

---

# Key Issues in Safety Assessment of Digital I&C Upgrades in Eastern type NPP's (10 years of German-Ukrainian collaboration)

*G. Schnuerer\*, M. Yastrebenetsky \*\*, A. Lindner \**

\* GRS/ISTec – Institute for Safety Technology, Research Campus, 85748 Garching near Munich, Germany

\*\* SSTC NRS – State Scientific Technical Center on Nuclear and Radiation Safety, 61002, P.O. Box 10125, Kharkov, Ukraine

---

## **Abstract:**

Collaboration between the Institute for Safety Technology (ISTec) from Germany and the State Scientific Technical Center on Nuclear and Radiation Safety (SSTC NRS) from Ukraine has been performed for about 10 years. While the collaboration from 1995 to 2000 was more or less characterized by an information flow from ISTec to SSTC NRS, it becomes meanwhile a real two-way cooperation. The main topics of cooperation have been assessment and qualification of digital safety I&C systems for nuclear power plants, licensing of those systems and elaboration of standards and guidelines for the licensing processes mentioned above. The collaboration helps the two organizations to improve their methods. Information about the application and the status of digital safety I&C in Ukraine and Germany has been exchanged. The paper gives a brief overview about the activities and results of the collaboration especially of the last five years.

## **1. INTRODUCTION**

Collaboration between the Institute for Safety Technology (ISTec) from Germany and the State Scientific Technical Center on Nuclear and Radiation Safety (SSTC NRS) from Ukraine has been performed for about 10 years. The issues of this collaboration from 1995 to 2000 have been reported at the EUROSAFE-2001 [1]. This paper presents key issues of the collaboration of the last five years.

While the collaboration from 1995 to 2000 was more or less characterized by an information flow from ISTec to SSTC NRS, it becomes meanwhile a real two-way cooperation.

The most spread types of Eastern European NPP's are NPP's with WWER reactors. Now 26 WWER-1000 and 27 WWER-440 units are in operation in 8 countries.

From the vantage point of the present, the origin instrumentation and control (I&C) designs of these units had a lot of safety deficiencies, mainly

- low level of reliability of hardware and I&C functions,
- non-satisfactory diagnostics,
- discrepancy of seismic requirements and I&C system properties,
- low quality of man-machine interface,
- missing information support systems for operator staff, etc.

That means these units did not satisfy modern safety requirements. Information equipment used did not correspond to state of art of computer technologies. Therefore wide upgrading of I&C systems has been done on practically all WWER units. The main direction of

upgrading is based on the use of digital computer techniques. The common advantages of digital I&C for improvement of NPP safety are:

- high reliability,
- high processing and data transmission rate, high accuracy,
- high system variability (capable of processing analogue and digital signals, extendable, enabling communication with other systems and processing of complex tasks),
- extended self-test functions, which can be established online; extended maintenance and diagnostic opportunities,
- modern man-machine-interface to support the operator (high productive workstations, displays with high resolutions, etc).

These advantages lead to essential changes in I&C of NPP:

- structural and functional decentralization,
- using of local nets, high-productive workstations, computer nets,
- using digital controllers, digital measurements, smart sensors and actuators,
- possibility of control by display, keyboards, etc.

But besides all advantages mentioned above digital I&C upgrades add new challenges to the task of safety assessment:

- necessity to analyze combination of hardware and software,
- growth of system complexity,
- no possibility of full testing in many cases,
- necessary to evaluate not only the system, but the process of system creation and tools for creation,
- rapid changing of computer hardware components, software and technology of software development.

These new tasks, their solutions and decisions are common for Germany and Ukraine and this is the topic of the collaboration between the two organizations which are supporting national regulatory activity - Institute of Safety Technology (ISTec) - Germany and State Scientific Technical Center on Nuclear and Radiation Safety (SSTC NRS) - Ukraine.

