Axiomatic Design Aspect of the Fukushima-1 Accident: Electrical Control Interferes with All Mechanical Functions (Draft version)

Masayuki Nakao (1), Kohei Kusaka, Kensuke Tsuchiya and Kenji Iino

Abstract: The independence axiom recommends independence among all functional requirements. Modern machines, however, are all driven by electrical power that follow commands from computers with algorithms dependent on instrumentation signals; electrical functions interfere with all mechanical functional requirements. Moreover, a typical machine loses its entire function when its single electrical system fails. The Fukushima-1 accident followed this exact scenario; the tsunami destroyed all power supplies and switchboards, then all pumps and valves turned inoperable from the control room. The failures led to loss of cooling functions and eventually to core damages. This interference is a fundamental design problem with modern machines.

Keywords: Axiomatic; Design; Failure

1. Introduction – Mechatronics Accidents

As of 2013, a glance at machines produced in modern countries reveals that they all have electrically driven control systems to operate their mechanisms in an ideal manner. The most common design employs "mechatronics" that operate mechanisms with electrical power controlled by digital signals. In other words, most machines have computers that estimate the state based on signals from sensors to optimally drive mechanical actuators. Mechatronics is now not only applied for robotics and automated factories, but also for appliances like TVs, cellular phones, washing machines, and air-conditioners as well as larger machines like automobiles, trains, and machining tools. The only traditional machine left in our daily life that does not rely on any electrical control is probably just the bicycle.

The big concern with a mechatronic machine is that it only has one set of a complex electrical control system, just like human having only one brain; when the control system fails, the entire machine no longer meets its functional requirement, like brain-death in our case. In fact, a single electrical point of failure, e.g., CPU, battery, capacitor, relay, connector or sensor, would cause confusion in the mechanism control leading to an accident due to failure in the mechanical functional requirement assigned to

the mechanism [1] [2]. For example, the 2010 recall by Toyota was in response to a runaway accident that a stepped-on gas pedal did not spring back to its off position. The computer was suspected to have continued to output a throttle-full-open signal but even NASA's investigation did not reproduce the failure situation. Even the designer cannot easily find whether a program of over 10 million lines contain a bug or not.

Upon failure of a mechatronic machine, human not equipped with the eye to capture the flow of electrons and without the overall picture of the system cannot patch up a quick fix. Even an engineer with Ph.D. cannot repair a malfunctioning washing machine, unless the problem is with the washing tub or a bent rotary shaft that the doctor can repair by hammering it in the right shape. If, however, the problem resides in the program or the electrical circuit, the engineering doctor cannot even bypass an interlock nor identify which electrical part has failed its function.

To overcome this difficulty, a mechatronic machine requires another mechatronic machine for its repair work. At an automobile garage, for example, even a skilled mechanic cannot identify a troubled sensor without an automatic diagnosis system. A railway control system depends on the automatic railway checking system to monitor the status of hundreds of railway signals and switches every few seconds. A system failure, probably caused by a tiny glitch in a circuit element, however with a significant consequence of stopping numbers of lines, will never pinpoint its exact cause without the automated diagnosis system and keep the neighboring lines down for hours. Another example is driving recorders mounted on automobiles and trains, these days, to record images, velocities and other data for a period of 1 minute or so immediately before and after abrupt braking. Our accident investigation without them will keep us wondering in the guessing game, just like in the old days. Such an environment is vulnerable to a power outage; for the first example, without the mechatronic diagnosis machine, the mechanic at a garage will probably have to throw his hands up and take a long break waiting for the electricity to come back on.

The radioactivity release accident at Fukushima-1 Nuclear Power Plant (Fuku-1 NPP) that broke out in March of 2011 was another one of such mechatronics failure. The accident took place with outdated boiling water reactors (BWR) designed by General Electric (GE) in the 1970s. Their base mechatronics electrically processed analog signals to drive mechanisms like pumps or valves, and upon losing all DC power sources, the operators lost the sensor readings and ways of remotely operating the valves. Even when

nuclear reaction is suppressed, the fuel keeps generating decay heat and the fuel rod damage is said to start within 3 hours following loss of water supply to a BWR reactor pressurized vessel (RPV). For Fuku-1 NPP, when the operators lost control of the reactor, the cooling that had to recover within hours relied on “manual” operations and insufficient hands inside the dark buildings could not stop the core damage.

