence.

The order of the pivotal elements makes a great impact on the size of the BDD structure. A dynamic ordering method has been chosen to select new pivotal elements from the remaining MCS list with multiple principles, e.g. number of event occurrences, cutset order, etc., which allows for a more concise BDD structure to be obtained. The algorithm will also try to group events together in modules to simplify the BDD structure. The modules are detected and created during the runtime based on the actual MCS list. ■

Wei Wang
Senior Software Developer
Wang.wei@lr.org

Software update

RiskSpectrum user group meetings

The place where ideas are born…

The annual RiskSpectrum Users Meetings in London and Beijing continue to draw 30–40 participants each year. In April 2014, we held the 14th user meeting in Germany. This annual meeting is hosted by AREVA and attracts some 10–15 participants each year.

Since the release of RiskSpectrum PSA in 2008, we have produced many new updates with added functionality. Many of these updates are the result of discussions and interactions at the meetings. It is a real pleasure for us to go to the meetings and deliver news of the many new sought-after features.

…and then realised

Since the PSAM 11 issue of RiskSpectrum Magazine was published in 2012, many new features and tools have been incorporated into RiskSpectrum PSA. These include:

- A fault tree transfer viewer;
- A brand-new MCS Editor;
- RiskSpectrum HazardLite – a tool for simplifying modelling of hazards, and seismic hazards in particular, in RiskSpectrum PSA;
- Improved multi-threaded analyses for RiskSpectrum PSA and RiskWatcher.

RiskWatcher Web has now been released and delivered, as has RiskWatcher BOP for monitoring risk levels on offshore drilling rigs. Read more about RiskWatcher Web in a separate article in this magazine and visit www.lr.org to learn more about the BOP Risk Model.

We have a lot more in store for the future. We are planning to release the following in not too long:

RiskSpectrum MCS BDD: read more in a separate article in this magazine and see also PSAM 12 paper #456 "Quantification of MCS with BDD, Accuracy and Inclusion of Success in the Calculation – the RiskSpectrum MCS BDD Algorithm".

RiskSpectrum PSA 1.3: a major upgrade with many new features:

- Event Tree transfer viewer;
- Event Tree "jumps";
- CheckModel;
- CCF Alpha staggered.

CompareModel: for comparing two PSA models.

Cutset tracer: for determining which sequence or fault tree path generates a particular cutset.

RiskWatcher BOP Web.

Read more about some of these new tools on pages 28-29.

In the past year, we have also been working on a project with the International Atomic Energy Agency (IAEA) to develop software for analysing extreme events based on a PSA model in RiskSpectrum PSA; see PSAM 12 paper #459 "Method for Analysing Extreme Events". ■

Johan Sörman
johan.sorman@lr.org

RiskWatcher Web sees the light in the Middle Kingdom

In 2011 risk monitor projects were launched at two Chinese nuclear power plants (NPPs) – Tianwan and Qinshan Phase II. The plants had selected web-based RiskSpectrum RiskWatcher (RiskWatcher Web) to support their risk-informed PSA applications. After three years of hard work by a program team led by senior software programmer Mr Wei Wang, RiskWatcher Web is now up and running at the two plants. This is the first plant application of the RiskWatcher Web program, and its success truly represents a giant stride in the history of risk monitor software.

Mr Jerzy Grynblat, Nuclear Business Director of Lloyd's Register Consulting (LR Consulting), has been a facilitator in realising the project. "The two projects are the result of our long-term commitment and close relationship with the Chinese nuclear industry, especially with our partner China Nuclear Power Engineering Company (CNPE), with whom we signed a cooperation agreement in March 2010," he explains. "Together we are seeking to deliver more products and services to the nuclear industry in China."

Mr Bo Zhao, Deputy Chief Engineer of CNPE, says, "I'm glad to see RiskWatcher Web software being successfully implemented for risk-informed PSA applications at the two plants. Both are pilot plants for PSA applications in China and the software is a very important tool for supporting their activities. I'm looking forward to seeing more applications in the Chinese nuclear industry."

Mr Jinlong Sun, PSA Division Leader of CNPE, comments, "We have cooperated closely with LR Consulting's China office and Stockholm office on the development of the living PSA models for the two plants. The models have been developed and maintained in RiskSpectrum PSA, thus they fit the RiskWatcher Web software very well. Through these projects, we have developed our in-house competence at CNPE, paving the way for more cooperation with LR Consulting in the future."


RiskSpectrum RiskWatcher is available in many languages.

