International Conference
Nuclear Energy for New Europe 2005
Bled, Slovenia, September 5-8, 2005

SOME ASPECTS OF DIGITAL I&C AND DIGITAL HUMAN-SYSTEM INTERFACE UPGRADES IN NUCLEAR POWER PLANTS

Damir Mandić
Nuklearna elektrarna Krško -NEK
Vrbina 12, SI-8270 Krško, Slovenia
dmandic@nek.si

ABSTRACT

Digital I&C technology introduces some new terms and new processes like software life cycle, process computer configuration control, digital human-system interface (HSI), software V&V (Verification & Validation), software common mode failure potential, software documentation, etc. Based on the experience from NEK, and other NPPs and published reports from other organizations, this paper sheds light on challenging tasks related to some aspects of the digital I&C upgrades and especially the **NPP MCR/MCB HSI** (**N**uclear **P**ower **P**lant **M**ain **C**ontrol **R**oom / **M**ain **C**ontrol **B**oard **H**uman-**S**ystem **I**nterface) upgrade. The Ref. [1], EPRI Report TR-1008122 was used as a guidance to analyze original NEK MCR/MCB HSI design (1970s), to describe migration from the original MCR/MCB HSI design to the 2005 AS-BUILT status and to propose the authors vision for the key planning aspects for I&C upgrades and MCR modernization. This paper submits the justified proposal for the endpoint vision and the migration path applicable to NEK MCR/MCB HSI modernization, as well as some of the possible risks and lessons learned.

1 INTRODUCTION

While producing electricity in a productive and efficient manner, operating NPPs strictly follow safety and reliability requirements. In order to continue meeting safety and reliability requirements and at the same time to optimize nuclear power plant operating costs, NPP licensees must be able to replace and upgrade equipment in a cost effective manner. In the last thirty years no other plant technology has passed through so spectacular development process as Instrumentation and Control (I&C) systems. All nuclear power plants, which comply with the US nuclear regulatory requirements, hindered implementation of the major I&C platform upgrades in nuclear power plants. The root cause for the NPPs hindered major digital I&C upgrades was in uncertainty regarding licensing. Attempts to clarify and harmonize regulatory requirements lasted almost ten years and that subject is summarized in the material Ref. [2], and it is partially quoted in this introduction. Implementation of the programmable digital systems has raised serious new issues related to the design, licensing, configuration control and Human System Interface (HSI) of the programmable digital I&C systems. Upgrades of the I&C systems can range from simple replacement of analog devices (pen chart recorder or single loop controller) with programmable digital technology (digital LCD recorder, digital single loop controller), to the implementation of new digital I&C

platform that is more or less integrated to include all plant I&C systems, and finally to the development and implementation of sophisticated software support like computer based operator procedures and other Computerized Operator Support Systems (COSS) software applications. Modifications of the existing digital I&C systems are also considered as digital I&C upgrade. Ambiguities that existed regarding the issue of digital upgrade licensing were resolved after the References [3], [4], and [5] were published. Programmable digital systems provide large variety of revolutionary new means for HSI design and implementation. Before the References [1] and [6] were published, there was no consistent and integrated guidance related to the digital HSI upgrade planning, specification, design, licensing, implementation, training, operation, maintenance and the Human Factors Engineering (HFE) program development related to the NPP MCR modernization. Regulatory requirements related to the specifics of digital upgrades were defined for safety systems, only. Regarding the non safety applications of the programmable digital systems, the general regulatory standpoint is that the decision about the degree of implementation of some of the regulatory requirements, that are originally intended to be used for safety related applications, only depends on the quality requirements for each particular application and on the programmable digital system quality that a plant licensee wants to achieve.

Ambiguities and lack of guidance did not completely prevent implementation of programmable digital I&C components/systems in NPPs. Moreover, it certainly did not prevent vendors to develop, market and sell programmable digital I&C systems to NPPs. Today, the programmable digital I&C components and systems can be found in numerous mostly non safety related applications in many NPPs. Concerning the 40 years of the designed plant life and life extension programs that could lead up to the plant life of 60 years, most of the plants that operate in compliance with the US codes are faced with the need to replace their I&C platform together with safety related I&C portion at least once in their life cycle.