This paper aims at finding ways to protect mechatronics machines from fatal damages. For this purpose we analyze the Fuku-1 NPP accident in Chapter 2. Chapter 3 then shows that mechatronics are coupled designs from the axiomatic design aspect, and Chapter 4 suggests design methods to avoid catastrophes.

2. Cause analysis of Fuku-1 NPP accident

A number of accident reports have been made available in Japanese and in English [3][4] about the Tokyo Electric Power Company (TEPCO) owned Fuku-1 NPP accident. The plant, still under high radioactivity, has not gone through thorough visual inspection and all these reports based their analyses on plant data during the accident, made public by TEPCO, and testimonies by TEPCO workers and the government, and thus reached similar technical conclusions about the accident causes.

The direct cause of the accident was the tsunami waves and not the earthquake. When the magnitude 9.0 earthquake hit at 14:46 (Japan Time) on March 11th, 2011, external power was lost due to failures of power line towers and switches, however, the operators had confidence in reaching the state of cold shutdown by just following the manual using emergency diesel generators and high pressure cooling functions. Damages on the RPV itself and its piping were not large enough to release detectible radioactivity to the environment.

52 minutes after the earthquake, a huge tsunami reaching as high as 15m, never marked in history or land since 869, hit the plant. Almost all emergency diesel generators, AC switchboards, and DC batteries for control at Fuku-1 NPP were submerged under water. The result was station blackout (SBO). The electrical power vehicles rushed to the site, however, were useless due to loss of switchboards. It took 10 days to recover AC power. In place for 125V DC power, TEPCO collected 24V bus batteries and 12V car batteries from their employees to hook up to sensors and valves, however, they needed hundreds of them; a number far beyond what were available on the site by March 13th.

The engineers, at the time, were following the planned emergency procedures in Figure 1 to reach cold shutdown even without AC power. The scenario was to start the high pressure cooling system to inject water into the RPV using the high pressure steam in the RPV, prepare the low pressure cooling systems while the high pressure was operating until it would stop due to lowered steam pressure, and then kick in the low pressure cooling systems. These high pressure systems were the Isolation Condenser (IC: condenses steam into water to return to the RPV with gravity) for Unit-1, and for Unit-2 and 3, the Reactor Core Isolation Cooling (RCIC) or the High Pressure Coolant Injection system (HPCI) that turn turbines with steam to run pumps to inject cooling water.

