Mikhail Yastrebenetsky
PhD, Dr. Sc., Prof. Honored Scientist of Ukraine
State Scientific and Technical Center for Nuclear and Radiation Safety

Chernobyl and Fukushima Lessons for Nuclear Power Plants Instrumentation and Control Systems

30 Years after Chernobyl Accident

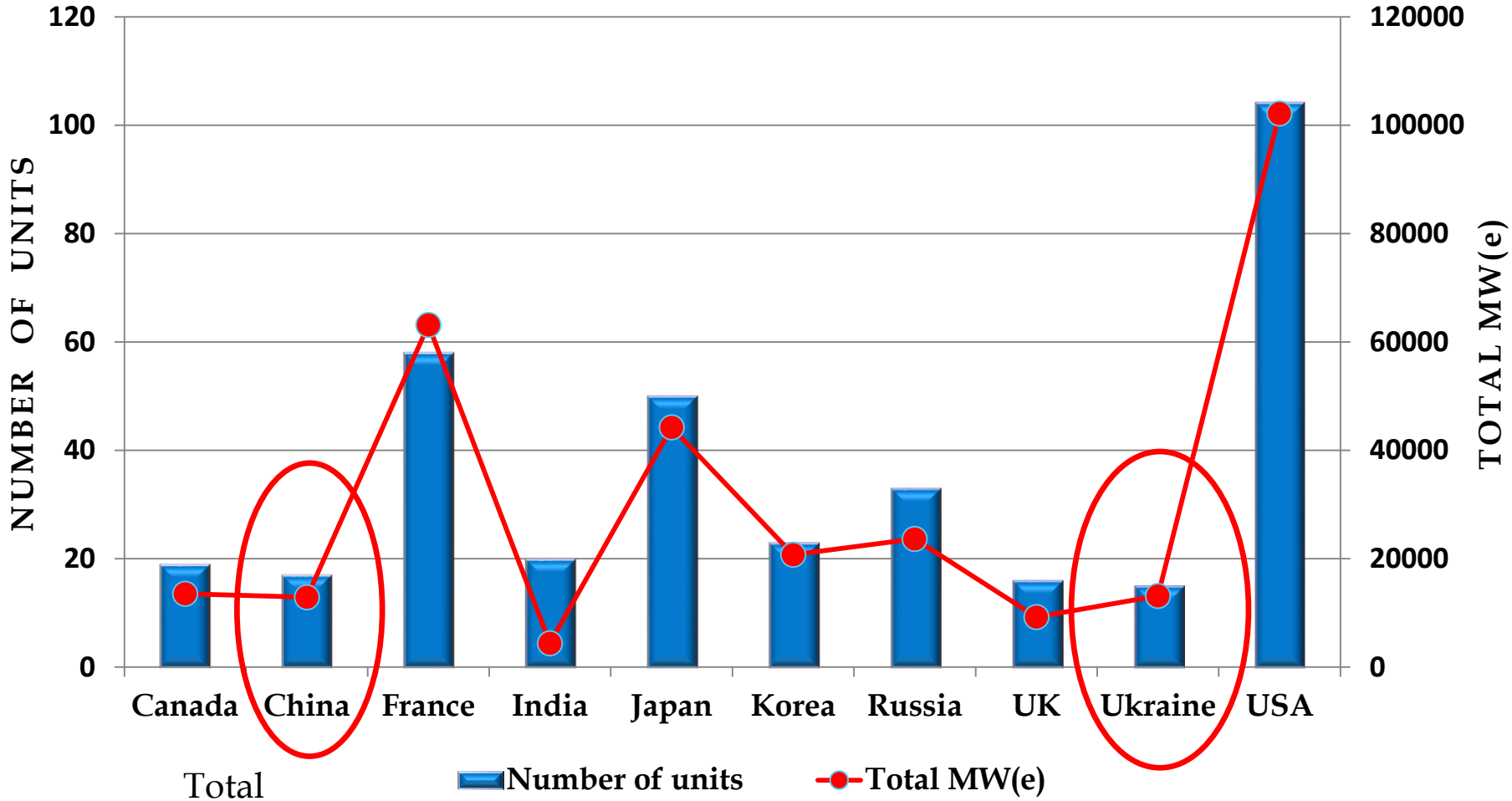
Boston,
IEEE, ASA, Institute for Operation Researches
2016, April 29

CONTENTS

1. Introduction
2. Chernobyl lessons
3. Fukushima lessons
4. Knowledge dissemination experience
5. Conclusion

INTRODUCTION

Reactors in operation
(countries with maximum number of reactors)



	Number of units	Total MW(e)
Total (all countries in the world)	437	373,069

NPPs generate 17% of energy budget in the world.

INTRODUCTION

Ukrainian NPPs

Chernobyl NPP

Total Gross Capacity:
13,835 MW
4 sites
15 units
2 units under construction

Zaporizhzhya NPP
The largest NPP in Europe
6×WWER-1000

Rivne NPP
2×WWER-1000
2×WWER-440

South-Ukrainian NPP
3×WWER-1000

Khmelnitsky NPP
2×WWER-1000
2×WWER-1000 under construction

Ukraine:
TOP 5 in Europe
TOP 10 in the World
About 53% of national power generation

INTRODUCTION

Instrumentation and control system (I&C)

I&C system is “central nervous part” of NPP.

Main purposes of NPP I&C:

automatic control of technological processes, systems and equipment;

automatic protection of technological equipment;

acquisition, processing, archiving, display, recording data.

.

The term is encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices.

INTRODUCTION

The peculiarities of NPP I&C

- Huge consequences after accident;
- Big economical loss after failures (even without accident) - 1 hour of unit 1000 MW downtime costs more then 100,000 EUR;
- The existence of an independent (from developers of I&C and from nuclear power plants) state organization that is entrusted with the task of assuring NPP safety and which performs certain kinds of activity related to development and operation of I&C;
- The need not only to assure but also to demonstrate a number of characteristics, etc.