The RiskWatcher Web has many advantages compared to traditional desktop tools:

- **It is easy to deploy, maintain and update.** All the deployment and maintenance work is conducted on the server side only. All users need to access the application is a standard web browser. This is very important in promoting the use of this PSA application by all staff at the plant.
- **Improved traceability.** Web applications are more traceable, as all data is centralised on the server side. Every user request is sent to the server and logged.
- **Multi-user application.** The RiskWatcher Web is a natural multi-user application. It is easy for multiple users to collaborate, as all data is centralised. Multiple users can access the same model data and plant configuration information at the same time, and can simultaneously perform many standard functions on the same model dataset without affecting other users or their data. These standard functions include, but are not limited to, viewing risk profiles, tracing operation logs, performing individual what-if analyses, printing reports, etc.
- **Stronger and scalable computing capability.** Calculation speed is very important since there may be many concurrent calculation requests. Series of measures have been taken to improve the performance of quantifications in the RiskWatcher Web. Calculation is performed asynchronously, thus the risk profile can be refreshed when calculation is finished. An intelligent scheduling algorithm has been adopted to manage the calculation resources more efficiently. Previous calculations can be re-used intelligently. In addition, calculation capability can be extended by increasing calculation cores and servers.
- **Easier end-user customisation, including user interfaces and functions.** RiskWatcher Web can be easily customised to support plant-specific needs for functionalities and interfaces. It has an effective interface with the plant's existing information system.
- **Easier input.** RiskWatcher Web can read information directly from the plant's maintenance plan system. It can even automatically update plant status from the plant information system (with user approval). A PI2RW module has been implemented in the Tianwan project that can read the plant information system every 10 seconds and update the RiskWatcher Web event log. If there is any change in plant status, calculation will be started. ■

Dr Xuhong He
xuhong.he@lr.org

Mr Hao Zheng
hao.zheng@lr.org

DSA vs. PSA

Why DSA and PSA are complementary

This article is an attempt to show, in a very simplified and basic manner, why two types of analyses – deterministic and probabilistic – are required in the design process for nuclear power plants (or other facilities) when the overall safety, or the overall risk, is considered. In addition to our work and experience, we have witnessed many instances of a "rivalry" between the proponents and practitioners of the two types of safety analyses. Long, fruitless discussions on the subject of which of the two approaches is "better" have in most cases been fuelled by some misunderstanding of the respective roles of the two approaches, which are actually complementary.

At the very beginning of this kind of consideration, an appropriate technical definition is needed for a quantitative measure of the "overall safety". One of the arguably best ways to present it is through its inversion: the "overall risk", which, in an engineer's terms, is quantitatively defined by the well-known" risk curve" shown in Figure 1.

Based on Figure 1, the overall risk is defined by the area below the risk curve, i.e.:

$$R = \int_0^\infty \left| C(P_E) dP_E \right|$$

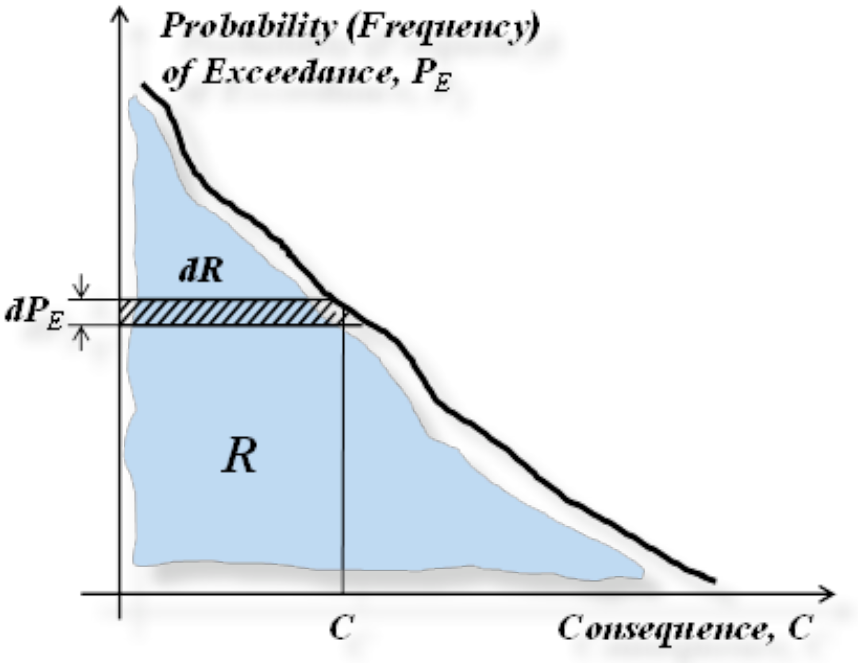


Figure 1: Risk curve or definition of risk for an engineer.

Two points regarding Figure 1 are worth noting:

1. The risk curve is defined in terms of a probability (or frequency!) of exceedance, which mathematically implies that it is a monotonously decreasing curve;
2. The simplistic formula "Risk = Probability x Consequence" (which can be found in handouts from numerous training courses on risk assessment for engineers) is valid only for a class of events with same consequence, where the term "probability" represents a probability of occurrence of an event in the class (for which it can be shown that it is a differential of a probability of exceedance, i.e.: $\Delta R = C \Delta P_E$).