A design of a new plant and a new main control room is not so challenging from the HSI point of view as a modernization of the existing MCR in the operating NPP.

When designing a new plant, the control room can be designed from the ground up, starting essentially with a clean sheet of paper. However, when modernizing an existing control room the starting point is what exists now, its design basis, and how it is operated. To define endpoint for the modernized control room, it is important to first establish the concepts behind the design and operation of the existing control room. (Ref. [1], 2.2.4.1, page 2-33)

The Krško NPP – NEK is not an exception from the family of other NPPs that were built and that operate in compliance with the US codes. NEK is a PWR plant (Westinghouse, two loop, 700 MW), that had the first synchronization in 1981. Its commercial operation started two years later. During twenty two years of commercial operation many modifications have been implemented (more than 400), and most of them included some kind of a HSI change, there was a significant number of modifications that included digital I&C and digital HSI upgrades, and there were few tens of modifications that included digital I&C upgrades with impact to the MCR/MCB HSI. After the NEK Engineering Services Division was founded in 1992, NEK has developed several programs and corresponding implementation procedures that deal with the 10CFR50 Appendix B quality criteria. For the purpose of this paper, two NEK programs are emphasized: Design Modification Control Program (Ref. [7]) and Process Computers Configuration Control (Ref. [8]). Up to now, NEK has not developed the MCR endpoint vision, a migration path, HFE program, plans and procedures for individual modifications and licensing plan as proposed by the documents Ref. [1] and [6].

In order to explain historic migration from the original design to the present solution of MCR/MCB HSI and to propose the way to define a control room endpoint vision and a future migration path, this paper presents author's interpretation and application of the guidance presented in the Ref. [1] to the Krško NPP – NEK.

2 MIGRATION FROM THE ORIGINAL DESIGN TO THE AS-BUILT 2005

2.1 The original MCR/MCB HSI design

Although 30 years old, the original MCR/MCB HSI design had some digital I&C equipment, some digital HSI and even at that time it could rather be classified as a hybrid MCR/MCB than the complete traditional or pure analog MCR/MCB. Digital I&C equipment and digital HSI was designed for both supervision and control and it existed on all three main workplaces regarding the MCR/MCB concept of operation (on MCB, on operator workplaces or desks within/in front the MCB horseshoe and "behind" the MCB). The following chapter helps understand the concepts behind the original design and operation of the control room.

The "U" shaped MCB consists of three main parts. The first from the bottom, was designed as a control desk with operator manual controls (switches, auto/manual stations, pushbuttons, dials, potentiometers) and indications associated with those controls (indicating lamps for valve status indication, breaker status indication, etc.). The middle or the vertical portion of the MCB was designed mostly for indication and it accommodated indicators, paper chart recorders and status light boxes ("sugar cube" type). The upper part of MCB, just below the ceiling and the same portion of auxiliary control boards and panels were designed to accommodate 29 annunciator panels with total of more than 1200 alarm windows.

The main digital equipment and digital HSI implemented in the original design of the MCB were four operator panels (push-buttons, indicating lights/pushbuttons, four digital indicators – projection type to the frost glass window) and the CRT (alpha numeric black & white) with CRT functional keyboard that were all associated with the DEH (Digital Electro Hydraulic) system for the control and supervision of the TG (Turbine – Generator) set.

The digital I&C system and digital HSI that was implemented on the operator workplaces-desks within the MCB horseshoe was related to the plant computer. The plant computer had about 600 hardwired field inputs and it was used to perform some specific nuclear calculations, online calorimetric calculations, to alarm operators regarding the status of input signals and calculated values, and to support data collection during the in-core flux mapping. The plant computer HSI consisted of three printers, operator console with functional push-buttons and two digital projection type indicators, the alpha-numeric black&white CRT and "fast & loud" line printer installed behind the MCB (in the plant computer room).