CHERNOBYL LESSONS

Collection and usage of statistical data about NPP reliability

NPP events/violations

Levels of events (IAEA International Nuclear Events Scale)

- 7 Major accident (Chernobyl, Fukushima)
- 6-4 Accidents with different types of consequences
- 3-1 Incidents
- 0 No safety significant event reactor protection systems

Failures of I&C systems (e.g., reactor protection systems)

Failures of devices of I&C systems (e.g., actuator, processor)

Failures of elements of devices (e.g., microprocessor)

CHERNOBYL LESSONS

CHERNOBYL LESSONS

Chernobyl NPP, unit 4, Ukraine, 1986, April 26

Nuclear accident level 7. Nuclear explosion because uncontrolled expansion.

Main reasons:

- mistakes of reactor design in admissible high of reactivity;
- mistakes of personnel (disconnections of safety systems).
- low quality of procedure rules
- Inefficiency of supervision and regulation of nuclear safety

Main lessons:

- changing of relation to NPP safety in the world;
- reorganization of safety regulations;
- widening of international cooperation in nuclear energy;
- I&C modernization;
- hardening of requirements to NPP, including NPP I&C.

CHERNOBYL LESSONS

Preconditions of Chernobyl accident in USSR

- Choice of reactor type - high power channel reactor RBMK - was influenced by:
  - needs of USSR military politics
  - industrial limitations in USSR
- RBMK didn’t consider the safety of personnel, population and environment to the full extent
- Excessive secrecy of RBMK design and operation

Chernobyl accident - one of the final shocks that lead to the fall of the Berlin Wall and the USSR disintegration

CHERNOBYL LESSONS

Safety deficiencies of NPP I&C

- The level of computerization in I&C did not coordinate with development of information technologies
- Low reliability

Example of operating reliability measures of unit computer information system

Name of device	MTBF, h
Processor	3200
Commutator	3800
Keyboard	7400
Display	5000

- Unsatisfactory level of hardware and software diagnostics
- Low quality of man-machine interface
- Absence of operator support systems (SPDC only began to introduce after TMI accident)

CHERNOBYL LESSONS

Widening of international cooperation in nuclear energy.
Branches of world nuclear organizations cooperation

CHERNOBYL LESSONS

Peculiarities of I&C changes in Ukraine

Ukraine after Chernobyl accident appeared in the center of attention of the world public opinion in all aspects, related to NPP, including NPP I&C. This attention included methodical support to Ukrainian regulatory body and to TSO from IAEA, USA, Germany, France, etc., delivery of foreign I&C systems (e.g., SPDS for all WWER-1000 units).

- Possibility after fall of “iron curtain” of using new modern element base of the best in the world market in NPP I&C, instead of USSR elements.
- The task of designer before was, according to John Von Neumann expression “Synthesis of reliable systems from unreliable elements”; now “Synthesis of advanced reliability systems from reliable elements”.
- Conversion of a lot of Ukrainian companies, that before designed and manufactured computer control systems for military techniques (missiles with nuclear warhead, e.g. missile “Satan”); these companies began to produce technologies for NPP I&C;

CHERNOBYL LESSONS

Rapid development of electronics, digital computer technologies, information technologies, which are more widely used in design of I&C. Advantages of these systems are as following:

- instead of analog computing circuit use more accurate digital calculations;
- providing operating personnel to manage manually elements of technological equipment directly with keyboard workstations;
- use of local computer networks for data exchange between devices allows providing high speed of transfer and required reliability of obtained messages over fiber-optic lines;
- providing technical diagnostics, display and record of diagnostic messages, allows quickly detecting faults;
- possibility of wider use of redundancy, including constructions with multiple redundancy, performing logic conditions “two-out-of-three”, “two-out-of-four”;

CHERNOBYL LESSONS

Essential improvement of reliability

Operating reliability measures of digital I&C (WWER-1000 units)

Name of system		Reactor protection systems			Reactor power and limitation control systems		Engineering safety features actuation systems	
		systems	sets	channels	systems	channels	systems	channels
Number		10	20	60	6	18	7	22
Operating time, h		318,000	492,000	1,476,000	124,000	372,000	85,000	236,000
Number of failures		0	0	9	0	2	0	3
Estimation of failures intensity, E-06	low confidence bound	–	–	10,6	–	19,2	–	32,8
	point	0	0	6,1	0	5,37	0	12,7
	high confidence bound	–	–	3,17	–	1,08	–	3,45

CHERNOBYL LESSONS

There weren't failures of systems or sets (main and diverse) as a whole.

High and low confidence bounds of channels failure intensity (every set had 3 or 4 channels) were determined for confidence probability 0.9.

We could pay attention to absence of software faults in these systems.

Short information about reliability of some elements of the systems:

- Average point estimation of failures intensity of different chips is 4,23E-08 1/h; failures intensity of these types of chips according to the data from manufactures – from 4,5E-07 to 7,8E-08 1/h.
- Particular attention paid to information about FPGA (A field-programmable gate array (**FPGA**) is an integrated circuit designed to be configured by a customer or a designer after manufacturing – hence "field-programmable".) Common number of FPGA is 14424. Common FPGA operating time during the time of observance equal $284 \cdot 10^6$ h. There were no FPGA failures of digital reactor control systems over this observation period.
- High confidence found of FPGA failure intensity (confidence probability – 0,9) equal 8E – 091/h.

CHERNOBYL LESSONS

Safety Parameters Display System (SPDS)

SPDS realized critical safety functions of monitoring in all NPP operation modes with the aim of identifying the signs of violation of critical safety functions and definition of personnel actions which are priority from safety point of view.
These systems were designed by Westinghouse Electric Corporation (USA). “Westron” (Ukraine) provided development and implementation of these systems.

These systems were provided at 11 NPP units in the framework of the International Nuclear Safety Program with the support of DOE (USA).
SPDS project is a good example of cooperative activity of the US companies (“Westinghouse”, “Burns and Roe”, US DOE) and Ukrainian NPPs, design organizations, regulatory Body and TSO (SSTC NRS).

CHERNOBYL LESSONS

Safety Standards

Quote: “Safety standards are written in blood”. It applies foremost to standards in nuclear power engineering, where accidents have a large-scale effect.