## **2. COLLABORATION BETWEEN ISTec (GERMANY) AND SSTC NRS (UKRAINE)**

Collaboration between ISTec and SSTC NRS starts in 1995. Content of the collaboration during 1995-2000 was already described in the report on the EUROSAFE-2001 [1].

The collaboration during 2001-2005 is characterized by a comprehensive information exchange to the application, qualification and licensing of digital I&C systems. The work has been done by regular meetings, training of Ukrainian experts and exchange of technical publications, regulative documents etc.

During the regular working meetings between ISTec and SSTC NRS the following topics were discussed:

- German and international requirements on safety and safety important I&C systems, explanation of the German compilation of information documents for electrical safety I&C system, for main, emergency and local control rooms,
- Requirements to modification procedures of safety important software during operation,
- operation experience with digital I&C, incidents and data gathering about faults and failures,

- test procedures during commissioning of digital I&C (factory acceptance test FAT, site acceptance test SAT),
- improvement and assessment of reliability of digital systems,
- information exchange and analysis of characteristics of different digital I&C system platforms e.g. Teleperm XS, Teleperm ME, Teleperm XP, Common Q, Tricon, etc.,
- development and application of standards e.g. standards for electro-magnetic compatibility applied in Germany, etc.

The training of Ukrainian experts took place in the framework of the TACIS Project U3.02/00 (UK/TS/25) “Improvement of scientific and technical support to the nuclear and radiation safety regulation in Ukraine by developing the infrastructure of SSTC NRS and its subsidiaries, including enhancement of training capabilities”.

One of the tasks in this project – Task 3 “Summary report by results of improvement of SSTC NRS expert evaluation methodology” – related directly to digital I&C. This task was performed during 2004-2005 and consisted in the following two subtasks:

- a) Subtask 3.1: Safety review of software of upgraded I&C systems.  
Main characteristics to demonstrate compliance of software with safety requirements are quality properties of the software. In other words, compliance of software with established quality criteria is one of the safety requirements. Tools for software analysis permit assessment of the properties determined by software quality having impact on I&C safety.
- b) Subtask 3.2: Reliability assessment of I&C systems.  
The reliability assessment of I&C systems is an important task and it is required for all new implemented and upgraded NPP systems important to safety. It is reasonable that reliability calculation tools should be applied for this purpose. The reliability analysis methodology used by these tools should comply with IAEA recommendations and internationally-accepted methodological principles. In the case of software reliability calculation is still the unsolved problem to establish a common accepted methodology.

The Ukrainian experts were trained with the following software packages:

- CATS (tool for static analysis of software),
- LDRA-Testbed (tool for static and dynamic analysis of software),
- Risk Spectrum (tool for probabilistic assessment of systems),
- SUSAN (tool for detailed probabilistic assessment),

Additional information about other tools was provided, e.g. PEAK, MALPAS, REVEAL.

The activities included also support and training in applying software tools mentioned above to assessment of compliance of I&C systems with regulatory requirements. In detail the following activities were performed:

- workshop with representatives of different companies producing software tools for I&C system assessment;
- overview of software packages suitable for SSTC NRS needs;
- training of SSTC NRS experts in ISTec with the purpose to study how to apply the chosen package of software tools;
- development of a guideline for applying the package of software tools to I&C safety assessment in SSTC NRS expert activity;
- performing a safety review of one upgraded I&C system at a selected Ukrainian NPP using the transferred software tools;

- summary report by results of the improvement of SSTC NRS expert evaluation methodology in the field of I&C safety assessment.
- At last but not least SSTC NRS and ISTec exchanged publications, took jointly part in meetings, conferences, etc. For example SSTC NRS specialists prepared a new definitive book [2] about NPP I&C safety that also includes experiences of the collaboration between SSTC NRS and ISTec. There has been a presentation of this new book at ISTec. Experts from ISTec presented a report at the international conference on “New NPP I&C systems: safety aspects” [3] which was organized by SSTC NRS in Ukraine [3]. There has been additional common participation in the IAEA International Working Group on I&C preparing IAEA documents (e.g. [4]) as representatives of Germany and Ukraine and in the Technical Committee TC-45 of the International Electrotechnical Commission (IEC) as representatives of Germany and Ukraine.