The main digital equipment and digital HSI implemented in the original design behind the MCB was the central unit of the temperature scanner system. The temperature scanner was a distributed temperature monitoring system with seven field data acquisition units that were used for acquisition of more than 700 temperature measurement signals (RTDs or TCs) related to signals of smaller importance. Because of the "behind the MCB" location of the central temperature scanner unit, the MCR operators were not able to see the HSI of that device from their regular work places. There was only one MCB annunciator alarm window (GENERAL WARNING) that would warn operators of a temperature scanner signal that needs operator's attention. To assess that warning, operator would have to walk behind the MCB and either read (digital, seven-segment LED indicator) or print (miniature, cash register type printer) data from the temperature scanner central unit.

2.2 Migration from the original MCR/MCB HSI design to the 2005 AS-BUILT

Since NEK was constructed according to the original plant design a number of modifications have been implemented thus changing the design of plant HSI. The major implemented modifications that included some form of digital I&C upgrade, including those that affected the original MCR/MCB HSI design, are listed in Table 1, together with their title-description and basic determinants regarding the installed HSI.

Table 1: Major NEK modifications implemented since 1983 that included digital I&C and HSI

NEK MODIFICATION that includes digital I&C and digital HSI	**HSI of digital I&C installed in**					**Comment**
	A	**B**	**C**	**D**	**E**	
AMSAC (ATWAS Mitigation Safeguard Actuation Circuitry)				X		HSI is used for maintenance only. **PIS, ANN**
ICCMS (Inadequate Core Cooling Monitoring Sys.), includes RVLIS, SMS	X			X		MCB HSI includes six analog and two digital (bar graph) indicators. **PIS, ANN**
PIS – Process Information System (includes SPDS or CFMS and many other nuclear specific applications and standard process monitoring functions)	X	X			X	MCB HSI includes 3 LCD & trackballs. MCR operator workplaces have 11 computer workstations sets (LCD, keyb., trackball), 2 OWS in TSC & 2 OWS in OSC. **ANN**
Chemnet – Off-line data acq. of chemical analysis data (prim & sec. sampling)					X	PC type workstations in chem. laboratories and some offices. Data link to → **PIS**
River Dam Control					X	Local Control and HSI, only. **PIS, ANN**
RCP Vibration Monitoring					X	Installed in a room close to MCR. **PIS, ANN**
TU Vibration Monitoring				X	X	In MCR and room close to MCR. **PIS, ANN**
Loose Parts Monitoring System- DMIMS				X		In computer room in MCR area. **PIS, ANN**
Seismic Instrumentation				X		In MCR area, behind the MCB. **PIS, ANN**
BEACON (Core Monitoring)					X	Installed in a room close to MCR. **PIS, ANN**
Meteorological Monitoring System				X	X	PC type workstation in SE (Shift Engineer) room. Other equip. out of MCR. **PIS**
SG Blowdown Control (digital discrete controllers and digital indicators)	X				X	2 digital indicat. on MCB. Field cabinet with digital controllers and indicators. **PIS, ANN**
Heater Drain Control, PLC					X	Local control & HSI only. **PIS, ANN**
Condensate Polishing, PLC					X	Local control & HSI only. **PIS, ANN**
IDDS, In-Drum Drying System, PLC					X	Local control & HSI only. **ANN**
Water Treatment, PLC					X	Local control & HSI only. **PIS, ANN**
Auxiliary Steam Boiler Control, PLC					X	Local control & HSI only. **PIS, ANN**
Switchyard Control & Monitoring (ABB MICRO SCADA – although it has remote control capabilities in the MCR it is used for switchyard monitoring only)		**Until 2006**			X	One computer workstation is installed at the EEO (Electrical Equipment Operator) workplace in MCR as a temporary solution until the outage 2006. After that all alarm log data will be available on PIS only. **PIS**
MCB Annunciator System	X	**Temporary**		X		The new annunciator panels look the same as the old ones. LCD Desktop (alarm log EDU) is installed on the SF (Shift Foreman) desk as a temporary solution. All ANN alarms (with the time stamp) will be transferred to PIS via data link after outage 2006. Remote Config. Workstation is "behind" MCB. **PIS, ANN**
ERDS (Emergency Response Data Sys.) Process data sent to Nuclear Reg. Body		X			X	**PIS** is the origin of all data used in ERDS.
FP – Fire Protection (Detection) System with addressable sensors			X		X	FP remote monitoring unit is installed on the MCR ventilation board. **PIS, ANN**
Radiation Monitoring System (Standard RM & PARMS – Post Accident RMS)			X			RM digital display units are installed on the RM cabinet in the MCR. **PIS, ANN**
RC BCMS- Reactor Coolant Boron Concentration Measurement System	X			X		Digital indicator on the MCB, central unit is behind the MCB. **PIS, ANN**
Replacement of all pen chart recorders with digital display and/or printing type	X		X			Large multipoint recorders send their data to PIS via serial data link **PIS**