Full set of requirements to NPP I&C became more tightened after Chernobyl and continues to toughen.

The main international standard bases for NPP I&C systems are:

- documents of the International Atomic Energy Agency (IAEA)
- International Electrotechnical Commission (IEC)

Besides international standards each country has a standard base concerning NPP, e.g. in USA American National Standards Institute (ANSI) – USA

In addition, standards of USA professional organizations are widespread:

- American Society of Mechanical Engineering (ASME)
- Especially concerning NPP I&C – Institute of Electrical and Electronic Engineers

FUKUSHIMA LESSONS

Storage of post-accident information

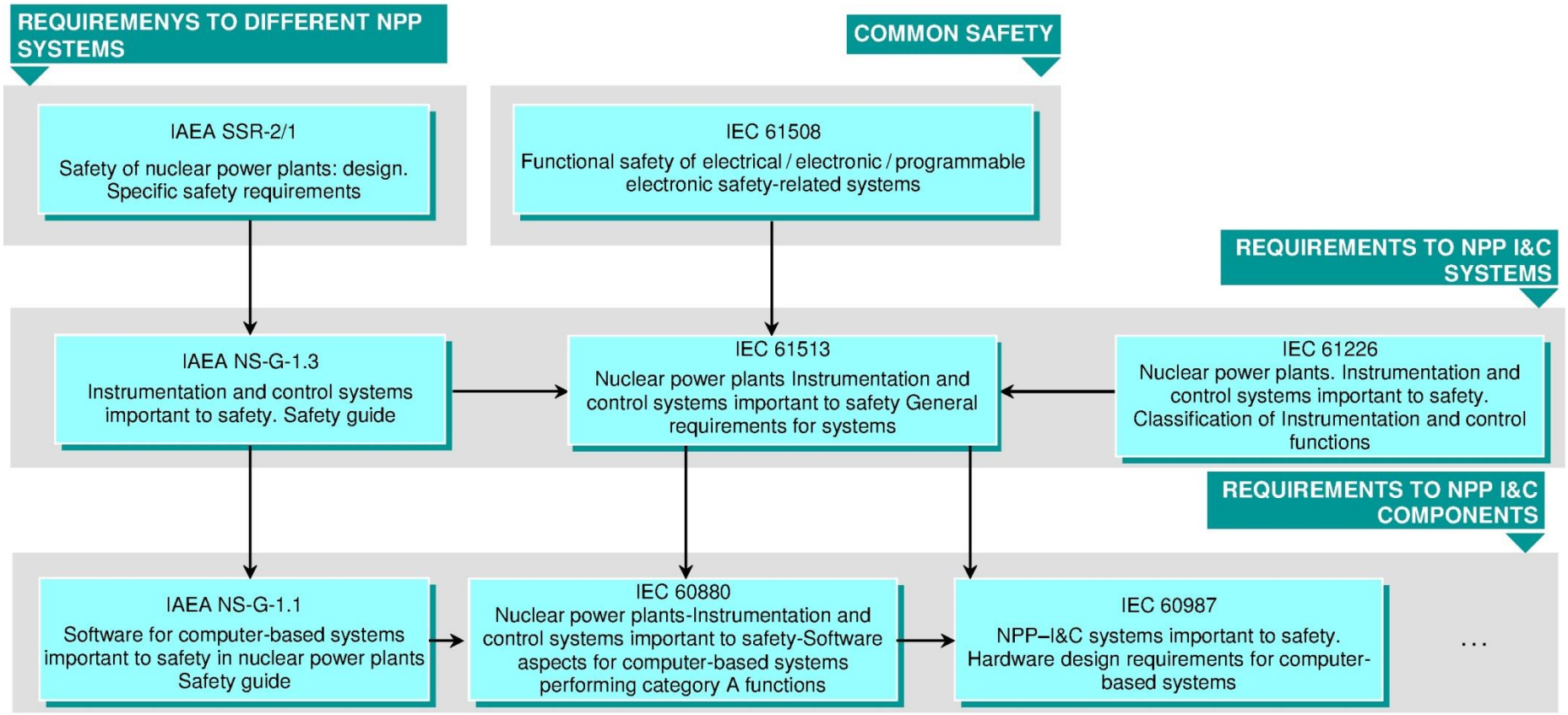
Main information for analysis of reasons of this accident was received by unit computer information system “Skala” with semiconductors. Computer was located in special room, not far from main control room. Technical means for registration of data were tape recorders located in a closed metallic shelf.

Housing of this computer after accident was destroyed, computer was flooded by radioactive water, level of radioactivity in this room was very high. The order to retrieve these tapes took place in two hours after accident. The keys from this shelf were not found and personnel opened this shelf by breaker (crowbar).

In spite of flooding by radioactive water, dropping of constructions, high level of radioactivity - information about accident was saved and used in accident analysis.

CHERNOBYL LESSONS

Interconnection between IAEA and I&C standards



Interconnection of the standards is as following:

- IAEA develops general safety principles for NPP I&C;
- IEC develops technical requirements that use and specify safety principles.

CHERNOBYL LESSONS

Safety measures change over time

Quality analysts of NPP safety changes can be received from statistical data about events in NPP operation.
Types of units – WWER (Ukraine) and PWR (USA)
Events:

