IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 00-00
www.iosrjournals.org

Embedded System on Safety Critical For Nuclear Power Plant

Sabarisan.V ,Prabhu.R ,Krishnaprasad.V
[1](Eee, Sns College Of Technology/Annauniversity,India

Abstract: ***Safety-critical systems*** *are embedded systems that could cause injury or loss of human life if they fail or encounter errors. Flight-control systems, automotive drive-by-wire,* ***nuclear reactor management****, or operating room heart/lung bypass machines naturally come to mind. Small system defects or situations can cascade into life-threatening failures very quickly.A low-level failure in some small part of a system can be viewed as a fault at another level, which can lead to errors at that level that can trigger failures that can turns out to as fault at a higher level. If these faults are allowed to "avalanche" to system-level failures, they can lead to hazards that have the potential to threaten injury or loss of life. For safety-critical systems, a thorough* ***hazard analysis*** *and* ***risk analysis*** *must also be done. Only then can architectural design get started. In this paper, the selection of safety-critical system architecture is discussed by reviewing a rigorous hazard analysis followed by risk analysis, in addition to conventional system requirements definition. System design may include combinations of redundant sensor configurations, shutdown systems, actuation monitoring, multiple channel architectures, and/or monitor-actuator structuring. Their true value is in protecting and saving human lives. Also a brief study of* ***Fukushima incident in Japan*** *and* ***safety features in Koodankulam Nuclear Power Plant*** *based on safety critical system is dealt in this paper.*

Keywords: *Nuclear Fission,Nuclear Fusion,Nuclear Reactor Management*

I. Introduction

Nuclear energy is the energy in the nucleus (core) of an atom. Nuclear energy can be used to make electricity. But first the energy must be released. It can be released from atoms in two ways: **nuclear fusion** and **nuclear fission**. In nuclear fusion, energy is released when atoms are combined or fused together to form a larger atom. This is how the sun produces energy. In nuclear fission, atoms are split apart to form smaller atoms, releasing energy. Nuclear power plants use nuclear fission to produce electricity.

Nuclear power plants are very clean and efficient to operate. However, nuclear power plants have some major **environmental risks**. Nuclear power plants produce **radioactive gases**. These gases are to be contained in the operation of the plant. If these gases are released into the air, major health risks can occur. Nuclear plants use uranium as a fuel to produce power. The **mining and handling of uranium is very risky** and radiation leaks can occur. The third concern of nuclear power is the permanent storage of spent radioactive fuel. This **fuel is toxic** for centuries, handling and disposal is an ongoing environmental issue.

1. Operation Of Nuclear Power Plant

An atom's nucleus can be split apart. When this is done, a tremendous amount of energy is released. The energy is both heat and light energy. This energy, when let out slowly, can be harnessed to generate electricity. Uranium atoms inside a nuclear reactor are split apart in a controlled chain reaction. In a chain reaction, particles released by the splitting of the atom go off and strike other uranium atoms splitting those. The process is continuous and hence it is called a **chain reaction**. In nuclear power plants, control rods are used to keep the splitting regulated so it doesn't go too fast. If the reaction is not controlled, you could have an explosion. The chain reaction also creates radioactive material. This material could hurt people if released, so it is kept in a solid form.

The chain reaction gives off heat energy. This heat energy is used to boil water in the core of the reactor. So, instead of burning a fuel, nuclear power plants use the chain reaction of atoms splitting to change the energy of atoms into heat energy. This water from around the nuclear core is sent to another section of the power plant. Here it heats another set of pipes filled with water to make steam. The steam in this second set of pipes powers a turbine to generate electricity.

1.1 NUCLEAR ACCIDENTS

Nuclear power stations produce unusual amount of heat by means of nuclear reactions of Uranium fuel particles bundled in packets and placed in reactor core where neutrons bombard the fuel and thereby abnormal

heat and new radioactive particles which damage living tissues are produced. If the nuclear fuel gets overheated and the packed radioactive particles are blown into the air the surrounding areas including the air, water, soil get highly poisoned and the cost of such an accident will be very high. Hence it is necessary to have a safety critical system to eradicate such problems.