From Figure 1 it can be seen that the purpose of the "safety management" or "risk management" basically is to minimise the area below the risk curve, or to suppress its "belly" as much as (practicably) achievable. This is illustrated in Figure 2, which also shows the two basic and most obvious principles of risk/safety management.

A simple example of principle a) could be: if an area contains ignition sources, then move away or minimise the presence of combustibles (to minimise potential consequences of an ignition). This can also be rephrased to represent an example of principle b): if an area contains combustibles, then move away or minimise the presence of ignition sources (to minimise the likelihood of an ignition).

In the real world neither consequences nor incredible scenarios can be completely eliminated. It should therefore be clear

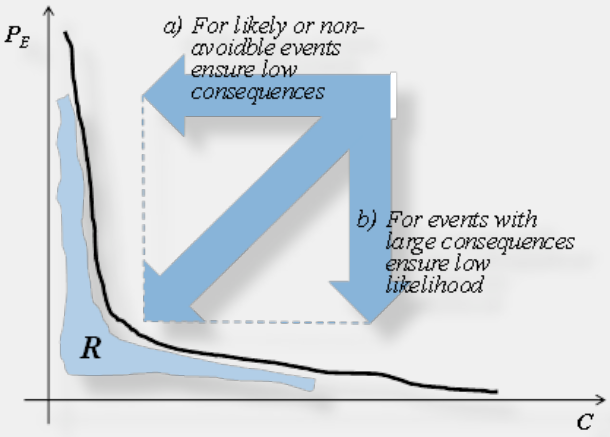


Figure 2: Two basic principles of safety/risk management.

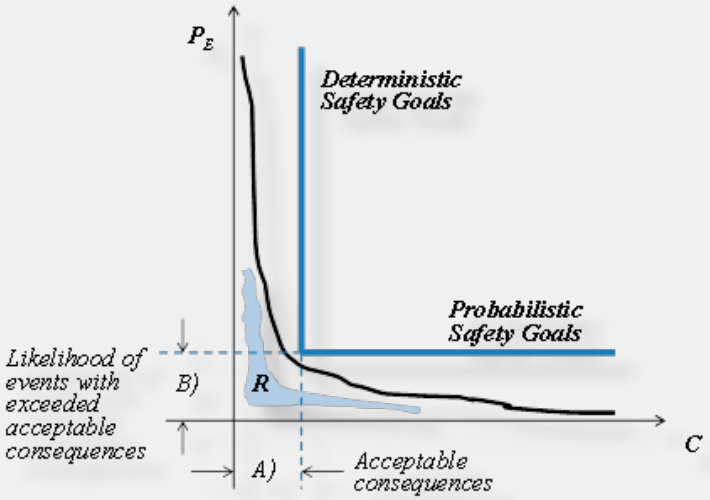


Figure 3: Usually, optimized risk reduction is achieved through combining deterministic and probabilistic safety goals.

that an enforcement of safety/risk management as illustrated in Figure 2 is only possible with two different sets of safety goals in the risk space. These safety goals are: A) deterministic and B) probabilistic, as indicated in Figure 3. It is only possible to demonstrate compliance with safety goal A) through a set of deterministic safety analyses. This is the case because the required analyses have to demonstrate by calculation the consequences (e.g. maximum pressure, maximum stress, maximum temperature, maximum exposure to radioactivity, etc.) resulting from the postulated events and conditions.

On the other hand, it is only possible to demonstrate compliance with safety goal B) through a set of probabilistic safety analyses. In this case, it is simply because the required analyses have to provide a calculation of likelihood (i.e. probability or frequency) for all the initiating events and scenarios for which the consequences were not demonstrated to be acceptable.

To continue with previous example: if strategy a) was selected and the presence of combustibles reduced but not eliminated, then it must be deterministically demonstrated that release of energy from the remaining combustibles in case of a fire would not exceed safety goal A). If strategy b) was selected and all combustibles retained (so that it is obvious that safety goal A) cannot be achieved), then it must be probabilistically shown that the likelihood of combustion due to the presence of ignition sources is such that safety goal B) is complied with.

To conclude on the basis of the above discussion, the overall process of "design for safety" would include the following stages:

1. Design postulation and development;
2. Design basis analyses to demonstrate that safety goals of type A) are met (deterministic safety analyses);
3. Design risk analyses to demonstrate that safety goals of type B) are met (probabilistic safety analyses);
4. Loop back and iterations, if required. ■

Ivan Vrbanic and Ivica Bašic at a plant walkdown, in the auxiliary building at the Krsko NPP. The walkdown was performed for the purpose of updating the internal flooding PSA to address observations from the periodic safety review.

Ivan Vrbanic
APoSS d.o.o., Croatia
ivan.vrbanic@zg.t-com.hr

Ivica Basic
APoSS d.o.o., Croatia
basic.ivica@kr.t-com.hr

Risk monitor recommended for Leningrad nuclear power plant

RiskSpectrum RiskWatcher has been implemented for trial at the Leningrad Nuclear Power Plant (LNPP) to transfer PSA-based decision-making technology to technical management.

