Fukushima Lessons for Safety of Critical Control Systems

Prof. Mikhail Yastrebenetsky,
Dr. Alexander Klevtsov,
Yuri Rozen,
Serhii Trubchaninov

State Scientific and Technical Center for Nuclear and Radiation Safety (SSTC NRS)
53, Chernishevska str., of.2, 61002, Kharkov, Ukraine
E-mail: ma_yastrebenetsky@sstc.com.ua

Abstract

The accident at Japan nuclear power plant (NPP) "Fukushima-Daiichi" has influenced not only to future development of the nuclear energetics as whole and different NPP systems (including, of course, their control systems). However, the lessons of this accident are important for safety of critical control systems in different branches of industry. Some propositions for their safety assurance followed from nuclear post-Fukushima experience are discussed below.

Key words: Fukushima, safety, control system, accident, earthquake.

Russian academician Boris Chertok, a designer of control systems for space vehicles, including the vehicle for the first cosmonaut Yuri Gagarin, noted subsequently: "When I wrote these memoirs, I have received validity of the statement that catastrophic, accident-related and off-nominal situations are one of the most powerful stimulus of the cosmic technics progress speeding up" [1]. This statement takes place not only for space, but for other branches of technics, where safety problems are very important. Meanwhile, catastrophic, accident-related and off-nominal situations in one branch, where there are critical control systems, can affect to critical system's[1] progress in the other branches of technics.

The accident on Japan NPP "Fukushima-Daiichi" in 2011 (so as accidents on NPP "Three Miles Islands" in the USA in 1979 and on Ukrainian NPP "Chernobyl" in 1986) exerted an essential influence on the development of safety activity not only for nuclear energy, but for different branches of the industry.

The reasons of the Fukushima accident had natural types. This accident was caused by the combination of off-design earthquake and tsunami. The signals about the earthquake entered the reactor control systems, resulted in an emergency shutdown of all units. The reserve diesel-generators were started-up after the loss of external power supply. However, the technological safety systems for reactor core cooling ceased their actions: the power supply commutators from normal supply to reserve diesel-generators were installed in flooding area. The design mistake was added: the spent fuel pools for the most dangerous nuclear fuel were outside of reactors containment. The nuclear fuel was overheated and the reactors were destroyed. The Fukushima

[1] Systems which purpose is the prevention of the equipment, machinery, plants from going into a dangerous state by taking appropriate actions on the receipt of the commands are known as the critical systems

accident did not have direct connections with mistaken actions of reactor control systems. But this accident leads to necessity to pay attention to a lot of new problems related to NPP safety of critical control systems and to such systems not only for NPP.

There are many publications devoted to Fukushima lessons for nuclear energy (e.g. [2-5]). These lessons were analyzed by international organizations in the nuclear energy area, first of all- International Atomic Energy Agency (IAEA), and by all countries where NPP are operated. These lessons

have a technical character (as set of actions on assessment and increasing of NPP safety), as well as a political character (related to the refusal from the building of new NPP or the discontinuation of existing NPP's operation). As opposed to the publications where lessons from the NPP Fukushima accident were analyzed for nuclear application, the lessons for safety of critical control systems (CCS) for other branches of industry will be considered below in this paper. Examples of these branches are chemical, petrochemical and gas industries, gas and oil transport, etc. The consideration of the main principles of NPP safety assurance will proceed with these lessons.

The principles of NPP safety assurance

The principles of NPP (including their control systems) safety assurance are described in IAEA documents [6-8] and in the national documents of different countries (e.g. [9]).

- There are special state organizations in all countries where NPP's are operated. The aim of these organizations is the regulation of the nuclear and radiation safety. These organizations are independent from NPP, from NPP designers or developers and suppliers of NPP equipment. The general name of these organizations is "Regulatory body", but official names are various in different countries (e.g., "Nuclear Regulatory Commission" in USA). Regulatory bodies fulfill different functions with the aim to create of regulatory mechanism for nuclear and radiation protection of people and the environment. The control of every NPP safety is realized not only by NPP equipment and personnel, but by Regulatory body as well - by central office and by their representatives who constantly are located at NPP sites. One of the functions of Regulatory body is the realization of the independent expert reviews for research, testing and analysis of compliance of all safety important NPP systems and components (including, of course, control systems and their components) with the requirements to nuclear and radiation safety. General diagram of NPP unit safety control is presented in fig.1. On this fig. 1 are shown the following elements:

