ADCHEM 2006

International Symposium on Advanced Control of Chemical Processes
Gramado, Brazil – April 2-5, 2006

BLOCK DIAGRAM PROPOSAL OF PROTECTION SYSTEM FOR A PWR NUCLEAR POWER PLANT

Francisco Joailton de Lima[1], Claudio Garcia[2]

Telecommunications and Control Engineering Department
Escola Politécnica of the University of São Paulo
Av. Prof. Luciano Gualberto, Trav. 3, 158 - Butantã
City: São Paulo - SP - Zip code: 05508-900 - Brazil
[1]francisco.lima@poli.usp.br, [2]clgarcia@lac.usp.br

Abstract: This text presents a block diagram proposal of protection system for a PWR nuclear power plant. It describes the plant operation, as well as it defines what a protection system is. Some of the main inherent definitions to protection systems are shown and the system operation is explained in a global form. The block diagram proposed for the protection system can be used as a project foundation for the protection automation.

Keywords: Fault tree, nuclear reactor, protection system, reliability, safety.

1. INTRODUCTION

There are approximately 440 nuclear power plants (NPP) in the world, according to figure 1. However, this kind of energy generation is still considered as a threat to human life and with a great potential to cause grave accidents, although modern NPP comply to strict project, building and operation criteria, which make them very safety.

The two greatest accidents that contributed to this insecurity representation of the nuclear power plants occurred at the TMI – Three Mile Island, Pennsylvania, in the United States on March, 28th , 1979 (Chairman at all, 1979) and at Chernobyl in the former Union of Soviet Socialist Republics - where today lies Ukraine - on April, 26th, 1986 (Edwards, 1987). In the first accident (TMI), despite having happened heating and deterioration of the reactor core, there was little emission of radioactive material into the environment. In the second accident (Chernobyl) occurred an explosion of the reactor and a great quantity of radioactive matter was spread into the atmosphere.

Besides other safety devices existing in a nuclear power plant such as the containment building, where the reactor is located which - if ever existed at the Chernobyl NPP - could have slowed down the amount of radioactive matter disseminated into environment, there is the protection system for a nuclear power plant that is the scope of this study.
At present, The Brazilian Navy is working on the LABGENE (Electrical Core Generation Lab) project at the Navy Technological Center in São Paulo (CTMSP), which consists of the development and construction of a nuclear power plant to generate electrical energy that will act as a basis and developing laboratory to another projects of nuclear reactors in Brazil (INFOREL, 2004).

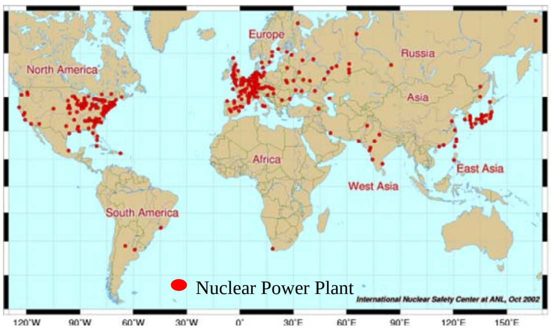

Fig. 1. Maps of Nuclear Power Reactors: WORLD MAP (Nuclear Plants, 2005).

As far as we know, articles presenting the block diagram of the protection system, as proposed here, have not been published yet. Thus, this is one of the reasons that led us to write it.

2. PWR NUCLEAR POWER PLANT

The acronym PWR stands for the English term “Pressurized Water Reactor”. This name is derived from the fact that in this kind of plant its cooling system is obtained from a pressurized water circuit.

The operating principle of the power plant illustrated in figure 2 is the following: the fission heat in the reactor core is used to increase the water’s temperature (coolant) of the primary circuit, the steam generator absorbs the heat from this water, transferring it into the secondary circuit in the form of steam; the produced steam runs a turbine that transmits mechanical energy to an electrical generator, which, then, converts the mechanical energy to electricity.

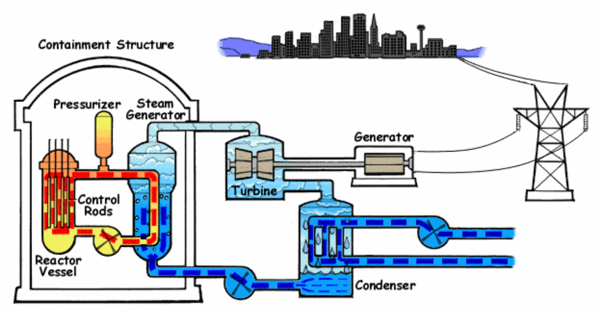

Fig. 2. Pressurized Water Reactor (Nuclear Reactors, 2005).

3. PROTECTION SYSTEM

Below are presented some definitions and is proposed block diagram of the protection system for a PWR nuclear power plant.

3.1 Definitions

3.1.1 The Plant Protection System

The protection system of a nuclear power plant has the function to take the necessary measures to avoid accidents which may lead to overheating and degeneration of the reactor core as well as contamination of the environment caused by radioactive matter. Moreover, it makes sure the plant will operate within the safety limits stated in the project. These actions consist on turning off the reactor, bringing to an end the fission of the fuel element and/or activating the protection system such as emergency diesel-generators, valves, emergency cooling-system, etc.

