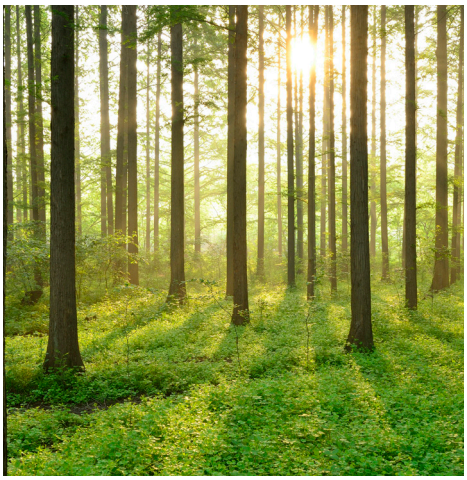
TRENDS IN NUCLEAR INSTRUMENTATION AND CONTROL SYSTEMS 2017

REPORT 2017:448



NUCLEAR

ENERGIFORSK NUCLEAR SAFETY RELATED I&C – ENSRIC

Energiforsk

Trends in Nuclear Instrumentation and Control Systems 2017

Report from U.S. conference NPIC & HMIT 2017

EMIL OHLSON

ISBN 978-91-7673-448-3 | © Energiforsk November 2017 | Photo: EDF Energy

Energiforsk AB | Telephone: 08-677 25 30 | mail: kontakt@energiforsk.se | www.energiforsk.se

Preface

U.S. conference NPIC & HMIT is one of the larger conferences covering the nuclear instrumentation and control area. Covering this conference is an efficient way of picking up international trends and tendencies.

The conference was covered by senior engineer Emil Ohlson from Forsmarks Kraftgrupp AB. This project is included in the Energiforsk Nuclear Safety Related Instrumentation and Control program – ENSRIC. The project is financed by Vattenfall, Sydkraft Nuclear/Uniper, Teollisuuden Voima Oy (TVO), Fortum, Skellefteå Kraft, Karlstads Energi and the Swedish Radiation Safety Authority.

Sammanfattning

Denna rapport sammanfattar intryck och reflektioner efter en större I&C och MMI konferens i San Francisco, USA. Utmärkande för konferensen denna gång var den kostnads- och prispress som gäller inom stora delar av elproduktionen då inte minst kärnkraften, och hur denna påverkar drift och underhåll samt moderniseringen av kärnkraftverk.

Summary

This report summarizes the impressions and reflection from a larger I&C and HMI conference in San Francisco, USA. Characteristic for the conference was the downward pressure on cost and price within large parts of electricity production, not least the nuclear power, and how it affects operation/maintenance and modernization of nuclear power plants.

Content

1	**Abbreviations**		**7**
2	**Introduction**		**8**
3	**Conference**		**9**
	3.1	General	9
	3.2	Content	10
	3.3	ANS Grand Challenges	13
4	**Trends**		**15**
	4.1	Delivering on the Nuclear Promise	15
		4.1.1 On-line monitoring and Maintenance optimization	17
		4.1.2 Positive environmental aspects of Nuclear Power	20
	4.2	Cyber security	21
	4.3	Small Modular Reactors – SMR	25
	4.4	Field Programmable Gate Array – FPGA	26
	4.5	Wireless applications in NPP	28
	4.6	Levels of Automation in the MCR	29
5	**Other Areas**		**32**
	5.1	Other Conference notes	32
6	**Conclusions**		**37**

1 Abbreviations

ANS	*American Nuclear Society*
CCF	*Common Cause Failure*
CGD / CGID	*Commercial Grade Dedication / Commercial Grade Item Dedication* Use of products not developed according to nuclear power criterions for safety applications. The utilization can be motivated by simulation programs, analyses, operational data or, most commonly, a combination.
COGS	*COTS Goal Based Salf Assessment* A ”claim-based” method used to justify COTS products.
COTS	*Commercial-Off-The-Shelf* Soft- or hardware which can be bought or licensed from an open market contrary to custom made solutions.
DDoS	*Distributed Denial of Service*
DI&C	*Digital Instrumentation & Control*
EMC	*Electromagnetic Compatibility*
FPGA	*Field Programmable Gate Array*
I&C	*Instrumentation & Control*
IAEA	*International Atomic Energy Agency*
IEC	*International Electrotechnical Commission* – A standards and conformity assessment body within El and I&C
LPRM	*Local Power Range Monitoring* A system to locally measure neutron flux within the reactor core. Several LPRM are typically used to form Average Power Range Monitoring (APRM).
MMI / HMI	*Man Machine Interface / Human Machine Interface*– The interface between operator and the process facility.
NPP	*Nuclear Power Plant*
PLC	*Programmable Logic Controller*
SSPS	*Solid State Protection System*
US NRC / NRC	*United States Nuclear Regulatory Commission*
V&V	*Verification & Validation*

2 Introduction

This report is a conference report from a major conference in the Instrumentation & Control (I&C) and Human-Machine Interface (MMI / HMI).

The report aims to reproduce the trends, presentations and reflections that the author perceived during the conference. The content does not reflect everything presented at the conference, rather it is limited to the sessions that the author (or any of his colleagues) could attend, as well as some areas where only the topic reports could be read (where it was not possible to attend this session).

The task to observe and report from the conference was submitted by Energiforsk to Emil Ohlson, Forsmarks Kraftgrupp AB.

3 Conference

3.1 GENERAL

During week 24 in 2017, a major conference concerning I&C and HMI within nuclear power was held at the Hyatt Regency Hotel, in San Francisco, CA, USA. The organizing unit was the ANS (American Nuclear Society) and the conference is a recurring event in which different areas of focus are addressed. This year's conference was the 10th in this topic.

The conference was an Embedded Topical Meeting to ANS Major Annual Meeting 2017, which deals with nuclear power at large and addresses much more areas than just I&C and HMI.

Each conference usually has a slogan that reflects the location, situation and mood for both the actual meeting and the industry as a whole. The slogan for this year's conference was "Innovating Nuclear Power" and reflects the great aspiration that currently appears in the industry to find ways to on the one hand, make nuclear power financially competitive, and also to find new solutions to improve operation/maintenance and, secondly, to promote nuclear power as a CO2-free and environmentally friendly electricity generation.

The conference was largely characterized by the "Nuclear Promise" or "Delivering the Nuclear Promise" initiative, which is a joint initiative between US nuclear power plants.

ANS is an international non-profit organization for research, education and organization in nuclear power. It was formed in 1954 and today has about 11,000 members representing over 1,600 companies, research institutes, universities and government agencies. The purpose of the organization is to work for understanding and knowledge in nuclear power technology.

ANS conferences are usually divided into two different ways; It is either a larger meeting with several different technology areas involved (e.g. I&C, Materials Technology, Calculation Program, etc.) or only area represented. This year's conference was of the large sort and comprised both nuclear power in general and specifically I&C and HMI. For more information on ANS different divisions, see www.ans.org or more specifically www.new.ans.org/about/committees/

The NPIC & HMIT conference was divided into two main tracks -I&C and HMI, which in turn were divided into several different technical areas. This meant that there were always 10 lectures and sessions that took place in parallel, which meant a lot of planning to participate in the lectures that were considered relevant and interesting to one's own.

Apart from the sessions there was also a larger exhibition going on where vendors and company’s within the nuclear area showed new technologies and equipment invited to dialog and technical discussions. The exhibition was in parallel with the conference during most of the week and was located just besides the meeting rooms. There were also a number of different demonstrations and smaller

"workshops" ongoing where the exhibition visitors could try different tools, applications and simulations SW.

During the weekend before the meeting, a two-day training was also organized within the field of *"Helping Deliver on the Nuclear Promise: A Digital I & C Licensing and Qualification Workshop"*, as well as a one-day workshop in *"Preparing for the Nuclear Engineering Professional Engineering Exam"*.

These workshops where led by engineers and experts from the different company's or laboratories at the conference and is aimed to provide a deeper knowledge and understanding within different areas.

Approximately 400 people representing different organizations and companies from around the world attended the conference. Most participants come from vendors, utilities or research institutes but several also came from regulatory bodies of universities. USA was most represented but the international participation was also large with over 30 countries represented at the conference.

Vattenfall had a relatively good representation this year with attendees from both Forsmark and Ringhals.

In total, about 250 reports (so-called "papers", meaning a shorter summary reports) were sent to the NPIC & HMIT conference, and at least as many additional to the larger annual general ANS conference.

