Proceedings of ICAD2013
The Seventh International Conference on Axiomatic Design
Worcester – June 27-28, 2013
ICAD-2013-17

AXIOMATIC DESIGN ASPECT OF THE FUKUSHIMA-1 ACCIDENT: ELECTRICAL CONTROL INTERFERES WITH ALL MECHANICAL FUNCTIONS

Masayuki Nakao
nakao@hnl.t.u-tokyo.ac.jp
Department of Engineering Synthesis
School of Engineering
The University of Tokyo
Hongo 7-3-1, Bunkyo-ku, Tokyo, 113-8656, Japan

Kohei Kusaka
kusaka@mech.t.u-tokyo.ac.jp
Department of Engineering Synthesis
School of Engineering
The University of Tokyo
Hongo 7-3-1, Bunkyo-ku, Tokyo, 113-8656, Japan

Kensuke Tsuchiya
tsu@iis.u-tokyo.ac.jp
Department of Mechanical and Biofunctional Systems
Institute of Industrial Science
The University of Tokyo,
Komaba 4-6-1, Meguro-ku, Tokyo, 153-8505, Japan

Kenji Iino
kiino@sydrose.com
SYDROSE LP
475N. 1st St., San Jose, CA, 95112, USA

ABSTRACT

The independence axiom recommends independence among all functional requirements. Modern machines, however, are all driven by electrical power and 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. Delayed counteractions led to a loss of cooling functions and eventually to core damage. This interference is a fundamental design problem with modern machines.

Keywords: Axiomatic Design, failure, Fukushima.

1 INTRODUCTION – MECHATRONIC 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 complex electrical control system, just like humans have 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 [Hatamura *et al.*, 2003; Nakao *et al.*, 2010]. For example, the 2010 recall by Toyota was in response to a runaway accident caused when 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, humans not equipped with the eye to capture the flow of electrons cannot patch up a quick fix. Even an engineer with a Ph.D. cannot repair a malfunctioning washing machine, unless the problem is with a dented 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 to pinpoint a tiny glitch in their circuits. Another example is accidental driving recorders mounted on automobiles or trains to record images, velocities and other data for a period of 1 minute before and after abrupt braking. Such an environment is vulnerable to a power outage; not only the mechanical machine itself, but also its mechatronic diagnosis machine could stop completely.

The radioactivity release accident at Fukushima-1 Nuclear Power Plant (Fuku-1 NPP) that broke out in March of 2011

was another such mechatronic 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. 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 reactor pressurized vessel (RPV) of BWR. For Fuku-1 NPP, when the operators lost control of the reactor, the cooling that had to recover within hours relied on "manual" operations, but insufficient slow hands inside the dark buildings could not stop the core damage.

This paper aims to find ways to protect mechatronic machines from fatal damage. 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 perspective, and Chapter 4 suggests design methods to avoid catastrophes.

2 CAUSAL ANALYSIS OF FUKU-1 NPP ACCIDENT

A number of accident reports have been made available in Japanese and in English [IAEA, 2011; INPO, 2011] about the Fuku-1 NPP accident. The plant, still under high radioactivity, has not gone through thorough visual inspection. All these reports based their analyses on plant data during the accident, made public by Tokyo Electric Power Company (TEPCO) owned Fuku-1 NPP, 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 as mentioned later. 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 13.1m, never marked in history since 869, hit the plant at 10m elevation. 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. The electrical power vehicles rushed to the site, however, were useless due to the loss of switchboards. It took 10 days to recover AC power. In place for 125V DC power, TEPCO collected 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. First, they start the high pressure cooling system to inject water into the RPV using the high pressure steam in the RPV. These systems were the Isolation Condenser (IC) which 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 (HPCI) that turn turbines with steam to run pumps to inject cooling water. Secondly, they depressurized the RPV and made up the piping route for low pressure cooling until the high pressure cooling could stop due to lowered steam pressure, and then kick in the low pressure cooling systems. Finally, they changed to the circulated cooling system to remove the heat to the sea with a heat exchanger, reaching cold shutdown.

