

CONTROL

PROMOTING EXCELLENCE IN PROCESS AUTOMATION CONTROLGLOBAL.COM



Béla Lipták on safety: Cyber security and nuclear power

“The weapons of wars of terror will not be limited to biological weapons and dirty nuclear bombs, but will also include software viruses and worms that will wage cyber warfare in attacking our infrastructure and industry, including our nuclear power plants,” says Béla Lipták, process control guru and author of the “Instrument and Automation Engineers’ Handbook,” in the 2009 introduction to this anthology. “My goal with this series of articles is not to spread fear, but to describe the power of process control to protect us.”

Along with providing a deep understanding of the causes of accidents, including Three Mile Island, Chernobyl and Fukushima, this anthology describes reactor facility design, control and interlock configurations. Lipták then draws upon his considerable experience to detail strategies by which process control can protect nuclear plants both from common accidents and cyber attacks.



Nuclear plant security and cyber terrorism	3
Nuclear plant security and cyber terrorism - part 2	8
The Fukushima nuclear accident - part 1	13
Preventing nuclear accidents by automation - part 2	18
How automation can prevent nuclear accidents - part 3	23
Automation could have saved Fukushima - part 1	27
Automation could have prevented Fukushima - part 2	31
Automation and Fukushima - part 3	35
What caused the Three Mile Island accident?	43

Nuclear plant security and cyber terrorism

How to improve nuclear power plant security

By Béla Lipták

I've written about the critical role that process control will play in converting our energy economy from an exhaustible to an inexhaustible one. In this series of articles, I will write about the role our profession will play during the transition when the planet seems to be drifting toward energy wars. The weapons of these wars of terror will not be limited to biological weapons and "dirty" nuclear bombs, but will also include software viruses and worms that will wage cyber warfare in attacking our infrastructure and industry, including our nuclear power plants.

My goal with this series of articles is not to spread fear, but to describe the power of process control to protect us. In order to illustrate my point, I selected the nuclear power industry to show how this can be done. I made that selection, because I want to deal with specific cases and nuclear power plants are convenient to illustrate the weak links that exist in this area (Figure 1).

Later I will describe the causes of such accidents as Three Miles Island or Chernobyl . By the way, not too many people realize that some 11 Chernobyl-type nuclear power plant blocks are still in operation in Russia (at Kursk, Smolensk, Leningrad, etc.) and one was also operating until 2009 outside Russia (the Ignalina II block in Lithuania). I will also discuss the causes of over 100 nuclear accidents of the past, plus the design and control configurations including interlocks that are used today. I will also describe the strategies by which process

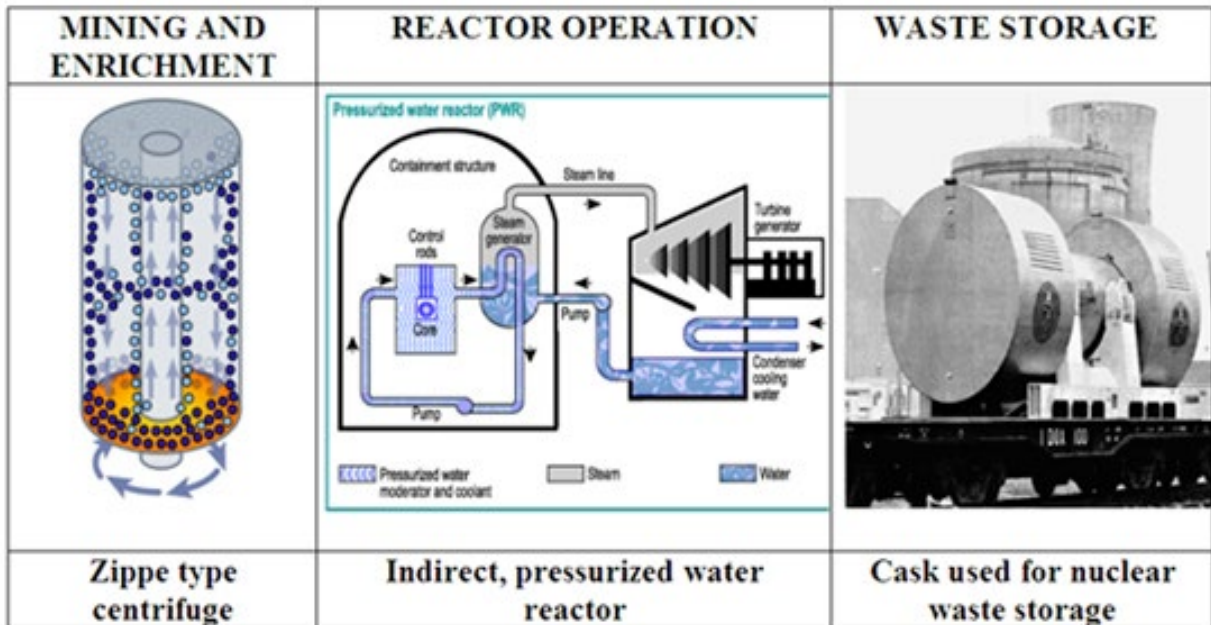


Figure 1: The three main process steps in the nuclear power cycle from mining to waste disposal

control can protect them from both the common accidents and cyber attacks.

While the targets of cyber attacks of the past also included other industrial targets, here I will concentrate on nuclear power plants and on their existing means of protection and on the changes needed to close the existing security loopholes. I will discuss the safety needs of all three processing operations: enrichment, power generation and waste disposal.

The grounds of Davis-Besse nuclear power plant in Ohio are patrolled by armed guards and are surrounded by a double row of tall fences which are monitored electronically, just as are all other nuclear power plants. Tall fences reduce the probability of

somebody driving a truck full of explosives into the plant. Yet, all of my readers know that fences do not protect against computer crashes, armed guards do not protect against viruses and software worms.

On Jan. 25, 2003 a Slammer worm penetrated the private computer network of Ohio's Davis-Besse nuclear power plant. The worm entered by first penetrating the unsecured network of a contractor and squirmed its way into the Davis-Besse corporate business network and because that network was connected to the plant's network, but bypassed its firewall, it spread to the plant network.

The following sequence followed. At 4 p.m. the operators noticed the slowing of the

Through a number of accidents we have learned that if an intruder worm tampers with the digital monitoring system (like in the case of Davis-Besse's SPDS and PPC), and if the operators are allowed to overrule the automatic safety interlocks, virus or worm attacks are possible.

plant network and at 4:50 p.m. the Safety Parameter Display System (SPDS) crashed. The SPDS monitors the operation of the coolant system, core temperature, radiation levels and other critical conditions. At 5:13 p.m. the Plant Process Computer (PPC) also crashed. Therefore, although the plant's network was protected by a firewall, both the plant's SPDS and PPC were disabled for about five hours. Fortunately at the time the plant was not in operation, because a hole in the reactor head was being repaired. Another reason why no harm was done is because the analog backups of the SPDS and the PPC could not be attacked by the worm.

We must remember that all our nuclear power plants are old and decades ago, the controls of all nuclear power plants were completely analog. There were no data highways and therefore the data transfer between the plants and corporate offices were secure from cyber attacks. Today, digital systems monitor the critical operating conditions (valve openings, pump status, temperatures, pressures, levels, radiation,

loading, etc.) of most nuclear plants, while they are still controlled by analog controls.

Through a number of accidents we have learned that if an intruder worm tampers with the digital monitoring system (like in the case of Davis-Besse's SPDS and PPC), and if the operators are allowed to overrule the automatic safety interlocks, virus or worm attacks are possible. We have also learned that the design and practices of the operator of the Davis-Besse plant (FirstEnergy) were apparently NOT in violation of NRC's cyber security regulations.

We also know that for financial reasons and because of management convenience, the whole nuclear industry is drifting toward installing completely digital controls to allow the remote operation of some plant functions. This trend could have disastrous consequences not only in newly built nuclear power plants, but also in refineries, chemical plants and throughout industry.

While in the above discussion I concentrated on the Davis-Besse accident, I

In order to improve nuclear plant security it is essential to realize both the need for totally separating the corporate business networks from the plant networks and to realize that digital firewalls do not guarantee this separation.

should note that this one Slammer attack has much wider implications. After this nationwide attack the National Security Telecommunications Advisory Committee concluded that the American electric grid as a whole is controlled by a “Byzantine network riddled by security holes, including unsecured SCADA systems and by unprotected connections between plant and company business networks.”

HOW TO IMPROVE NUCLEAR POWER PLANT SECURITY

In order to improve nuclear plant security it is essential to realize both the need for totally separating the corporate business networks from the plant networks and to realize that digital firewalls do not guarantee this separation. This separation must be absolute and software firewalls are not! Because the safety of the public is involved, the implementation of this separation cannot be left up to each plant owner or operator, but must be mandated by the NRC; otherwise the people living near nuclear power plants, (such as the residents of Long Island, N.Y.) can not feel safe.

Therefore, the NRC must totally forbid not

only the remote operation of nuclear plants, but also the linking of plant operations networks with corporate LANs (local area networks). The convenience and cost savings associated with these corporate links cannot justify the risk they cause to the public. This also means that the NRC should require total separation between the corporate networks of utilities and the SCADA networks of the plants. These SCADA networks control the remote terminal units (RTUs) sprinkled throughout the plants, directly monitoring and/or controlling the operation of power plant equipment.

As I will be discussing in more detail in the coming articles, the steps to be taken to guarantee plant safety and security are not limited to providing digital separation. For example, one must also guarantee both the reliability of the data reaching the operators AND must protect the plant from operator errors, which can be unintended OR INTENTIONAL. The 21st-century interpretation of Murphy’s law says that it is just as possible for an operator to smuggle a bomb into the control room as it is to smuggle in a software package.

Therefore, the protection in nuclear power plants must be served by both redundancy and automation. In addition, the redundancy should not be a simple backup, but a triple-redundancy voting system implemented for both the hardware and the software of the plant. This means that in all nuclear power plants, all critical measurements and status indicators would be made by three accurate sensors, and the control system would act on the “majority view” which would automatically schedule the “disagreeing sensor” for maintenance and recalibration. The same would apply to all software packages including SCADA, SPDS, PPC, etc. networks in the plant.

Similarly, in case of the digital systems and networks, as soon as one disagrees with the “majority view,” that one would be disabled and checked for virus or worm attacks.

In the area of protecting the plant from intentional or unintentional operator errors, I would provide hardwired interlocks on all critical safety systems and would configure the controls in such a way that the operators cannot bypass them or shut them down. In addition, I would set up a national review board that would not only train and check the background of operators, but would also arrange for the review of all existing process control loops in all 125 nuclear power plants to make sure that the conditions that have caused the

over 100 accidents of the past are not still present in any of them.

In the area of nuclear waste management, we know that each reactor produces 20 tons of nuclear waste per year, and this waste is locally stored, usually in steel casks at temporary waste sites. These casks can be penetrated by regular weapons and will release radioactive cesium gas. While these waste sites can be guarded 24 hours a day, the only safe solution would be to have a permanent waste repository. In the meanwhile, process control can much improve the security of these waste sites right now.

In addition to making the nuclear power plants more secure I would also require the NCR to use the tools of process control to improve the security of the uranium enrichment, transportation and waste storage (including military waste) in order to minimize the potential for theft. For obvious reasons, here I will not elaborate on the tools process control can provide to monitor and protect such sites, but just mention that it should be utilized if we want to protect societies around the globe from possible “dirty bomb” attacks.



Béla Lipták, PE, control consultant, is also editor of the “Instrument Engineers’ Handbook”

Nuclear plant security and cyber terrorism – part 2

The overall topic of the nuclear power plant operation and the use of process control to protect against nuclear accidents

By Béla Lipták

First we need to familiarize ourselves with the basics of the nuclear power generation process, because we can only control a process if we fully understand it!

HISTORY

In 1905, Albert Einstein identified the relationship between matter and energy as $e = mc^2$. In 1923, he received the Nobel Prize in physics for it. It took 103 years to prove his theory, but this year, he was finally proven right.

The concept of a nuclear reactor utilizing the chain reaction of fission was developed by the Hungarian-American scientist Leó Szilárd in 1933. He patented the process and later (1942) demonstrated it while working with a team of scientists headed by the Italian-American Enrico Fermi. This chain reaction was later used by the team of the German-American L. Robert Oppenheimer during the Manhattan Project in building the first atomic bombs.

Another way to release the energy of the atom was taken by the Hungarian-American scientist, the Hungarian-American Edward Teller in 1952, who proved that the fusion of hydrogen atoms can also be used to initiate a chain reaction. Teller also participated in the Manhattan Project and wanted to develop this weapon only to be used as a deterrent and later did all he could to prevent its use on civilian targets. In the last years of his life, he became convinced

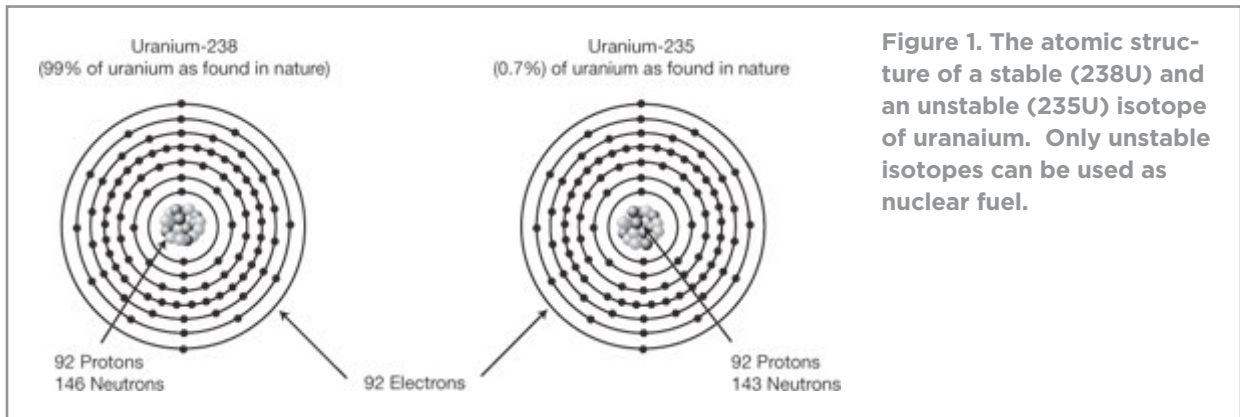


Figure 1. The atomic structure of a stable (^{238}U) and an unstable (^{235}U) isotope of uranium. Only unstable isotopes can be used as nuclear fuel.