3.1.2 Reliability

A very important requirement to the protection systems is their reliability, which can be defined as the probability of a system to work accurately (according to its project specifications) within a time interval [t_0 ; t], in which it was working properly at the starting point t_0.

3.1.3 Redundancy

Consists in the use of more than one equipment to execute the same function, that is, in case of failure of the first device, the next can be able to warrant the continuity of that function in the system, increasing the system reliability. This procedure is applied to protection systems, e.g. when three sensors are used to measure a certain temperature variable. If two of these measures are above a pre-established value ("set point"), the system acts by disconnecting, alarming and/or activating the security system. When that happens, it is said that occurred a voting of 2 out of 3.

3.1.4 Fault Tree

Fault Tree is a tool used for the analysis of the reliability in protection systems. A fault tree represents a system or a subsystem through a diagram that has a top event which occurs from a combination of other events. This combination is represented by symbols that interconnect those events by means of logical operations such as "AND", "OR", etc (McCormick, 1981). A qualitative analysis can be performed by checking in the fault tree which basic events and paths lead to the occurence of the top event. On the other hand, the quantitative analysis is applied when it is possible to determine the probability of the top event to occur because of the probabilities of the basic events. The diagram permits us to visualize the fault sequences which must happen in order to the top event to occur. After the building of the fault tree, it is possible to insert the probabilities of each represented event to occur. In this way, it is possible to calculate the probability of the top event to occur.

3.2 Block Diagram Proposal

Figure 3 presents the suggested block diagram for a protection system in a nuclear plant. The blocks to the left of the dotted line are directly linked to the security function, while the ones to the right are used for audits and interface with the operator in the form of alarms and indications. Each block that comprises the diagram presented in figure 3 will be described below.

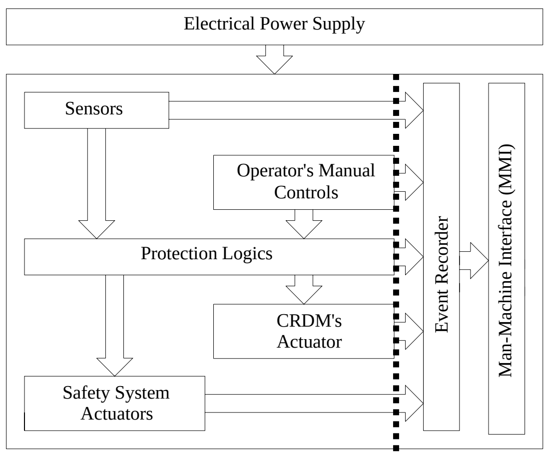

Fig. 3. Block Diagram Proposal of the Protection System.

3.2.1 Electrical Power Supply

It is the common component to all other system blocks, responsible for the supply of electrical energy. This block is normally comprised of more than one source of electrical energy, such as energy produced by the plant itself, batteries, diesel-generators and, whenever available, the electrical wiring of the energy supplier company, originated from other type of generating source (hydroelectric, or thermal powers, for instance).

3.2.2 Sensors

The sensor is an equipment that responds to a certain physical phenomenon and conveys this response to another component of the system that will apply it to control a process. In the case of the protection system, the main used sensors are to measure temperature, pressure, level, voltage, neutron flow (or neutron detectors) and radioactivity. According to the values given by the sensors and operator manual controls, the system protection processes the protection logics. This fact reveals the fundamental relevance of those components without which it is not possible to operate or manage the power plant in a safe way.

3.2.3 Operator's Manual Controls

These are the controls originated by the nuclear power plant operator. The manual command of turning off the reactor due to any abnormal condition recognized by the plant operator has the highest priority over any automatic action of the protection system, because it cuts off the power supply to the CRDM'actuator (Actuator of the Control Rod Drive Mechanism) which, as a result, shuts the reactor down through the fall of the control rods into the reactor core (Glasstone, 1994). In case of operator omission, the protection system starts to operate when an abnormal condition is detected.

The increase of the reactor power occurs gradually since its initial cold condition until the nominal power of operation, usually called the start-up procedure. During this procedure, the operator generates the range change controls for the detection of the neutron flow according to the plant operation conditions (neutron flow, temperature and pressure); such ideal conditions are guaranteed to be within the safaty limits by the protection system. If any limit condition is exceeded, the protection system shuts the reactor down and, at the same time, starts the safety systems necessary to remove the residual heat and sustain the reactor integrity.

3.2.4 Protection Logics

At this block, system decisions are made in conformity with the inputs originated from the sensors and the operator manual controls. The protection logics are intended to guarantee that the plant operation safety boundaries are not exceeded.
Below are listed the protection logics which lead to the scram of water-cooled reactors (Glasstone, 1994) and/or the activation of safety systems:

- Quick increment of the neutron flow during the start of the reactor;
- High flow of neutrons at the range power, indicating over power;
- Abnormal pressure and temperature;
- Loss of coolant water;
- Damage of the steam line;
- High level of water in the pressurizer in PWR;
- Low level of water in the BWR reactor vessels ("BWR – Boiling Water Reactor");
- Low level of water in the steam generator in PWR;
- High level of radiation in the steam; and
- Low voltage or power loss (safety buses).