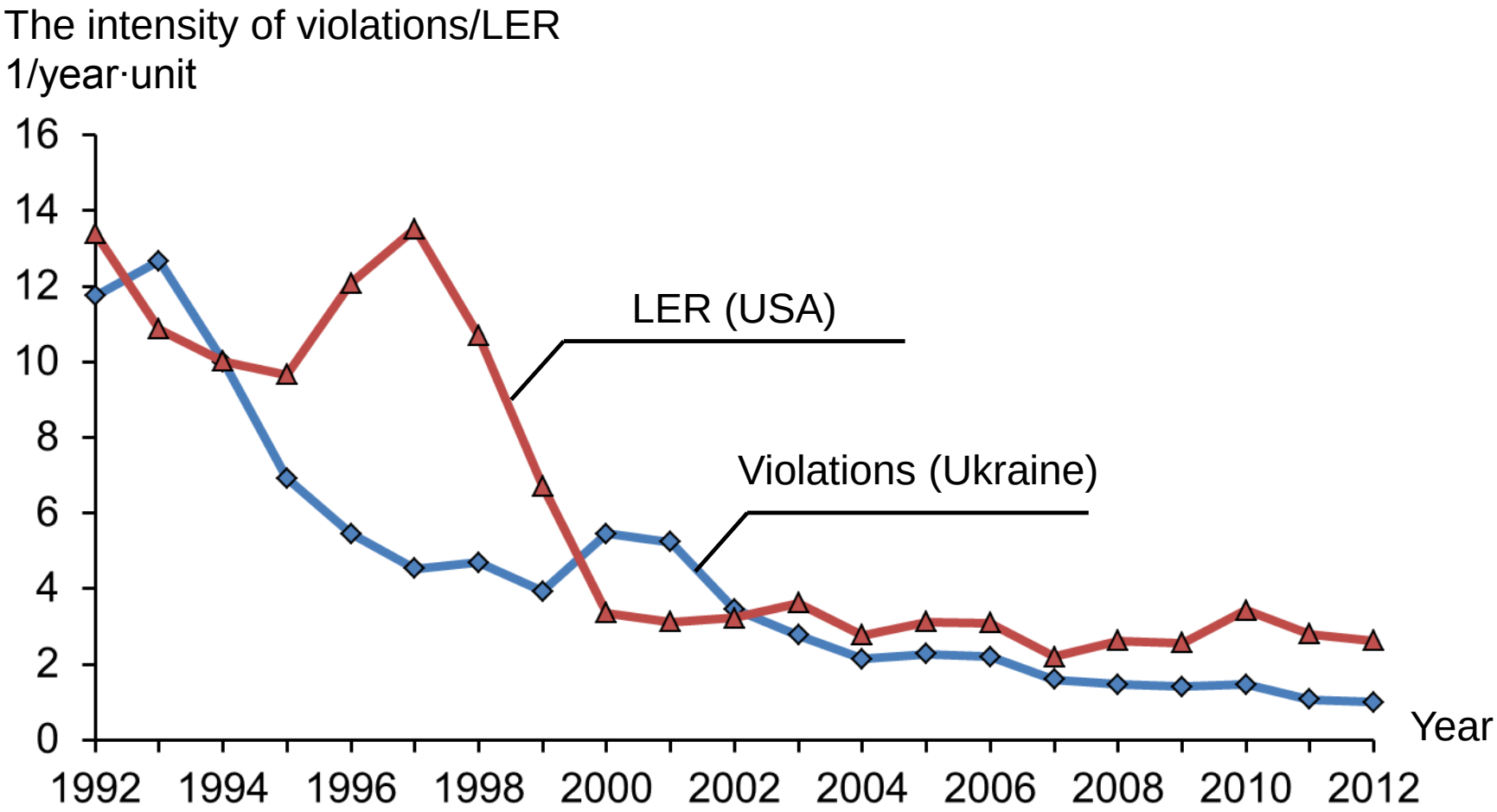
- violations (Ukrainian practice)
- licensee Event Reports (USA practice)

Difference between these definitions - LER include more wide class events, then violations. But tendencies of events intensity changes from 1992 to 2012 is similar:

- decrease of events intensity
- improving of operation and safety measures (including struggle against ageing) overcome tendency to ageing.