Legend: **A – HSI of digital I&C system on MCB ("U" shaped part) in MCR (Main Control Room)**
B – HSI of digital I&C system on operator workplaces/desks in the MCR area
C – HSI of digital I&C sys. on aux. CB and panels in MCR, visible from operator workplaces
D – HSI of digital I&C within MCR area, but HSI not visible from operator workplaces
E – HSI of digital I&C system out of MCR area, somewhere in the plant, in the field
PIS – System status, measurements & calc. points provided to PIS (hardwired I/O or data-link)
ANN – Warning status/alarm signal(s) are sent to the central MCB annunciator system

2.3 Common basic characteristics of all HSI upgrades up to the 2005 AS-BUILT

The analysis of Table 1 leads us to the conclusion that although NEK did not have officially established, written and approved MCR/MCB HSI endpoint vision nor the migration path, significant modifications were implemented, and all the modifications that included digital I&C and/or MCR/MCB HSI were implemented very consistently. The common key HSI characteristics of all implemented modifications were as follows:

- **The new digital I&C and HSI equipment on the MCB** that was introduced by several modifications (RVLIS, MCB annunciators, PIS, digital recorders, BCMS, SG BD, FP) **is used for monitoring only with no control functions.** It did not cause significant changes to the concept of operation in the MCR and operator's way of work.
- Although a relatively large number of a computer workstations (PIS, temporary installed Switchyard SCADA, temporary installed Annunciator Alarm Log EDU – Electronic Display Unit) were installed at operator's workplaces, the **operator's workplaces/desks are still used for the technological process monitoring** only.
- All **MCR controls are still performed from the MCB (with aux. boards & panels)** only, and not from the desks and computer workstations installed at operator's workplaces.
- Numerous other new digital I&C systems that are used to control some **auxiliary systems and systems used for equipment monitoring have their HSI outside the MCR**, while at the same time they provide essential information to operators through the annunciator system and/or PIS (Process Information System).

3 I&C UPGRADES AND CONTROL ROOM MODERNIZATION PLANNING

The objectives of the planning effort related to the HSI modernization in a NPP are well described in the Ref. [1], section 2.1.2, page 2-6. NPPs that implemented very small number of less significant digital I&C and HSI upgrades do not need to worry about the fact that they missed to develop I&C upgrade and MCR modernization plan. If future developed plan and HFE program demonstrate that some of implemented modifications did not adequately address issues of HSI design, there will be relatively small effort to ensure adequacy of implemented solutions later. NPPs, without consistent and harmonized planning and HFE program, which at the same time implemented a larger number of digital I&C and HSI upgrades including some that are significant, should seriously asses and reconsider all HSI and other digital specific aspects of the implemented modifications. Harmonization of discovered inconsistencies could be time consuming and very expensive. Among NPPs that operate in compliance with the U.S. codes, NEK is among the plants, which implemented larger number of digital I&C and HSI upgrades.

NPPs with a large number of digital I&C and HSI upgrades without having an I&C Upgrade and MCR Modernization Plan as well as HFE Program, should not proceed with any new modification that installs new digital I&C and HSI before the Plan and HFE program are developed, reviewed and approved by the plant management. We should not forget that the planning of both the digital I&C upgrades and the MCR modernization should always be conducted as a part of the plant Design Modification Control Program (Ref. [7]) with strong interactions to the Process Computers Configuration Control (Ref. [8]). The key aspects of the MCR modernization planning should be based on:

- **Management Considerations**
- **MCR/MCB Endpoint Definition**
- **Migration Strategy**
- **Human Factors Program Planning**
- **Planning for Regulatory and Licensing Activities**

4 NEK MCR/MCB ENDPOINT VISION AND MIGRATION PATH

Concerning the originally designed plant life of 40 years of operation (1983–2023) and at this time expected implementation of the life extension program that could lead up to 60 years of plant operation, it is most likely that the present analog I&C platform as well as the MCR/MCB HSI will have to be replaced and upgraded at least once in the plant life time.