This article is a summary of the technical paper "PSA applications and risk informed approaches. Introduction of risk monitor technology at the Leningrad NPP, challenges and experiences", authored by Sergey Kukhar and first presented at the Castle Meeting in Sweden in 2011.

The wide-ranging experimental work of implementing a risk monitor based on RiskSpectrum PSA and RiskSpectrum RiskWatcher software from Lloyd's Register Consulting at LNPP Unit 1 was carried out during the period 2007–2008, in accordance with a decision by Rosenergoatom.

The purpose of the risk monitoring system is to:

- Assist the technical control operators to exclude hazardous maintenance configurations of the power unit;
- Support maintenance planning and checking equipment availability, taking into account the current risk information;
- Define and assess the accident precursor events;
- Assess AOTs in current configurations based on safety assurance conditions.

Recommendations of use

With a number of directives and protocols in place, it was possible for LNPP staff to start testing the PSA model, which was expanded with modelling for risk monitor purposes and compiled for use in RiskWatcher. Based on their findings, a number of recommendations were compiled.

Here are a few of them:

- It is necessary to perform calculation including the entire model.
- A shutdown model should be used after a reactor's successful shutdown.
- An indicator of relative risk values should be defined and have a determined allowed maximum.

Findings regarding AOT

Two tasks were formulated with regard to Allowed Outage Time (AOT) calculations:

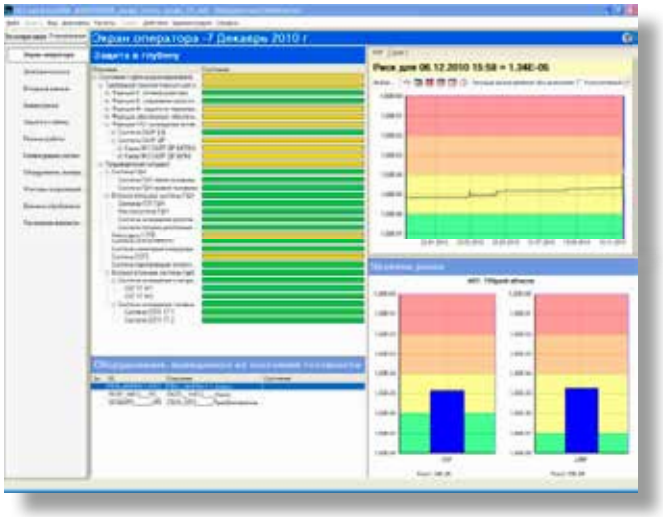


Figure 1. Risk monitor in trial operation at LNPP Unit 1 Main Control Room.

- Assess AOT for several configurations using the RiskWatcher and Unit 1 risk monitor model;
- Compare calculated AOT values with AOTs stated in the technical specifications for Unit 1 for the appropriate configurations.

One hundred and six equipment configurations of LNPP Unit 1 were analysed. These included combinations of unavailable equipment in the reactor cooling systems, service water supply pumps and diesel generators.

As a result of the AOT calculations, it was possible to identify some configurations in the technical specifications that were too conservative and others that were too optimistic. The results obtained showed that there are configurations with no limiting conditions of operations, called "While in planned maintenance", which the risk monitor indicates with noticeable risk; i.e. the technical specifications are too optimistic. To be more exact, 12 of the 106 configurations indicated that the AOTs based on the technical specifications were too optimistic and 14 were too conservative.

Facts:

Sosnovy Bor (Russian for pine wood or pine forest) is a town in Leningrad Oblast, Russia, situated on the southern coast of the Gulf of Finland, 81 km west of St Petersburg. Population: 66,132 (2002 Census). Very high percent of people with higher education.

The town was founded in 1958 as a settlement serving the Leningrad nuclear power plant, and received town status in 1973.

The town is known not only as an "atomic city", but also for its research institutes and building industry. There are about five hundred large, medium, and small enterprises functioning in the town; many of them are technologically oriented.

The city also has nice beaches – a big sandy one with shallow water, which is good for children, and one with sand, rocks and pine trees. A section of the latter is a nude beach. Although situated at the seaside, the city itself has no quays, and is separated from the Gulf of Finland by a forest, which protects it from storms.

Source: www.cityphotos.info

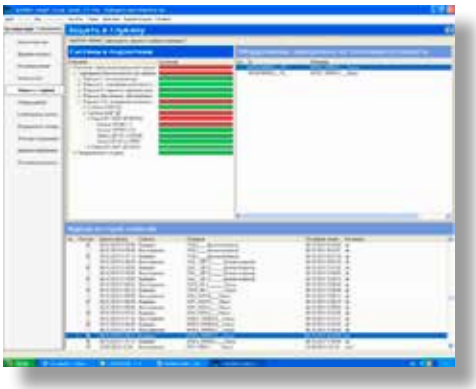


Figure 2. Defence-in-depth evaluation for two small feed water (MPEN) pumps in one group.