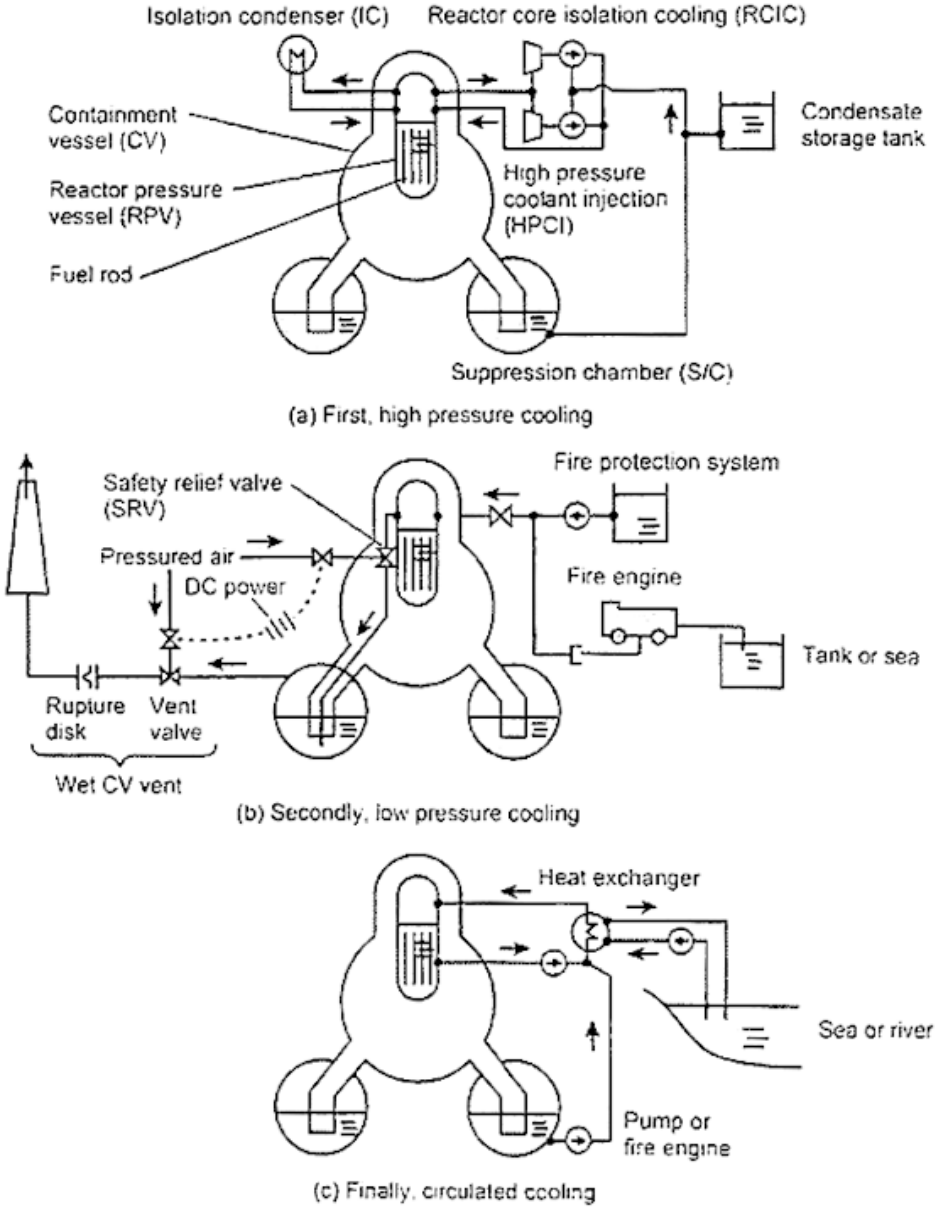

Figure 1 Emergency cooling procedure of a BWR nuclear power plant

RCIC for Unit-2 and 3 were for emergency use and the circuits were designed to “Fail as is” and upon losing DC power after the tsunami, the valves remained open to keep the RCIC running. The IC system for Unit 1, on the other hand, was designed so its valves would “Fail Close” and the loss of DC power after the tsunami closed the valves; a situation that is the same as when the piping broke. Water in Unit-1 RPV then evaporated to lower the water level and as the simulation predicted, fuel rod damage started around 19:00 on the 11th. GE had designed the IC as a system for RPV depressurization to operate under normal conditions and had adopted “Fail Close” to avoid human errors. TEPCO, on the other hand, normally used Safety Relief Valves (SRV) for RPV depressurization and the IC, for 40 years, only worked during testing and none of the plant workers recognized this interlock.

The General Manager of Fuku-1 NPP issued instructions, in the early stage of an hour and a half from the tsunami, to “Prepare a low pressure cooling system using the fire engines while this high pressure system was running.” Japanese nuclear power plants had prepared, several years ago, water fillers from outside the buildings to counter fires inside them. The workers had opened some of the valves in preparing piping routes for water injection into the RPV on the same day. Instructions from the General Manager would have required the following additional valve operations. Open the SRV of the RPV to release steam into the Containment Vessel (CV), and then open the CV vent valves to exhaust the steam into the atmosphere. This procedure would lower the RPV pressure from 7 MPa to about 0.5 MPa to allow 1 MPa water injection from the fire engines into the RPV. Nuclear power plant engineers are all familiar with this procedure and all the eight power plants at Fukushima-2, Onagawa, and Tokai completed it to successfully reach cold shutdown.