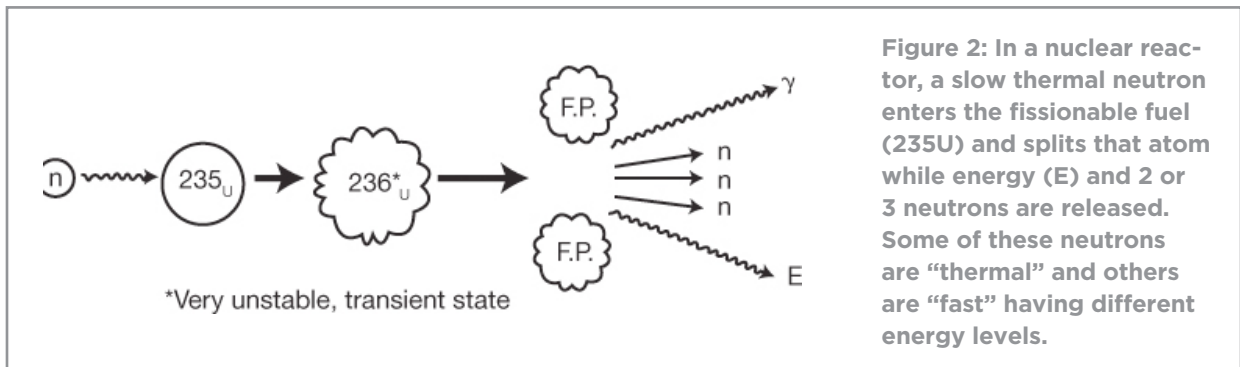


Figure 2: In a nuclear reactor, a slow thermal neutron enters the fissionable fuel (^{235}U) and splits that atom while energy (E) and 2 or 3 neutrons are released. Some of these neutrons are "thermal" and others are "fast" having different energy levels.

that nuclear weapons threaten human civilization and became one of the advocates of total nuclear disarmament. Teller also understood the great importance of process control and wrote the preface to the first edition of my Instrument Engineers' Handbook.

Here, as an energy source, I will not discuss this fusion process, (which occurs in the sun), because that process operates at millions of degrees temperature and, therefore, is unpractical on this planet. I will just mention that to date, controlled fusion has only been achieved in experimental devices although a large fusion reactor is under construction in France with international support.

UNDERSTANDING NUCLEAR FISSION

An atom is composed of a central nucleus consisting of protons, neutrons and other particles plus electrons orbiting in shells around the nucleus at discrete energy levels. These are referred to as electron shells. The proton has a positive charge equal to that of the electron and a mass which is a couple of thousand times greater. The neutron has no electric charge and has a mass similar to that of the proton. When basic particles combine to form an atom, a certain amount of mass is converted into the binding energy of the atom, which is needed to hold the nucleus together. As I noted earlier, Einstein defined this conversion by the equation $e = mc^2$,

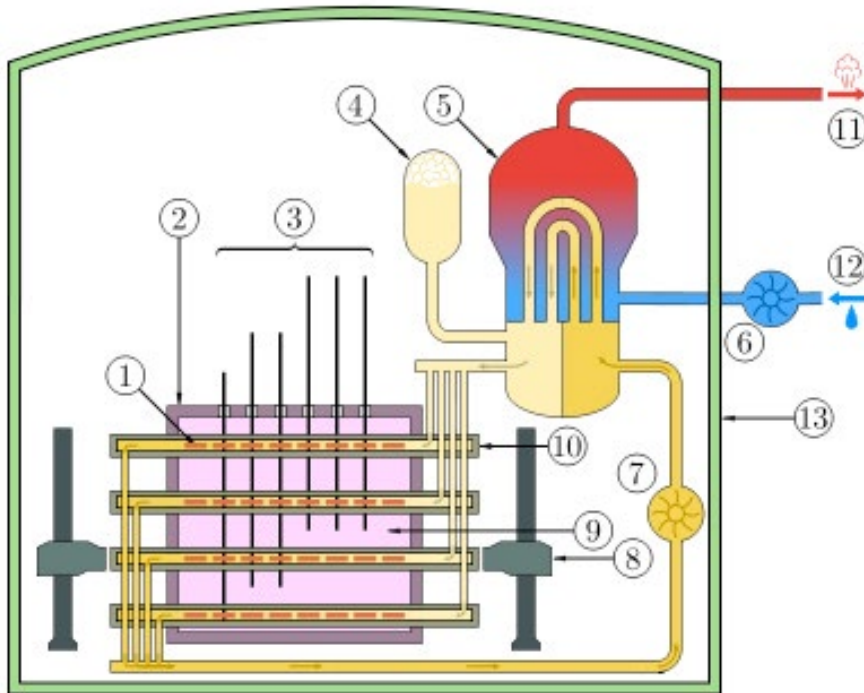


Figure 3: Schematic Diagram of a CANDU reactor: The primary loop is in yellow and orange, the secondary in blue and red. The cool heavy water in the calandria can be seen in pink, along with partially-inserted shutoff rods.

where e is the energy, m is the mass, and c is the velocity of light in a vacuum.

In chemical reactions, the changes occur in the electron shells. In nuclear fusion, the release of energy is caused by the change in the nuclei as atomic particles are fused together. In fission, mass is converted into energy and energy is released, because the atoms of isotopes are split. Fission events release more than 2 million times more energy per event than do chemical reactions.

Atoms are neutral when their number of electrons equals the number of protons within their nucleus. When the number of

electrons differs from the number of the protons, they have an electric charge and are called ions which can “chemically” combine with other ions of opposite charge.

Different elements have different numbers of protons (atomic numbers) in their nuclei and atoms of the same element can have different atomic masses because they may contain different numbers of neutrons. These are called isotopes (Figure 1). The stable isotopes have definite ratios of neutrons to protons in their nuclei (U-238), while unstable isotopes (U-235) do not. During fission, a heavier unstable nucleus splits into two or more lighter nuclei, while

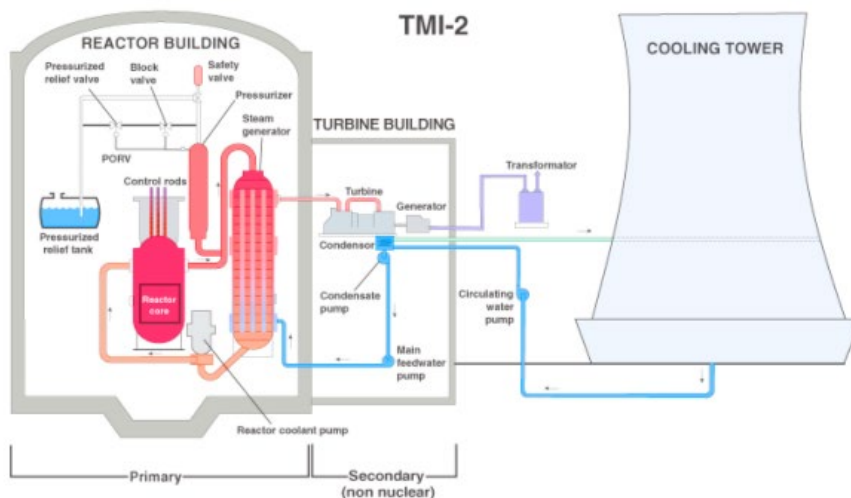
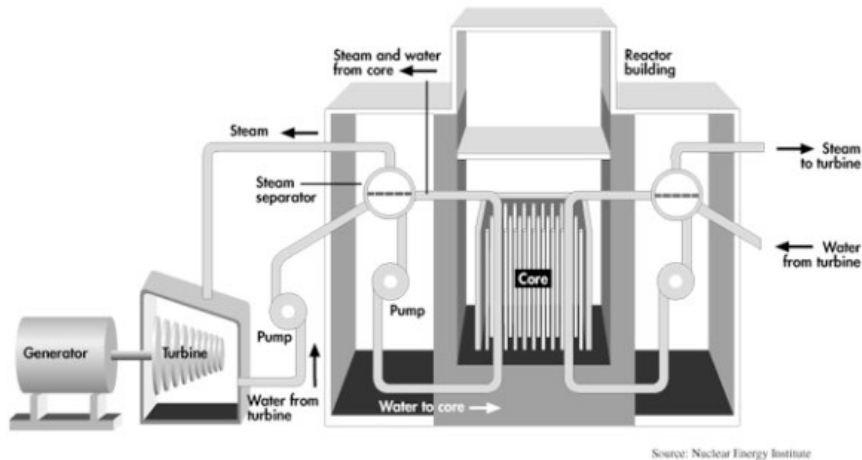


Figure 4: A schematic (top) and a more detailed view (bottom) of the reactor design which in 1986 at Chernobyl caused the most severe nuclear accident to date. The design is referred to as the RBMK (Reactor Bolohoj Moshosztjl Kanalnyj) reactor.

releasing a substantial amount of energy. Fissionable materials include the naturally occurring isotope ^{235}U and the man-made isotope ^{239}Pu . Fission is initiated when a free neutron of the proper energy (thermal neutron) is captured by the nucleus of a fissionable atom. The most common way of generating thermal neutrons is to allow neutrons from a source—reactor, accelerator or spontaneous fission neutron emitter—to dif-

fuse outward through a large block or tank of very weakly absorbing moderator. When the nucleus captures a thermal neutron, it will “split” producing two or more fission products (atoms of different elements formed from the protons, neutrons, and electrons originally comprising the original nucleus before its fission) plus two or three free neutrons and a tremendous amount of energy (Figure 2).

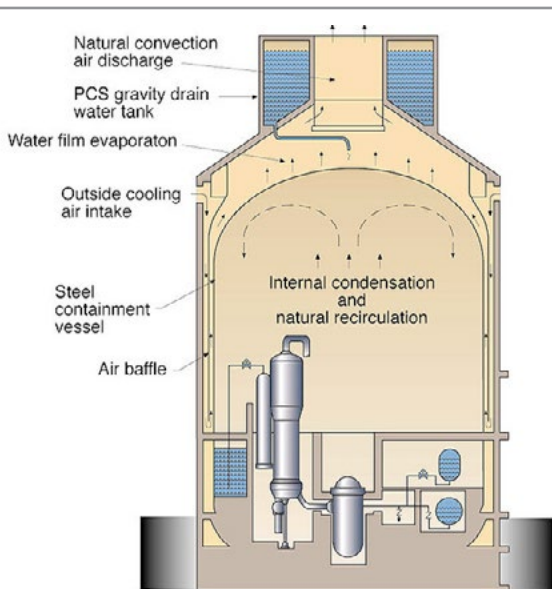


Figure 5: Diagram of AP600/AP1000 passive safety systems .

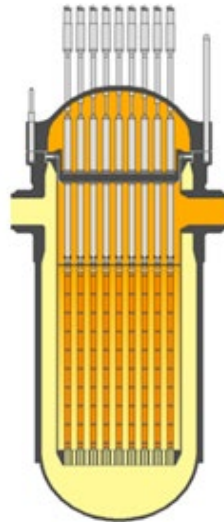


Figure 6: The French EPR design

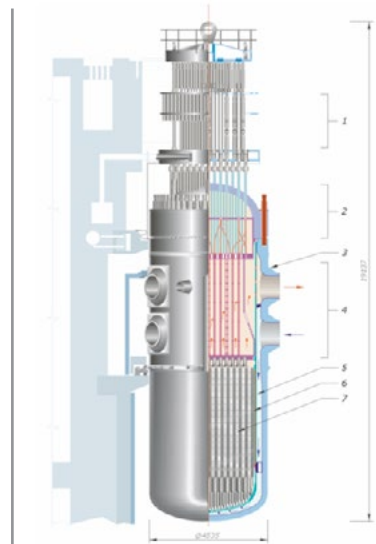


Figure 7: WWER-10ff (also VVER-1000 as a direct transliteration from Russian-1000). WWER-1000 (Water-Water Energetic Reactor, 1000 megawatt electric power) is a Russian nuclear power reactor of PWR type.

The emission of two or three free neutrons can split other unstable atoms (produce other fission events), which in turn will cause the emission of even more energy and more free neutrons. Within a few generations, the total amount of energy and the number of free neutrons can become tremendous, sufficient to cause a nuclear explosion. For sustained chain reaction, it is necessary to moderate the process, to capture the “fast neutrons” while utilizing the energy released by the neutrons in the thermal range.

REACTOR DESIGNS

Today, there are basically three more advanced nuclear power plant designs in use. One is the CANDU system developed in Canada using heavy water moderator tubes

(Figure 3). This design is similar to the Chernobyl RBMK design (Figure 4) only in that it uses pressure tubes instead of a pressure vessel, which facilitates on-line refueling, but otherwise it is much safer, because it contains much more cold heavy water. The General Electric design is a direct design (the moderator and the source of the steam to the turbine-generators is the same water). The third is the Westinghouse indirect design (Figure 5) (The high-pressure water in the reactor is the moderator and the coolant) in which the heat from the pressurized moderator water is used to boil the secondary water that is used to generate the steam for the turbines. This indirect Westinghouse AP1000 design is also the basis of the French EPR (Figure 6), and the Russian VVER1000 (Figure 7).