The comparison was carried out by defining the defence-in-depth model in RiskSpectrum RiskWatcher based on the technical specifications. For the prohibited and limited configurations specified in the technical specifications, the defence-in-depth colour changes to red in the RiskWatcher defence-in-depth view. All other configurations with no limiting conditions of operations according to the technical specifications stay green.

The AOT was then calculated in RiskWatcher for each configuration that indicated limiting conditions of operations according to the defence-in-depth display and compared to the AOT as stated in the technical specifications.

Accumulated risk for regulatory compliance

The paper also demonstrated how employing the cumulative calculations of e.g. CDF and the defence-in-depth view based on regulatory compliance could be used for risk-informed planning to take equipment out of service (technical maintenance).

Figure 3 shows the cumulative risk calculations for three different scenarios:

Black line: All tests are successful, i.e. no malfunction is detected.

Blue line: The technical specifications' safe operation requirements are met, but the test's schedule has been violated.

Red line: The technical specifications' safe operation requirements have been violated, but the routine safety systems testing schedule has not been breached.

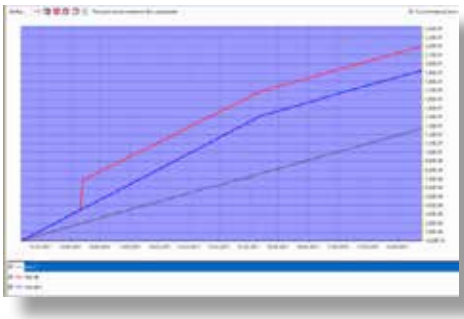


Figure 3.The cumulative risks for three different tests schedules for the reactor cooling pumps.

Depending on the risk criteria set at the plant, both the blue and red options may be acceptable with regard to the cumulative risk criteria.

To conclude

The paper concludes that the approach used for the trial implementation of a risk monitor at LNPP was successful. It is recommended that a risk monitor is implemented at LNPP Unit 1 and then extended to other power units. Developing the LNPP PSA to include start-up and shutdown modes of operations is also recommended, as is developing the PSA Level 2 for all operating states.

LNPP should take part in the further development of procedures and decision-making documents, taking into account the results generated by the risk monitor. ■

Johan Sörman
johan.sorman@lr.org

Justifying maintenance in operation at Kozloduy

From 2012 to 2013, the PSA model at the Kozloduy Nuclear Power Plant (KNPP) in Bulgaria was adapted for RiskSpectrum RiskWatcher. Lloyd's Register Consulting was chosen to help the PSA team at the plant to complete the work and launch the risk monitor implementation programme at KNPP.

RiskSpectrum Magazine asked Mr Emil Kichev, head of the PSA team at KNPP, to tell us a bit about the reasons for investing in a risk monitor and how and for what purposes they use it at the plant.

Risk monitoring was developed within the framework of the project for maintenance optimisation of Unit 5 and 6 (WWER-1000) at Kozloduy NPP. The project was one of many steps taken by the Kozloduy NPP management to achieve a high safety level and competitive operation in a deregulated electricity market in Bulgaria. The deregulated electricity market was planned for introduction in 2007.

The main goal of the project was to justify a reduced duration of the units' outage without compromising safety, by means of optimisation of maintenance, an in-service inspection programme (ISI), test intervals and equipment Allowed Outage Time (AOT).

Since 2005, the KNPP PSA Level 1 has been updated twice. In the RiskWatcher implementation project, the PSA Level 1 model including full power and low power operation and shutdown mode for internal events, internal floods, internal fires and seismic activity was adapted for use in RiskWatcher. The Bulgarian Nuclear Regulatory Agency (NRA) requires that a PSA Level 1 and PSA Level 2 are developed and maintained for continued licence to operate the units. There are also NRA guidelines describing the areas of application of PSA. One of the tools for ensuring safe operation of the units is risk monitoring but the development of a risk monitor is not obligatory. The decision to invest in a risk monitor is one taken by the KNPP management on its own.