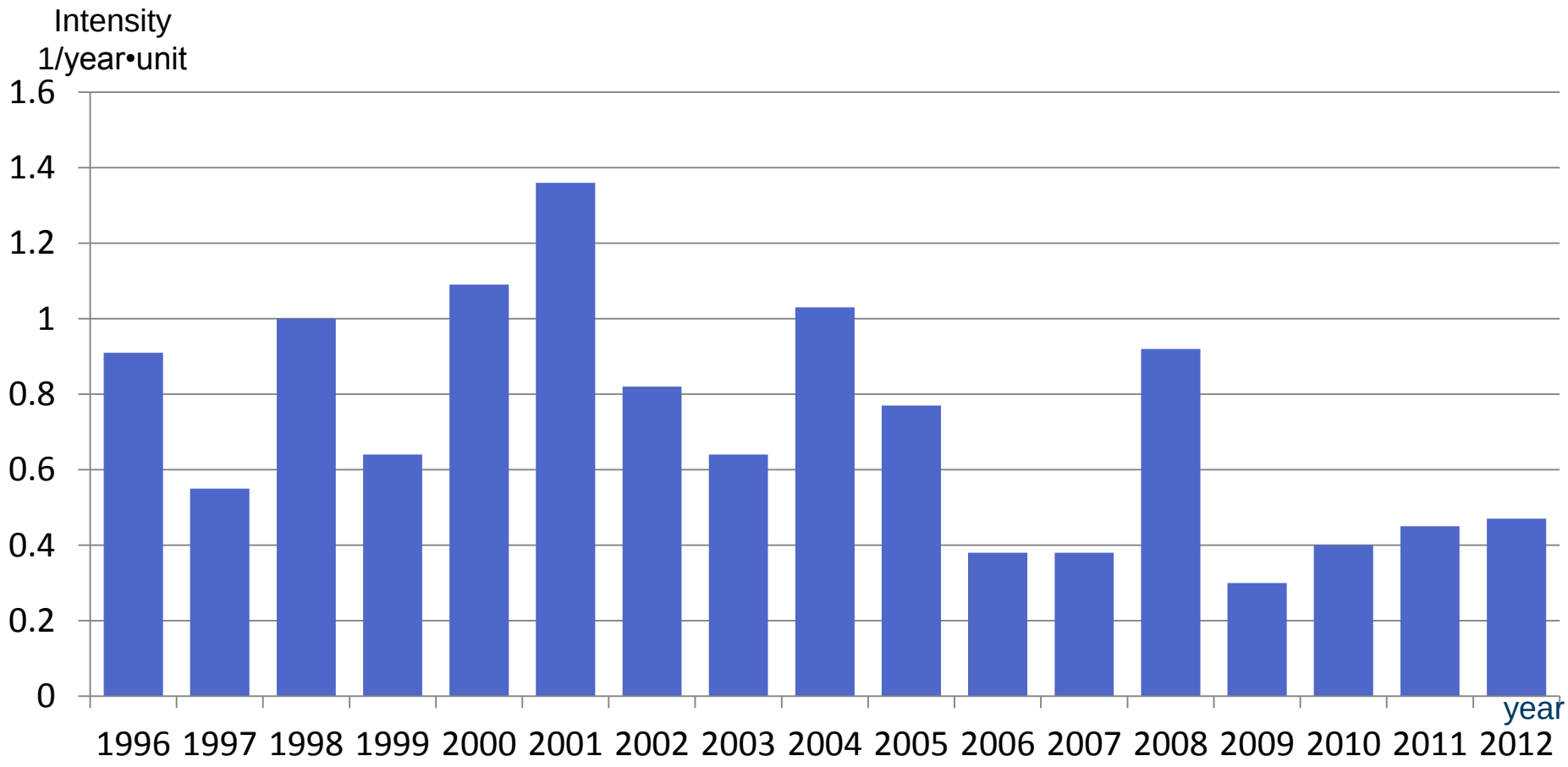
CHERNOBYL LESSONS

Comparison Of intensity of violations (Ukraine, 15 units WWER) and Licensee Event Reports (LER) (USA, 69-73 units PWR)



CHERNOBYL LESSONS

The intensity of Ukrainian NPP's violations caused by I&C incorrect functioning



Share of violation, caused by incorrect functioning of I&C, in relation to total number of violations in operation of NPP units with WWER was equal to 25%.

CHERNOBYL LESSONS

Some comparisons with events analysis in USA

	J.Bickel (Reliability Engineering and System Safety, 2008)	B.Geddes, R.Torok (ICONE-16, 2008)	Ukraine
Type of system	Digital reactor protection systems (1st generation)	1E and non 1E digital I&C	Digital and non digital I&C
Data of collection	1984-2006	1987-2007	1996-2007
Number of events	141	Operating Experience Report (OER) – 500 NRC database (LER) – 324 1E – 49	Digital – 33 All – 123

CHERNOBYL LESSONS

Some comparisons with USA (continue)

Share of events in digital I&C because of software

Ukraine	USA
2 out of 13 (digital systems 1-st generation), 0 out of 20 (digital systems 2-nd generation)	**4 out of 49 (1E systems)**

Conclusion: Protection against the software failures is already at a “reasonable assurance” level.

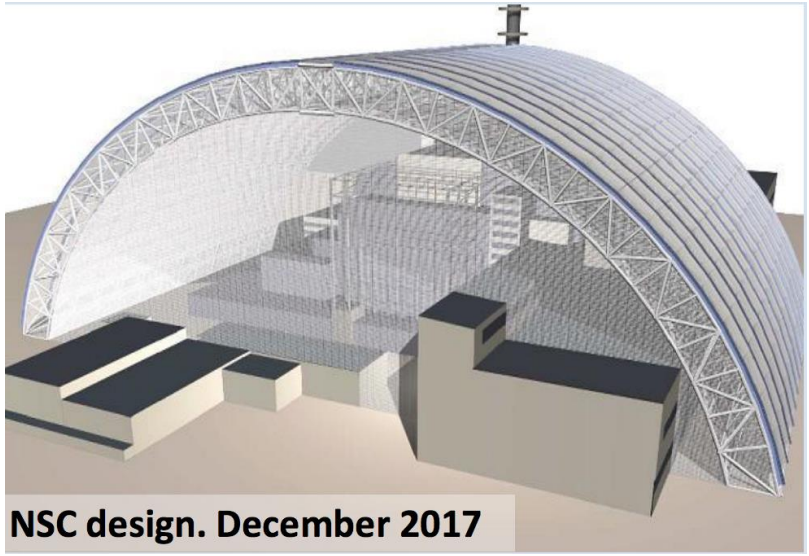
Some comparisons with rocket and space systems

- 20% emergencies in rocket and space system in rocket and cosmic system were due to digital computer systems – (as NPP);
- 80% emergencies in rocket and space system due to computer systems took place because of software (difference from NPP).

CHERNOBYL LESSONS

Chernobyl Confinement


NSC construction. October 2015


NSC design. December 2017

- **Project Highlights:**
- At 541 feet long, 853 feet across and 360 feet high, it will be tall enough to house Paris' Notre Dame cathedral.
- It will weigh more than 33,000 tons,
- The structure will be strong enough to withstand a tornado
- It will house a sophisticated ventilation system and cranes for dismantling and waste management.
- The contract to build the structure was awarded in 2007 to the Novarka consortium, led by the Bouygues and Vinci companies of France.
- It is funded by the Chernobyl Shelter Fund established in 1997. Forty one individual countries (including the U.S.), the European Community and the European Bank for Reconstruction and Development had contributed more than $ 2 billion to the fund.

FUKUSHIMA LESSONS

FUKUSHIMA LESSONS

Fukushima Daiichi NPP, units 1, 2, 3, Japan, 2011

Main reasons:

- combination of earthquake and tsunami;
- mistakes in design (wrong accounting of stressing environment, wrong placement of diesel-generator switch and cooling pond, etc.).

These reasons don't have straight connection with mistaken actions of I&C. Reactors were stopped by emergency protection systems, reserve diesel-generators were switched on, pumps for emergency heat removal were switched on, etc.

But nevertheless Fukushima accident lead to necessity to pay attention to a lot of new problems related to I&C in all countries with NPP.

Main lessons:

- reevaluation of safety of acting NPPs (including stress-tests of I&C equipment);
- hardening of requirements to NPP (including NPP I&C);

FUKUSHIMA LESSONS

Reevaluation of acting NPP safety

Immediately after earthquake Regulatory Bodies of all countries with NPP declared an urgent necessity of safety reassessment of NPPs based on a overall and open of risk assessment (“stress-tests”).

“Stress-test” - is the additional checkup based on the design materials, safety analysis reports, performed researches, expert assessments and engineer assumptions with taking into account more severe impacts and possible overlap of negative factors (in the lights of accident on Fukushima NPP).