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 coupled 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 plugs for fire engines 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 at night on the 11th. Instructions from the General Manager would have required the following additional valve operations: as shown in Figure 1 (b), 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 the vent vales are directly above the donut shaped suppression chamber (S/C). These valves are too large to operate by hands; they require DC power and compressed air to open and keep opening against the spring. Compressed air is generated by a compressor run by AC power. Both the SRVs and the vent valves are coupled with the electrical power. Each successful plant, 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 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 the Japanese nuclear industry had historically lacked the proper safety culture even for a low-probability but high-loss accident. The Nuclear Safety Commission of Japan in 1993, had decided that a loss of AC power that lasts over 30 minutes does 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 (U.S.), on the other hand, after the 2001 terrorist attack on the World Trade Center, nuclear safety was reviewed and in 2006, the Nuclear Regulatory Commission issued Advisories and then Orders with Section B.5.b 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 equivalents, 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 explosions, 1 PBq upon "wet" (filtered radioactive elements through the water) CV venting from S/C, and about 900 PBq (about 100%) due to leakage from the piping/wiring joint seals when the CV was exposed to high pressure and high temperature. Making up the CV vents of Unit-2 and -3 were delayed for several hours even after opening vent valves because the rupture disks (Figure 1 (b)), whose brakeage pressure was twice of the nominal CV pressure, were not broken easily. This released radioactivity was strongly coupled with the delayed breakage of the rapture disk. BWRs in the U.S., on the other hand, didn't have any rupture disks for early venting [INPO, 2011]. Radioactivity drops to about 1% when the carrier material passes through water. If the wet CV venting had immediately succeeded, the radioactivity release would have been about 1 tenth of the 900 PBq.