The examples given above demonstrate the fruitful collaboration between German and Ukrainian expert organizations in the field of digital safety I&C.

### 3. ELABORATION OF STANDARDS AND REGULATIONS FOR DIGITAL I&C

The Ukrainian “pyramid” of regulations and standards is given in figure 1.

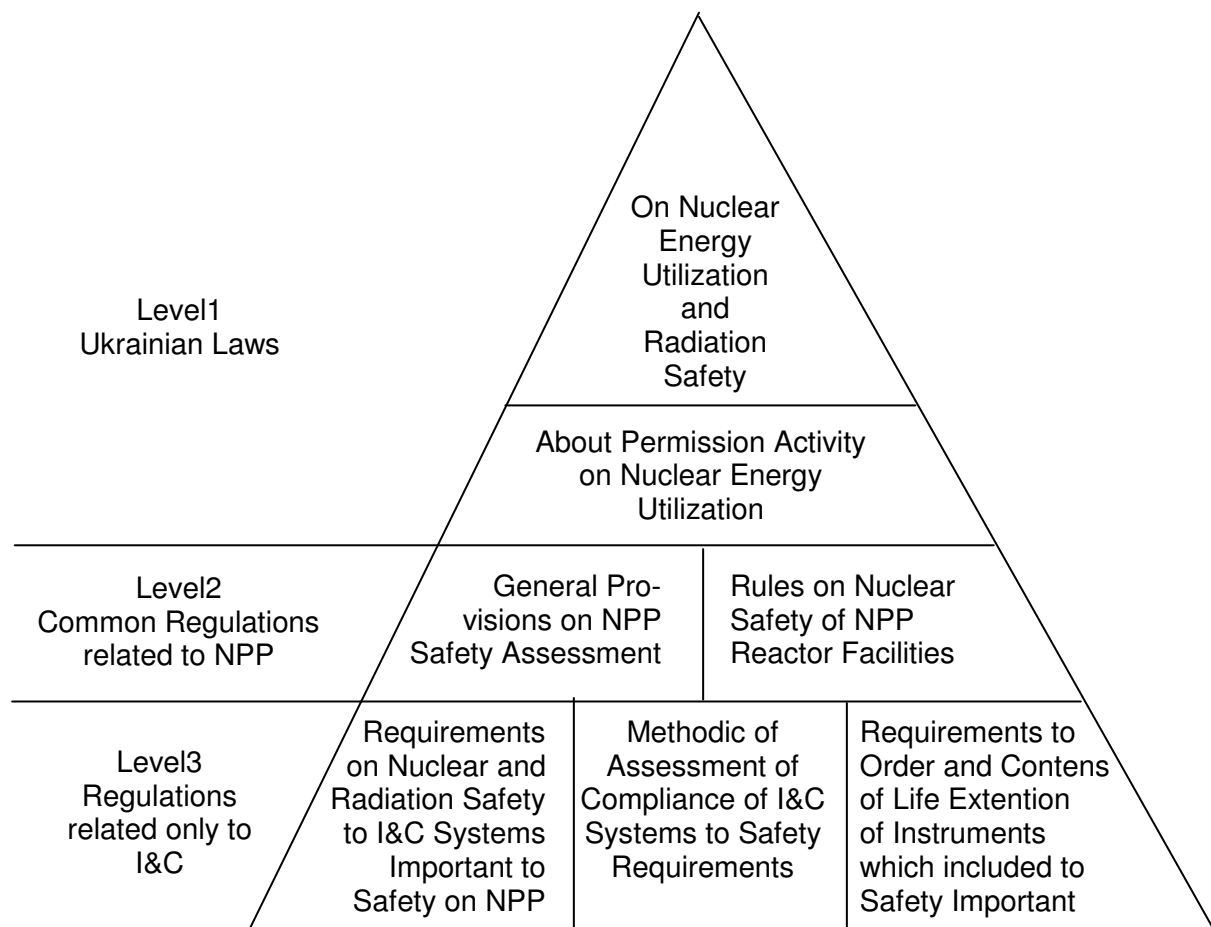


Fig. 1: Ukrainian regulations and standards

The high level is Ukrainian laws. The Law “On Nuclear Energy Utilization and Radiation Safety” contains main principles of licensing, as one of the main direction of regulatory activity.

The level 2 contains two types of documents: documents which are an “inheritance” of USSR, are common for Ukraine and Russia and didn’t change during Ukraine independence (for example “Rules on Nuclear Safety of NPP Reactor Facilities”) and documents which were elaborated in Ukraine and acted now instead of past USSR documents (for example, “General Provision on NPP Safety Assessment”). Documents of this level contain common requirements to different types of systems important to safety.

Documents of level 3 are related directly to I&C systems. These documents were elaborated by SSTC NRS and approved by Ukrainian Nuclear Regulatory Authority (NRA). First of them is “Requirements on Nuclear and Radiation Safety to I&C Systems Important to Safety” [5].

Areas of application of this document are:

- NPP I&C important to safety,
- software-hardware complex (SHC) as a set of hardware and software components intended for use as part of I&C systems,
- hardware intended for use in I&C directly or as part of SHC,
- software for I&C and SHC.

Software-hardware complex is a new subject of regulation. Normally, SHC is a central part of I&C, composed by a set of hardware components integrated with software modules, which are connected to peripheral items on the NPP site to implement functions of a specific I&C system. The term SHC is mainly used for I&C modernization at which a modernized I&C system replaces only central parts – the SHC - and does not replace sensors, cable, etc. Using SHC increase the level of equipment ability and decrease time to system check-out and testing. That is important because most parts of I&C upgrading take place during annual unit outage time for repair and fuel-element shuffling.