The conference with all presentations, workshops and the exhibition is considered a very good opportunity to see what is going on at different vendors and what other utilities and organizations work with and see as their main challenges. It is also seen as a very good opportunity to establish contacts within the industry.

3.2 CONTENT

As mentioned, the conference was divided into two main tracks –I&C and HMI, and under these main areas there were technical sessions with presentations and panel discussions according to the list below. Certain sessions are extensive and are therefore divided into different rounds (one round equals the morning or the afternoon). In the morning prior to the first regular technical session, there were also so-called Plenary Sessions with more general speakers without any given theme; these were often specially invited lecturers who often had high positions in the industry (e.g. CEOs from different companies, people from the Department of Energy, Commissioners from NRC mm).

Each session then contains between 3-20 presentations. The different sessions at the conference were (without relevant order but divided into the different "tracks"):

- Nuclear Power Instrumentation and Control:
    - Advanced Surveillance, Diagnostics, and Prognostics—I
    - Cyber Security in Digital I&C—I
    - General Sessions in I&C—I
    - Digital System Reliability—I

- SMR Instrumentation and Control—I
- Electromagnetic Compatibility (EMC) and EMI/RFI Issues
- Cyber Security in Digital I&C—II
- Advanced Instrumentation and Monitoring Methods for Dry Storage of Spent Nuclear Fuel
- Automation: Effects and Applications
- Nuclear Energy R&D in I&C Areas
- SMR Instrumentation and Control—II
- Advanced Surveillance, Diagnostics, and Prognostics—II
- Modeling Digital I&C Systems in PRA/PSA
- Light Water Reactor Sustainability (LWRS)
- Research Reactor I&C
- Advanced Surveillance, Diagnostics, and Prognostics—III
- Cyber Security in Digital I&C—III
- Advanced Sensors and Measurement Technologies—I
- General Sessions in I&C—II
- I&C for Advanced Reactors
- Next Generation I&C Systems
- Measures—I: Operator and Team Performance
- Measures—II: Data Collection Methods and Challenges
- Safety Critical Software Development, Qualification, and V&V—I
- Digital Control System Applications
- I&C Modernization Experience—I
- I&C Lessons Learned from Fukushima
- Diversity and Defense in Depth (D3)—I
- Measures—III: Eye Tracking Applications and Methods
- Advanced Sensors and Measurement Technologies—II
- Safety Critical Software Development, Qualification, and V&V—II
- On-Line Monitoring for Maintenance Optimization—I
- Advanced Surveillance, Diagnostics, and Prognostics—IV
- Cyber Security in Digital I&C—IV
- Field Programmable Gate Array (FPGA)—I
- General Sessions in I&C—III
- On-Line Monitoring for Maintenance Optimization—II

  - General Sessions in I&C—IV
  - Diversity and Defense in Depth (D3)—II
  - Field Programmable Gate Array (FPGA)—II
  - Digital System Reliability—II
  - I&C Modernization Experience—II
- Human Machine Interface Technology
  - Human Machine Interface Design and Evaluation
  - Verification and Validation of Control Room Designs and Modifications
  - Case Studies of HFE Program Implementations
  - Virtual Reality, Augmented Reality, and Alarms
  - Human Performance and Lessons-Learned in Beyond-Design-Basis and Extreme Conditions
  - Human Reliability Applications for Improving Understanding and Performance in Plant Operations
  - V&V Methods and Applications for Control Room Designs
  - Human Factors Engineering Programs, Standards, and Guidance Initiatives
  - Computerized Procedure Systems
  - Computer-Based Tools for Improving Operator and Plant Performance—I
  - Computer-Based Tools for Improving Operator and Plant Performance—II
  - Experience with Control Room Modernization—I
  - Supporting the Development, Practice, and Integration of Human Factors Engineering
  - Experience with Control Room Modernization—II
  - Soft Controls
- General and Panel Sessions
  - NPIC&HMIT 2017 Opening Plenary
  - Think Smart Think Digital: Delivering the Nuclear Promise through Digital I&C–Panel
  - U.S. Department of Energy Advanced Sensors and Instrumentation Research–Panel
  - The Future of I&C: Compelling Projects Lead by Young Engineers–Panel
  - Robotics for Maintenance of Advanced Reactors–Panel

- Experience with NUREG-0711 Rev. 3–Panel
- Near-Term Improvements to the Digital I&C Regulatory Infrastructure—Panel
- I&C Research Plans and Activities by Leading Organizations–Panel
- Human Factors Engineering: Improving Nuclear Safety and Efficiency with Digital Controls–Panel
- I&C Regulations, Standards, and Guidelines—I
- I&C Regulations, Standards, and Guidelines—II

In total, nearly 70 different sessions were held within the NPIC&HMIT section, and at least as many sessions at the general ANS annual conference where NPIC&HMIT was a subcommittee.

In addition to these sessions above, a general plenary session was held each morning that included 3-5 presentations of I&C, HMI or of general nuclear technology interest.

As can be seen, the scope of sessions and presentations is very large and since most of them go in parallel, it is impossible to be able to listen to all that is interesting, and it can therefore be good to be more than one person from the same company, then you can split between different sessions and then exchange experiences.

During the week with I was able to listen to 66 different technical presentations, overall lectures and panel discussions.

3.3 ANS GRAND CHALLENGES

Similar to the initiative *"Delivering on the Nuclear* which is described in Section 4.1, ANS has also launched a program to meet what they sees as the industry's major challenges, now and in the coming years. The ANS members and others experts were asked to make suggestions and provide input on what they considered were the biggest challenges. This rendered in more than 300 proposals received and analyzed, grouped and prioritized, and finally made a list of the following areas ANS together with the industry, intends to work with in the future:

- Low-dose
- Public Engagement
- Cycle
- Radioisotopes
- Rejuvenate Infrastructure
- Advanced Materials
- Simulation / Experimentation
- Expedite Licensing
- Knowledge Transfer

Most of these areas appeared during the conference as important subjects and during debates. More on these areas and the initiative can be found on the ANS website www.ans.org/challenges/

4 Trends

Below are a number of areas that I perceived as vital, leading or otherwise in focus at the conference. Some of them have been present for several years (such as the Cyber Security and FPGA) while some are relatively new trends.

Both technical areas and more "soft" issues have been listed as trends if they were perceived as important during the conference.

4.1 DELIVERING ON THE NUCLEAR PROMISE

The nuclear industry in large parts of the world –exception is probably only Southeast Asia, primarily China, is struggling with more or less the same problems:

- Falling prices for electricity
- Rising costs for modernization and refurbishment and increasing production rates (in the United States, the production cost per MWh increased by 28% over the last 12 years)
- Unwillingness from owners to make the large and long-term investments which are often needed
- New regulatory requirements impose ever higher and higher requirements and often involve high costs
- Other types of production (e.g. solar and wind) receive subsidies and does not have the same cost driving authority monitoring
- Hard to gain trust in the public and difficult to highlight the environmentally beneficial parts of nuclear power to the common man

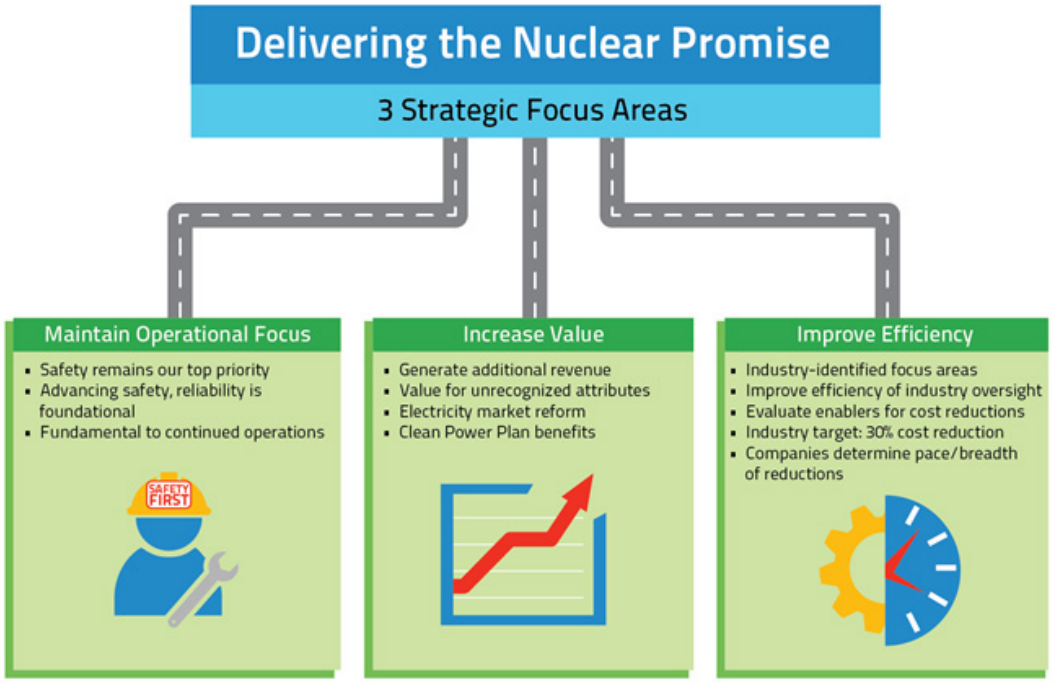
In short, it is currently very difficult to be profitable and competitive and to win the public support they need to provide the basis for continued operation and production.