Detail program of “stress-test” was fulfilled for every NPP with allowance for differences of NPP site, types of operating reactors.

Initiating events conceivable at the plant site were earthquake, flooding, tornado, extreme high/ low temperature, external fire, combination of external influence.

The most important initiating event to I&C systems was earthquake, exceeding design basis.

FUKUSHIMA LESSONS

Risk assessment from earthquake consisted of seismic qualification of hardware which should cover the components of safety systems including systems for support systems (e.g. emergency diesel-generator). Seismic qualification performed during validation process and stipulated the assessment of seismic influences on hardware as well as on their fastening to building construction and on external electric or optic cables in the places of their connections to hardware.

Results of “stress-tests” of Ukrainian NPP’s:

- Additional analysis of seismic for all sites were fulfilled; their project seismic characteristics were validated .
- Equipment including I&C systems hardware which necessary for fulfillment of main safety functions are stability under project seismic influence and have safety margins .

FUKUSHIMA LESSONS

Identification of dangerous events

Identification of dangerous events is actual task as well. Some of the I&C should detect dangerous external and internal events which can lead to extreme influences on NPP equipment and initiate the operation of actuators for minimization of the risk from these influences. Failure of these systems (components) may lead to abnormal situation which can grow intro accident. It was necessary to make reassessment which confirmed compliance of seismic sensors with new, more severe requirements to functional safety (and particularly, to accuracy).

FUKUSHIMA LESSONS

The next lesson of Fukushima - strengthening of emergency availability and response.

This lesson for I&C is related by post-accident monitoring system (PAMS).
PAMS should realize support of NPP personnel and safety experts for the accidents control, for elimination of their consequences, for return of reactor facility to controllable state and for the following analysis of the causes and ways of the passing of accident.
Displays of PAMS should be placed in the control rooms and in crisis centers.

Necessity of creation PAMS was dictated by the big NPP accidents.
After Three Mile Island accident IEEE developed in 1981 standard with PAMS requirements (IEEE-497-1981). US NRC – developed document with guidelines for creation of PAMS (Regulatory Guide-1.97) .
But international standards for PAMS began to elaborate only after Fukushima accident.
In some countries, included Ukraine, the question about creation of PAMS began only after Fukushima accident.

FUKUSHIMA LESSONS

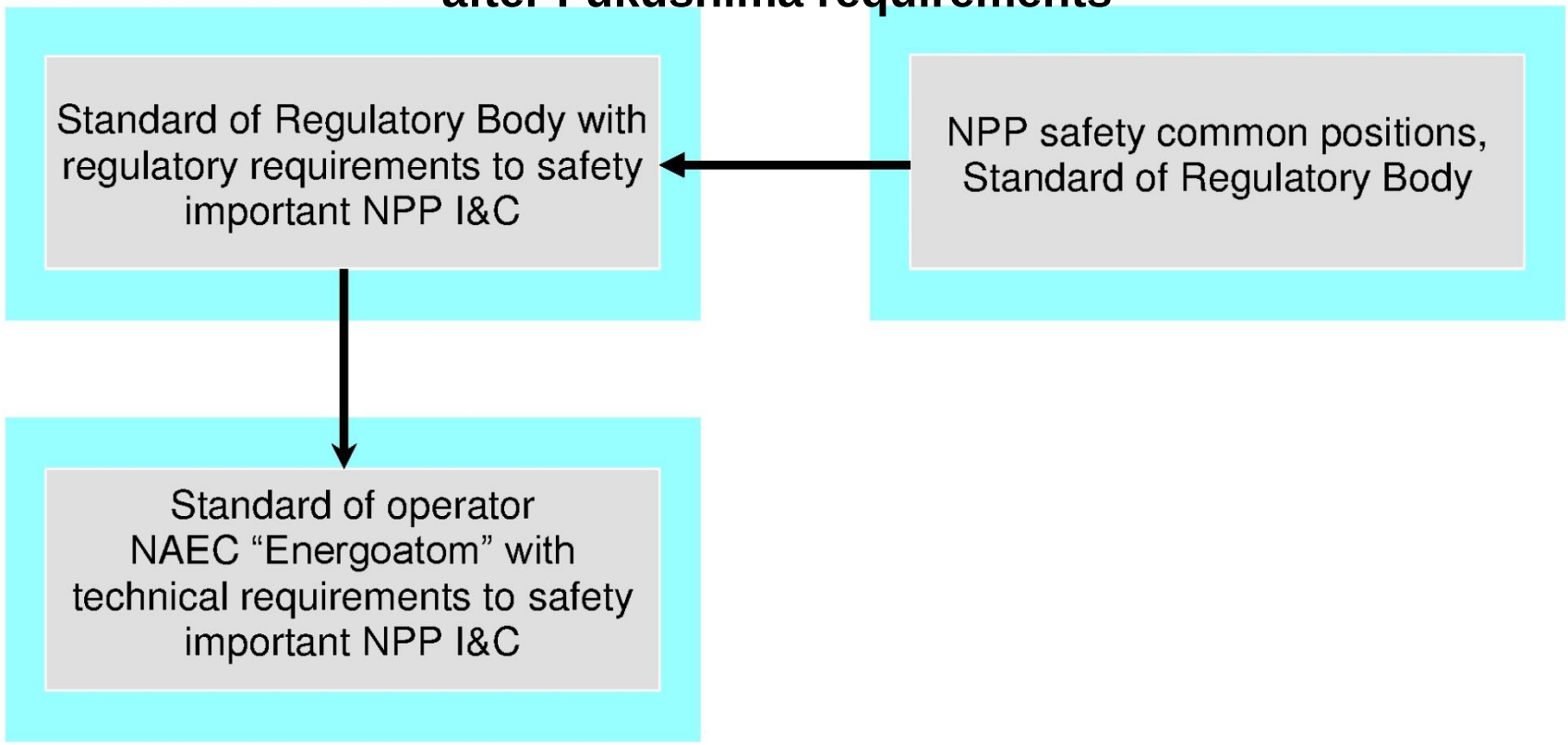
Hardening of requirements to NPP I&C

- Requirements to seismic resistance are toughened considerably. Japan earthquake forces to revise the design rules.
- Requirements for sensors for post-accident monitoring
- The next requirement-additional energy supply will be connected to every NPP by special reserve schemes (e.g. from nearest generators of hydroelectric power plant).
- Safety classification of functions is more exact (e.g. the functions which detect dangerous external influences - earthquake or fire) and fulfill the actions for softening of their consequences .