1.2 Three Mile Island Incident

Three Mile Island-The TMI-2 accidents involved a **small leak of water from the reactor** system that wasn't correctly diagnosed. Inadequate control room instrumentation and emergency response training proved to be root causes of the operators' inability to respond properly to an unplanned automatic shutdown of the reactor at 4:00 am on 28 March 1979. So, safe operation in Nuclear Power Plant is the need of all time.

II. Architectures For Nuclear Power Plant

For many safety-critical systems, such as Nuclear Power Plant the safe state is to immediately stop and turn the system off. For other safety-critical systems, no safe state exists. For these systems, stopping is simply not an option. These systems must not stop or turn themselves off when a hazard is detected; their embedded services must instead continue to be available while failures and hazards are present. Fig. 1 illustrates the relationship between safety-critical and high-availability systems with regard to hazards and safe states.

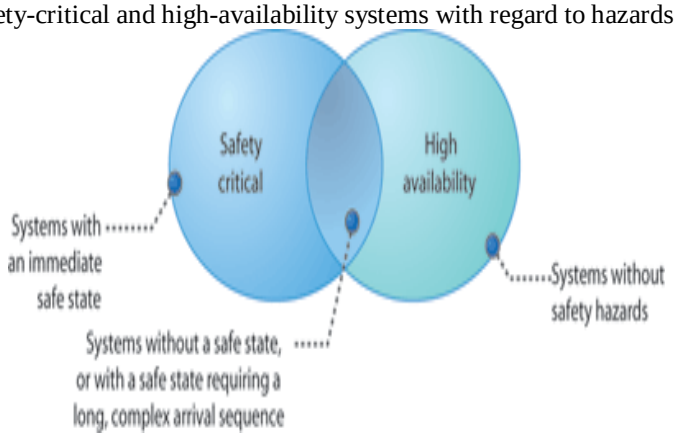


Fig.1: Safety-critical vs. high-availability systems

In this Venn diagram, safety-critical systems would fall into the leftmost section, while controllers fall into the center section where safety-critical and high-availability systems overlap. The rightmost section of the diagram is for high-availability systems that are not safety-related, such as online banking, stock exchanges, and business-critical websites.

III. Step-By-Step Approach [Hazard Analysis & Risk Analysis]

The objective of **hazard analysis** is to systematically identify the dangers to human safety that a system may pose, including an evaluation of the likelihood of an accident resulting from each hazard. A popular technique for doing hazard analysis is called **fault tree analysis**. It takes a top-down hierarchical decomposition approach decomposing undesired system events in order to identify which combinations of hardware, software, human, or other errors could cause safety-threatening hazards.

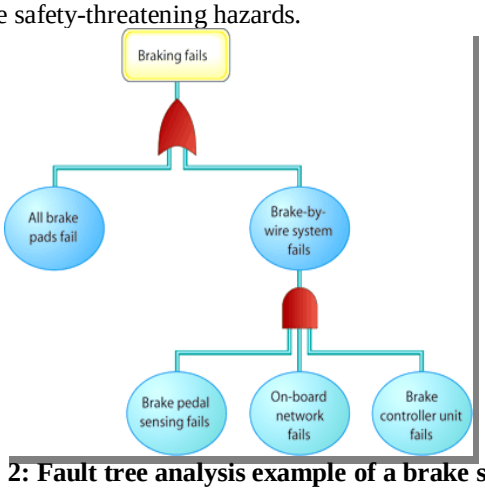


Figure 2: Fault tree analysis example of a brake system

A fault tree analysis begins at the three (or six or seven) most life-threatening things the system could conceivably do. Each safety threat come up which will become the top node of its own fault tree as shown in Figure 2. Then the other sorts of things could cause this to happen. It will be shown as the first level of decomposition of the fault tree. Then the other sorts of things could cause each of these to happen. It will become the next level of the fault tree; and so on. After hazard analysis, the next step is **risk analysis**. Risk is the combination of the probability of an undesired event occurring and the severity of its consequences. This can often be done using:

- hardware overrides to bypass risky software components
- lockouts to prevent entry into risky states
- lockins to ensure remaining within safe states
- Interlocks to constrain sequences of events in order to avoid hazards.

If it's not possible to totally avoid or remove the hazards, the risk of accident must be minimized; if an accident does occur the risk of loss of life must be minimized.
Together with the system requirements, the results of the hazard analysis and risk analysis will guide a safety-critical system's architectural design.