The Fukushima nuclear accident - part 1

Exploring the safety processes used at the Fukushima plant

By Béla Lipták

A few months ago, I described the safety controls that could have saved the 11 lives lost in the BP accident. In this series I will first describe the process used at the Fukushima plant; next I will show the safety controls that could have prevented this tragedy; finally, I will describe the steps that American nuclear power plants should take to protect against the repetition of such accidents, which can be triggered by earthquakes along active faults, hurricanes, terrorism, cyber terrorism or other unexpected events.

The regular nuclear power plants are not potential atomic bombs because the fuel is not concentrated sufficiently to explode like a bomb. The main difference between fission plants and fission bombs is that the plant releases the energy continuously, while the bomb releases it all at once. As of today, some 10,000 fission type nuclear weapons are in storage, and plans are to convert their plutonium into nuclear fuel. Some 440 nuclear power plants are in operation around the world (104 in the United States) generating some 7% of the global energy consumption and about 13% of the global electricity consumption.

Currently there are two breeder reactors in operation, one in Beloyarsk, Russia, and the other in Tsuruga, Japan. If in the future, breeder reactors are built, the risks will increase, because their product (plutonium with a half-life of 24,100 years) can be used directly to build bombs. Research is also in progress to build fusion plants, which operate at millions of degrees temperature and continuously release the same energy that hydrogen bombs release all at once.

Table 1: Radioactive products

Isotopes of	Radiation type	Half-life	Entry into body	Accumulates in
Iodine 131	Beta, gamma,	8 days	Inhalation, ingestion, wounds	Thyroid
Cesium 137	Beta, gamma	30 years	Inhalation, ingestion, wounds	Kidneys
Plutonium 239	Alpha	24,000 years	Inhalation (very toxic)	Lungs, bones, liver, testicles

The main concern with today's nuclear power plants is that in case of a meltdown they release radioactive isotopes (See table above). The safety record of the nuclear industry is good (about a dozen meltdowns occurred during its 50 years of existence). Based on that record, the probability of meltdowns globally is one per every two years.

With the exception of two small breeder reactors, one in Beloyarsk, Russia, and the other in Tsuruga, Japan, today only fission plants are in operation which cannot explode like atomic bombs, but they are still dangerous because they can release radioactive iodine, cesium or plutonium, which cause cancer if inhaled or ingested.

In case of a partial or complete meltdown, the produced plutonium can make the region uninhabitable for thousands of years. At Fukushima, the meltdown amounted to 75% of the core at one, 33% at another reactor and plutonium was found in the soil, but as of this writing, its source was not clearly established. (Ed. note: For current information on the status of the Fukushima reactors, go to the IAEA [website](#).)

THE FISSION PROCESS

The heart of a nuclear power plant is a high-pressure boiler similar to one burning coal, oil or gas. Yet there are major differences between them. One difference is that the fuel is located inside the reactors. The second difference is that this heat source cannot be turned off completely (by inserting the control rods and by stopping the recirculation pumps), but continues to release heat at a 5% rate for a long time. Therefore, continued cooling is required, even after the plant is shut down.

The third difference is that in a nuclear power plant, a serious accident will result if cooling is lost. Finally, the most important difference is that the waste produced in a nuclear reactor still contains some fuel (uranium in five of the six blocks and MOX in Block 3, which is uranium mixed with plutonium), which continues to generate heat practically forever and, therefore, without cooling, it could melt down. For this reason, nuclear waste would require safe and permanent storage, which was expected to be built a half century ago, but still does not exist. Consequently, the waste just accumulates and is overloading the temporary storage pools everywhere.

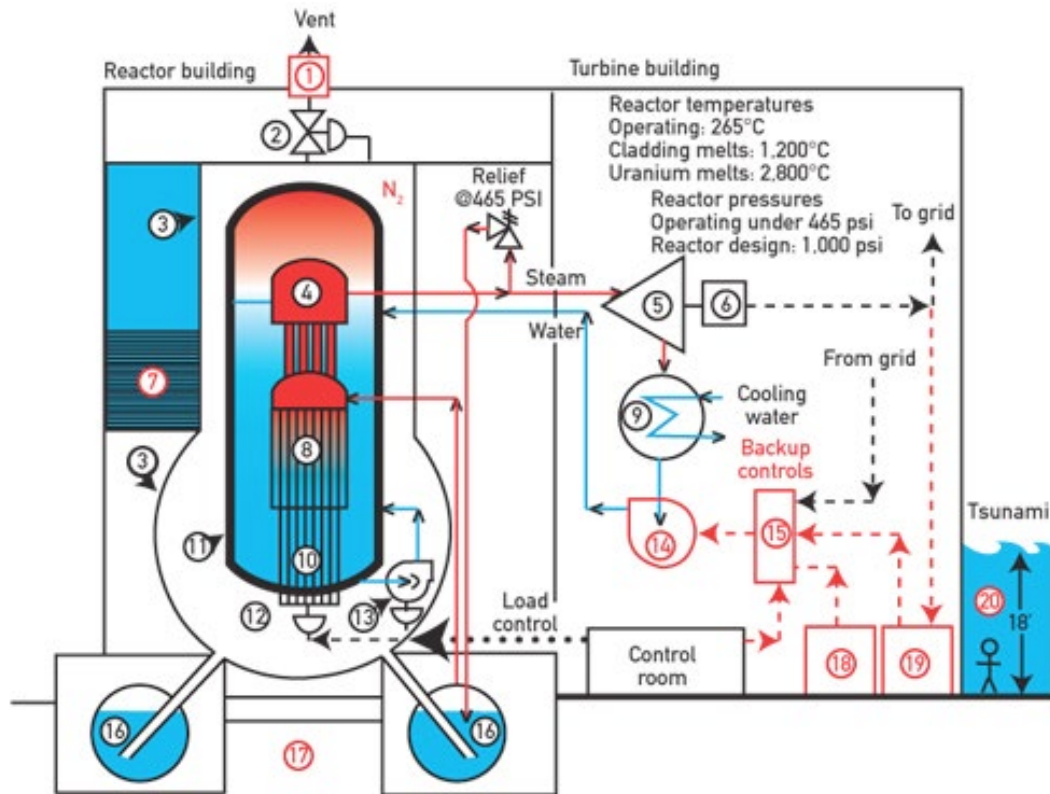


Figure 1: The main components of the Fukushima nuclear power plant (The components numbered in black were designed and operated correctly, the ones in red did not). 1-solids filter, 2-vent valve, 3-primary container or drywell, 4-steam separator & dryer, 5-turbines, 6-generators, 7-spent fuel rod

Although some argue that this is no worse than what the burning of fossil fuels causes because that waste also accumulates in the water and the air, causing more and more cancer, asthma or global warming. This is not so, because nuclear waste will still be with us even after we run out of uranium, while the consequences of fossil waste will slowly disappear after we run out of fossil fuels.

In a fission reaction under normal operation, a slow-moving neutron is absorbed by the nucleus of an uranium atom, which in turn splits into fast-moving lighter elements:
 $23592\text{U} + n = 23692\text{U} = 14456\text{Ba} + 8936\text{Kr} + 3n + 177 \text{ MeV},$

and releases three free neutrons and a steady supply of useful energy. This is different from a nuclear bomb, because that is designed to release all its energy at once. During an accident, as the temperature rises, the zirconium cladding (the material that covers the fuel rod) melts at 1200 °C and reacts with the water in the reactor:
 $\text{Zr} + 2\text{H}_2\text{O} = \text{ZrO}_2 + 2\text{H}_2.$

If this hydrogen comes in contact with oxygen, it can explode. This is what occurred in the Fukushima plant where due to the melt-down of fuel rods (both in the reactor core and in the spent fuel rod pools) hydrogen was generated. The hydrogen from the core

accumulated in the primary and from the spent fuel pools in the secondary containments, and since both had air in them (not inert gas), they exploded. As the temperature increased further, at 2800 the uranium in the fuel rods also melted releasing radioactive isotopes.

THE FAULTY DESIGN AT FUKUSHIMA

Figure 1 shows the design of the Fukushima plant's main components. The red numbers identify equipment and areas where the design was unsafe. One of the worst errors in all BWR designs around the world, including the American ones, is that the cooling water pumps could operate only at low pressures. Therefore, as the reactor temperature and the steam pressure increased, they could no longer pump the cooling water and first required the venting of the radioactive steam ("feed and bleed"). Also, in a properly designed plant, means would have been provided to lower the steam pressure by condensing the high pressure steam and return it with the feedwater.

Another major design deficiency common to most early reactors was that no piping was provided to pump water from the outside into the reactors or into the spent fuel rod ponds. This and the lack of elevated water storage provided with separate diesel generator operated pumps made it impossible to use mobile portable pumps, which should have been stored at the plant. Actually, neither stored fresh water, nor diesel

fuel or portable pumps were in storage at the plant. This made it necessary to dump sea water from helicopters and fire trucks.

The 140 tons of fuel rods (8) were in the reactors. The fuel rods were provided with four levels of protection: The first was the zirconium cladding on the fuel rods. The second was the wall of the reactor vessel (11). The third was the primary containment (3), and the fourth, the secondary containment, the reactor building itself. In case of the Fukushima plant, both the building and the primary containment were well-designed, as (to my knowledge) they were not damaged by either the earthquake nor by the 45-foot-high waves of the tsunami, which were still about 18 feet high (20) when they reached the plant.

POWER SUPPLY BACKUP

The earthquake destroyed the electric power supply of the plant (the connection to the grid) which by itself should not have been a serious problem, because backup diesel generators (18) were provided. It seems they failed because they were not elevated and the 18-foot waves of the tsunami reached and damaged them. The reason for their being installed at low elevation was probably both convenience and concern for their stability. The destruction of these generators could have occurred because water entered the diesel fuel tanks and sank to the bottom because water is heavier than the diesel fuel. As the engine takes its fuel supply from the bot-

tom of the tanks, water instead of oil reached it. It is also possible that the air intakes of the engines were not elevated and ended up under water. If either or both of these conditions existed, the engine could not operate.

The secondary battery backup (19) was of no use either because it was drastically undersized. It provided only about eight hours worth of electricity, while about ten times that would have been needed to supply the electricity needed for a safe shutdown. (It should be noted here that of the 104 American reactors, 93 are provided with only four-hour battery backups). Another problem in the Fukushima plant was the lack of automatic battery recharging. This could have been provided because the plant was still generating steam at a rate of about 5% of full capacity and, therefore, some of the turbine-generators could have been kept in operation.

No other backup was provided at the Fukushima plant. This is unfortunate, because electricity itself is not essential to cool the reactors. For example, if emergency cooling water tanks were provided on the roof, they would have made it possible to charge water just by gravity, and if those tanks were properly sized, the accident could have been prevented.

Similarly, in any plant where excess energy is present, that excess energy can be used directly to run the plant and its cooling systems. This could have been done by providing backup pumps with steam or Stirling type

heat drives. The design of the Fukushima plant did not provide for any of these options.

OTHER DESIGN DEFECTS

Probably the worst design defect was the under-sizing of the spent fuel rod storage pool. This was a universal practice 40 years ago, because everybody assumed that means for permanent storage would shortly be available, but that never occurred. Therefore, at the Fukushima plant 1760 tons of spent fuel rods were in the temporary storage pool (10 times the amount the pools were designed for), requiring continuous cooling to protect against a meltdown. The melting of these spent fuel rods outside the primary containment (3) also caused hydrogen explosions and release of radioactivity. The running out of space in the temporary storage pools is a common problem all over the world because permanent and earthquake-proof storage facilities are still not available anywhere.

Some improved storage technology did evolve over the years, such as storing the spent fuel rods in dry casks and/or underground, but these storages are also only temporary. What is even worse is that, while the temporary storage facilities are getting full, governments are not concentrating on building permanent ones. For example, in President Obama's 2011 budget proposal, all funding for nuclear waste disposal was eliminated. So as of today, nearly 500 nuclear power plants around the world operate without permanent means of storing the waste they produce.

Preventing nuclear accidents by automation - part 2

Béla Lipták discusses the design and control errors at Fukushima, because they still exist in many American boiling-water reactors (BWR) and must be corrected

By Béla Lipták

Part 1 of this series listed some of the process control errors that contributed to the Fukushima accident. In the coming parts of this series I will discuss those design and control errors, because they still exist in many American boiling-water reactors (BWR) and must be corrected to protect against new accidents. I will discuss one error in each of this series of articles. In this issue, I will describe both the causes of the hydrogen explosions at Fukushima and the controls needed to protect against hydrogen explosions at American BWRs. In the third part, I will describe the sensors that are needed in the reactor core which will measure water level, steam/water ratio, temperature, etc., and which did not exist at Fukushima and meant that the operators there were operating “blindly.”

PREVENTING HYDROGEN EXPLOSIONS

Cooling of both the BWR reactors and the spent fuel rod storage ponds is essential for safety. As I have described in my previous article, well-designed backup systems, such as cooling water ponds on the roofs of earthquake-proof reactor buildings, can provide such backup, as gravity flow is always available even when electric power is lost. Some American plants provide such ponds, but not all.

When cooling is lost, as at Fukushima, the heat generated by fission will increase the temperature until first, the zirconium cladding and later, the fuel rods themselves start to melt. As the water level drops, and the zirconium cladding reaches about 1,000 °C, it will react

with the water to split it into hydrogen and oxygen. As the temperature rises, the top of the fuel rods (the uranium dioxide fuel inside the cladding) also melts, resulting in a partial or total meltdown.

As the water splits into oxygen and hydrogen, the hydrogen is released and mixes with the steam being generated in the reactor (Figure 1). Once the fuel rods start melting, the steam becomes radioactive. When the steam piping leaks/ruptures, or if the steam relief valve (PSV on Figure 3) opens, the mixture of steam and hydrogen is sent into the primary containment vessel or into the wet well.