At the moment the upgrade plans are not defined yet. Based on the current state of the art of digital I&C technology, plans for future digital I&C technology development and experience from new NPP constructions and ongoing modernizations ([9], [10], [11]), we can be sure about the main design characteristics of NEK MCR endpoint vision. The migration path to the NEK MCR/MCB endpoint vision is not single absolutely correct and "must have" solution. It can be implemented through several plant outages and it can last many years. Minor changes in the migration path are possible. Instead of insisting on one absolute solution, it is much more important that the partially implemented solutions are consistent, harmonized and implemented in such a way that, if the upgrade process is interrupted after one outage, the intermittent solution can stay as long as needed. The author takes the opportunity to propose NEK MCR endpoint vision and the migration path with this paper.

4.1 NEK MCR/MCB Endpoint Vision

Although the detail MCR/MCB endpoint vision applicable to NEK NPP depends on a design to be performed, the author proposes the following <u>key</u> HSI characteristics:

- **The main MCB annunciator system stays as it is now**, organized in 29 annunciator panels with more than 1200 independent windows. Cognitive aspects of the existing MCB annunciator system are superior to any kind of alarm presentation on the VDU (Video Display Unit) in the form of time stamped alarm log. Traditional MCB annunciator system could only be replaced by an alarming system based on expert software application. Expert alarm software system would have to be able to prioritize and organize alarm presentation on different VDU screens based on importance of particular alarm that is a configurable attribute, current plant mode, current system status, current equipment status (bypassed or inoperable or in test), recognition of regular operator procedures, recognition of equipment/sensor malfunction and association of alarms to particular operator's workplace or VDU screen image. Until such an expert alarm system is developed, tested and implemented, it is better to keep the old annunciator system as it is.
- **MCB (vertical portion below annunciators) accommodates three or four large screens** with constant visual image configuration. The screens present graphical image of current status of the most important plant systems and functions with dynamic values indication and dynamic status indication. They are only used for the plant monitoring purposes. Its content is clearly visible and readable from workplaces of all operators. Most of the existing indicators and recorders are removed. Only a small number of indicators and/or recorders, justified by the design analysis that they are needed as a diverse or backup visualization option for some SR indications, can stay on the MCB. If the large screens (or multifunctional tile type mimics) are designed and implemented as an option for the diverse indication of SR indications, no other MCB indicators are needed.
- **MCB control portion (almost horizontal MCB part – "control desk" with controls) accommodates only those controls that are used as 3D (Defense-in-Depth and Diversity) and/or manual backup functions for a reactor trip and selected engineered safety features controls** (needed to establish and maintain safe shutdown). All other controls are removed from the MCB and their function is replaced by the soft-controls available through operator workstations installed at the operator's workplaces – desks.

- **The operator's workplaces-desks accommodate computerized Operator WorkStations (OWS) used for soft control and monitoring of the whole plant.** The OWS acts as the HSI of an integrated digital I&C architecture built around unique process database that stores current signals of all control outputs, process measurements and statuses, current calculated values, process data history (time stamped outputs, measurements, statuses, calculated values), history log of operator entered data, history log of all actions performed by operators and history log of all digital I&C system events (system messages, system errors, system configuration changes, system administrator actions,...). Rather than being dedicated to the technical capabilities of the OWS (e.g.: That certain OWS is technically limited to control and to monitor only the FW system), the OWS are dedicated to its location on certain operator's desk (SS, RO, BOP, SF, EEO, SE) or to the organizational aspects of MCR operation (emergency workplaces). The only real differences among the OWS HSI can be related to the requirement that the qualified version of OWS is needed for the soft controls of SR (Safety Related) functions.