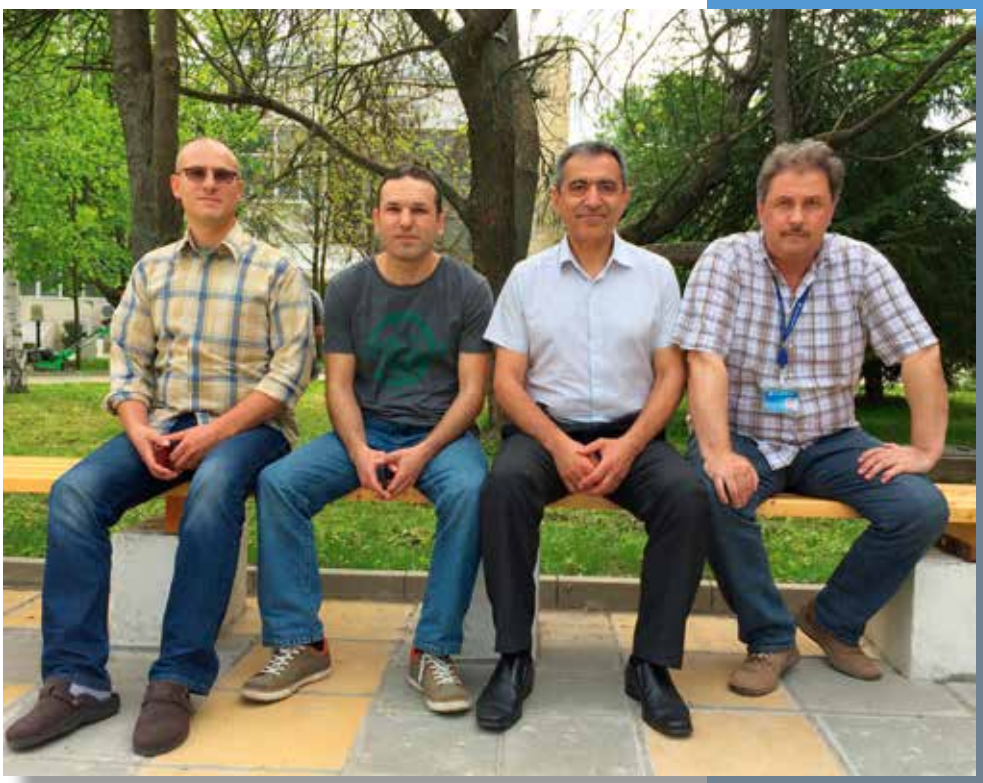
RiskWatcher is used for calculating the risk profile, and this information is used for justification of equipment maintenance scheduled in the unit's outage. RiskWatcher is also used for supporting decisions to take equipment out of

"Today we can use RiskWatcher for quickly justifying a maintenance schedule for equipment included in the unit's outage or at power."

service in limiting conditions of operations and calculating the relevant AOT. One example is maintenance of the service water system (support safety system, called QF – three trains, six pumps). It is included in each unit's annual outage in the original scheme (shutdown mode). However, for a couple of years, maintenance of QF has been done at power (before the annual outage). This takes between five to 15 days, depending on the type of maintenance. The decision to do this was supported using the results of the probabilistic assessment too, including calculation of risk profile at power with and without one train of QF available.

There are also some nice features in RiskWatcher that we did not initially foresee. The cumulative risk calculations for comparing two or more risk profiles are useful when planning outages. The combination of quantitative and qualitative risk calculations (defence-in-depth) for making risk-informed decisions has proven to be very useful for us as well. ■

Emil Kichev
ESKichev@npp.bg



The PSA team at Koxloduy NPP - from left to right; Plamen Naydenov, Emil Stefanov, Emil Kichev, Krasimir Atanasov

Emil Kichev was appointed risk management section manager at the Kozloduy Nuclear Power Plant in 2005. However, he started working at KNPP as far back as 1984 as a reactor engineer and unit shift supervisor.

The PSA team is responsible for updating the PSA and its application and for supporting the decision-making of the KNPP management concerning safe operation of the units at KNPP.

Facts on Kozloduy NPP

The Kozloduy Nuclear Power Plant is a nuclear power plant in Bulgaria situated 200 km (120 miles) north of Sofia and 5 km (3.1 miles) east of Kozloduy, a town on the Danube river, near the border with Romania. It is the country's only nuclear power plant and the largest in the region. The construction of the first reactor began on 6 April 1970.

Kozloduy NPP currently manages two pressurised water reactors with a total output of 2,000 MWe. Units 5 and 6, constructed in 1987 and 1991 respectively, are VVER-1000 reactors. By 2014 they will be upgraded to reach a capacity of 1,100 MWe each. A project for construction of a new nuclear power unit is underway.

Source: Wikipedia

Can't see the forest for the trees?

Here are some new tools to help you better navigate your event trees in RiskSpectrum PSA.

ET jumps

As you know, you can use transfers in fault trees to break up large fault trees in fault tree pages in RiskSpectrum FTA and PSA. We are now working on implementing the possibility of jumping between linked event trees in a similar way as jumping transfers in fault trees.

We have added a column in the event tree editor that displays an arrow for sequences with linked "child trees". When you double-click on the arrow, you will automatically be transferred to the child tree. There you will see an arrow underneath the initiating event, and when you double-click on that you will be transferred back to the "father tree". If there are links to several event trees, you will be prompted to choose one of them to jump to. This selection will then be stored to make it faster to navigate the chain. If you wish to re-select the working event tree chain, right-click and the selection dialogue will appear.

ET transfers

An event tree transfer viewer is also being developed. The idea is very similar to the fault tree viewer available in RiskSpectrum FTA and PSA version 1.2. The list of event tree pages will be organised showing event tree pages with links to other event tree pages. Unfolding the tree view will explore the transfer structure downwards.