If the hydrogen accumulates and comes into contact with air, it will explode (oxidize back into water). It is for this reason that both the primary and secondary containment should have been filled with nitrogen. They were not and, therefore, the hydrogen explosions at Fukushima destroyed the buildings and cracked some of the primary containment walls, allowing the leakage of radioactive water into the ground and the steam/hydrogen mixture into the air. The same scenario can be repeated in many American plants, if cooling is lost due to earthquakes, hurricanes or terrorist acts.

Meltdowns can also occur in the spent fuel ponds if cooling is lost. These ponds are even less protected as they are outside the primary containment (Figure 3). Stor-

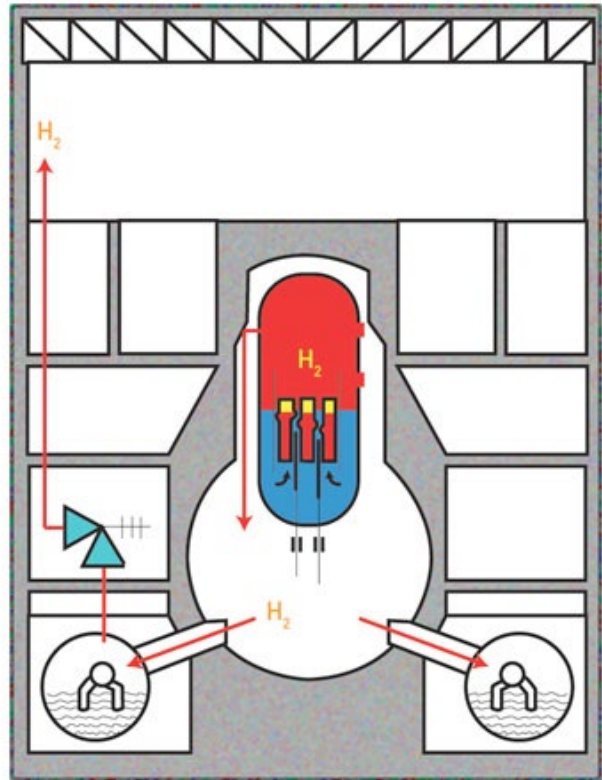


Figure 1: In many American plants, in case of a meltdown, the hydrogen generated is released inside the reactor building, where it accumulates, and if the building contains air (not N₂), it explodes. Once the hydrogen explodes, it will destroy the building and release radioactivity into the air.

age pond accidents are becoming more frequent when the ponds are filled beyond design capacity. At Fukushima, built in 1971, some 500,000 used fuel rods have accumulated. This is ten times the amount which the ponds were designed for. In many American plants, the spent-fuel pools represent a worse radiation threat than the reactors, because they contain far more uranium than is in the reactor cores.

There are safer temporary storage alternatives (“dry casks”), which do not require continuous cooling, but few American plants use

them. The typical temporary storage pool used at American plant is shown in Figure 2.

MANUAL OPERATION IS INHERENTLY UNSAFE

Below, I will describe the automatic controls that would have prevented the hydrogen explosions at Fukushima and can prevent their repetition in many American plants. First, (in Figure 3) I will show the bad design that was used in Japan and in many American plants. The reasons why these designs are unsafe are the following:

1. The pressure relief valves on the wet well (torus) are manually operated (SS in Figure 3). At Fukushima it was seven hours until the operators finally opened these valves. In many American plants, this valve is similarly under manual control.
2. When, after the first explosions, the operators at Fukushima finally decided to open the vent valves, the mixture of hydrogen and radioactive steam was vented without any filtering and, therefore, radioactive solid particles were released. Many American plants have no filters either.
3. The steam/hydrogen mixture was not vented to outside the building, where it would have been diluted by the wind and quickly risen (because of its low molecular weight of hydrogen), but was allowed to accumulate inside the building, where it exploded and caused structural

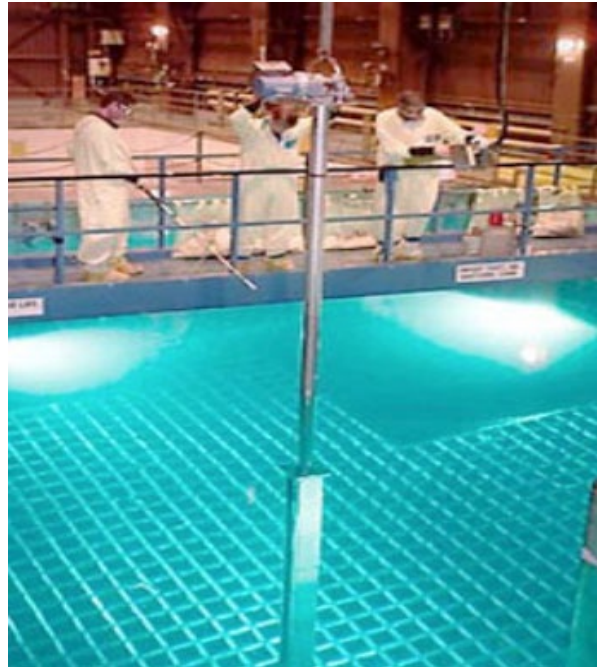


Figure 2: The spent fuel rods in the majority of American plants are stored in temporary storage ponds that require continuous cooling water circulation. In case of loss of coolant these spent fuel rods can also cause meltdowns and hydrogen explosions.

damage. The same could occur in some American plants.

4. The building was filled with air (not inert gas, N₂) and, therefore, oxygen was available to support the hydrogen explosions. In the newer and safer reactor designs the primary and the secondary containment structures can be purged or filled with inert gas (N₂), which, at the cost of operator inconvenience, increases safety. In the Fukushima plant and in most older American plants, the containment structures (including the torus) are not designed for purging with nitrogen and therefore, even during an accident, oxygen is available to support hydrogen explosions.

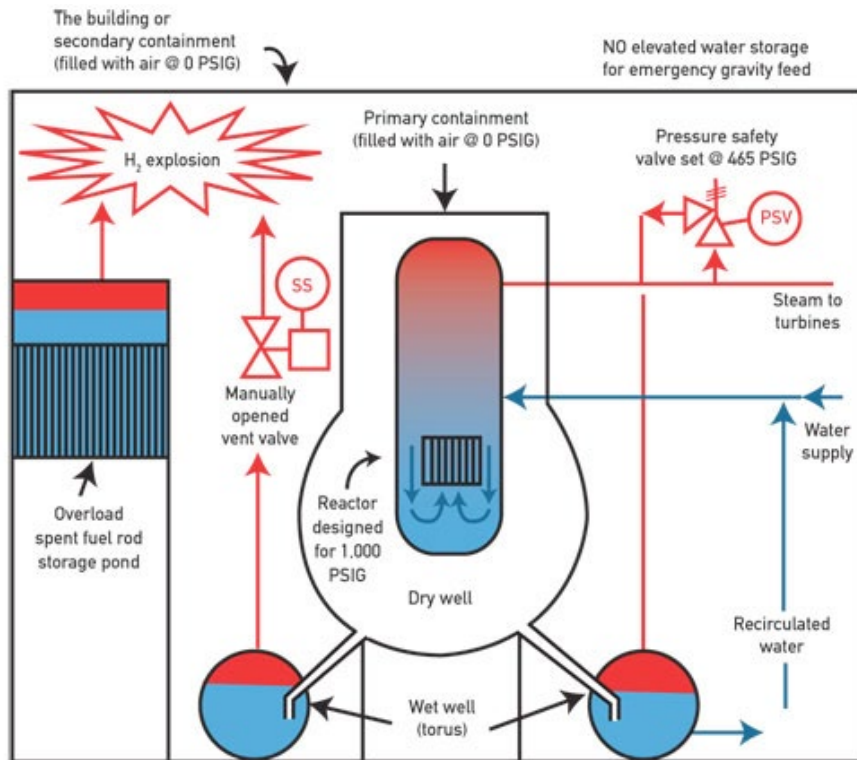


Figure 3: In many American BWR plants, if the radioactive steam, which is relieved by the PSV, does not condense in the wet well (due to loss of cooling), the pressure can build up and crack the primary containment unless the operator manually opens the vent valve (SS). At Fukushima this valve was not opened for 7 hours. Also, once this valve was opened (after the containment already cracked) hydrogen was not released from the building, but accumulated inside, mixed with air and exploded.

THE CORRECT DESIGN REQUIRES AUTOMATION

Figure 4 shows the automatic overpressure protection design that eliminates all the problems in the above list. The main reason why this design is safe is because it is automatic. Therefore, there is no operator's judgment involved. There is no hesitation for seven hours. It works automatically by venting whenever its set pressure (usually 75% of the design pressure) is reached. Period.

The second important feature is that the

released hydrogen is not allowed to accumulate inside the building, but is released into the atmosphere, where it is diluted and the hydrogen quickly rises up, away from the building. In addition, the radioactive particles are filtered out so they do not contaminate the area around the buildings.

Another important feature is that as soon as the excess pressure is released, the pressure safety valve (PSV) recloses. In case of the Fukushima (or any other plant where the vent valve is manually opened),

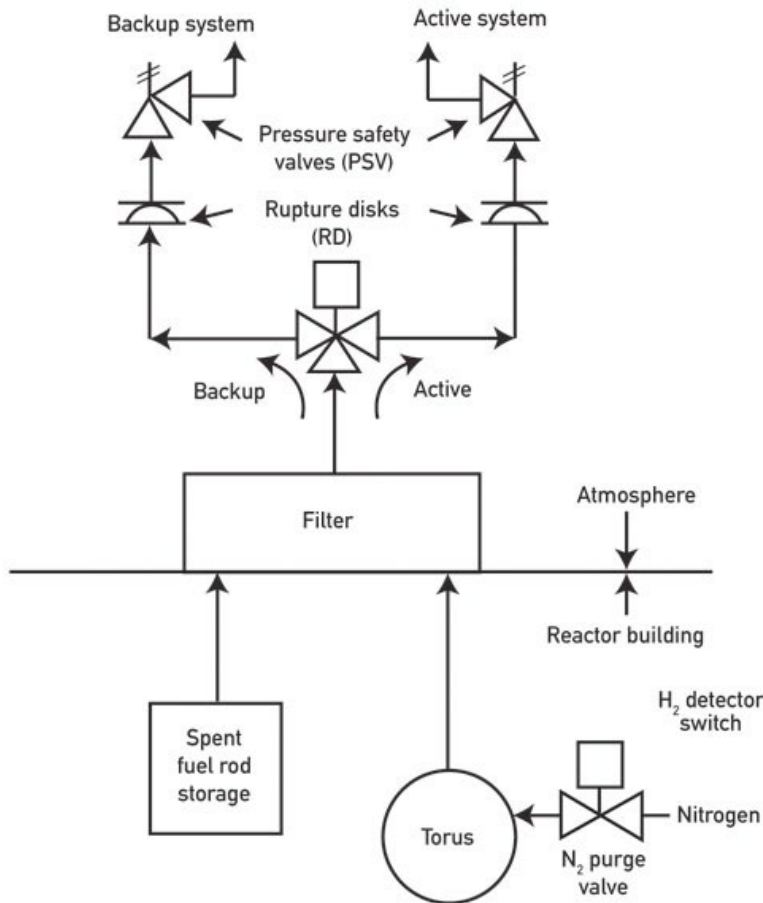


Figure 4: The vent is automatically opened at the setting of the rupture disk (RD) at 75% of the design pressure of the primary containment. The released steam/hydrogen mixture is filtered to remove radioactive particles. When the pressure drops, the pressure safety valve (PSV) is automatically reclosed.

the operator can forget to close it, releasing additional radioactive vapors. It is also important that full backup is provided for the automatic pressure relief system and that the burst rupture disk can be replaced while the plant is in operation.

In the next article of this series, I will describe how to measure the water/steam ratio, the swelled and collapsed water level and the temperature inside the reactor core, in order to eliminate guesswork. As we know, at Fukushima, and at many American plants, the operators do not have this information and are only guessing when answer-

ing such critical questions such as, are the fuel rods covered or if melting has started, how far has it progressed?

There has been, as yet, no time for the American nuclear industry to automate its manual systems based on the type of safety advice presented in this series of articles, but they are already becoming more vigilant. For example, during the latest flooding of the Missouri Rive, the Fort Calhoun plant near Omaha, Neb., was placed into “cold shutdown,” and plants in Louisiana and Florida were shut down when hurricanes were approaching.

How automation can prevent nuclear accidents - part 3

Watch out for outdated and/or unreliable instruments; these can cause major disasters

By Béla Lipták

In this article I will discuss how outdated and/or unreliable instruments caused the Japanese operators of the Fukushima Dai-ichi nuclear reactor to operate blindly because they did not know the water levels, water/steam ratios, temperatures and the degrees of meltdown in their reactors or in their spent fuel rod storage ponds. In the case of the Fukushima accident, this resulted in the operators' guessing at the level of cooling water, and because they guessed wrong, they drastically delayed the start of cooling by the few emergency means at their disposal, such as by using helicopters, fire trucks and sea water. In this article I will describe the sensors that American plants should install in order to provide reliable information during both normal and emergency operation of boiling water reactor (BWR) plants.

The BWR reactor's core is surrounded by a shroud. The cooling water enters into this "jacket-like" space between the shroud and the wall of the reactor (Figure 1). The water travels down the outside of the core and then rises up inside it. As it rises, the fuel rods heat it until it starts to boil. As the steam bubbles form, the water "swells" (its steam-to-water ratio rises). The goal of the control system is to keep the fuel rods always covered in order to protect against their overheating and melting.