One notable fact of this is that in recent years a number of commercial NPP closed down, or took a decision on the close in advance (before end of license), and all of these early closings have been due to lack of profitability or other economic reasons. According to the IAEA, a decision to shut down early was taken for 12 reactors worldwide, all due to financial reasons in 2016. And in Sweden this is certainly very obvious where we are seeing the shutdown of the O1-O2 and R1-R2 because of these reasons. And from an capacity perspective, it is estimated that twice as much nuclear power can be shutdown compared with what is expected to be built and commissioned up to 2030.

In addition, the nuclear power plants are aging, and in order to continue operation, major investments are often required, and in the current situation these investments are very difficult to deem profitable. The nuclear industry -in the western world, are therefore facing a rather precarious situation, if it does not manage to reverse the trend, it will liquidate itself.

The Nuclear Energy Institute -NEI, together with INPO and EPRI and all the NPP in the USA initiated something that they call the Nuclear Power Initiative intended

to address the problem described above. Simplified, it is divided into three main focus areas - Maintain operating and production focus, Increase the value / profits, and Increase efficiency. The image below shows how the initiative is visualized.



How this is handled by different nuclear power plants, institutes, universities, suppliers, etc., to a large extent characterized the content and feeling of the conference. Everybody wanted to pitch in and help the industry, and how this was intended to be done by the various actors differed quite a bit in many aspects. Where certain countries and companies intend to hold back on all costs and only to do what is absolutely compulsory (and then risk of having problems in a few years with degraded systems), others see an opportunity to use better solutions for operations and maintenance (and thus make some initial investments) and through that become more efficient and avoid cost in the future.

In the United States, nuclear power accounts for 20% of total energy, but for the full 62% of its "Emission Free Electricity".

David Blee, CEO of the US Nuclear Infrastructure Council, said that the United States faces a number of tough challenges in terms of electricity generation and nuclear power. The goal is 2050 to have 30% renewable and 14% nuclear power, but by this time most NPPs in the US will have been closed down and there is currently no evidence that the nuclear capacity will be sustained through new construction. In future, China is expected to lead the NPP market with Russia as a strong partner, and if nothing is done from political or corporate affairs, the United States and the Western world will sluggish in development and the market position. David Blee said that a long-term commitment to nuclear power that the

market, the companies and the public can support, and sometimes it is important to invest in what you believe to be right. *"The choice for USA is to be a leader or to be THE leader. There was no plan B for D-Day..."*

4.1.1 On-line monitoring and Maintenance optimization

By using the modern I&C systems full potential utilities are able to optimize Operation and Maintenance and hence be more efficient and increase availability. This is at least what many vendors and plants said during the meeting, but can this be achieved in practice at a plant with large part of it's I&C still analogue?

One way to help reduce costs and enhance operation and maintenance optimization is to use on-line monitoring to better determine the need and extent of calibration, component exchange, etc. Most of the new builds in progress already have wireless networks, HART protocols or similar programs to get status and maintenance information from pumps, motors, valves, etc. without "down loading" the regular infrastructure for information and signals. For many, the purpose is to do maintenance actions such as replacing certain components or calibrate only when needed (on demand) and not at a certain date (Preventative Maintenance). Of course, a certain intermediate path between these two alternatives is required because some equipment might only be available during outage and cannot be accessed during the operation cycle. But there were many examples of initiatives and projects that were successful in adopting an on-demand management for certain components in the plant.

One example was from Sizewell B who had implemented a joint project with US AMS to reduce the amount of calibration during outage. Sizewell B is a PWR with dual RPS systems which means that it has a very large amount of transmitters. For some time, they have been using on-line monitoring -OLM, for different transmitters (pressure, flow, level, etc.). The large amount of transmitters and the fact that they have a relatively low staffing cause's calibration and calibration checks to take up a relatively large part of the planned outage. Since most of the signals to the OLM system already where sampled in high frequency, there was very much available data during the operating cycle on the functionality, health, performance and reliability of the equipment. Something that often limits the possibilities of OLM is that the signals are not sampled at sufficient frequency to make noise analyzes, etc. Sizewell B also had records that showed that most transmitters checked during the outage were ok (reportedly about 80% was OK during the calibration check) and did not have to be calibrated. However, this control took time and the manual action had also introduced errors during reinstallation (many times, the transmitter must be disconnected and connected to test equipment) which caused problems and malfunctions. By analyzing the transmitter's signal and dynamics with different analysis tools at three different times during the operating cycle (start up, mid-cycle and just prior to outage), it was found that most transmitters were ok and did not have to be calibrated in a normal manner, thus focusing solely on the subject that showed calibration errors or uncertainties. The assessment of the calibration set for the outage was done approximately in the middle of the cycle (in order to plan the outage work with

respect to calibration) and this was verified by the analysis just prior to outage shut down. In this way, they state that they reduced the calibrations required by almost 75%, thus reducing the outage length by several days, which very quickly saved up the investment made in the project.

Something that could be a problem with a similar strategy that Sizewell B used is that the Tech Specs often states that calibration should be performed at a specific part of the transmitters total measurement range. Towards the Authority, Sizewell B motivated their strategy by claiming that they had very good information about concerned signals, keeping good track of the history and by showing that their transmitters rarely had changed in value between calibrations. A report of Hashem Hashemian from AMS that were referred to at various presentations showed that only 5-10% of all transmitters had gone out of control calibration during calibration check.

Another positive effect of OLM is that you get information faster if any transmitter actually has gone off-calibration, compared to if you wait for the next scheduled calibration check at upcoming outage.

Brent Shumaker from AMS also stated that they implemented Response Time tests of pressure transmitters by studying frequency analyzes of the natural noise introduced by the plant process, without even taking the equipment out of service.

Rolls Royce also told that they were working with a customer who changed their RTD (Resistance Temperature Detector) every 8 years at Scheduled Preventive Maintenance. After a review and analysis - both statistically and technically, this interval could be extended to 12 years without any negative aspects being encountered.

Andrei Gribok from Idaho National Laboratory presented how they worked with OLM for aging and degradation of piping. According to him, there was even more money to be saved on piping and mechanical devices than on transmitters when using OLM. They worked with testing by asking 6 questions for each position:

- What? (what type of equipment shall be tested?)
- Why? (why shall we test this particular equipment?)
- How? (how can we test just that particular thing we are aiming to prove?)
- Then What? (what do we do if something isn't as we expected?)
- Where? (where can this equipment be tested? Lab? Plant? etc)
- When? (when in time do we have the possibility to perform this test?)

One problem with OLM may be that it requires a variety of new sensors / transmitters and additional cables and wiring, which is often very expensive. This means that many people choose to install wireless networks for this type of signals.

Since it often are Human Factor's aspects involved with testing/reinstallation (ie introducing errors through human intervention), it may also be beneficial to keep a component on-line at all times and not risking that the test itself leads to a fault in the system. If the same maintenance technician is working with calibration or maintenance of two diversed systems, this may in fact be a CCF risk. If the systems do not need to be taken off line or even calibrated, this risk is then minimized.

The amount of data collected in OLM systems have many times shown to be useful during other activities such as modernizations, event analysis or other projects. The NPPs many times has a very large amount of data (in e.g. plant computer, measurement computer) but this data is rarely used for something else that historical purposes (analyzing data and measurement signals during a certain event in the plant). According to many speakers and attendees at the meeting, this data actually provides large possibilities for OLM and similar activities if the plant only uses the right tool/program to analyze the data that they already have.