The main peculiarities of new regulatory requirements to I&C are:

- the requirements take into account only I&C which is qualified for use as safety important systems,
- the requirements had to coordinate with high level documents in the standard pyramid,
- it was necessary to harmonize these requirements with international standards, codes and rule (IAEA, IEC, etc.),
- the requirements have to consider that most of modern I&C is digital and based on microprocessors with software.

The goal of this document is not the elaboration of the full set of the technical requirements to NPP I&C, but the requirements which are important to safety and have to be included to the set of regulatory requirements, which Ukrainian Nuclear Regulatory Administration (NRA) will be use for licensing and supervision activities.

According to the document “Methodic of Assessment of Compliance of I&C System to Safety Requirements” [6] expert assessment contains:

- identification (certain definition) of regulatory requirements to the system and its components,
- establishment of compliance between the system with its components and each of the regulatory requirements imposed to them,

Expert evaluation has to start at the earliest stages of I&C creation (NPP Technical Decision).

One of the first steps in licensing is the elaboration of the licensing plan that establishes communication between NRA and licensee. The contents and details of a licensing plan are different for different systems, but main parts of this plan should be:

- short information including safety classification, presence of re-used and commercial-off-the-shelf (COTS) software and hardware, etc.,
- list of regulatory requirements,
- list of reviews which would be prepared by experts,
- list of licenses (permits, certification) which NRA would send to licensee,

Expert evaluation includes:

- software and hardware analysis along with analysis of the systems as a whole,
- analysis of the interface between upgraded and unchanged parts of the I&C system,
- analysis of the process of software development, verification and validation, etc.