In most of today's BWR reactors, the levels and the steam/water ratios within the core are not measured. The water level outside the shroud is measured, but does not reflect the level

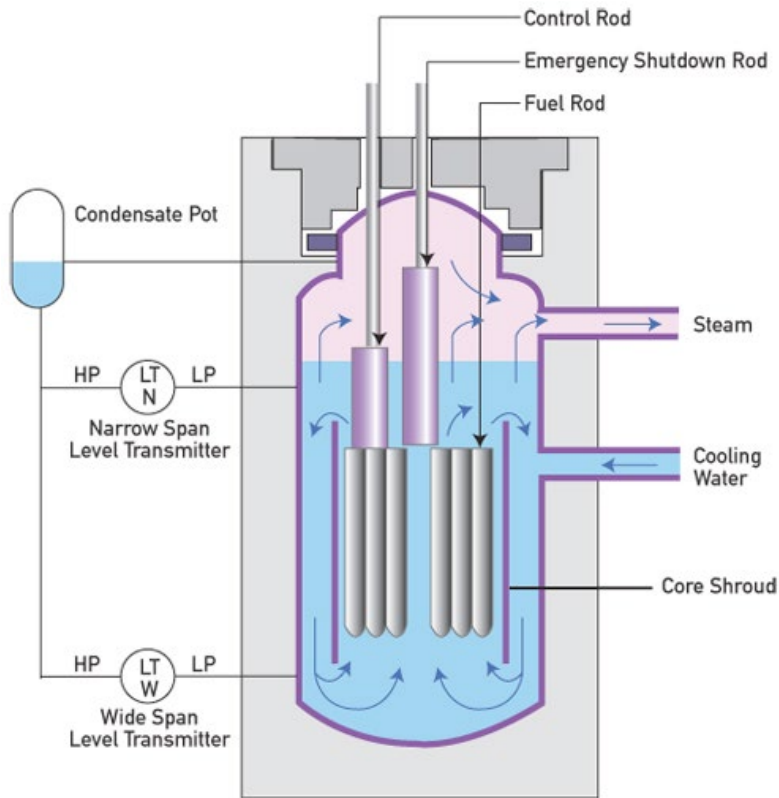


Figure 1: In conventional BWR reactors, the water level is measured only between the shroud and the reactor wall. This measurement does not reflect the water level inside the core when coolant is lost.

inside once the water level drops below the suction of the jet disperser. Consequently, this level measurement is meaningful only during normal operation, and is useless during emergencies caused by loss of cooling.

The level outside the shroud is usually measured over two ranges, a narrow (LT-N) one and a wide (LT-W) one. The narrow span LT-N is more sensitive and is a better indicator of the surface level while LT-W detects the total hydrostatic head in the reactor (the collapsed level). They both usually are the d/p types, provided with condensate-filled wet legs. The condensate pots are uninsulated, and drain back into the reactor through a sloped connecting pipe. In old plants, these transmitters (or d/p indicators) are often

located in the control room through long, water-filled lead lines connecting them to the reactor. This is a terrible idea because these long lead lines often cause gas blockage, leaks or oscillation, but 40 years ago they were in use by some.

These level transmitters are inverse-acting (the reference leg is the high-pressure side), and therefore, a maximum level produces a zero-differential reading, while a zero level causes a maximum output signal. The measurement also assumes that the wet leg is full with condensate at ambient temperature. During an accident, neither of these assumptions is guaranteed. In fact, they are likely to be wrong, because once the level in the reactor drops below the low-pressure tap of

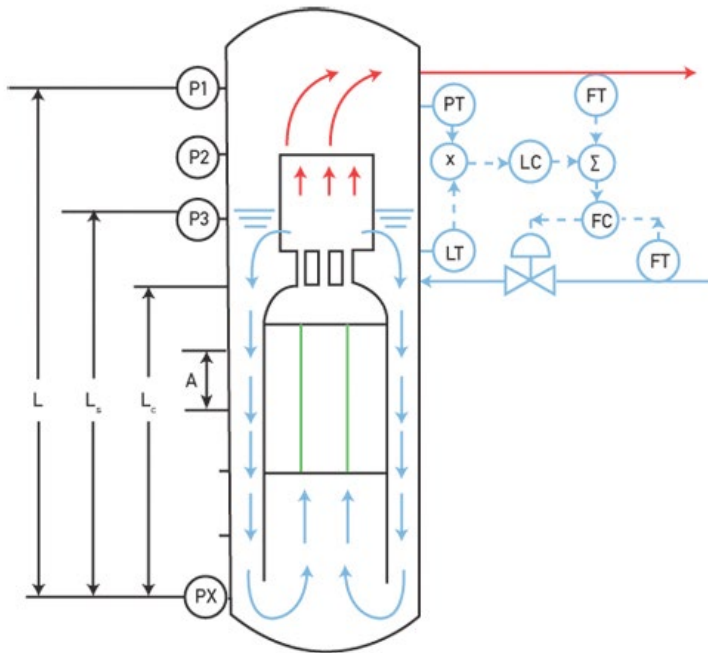


Figure 2: The red arrows show the steam, the blue arrows the water flow. Readings of P1, P2, etc., to PX (on the left) measure the level and steam/water ratio outside the core.

LT-N, the reading is meaningless (zero).

Also, if the water in the reactor is boiling, these d/p cells detect the hydrostatic head (mass of water), not the level. The more bubbles form (swelling), the lower the density. Therefore, the lower level is reported by the d/p cell. Inversely, as the rate of steam formation drops (shrink phase), the density increases, and the level reading rises. In other words, when the surface of the boiling water rises (swell condition) the level reading drops, and when the boiling rate and, therefore, the level drops, the measurement rises.

The level shrinks or swells whenever the loading of the reactor changes because during that time, the rate of water entering is different from the rate of steam leaving. Swelling occurs when the steam pressure drops (the

steaming rate increases), and shrinking occurs when the steaming rate is reduced (the steam pressure rises), and bubbles collapse. Therefore, the d/p cell outputs can be converted into indications of the surface level only if the density is separately determined.

At Fukushima and at many American plants, this correction was/is inaccurate or nonexistent. Therefore, these level measurements are unreliable or useless. Because of this, the level control loop cannot be closed (cannot be placed in automatic) and is often under manual control, which is unacceptable.

DETECTING LEVEL CORRECTLY OUTSIDE THE CORE

In order to accurately measure the level outside the core, several pressure detectors (P1 to PX on the left of Figure 2), should be

The solution is to measure the in-core level and automatically start emergency cooling.

installed at equal distance (A) from each other. The smaller the distance A is, the higher will be the precision of measurement. If we define ΔP as the pressure difference between any two adjacent sensors, when ΔP is zero, there is no water at that level—this is the case between P2 and P3 in Figure 2—and if ΔP equals $A(SG)$, that means that there is no steam at that elevation. (SG is the specific gravity at the actual temperature). By this method, both the level of the boiling surface (Ls) and the pressure at that elevation (Ps) can be determined. (The resulting Ls reading is the same as the one detected by LT-N in Figure 1).

The various combinations of these measurements can be used to obtain the following information:

- Steam/water ratio (S/W) at any elevation is $S/W = \Delta P/A(SG)$.
- Collapsed total water level is $L_c = \Delta P_s / (P_X - P_1)$.
- Total S/W in the whole reactor $S/W_r = (P_X - P_1)/L(SG)$.
- Steam/water ratio of the boiling column of water from up to the elevation Ls is $S/W_s = (P_X - P_s)/L_s(SG)$.

I would provide both the d/p cells (Figure 1) and the pressure detectors (Figure 2) with

battery backup and with wireless output signal backup, so that if either the regular power supply fails, or the regular output signal wires are damaged, the level information will still be available and can be read not only in the control room, but anywhere.

At Fukushima and in many American BWR reactors, level inside the core was/is not measured at all. During emergencies when the regular water supply is lost, the in-core level is not the same as the ex-core reading, yet it is the in-core measurements that are critical in deciding when emergency cooling is needed.

The solution to this unacceptable situation is not only to measure the in-core level, but when the fuel rods are about to be uncovered, automatically start emergency cooling by opening the gravity flow from elevated open or from pressurized closed tanks (or from helicopters, fire engines, etc.).

As to the method of detecting the in-core water level, I would use probes designed to measure the temperature at the different elevations in the core (Figure 2). The temperatures at the different elevations reflect the steam/water ratio, because water is a better heat conductor than steam, and therefore, the probe temperature will rise as the proportion of steam bubbles rise.

Automation could have saved Fukushima - part 1

Lipták says that if the Fukushima level detectors had operated correctly, the hydrogen explosions would have been prevented

By Béla Lipták

In the forthcoming articles of this series, I will describe how automation could have prevented the Three-Mile Island and Chernobyl accidents. Here, I will do the same for Fukushima, but because of the importance of that accident, I will devote more than one article to it. In this first article I will concentrate only on the measurement of the water level in the reactor. This is an important topic, because if the Fukushima level detectors had operated correctly, and if the operators had flooded the reactors as soon as the earthquake was detected (some 40 minutes before the arrival of the tsunami) and would have started the venting of the hydrogen as soon as the fuel rods were uncovered, instead of waiting five or six hours, the hydrogen explosions would have been prevented.

THE TRADITIONAL REACTOR LEVEL MEASUREMENT

Figure 1 shows the traditional method used in the majority of nuclear reactors. Here, the cooling water enters a jacket-like space between the shroud and the reactor wall and is pumped downward by a jet dispenser (not shown). It travels down “ex-core” (on the outside of the core) and then rises up “in-core.” As it rises, the fuel rods heat it, and the water boils and, therefore, “swells.”

In most nuclear power plants, the ex-core level is measured by two differential pressure transmitters (Figure 1). One has a narrow span range (LT-N) and the other a wide one (LT-W). The narrow span transmitter (LT-N) is a better indicator of the surface of

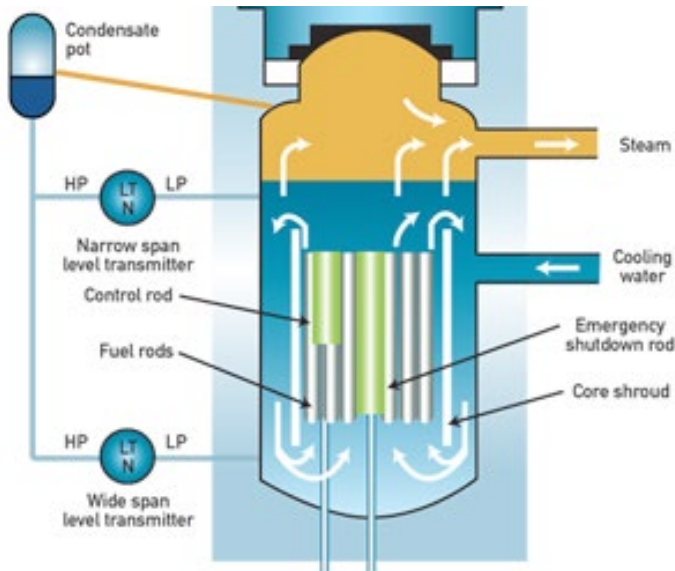


Figure 1: This traditional system uses condensate pot compensated d/p transmitters. In such a system, if the condensate in the reference leg is lost (boils off), the level transmitters will over-report the level.

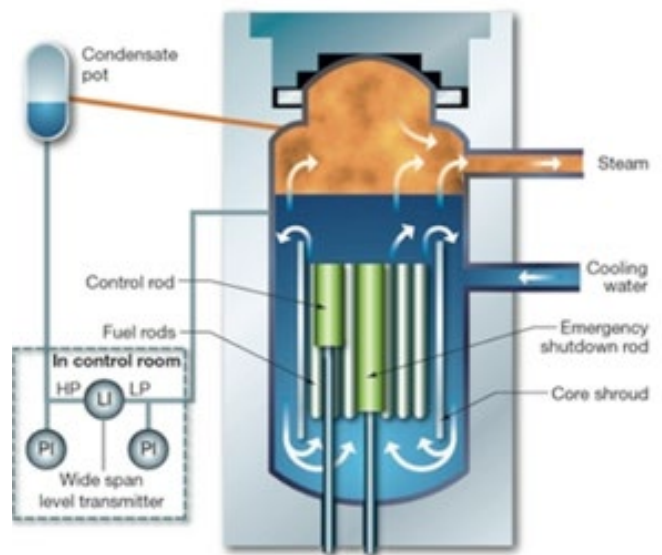


Figure 2: Direct-connected remote level indicators (LI) were used at Fukushima which further reduced reliability.

the boiling water, while the wide-range transmitter (LT-W) detects the total ex-core hydrostatic head (mass of water) in the reactor (the weight of the “collapsed water column”).

These level transmitters are installed with condensate pots which connect these reference legs (“wet legs”) to the high-pressure side of the d/p cells. These level transmitters are “inverse-acting” (if the level rises, the transmitter output drops), because the hydrostatic head of the condensate in the reference leg is always higher than the weight of the water column inside the reactor. Therefore, the

transmitter outputs are zero when the water level is at its maximum, and zero level generates a maximum output signal.

The reliability of this measurement depends on the assumption that the wet leg is full of condensate and that it is at ambient temperature. During an accident, these assumptions can be wrong because the condensate in the reference leg can overheat or drain. Even under normal operating conditions, the more bubbles that form (swelling), the higher will be the apparent actual level, but the lower its density and, therefore, the detectors will under-report the level. Inversely, as the steaming

rate drops (shrinking phase), the density increases, and the actual level drops, while the level reported by the transmitters increases. Therefore, these level measurements are either unreliable or useless. The operators, after a while, notice that and start to disregard them or even disconnect the automatic level controllers and try to manipulate the level manually.

THE FUKUSHIMA DESIGN

In the case of Fukushima the design was even worse, because no transmitters were used at all. Only d/p indicators were provided, and they were located in the control room (Figure 2), requiring long lead lines. One of the lead lines detected the high-pressure reference from the condensate pot.