Another aspect of OLM and access to data is that one often needs to be successful the first time when installing something in an NPP because extended outages are very costly in an already cost-prone business. Developing something by testing your way to a working solution as Edison did when he invented the bulb (he is told to have done over 1,000 different attempts before he succeeded) is nowadays completely impossible. This means that you have to have very good models and test systems for the plant, and many times DIC is the part where it's hardest to know in advance what problems may occur when commissioning etc.

Other areas within the OLM and optimization area that had many presentations were the Accuracy of Parameters used in the calculation of the thermal power. Improving accuracy and reducing uncertainties allows you to increase the power without risking to exceed the limitations that you have in thermal power (usually a plant would operate below the given limit with a certain margin just to be on the safe side). Different methods and mathematical correlation models were a theme for multiple presentations. Steve Black of Areva talked about their use of Linear Quadratic Estimation - LQE, (also known as Kalman Filter). Where they have combined several measurements and parameters in an Steam Generator and thereby been able to halve the standard deviation for the estimation of Steam Generator level compared to before.

Pradeep Ramuhalli from the Pacific Northwest National Laboratory presented something called Enhanced Risk Monitors (ERM) that combines Risk Monitors (and thus PSA/PRA) with the type of OLM systems and other Component Health systems to predict failures and needs of replacements. This is thus a step further than just using OLM and is used to predict how many more maneuvers a specific valve can actuate, and then provide probability values that can be used to determine which year/outage you are should do certain component exchanges. And these figures can then be followed during the operating cycle if something deteriorates so that you need to reevaluate your plan. The numbers are updated in real time for changes in input data (from, for example, OLM) and can also show numbers for both Safety risks and financial risks is you change or don't change a particular component during a certain outage.

A prerequisite for OLM is often access to information in the form of measurement data or diagnostics. Javier González from Spanish Tecnome told us that since there is a lot of money to be saved using OLM, an initial investment that NPP does not always want to do is often required, but in order to use OLM, a lot of information is often required. *"What cannot be measured; cannot be improved"* he said.

Due to the large amount of data covered by OLM, the *"Big Data"* concept was also something that often appeared in these presentations.

4.1.2 Positive environmental aspects of Nuclear Power

If nuclear should have a place in the future energy mix, it must be accepted by the public. How can the industry help turn the public opinion so that nuclear can compete on the same terms as other power sources?

Given the problems raised, the perception was that nuclear power must begin to gain public confidence and thus earn its place in the future energy mix. The industry thinks it has a good product but it is presented in a skewed way in the media. In order to reverse the trend and opinion, many people argued that the industry needs to be better at communicating with the public and demonstrating the benefits with nuclear power.

Many general and plenary presentations were addressed to this subject and the guest speech on the joint dinner on Tuesday was devoted to this topic.

Michael Shellenberger from the Energy and Environmental Organization *Environmental Progress* held a highly appreciated presentation on Myths and Facts about nuclear power and other power sources. He said that the major problems of nuclear power are not the technical challenges or the risks that comes with nuclear, but rather the large anti-nuclear lobby that exists and often plays at emotions and "old propaganda" rather than facts. He also believes that nuclear power has put an enormous amount of resources and effort on Safety and that, in practice, nuclear cannot be much safer than it already is. The new safety modernizations the utilities make today only produce minor improvements in safety, while they often cost a lot of money. In addition, the "aim" for the required safety level is not even close for other generating sources or other industries when compared with nuclear. An NPP accident actually does not result in a large number of deaths, but rather gives great geographic impact and leaves large areas uninhabitable for the foreseeable future. But this effect is actually quite locally isolated to a delimited site (although this site can be fairly large). In terms of actual deaths per produced MWh, nuclear power is clearly better than basically all other power types. However, emissions of CO2 and other greenhouse gases will have global impact and can actually devastate large parts of the ecosystem if the trend is not changed.

As part of the Nuclear Promise Initiative, companies and organizations will jointly try to highlight the positive aspects of nuclear power in the communication to the public. This feels interesting since it is one of the first times the industry tries to find ways other than purely based on technical solutions to solve problems. Previously, the utilities tried to solve this by designing additional safety systems and further improving safety. But it's pretty fruitless if the basic problem - in this case, humanity's attitude and knowledge about the risks - will not be changed by creating safer systems. The aim is to work with a campaign focusing on Man instead of System, instead of *"WHAT makes nuclear safe"*, one wants to focus on *"WHO makes nuclear safe"*. And this is a major part of the conference's slogan *"Innovating Nuclear Power"*.

4.2 CYBER SECURITY

With an increasing amount of digital equipment in the plants and more and more administrative systems connected with the Internet, cyber security has become one of the larges areas within the industry over the last 10 years. How to protect your plant from cyber threats and at the same time benefit from the advantages with digital and connected equipment was in focus at the conference.

As in previous years, cyber security was a very big topic. Considering the number of sessions and presentations, it was definitely one of the conference's largest specific areas. In total there were 4 sessions - almost two full days, and 18 presentations reported on the subject. For priority reasons, I could not attend all of these sessions but chose those who seemed most interesting/relevant/rewarding.

One of the more interesting -and also scary, presentations was held by Joseph Weiss from Applied Control Solutions, where he talked about the cyber-attacks that occurred in 2015 and 2016 to the power grid of Ukraine. In 2015, the attack was against the distribution system and 2016 it was directed against the transmission system. In these attacks, the hackers had most likely introduced malware long before the actual attack (about 8 months before) through Word files sent to the administrative network and where staff were tricked into opening the files in believing that they were documents they should read –a so-called phishing approach. The code used was a variant of *"BlackEnergy Remote Access Trojan*" which can log users and passwords, perform DDoS attacks, etc. Through this, the hackers came across passwords, etc. and were able to create their own privileged users, identify items to attack, etc. During the attack, hackers could control workstations, control some switches and relays and thus create a major power outage in large parts of the network. The attack was coordinated and scheduled so much of the network was attacked at the same time which worsened the situation. When the switches had opened, incorrect firmware updates were sent to the switches, and thus they became unmanageable for operators who thus had difficulty in restoring the systems. Something that was not done -but many, including Joseph Weiss think may have been part of the plan, was that after the hackers had taken control of circuit breakers, relays, and AC motors, they would have been able to reconnect relays and motors out of phase or imbalanced with the grid, or through use of quick Open and Closing orders that alternates and thus damage the equipment rendering it unusable for the operators and system. This is seen as a relatively likely threat to the NPP and others connected to the grid that also generates electrical power for its own use. Events in Forsmark 3 2013 and 2007 and tests at the Idaho National Laboratory show that NPP can be sensitive to phase imbalance or phase failure. This vulnerability is also called *"The Aurora Vulnerability"*. Notable is that this went very quickly, according to data, the attack took less than 1 minute. For NPP, this could cause LOOP and also damage to its own equipment for power supply such as EDG, motors, switches, transformers, relay protection, etc.

Similar attacks have also occurred in Germany where malware came in via a pdf file on the administrative network and then spread to SCADA systems, which were then manipulated to cause damage to the facility. Christopher Lamb from Sandia National Laboratory took up his presentation of Dynamic Attack Surfaces

in NPP, saying that as a utility, you should analyze the cyber threat from two different perspectives:

- Threat Centric – Meaning What damage can someone possible cause in the worst case (core melt down, radioactive emission etc)
- System Centric – Meaning What in my system is vulnerable (digital control systems, breakers etc)

Combining these two perspectives gives you the basis for what should be prioritized and hence most protected for cyber-attacks. However, Lamb believes that NPP in particular has relatively large so-called "surfaces" that are vulnerable. It's a big and complicated process with very much equipment involved, and where many parts of the process can affect other parts –e.g. if manipulating the feed water can affect reactor core situation, etc. Zones and network partitioning are good ways of protection, but can actually be razed or bypassed by someone using a USB or similar to move or copy any measurement data they need for some purpose. Often, the vendors also use their own laptops or other digital tools when installing or testing their equipment in the plant. This action can completely bypass the Zone partitioning that is implemented at the facility.

Something that was often mentioned as a threat to cyber security is the pressure for cost reductions that all NPP are facing today. This generates two opposing forces; costs are reduced by the use of more commercial equipment and digital equipment in more and more positions, while at the same time making this increasingly vulnerable to cyber threats. Often this leads to major campaigns to strengthen cyber security, which is often difficult if you initially did not design the system for with this as a requirement, and may sometimes lead to the installment of surveillance (digital) systems to monitor cyber threats that are often considered safer but have more rights/privileges they the other systems and are therefore even more sensitive if it's hacked.

