Recommendations by TWG-NPPIC Member States as stated in their Country Report Presentations

22-24 May 2013, Vienna, Austria

Argentina

- Reduction of unnecessary workloads and human errors recommending change from manual actions to automation actions, controlled by operators (OLM)
- Recommend examine other risk industries, adapt their best practices, adopt the new technologies they use (Cyber security, COTS, Wireless communications)
- Shared simulation environments, common testing environments and capabilities between countries sponsored by IAEA
- Electro-Magnetic Compatibility TWG or WS to study RF in Wireless systems in NPP.
- Control room operability in severe accident sequences (primary protections, redundancy, wireless communications)
- Recommend countries to change their obsolete I&C systems with new technologies. Communicate study cases (countries) and promote providers workshops in those countries with old technologies.
- Simplify, Reduce Standards and help to understand concepts to members

Brazil

- Harmonization for digital I&C licensing
  - from safety systems to HMI
- Safety assessment of digital I&C
  - including diversity, CMF, Software V&V and best practices
- Other industries
  - examination of other industries best practices and technologies (should the incorporation of other industries experiences be a goal?)
- Human factors and digital I&C
  - from control room conception in the digital age to awareness and management of the overwhelming information flow allowed by new technologies

Canada

- Harmonization of international standards for
  - Qualification of important to safety I&C equipment
  - Cyber security for real time systems
  - Coordinated emergency response
  - FPGA technologies – emphasis on development and V&V

    - Reliability testing (Statistical) for safety systems
- Instrumentation for Design Extension Conditions
    - High Temperature Operation
    - Hydrogen Monitoring
    - Survivability Assessments
- Role of secondary control area
    - Manual Overrides for automatic safety functions
- Digital Communication
    - Guidance for Unidirectional Links
    - Guidance for bidirectional safety communication for normal control

China

- IAEA has complete set of 'Requirements' and 'Guides', but there is no 'Standard ' which can be used as support of the Requirements and Guides, and can give more detail instructions for implementation. On the other hand, when applying IEC standards, it's also lack of instruction or endorsed by the top level Code and Guidance. We suggest IAEA and IEC work more closely, to setup a complete series of 'Requirements-Guides-Standards' system.
- IAEA to support more education and training actives for I&C application in NPP depends on need.
- Enhance corporation and communication on technical research, such as, on software reliability study, on Human Risk Analysis (HRA) , and on advanced surveillance and diagnosis system of NPP study, etc.
- Further study is need on 'availability of I&C device', especially during and after severe accident, and the environment qualification requirements, the seismic margin requirements, etc. What those requirements for NPP already in service, and what those requirements for new NPP.
- Co-research on dealing with common mode failure of software based safety system and diversity requirement, IAEA please give more clear opinion.
- Co-research on I&C improvements after Fukushima accident, IAEA to give clear opinion or guidance.
- Co- research on DVU based control room, operating experience collection, sharing the benefit gets and the deficiency need to be improved.
- For NPP, normally full scope simulator is need for operator training one year before fuel load, but full scope simulator build rely on NPP design data, such as core design data, process systems design data, control system configuration and HMI final design results, so on. Some time there are mismatch between schedules, Please IAEA membership give some advice on this based on their experience.
- Suggest IAEA to constitute guidance on Commercial Grand Dedication activities for equipment (including spare parts) to be used in safety system of NPP.

Czech Republic

- Severe Accident Monitoring

  Motivation

  - There are not many recent guides or standards for accident monitoring (IEEE 497 / RG 1.97)
  - In the light of post-Fukushima improvements, updated guidelines for accident monitoring are needed (i.e. equipment qualification for severe accidents etc.)

  Goal

  - To define requirements/recommendations on severe accident I&C
- Cyber Security

  Motivation

  - Cyber security is an essential part of overall safety
  - It introduces new types of threats, requirements and measures
  - There are many sources of information for IT security area
  - There are several ongoing activities for nuclear area (EPRI, IEC 62645, IEC 62859, NRC RG 5.71,…)
  - No real IAEA guides exist (IAEA NSS No.17)

  Goal

  - To create cyber security guide which would focus on nuclear specific issues (such as safety versus security or overall I&C architecture)
- Process Performance Optimization

  Motivation

  - Deep view inside the process
  - Understand the actual plant thermal performance
  - Performance parameter calculation enhancement
  - Process and equipment imperfection early warning
  - Finding lost megawatts

  Goal

  - To create practical guide which would focus on enhancement of right process information
  - To organize technical meeting with topic – process performance optimization

Finland

- Guidance and support material should be developed for more systematic evaluation of software intensive I&C systems.
- Guidance and support material should be developed also for evaluation methods and processes for software only, because traditional methods and models do not work so well for software.
- IAEA should support development of a global market of nuclear safety I&C equipment.