4.2 NEK Migration Path to the MCR/MCB Endpoint Vision

In general, three approaches are possible as migration path from the existing design up to the NEK MCR/MCB endpoint vision. The author lists all three approaches, while he prefers the last approach (when possible) out of the three described below:

- **Single Outage Approach:** Complete plant I&C platform replacement and MCR/MCB upgrade is performed during single extended outage. This approach requires very long preparation and implementation period covering the following: the conceptual design development, the MCR/MCB HSI test on a plant MCR mock-up, the full scope modification design, resolution of all impacts to the plant, FAT (Factory Acceptance Testing) of the ready-to-ship system, MCR/MCB HSI installation on a full scope plant simulator, HSI testing on a plant full scope simulator, operator training, implementation of as much as possible preparation activities before the outage, plant installation of the new plant I&C platform and the new MCR/MCB HSI during a single extended outage, testing before the plant start-up, and testing in limited number of test cases on running plant.
- **Phased Endpoint Vision Approach:** Similar to the first approach, but it is much smoother because of several reasons. Complete plant I&C platform replacement and MCR/MCB upgrade is performed during several outages in a consistent and harmonized manner, partially implementing the endpoint vision during each outage. The first phases could provide experience feedback that could improve implementation of later phases.
- **Phased Behind-the-Board Approach:** Complete plant I&C platform replacement is performed in phases similar to the previous approach with one difference - during each phase the MCR/MCB HSI is minimally changed or not changed at all. When all or most of the existing I&C platform is replaced and tested during several years of operation, the MCR/MCB HSI is replaced during one, not necessarily very long outage. The example for the Behind-the-Board upgrade is the situation in which analog loop control circuitry (example: a loop control from ACM7300 cabinets) behind the MCB is replaced by the digital loop controller, while the old auto/manual & setpoint station stays on the MCB. In the last phase, when complete plant I&C platform is finally replaced, workstations are installed at operator's workplaces-desks, auto/manual & setpoint stations on MCB are removed and control functions are implemented through the OWS soft controls.

As mentioned already, in the real project of MCR/MCB upgrade it is impossible to stay absolutely on single approach for the migration path. Most likely some combination of the Phased Endpoint Vision (e.g.: 35%) and Phased Behind-the-Board (e.g.: 65%) approach would be the most appropriate solution for the NEK MCR/MCB upgrade migration path.

5 RISKS OF IMPLEMENTING NPP MCR/MCB DIGITAL HSI UPGRADES

There are many risks associated with the digital I&C plant upgrade that implements the digital MCR/MCB HSI in an operating NPP. The most outstanding implementation risks are:

Risk No. 1: The NPP MCR/MCB HSI should not become the testing field or exhibit show of the contemporary digital I&C and HSI technology. We should never forget that the main purpose of a NPP is to produce electricity in a safe, reliable and a cost-effective way. The necessity for the MCR/MCB HSI digital upgrade in an operating NPP can be justified only, if among other benefits, it contributes to the improvement of human (operator) performance. It is always better to follow good operating references, than to be the first one doing that. The NPP MCR/MCB HSI upgrade is not a "nice to have" feature.

Risk No. 2: Bad planning and scheduling of the digital I&C and MCR/MCB HSI upgrades can unnecessarily extend outage duration. Do as much as possible on-line.

Risk No. 3: Phased approach to the MCR/MCB digital HSI upgrade with installation of the **dedicated computerized OWS** (display, keyboard & positioning device on operator's desks in the MCR) that are designed to monitor and to control only one system or portion of the plant systems **is a very bad solution**. The situation is even worse if the solution includes dedicated workstations from different vendors and/or different hardware/software platforms. Theoretically speaking, different I&C platforms could be interconnected to provide unique process data base needed to run integrated plant applications and to provide unique plant history, but the negative technical, configuration control, commercial, maintenance, system administration crew team and other consequences are much more serious in comparison to the questionable benefits that arise from the approach such as: "Cheaper partial solution and independence from the single vendor". The digital HSI device that is dedicated to the control and monitoring of one particular system or part of the plant is acceptable on the MCB only in two cases: justified diverse backup option or an intermittent solution along the migration path.