Analysis of software verification includes the following:

- analysis of the software conformity to all requirements of the specifications, standards and other normative documents which should be tested during verification,
- analysis of independence which should be observed during verification. For software of safety systems it is obligate to establish complete administrative and financial independence of the division that perform the verification tests from the software development division. For software of safety related systems (but not safety systems) partial independence is admissible, when development and testing of software can be carried out by various experts of the same division,
- analysis of the verification plan and report, test programs, test procedures etc.,
- analysis if the documentation of the software verification is reasonable by persons not participating in the software development and verification.

The third document consists of requirements to life time extension of instruments which are included into I&C systems important to safety.

Table 1: Typical stages of licensing and expert reviews

Stage of licensing	Expert review
1. Accordance of NPP Technical Decision about modernization	Expert review of NPP technical decision about modernization
2. Accordance of Terms of Reference (Specification)	Expert review of Terms of Reference
3. Accordance of Permission to Mounting	Expert review of software verification plan
	Expert review of software verification report
	Expert review of report about reliability
	Expert review of preliminary safety analysis report
4. Accordance of Permission to Operation	Expert review of SAT programs and methods
	Expert review of experimental operation program
	Expert review of final safety analysis report

The German “pyramid” of regulations and standards is given in figure 2.

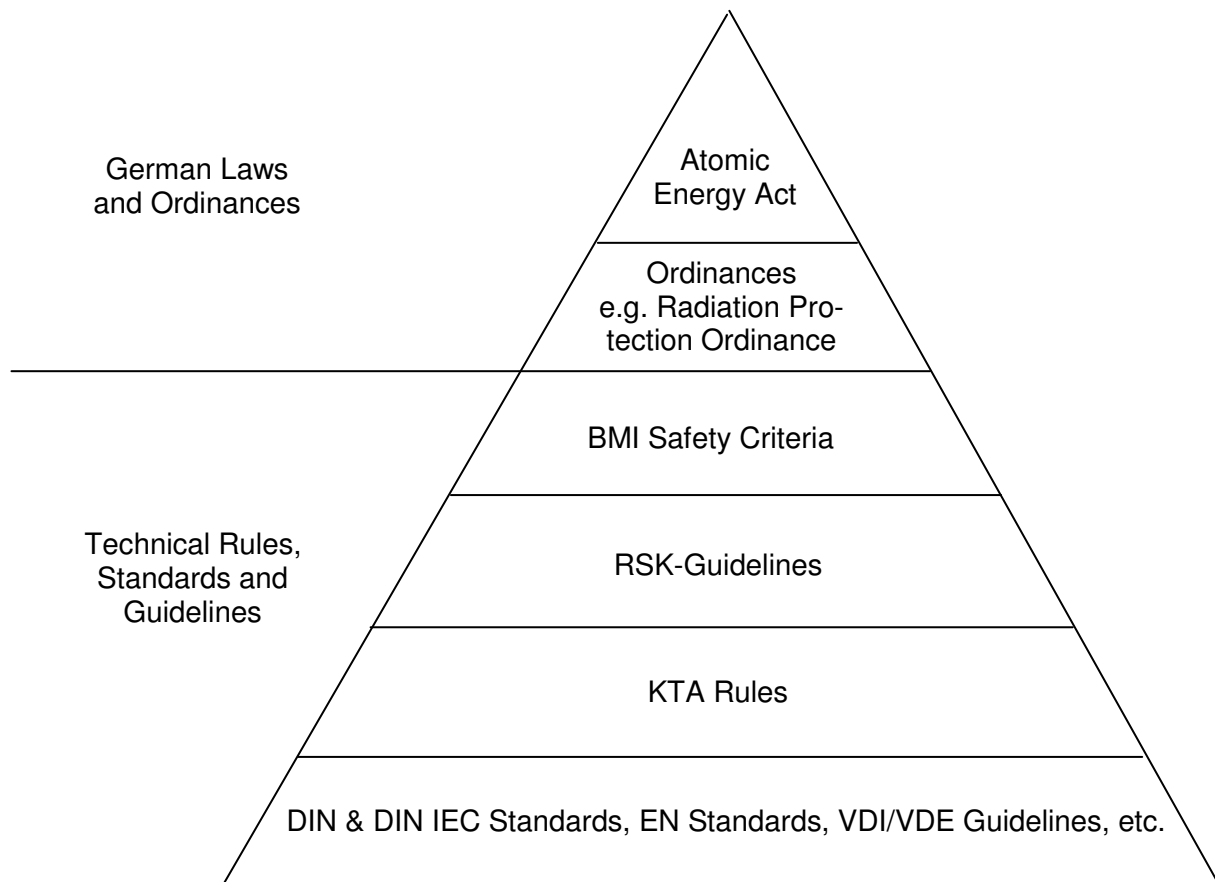


Fig. 2: German regulations and standards (present situation)

At present the two upper levels of the Technical Rules, Standards and Guidelines (BMI<sup>1</sup> Safety Criteria and Guidelines of the Reactor Safety Commission (RSK) are under revision. The existing documents will be integrated to one document “Safety requirements for Nuclear Power Plants”. The actual draft of the document is published for discussion [7]. During the revision of the “Safety requirements for Nuclear Power Plants” state-of-the-art requirements from international standards and guidelines are incorporated into the German requirements document.