The cost of carrying out relatively extensive attacks has decreased and now you can even "buy" attacks or software for attacks for relative small cost compared to what damage they can cause. This means that the hacker can be a relatively small organization or group of people who do not need to be well funded or technically equipped. There are also statistics that show that most attacks are controlled/initiated from other countries than where the attack occurs. This often makes it more difficult for the police, authorities, etc. to be able to prosecute or even catch the perpetrators. This provides a need for international laws, standards and protection measures, which IAEA and IEC is currently working with.

Information availability is also a threat nowadays, as more players (authorities, parent companies, owners, etc.) want to have access to certain parameters and values from an off-site location. One can often assert that this should not be a problem because it is "one-way communication" but there are examples when this kind of contact or communication has been used to implement or spread malicious code. All communication paths into the system are a threat, and the more you have, the greater the likelihood that something can be exploited.

Since nuclear power is a medically exposed industry, there is always the risk that different political groups want to cause damage to the industry, and according to

Athi Varuttamaseni at the Brookhaven National Laboratory -BNL, this can happen without actually accessing any safety equipment. BNL has conducted a study in which they look at models and attack patterns against NPP, saying that even Non-Safety classed equipment can often be of great (medial) value for hackers with a political agenda. If equipment in a nuclear power plant would be damaged a virus or cyber-attack, this would cause close attention from the media, even if this equipment was non-safety equipment. It could also impact the plant very hard financially if large vital components such as transformers are targeted. The attack in Ukraine and the tests performed in Idaho National Lab 2007 shows that not only can equipment be temporarily taken out of operation, but it can also be destroyed by phase imbalance, etc. These large components often take a very long time to replace and this can then have enormous financial consequences for the plant in means of non-generating time and replacement costs. The assessment and dialogue after the presentation was that since many plants are having difficulty with profitability, such an attack could actually result in the plant being shut down due to costly repairs and long outage periods in combination with the licensing work likely to be required for restart.

The IAEA is one of the leading players in the field of cyber security in NPPs and they have been working on this issue for many years. When they started their cyber security group in 2002, they were 6 people were working on the issue, now they are over 90 people working with these questions. The IAEA has many guides and reports in this field, and their next upcoming document (*"NST036 Computer Security of I & C Systems at Nuclear Facilities"*) is scheduled to be released in 2017. The IAEA states that many now choose the same level of cyber security for their Security Systems as for their Safety Systems, but some still mainly focus on Safety Systems. They also say a little jokingly that *Gates*, *Guards* and *Guns* were previously the means to prevent an intrusion, but now *Geeks* (ie IT experts) must be added to protect their facilities physically and informally. The analyzes and investigations made by the IAEA over the years show that it is very difficult - and costly - to build in cyber security afterwards in a system that was not designed for this originally. It tends to be a lot of "*patch-and-fix*" and this in turn creates new threats and vulnerabilities. Their recommendation is therefore to have a comprehensive and well-developed plan for how cyber security should look and be designed, and then implement this at a timely rate. You should not look at system-by-system or project-by-project, but have an overall strategy for the entire cyber security, both for the Safety Systems, Security System and Operating Systems.

Juergen Botchler from IEC / Siemens introduced a forthcoming cyber security standard for NPP; "*IEC 63096 Security Controls*", scheduled to be released by 2019. This divides cyber security into 3 levels S1/S2/S3 similar to how IEC 61226 divides safety features in category A/B/C where the cyber levels follow the security categories, i.e. S1 corresponds to cat A, S2 cat B and S3 cat C.

One reflection is that the development of new types of digital equipment and devices goes extremely fast, new viruses and Trojans are also developing very fast. More and more NPPs install new types of digital equipment and it becomes easier to organize or carry out a cyber-attack. At the same time, the development rate of guidelines and standards within the IAEA and IEC is very slow; it often takes

several years to develop a new standard. Will the standard really be published in due time, or is it outdated when it is published? There are now also an incredible variety of standards and guidelines available that all address or focus on a specific part or specific aspect. The utilities often consider that no organizations standards are comprehensive for their needs without the need to complement the different actors' standards. It is therefore very difficult for the NPP to get a holistic approach or to know how these different documents should be linked and related to each other. This is especially important as many documents are developed by different organizations, making it difficult to put in a hierarchy.

Sofia Guerra from Adelard talked about the interplay between Safety and Security, something that is often underestimated or weighing over to the Safety page: *"Safety must be security-informed: if a safety-critical system is not secure, it's not safe."* They had looked at ways to integrate Security into the development work of a Safety related Smart Device.

The Ukrainian company Radiy who works a lot with FPGA has something they call Secure Environment Establishment for Safety related systems, where they during development clearly describe Who, When and How to address cyber security. They also indicate that (currently) there are no known viruses or malware that could damage HDL encoded configurations. Certainly, FPGA can be reconfigured, but this must be done via a specific proprietary interface as - normally, is not available to any hackers. Radiy also points out that if you need a cyber-proof system, this must be developed through close contact together between the vendor and the customer if it is to be comprehensive. Many shortcomings or weaknesses in hacked systems are due to misunderstandings between vendor and customer, which gave rise to security holes that can be utilized by a hacker or third party.

One of the easiest ways to reach relatively far in cyber threat work is to have established, supervised and controlled zones for data traffic and computer equipment, as well as to use firewalls and data diods between these zones. But although this is generally a good protection, it does not mean immunity to attacks.

A feeling regarding cyber security at the conference was that not much new had actually happened since the last meeting in Charlotte 2015. A lot of new attacks have indeed been taken place since then and many organizations -IAEA, NRC, IEC, EPRI etc., work a lot with standards and technical reports in the area, but not much new had been done with the vendors and the plants. In many aspects the utilities were still remaining in the same place as 2015 with regards to cyber-security. They are well aware of the threats and do what they can do to protect themselves, but are introducing digital equipment and other "Smart Devices" at a relatively high pace, so the overall exposure has often gone up, even if considering the countermeasures that have been installed since 2015. One reason for this slow action plan may be that much of the research in the field is relatively abstract and difficult to practically apply to the NPP. It is often difficult to know how to go from the results presented in research to something that can actually be implemented and used in the plant. There is also no "Total Solution" that ultimately takes care of cyber threats with 100% efficiency, and it will never be as long as you have programmable equipment and digital networks. This is a reality that every NPP

must relate to, and they all seem to be convinced that the best way to do this is to have as comprehensive overview as possible about their vulnerabilities and then work proactively and continuously with them.

4.3 SMALL MODULAR REACTORS – SMR

As the regular new build NPP are struggling with delays and cost and as there is a big need for clean energy at many remote locations, the industry are starting to look for other alternatives for large NPP. Small Modular Reactors – SMR, just might be one of the answers.

An area within the industry that has been on the rise within research and development in the last 10-15 years is Small Modular Reactors -SMR. And this year was the first time this topic wes a prominent part of the conference's agenda and content. It has been mentioned several times in earlier years but then a bit more as part of other topics. 2 sessions during the meeting were dedicated to SMR related I&C, and questions about SMR also came up at other sessions such as MCR design and automation levels in MCR.

SMR is smaller NPP both to power (IAEA definition of Small Reactor is a reactor below 300 MWe) and physical size. Their advantages are often that they can be built in a location that does not have the infrastructure required for a normal reactor and that they are often considered to be more economical to build than regular reactors. As these are often relatively new designs, they comprise many passive safety features similar to Gen4 reactors, and this, in addition to their smaller core/residual heat, also makes them safe with a limited need for cooling after an accident. Some suppliers indicated that in case of an accident, the operators could in principle just go home because the passive cooling and other passive containment capabilities would cover safety needs both in the short and long term perspective.

SMR fits specifically well into the conference's slogan *"Innovating Nuclear Power"* with modern reactors with passive safety features, less space needed and the ability to generate power in places that have previously found it difficult to find stable energy solutions. This also becomes a part of the focus on "clean" power supply with minimal emissions.

The costs of researching/designing and then building SMRs are assessed significantly less than the usual NPP, but the cost is by no means small, and for financing an SMR large amounts of money are required. However, it is usually not the large vendors that are currently building NPP today who leads the development of SMR´s, but most often smaller companies - for example, the Swedish company Blykalla Reaktorer. And for SMR, a lot of private financiers come in as many see this as a potentially growing market within a few years.