3.2.5 Actuator of the Control Rod Drive Mechanism

The actuator of the Control Rod Drive Mechanism is the main component for reactor control and scram. This component enables to remove or to insert the control and safety rods (rods that absorb radiation) in the interior of the nucleus, increasing or decreasing, respectively the nuclear power (McCormick, 1981). This device has a solenoid that, when it is turned off, makes possible the abrupt fall of the rods inside the nucleus by action of the gravity and springs, what provokes the reactor shutdown. This shutdown form is fail-safe because the electric power failure the turns off the reactor.

For effect of plant control, the actuator position indicator is important because by manipulating the rods position, the nuclear power can be controlled. However, for the protection system, it will only be important the information of turned on or off actuator.

3.2.6 Safety System Actuators

When the protection system identifies an abnormal situation, besides shutting the reactor down, it takes actions to assure the safety of the plant. The action of the protection system, when an abnormal situation is detected, consists of one or more of the following actions:

- Turns on diesel-generator to assure the power supply;
- Activates the Emergency Cooling System to assure the nucleus cooling and integrity. This system consists in injection of boron water through circulation pumps or nitrogen pressure;
- Isolates damaged steam line;
- Turns off circulation coolant pumps to minimize coolant loss, in the case of LOCA - Loss-of-coolant accident; and
- Isolates the containment (the place where the reactor is installed), avoiding the radioactive material release to the atmosphere.

3.2.7 Event Recorder

All of the blocks of the protection system are interconnected with the event recorder, where the information is stored during the operation of the plant. The recording of those information will make it possible to trace subsequently the reactor scram or the activation of safety system cause, since an appropriate physical media is employed (hard disk, magnetic storage, optical tape recorder, memory, etc), chosen in function of the hardware specification in the project.

3.2.8 Man-Machine Interface (MMI)

This block reads the data recorded by the event recorder and it introduces them to the operator in alarm or report form. The alarms will be used on-line during the operation of the plant and they are displayed in visual form and/or audible in the panel of the protection system, while the reports will be used later for evaluation and supervision of the system, as well as for finding out the causes of reactor scram or activation of safety systems, and they are displayed in printed form in agreement with the information requested by the user.

4. CONCLUSION

Starting from the reliability level required to the protection system that the project is aimed at, having the tools such as the fault tree or Markov model, and also after the detailing of the block diagram, the study will seek to establish the necessary redundancy for the components of the protection system.

The components of the protection system connected to the safety function are of the 1E class (IEEE Std 603, 1998). This classification is given to equipments or safety systems that are essential for the scram of the nuclear reactor, insulation of the containment and the cooling of the reactor, in order to avoid radioactive matter emission to the environment.

Although digital electronics has evolved over the years, there is still prudence in using different kinds of software in safety systems. As an illustration, digital protection was not considered to be used in China before the year 1990. The first digital system of the kind only appeared in 2002 for a 10 MW reactor (Li, F.; Yang, Z.; An, Z.; Zhang, L, 2002).

The great challenge for the safety system project designer will be to detail each component of the block diagram proposal, organize ways to test the integrated system and guarantee the reliability. The expectation is to employ this work in the development of the safety system at LABGENE in the future.

REFERENCES

Chairman, John G. Kemeny at all. *Report of The President's Commission on The Accident at Three Mile Island (TMI).* Washington, DC. 1979.

Edwards, M. Chernobyl-One Year After. National Geographic, May 1987.

Glasstone, Samuel; Sensonske, Alexandre. *Nuclear Reactor Engineering: Reactor Systems Engineering.* 4th ed. New York: Chapman & Hall, 1994. v.2.

IEEE Std 603-1998. *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.* New York: Institute of Electrical and Electronics Engineers. 1998.

INFOREL – Relações Internacionais, Notícia e Informação. Brasília. *Interview with the Brazilian Navy Minister in December 10, 2004.* Available at: <http://www.inforel.org>. Access in February 3, 2005.

Li, F.; Yang, Z.; An, Z.; Zhang, L. (2002). *The first digital reactor protection system in China.* Nuclear Engineering and Design, n. 218, p. 215–225.

McCormick, Norman J. *Reliability and Risk Analysis – Methods and Nuclear Power Applications.* Department of Nuclear Engineering – University of Washington Seattle, Washington. California: ACADEMIC PRESS, 1981. 446p.

Nuclear Plants around The World. Available at: <http://www.nucleartourist.com/ >. Access in February 21, 2005.

Nuclear Reactors. *U. S. Nuclear Regulatory Commission – Pressurized Water Reactors.* Available at: <http:// www.nrc. gov/ reactors/ pwrs.html>. Access in May 22, 2005.