- A common type approval or product certification practice for field instruments, platforms etc. is necessary for this purpose.
- A common (European) practice would be a remarkable step forward.
- Harmonization of standards.
- Harmonization of definitions and terms.
- Guidance and recommendations to decrease complexity in I&C architecture, design, implementation etc. which causes extra work, extra cost, extra difficulties for V&V.
- Digital I&C PRA
- Software reliability

France

EDF considers that most of the topics provided at the previous TWG-NPPIC meeting (2011) are still current topics on which IAEA should focus.

- Maintaining the existing Nuclear Power Plants (old and recent) with a High Safety level:
  - Rising up the Safety Level of old plants, in order to achieve the best accessible Safety level (but not necessary the current Safety level applicable to the new NPPs).
  - Post-Fukushima actions: exchange on the best practices.
  - Survey the ageing of I&C equipment and control the Obsolescence (analog as well as digital equipment, cabling, connectors…):
    - Understanding of ageing mechanisms.
    - Maintenance strategies: e.g. periodic replacement or on failure?
    - Evaluation of costs, risks, benefits of different I&C maintenance options: modernization, repair….
    - How to deal with the short life time of the new digital system (software evolution…)? Implement each new software release?
  - Integrate the ageing workforce, the "inadequate" existing documentation and the new generation in a long-term management of I&C expertise :
    - Identification and documentation of key knowledge, including I&C design basis.
    - How to retrieve, rebuild, structure and pass the documented knowledge to the new generation?

How to attract and keep the new generation? How to train the current I&C engineers to the new technologies?

- Safe Aspects :
  - International consensus on Safety requirements for new NPPs
    - Define more precisely the Safety Level to reach: between the high level requirements and the National Regulator requirement/IEC Standards.

    - Define a minimal number of unavoidable requirements (from various standards, norms, rules…) that all the units must satisfy for their I&C architecture and components.

- Efficiency Aspect
  - Specification & Design of I&C architecture taking lifetime into account. Product Lifecycle Management (PLM) : requirements traceability, Modification…
  - Methods & tools for Plant performance improvement:
    - New technologies for reduction of uncertainties in measurements to increase power output while maintaining safety margins
    - Reduction of likelihood of human errors
    - Reduction of operation & maintenance costs (information systems, on-line monitoring, diagnostic…)
- New Technologies - Impact
  - Evaluation of COTS I&C equipment and I&C architecture
    - I&C platforms, architecture, "smart" devices… (we are at the limits of the acceptable complexity)
    - Representation of digital systems in probabilistic models
    - Realistic consideration for assessment of software (system + application) : Verification and Validation (tests) as complementary tools. Test coverage. Software common cause failures
    - Classified HIS : same interface for the operator (HF aspect)
- New Technologies - Impact (cont.)
  - Regulatory uncertainties regarding "new" technologies : ASICs / FPGAs, Smart Devices, Data communication networks (including fieldbus), Wireless technologies,
- Cyber-security
- SMR (Small Modular Reactor)
  - Impact on Safety and Security rules of a centralized CR for multiple small reactors
  - Level of automation (because of reduced team for operation)

<u>Germany</u>

- Cyber-security
  - Attacks from networks
  - Malware
    - Initiated during system development
    - Inserted during maintenance
- Accident monitoring and management

- Monitoring and control of severe accidents and post severe accident conditions
  - Control of severe accident conditions e.g. hydrogen
  - Monitoring of spent fuel pools
  - Long term emergency power supply by emergency diesel generators

- Software (or digital I&C) issues (evaluation, reliability assessment, etc.)
  - Evaluation of reliability of modern I&C based on software or FPGA technology
    - Complexity of I&C systems, equipment, software and FPGA
    - Concentration of functions on single CPUs vs. parallel computation of functions in a FPGA
    - Qualification and use of FPGA and similar "hard programmed" equipment
    - Use of I&C equipment not designed for use in NPPs in nuclear safety applications
    - Evaluation of software reliability
- Recommended WS / training course topics
  - Harmonization of licensing processes for safety I&C systems