At Fukushima, soon after the cooling water pumps stopped, the condensate temperature in the uninsulated pot reached boiling point and boiled off. Once the lead line to the high pressure side of the level indicator emptied, the indicator over-reported the water level in the reactors by several meters, which gave the operators a false sense of security.

RELIABLE EX-CORE LEVEL MEASUREMENT

There are at least three ways to eliminate the level measurement error caused by the boiling off of the condensate from the wet legs. These are 1) Use different

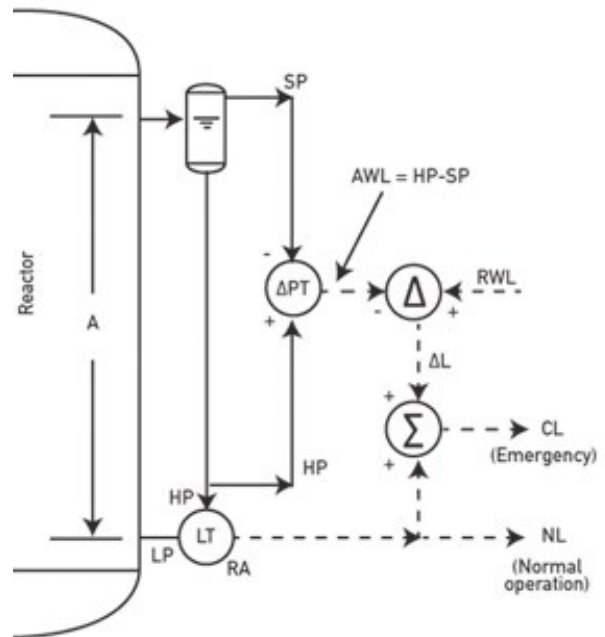


Figure 3: This control system continuously calculates the correct level (CL) if during an emergency, some or all of the condensate has boiled off from the wet leg. Converting a traditional system (Figure 1) to this one is easy and does not require a plant shutdown.

type level detectors; 2) Move the condensate pot, wet leg and d/p cell outside the primary containment; 3) Keep the existing system, but detect the height of the reference leg and if it drops, compensate for that drop.

Choices 1) and 2) require plant shutdown, while 3) can easily be implemented without shutdown and without much expense (Figure 3).

Figure 3 shows how the actual weight of the (remaining) condensate in the wet leg (AWL) is measured and how that is subtracted from the normal reference wet leg (RWL). The calculated difference (ΔL) is

the height of the lost condensate in the wet leg. Under emergency conditions, by adding this amount (ΔL) to the level reported by the d/p cell (NL), the corrected level (CL) is obtained. It is recommended that both signals (NL and CL) be sent to the control room to provide the operators with the needed information concerning the conditions in the reactor. Any number of d/p cells (LT) can be added to the reactor, and the closer they are vertically, the more accurate their readings will be. In addition to reporting the level, they can also measure trends and other variables, such as the steam-to-water ratio, etc.

IN-CORE LEVEL MEASUREMENT

The ex-core level measurement will approximate the in-core level only so long as the fuel rods are covered by water, but once the ex-core level drops below the suction of the jet diffusers, it will not. Therefore, direct in-core measurement is also needed. In many cases, such as Fukushima, they were not provided.

One method of in-core level measurement is to correlate it with the gamma radiation distribution inside and outside the reactor. The vertical gamma radiation distribution is related to water level, because water is more of a moderator than steam. On the other hand, because gamma radiation is also a function of the neutron flux and of the speed of water recirculation, special correction models and algorithms

are needed to obtain the water level from gamma radiation distribution.

Other possible ways to detect in-core level (or steam/water ratio) are based on the thermal or electric conductivity, or neutron modulation, etc. differences between water and steam.

Dr. David Nyce designed such a thermal conductivity-based, in-core level sensor for the Knolls Atomic Power Laboratory. In that design, a number of different length metal probes are inserted, each equipped with two vertically separated thermocouples (TC). The one located at the tip is heated, while the second, unheated reference thermocouple is a few inches above the tip. In the case of this sensor, if water covers both TCs, the temperature difference (ΔT_w) will be lower than the temperature difference (ΔT_s) when both are covered by steam.

If all nuclear power plants used the correct level measurement design shown in Figure 3, their safety would be much improved. In the next article in this series, I will describe other ways automation could have prevented the Fukushima accident.

Automation could have prevented Fukushima - part 2

Lipták discusses automatic vs. manual operation of the emergency cooling systems, and the roles the bad designs of control and block valves played in this nuclear accident

By Béla Lipták

In part 1, I discussed some of the factors that lead to the Fukushima meltdown. Here I focus only on the automatic vs. manual operation of the emergency cooling systems and the roles the bad designs of control and block valves played. The main emergency cooling systems that should have been fully automated were the high-pressure coolant injection (HPCI), the reactor core isolation cooling system (RCIC) and the isolation condenser (IC).

As to the desirable features of valve designs, the following were often neglected:

- All valves should have been provided with position-detecting limit switches.
- All valves on cooling service should have failed open.
- All valves between pressure relief devices and the protected equipment should have been sealed open.
- All valves should have been provided with hand wheels and backup operating power.
- Pressure control valves should have been completely automated and manual operation inhibited.

THE HPCI SYSTEM

The HPCI was the first line of defense to take over the feeding of cooling water into the reactor pressure vessel (RPV) if the main cooling water pump failed. It had a pumping capacity of 5000 gpm, but was a bit slow (took some 30 seconds to come

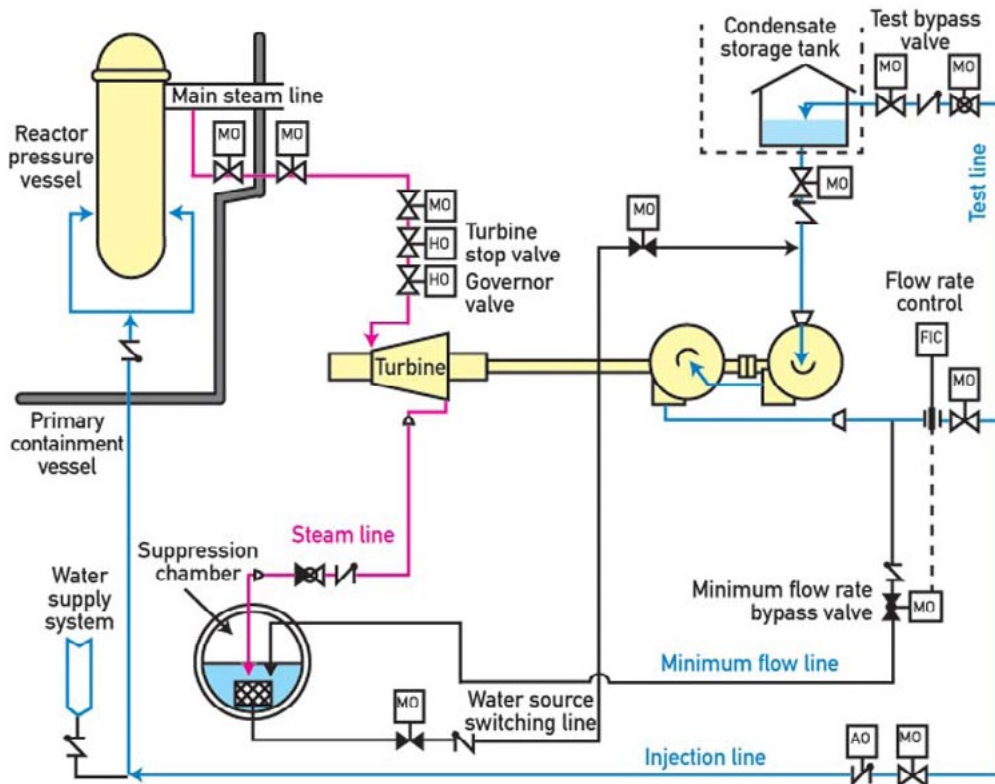


Figure 1: The HPCI system at Fukushima Dai-ichi NPS Unit 1 with motor-operated (MO) valves, hand-operated (HO) valves and air-operated (AO) valves. Courtesy of Tokyo Electric Power Co. (TEPCO)

on), so there was also a 600-gpm system, called the RCIC, which operated the same way, but activated faster.

The HPCI was a reliable system because it did not need electricity for its operation, because its pumps were operated by steam turbines, and decay steam was available from the reactor (Figure 1).

The HPCI took its water supply from storage tanks and from the wet well, which contained 3000 m³ of water. This amount of water would have been ample to keep

the reactors cool. The HPCI pumps were controlled on the reactor level, stopping when the level was high, and starting when low.

Reactor overpressure was to be relieved by pressure safety valves, which were set to relieve at about 75 atmospheres (PSV in Figure 2) and discharged into the wet well, where the steam should have condensed.

This system would have operated at Unit 1 if the reactor level was correctly mea-

sured and the PSV automatically opened at 75 and closed at 70 atmospheres.

In other words, depressurizing the RPV by allowing the PSV to work, while adding sufficient coolant with the HPCI system, would have been essential for avoiding a meltdown. This is proven by the fact that there was no meltdown at Units 2 and 3, where the operators allowed the PSV to do its job.

Unfortunately, the system at Unit 1 was not automatically controlled, and the level measurement was wrong. On top of that, the operators used the isolation condenser (IC) system to control the reactor pressure instead of letting the PSV do it, and did it in on/off manual fashion.

This, in combination with the IC, caused depressurizing, resulting in the swelling of the level, causing HPCI to stop, which in turn caused the dropping of the reactor level, so the fuel rods overheated and the meltdown followed.

ISOLATION CONDENSER (IC)

IC is a heat exchanger located above a containment pool. This 500 tons of water pool was open to atmosphere (Figure 3). Under normal conditions, the top of the IC condenser was connected to the reactor pressure vessel (RPV) through an open valve, so the condenser filled with conden-

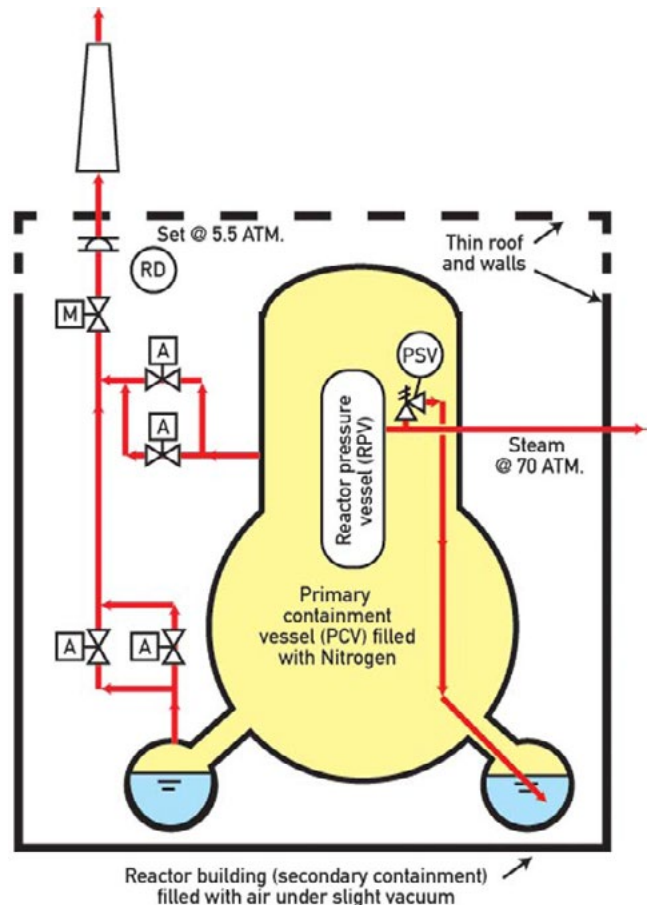


Figure 2: At Unit 1, the PSV was not used to relieve overpressure. The cracking of the primary containment vessel (PCV) could have been prevented if the rupture disk (RD) had ruptured as soon as the pressure in the PCV reached 5.5 atmospheres, but block valves (A and M) could not be opened.

sate, which normally just stayed there. During an emergency, the IC system automatically opened the motor-operated valves at the bottom IC, which sent the condensate back into the reactor by gravity and by condensing the steam and cooling the reactor. This was a good system because, once activated, it required no outside energy source; it worked on gravity.

At Unit 1 at Fukushima the sequence of events was:

- 2:46 a.m.—Earthquake detected and reactor scrammed.
- 2:52 a.m.—IC automatically started.
- 3:03 a.m.—IC closed manually by an operator (this on/off control approach continued for a day!)
- 3:30-3:35 a.m.—Tsunami arrived. IC would have continued to operate, if not turned off.

The reason why the isolation valves (M in Figure 3) were provided was to allow the operators to control the rate of pressure drop in the RPV because excessively fast pressure reduction could have cracked the RPV walls. Naturally, in a properly automated plant, this rate of pressure reduction would have been automatically controlled.

In the next article of this series, I will explain how, even after the meltdown at Unit 1, automatic safety controls could have prevented the explosions and fire that caused the release of radioactivity.