I&C and HMI for SMR have slightly other prerequisite than usual NPP. As mentioned, SMR has many passive safety features and the I&C has a more supervising role for operation than a safety actuation role. Many of the parameters that need to be monitored and measured are very different from today's NPP, which imposes new requirements on measuring equipment with regard to for

example monitoring principle, temperature tolerance etc. This development is something that can provide positive effects for today's NPP in terms of new, better measurement capabilities and techniques. Since SMR is often built in modules with 2 or more reactors in one site/facility, control rooms are often designed to handle multiple reactors at the same time. E.g. the company NuScale Power has 12 SMR on one site supervised by one control room with 6 operators in the MCR, which also reduces operator costs. This approach is considered to be both possible and appropriate due to the fact that less interaction is deemed necessary between operator and process, but it sets new requirements for how the MCR for these facilities must be designed, a topic the was addressed and handled in a number of presentations.

It can also be mentioned that the Reactor Protections System for NuScale SMR is implemented in a FPGA system called HIPS – Highly Integrated Protection System.

It is the design of the core that largely gives the safety requirements of a reactor, thus also sets the requirements and design of I&C. And since SMR has a different core design, this brings new types of I&C systems and solutions for SMR compared to regular NPP.

A small problem for SMR currently is the cost of licensing versus profitability factor for the plant. The output power and thus the possible income are smaller for SMR, but the licensing costs are at the same levels as normal NPP with much larger power. Thus, there are large initial costs for designing and licensing these "small" units, something that probably hinders the development at present time.

4.4 FIELD PROGRAMMABLE GATE ARRAY – FPGA

Field Programmable Gate Array - FPGA, is a system built up of a large network of logic gates/logic blocks and reconfigurable connections between these gates/blocks. Since many logic blocks can be used in one FPGA, large complex functions can be realized using FPGA. FPGA is nothing new in the I&C world (although the interest from nuclear power is relatively fresh) and the function that is seen as one of its major advantages in other industries - the possibility of reconfiguration in the field, is not an option considered to be used by the nuclear industry that rather see other benefits with using FPGA in the nuclear industry.

One of the advantages in nuclear related I&C with FPGA versus software (SW) based systems is that FPGAs are considered more deterministic and to have a more predicable execution and are hence easier to license. On the same theme, it is considered easier to demonstrate that the claims and assumptions that are made regarding the systems safety performance are valid using FPGA versus SW.

The first time I heard of FPGA at any NPIC&HMIT meeting was in 2006 in Albuquerque where Toshiba introduced an LPRM system implemented using FPGA, something Toshiba said would make it easier to license compared to a software based system because it was based on pure logic. This was encountered with very strong criticism from the audience at the meeting, which meant that

"Software IS logic" and hence, FPGA would have no benefit versus SW. A few years later, at the San Diego meeting in 2012, the wind had really turned for FPGA, and FPGA was then the biggest topic of the conference and then had 3 whole sessions dedicated. These sessions also attracted so many people that they had to switch to a larger room so that everyone could fit. At NPIC&HMIT in Charlotte in 2015, the interest had gone down somewhat but it was still a big topic. 9 FPGA presentations were held in 2015. At this meeting in San Francisco, FPGA was again a major topic and had 8 presentations in two sessions.

However, the NRC seems to regard and review FPGA almost equivalent to software in the licensing process, largely because different software tools are used in the development, design and management of FPGA. This means - at least in the US, that many of the benefits that were seen with FPGA with regards to licensing is actually not possible to gain. Rather the licensing process will be almost the same. This has somewhat cooled down the huge future seen for FPGA at the San Diego meeting in 2012.

It can be noted that the FPGA area has not taken the same big steps forward since the last conference in 2015 regarding the implementation of major modernization projects in the NPP. This is judged not to be due to any shortcomings in the FPGA technology, but primarily because the amount of major modernizations within NPP has ceased in recent years, as mentioned in the section above.

The exception may be China where, for example, Lockheed Martin has its FPGA based platform NuPAC installed for safety related systems. However, many utilities and plants have begun to use FPGA at component exchanges project where they want to re-manufacture an obsolete component with a new manufacturer (similar to Re-engineering). For example, the Ukrainian company Radiy (and its subsidiary RadICS LCC), can do Re-engineering and Form-Fit-Function replacement for components or systems using their FPGA based platform RadICS. Radiy has also used FPGA within NPP for a very long time (since early 2000s) and can be seen as one of the more experienced FPGA vendors in the nuclear industry.

Lockheed Martin also has a purely discreet logic platform, which is compatible with their NuPAC FPGA platform and also has the same fit/form and can thus be used to complement the FPGA platform with pure analog card/features for example provide self-monitoring using a different (diverse) technical principle, or to increase functional separation within the system. NuPAC can be configured to either share information between trains (local coincidence), or to not share information (central coincidence) depending on customer requirements and needs.

Richard Hite from Virginia Commonwealth University presented a system that they had developed, called SymPLe, which uses small function blocks that are then connected and burned into an FPGA chip. This provides a product that is considered easier to verify (and then ultimately license if you would go so far) and provide better overview and more deterministic behavior (easier to "prove" the end state and output). However, it is only possible to implement simpler functions, for example, advanced features such as graphical interfaces etc. cannot be built with this technique/system. Some tests have been performed with SymPLe on real NPP

features (e.g. Emergency diesel start logic and various PID controllers) and these have shown good functionality of the system. The product's great advantage would, according to the presenter, be these simple V&V. Research on COTS products projects shows that where the purchase price is in the order of 100-1000 USD, the cost of licensing and installation for the same component may be 10-100 MUSD when implemented in an NPP. The technique of SymPLe is in the "research stage" and if it becomes a real product for the customer market or it is not early to decide.

Part of the next step in SymPLe development is a system called BIO-SymPLe. This is a system and technology inspired by our immune system and stem cells. By using different "layers" of functions where one "layer" contains the active functions of the system (ie control, measurement, control, etc.) and another "layer" monitors the "health" of the active function layer. Simplified, it can be said that, in the case of detected errors, the monitoring layer can re-route the FPGA/SymPLe functions to "healthy" parts (logic blocks, intersections etc.) and thus the BIO-SymPLE board can "fix" itself. BIO-SymPLE is a very interesting system, however it probably lies even further in the future then the SymPLe system. However, this type of technology exists today in different parts of the world and is in use, even though it is at an early stage.

Something that was addressed already in 2015 was that many vendors mix SW and FPGA within the same system/components, and this seems even more common nowadays. You should look at the system as a whole entity and simply apply the most appropriate technology for each application/function to be handled. This mix is probably also partly due to the fact the NRC etc. is considering FPGA relatively similar to SW, and treats it the same in terms of licensing, and by that a large part of one of the main benefits with FPGA (easier to license compared to SW) goes lost and the driver to have a sole FPGA system decreases.

In summary, FPGA is beginning to be seen as a natural part of the I&C structure at NPP and it is here to stay. The major development predicted in 2012 did not really turn out, but it is more likely due to financial and political winds have influenced investments and modernizations at the plats rather then that technology did not live up to expectations.

4.5 WIRELESS APPLICATIONS IN NPP

Most of the other industry such as cars, and home applications are being connected wireless to provide more functions, and better usability. The use for wireless is obvious even in NPP but given the high safety requirements and the use of many times 30 years old electronics in many places means certain challenges for wireless to be used in NPP. Still many utilities and vendors believe that wireless is a good solution and will be a normal part of the nuclear industry in the future.

The topic of wireless applications has also been around for a few years at this conference. Typical applications in the NPP have been service functions such as maintenance data collection (self-monitoring, etc.), temporary measurement points for outage or hard-to-access locations. Often, you also use wireless applications

when you want to decrease the amount on cables or cable wiring and in some cases to keep down the amount of combustible material (in these case cables) in some areas.