<u>Hungary</u>

- Role of I&C in BDBA and SA situations
  - I&C designs to cope with BDB and severe accidents
  - Improved ("hardened") instrumentation and process monitoring
  - Improved emergency response capabilities, including
    - on-site support (with the capability to handle multi-unit accidents)
    - off-site support (with simulation, planning + prediction capabilities)
    - improved training (with advanced simulation + visualization tools)
- Harmonization of I&C standards and safety regulations
  - Focusing on safety I&C requirements for new plants
  - International co-operation to establish a reference safety I&C architecture for LWR plants
- Computer security protection measures
- Special considerations for the I&C design of the new plants
  - Relatively long time between bidding and commissioning and very short life cycle of the I&C *(How to avoid obsolescence already at commissioning?)*
  - Design for easy refurbishment during the long service life of the plant
  - Design for supporting configuration management
  - Design tools in general, and integration of the tools of different areas
  - The role of the simulators in the design of I&C

- Technical missions to the different stakeholders
  - Nuclear I&C training for utilities and regulators,
  - IERICS to the utilities, evaluating design solutions prior to installation,
  - ICSAS missions,

India

In the present plants the HW and SW is very diverse in nature. We are planning to standardize the same by using identical HW and SW. Therefore, the following activities are planned and expected to be completed by 2016-17.

- Development of Hardware
  - Hardwired Protective systems
  - Hardware modules for digital C&I systems
- Development of Software,
  - Real time executive
  - Application Program for embedded systems
  - HSI Software

Japan

- Wireless Technology for Control Systems and Safety Systems in NPPs
- Decision Making Support System at Severe Accident at NPPs
- Roles and Functions of Main Control Room and Remote Control Room for Mitigating Severe Accident at NPPs

Korea, Republic of

- Digitalized MMIS for NPP with safety, reliability and maintenance ability
- Modernization of NPP with digitalized MMIS
  - Based on unification design of PLC/DCS Platform, fully digitalized MMIS system replacement is recommended.
  - Considering overhaul schedule and limited installation period, the scale of target systems should be selected at each phase in detail.
  - Integrated MMIS prototype facility could be used.
- Licensing requirements for cyber security
  - Technical standard and strict requirement for cyber security including penetration test is essential for PJT execution in advance.
- Seismic requirements for LDP
  - Operator's safety coverage during seismic event

- Just falling down of LDP screen not be considered as missile hazard behavior

– 3rd party controller for NPP using FPGA platform
  - Verification method for application software constructed by gate array
  - Fault detection and self-diagnostic method suited for the FPGA platform

Pakistan

– Implementation of Human Factor Engineering in Digital MCR
– Behavior of MCR in Severe Accidents
– Post-accident Monitoring and emergency preparedness
– Methodology to address the obsolescence of I&C equipment / system
– Adaptation of new technologies in running NPPs
– Harmonization of I&C safety classification and code & standards

Russia

– Further development of the requirements to safety and safety-related systems design and operation after Fukushima NPP accident (meetings, conference, TECDOC).
– Post-accidents monitoring systems (meetings on the philosophy, principles, requirements, good practices, TECDOC, Coordinated Research Program).
– I&C design for NPP of small power, including I&C for floating NPP, taking into account their peculiarities (meetings, TECDOCs)
– Development of HMI to support the cognitive activity of NPP operators and enhance NPP operational performance (meetings, TECDOCs).
– Transference of principles of independency and physical separation to APCS upper level (meeting or special topic in other meetings).
– Further development of methods and tools for NPP I&C V&V (meetings, TECDOC on new approaches and good practices).
– Knowledge management in the organizations which are designing and operating NPP I&C, first of all, I&C for reactor control and protection (participation of I&C specialists in KM schools, in Italy, Russia and others, cooperation with IAEA KM section).

Spain

– About evaluation of the Safety Level
  - Avoid different interpretations
  - To elaborate a common framework to perform audits on current safety level by an independent entity
  - To define or assess the software reliability in digital systems

- About COTS I&C equipment
  - "Smart" devices dedication optimization (Spain is working since 2010)
  - Use of SIL Level? Gap between IEC-61508 & IEC-61513
  - List of dedicated COTS I&C equipment in order to reduce costs?
- About regulatory position
  - FPGAs
  - Wireless technologies
  - Cyber-security

Sweden

- Safety vs Security
  - What type of security (if any) should be implemented in safety I&C.
- Spread the knewledge of how to get a proper design (all the way from need-standards-requirements- …. -installation-verification-documentation). Missing fundamental knewledge about proper way to make good verified designs. Competence and how to keep it. Learn by history.
- Software (and systems) VoV and Qualification.