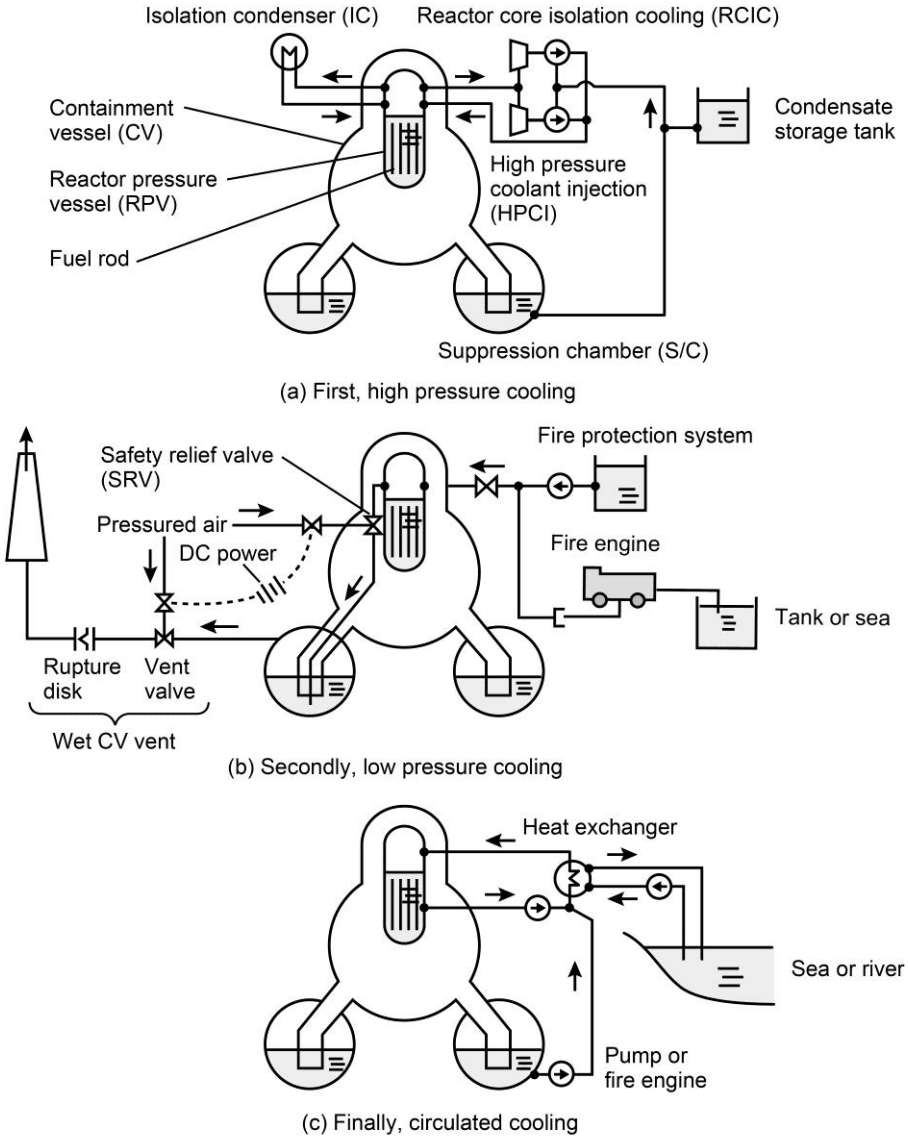

Figure 1. Procedure of cooling of nuclear power plant of BWR in case of emergency.

3 AXIOMATIC DESIGN ANALYSIS OF MECHATRONICS COUPLED DESIGN

This section illustrates the problem of electronics interfering with mechanisms using Suh's Axiomatic Design [Suh, 2001].

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 often selects readily available but redundant parts that affect other FRs or constraints (C) to complicate an uncoupled design or even make it impossible. An example is a bicycle that uses the DP of readily available chain and sprocket to meet the FR of transferring torque from the pedals to one of the wheels. This redundant DP, however, affects another FR of shifting the transmission and imposes the additional C of keeping adequate tension in the chain.

Many machines, nonetheless, are designed to the next-best decoupled design as Figure 1 (b) shows. For such decoupled designs, the designer from the one-to-one relation of FR1 and DP1, finds DP_1 to satisfy FR_1. He then substitutes the DP_1 to the one-to-two relation of FR_2 to DP_1 and DP_2 to determine DP_2, and similarly substitutes the set of DP_1 and DP_2 into the FR_3 to DP_1, DP_2, and DP_3 relation to determine DP_3. Arranging the process of determining DPs in such a manner allows all DPs to be easily solved. The design matrix is then is an upper or lower triangular matrix.

In contrast, if the machine design is coupled like Figure 1(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. The information axiom states the information content of the coupled design is larger than that of the decoupled/uncoupled design, meaning the coupled is worse than the decoupled/uncoupled.

Now let's turn our attention to a mechatronic machine. The design is certainly coupled. Figure 1 (d) shows the FR_e of electronically controlling the machine (not in an open way but with feedback) that is affected by the sensing status of all mechanisms DP_m (all the effects are shown as Xs in the lower left-hand corner of the design matrix, Interference Group 1). The electrical control system DP_e affects all mechanical functional requirements FR_m 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. The long and unwelcome lines of Xs in Interference Group 1 and 2 cannot be decoupled easily and make the information content larger.

Design Structure Matrix (DSM) methods also mention a strong interaction among most components [Eppinger *et al.*, 2012]. It indicates the similar long and unwelcome lines of interactions in the matrix of component by component though the matrix is not the one of function by component in Axiomatic Design. DSM introduces four types of interactions: special proximity, material flow, information flow and energy transfer. Fuku-1 NPP included the problem of interactions of information flow and energy transfer for controls.

In developing such a mechatronic machine, tweaking the DPe in the program for electronic controlling allows minor adjustments in the mechanical FRm during the final stage of development. Such adjustments can make smaller variation in the performance of FRm; 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 upon exchanging a single degraded mechanical part will require readjusting the entire system. This complex readjustment needs another automatic diagnosis mechatronic machine. The modern designers employ the useful electricity for most of machines; however they ignore the implicit risk 3.