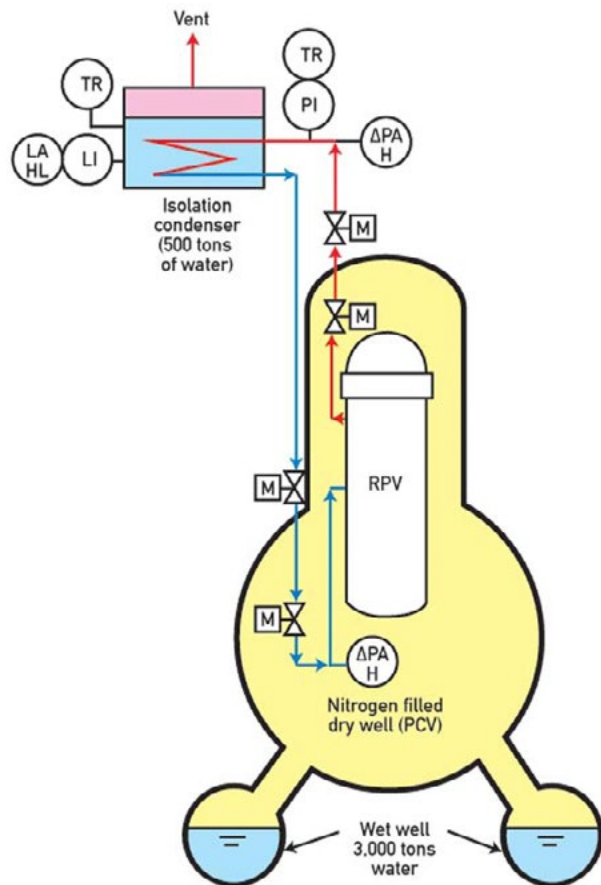


Figure 3: This IC system would have continued to operate by gravity, but was manually turned off. If the system was automated, IC cooling would have not stopped.

Automation and Fukushima - part 3

Watch out for outdated and/or unreliable instruments; these can cause major disasters

By Béla Lipták

I'm describing the three phases of the sequence of events that led to the accident at Fukushima. At the time, three of the six reactor units were in operation (Units 1, 2 and 3). Unit 4 was de-fueled, and Units 5 and 6 were in cold shutdown. My goal is to show that in each phase of this sequence of events, automation could have prevented the continuation of the process that led to the accident.

In part 1, I showed that upon detection of the earthquake at 2:46 p.m. on March 11, 2011 (45 minutes before the tsunami), automation would have started all cooling systems, including the flooding of the reactors with sea water before the tsunami hit. Automation would have also corrected the defective reactor level transmitter, which was indicating high cooling water level when, in fact, it was low. This would have prevented the confused operators from manually turning off the isolation condenser (IC) cooling system at Unit 1, and would have prevented the meltdowns.

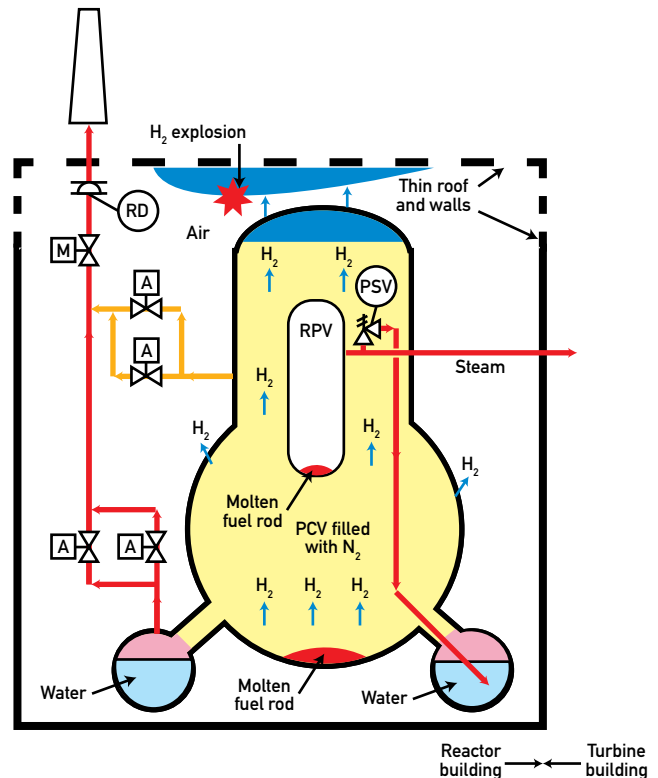
In part 2, I showed that if the controls were automatic, venting would have started as soon as the pressure reached 5.5 atmospheres in the primary containment vessel (PCV). In addition, all valves would have been provided with hand wheels and local backup power, so that it would not have been necessary for the operators to drag batteries and portable air compressors to the valves to open them.

Here, I will show that even after the melt-down, automatic controls would have prevented the hydrogen explosion, which destroyed the building and released all that radiation. Naturally, three brief articles do not do justice to this complex subject. For this reason I also wrote *The Next Fukushima: Automation Can Prevent It*, published by the ISA.

AUTOMATIC PREVENTION OF THE HYDROGEN EXPLOSION

If automatic safety controls existed at Fukushima, hydrogen detectors would have been provided both inside the PCV and near the roof of the reactor building, so that if hydrogen were detected at either location, its venting would have started automatically. Instead, nothing was done for 12 hours. In fact, I could not find any information that would have proved that hydrogen detectors existed!

We do know that 12 hours after the earthquake, by 2:45 a.m. on March 12, the pressure in the reactor pressure vessel (RPV) dropped to 9.5 bars (from 69 bars), while the pressure in the PCV containing the reactor increased to the same value. This was a clear indication that the reactor walls cracked or ruptured, and that the molten fuel rods first collected at the bottom of the RPV and leaked out, collecting at the bottom of the PCV.



VENTING NEEDED

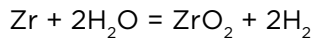
Figure 1: The figure shows that the hydrogen explosion could have been prevented if the hydrogen from the pressure containment vessel (PCV) had been vented before its walls ruptured. Automatic venting could not occur because the vent connection was on the side of the PCV, not the top, and the rupture disk (RD), which was set to rupture at 5.5 bars, was blocked from the PCV by valves that were stuck closed. (The molten fuel rods are shown in red; nitrogen in yellow; water in light blue; and hydrogen in dark blue.)

THE FORMATION OF HYDROGEN

The first step in the sequence of events leading to the hydrogen explosion was the formation of hydrogen caused by the melting of the cladding of the fuel rods. This occurs at a temperature of about 1200 °C, at which point the zirconium in the cladding oxidizes by taking oxygen from the steam, and thereby generating a

If the hydrogen explosion is to be prevented, the signaling of the presence of hydrogen must automatically initiate venting.

large quantity of hydrogen:



In order for an explosion to occur, the generated hydrogen has to travel to an area where oxygen is present, has to accumulate to a concentration of about 3%, and has to find an ignition source. Therefore, if the hydrogen explosion is to be prevented, the signaling of the presence of hydrogen must automatically initiate venting, which requires continuous monitoring of the hydrogen at the high points in both the PCV and the building.

At Unit 1, the melting of the fuel rods probably started at around midnight on March 11, some nine hours after the tsunami hit, while the explosion occurred some 13.5 hours after that at 3:36 p.m. on March 12. In Units 2 and 3, the accumulation of hydrogen took longer (days) until similar explosions occurred on March 14 and 15. So in each case, there was plenty of time to vent the hydrogen, but it was not done. Why?

THE VENTING OF THE HYDROGEN

Let us first ask, how did the hydrogen find its way to an area where oxygen was present, and how did it accumulate there? Well,

in order to reach an area containing oxygen, the hydrogen first had to escape from the PCV after the walls of the PRV ruptured. At that point, the molten fuel rods leaked to and accumulated on the bottom of the PCV. So, the formation of hydrogen continued there (Figure 1), and being a low-molecular-weight gas that is not soluble in water, the hydrogen rose to the top of the PCV and accumulated there.

As long as the generated hydrogen stayed inside the PCV, it could not explode, because this primary containment was inerted (filled with nitrogen). Under these conditions the hydrogen just rose and accumulated in the upper part of the PVC. From there it could not be vented because the vent connection was not on the top (a design error), but on the side of the PCV. Therefore, it just accumulated until the PCV ruptured. It ruptured because the rupture disk protecting it (RD in the figure) was blocked by closed valves, which the operators could not open.

The reactor building itself was not inerted (once hydrogen was detected, inerting should have started automatically), and therefore, once the hydrogen entered the building, it made contact with oxygen. Once its concen-

Naturally, if automatic safety controls were provided, none of this would have happened because the safety system would have monitored the presence of hydrogen, and as soon as it was detected, would have vented it.

tration reached 3%, all that was needed for an explosion to occur was an ignition source. Naturally, if automatic safety controls were provided, none of this would have happened because the safety system would have monitored the presence of hydrogen, and as soon as it was detected, would have vented it. In addition, before the hydrogen was released to the outside, filters should have been provided to remove the radioactive particles. (I could not find such filters.)

CONCLUSIONS

I hope that with this series of articles I have dispelled the notion that Fukushima was unpreventable, and convinced most readers that automation, which blocks unsafe operator overrides, could have prevented it. I know that by 2022 Germany is planning to terminate the use of nuclear energy, with other nations following later, but I also know that others are building plants. For example in the United States, only two plants have been shut down in 2013 (San Onofre and Crystal River 3), while the Nuclear Regulatory Commission extended the operating licenses of several that are over 40 years old because decommissioning costs about \$3 billion and results in the loss of more than 1,000 jobs. So most of the 435 operating nuclear power plants

around the world, having an average age of 25 years, will be around for some time. I also know that, in this age, when on the one hand we trust robots to explore Mars and operate drones in our wars, and on the other hand we have a time of cyber-terrorism in which background checks of operators is never foolproof, we still don't trust full automation without manual overrides when the task is to boil water.

I know that there will be readers who will defend the safety practices of this industry because for a lifetime they applied and got used to its practices, and because it is human nature to defend the practices of one's industry, particularly if criticism comes from the "outside." I also know that having, on the average, 25-year-old controls, it would take a lot of effort to eliminate operator overrides and convert to full automation. Yet, if even some of the readers of *Control* would fail to trust the capabilities of our own profession, why should the general public? Of these few doubters I would ask: Do you know of a single nuclear power plant, which, upon the failure of both the internal and external electric power, would automatically and safely shut down, no matter what the operators did?

Chernobyl did not need to occur

Good process control could have prevented this historic meltdown

By Béla Lipták

We now know that properly designed process controls could have prevented the meltdown at Chernobyl. The causes of this accident were similar to those at 3 Mile Island seven years earlier. Both of these accidents occurred at night, after a shift change of operators who were poorly trained, uninformed and were operating the plants under manual control while their safety controls were bypassed. Ironically, the Chernobyl accident occurred during a test run, which was conducted to improve plant safety. This accident proved once more what experienced control engineers have all learned: that a process must be understood before it can be controlled.

The accident occurred while the reactor was being tested at low loading (20%) to determine the time period during which the plant would stay stable and continue to produce electricity after being shut down. The test was conducted in the middle of the night, by an inexperienced crew, while the control computer was disabled. The Chernobyl design had a positive void coefficient (VC), meaning that an increase in core temperature (more boiling) further increased power generation.

During the test on April 26, 1986, at 1:23 a.m., a runaway condition developed during which the power generation reached over 100 times the design capacity and caused a steam explosion that blew off the 2,500-ton top of the reactor. As air entered the reactor, the graphite in the core also ignited, further worsening the meltdown. As a result of the explosion and

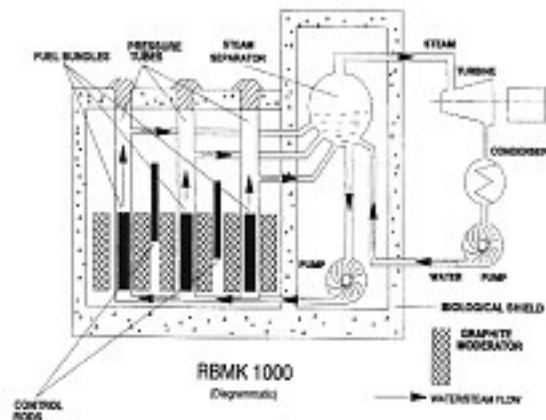
fire, 20 million curies of radioactivity was released, an amount which is 30 times the nuclear fallout that occurred at Hiroshima and Nagasaki. Thirty operators and fire fighters died and some 1,800 thyroid cancer cases (700 of them children) were reported (most of them survived). The accident also resulted in a massive relocation of the population as radiation made human life impossible over a 5,000 square-kilometer area.

MATCHING THE CONTROLS TO THE PROCESS

I cannot possibly list all the errors in the process control system, because practically none was provided. The lack of process control can be explained partly by the fact that the plant was built for military purposes and, therefore, was designed to operate at constant loading in a plutonium-production mode. The second cause was the prevailing operating philosophy at the time in the Soviet Union, which did not trust automation and relied on operators who did not understand the process.

Examples of this lack of understanding included the use of constant controller gains on a variable gain process. The gain of this process increased (the process became more sensitive) as the load was reduced.

The operators did not understand the “inverse response” of the process either. They did not know that as the control rods are lowered into the reactor core, the



The RBMK* core details showing the water passing up around the fuel rods while power generation (heat release) is controlled by the depth of insertion of the control rods

Figure 1 describes the 1000-MW Unit 4 of the Reactor Bolohoj Moshosztjl Kanalnyj (RBMK) nuclear reactor at Chernobyl, in the Ukraine.

reactivity does not drop immediately, but it first rises and drops only later. (Reactivity refers to the portion of nuclear energy that is available to generate steam. Reactivity is reduced—the “energy insulation effect” increased as the absorber rods are lowered. The second most effective moderator is water. Graphite is the third, and steam is the least effective moderator. Reactivity therefore increases with increased steam void formation or boiling.) In other words, they viewed a variable gain and “inverse response” process as if it was neither. Therefore, as the load dropped (reaching 7% of full loading), the VC became so large that it overwhelmed all other influences, and the meltdown of the core resulted.