1. The influence of the external environment to the NPP (from power consumers, earthquakes, flooding, dropping of an airplane, etc.).
2. The information about the technological equipment conditions entered to the control system.
3. The control action from the control system to the technological equipment.
4. The information about the technological equipment and the control system conditions, which represented to NPP operating personnel.
5. The control action from NPP operating personnel to the control system.
6. The information from the control system and NPP operating personnel about safety important parameters, which represented to the NPP administrative-technical personnel.
7. The information (directives) from NPP administrative- technical personnel represented to NPP operating personnel.
8. The information about parameters which defined unit safety, which represented in Regulatory body.
9. Directives of Regulatory body (safety standards, safety reviews, results of supervision by representatives of Regulatory body at the NPP site, etc.) to NPP administrative-technical personnel.

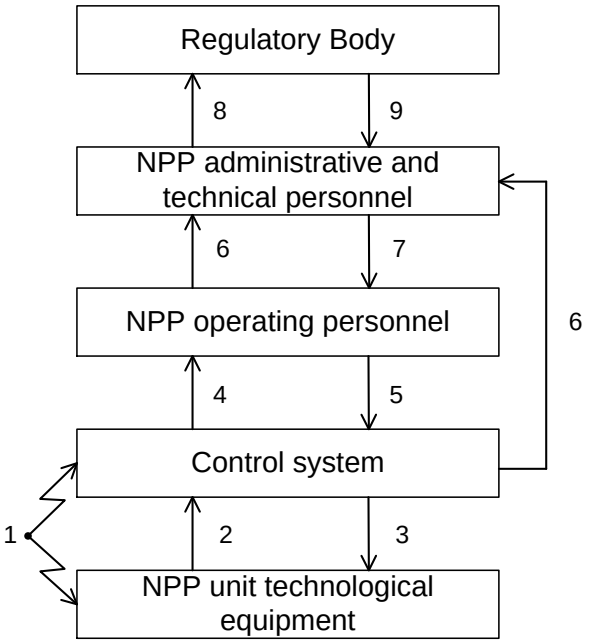

Figure1. General diagram of NPP unit safety control

- The operating organization ensures NPP safety and bears full responsibility for it, including the measures to prevent the accidents and mitigate their consequences, the inspection of nuclear materials and radioactive substances, the protection of the environment. This responsibility doesn't reduce connection with independent activity and responsibility of the designers, suppliers, builders and the Regulatory body.
- Observance of normative documents (norms, rules, guidelines, standards, etc.), which pertain to NPP safety, is mandatory in carrying out of all kinds of activity related to the use of nuclear power. One can agree that the necessity of a special permission system in this field of relationships replaces the popular democratic principle of "everything is permitted that is not prohibited in particular" with the opposite one - "everything is prohibited that is not permitted in particular".
- Fundamental principle of NPP safety assurance is "defense in depth" which based on:
  - the system of physical barriers, which assure the possibility of continuous prevention of the release of the ionizing radiation and the radioactive substances into the environment;
  - the system of levels of technical and organizational measures to protect the physical barriers and preserve their effectiveness for the purpose of protecting the personnel, the population and the environment.
- One of the factors that substantially influences on NPP safety is activity of IAEA – the international organization which is connected by an Agreement with the United Nations Organization. Activity of the IAEA consists in emergency assistance in case of accidents, technical cooperation, information exchange, different inspections of NPP and suppliers (examples: missions of NPP control systems independence review in the Republic of Korea, Russia and Ukraine), training of personnel, and also development of IAEA safety standards coordinated at an international level.

Propositions for the control systems safety improvement

The aim of this section and this paper as a whole isn't the recommendations for implementing post-Fukushima actions for the concrete equipment under control (EUC) and the concrete EUC control systems. But the aim is to draw attention of safety specialists on post-Fukushima actions for following evaluation of the possibility of implementing these actions in non-nuclear EUC.