The SRVs, however, are inside the CV and vent vales are directly above the donut shaped suppression chamber and they require DC power and compressed air to open. Compressed air is generated by a compressor run by AC power. Each plant of Fukushima-2, Onagawa, and Tokai, even after the tsunami, had at least one AC power available to supply the needed electricity. Whereas, Fuku-1 NPP was out of them and the delay in the procedure caused core damage on the 14th to Unit-2 and 13th to Unit-3. If they had prepared a large number of 12V batteries for automobiles and an engine operated compressor or a compressed air bottle beforehand, and the operators had rushed to the locations within an hour to open the valves,

Unit-2 and –3 would have survived the disaster to reach cold shutdown without damaging their cores.

In any case, this accident revealed that Japan had historically lacked the proper safety culture for the people in the country and to overseas. Nuclear Safety Commission of Japan in 1993, had decided that a loss of AC power that lasts over 30 minutes do not require assessment because such an event would not happen and a total loss of switchboards and DC power were not even discussed for evaluation. In the United States, on the other hand, after the 2001 terrorist attack on the World Trade Center, nuclear safety was reviewed and in 2006, NRC issued Advisories and then Orders with Section B.5.b [5] to, e.g., design valves so they can be opened by hand or store portable power supplies and air bottles near the valves [U.S. NRC, 2006]

The amount of radioactivity released with this accident was, according to a TEPCO announcement, 900 PBq iodine equivalent, i.e., 17% of that of the Chernobyl accident that released 5,200 PBq. The announced release was further broken down into 5 PBq at the times of the hydrogen explosion, 1 PBq upon wet venting, and about 900 PBq (about 100%) due to leakage from the piping joint seals when the CV reached high temperature. Radioactivity drops to about 1% when the carrier material passes through water. If the wet venting had succeeded, the radioactivity release would have been about 1 tenth of the announced amount even with damaged fuel rods.

3. Axiomatic design analysis of mechatronics coupled design

This section illustrates the problem of electronics interfering with mechanisms with Suh's axiomatic design.

The independence axiom states that an ideal design has Design Parameters (DP) so that each Functional Requirement (FR) maps to a single DP in a one-to-one manner. The design matrix for this uncoupled design is diagonal as Figure 2(a) shows. In reality, the designer, from efforts to cut cost, often selects off-the-shelf parts, with unwanted features and secondary Constraints (C), that affect other FRs to complicate an uncoupled design or even make it impossible. An example is a bicycle that uses off-the-shelf chain and sprocket to meet the FR of transferring torque from the pedals to one of the wheels. The DP of chain and sprocket, however, affects the FR of shifting the transmission and imposes the C of keeping adequate tension in the chain. The DP interference to another FR and additional C forces the designer to struggle for the optimum solution with all factors under consideration.

Many machines, nonetheless, are designed to the next-best decoupled design as Figure 2(b) shows. For such decoupled designs, the designer from the one-to-one relation of FR1 and DP1, finds DP1 to satisfy FR1. He then substitutes the DP1 to the one-to-two relation of FR2 to DP1 and DP2 to determine DP2, and similarly substitutes the set DP1 and DP2 into the FR3 to DP1, 2, and 3 relation to determine DP3. Arranging the process of determining DPs in such a manner allows easily coving all DPs. The design matrix is then is an upper or lower triangular matrix.

In contrast, if the machine design is coupled like Figure 2(c) shows, the design matrix is non-triangular with components in both upper and lower parts forcing the designer to simultaneously solve a set of design equations. Repairing such a machine or modifying one of its DP would interfere with multiple FRs and result in making changes to multiple DPs at the end. The machine is difficult to work with in terms of service and sooner or later disappears from the market.