Especially on the level of KTA<sup>2</sup>-Rules requirements to digital I&C are just partly covered. That’s why for digital I&C the DIN<sup>3</sup> IEC standards, EN standards and VDI/VDE<sup>4</sup> guidelines have to be applied. Nevertheless, approved requirements that are independent from the I&C technology will be maintained.

ISTec as well as SSTC NRS is involved in several international working groups, projects and committees like subcommittee SC45A of the IEC, the COMPSIS-project<sup>5</sup> of the OECD/NEA (ISTec only) and the Technical Working Group on Nuclear Power Plant Control and

<sup>1</sup> Federal Ministry of the Interior

<sup>2</sup> Kerntechnischer Ausschuss

<sup>3</sup> Deutsches Institut für Normung e.V.

<sup>4</sup> Verein Deutscher Ingenieure e.V./Verband der Elektrotechnik Elektronik Informationstechnik e.V.

<sup>5</sup> COMPUter based Systems Important to Safety

Instrumentation (TWG-NPPCI) of the IAEA. It became good practice during the collaboration of SSTC NRS and ISTec to exchange information and experiences from those activities. This helps to establish joint activities e.g. in working groups of SC45A.

#### **4. EXPERT REVIEWS FOR UPGRADED DIGITAL I&C SYSTEMS**

The most important event in nuclear industry in Ukraine in 2004 was the start of two units WWER 1000: Khmelnitsky 2 (KhNPP 2) and Rovno 4 (RNPP 4).

The construction of KhNPP 2 and RNPP 4 began in 1983 and 1984 respectively. In 1990 the construction of both units was halted due to the Moratorium on construction of new power plants adopted by Verkhovna Rada of Ukraine (preservation and equipment conservation works were conducted).

After the Moratorium lifting by the Verhovna Rada Decree the civil works were renewed.

KhNPP 2 and RNPP 4 received I&C equipment before the moratorium (1990). The equipment was preserving all time from 1990. The design was improved during 1998-2003.

The main principles of new design:

- a) I&C systems have to satisfy the new Ukrainian Regulations [5] (which was harmonizing with international requirements) and IAEA standards (NS-G-1.3, NS-G-1.1, NS-R-1) and recommendations.

Example: Requirements to diversity, which were realized in protection systems (apparatus diversity) and automatic control systems of reactors (program diversity).

- b) Technical decisions to implement state-of-art technology:

- wide use of digital microprocessor technique,
- modern man-machine interfaces (MMI),
- distributed control, local nets,
- high level of diagnostic,
- using microprocessors and other components which produced by well established companies.

Example: Protection system, which has main and diverse sets, 3 independent channels in every set using Field Programmable Gate Arrays (FPGA) produced by "Altera" (USA), different devices in the sets.