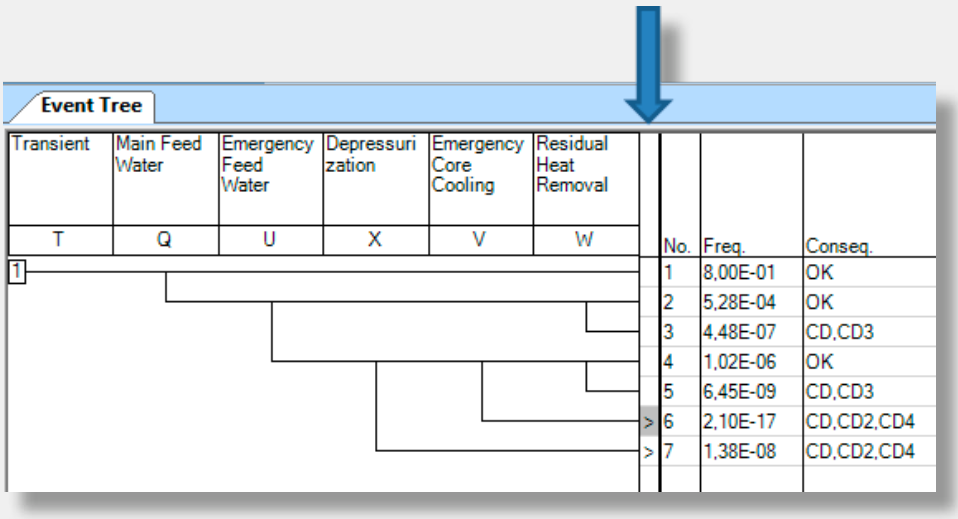


Figure 1. A column with a clickable arrow has been added to sequences that are linked to other event tree pages.

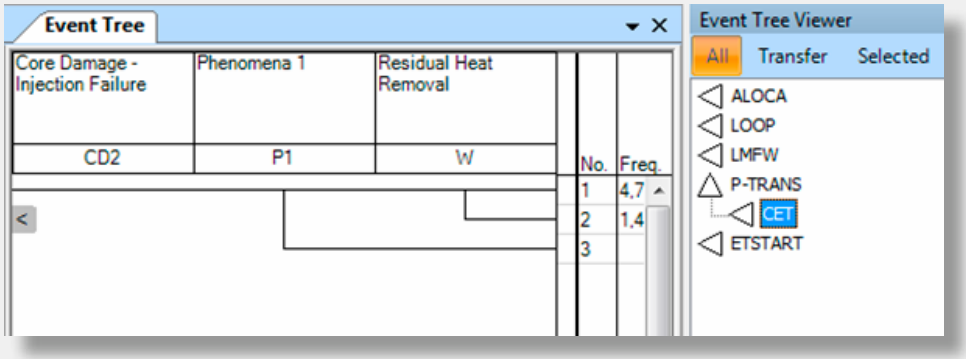


Figure 2. After opening the event tree viewer, you can choose to display it as a floating window or tiled with the other windows.

New tools for...

...sanity check

A cutset tracer has been on the RiskSpectrum User Group's wish list for many years. With the support of the user group, we have now been able to allocate the resources needed for this rather complex development. The cutset tracer is a tool that can help you to quickly understand which fault trees and which sequence lead to a particular MCS. The tool is designed to find the sequence that the MCS comes from.

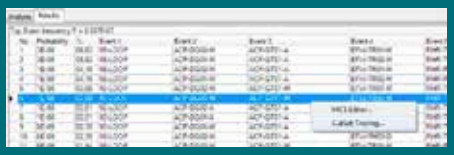


Figure 1. By right-clicking on the MCS list in the Results view, you can open the CutSet Tracer.

Figure 2. The CutSet Tracer opens in a separate window and generates a view based on the MCS you have selected. The view shows the failed sequence resulting in the selected MCS.

The beta version of the tool displays the event tree with its function events (FE). The FEs that have not failed are colour-coded green, while the ones that have failed are colour-coded red. There is also a fault tree hierarchy displaying the events that are true due to the events in the MCS. There is still work to be done on the tool to make it user friendly, particularly when it comes to large fault tree structures.

...model check

We are also working on the development of a tool for checking the integrity of the database in which RiskSpectrum FTA and PSA store the model as well as a tool for comparing two models.

The check model functionality is very similar to the referential integrity model check that was available in RiskSpectrum PSA Professional. The check model we are developing for RiskSpectrum FTA and PSA is, however, much more complete and includes e.g. verification that record properties are within range, as defined in the manual.

...and model compare

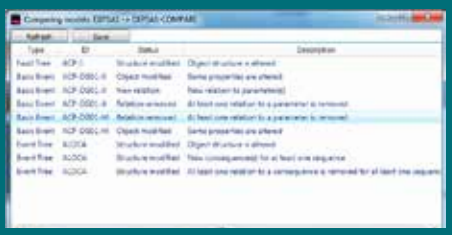


Figure 3. The RiskSpectrum PSA model compare is a tool that opens two SQL databases and lists differences between them as they are being edited.