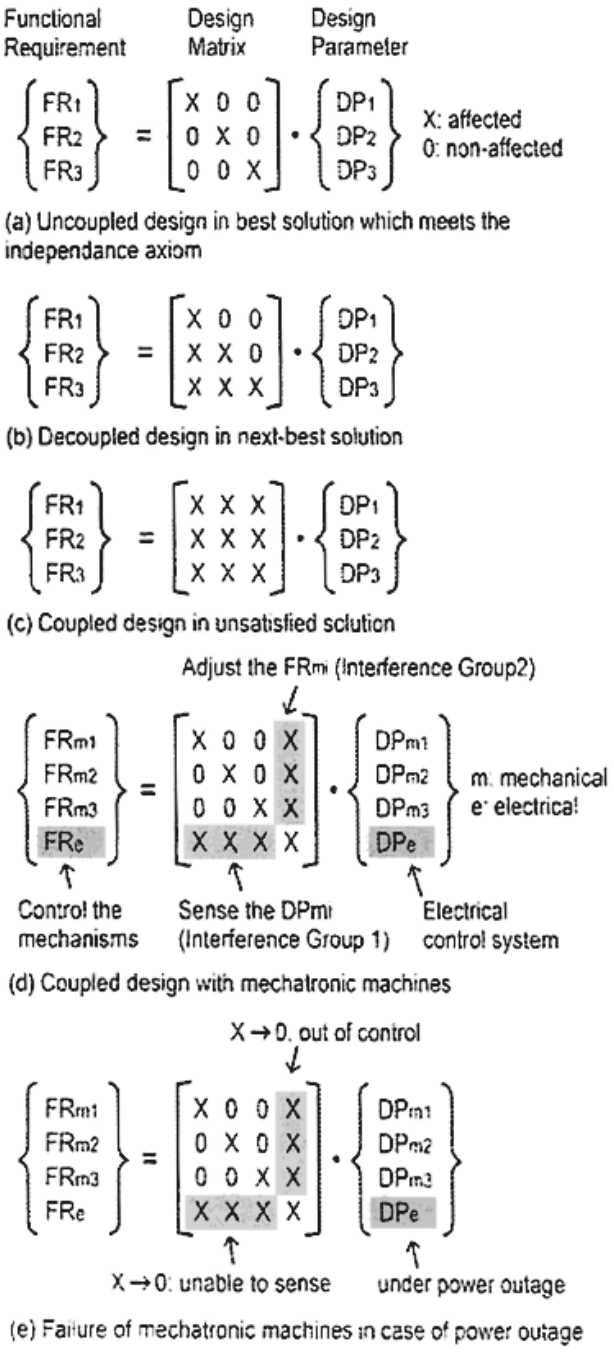

Figure 2 Interference of FRs of mechatronic machines in Axiomatic Design

Now let's turn our attention to a mechatronic machine. The design is certainly coupled. Figure 2(d) shows the FRe of electronically controlling the

machine (not in an open way but with feedback) that is affected by the sensing status of all mechanisms DPm (all the effects are shown in the lower left-hand corner of the design matrix, Interference Group 1). The electrical control system DPe affects all functional requirement elements FRm via controlling the actuator movements (the effects appear as Xs in the upper right-hand corner of the design matrix, Interference Group 2). The resulting design equation clearly shows a fully coupled design with nonzero components in the upper and lower areas of the design matrix.

In developing such a mechatronic mahine, tweaking the DPe in the program for electronic controlling allows minor changes in the mechanical FRm during the final stage of development. Such adjustments may cause small variations in the mechanical functions, however, each mechanism is tuned to the best state. This is the biggest advantage of mechatronics. On the other hand, such a structure reveals the disadvantage of coupled design that upon exchanging a single failed mechanical part will require readjusting the entire system with another automatic diagnosis mechatronic machine.

Figure 2(e) shows yet another disadvantage of coupled design uncovered at a time of emergency. For Interference Group 1 described above, when DC power is lost, the sensors are stuck at low output and the electronic control system upon receiving such signals will enter an abnormal state to either cause runaway actuators or force shutdown with interlocks designed to the safe side. The later was the case with Fuku-1 NPP accident. Mechatronics with feedback control all have such interlocks, for example, parallel drive mechanisms are designed to stop the motor when an encoder signal line brakes or short-circuits.