FUKUSHIMA LESSONS

New Ukrainian Regulations for I&C systems important to NPP safety.

SSTC NRC in 2016 ended elaboration of two interconnected standards related to NPP I&C instead acting standard 2000, which considered after Fukushima requirements



FUKUSHIMA LESSONS

Structure of requirements to durability NPP I&C of functions execution in new standard of Ukrainian Regulatory body

- protection against common cause failures;
- observance of single failure criterion;
- observance of redundancy principle
- observance of the diversity principle
- requirements to prevention of personnel error;
- requirements to protection from unauthorized access;
- requirements to technical diagnostic;
- requirements to reliability measures.

FUKUSHIMA LESSONS

Some private considerations

1. According to the IAEA and different countries rules, operators are responsible for NPP safety. Government intrusion isn't mentioned. But in Fukushima case, there weren't enough of NPP and company efforts. The government delayed with actions for accident elimination.
Chernobyl situation – another extremity – tough management from the government.

2. Repeat of Chernobyl situation: there were some opinions of competent specialists about lack of reactors (Chernobyl NPP) and about possibility of tsunami (Fukushima). They weren't considered .

3. Lack of information about NPP situation at once after accident (e.g., meeting “25 years after Chernobyl”).

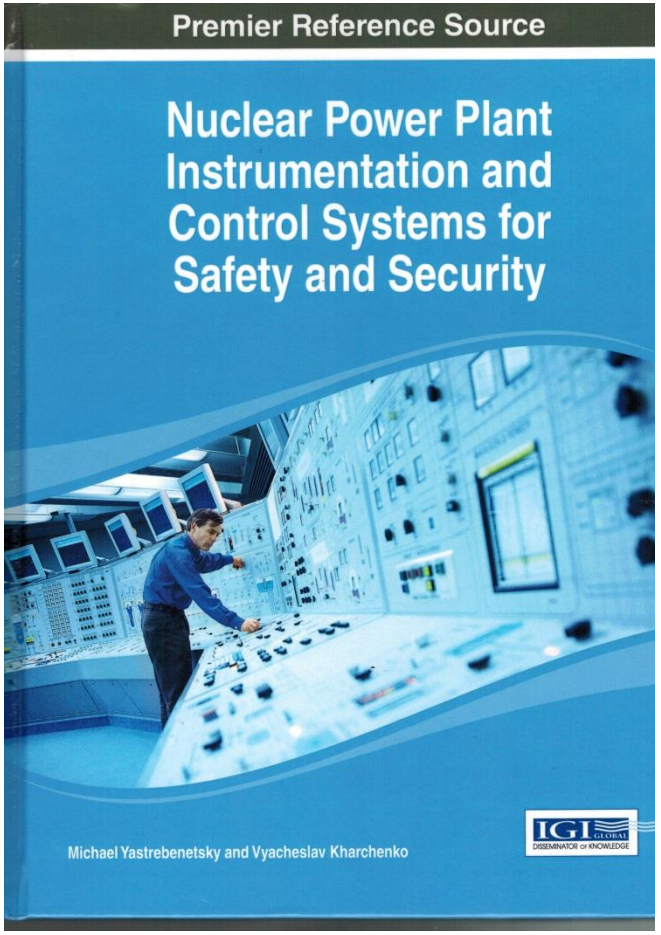
4. Delay of external power supply to the site.

KNOWLEDGE DISSEMINATION EXPERIENCE

“NPP I&C Systems for Safety and Security”

The book “Nuclear Power Plant Instrumentation and Control Systems for Safety and Security”, was published in USA in 2014 in English (Engineering Science Reference, an imprint of IGI Global), 450p., Hershey PA.
Editors – M. Yastrebenetsky, V. Kharchenko.

The book is based on the experience of State Scientific and Technical Center for Nuclear and Radiation Safety and National Aerospace University named after N.E. Zhukovsky .

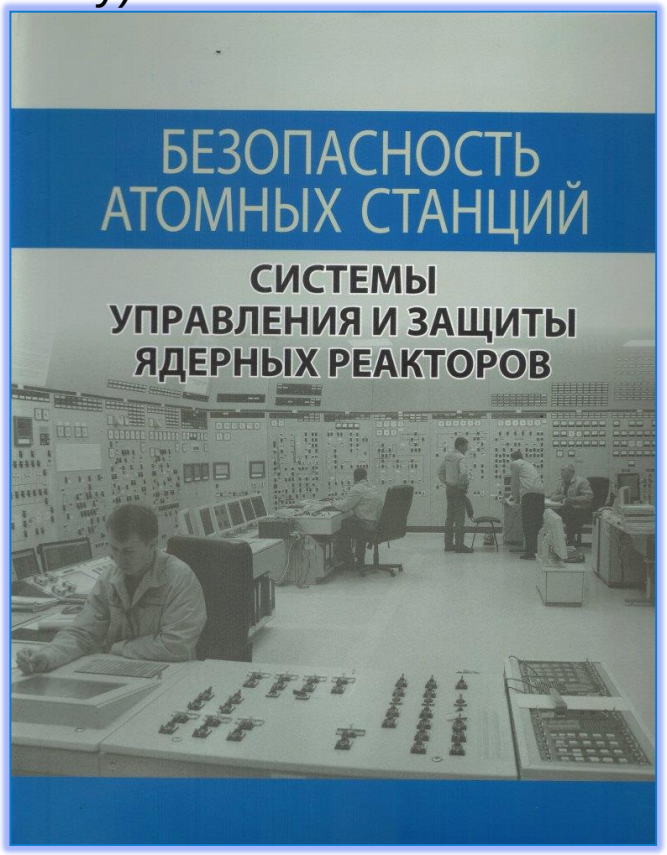


KNOWLEDGE DISSEMINATION EXPERIENCE

“Nuclear Power Plants Safety. Nuclear Reactors Control and Protection Systems”

The book “Nuclear Power Plants Safety. Nuclear Reactors Control and Protection Systems” (authors – M.Yastrebenetsky, Y.Rozen, S.Vinogradska, G.Johnson, V.Eliseev, A.Siora, V.Sklyar, L.Spector, V.Kharchenko) was published in 2011 (Kiev, “Osnova-Print”, 768 p., in Russian, editor – M.Yastrebenetsky).