As the operators did not understand the process, they attempted to control a very fast process, which at the time of the explosion had a time constant in seconds, by slow final control elements. The speed of the control rod movement was 0.4 m/s, corresponding to a stroking time of 15 seconds to 18 seconds. In addition, these manual controls used a measurement with a dead time of 15 minutes, because the intermittent calculation of the operating reactivity margin (ORM), using 4,000 data points, required that much time and on top of that, the calculation was done outside the control room at a different location from where the operators worked.

The ORM is the ratio obtained if all control rods are withdrawn divided by the effect on the total reactivity of one rod. In this case, ORM should have exceeded 30, and it was 7. In addition, ORM calculation was intermittent, took 15 minutes and was done 150 feet away from the control console.

If an experienced process control engineer had been on site she would have known that in order to maintain stability, supply-demand matching controls were needed. This demand controller, under steady load conditions and stable conditions would have met the variations in electric power demand by modulating the thermal energy supplied by the reactor core. This electricity demand controller would have been de-

signed as the cascade master of slave controllers that were modulating all final control elements. The slave controllers should have modulated the flow of cooling water and the position of control rods (in this case 211 boron carbide absorber rods). Naturally, these final control elements would have been selected to be faster than the process they control.

It can, therefore, be seen that, if properly designed automatic controls were used, the cascade master demand controller operating inside a safety envelope would have kept ORM above 30 and the positive void coefficient (PVC) influence within safe limits. None of these conditions were met. In addition, the test was conducted under manual control and all automatic safety systems (both the emergency protection system and the emergency core cooling system) were disabled, which is a recipe for disaster.

THE DESIGN

Design errors also contributed to the disaster. The plant had no containment building. Consequently, only the zirconium cladding and the reactor walls insulated the uranium fuel rods from the outside surroundings. On top of that, an ignitable graphite moderator was used and xenon poisoning increased as the load on the reactor was reduced.

Furthermore, the designers did not understand that once the core starts melt-

ing, the zirconium cladding will burn and thereby generate hydrogen as the oxygen in the steam is used up. In addition, they did not understand that the produced hydrogen will not only displace the cooling water (and thereby reduce heat removal), but this extremely hot hydrogen will also quickly rise, increasing the pressure in the vapor space of the reactor. At Chernobyl, as this pressure increased, it lifted the top of the reactor, and as it entered the atmosphere, it formed oxy-hydrogen, initiating a detonation.

The lessons learned at Chernobyl include that (while there is no such thing as a safe nuclear power plant) understanding process dynamics and providing redundant automatic controls to match them can minimize the probability of accidents. To maintain such safe operation, the use of manual must be minimized, and the redundant automatic safety interlocks must not be bypassed. An even more important lesson is that designing a safe control system requires the in-depth understanding of the process by experienced process control engineers, and that safety will not be improved by relying only on the advice of manufacturer's representatives alone. The designers of Chernobyl did not realize that in designing the plant controls, process control professionals (not salesman) must play a primary role, if nuclear safety is to be improved.

What caused the Three Mile Island accident?

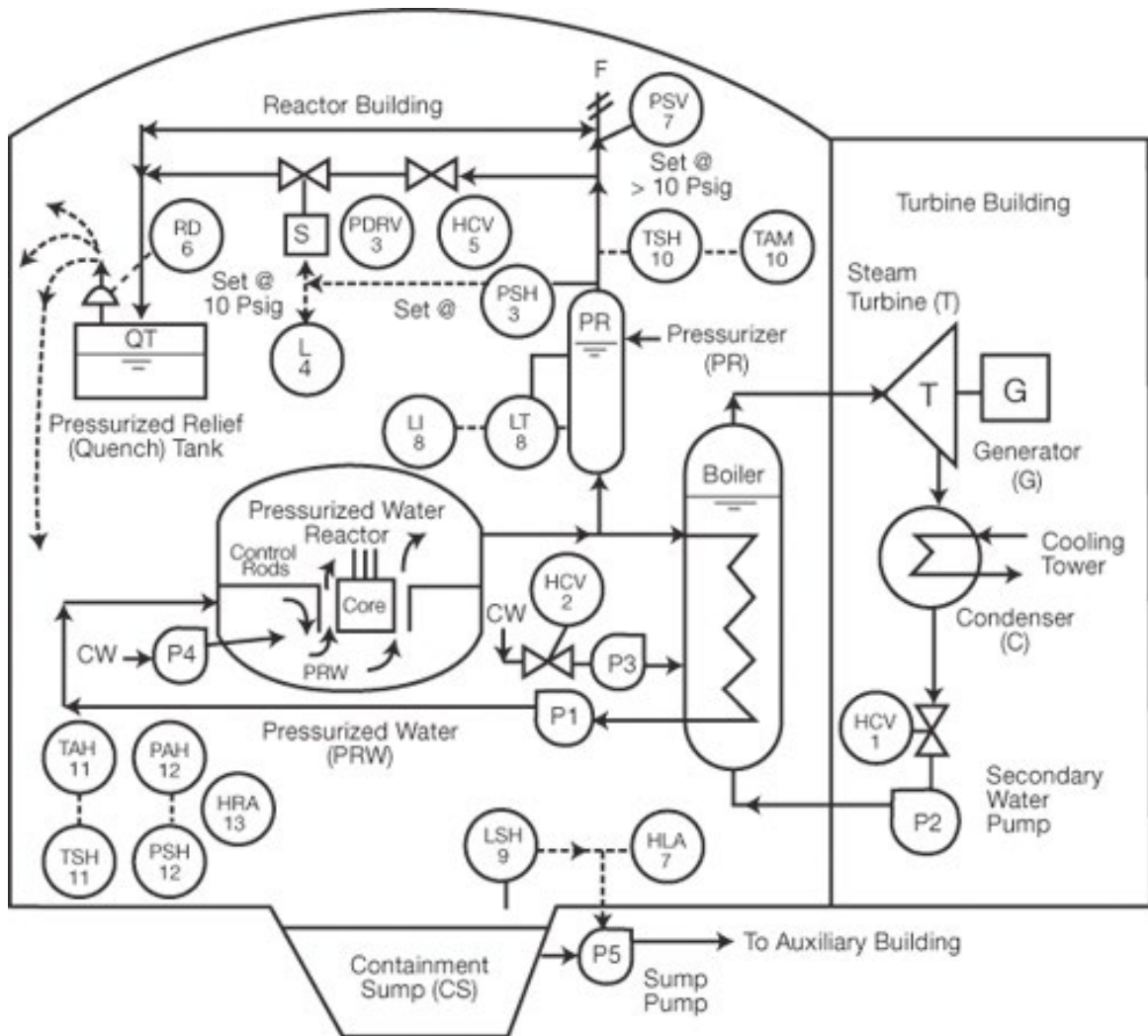
Lipták describes the sequence of events and the primitive controls that led to the Three Mile Island accident

By Béla Lipták

At 4 a.m. on March 28, 1979, Unit 2 of the 900-MW reactor at the TMI-2 plant at Three Mile Island in Pennsylvania experienced a partial core meltdown. Between 13 and 43 million curies of radioactive krypton gases were released, half the core melted, and 90% of the fuel rod cladding was destroyed. The maximum offsite radiation reached 83 millirem, but the radiation dose received by the community was small.

Figure 1 shows the main components of the plant and the instrumentation that had a role in the accident (other instrumentation has been eliminated from the drawing). This simple process consisted of three heat transfer loops, located from the left to the right in the figure. The first or “primary” loop transfers the heat generated by nuclear fission into the high- pressure reactor cooling water (PWR). The heat from this closed circuit is transferred into the “secondary” feed water loop that takes it into the steam boiler. The steam is used to generate electricity in the turbine generator, while the waste heat from the condenser is sent to the cooling tower.

Here, I will describe each “domino” in the sequence of events that led to this accident and contributed to the public distrust of nuclear energy. After each event, I will note in parenthesis how properly designed process control systems and better operator training could have prevented the accident.



1) Operators working on an upstream demineraliser at 4 a.m. unintentionally caused one or more of the three HCV-1 valves to go to “fail-closed” by accidentally admitting water into the instrument air system. The valves were badly designed because all valves on cooling applications should fail open. In addition, the operators did not realize that the valve(s) had closed. (Remedy: Select valve failure position correctly, and

do not allow water or anything but air into the instrument air system. Add an electric motor-actuated parallel backup valve and provide limit switches on all valves with status displays and alarms in the control room.)

2) This caused the main feed water pumps (P2) to stop. (Remedy: Provide bypass valve(s) around HCV-1 and automatically open them if HCV-1 should be open and it is not., On all automatic valves in the

plant, provide limit switches that trigger alarms if the valve doesn't take the automatically requested position).

- 3) Because the secondary feed water was stopped, the heat from the primary reactor coolant water (PRW, circulated by P1) was no longer being removed. This caused the temperature to rise and the reactor to scram (control rods inserted to cease fission). (Remedy: Alarm and automatically open HCV2, start the auxiliary feed water pump(s) P3, and actuate high-temperature alarm on the PRW inlet.
- 4) The reactor that was shut down continued to generate "decay heat," and the stationary secondary water in the boiler quickly turned into steam. This automatically started the emergency cooling water pump (P3), but that did no good because valve(s) (HCV-2) were also failed closed because of the water in the instrument air supply line. (Remedy: Same as in 1, plus provide safety interlock that automatically starts a backup pump and opens its valve if P3/HCV2 fails to respond.)
- 5) Next, the PRW temperature and pressure in the reactor started to rise. The high-pressure switch (PSH-3) on the pressurizer tank opened the pilot-operated relief valve (PORV-3), which started to relieve the PRW water into the quench tank (QT). When the pressure dropped and PSH-3 signaled PORV-3 to close, it remained open. (Remedy: The selection of fail-in-last position valve was wrong, so use designers who know how to select valve failure positions. Also automate the block valve HCV5 with an electric motor and close it if PFH-3 signals PORV-3 to close and it does not).
- 6) The operators did not know that PORV-3 was stuck open because the status light (L-4) was hidden from their view and because it was not operated by a limit switch on the valve, but only by the PSH-3 signal to the valve actuator solenoid. (Remedy: Place limit switch on PORV-3, and alarm if the valve status conflicts with the signal from PSH-3).
- 7) As a consequence of the discharging steam to the quench tank (QT), the reactor pressure dropped, causing more steam to flash. When the quench tank filled, its rupture disk (RD-6) burst, and steam and PRW were released into the containment building. (Remedy: The quench tank should have had high-pressure and level alarms in addition to an inlet flow detector.)
- 8) The worst design error was that the pressurizer (PR) level indication (LI-8) was based on volume, not mass. There-

fore, as steam pockets formed near the core, the PRW volume in the reactor increased, which in turn pushed more water into the pressurizer. Therefore, LT-8 indicated the level to be high when, in fact, the amount of water in the system was dropping. (Remedy: This “inverse response” must be corrected by measuring the weight of the water column between the bottom of the reactor and the top of the pressurizer by a d/p cell, which would indicate when boiling occurs, because the detected column weight drops).

9) Yet another reason why this control system failed was that the presence of water covering the core was not measured. (Remedy: Use capacitance or radar level detectors to detect if the core is uncovered and if it is, automatically start the emergency high-pressure injection pump P4.)

10) Detecting low pressure in the reactor started the emergency core cooling pumps (P4), but the operators trusted the pressurizer level (LI-8) indication, which was getting high, and cut this flow to a minimum. This sped up the melting of the core. (Remedy: Detect the weight of the water column, described in Step 8 above).

11) By 4:11 a.m., the quench tank (QT)

overflowed, and started to spill water and steam into the containment sump (CS). By 4:13 a.m. the sump overflowed and LS-9 triggered a high-level alarm (HLA-8) and started sump pump P5, which sent the radioactive water into an auxiliary building. This, together with the high-temperature alarm at the pressurizer outlet (TAH-10) plus the high-temperature (TAH-11) and high-pressure alarms (PAH-12) in the containment building, should have triggered a general alarm, but it was ignored, because the operators did not trust any of the alarms. By 4:15 a.m., the quench tank filled, its relief diaphragm ruptured, and radioactive coolant started to leak into the containment building, until at 4:39 a.m., the operators stopped the sump pumps. (Remedy: Increase reliability of safety alarms and thereby operators’ trust by using back-up, voting or medium selector sensors.)

12) At around 5:30 a.m., the RPW pumps (P1) started to vibrate—probably due to cavitation as the steam bubbles in the water collapsed—and to avoid vibration damage, the operators stopped these pumps (P1). This further reduced core cooling and increased steam formation. By 6:00 a.m., the reactor core overheated, and the zirconium cladding on the uranium fuel rods

reacted with the steam to form hydrogen, which further damaged the fuel rods. The operators did not believe the alarms in the containment building. (Remedy: Use redundant alarm switches.)

13) At 6 a.m. a new shift started, but the old shift still did not know what was going on, and therefore was unable to inform them of the plant's status. (Remedy: The status of all equipment and variables should be continuously displayed for the whole plant.)

14) At 6:30 a.m., the new shift realized that PORV-3 was open and (after the loss of 32,000 gallons of radioactive coolant), closed its block valve (HCV5). At 6:45 a.m. the badly located radiation alarm (RAH-13) actuated, and at 6:56 a.m. a site emergency was declared. The operators still did not realize that the low water level in the reactor exposed the core. Finally, at 11 a.m. the addition of coolant into the reactor started. In the afternoon, the pressure in the containment building spiked to 29 PSIG, probably caused by a hydrogen explosion from the zirconium-steam/water reaction. At 8 p.m. the primary pumps (P1) were restarted, and the core temperature began to fall. (Remedy: Better operator training).

Conclusion: To properly control a process, it must be fully understood. Also, in nuclear environments, instrumentation reliability must be guaranteed by multiple sensors and must be designed to withstand severe accidents. The controls must be designed by competent process control professionals, operators must be well-trained and hydrogen recombiners should be provided in the containment building. Last, but not least, Murphy's Law must always be honored.