As part of the Nuclear Promise, EPRI works with a project called *"Modular Wireless Sensor for Equipment Condition Monitoring"* and is a topic within both Wireless and OLM. Their perception of wireless was that one of the major challenges lies in battery time, if you have a device that can send the signal wirelessly but still need to be connected to the power grid for the power supply, very little has been gained and having to change batteries too often can "eat up" the cost savings made on the wireless installation. Their project is thus trying to find solutions to address this problem. E.g. they have developed systems that do not transmit data all the time, but collects data continuously and then "wakes up" the communication section and transmits large amounts of data at certain intervals. By this means, the goal is that the battery time of the equipment will be about two years. You also look at what is called *"Power Harvesting"*, where the sensor itself can gain energy from its given environment, e.g. use vibration and piezoelectric elements to allow the sensor to generate (subset of) its own energy from the process it is installed in. They also showed analysis of different protocols for communication requiring different amount of energy depending on frequency, distance, etc. By combining Power Harvesting, non-continuous data transfer, transmission rates and power requirements, EPRI aims to extend the battery time of wireless devices significantly. But they also say that there will be no specific universal solution that solves everything at every plant; rather it will be a plats and application specific analysis that will determine the best solution for the specific case. EPRI also states that apart from battery life, cyber security is one of the biggest challenges with wireless applications.

Last meeting, there were dedicated sessions for wireless applications but during this meeting there were no own sessions, instead there were presentations about wireless within NPP at other sessions (EMC, Maintenance Optimization, etc.). If the decreasing attention is due to decreasing interest or if the area is considered to have passed the News Stadium -and is now seen as a natural part and focus is on its applications, are uncertain, but many at the conference saw wirelessly as a natural part of today's I&C, even at NPP.

4.6 LEVELS OF AUTOMATION IN THE MCR

New I&C systems can automate almost every control action needed in a NPP today, and it can even be proved with tests that fewer mistakes are made using automated system control compared to human operator control. But do we really want to have no operator involvement at all in our plants? What happens if the systems fail and the operator then must take over and perform tasks/actions that he/she has not performed in years, or perhaps never before?

The question of the degree or levels of automation in MCR was raised many times during this conference. New I&C systems have many times the opportunity to completely take over the supervision and control of the plant, which risks passivizing the operators. At the same time, there is enormously great opportunity for the system to act quickly and analyze large amounts of data if functions are

automated. Thus, the balance between Automation and Operator Involvement is a somewhat nosy question that several institutes and universities are researching and several suppliers are also making great efforts. It is not about removing supervision or control of certain parts without redistributing the responsibility between Operator and System.

What is of great importance in this area is that operators are very well aware of how the technical system works and how its automation works. Compared to the aerospace industry that has come further in the automation of functions; there is a clear trend that accidents/incidents do not due to system or equipment failure rather that the operator/pilot has misunderstood the control system function or the distribution of tasks and responsibilities between System and Operator/Pilot. Such an example from San Francisco just happened in 2013 when a passenger plane (Asiana Airlines Flight 214) missed the runway during landing and the rear of the plane crashed into the dock (the runway starts right at the water). All systems had worked just as they should but in just this particular automation mode where the plane was about to land, the pilot should control the altitude of the plane, but the pilot thought the plane would handle this parameter. This was an exception to the normal distribution of tasks and was specific to this automation mode. When the pilot finally realized that the plane did not regulate the altitude, he pulled too hard on the flaps and the plane stall and lost speed and finally the tail hit the quayside and the plane crash landed.

Katya Le Blanc from Idaho National Laboratory said that many vendors and HMI designers actually added more interaction and operator involvement than the system actually needed. This was in order to "learn" and involve/enable the operators to a greater extent.

Generally, when some certain chores have become a habit they tend to go fast but give some careless mistakes. Take the example of a keyboard to a computer, we know where the different keys are placed and therefor often write quite fast but there will be some errors along the way. If you would change the positions of all the keys, you must look carefully before any downturn, which would probably generate fewer errors, but that would make the work much slower.

Future operators need not only be knowledgeable about the actual process they control and monitor, they must also be experts on the I&C systems they have at their disposal. Much goes in the direction that the system is more and more managing the process and operators is more monitoring that the operating systems work properly. Playfully, Rodger Lew from the University of Idaho said that in the future, only two employees will be required in a modern control room; a human and a dog. The human task is to feed the dog and the dog's task is to bite man if he/she tries to interfere with or adjust the control systems.

John O'Hara of Brookhaven National Laboratory had conducted a study of the degree of automation, and said that even if the system can run completely on its own, operators must be deeply involved in the development and design of system performance and appearance. And that extra attention and focus must be committed to obtaining and maintaining high operator skills with these new systems. Many times, the I&C system tends to have functions where the levels of

automation changes depending on different parameters such as the operation mode or the workload (amount of signals) to the operators, and it is therefore essential that operators always know exactly which mode or degree of automation the system is in right now and how the workload between system and operator is divided right now. The study showed that most operators found that systems with different degrees of automation were positive, but that many would like to choose themselves when a switch to a new automation mode should take place.

5 Other Areas

5.1 OTHER CONFERENCE NOTES

Following are a few notes from presentations, panels, conversations or other sessions. They are reproduced without any order or priority. Notes in any of the Trend areas summarized in Section 4 have been grouped into respective associated areas.

- Sofia Guerra from Adelard presented a work on comparing V&V for software based systems and FPGA based systems. The conclusion is that many parts are very similar but that differentiates when it comes to behavioral characteristics and the vulnerabilities of the different systems.
- Another aspect of the V&V area was raised by Richard Hite of Virginia Commonwealth University who pointed out that although a new system designed today actually does not contain software (or only minor features implemented in software), all systems and features today have been developed by tools and computer aids that contain software. Even for fully functional analogue systems and circuit boards that are being developed today; Gerber files (file formats used in circuit board manufacture), layout drawings, etc. are made using software based tools. This means that, for example, the manufacturing chain can have cyber security problems, etc. So to say that you can get rid of cyber security issues, CCF, licensing, etc. related to software just by using an analogue end product may depend entirely on the scope of your review.
- Many talked about the possibilities of "standardized" type reactors and type solutions as a way to keep costs down. EdF is an example of where this has been conducted for a long time. One of the presenters from the United States pointed to the differences between France and the United States in this case and said that some of the United States problems (with licensing, costs, etc.) are a result of having a too wide variety of reactor designs. *"In France, there are three types of nuclear reactors and 100 kinds of cheese, in the United States it's the opposite."*
- Next Generation of Reactor Operators and Shift Managers may be at the age of 10 today, how do they get them interested in nuclear power? NuScale has taken a little new grip on the question and invited children groups to their simulator to test operate and interact with the systems, which also gave rise to ideas about how future MCR (where these children are operators) can look and work.
- An area that has become more and more interesting to many is CGD (Commercial Grade Dedication), which means using equipment that was not originally designed for NPP safety applications. This is done by setting up programs for tests and certifications for this particular component in just one application and on a case-by-case basis, can justify a component of a safety system, even if it was not originally designed for this purpose.

Note that it is not about lowering the requirements but rather making more specific assessments. The reason for the growing interest is that very few suppliers now produce equipment according to NPP standards. For example, today when, almost all equipment contains software, it is very difficult to find certain types of transmitters designed according to the IEC standards applicable to, for example, 1E equipment. Being able to justify using a specific transmitter for the current application, by means of tests and analysis, is often the only option available if you have to change equipment. However, CGD is quite a workload in terms of both testing and paperwork. But is also an area in which the IAEA's I&C working group plans to do a job to facilitate the use of this method in different utilities. Today, at the Swedish NPP, there are a number of works that use this principle.

- Installations and major I&C modernizations often take longer time in installation and deployment phases than initially estimated and planned. A consequence will often be extended outages and production losses. Mark Peres from company Fluor made a comparison with the dance and theatrical world where you spend a lot of time on repetitions and preparations for the actual show, where everyone are involved in practicing and memorizing their role or part. Their experience of I&C installations in the NPP was that it was often expected that everything would go according to plan. Even if some risk analyzes were performed for certain events, the time spent on practicing and preparing in order to prevent these risks from falling out was too short. To have "general rehearsals" and larger preparations for some major jobs should be common practice according to Fluor.
- An area that many people talked about or started using was *"Augmented Reality"* -AR, where you can use a mobile/tablet or special AR glasses/screens where you can see, for example, a room via the screen, but also "add" some computer-animated items such as pumps or other equipment. This was often seen as a good tool for planning and installation preparation. However, it requires some technical infrastructure (often such as wireless networks, etc.) to be used optimally. As the video game industry has been a driving force in this area, technology has taken great steps forward while costs have fallen sharply in recent years. There are actually cooperation within Sweden (plants and KSU) to start looking into the possibilities to use this technique at Swedish NPP. An example of AR is shown in the picture below.