The tool for comparing models can be used for comparing record properties and relations between records in the SQL database. The results are presented as records that have been modified, relations that have been removed or added, and fault tree and event tree structure that has been modified. ■

Johan Sörman
johan.sorman@lr.org

A comment from the project manager of the Cutset Tracer development

The development of the cutset tracer has been particularly challenging due to the fact that RiskSpectrum PSA generates a master fault tree from the sequences in the event trees. At the same time, it also applies all boundary conditions sets and prunes the tree. So the master fault tree can be very different from the original logic in the fault trees and event trees. This means that finding the origin of a cutset is not so easy.

The approach we used was to first identify all the initiating and function events included in the sequence from which the cutset originates. Then we applied other settings such as "Ignore ET success" and boundary conditions such as exchange events and event status settings. The boundary conditions must consider both settings regarding heritage between event trees and the different priorities between the BC sets depending on where they are defined in the model. After this, each input fault tree structure for the function events is built up in parallel to increase the performance of the application. Having the whole logic model in place, the cutset is propagated to perform the actual tracing.

The interface design of the Cutset Tracer is not 100% decided yet. The aim is to present the outcome clearly, to enable users to get a quick overview of the traced cutsets' effect on top gate, while at the same time making it possible to view more details about the components providing the result. Balancing these can be a little bit tricky, as we do not want the interface to be cluttered with information, but we still want to present information regarding exchanged events and other configurations that helps in understanding the results. The problem lies in displaying all the items needed in a well-structured way, but not making it too complicated, given that the main emphasis of the feature is to provide the functionality.

Helena Troili, MSc, software developer at Lloyd's Register Consulting, Stockholm, Sweden

PSAM 13

13th International Conference on Probabilistic Safety Assessment and Management

2-7 October 2016

Sheraton Grande Walkerhill - Seoul, Korea

Abstract submission due: 31 December 2015
Online abstract submission will be open from 1 September 2015.

In October 2016, the 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13) will take place in Seoul, the capital of Korea. We hope that this thirteenth edition of the conference will be the largest PSAM yet, and we encourage attendees to bring their families.

The PSAM conference brings together experts from various industries, research organizations, regulatory authorities and universities. It offers a platform for contacts between different fields from nuclear, process and chemical industries, offshore and marine, transportation, space and medical technology, civil engineering, financial management and other fields. The multi-disciplinary conference is aimed to ensure the cross-fertilization of methods, technologies and ideas for the benefit of all.

Dr Joon-Eon YANG
Korea Atomic Energy Research Institute, Korea
jeyang@kaeri.re.kr

Seoul, the Capital of Korea

Over the centuries, Seoul has assumed great strategic importance in the nation's politics, economy, society and culture. With more than 600 years of history as the nation's capital, Seoul has become both a metropolis with a population of over 10 million people and a vibrant city full of tradition and history. Seoul is home to many old historic sites like Gyeongbokgung and Changdeokgung Palaces, and places of traditional culture like Bukchon Hanok Village, Insa-dong, and Namdaemun Market. The shopping and entertainment districts of Myeongdong and Apgujeong, and Asia's largest underground shopping center COEX Mall also draw a large number of tourists every year. The Han River, which runs through the center of the city, is also a distinctive landscape of Seoul that offers a myriad of resting areas for citizens.

About Sheraton Grande Walkerhill

Located in the Northeast region of Seoul with a panoramic view of the Han River and nested amidst the beautiful and serene natural elements of the Acha Mountain, the Walkerhill offers nothing but satisfaction with its five-star service and value. Walkerhill features 2 luxury hotels: the Sheraton Grande and W Seoul, with a combined total of 830 guest rooms, 15 restaurants and bars, and extensive conference centers and wedding halls. The organizing committee of PSAM 13 will prepare a special rate for the conference attendees, which will be available on the conference website a year before the conference.

For more information, please visit the official website: **www.psam13.org** or contact the secretariat by email at **info@psam13.org**.

Lloyd's Register Consulting

Lloyd's Register Consulting provides independent risk management and engineering dynamics services to a wide range of international clients. Every day, all over the globe, we solve complex problems for our clients, reducing technical, operational and commercial risks while enhancing asset performance.

Our broad experience covers the full life cycle of activities in industries like oil and gas, marine, nuclear energy, transportation, power generation and chemical industries.

Our service portfolio includes:

- Risk based management
- Risk analysis
- Technical safety and consequence modelling
- Reliability and asset performance
- Human factors and work environment
- Engineering dynamics
- Software development

Lloyd's Register Consulting is represented in 26 offices in 14 countries.

For further information, please visit **www.lr.org/consulting** or contact **info.consulting@lr.org**

For more information about RIskSpectrum, please visit **www.riskspectrum.com** or contact **sales.riskspectrum@lr.org**

www.lr.org/consulting

Lloyd's Register is a trading name of Lloyd's Register Group Limited and its subsidiaries.
For further details please see www.lr.org/entities