- After the Fukushima accident the reassessment of the safety vulnerabilities of NPP took place in the light of lessons learned from the accident. These actions for different types of NPP systems (including control systems) received the name "stress-tests" - the additional checkup based on the design documents, the safety analysis reports, the performed researches, the expert assessments, the tests and the engineer assumptions by taking into account more severe impacts and the possible overlap of negative factors. The initiating events conceivable at the plant site are earthquake, flooding, and other extreme natural events (e.g., extreme high and low temperature).

The most important initiating event that leads to the accident was the earthquake, exceeding the design basis. Earthquake in Fukushima forced to the revise parameters of the seismic influence spectrum. After the Fukushima accident, seismic analysis of control systems equipment was fulfilled for all NPP's. During this analysis was taken into account the accelerograms of the ground for maximum earthquake, the coefficient of building constructions damping, the height of placing, the intermediate constructions (the panels, the desks, the consoles, the technological equipment, if the devices were mounted on them), ageing. The analysis covered all components of the NPP safety important control systems (e.g. a control system for the emergency diesel-generators), including not only devices, but electrical and optical cables in the places of their connections with hardware devices. The requirements for the testing impact, which imitate of the earthquake response spectrum, became tougher.

This practice may be recommended for the critical control systems for the different EUC located in the places where earthquakes are possible. It should be noted, that one of the first investigations devoted to analysis of mechanical impacts to hardware was fulfilled by Igor Ushakov with his colleague Yuri Konenkov [10].

- The Fukushima accident had shown the necessity of the taking into account not only of possible influence taken separately, but also the combination of the different extreme influences (fire, extreme high/low temperature, flood, tsunami, tornado), as well as the common cause failures of control systems due to the extreme influences and their effects. The requirements for the defense in depth, reservation, diversity, independence have to be determined by the accounting of the combination of these influences.
- The identification of dangerous events is actual task as well. Some of the control systems should detect dangerous external and internal events, which can lead to extreme influences on equipment and initiate the operation of the actuating systems for the minimization of the risk from these influences. The failure of these systems (components) with the high probability leads to the abnormal situation what can grow into accident. The examples are seismic sensors, which have to identify earthquakes. It is necessary to make the reassessment, which confirms compliance of these sensors with new, more severe requirements. The actual problem for seismic sensors is the experimental validity of sensor response to different forms of the spectrum acceleration on the sensor input.
- After the Fukushima accident took place loss of external power supply because of the earthquake. The next event was loss of internal power supply from 13 diesel-generators because of the tsunami. These events led to full de-energization of all NPP units and reactor cores were melted. The most of control system instruments remained unbroken, but the absence of power supply by either direct or indirect current provoked a full loss of the information. The main control room and the supplementary control rooms were useless due to loss of power supply. It's interesting to describe some measures, which were already realized or planning to realization in future to avoid the same situation:
  - The development of indicating and recording devices for the most important safety parameters, which can operate regardless of general power supply of the equipment under control. It is necessary to provide the autonomous power supply for these devices during some time after the accident. Another further way is a creation of the sensors which can operate without an external supply (e.g. receiving energy thanks to high temperature on the placement of location);

- The installation of the special mobile and moveable individual diesel-generators for power supply in the case of fault of the stationary diesel-generators.

- The necessity of NPP control assurance by the personnel after accident (the control rooms "habitability"). A destruction of infrastructure near control systems, including communication cables and channels of data communication should be taken into account.

- There is a new type of NPP control system – post-accident monitoring systems (PAMS). PAMS began to operate before Fukushima accident, but these systems received wide distribution after this accident. PAMS realizes support of NPP personnel and safety experts during and after accident for:
  - receiving of information about the type and the time of the initiating events appearance, the violations of operating limits and conditions, the emergency situations and accident development;
  - receiving information about the state of safety important constructions, systems and elements, the values of technological parameters, about radiological conditions of environment;
  - the elimination of the accident consequences;
  - return of reactor facility to controllable state;
  - following analysis of the causes and the ways of the passing of design basis and beyond design basis accidents;
  - saving of archive data about accident against premeditated or unpremeditated alternations.

PAMS should provide acquisition, archiving, saving, displaying and registration of information in severe conditions, during internal and external influences after an emergency, including accidents. Now International Electrotechnical Commission (IEC) is elaborating international logo-standard IEEE/IEC devoted to PAMS on the base of the Institute of Electrical and Electronic Engineers (IEEE) standard [11]. NPP's experience in the creation of PAMS may be useful for some branches of industry (e.g., chemical and petrochemical).