Picture from Google Picture Search

- John Lubinski at the NRC presented the NRC's *"Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure"*. He reported on 4 activities or "Modernization Plans" -MP that should be handled in order to facilitate the licensing process:
    - MP #1. Protection Against Common Cause Failure
    - MP #2. Considering Digital Instrumental & Control in Accordance with 10 CFR 50.59
    - MP #3. Commercial Grade Dedication of Digital Equipment
    - MP #4. Assessment for Modernization of the Instrument & Control Regulatory Infrastructure
- Alarm Management was also under discussion and one of the more interesting presentations was from Ian Nimmo from *"User Centered Design Service Inc"* that spoke about alarm priority and alarm overflow. He took examples from the oil industry where he showed two major fatal accidents where the lack of a functioning alarm system for the emerging situation meant that the operators could not handle or deal with the situation. At one of these events, operators received 20-30 alarms per minute and a total of 270 alarms in the first 11 minutes, were one hundred of them had a Priority Flag meaning they had to be managed within 3 minutes. This was obviously impossible for operators to handle and given the situation, not all alarms should have been prioritized, which also led operators to act on partially wrong things. Ian reflected that alarms are often associated with problems or something negative (e.g. a car alarm or an alarm clock), but what one should really be looking for is to warn the operators before anything happens so that they can avoid the upcoming situation or guide them into where to start acting. Studies show that engineers who work with a system often insert more alarms than needed and often overestimate the priority of alarms in their systems. An alarm should have an operator action associated; otherwise it's not an alarm but just plain information. Here Ian advocated that NPP should have alarms for operators in MCR, but also "Alarms" that go to Maintenance for action, and not have the Maintenance alarms go to the MCR for forwarding. And if

you have an alarm priority (as suggested), an assessment should be repeatedly made of the alarm priority. This is because the plant changes and operators learn what they need to see and what they need help with. There should also be some limitations in the alarm levels, such as only 5% can be priority 1, 18% priority 2 etc. so that not everything becomes priority 1 because then the entire prioritization idea fails. Ian also said that engineers often start from the process and process flow when developing HMI and alarm systems. However, if you look at the interface of a modern car, the driver information on the dashboard shows no process flow at all (e.g. gasoline> carburetor-> engine and gearbox) but is rather showing a variety of parameters considered important to the driver (speed, engine rpm, engine temperature etc.) without taking into consideration how these parameters relate to each other in the process flow. Yet all car drivers think that the information is logical. HMI and alarm systems in industries can learn from, for example, cars, smartphones and other more conventional interfaces, Ian said.

- Dennis Milson from Curtis Wright talked about their experiences from a project concerning the Krsko NPP Emergency Control Room. The project was actually relatively simple in terms of technology, but was made difficult by the huge amount of signals (i.e. cables) that were coming in and out of the cabinets, and as in this case meant making some special solutions on cabinets and peripherals. He meant that in this type of project it is important to identify the most difficult task in the project early, and to work on solving that task first. And if you fail to get a grip on the solution of the difficult task early, this must be addressed to the customer (in this case Krsko). The American Navy apparently had an old saying for this: *"When in danger or in doubt, run in circles, scream and shout. Do not go as everything was going well"*. Something that is quite similar to the Swedish model STARK.
- The NRC is starting to look more and more at CCF at component level rather than at system or functional level. Since a certain digital component may exist in several different systems and perhaps from different vendors, this approach can be problematic for NPP. Richard Wood of the University of Tennessee worked on this issue in a research project and called such components Embedded Digital Device -EDD, and attempted to find methods to exclude CCF in these EDDs by analyzing the actual component. One way to do this is to create "mutants" in the code (simulating functions that have been corrupted by any event/CCI) and then see if the system successfully identifies these mutants. Richard believes that in this way (or any way at all actually), one cannot prove that the system is safe from CCF. But by doing this, it can be demonstrated to a great extent that you have tested as much as possible and that you have done a lot of work to minimize those parts that you cannot verify with tests. This should ease the dialogue with the NRC in the CCF issue.
- There were also a large number of presentations on different types of process analysis and parameter prediction and parameter simulation tools (similar to Process+ used at Forsmark). These can -by including a large

number of measurement values and process knowledge in systems, predict parameters and values in the process and thus reduce the number of transmitters and measurement equipment as the program simulates and predicts a certain value instead of having conventional measuring equipment. There are many such programs in laboratories and within research today, but also a number of cases were NPP uses applications in this way. The simulated values are exclusive of service, Maintenance, or non-safety character. No safety related values or parameters are simulated today, even if you be some means can see a parameter such as thermal power as a simulated parameter that is calculated based on other measurement values.

- The company Lockheed Martin showed a tool that could generate testable logic functions based on a Visio model, meaning that some designs could be tested at a very early stage.
- Standards and guide lines are a big concept within the nuclear world, including I&C and HMI. The IAEA and IEC are some of the institutes that produce the most standards and guides internationally, but in the US, the NRC and IEEE are often referred to in this area. 2 sessions in General Standards, 1 within HMI related standards were held and these sessions contained 13 presentations. In addition to this, there were a number of panel discussions within standards and also some sessions directed at specific guide, such as the panel session *"Experience with NUREG-0711 Rev 3 - Panel"*. A problem with standards previously mentioned is the long development time that different standards have in their organizations (often 2-4 years) and that this becomes increasingly problematic within areas such as digital equipment or cyber security were both areas often have very rapid development and quick rate of change.
- Although Re-engineering did not have any own sessions this time, it was still a topical subject, perhaps more than ever since many see the cost benefits of re-engineering in many cases. Companies involved in re-engineering (such as ATC and Curtis Wright et al.) were attending the conference exhibition and many NPP talked about re-engineering as something that was now used as a normal routine. Other suppliers also had concepts where they did some major modernizations and, in some cases, did not replace all equipment, but used re-engineering to manufacture spare parts for some of the systems they modernized.

6 Conclusions

Although nuclear plants are being built at several locations in the world at this time, it is many times not without problems that these designs proceed. In particular in the western world, NPP new builds are struggling with delays and increasing cost. In Asia however, the new builds are going according to plan without the problems seen in the west.

The call for lowering costs and increasing availability at existing NPP has made a big impact on this year's conference. Particular, it was a great focus on how the plants could benefit from modern I&C to provide a more optimized Operation and Maintenance.

A somewhat new trend was observed during this year's conference; and that was to focus on promoting nuclear power from its environmental positive aspects with low CO2 emissions and high availability. This also made a mark in the conference content.

It is believed that in order to provide the amount of clean reliable electrical energy needed to lift large parts of the world out of poverty, there is no alternative to nuclear. But in order for this to happen, nuclear power must be compatible in terms of cost.

The conference was very interesting and informative and covers very many aspects of the I&C and HMI that is used in NPP today, and in the future. This conference is most likely the biggest and most comprehensive event within nuclear I&C in the world and it is important that experiences and results can be obtained even for the Nordic market.

Although the conference is going on for a week, there are many parallel sessions at all times making it hard to attend even half of what is considered interesting. And therefore the content of this report should be seen as what was covered by the author and not what was presented at the whole conference.

Considering the trends and topics mentioned in this report the following areas are recommended by the author for Energiforsk to consider as future project areas:

- Using modern I&C application for optimizing Operation and Maintenance
- Hands-on guidance for Practical Cyber Security Plans at Nordic NPP´s
- Re-engineering "complex functions" using FPGA
- Possible infrastructure for Wireless in Nordic NPP´s
- Commercial Grade Item Dedication

This report was made in cooperation between Energiforsk and the nuclear industry (in this case Forsmarks Kraftgrupp AB) and it is believed that this type of cooperation is very rewarding to both parties, bringing research and industry closer together.

TRENDS IN NUCLEAR INSTRUMENTATION AND CONTROL SYSTEMS 2017

This report summarizes the impressions and reflection from a larger nuclear instrumentation and control and Human-Machine Interface conference in San Francisco, USA.

The report highlights important trends or topics that were mentioned at the conference as well as personal views on how these trends affect or could be of interest to the Nordic nuclear power plants.

Characteristic for the conference was the downward pressure on cost and price within large parts of electricity production, not least the nuclear power, and how it affects operation/maintenance and modernization of nuclear power plants.

Energiforsk is the Swedish Energy Research Centre – an industrially owned body dedicated to meeting the common energy challenges faced by industries, authorities and society. Our vision is to be hub of Swedish energy research and our mission is to make the world of energy smarter!

Energiforsk