Switzerland

- Beyond design basis accidents
  - a. Design modifications to mitigate severe accidents
  - b. Seismic trip systems, severe accident monitoring
  - c. Control room operability in severe accident sequences (primary protections, redundancy)
  - d. Improved instrumentation, communication networks, etc.
  - e. Improved emergency response plans including command and control, off-site preparations and off-site support
  - f. How far beyond?
  - g. Datalinks to regulator
  - h. Crisis centers
- People" support
  - c. Training, pre-job briefing
  - d. Knowledge management, knowledge capture and retention, knowledge presentation
  - e. Emergency preparedness special trainings for emergencies and simulations
  - i. Reduction of human errors
- Cyber security (high)
  - a. Vulnerability of digital I&C systems in NPPs' control and safety systems
- Standards, requirements and regulations, safety classifications, definitions

    - a. Harmonization and reduction (first, in safety systems only)
    - b. Assistance with standards interpretation
    - c. Harmonization of definitions
- Information management and sharing (medium)
    - a. Develop an information sharing system
    - b. Lessons learned from incident reporting systems databases
    - d. Network of I&C experts
- IAEA should take a lead in analysis of I&C operations during and after Fukushima accident progressions and publish report
- Wireless technology in normal operations and accident conditions
- Online monitoring, diagnostics and prognostics
    - a. How to separate process effects from sensor effects
    - b. Adequacy of periodic testing

<u>UK</u>

- Estimating and extending life of I&C equipment to address ageing and obsolescence.
- Supporting the evaluation, acceptance and licensing of digital I&C system.
- Lessons learned from I&C project implementation: guidance for modernisation and new plant projects.
- Design and management of I&C systems for future upgrading
    - This relates to the problem of the much shorter life that can be expected from I&C systems in comparison to that of NPPs.
    - It is proposed that the 'research' could address:
        - the techniques that may be used at the design stage to promote future upgrading,
        - the measures that would also be needed to ensure that the ability for future upgrading is retained,
        - the experience available of adopting such techniques and measures,
        - recommendations to I&C system specifiers, I&C system suppliers and NPP operators arising from the above.

<u>Ukraine</u>

- “Peopleware” support and development:
    - Knowledge management for safety culture supporting
    - Key Performance Indicators (KPIs) for knowledge management assessment
- Standards requirements and regulations, safety classifications, definitions:

- Harmonization

– Information management and sharing:
  - Experts communications development and improvement
  - Awareness about best practices and success stories in new I&C technologies implementations (FPGAs, wireless etc.)

– Cyber security:
  - Safety – Security relations
  - Cyber security defensive measures

USA (additions to the 2011 recommendations)

1. "People" support (high)
   a. Human cognitive based modeling, simulation and design
   b. Human productivity improvement support systems
   c. Training, pre-job briefing
   d. Knowledge management, knowledge capture and retention, knowledge presentation
   e. Emergency preparedness special trainings for emergencies and simulations
   f. Reduction of unnecessary workloads and stress, manual vs. automation
   g. Attract new people and retain them
   h. Balance of his safety interconnections
   i. Reduction of human errors
   j. Support for field workers – smart devices and 2 way communications with information sources and experts (include addressing cyber and EMC issues)
   k. Teamwork and appropriate function allocation between human and automation as automation increases
   l. Technical basis for control room staffing for small modular reactors
2. Standards, requirements and regulations, safety classifications, definitions (high)
   a. Harmonization and reduction (first, in safety systems only)
   b. Assistance with standards interpretation
   c. Harmonization of definitions
   d. Approaches for increased likelihood of international acceptance of digital systems – alternative/complement to harmonization
3. Information management and sharing (medium)
   a. Develop an information sharing system
   b. Lessons learned from incident reporting systems databases
   c. Examine other industries, adapt best practices, new technologies
   d. Network of I&C experts
4. Modeling and simulation (medium)
   a. Sponsor I&C simulators
   b. Shared simulation environments, common testing environments and capabilities
5. Cyber security (high)
   a. Vulnerability of digital I&C systems in NPPs' control and safety systems
   b. System designs for resiliency to cyber intrusions
6. Supply chain (medium)
   a. Commercial-of-the-shelf
   b. Obsolescence (including parts of equipment over construction period)
   c. Counterfeit, fraudulent, etc. parts
7. Beyond design basis accidents (high)
   a. Design modifications to mitigate severe accidents
   b. Seismic trip systems, severe accident monitoring

c. Control room operability in severe accident sequences (primary protections, redundancy)
d. Improved instrumentation, communication networks, etc.
e. Improved emergency response plans including command and control, off-site preparations and off-site support
f. How far beyond?
g. Datalinks to regulator
h. Crisis centers
i. Remote access to plant sensor data