- c) Some parts of equipment (actuators, cables, some sensors, etc) were not replaced. Special activities of checking and tests were performed before start-up.

- d) Designers of the most systems were Ukrainian companies:

- companies who have big experience (from 1981) in producing I&C systems for Russian, Ukrainian, Bulgarian WWER reactors,
- companies who have produced computer systems for military aims before conversion.

- e) Wide approbation of new systems designed by Ukrainian companies before using on new units:

- operation of control systems in open loop,
- operation of information systems in emergency control room, etc.

The list of new digital I&C systems which have been implemented on RNPP 4 is shown on table 2. All systems have been assessed by SSTC NRS.

Table 2: Digital I&C Systems which have been implemented on new unit Rovno NPP-4

Name of System	Designer	
	Name	Country
Reactor Protection System	Radium	Ukraine
Reactor Power Control System, Reactor Power Limitation System	Radium	Ukraine
Neutron Flux Monitoring System	Impuls	Ukraine
Computer Information System	KhIKA, Impuls	Ukraine
In-Core Monitoring System	KhIKA, Impuls, SNIIP	Ukraine Russia
Group and Individual Control Rod System	Skoda	Czech Republic
Automatic Control Systems of 1 <sup>st</sup> Circuit	Shevchenko Plant	Ukraine
Automatic Control Systems of Machine Room	Shevchenko Plant	Ukraine
Refuelling Machine Control System	GANZ	Hungary

The second direction in SSTC NRS licensing activities was turned towards expert reviews of upgraded digital I&C systems. Ukraine has a government program for NPP I&C upgrading which starts to be fulfilled in 2000.

Table 3: Upgraded digital I&C Systems which have been implemented at operated units during 2001-2005

Name of system	Designer		NPP
	Name	Country	
Reactor Protection System	Radium	Ukraine	ZNPP - 1, 3
Group and Individual Control Rod System	Skoda	Czech Republic	SUNPP - 3 ZNPP - 1, 3
Neutron Flux Monitoring System	Impuls	Ukraine	ZNPP - 4 SUNPP - 3
Computer Information System	Westron	Ukraine	SUNPP - 2, 3
Reactor Power Control System, Reactor Power Limitation System	Khartron	Ukraine	RNPP - 2
Computer System from Machine Room Control	Shevchenko Plant, LvivORGRES	Ukraine	ZNPP - 4
In-Core Reactor Monitoring System	Tensor, Kurchatovski institute	Russia	RNPP - 1, 2
	Impuls	Ukraine	ZNPP - 3
Steam Generator Level and Feedwater Control System	Westron, LvivORGRES	Ukraine	SUNPP - 3
Refuelling machine Control System	GANZ, Evig	Hungary	SUNPP - 1, 2
ZNPP – Zaporozhje NPP, SUNPP – South-Ukrainian NPP, RNPP-Rovno NPP			

The list of upgrading digital I&C systems which have been implemented on operated units during 2001-2005 is shown in table 3. All these systems have been assessed by SSTC NRS. Typical stages of licensing and expert reviews belonging to them are shown on table 4.

ISTec has long term experience in assessment of modern digital safety I&C [8]. This holds for both, the generic qualification of I&C platforms as well as the assessment of plant specific applications.

As an example ISTec established and performed the generic software qualification procedure for the TELEPERM XS system. This procedure comprises the "type-test" of each hardware and software component and a plant-independent system (integration) test with a representative system configuration. During the plant-independent system test especially the properties and the behaviour of the system software were evaluated. Because of the plant-independent qualification the plant-specific qualification can be performed much more effectively.

During the type test all manually developed software modules were qualified. Those modules are not modified during the application software design (automatic generation). Therefore, the plant-independent system software is already validated during the type test procedure. Only the automatically generated application software must be evaluated during the plant-specific software qualification. The software qualification approach applied to the TELEPERM XS platform was discussed with SSTC NRC.