3.1 Detecting sensor errors using redundancy approach:

Correct sensor data are so crucial to safe operation that many systems use redundancy in their sensor data acquisition. Redundancy doesn't always mean sensor replication as shown in Fig. 3 with two identical sensors. It could also mean functional redundancy or the measurement of the same real-world value in two different ways.

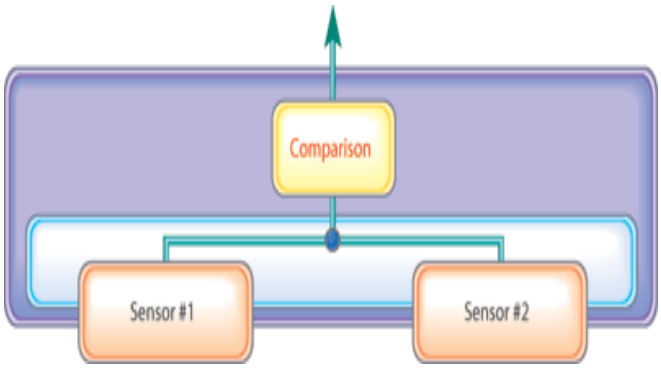


Fig. 3: Sensor-input comparison

Redundancy as analytic redundancy, which is the comparison of a measured value with a value derived in some other way, as shown in Fig. 4.

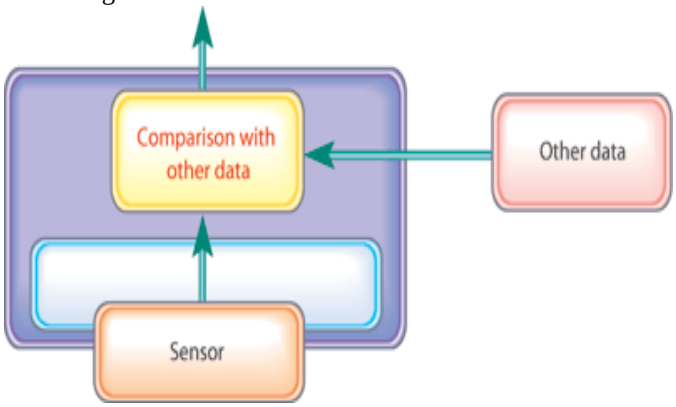


Fig. 4: Analytic redundancy: comparison with other data

If the calculated and measured values agree pretty closely implies that the sensor is working correctly. But to know which sensor is wrong, it's often best to just shut down the entire redundant pair in what's called a fail-stop. An alternative approach is to add a third redundant element and to replace the two-way comparison with **three-way "voting."** Three-way voting in a strictly replication-based design such as Fig. 4, the result is called **triple modular redundancy (TMR).** But this could also be done in a mix-and-match sort of way,

resulting in a combination of several kinds of redundancy. In the various triple redundancy approaches, a faulty sensor can be identified and shut down while the remaining redundant elements can continue to operate safely.

IV. Shutdown Systems:

If a safety-critical system has an immediate safe state, a shutdown system can be used to terminate a hazardous situation as soon it detects it. The basic shutdown architecture is illustrated in Fig. 5.