Risk No. 4: If some intermittent MCR/MCB HSI solution or the endpoint vision includes **hierarchical connection of two or more I&C and HSI systems it is good that the control is hierarchically organized, too**. Example: The redundant digital I&C system "A" that is installed in the field performs monitoring, control, protection and HSI functions (local-field operator) for an auxiliary plant system. The data link on SCADA application level connects system "A" and the system "B" that is the main digital MCR/MCB HSI platform. Theoretically, HSI of the system "B" could be used to do anything that is possible on the HSI of the local system "A". By the system application software, or by the configuration or by system administrative measures we should insure that the system "B" HSI should not be used to utilize component "manual (over HSI)" or semi-auto controls. The system "B" HSI should be used to change setpoints, to put the system in certain mode of operation and to perform system START/STOP functions (all to be utilized from the system "B" HSI, but over an application data link and sys. "A" acting as the command validator and an actuating system).

Risk No. 5: Redundancy in digital I&C systems is an excellent system characteristic that is widely accepted and implemented. **The use of diverse backup digital I&C and HSI systems can be implemented to address software common mode failure concerns in the MCR/MCB HSI and plant I&C, but only for those applications for which this is required either by the regulatory requirements or by the system design failure mode analysis.** In all other applications the use of diverse I&C backup or backup manual controls is not appropriate and it presents distrust to the digital I&C upgrade solution. If for example, we decide to replace a non redundant and a Non Safety Related I&C control system based on discrete analog loop controllers with the redundant digital system and the design failure mode analysis for the new digital I&C system suggests the existence of manual backup controls, something is seriously wrong. Are we talking about an I&C upgrade or a downgrade ?

Risk No. 6: In the early stages of the MCR/MCB modernization with phased approach, the **spacing requirements can be challenging**. The MCR/MCB available space, operator's standard access walking routes and operator's way of work should be seriously considered before installing any new HSI equipment in the existing, mostly crowded with equipment, MCR and/or MCB. Usually, significant amount of the new HSI equipment can not be installed in MCR/MCB, before some old equipment is removed or consolidated.

Risk No. 7: The phased approach to the MCR/MCB digital HSI upgrade hides risk associated with **operator's performance during the period in which operators will have to learn and to exercise on simulator a new concept of MCR operation before each plant outage startup.** After each new outage the border between the use of old traditional controls and digital HSI soft controls will move towards the use of full soft controls. Operators could be confused asking themselves if they are going to operate some device from the old MCB or through digital HSI soft controls. During long time period, every outage startup shall include a revision of significant number of operator's procedures and other documentation.

Risk No. 8: Availability of the qualified or even expert personnel to perform the early stages of needed analysis, to design, develop, evaluate and implement modernization can be the limiting factor. The modernization approaches with mostly outsourced support (turnkey projects) increases cost and it does not ensure transfer of the knowledge.

Risk No. 9: The phased approach in the digital I&C and MCR/MCB upgrades in a NPP can last many years and it is hard to ensure that the same personnel will be available until the project completion. **The turnover of personnel on the project team should be considered.** In addition to its regular purpose, appropriate plans, guidelines, procedures and other documentation should be developed to document "the knowledge" and to enable turnover of personnel easier. Management attention to this issue early in the project preparation may help to ensure long-term availability of key people and minimize turnover.

Risk No. 10: The digital upgrades of the MCR/MCB HSI can give pure results if not associated with the **design review and modification (if necessary) of the MCR lighting**.

Risk No. 11: In theory, every new generation of I&C or computer technology is smaller, more compact, faster, more powerful, less demanding regarding the power supply needs and cheaper than the previous generation of the same type of I&C or computer technology. In the real world a lot is in contrast to theory. Very often, the design impact analysis for the digital I&C and MCR/MCB HSI upgrade shall demonstrate that:

- **Capacity of the existing I&C inverters** used for power supply is not sufficient.
- **Capacity of the existing batteries** that supply DC input to the I&C inverters in the case of plant blackout is not sufficient to ensure needed autonomy (e.g. 4 hours).
- **HVAC capabilities** are not sufficient to accommodate newly installed digital I&C and HSI equipment and to ensure adequate habitability of the MCR, computer room and other areas that are activated only in emergency situations such TSC (Technical Support Center) and OSC (Operational Support Center).