A few I&C systems in German NPP's have been upgraded during the last years. A brief overview is given in table 4. Additionally several safety related and non safety related digital devices are installed in German nuclear power plants like refuelling machine control systems, neutron flux measurement systems, etc.

Table 4: Upgraded digital safety I&C Systems in German NPPs

<b>NPP</b>	<b>System</b>	<b>Platform</b>	<b>Status</b>
KKU	Power control and limitation system	TELEPERM XS (Framatome ANP)	In operation
GKN	Power control and limitation system	TELEPERM XS (Framatome ANP)	In operation
GKN	Reactor protection system	TELEPERM XS (Framatome ANP)	In planning
KKI	Limitation system, control system, Modern computerized MCR	Symphony, Melody (Westinghouse)	In operation
KKP	Emergency safety system	TELEPERM XS, TELEPERM XP (Framatome ANP)	In operation
KWB	Limitation system	TELEPERM XS	In operation
FRM2 <sup>6</sup>	Reactor protection system	TELEPERM XS (Framatome ANP)	In operation

ISTec was also involved in the licensing of digital safety I&C systems for the FRM2, NPP Bohunice / Slovak Republic, NPP Paks / Hungary, NPP Beznau / Switzerland. The activities have mainly been dedicated to plant specific assessment of the TELEPERM XS platform that has been applied in all projects mentioned above. During the collaboration with SSTC NRS an outstanding exchange of the experiences of the licensing process took place. In this way ISTec and SSTC NRS could learn from each other and improve their own methodology.

<sup>6</sup> The FRM2 is the research reactor of the Technical University of Munich.

## 5. CONCLUSIONS

The information exchange regarding elaboration and application of standards and guidelines provides the basis for better understanding of the licensing approaches in Ukraine and Germany.

Due to the collaboration between SSTC NRS and ISTec both partners get an overview about the procedures for backfitting of digital safety I&C in nuclear power plants. This is helpful for the Ukrainian experts to enhance their methodology of safety assessment and to get information about Western practices in this field. Otherwise the German experts learn about backfitting of Russian type WWVER reactors which are also operated in several East European countries of the European Union.

Since Ukraine is not involved in all important international projects (e.g. the COMPSIS project of the OECD/NEA), the collaboration between SSTC NRS and ISTec provides an opportunity for information exchange especially in the field of evaluation of operational experience of digital I&C.

## 6. REFERENCES

- [1] M. Yastrebenetsky, D. Wach, B. Mulka, S. Vinogradskaya. German-Ukrainian collaboration in the assessment of digital I&C systems for safety applications in NPPs. EUROSAFE. Nuclear Installation safety. Assessment and analysis. Paris, 2001.
- [2] M. Yastrebenetsky, V. Vasilchenko, S. Vinogradskaya, V. Goldrin, Y. Rozen, L. Spektor, V. Kharchenko. Nuclear Power Plants Safety: Instrumentation and Control Systems. Kiev, 470p (in Russian) 2004.
- [3] G. Schnürer, M. Kersken, F. Seidel. Technical Requirements on Maintenance and Modifications of Digital I&C Systems Important to Safety. International Scientific-Technical Conference "New NPP I&C: Safety Aspects". Abstracts. Kharkov, 2005.
- [4] IAEA TECDOC-1328. Solution for cost effective assessment of software based instrumentation and control systems in nuclear power plants. IAEA, 2002.
- [5] НП 306.5.02/035 2000. Requirements on Nuclear and Radiation Safety to I&C Systems Important to Safety (in Russian).
- [6] ГНД 306.7.02/2.041 2000. Methodic of Assessment of Compliance of I&C System to Safety Requirement (in Russian).
- [7] <http://regelwerk.grs.de>
- [8] A. Lindner, D. Wach, Experiences gained from Independent Assessment in Licensing of Advanced I&C Systems in Nuclear Power Plants, Nuclear Technology Vol. 143, Aug. 2003, pp. 197-207.