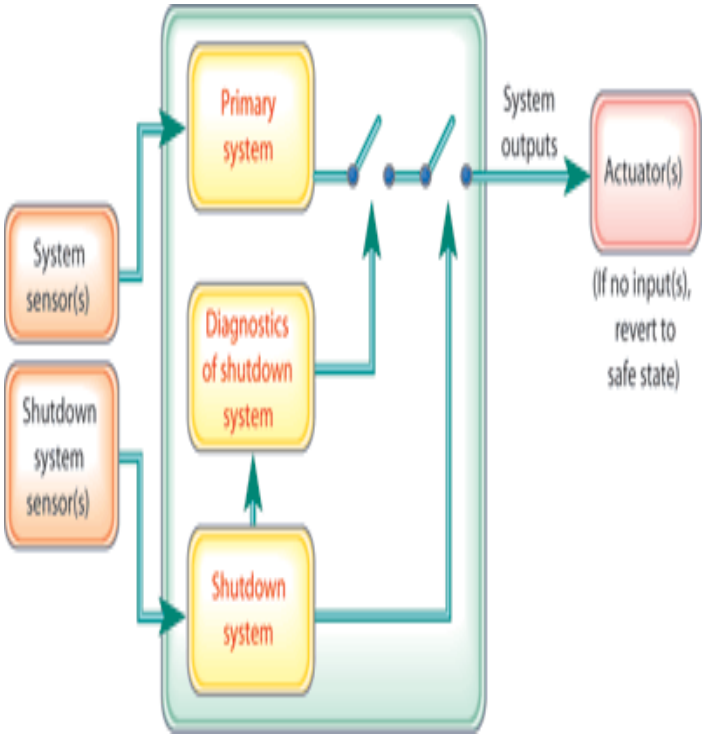


Fig. 5: Basic shutdown architecture

The shutdown system is a dedicated unit with responsibility for identifying dangerous situations. It will force the entire system into a safe state (in other words, off) whenever a hazard is detected and thus lock the system out of a life-threatening state. The shutdown system is independent of the primary system that is normally in control, and operates in parallel with it. To ensure its complete independence, the shutdown system has its own separate sensor(s).

4.1 Safe Shutdown Earthquake Condition:

The NRC defines the Safe Shutdown Earthquake as the maximum earthquake in which certain structures, systems, and components, important to safety, must remain functional. Under an "operating basis earthquake," the reactor could continue operation without undue risk to the safety of the public. Ground motion at any specific location, such as a nuclear plant site, depends on the earthquake source, magnitude, distance to the source, and the attenuation (dampening) caused by rock and soil characteristics. A nuclear power plant responds to an earthquake depending on how its individual structures, systems, and components resonate, or vibrate, with the ground shaking. Heavier and more massive structures resonate at lower frequencies, while light components resonate at higher frequencies.

During an earthquake, ground motion transmits vibrations to a nuclear power plant's foundation and structure. The vibrations cause back-and-forth acceleration of a structure, system or components that is measured relative to the earth's gravitational acceleration constant (g). Both vertical and horizontal components of ground acceleration place loads, or stresses, on a nuclear power plant's structure. Peak Ground Acceleration (PGA) is a measure that has been widely used in developing nuclear power plant "fragility estimates," which represent the sensitivity of nuclear plant structures, systems, and components (SSCs) to the inertial effects of acceleration during ground shaking.

4.2 BWR (Boiler Water Reactor) Safe Shutdown Condition:

During normal operation, reactor cooling relies on the water that enters the reactor vessel and the generated steam that exits. During safe shutdown, after the fission process is halted, the reactor core continues to

generate heat by radioactive decay and generates steam. The heat from this radioactive decay initially equals about 6% of the heat produced by the reactor at full power and gradually declines. Under this condition, the steam bypasses the turbine and diverts directly to the condenser to cool the reactor. When the reactor vessel pressure decreases to approximately 50 psi, the shutdown-cooling mode removes residual heat by pumping water from the reactor recirculation loop through a heat exchanger and back to the reactor via the recirculation loop. The recirculation loop design limits the number of pipes that penetrate the reactor vessel.

4.3 PWR (Pressurized Water Reactor) Safe Shutdown Condition:

During normal operation, a PWR does not generate steam directly. For cooling, it transfers heat via the reactor primary coolant to a secondary coolant in the steam generators. There, the secondary coolant water is boiled into steam and sent to the main turbine to generate electricity.

Even after shutdown (when the moderated uranium fission is halted), the reactor continues to produce a significant amount of heat from decay of uranium fission products (decay heat). The decay heat is sufficient to cause fuel damage if the core cooling is inadequate. Auxiliary feed water systems and the steam dump systems work together to remove the decay heat from the reactor. If a system for dumping built-up steam is not available or inoperative, atmospheric relief valves can dump the steam directly to the atmosphere. Under normal operating conditions, water flowing through the secondary system does not contact the reactor core; dumped-steam does not present a radiological release.

In fact, some safety-critical systems have **dual shutdown systems** working in parallel (with either "AND" or "OR" logic for deciding when to shut down the primary). In extreme instances, a safety-critical system can be designed with three shutdown systems working in parallel using **TMR-style voting** among them. The idea of shutdown monitoring can also be extended to the output side of a system. This is called **actuation monitoring.**

4.4 DUAL-CHANNEL ARCHITECTURES:

For safety-critical systems without an immediate safe state, dual-channel architectures can be used to allow a system to continue operation even when one of its channels has "fail stopped."