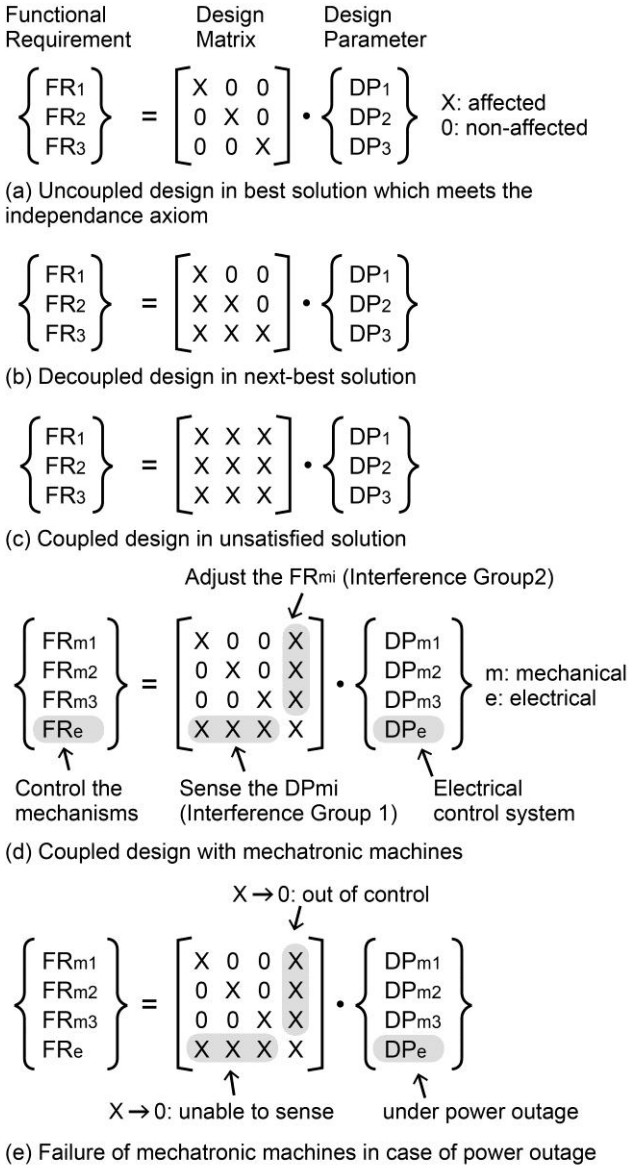

Figure 2. Interference of FRs of the mechatronic machines in Axiomatic Design.

Figure 1 (e) shows yet another disadvantage of a 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 IC of Unit-1 in Fuku-1 NPP accident. Mechatronics with feedback control all have such interlocks, for example, motor-driven mechanisms are designed to stop the motor when an encoder signal line brakes or short-circuits. Even the safety interlock may induce the worse situation after stopping the machine or cutting the electricity. In 1972, the electrical train with a burning dining car stopped in the long Hokuriku tunnel according to the operation manual in Japan; but the train could not evacuate from the tunnel after the fire melted the power line; 30 passengers died from smoke inhalation.

Similarly with regards to Interference Group 2, when the electrical control system DP_e fails due to some external disturbance, all mechanical FR_m turn uncontrollable or stop in response to the emergency situation like most of FR_m of Fuku-1 NPP except the "fail as is" systems. In the mechatronic machines, when 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 when its mechanisms run away upon a power outage just 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. Some network servers that could not counter the accident without enough time for capacitors or batteries for gentle shutdown froze immediately. A large number of corporations had to devise Business Continuity Plans to cope with their loss of business 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 eight external power lines and fourteen emergency diesel generators; however, their functions were all washed away by the earthquake and tsunami.