Risk No. 12: Although the new digital I&C platform strives to present integrated computerized plant process image and the main process control point for whole plant**,** the **requirements for the new I/O signals have to be appropriately limited**. The full plant digital I&C and MCR/MCB HSI upgrade generates tendency to automate systems that were not automated before. Sophisticated expert software applications are being developed to provide computerized operator support and equipment condition monitoring. Both processes require significant number of new I/O signals (transducers, cabling, control and actuating devices) that presents an effort and cost that is not negligible. This effort has to be properly considered, justified, precisely defined by scope and approved before implementation. We have to accept that the number of field signals connected to the digital I&C platform in the upgraded plant is usually much smaller than it would be in the new designed plant.

Risk No. 13: During the implementation of the migration path to the MCR/MCB endpoint vision the **tendency shall develop that most or all of local I&C process controls and local digital HSI are moved to the MCR**. For an old plant that is being upgraded that will not be appropriate for all auxiliary systems. For some of the auxiliary systems that are controlled locally by the original design it is not appropriate to move control to the MCR because the system needs attention and physical presence of the local operator. We must accept the fact that for some auxiliary systems it is more appropriate to have local digital HSI used for control and supervision, while the system status and the most important signals are transferred to the MCR via MCB annunciator system and/or MCR main digital HSI platform.

6 CONCLUSION

It is not approapriate to proceed with digital I&C and MCR/MCB HSI upgrades before two initial key aspects of the long-term modernization planning are defined and approved:

- **NEK MCR/MCB endpoint vision, and**
- **NEK migration path to the MCR/MCB endpoint vision**

After that, the implementation of smaller digital I&C upgrades along with the activities related to the MCR modernization planning and HFE (Human Factors Engineering) program implementation (programs goals and scope, review, analysis, procedures,...) can be continued.

Before any large digital I&C upgrade with significant impact to the MCR/MCB HSI is implemented, the **technology and architecture for an integrated plant I&C and MCR/MCB HSI platform** should be selected.

REFERENCES

[1] Human Factors Guidance for Control Room and Digital-System Interface Design and Modification: Guidelines for Planning, Specifications, Design, Licensing, Implementation, Training, Operation, and Maintenance, EPRI, Palo Alto, CA, the U.S. Department of Energy, Washington, DC: 2004.1008122.

[2] D. Mandić, M. Smolej, B. Sučić, Some Aspects of Programmable Digital System Usage in Nuclear Power Plants, *Proceedings: 5th International Conference On Nuclear Option in Countries with Small and Medium Grids*, Dubrovnik, Croatia, May, 2004, paper S-3.10

[3] NEI 96-07 Revision 1. Guidelines for 10 CFR 50.59 Implementation, Nuclear Energy Institute, Washington, DC: November 2000.

[4] EPRI TR-102348 Revision 1 – NEI 01-01. Guideline on Licensing Digital Upgrades: A revision of EPRI TR-102348 to Reflect Changes to the 10 CRFR 50.59 Rule, EPRI, Palo Alto, CA: 2002. 1002833.

[5] NRC Regulatory Issue Summary (RIS) 2002-22 (November 25, 2002): Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule,"

[6] NUREG-0711 Revision 2. Human Factors Engineering Program Review Model, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, February 2004

[7] NEK Program ED-1, Rev 1, Jan. 1997: Design Modification Control Program

[8] NEK Program ED-11, Rev 1, Feb. 2001: Process Computers Configuration Control

[9] D. Harmon, S. Kerch, D. Peffer, AP1000's Advanced Control Room, *Proceedings: 13th International Conference on Nuclear Engineering,* Beijing, China, May 16-20,2005, paper ICONE13-50918.

[10] D. Harmon, I. D. Kim, Y. C. Shin, S. M. Beak, M. J. Choi, Implementing Strategy for Shin Kori 3&4 Man-Machine Interface Systems, Westinghouse Electric Company – Korea Hydro & Nuclear Company – Korea Power Engineering Company, May 2005.

[11] D. Walling, Going Digital at Comanche Peak, *Nuclear News*, Feb. 2005, pp. 33-36.