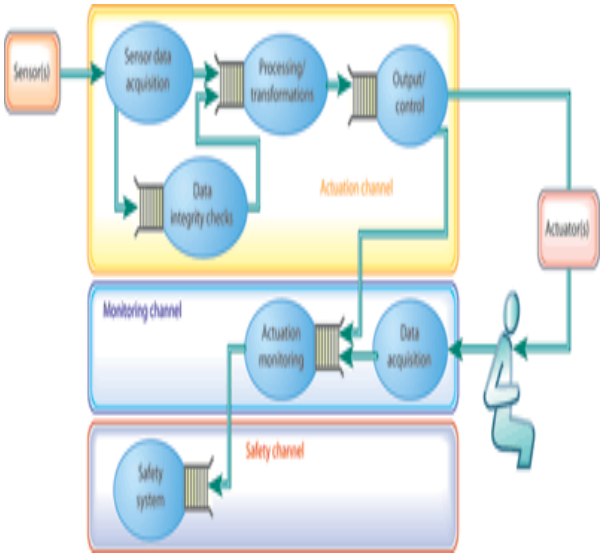
In dual-channel architecture one of the channels serves as the **primary or active channel** and the other is a **standby or backup channel**, ready to take over system operation if the current primary channel suffers faults or failure. Depending on the needs of the specific safety-critical system, the standby channel when becoming active could either continue normal operation of the system or it could take the system through a possibly long and complex sequence of steps to bring it to its eventual safe state

In a nuclear reactor control system, in cases of failure of one of its internal embedded processing channels, would be expected to stay in operation long enough to shut down the reactor by proceeding through a lengthy sequence of activities: stepping the graphite moderator rods down into the full depth of the reactor core while accelerating the flow of coolant through the reactor, and monitoring the gradual slowdown of the nuclear reaction through myriad sensors—until the reactor can be declared safe for human access.

Dual-channel architecture is going to have **higher unit costs** than previous architectures we've discussed. Dual-channel architecture has a number of popular variants. If the two channels use the same replicated software and hardware, the architecture can handle random faults well but it can't handle systematic faults such as software design or coding defects that would be reproduced in both channels. If this is of concern in your system, heterogeneous dual-channel architecture is preferable. Development costs as well as the unit cost for doing this would be high. Another variant of the dual-channel architecture is multi-channel voting architecture. This extends the TMR approach discussed earlier for sensor error detection into the realm of entire replicated processing channels. In this architecture, three (or more) channels operate in parallel. A "voter" compares the outputs of the channels: if a majority of channel outputs agree, this will become the system's output. If some channels disagree, they will be fail-stopped.

V. Monitor-Actuator Architecture:

Many safety-critical systems do not have an immediate safe state, but can't incur the high costs of a full dual-channel or multiple-channel architecture. A lower-cost compromise solution is the monitor-actuator architecture shown in Fig.



Monitor-actuator architecture

This architecture doesn't have replicated identical channels, but instead has heterogeneous channels that differ from one another. It has a **single primary actuation channel** that normally controls the system, shown in the upper portion of Figure. The operation and results of this channel are examined by a **separate simpler monitoring channel** shown below it. If the monitoring channel detects a fault in the actuation channel, normal operation of the actuation channel can't continue. Instead, control of the system is passed to a separate safety channel shown at the bottom of the figure, which has responsibility for bringing the system to a safe state. Depending on the needs of the specific safety-critical system, the safety channel could take the system through a possibly long and complex sequence of steps to bring it to its eventual safe state.

The selection of safety-critical system architecture is driven by a rigorous hazard analysis followed by risk analysis, in addition to conventional system requirements definition. System design may include combinations of redundant sensor configurations, shutdown systems, actuation monitoring, multiple channel architectures, and/or monitor-actuator structuring. These embedded systems architectures are much more valuable than can be measured in dollars and cents. Their true value is in protecting and saving human lives.

VI. Fukushima incident in Japan

(A detailed study based on safety critical systems):

The **Fukushima Dai-Ichi Nuclear Power** Station is located in the towns of Futaba and Ohkuma, 250km north of Tokyo city in Japan. The plants at Fukushima are **Boiling Water Reactors (BWR)**. A BWR produces electricity by boiling water, and spinning a turbine with that steam.