- After the Fukushima accident the standards related to safety of NPP control systems were revised by many organizations. New IAEA standard related to NPP control systems safety, issued in 2016, is described in the paper [12] in this Journal. The authors of this paper were the heads of the international team, which elaborated this standard. The Technical Committee "Nuclear Instrumentation" of IEC made changes in their set of standards, as well as the Regulatory bodies of many countries. For example, new Ukrainian standard [13], related to NPP safety important control systems, established new regulatory requirements for these systems:
  - the requirements to archiving and storage of the data needed to analyze the accident causes and progress, which should remain intact under any possible effects during the design and beyond design basis accidents;
  - the seismic resistance classification criteria and rules for modeling the seismic impact under seismic resistance testing are established. They take into account conservative assessment of the damping coefficient of the building structures in defining their response to the ground movement, etc.

It may be recommended for designers of critical control systems in the other branches of industries to take into account some of provisions of these standards (of course, taking into account the branch specifics).

- It should be noted that one of possible directions for NPP safety increasing, accident management and post-accident monitoring is the use of wireless technologies, which give some advantages in comparison with traditional cable links:
  - The possibility of placing of wireless sensors in places where the use of cables is complicated or impossible;
  - increasing of reliability of data transferring from wireless sensors by means of excluding of the potential possibilities of cables damages (particularly, in accident conditions);

- increasing of mobility by means of easy replacing of wireless devices;
- the possibility of installation of any quantity of additional sensors for more accurate monitoring or in case of failures of the operated sensors.

Without doubt, the use of wireless technologies on NPPs requires the solution of some technical problems (supply with electrical power, high data transfer rate, resistance to electromagnetic interferences, protection of information, etc.), approbation, nuclear and radiation safety assurance and development of an appropriate regulatory framework. However, this is a prospective direction for further research.

Conclusions

The Fukushima accident lessons which were used for safety of NPP control systems could be applied for development and manufacturing of components, for design, integration, tests, operation of critical control systems not only for NPP, but for critical control systems in the other branches of industry.

References

1. Chertok B. Rockets and people. Moon race. Moscow, Mashinostroenie. 1998. (In Russian)
2. The Fukushima Daiichi Accident. Report by the Director General and Technical Volumes. Vienna, IAEA, 2015.
3. Way Kyo. Energy: Environmental Protection and Safety in the Wake of the Fukushima Nuclear Accident, John Wiley & Sons, 2012.
4. G. Johnson (Editor). Severe Nuclear Accidents: Lessons Learned for Instrumentation, Control and Human Factors. Electric Power Research Institute, Technical report, 3002005385, Palo Alto, CA, USA, 2012.
5. M. Yastrebenetsky, Y.Rozen, A.Klevtsov, S.Trubchaninov, V.Lebedynskiy, V.Martinenko, S.Lebedynskyy. Fukushima Accident Lessons for I&C Systems 8th International Topical Meeting on Nuclear Power Plant Instrumentation and Control, and Human-Machine Interface Technologies (NPIC&HMIT 2012), American Nuclear Society, San Diego, 2012.
6. IAEA Fundamental Safety. Principles Safety Fundamental. SF-1. Vienna, IAEA, 2006.
7. Safety of Nuclear Power Plants: Design. SSR- 2/1. Vienna, IAEA, 2016.
8. Safety of Nuclear Power Plants: Commissioning and Operation. SSR- 2/1. Vienna, IAEA, 2016
9. General Provision of Nuclear Power Plants Safety. NP 306.2.141-2008. Ukrainian State Committee of Nuclear Regulation. Kyiv, 2008. (In Ukrainian).
10. I. Ushakov, Yu.Konyonkov. Reliability of Mechanical Equipment. (part1,2). Znanie, Moscow, 1973, 1974. (In Russian).
11. IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations. IEEE Std 497™-2010.
12. G.Johnson, A.Duchac. The development of the new IAEA safety guide for design of instrumentation and control systems for nuclear power plants. Reliability: Theory and Applications. 2017, 1.
13. Requirements for nuclear and radiation safety of instrumentation and control systems important to safety of nuclear power plants. NP 306.2.202:2015. Official Bulletin of Ukraine, 2015, No.56 (In Ukrainian).