What we need is to add variety. As shown examples in Figure 3(a) to (d), we should install a mechanical safety system DP_{ms} that does not require normally used electricity: (a) handle for manually opening a valve by hand. Even the SRV inside the CV can be opened with a handle equipped with a long shaft to turn it from outside the CV; (b) dispatch an emergent electrical power supply vehicle stationed at high elevations to feed power to a backup switchboard built also at high elevations; (c) release water from a reservoir at a high elevation to drop cooling water with gravity for cooling from outside the CV; (d) build floating nuclear power plants in the ocean to submerge the CV under the sea in the accident; 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 (e) explains this concept with Axiomatic Design. The design matrix is still a fully coupled one; however, the information content could be decreased because the mechanical FRs can be controlled by the mechanical safety system DP_{ms} even after station blackout, meaning that the information content is not infinite any more. For example, to prepare manually operated valve openers FR_{ms} monitored with human eyes to replace electrically operated FR_e when they fail. The return of Apollo 13 in 1970 is a good example of FR_{ms}. When its oxygen tank exploded and the power generation system failed, the astronauts controlled the angle of atmosphere re-entry by watching the earth from a small window. During the great east Japan earthquake, a control system at home, originally designed to generate AC power to sell to TEPCO by converting solar generated DC power, failed due to the power outage; however, some systems had terminals to directly output DC power and they helped residents by offering DC power for charging cellular phones and for boiling water. Radios and flashlights charged by manually turning handles helped the people in a refuge. Recent electrical motors allow acceleration, braking and stop

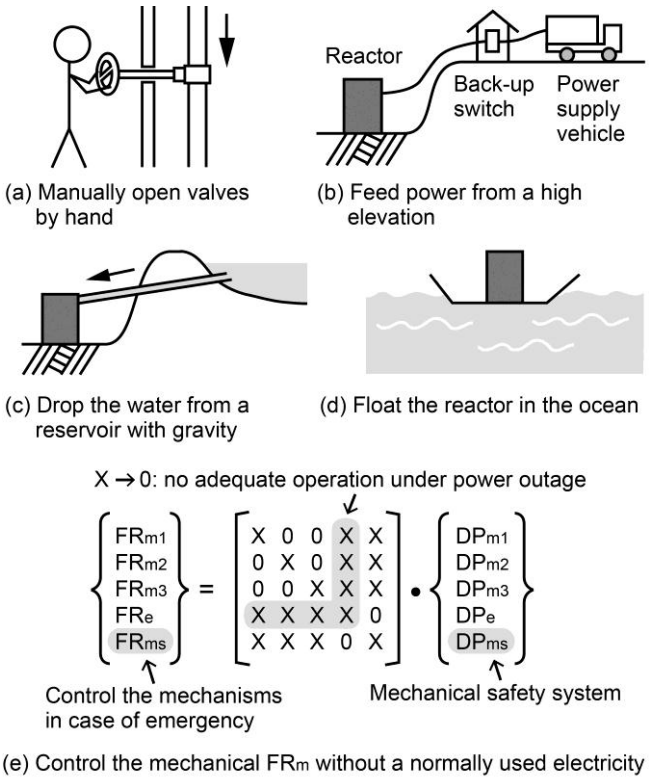

Figure 3. Mechanical safety system to avoid catastrophes.

position control using electricity from regeneration brakes. They are used for the super-expresses, elevators in high rises, and linear motors for machining tools. Nevertheless, all these machines are also equipped with large friction brakes in case of emergencies and terminals have large cushion dampers called buffer stops to avoid collision in the unlikely case of running away without brakes.

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 researcher*s* 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.

5 CONCLUSION

We studied the Fukushima-1 accident to find that electrical control interferes with mechanical functional requirements and if it loses electricity 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 compensating such electrical interference under blackout requires design solutions with an emergency mechanical control to prevent runaway mechanisms. The measures can reduce the information content of the coupled design.

These mechatronic types of coupled designs are fundamental problems with modern machines. We are concerned that if young researchers study only mechatronic design methodologies, they will fail to implement purely mechanical safety measures for cases of emergency.

6 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/corporatesite/media/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: Advanced and Application*, Oxford University Press, 2001.

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