Similarly with regards to Interference Group 2, when the electrical system fails due to some external disturbance, all mechanical FRm turn uncontrollable or stop in response to the emergency situation. When, for example, the DC power for semiconductors is lost, the control circuit fails and mechanical actuators either runaway or stop with interlocks to land them in their safer side. A system designed to produce DC power by rectifying AC will face the most dangerous moment upon a power outage when its mechanisms runaway before the interlocks kick in. In 2006, a boat with a crane accidentally cut a TEPCO power cable while it was traveling in a river and the city of Tokyo suddenly lost power. Network servers that could not counter the accident without enough time for capacitors or batteries for gentle shutdown froze immediately, and a large number of corporations had to devise Business Continuity Plans to cope with their loss of records.

4. Plans to save mechatronics machines from fatal accidents

Multiplicity and variety of emergency safety systems are said to save machines from fatal accidents. Nuclear Safety Commission of Japan has imposed multiplicity or variety and Fuku-1 NPP had enforced multiplicity. For example, it had multiple external power lines and emergency diesel generators, in addition to switchboards shared with the adjacent units, however, their functions were all washed away by the tsunami. When they lost DC power, workers were faced with the situation that all safety mechanisms requiring electricity failed.

What we need is to add variety. For example: Install a mechanical safety system that does not require electricity (e.g., a handle for manually opening a valve by hand. Even the safety valve inside the CV can be opened with a handle equipped with a long shaft to turn it from outside the CV); dispatch an electrical power supply vehicle stationed at high elevations to feed power to a backup switchboard built also at high elevations; release water from a reservoir at a high elevation to drop cooling water with gravity for cooling from outside the CV; build floating nuclear power plants in the ocean to submerge the CV under the sea; and so on. In fact, Fuku-1 NPP had planned some variety like low-pressure water injection from a fire engine. If that were even lost, the RPV would have ruptured to release about 10 times the radioactivity.

Figure 3 explains the concept with axiomatic design. Prepare manually operated valve openers FRms monitored with human eyes to replace electrically operated FRe when they fail. The return of Apollo 13 in 1970 is a good example of FRms. When its oxygen tank exploded and the power generation system failed, the astronauts controlled the angle of atmosphere reentry by watching the earth from a small window. During the great east Japan earthquake, a control system, originally designed to generate AC power to sell to TEPCO by converting solar generated DC power, failed due to the power outage, however, the system had terminals to directly output DC power and they helped the plant workers during their recovery efforts by offering DC power for charging cellular phones and for boiling water. Radios and flashlights charged by manually turning handles helped the people for extended hours. Recent advancements with devices for electrical motors allow acceleration, braking and stop position control using electricity from regeneration brakes. They are used for the super-expresses and other trains, elevators in high rises, and linear motors for machining tools. Nevertheless, all these machine are also equipped with large friction brakes in case of

emergencies and terminals have large cushion dampers called buffer stops to avoid collision or trains running off the end in the unlikely case of them running away without brakes.

A senior mechanical engineer has to learn about electrical control. Design in the coming years will be more demanding that the designer has to plan how to safely stop machines in case its control system fails. Many young researchers in the field only know the design of mechatronics. Mechatronics is certainly a convenient methodology that applies to almost any machine, however, that alone does not enrich the design and carries with it the danger of blocking the designer's ideas for such mechanical safety measures we explained above.