The book is devoted to control and protection systems of nuclear reactors. Standards of IAEA, IEC, Ukraine that pertain to these systems are examined, requirements to these systems and their components determined. These systems of different generations which are operated in Ukrainian NPPs are described: neutron flux monitoring systems, emergency and preliminary protection systems, power limitation and power control systems, group and individual control rod systems. The main attention is attended to new computer based systems and peripheral devices, described by Ukrainian companies.



KNOWLEDGE DISSEMINATION EXPERIENCE

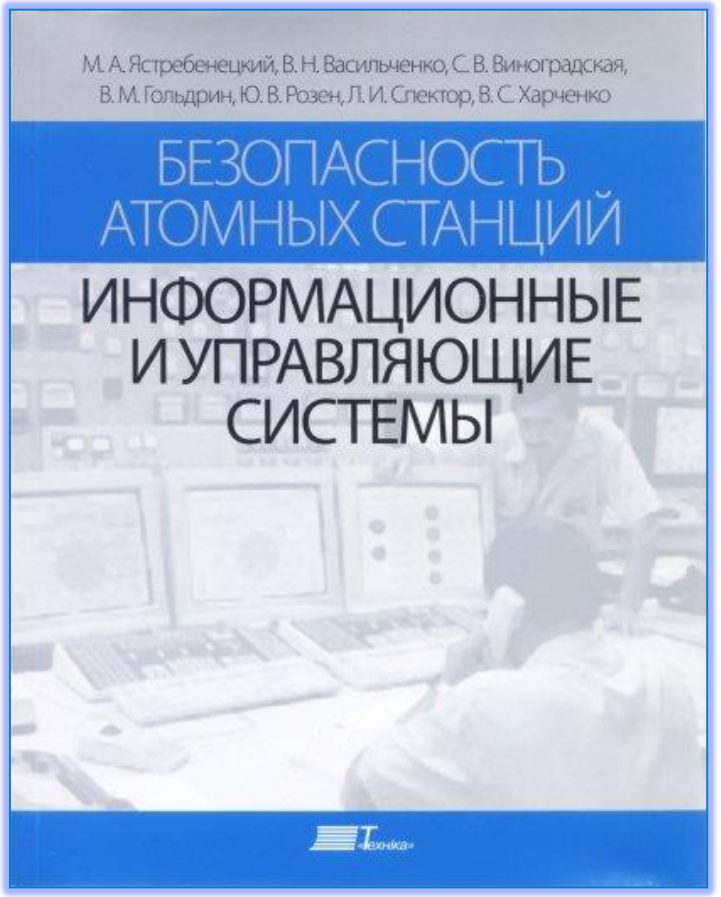
"NPP Safety: I&C Systems"

The book "Nuclear Power Plants Safety: Instrumentation and Control Systems" (authors – M.Yastrebenetsky, V.Vasilchenko, S.Vinogradska, V.Goldrin, Y.Rozen, L.Spektor, V.Kharchenko) was published in 2004 (Kiev, State Publish House "Technika", 466p., editor – M.Yastrebenetsky)- in Russian.

The book is based on the experience of State Scientific Technical Center of Nuclear and Radiation Safety in safety assessment and assurance of I&C systems for 13 units WWER-1000 and WWER-440 NPP during 1993-2003 and in creation standards related to NPP I&C.

I&C systems designed not only by Ukrainian, but designed by Russian, USA, Czeck republic, France, Hungarian companies are used in Ukrainian NPP's. That gives possibility to authors in receiving knowledge of these countries in I&C creation and safety assessment.

Translated in English by US Nuclear Regulatory Commission (2007).



The book has 4 parts,
16 chapters, 3 attachments

KNOWLEDGE DISSEMINATION EXPERIENCE

Ukrainian Regulatory Body, State Scientific and Technical Centre for Nuclear and Radiation Safety, NAEC "Energoatom“, National Academy of Sciences of Ukraine organized

International Scientific-Technical Conferences “NPP Instrumentation and Control Systems: Safety Aspects”.

The last 5-th conference – October 2013 (Kharkov, Ukraine).
Chair – Mikhail Yastrebenetsky.

PAPERS
for American Nuclear Society International Topical Meetings "Nuclear Plants Instrumentation, Control and Human Machine Interface"

- 2000 - SPDS impact on WWER-1000 safety
- 2004 - Model of modernized I&C system expert review
- 2006 - Evaluation of NPP functional safety measures
- 2009 - Operating reliability of WWER digital I&C systems
- 2010 - Ukrainian NPP I&C standard base
- 2012 - Fukushima accident lessons for I&C systems (Ukrainian experience, first steps)
- 2015 - Experience of I&C modernizations for unit life extension

CONCLUSION

Some directions for future activity

- Instrumentation (sensors, transmitters, cables, computers, nets) for design extension conditions. The problem- the cost of developing and qualifying sensors for use in high radiation, high temperature, pressurized steam, and chemically aggressive environments are very high. Cost is a direct factor that makes procurement of sensors expensive. Small market for nuclear equipment when compared with other industries
- Measuring of pressure, temperature, level, flow rate in damaged reactor;
- In-Containment wireless applications:
    - Vibration monitoring;
    - Containment environmental monitoring;
    - Containment cooling system, etc.;
- Sensors which can operate without external supply (receiving energy for account of high temperature or high vibration on the placement of location).

THANK YOU

Mikhail Yastrebenetsky

ma_yastreb@mail.ru