The **earthquake** that hit Japan was several times **more powerful** than the worst earthquake the nuclear power plant was built for.The power plant survived the earthquake and was **shut down**. **(**Limits are set on the levels of velocity, acceleration and displacement in every power plant. The plant stopped functioning when the limits exceeded. Atomic reaction thus stopped.) Within seconds after the earthquake started, the control rods had been inserted into the core and the nuclear chain reaction stopped (**Basic Shutdown Architecture**).

The earthquake destroyed the external power supply of the nuclear reactor. The reactor and its backup systems are designed to handle this type of accident by including **backup power systems** to keep the coolant pumps working. Furthermore, since the power plant had been shut down, it cannot produce any electricity by itself.

(**Multi channel Architecture**) For the first hour, the first set of multiple emergency diesel power generators started and provided the electricity that was needed. However, when the **tsunami** arrived (a very rare and larger than anticipated tsunami) it flooded the diesel generators, causing them to fail.

When the **diesel generators failed** after the tsunami, the reactor operators switched to emergency battery power. The batteries were designed as one of the **backup systems** to provide power for cooling the core for 8 hours. And they did. After 8 hours, the batteries ran out, and the residual heat could not be carried away any more.

To protect the integrity of the vessel and containment, the operators started **venting steam** from time to time to control the pressure. Hence, steam and other gases are vented. Some of these gases are radioactive fission products, but they exist in small quantities. Therefore, when the operators started venting the system, some radioactive gases were released to the environment in a controlled manner (i.e., in small quantities through filters and scrubbers). While some of these gases are radioactive, they did not pose a significant risk to public safety to even the workers on site.

6.2 KOODANKULAM NUCLEAR POWER PLANT (A general study of its safety features):

Koodankulam Nuclear Power Plant is a nuclear power station currently under construction in Koodankulam in the Tirunelveli district of the southern Indian state of Tamil Nadu.

The reactors have some advanced safety features like **passive heat removal system, double containment, Core Catcher, and hydrogen re-combiner** instead of conventional systems. These reactors belong to the **Generation 3 + category** (with more safety features than Generation 3) with a simpler and standardized design.

The Koodankulam site is located in the lowest seismic hazard zone in the country. The water level experienced at the site due to the December 26, 2004 tsunami, triggered by a 9.2 earthquake was 2.2 metres above the mean sea level. The safety-related buildings are located at higher elevation (**Safety Diesel Generators, 9.3 metre**) and belong to the highest seismic category and are closed with double sealed, water leak tight doors. It has a **safe shutdown system** in case of earthquake.

(**Dual channel Architecture**) Besides fast acting control rods, the reactors also have a "**quick boron injection system**", serving as a back-up to inject concentrated boric acid into the reactor coolant circuit in an emergency. Boron is an excellent neutron absorber.

Its **Passive Heat Removal System (PHRS)** is capable of removing decay heat of reactor core to the outside atmosphere, during Station Black Out (SBO) condition lasting up to 24 hours. It can maintain hot shutdown condition of the reactor, thus, delaying the need for boron injection.

The reactor has **double containment**, inner 1.2 metre-thick concrete wall lined on the inside with a 6 mm layer of steel and an outer 60 cm thick concrete wall. The annulus between the walls is kept at negative pressure so that if any radioactivity is released it cannot go out. Air carrying such activity will have to pass through filters before getting released through the stack. Multiple barriers and systems ensure that radioactivity is not released into the environment.

The reactors are equipped **with passive hydrogen recombiner's** to avoid formation of explosive mixtures .The reactors have a reliable **Emergency Core Cooling System (ECCS).**

VII. Conclusion:

In this paper, possible architectural approach towards safety operation of Nuclear Power Plant is dealt, which would be crucial for all similar life critical applications. The most vital deployment of any technological innovation should always aim for life saving application. So, the Embedded based architecture for safety critical application especially for Nuclear Power Plant will be a boon to mankind.

References:

[1]. Storey, N. Safety-Critical Computer Systems. Harlow, UK: Addison-Wesley, 1996.
[2]. Douglas, B. P. Real-Time Design Patterns. Boston, MA: Addison-Wesley, 2003.
[3]. Dunn, W. R. Practical Design of Safety-Critical Computer Systems. Solvang, CA: Reliability Press, 2002.
[4]. Fukushima Nuclear Accident – a simple and accurate explanation @ BraveNewClimate.com