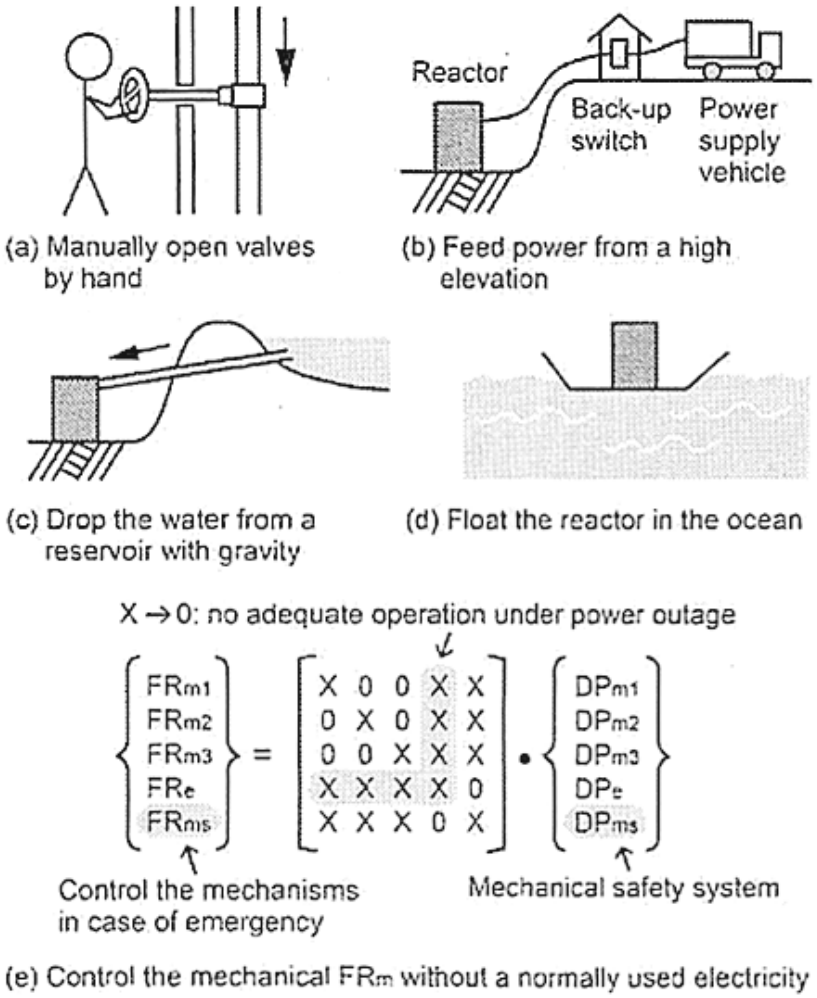

Figure 3 Mechanical safety system to avoid catastrophes

5. Conclusion

We studied the Fuku-1 NPP accident to find that electrical control interferes with mechanical functional requirements and if it fails in case of emergency, mechanisms turn uncontrollable. From the viewpoint of axiomatic design, we showed that machines controlled with electrical feedback are coupled designs and that decoupling such electrical interference requires design solutions with mechanical control to prevent runaway mechanisms that have lost electricity. These types of coupled designs are fundamental problems with modern machines. We are concerned that if young researchers study only mechatronics design methodologies, they will fail to implement purely mechanical safety measures for cases of emergency.

References

[1] Eppinger, S., Browing, T., Design Structure Matrix Methods and Applications, The MIT Press, 2012

[2] Hatamura, Y., Iino. K., Tsuchiya. K., Hamaguchi. T., "Structure of Failure Knowledge Database and Case Expression," Annals of the CIRP, 52(1), pp.97-100, 2003

[3] IAEA (International Atomic Energy Agency), "IAEA International Fact Finding Expert Mission of the Fukushima Dai-ichi NPP Accident Following the Great]East Japan Earthquake and Tsunami," 2011. http://www-pub.iaea.org/MTCD/meetings/PDFplus/2011/cn200/documentation/cn200_Final-Fukushima-Mission_Report.pdf

[4] INPO (Institute of Nuclear Power Operations) "Lessons Learned from the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station," 2011. http://www.nei.org/filefolder/INPO_11-005_Fukushima_Addendum_1.pdf

[5] Nakao, M., Miyamura, T., Tsuchiya, K., Iino, K., "Two Design Problems Identified in Consumer Product Recalls: Degradation over Extended Use and Scarce FR-Coupling," Annals of the CIRP, 59(1), pp. 163-166, 2010.

[6] Suh, N.P., Axiomatic Design: Advances and Applications, Oxford University Press, 2001.

[7] U.S. NRC (United States Nuclear Regulatory Commission), "B.5.b Phases 2 and 3 Submittal Guideline," Engineering and Research, Inc. NEI 06-12, Revision 2, 2006