Identifying Poor Designs with Conflicts in Design Parameters

Kenji Iino, Masayuki Nakao
The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
kiino@esc.u-tokyo.ac.jp

Abstract. Mechanical design is an act of defining machines that produce values to people; however, a poor design sometimes causes mechanisms to fail. Such failures can lead to harms to people, the environment, or both and in the worst case, it can even cause people’s death. Axiomatic design is a design tool that helps the designer come up with more stable and robust designs by identifying interference among parts. Taking a design through axiomatic analysis only at an abstract level, however, can miss finding interferences within. A product, through its lifetime, can also experience disturbances that the designer overlooked at the time of design. This paper discusses a trouble that arose with bicycles with a new safety feature of locking the front wheel when parked. The locking mechanism faced an unexpected part failure that caused the handle to lock while riding. Another topic is an inherent interference that existed from the very beginning of a design that the designers could not identify probably due to the extreme complexity of the system, the Fukushima Nuclear Power Plant-1, Unit-1. Analysis for evaluating how well a design will meet its functional requirement without trouble should go into the detail level, especially for all modes of operation, to avoid oversight of hard-to-find interferences and conflicts. This paper also suggests carrying out design analysis after production if phenomena, unexpected or unforeseen at the time of design, arise after a product is placed into service.

1. Introduction
Mechanical design is an intriguing act of defining shapes of new parts, how they assemble with machine elements and instrumentation to form new products, how the sub-assemblies interact with other sub-assemblies, or even defining complex systems like automobiles with tens of thousands of parts [1]. In this paper, we call the subject of design, a machine, regardless of its size or complexity, from a single part shape to a complex system.

The designer aims at providing value to the users, societies, or even the entire globe, however, responsibility comes with such development of machines to make sure they do not cause harm to the target users or the environment.

As complexity of our design grew with modern industrialization that started in the 18th century, assuring safety with design turned more challenging and since the latter half of the 20th century, people devised many analytical tools to help the designer keep the design trouble free. Such tools include finite element method for stress analysis, computational fluid dynamics to predict fluid flow behaviors, design review to take advantage of knowledge of more people, or quality control primarily to keep eyes on the manufacturing processes.

Design theorists, around this time, pointed out that the product cost and whether it will succeed in the market or not are almost determined in the early design stage of conceptual design, e.g., [2], and
they came up with tools for helping the designer with conceptual design. Among such tools, this paper
discusses Design Record Graph [3] and Axiomatic Design [4], especially, how they can detect design
problems in the conceptual design stage.

The design problems this paper discusses are two; one with a recent recall of a bicycle, and the other,
the 2011 Fukushima Nuclear Power Plant (NPP) accident.

2. Design Record Graph and Axiomatic Design
This section briefly describes the two design tools that designers often use in their conceptual design.

2.1. Design Record Graph
Figure 1 shows a design record graph (DRG). The use of design record graph is twofold; in producing
a new design or analyzing an existing design. For creative design of coming up with a new product that
did not exist before, the diagram starts from the left end node, the product functional requirement, and
generally proceeds to the right. The designer iteratively divides the functions on the left to collections
of smaller functions to the right until the designer reaches a set of functional elements (FEs). An FE is
one that is not practical to divide into smaller functions.

The designer then maps each FE to one or more physical elements (PEs) which are typically machine
parts that produce the corresponding function. This time, the designer is moving into the physical space
from the functional space. The mapping can take any form of one to one, one to many, or many to one.
Once in the physical space, the designer can start defining assemblies that collect multiple parts, then
higher-level assemblies or modules consisting of multiple assemblies until the designer reaches the
destination of a product; this goal, the product meets the product functional requirement defined at the
starting point. This design does not necessarily proceed strictly from the left to right; the designer can
jump back and forth over the border of functional space and physical space in a zig-zagging manner.

A DRG is also useful in analyzing existing products. In this case, the product functional requirement
at the left end and the product at the right end are known, as well as all the PEs. The analysis proceeds
by figuring out FEs for the PEs and how the two types of elements combine into higher level functions
and assemblies, in other words, the analysis identifies the arcs in the DRG.

2.2. Axiomatic Design
Axiomatic Design (AD) calls FEs and PEs in DRG, functional requirements (FRs) and design
parameters (DPs), respectively. It shows the correspondence among FRs and DPs with a matrix named
design matrix (DM). By placing the FRs and DPs in the form of vectors $\mathbf{FR}$ and $\mathbf{DP}$, AD expresses the
design with the following matrix equation.

$$\mathbf{FR} = \mathbf{A} \mathbf{DP}$$

(1)
where $A$ is the DM. If we number the 10 FRs in figure 1, FR1 to FR10 and the 9 DPs, DP1 to DP9, AD expresses this design with the following matrix.

\[
\begin{pmatrix}
FR1 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
FR2 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
FR3 & 0 & X & X & 0 & 0 & 0 & 0 & 0 & 0 \\
FR4 & 0 & 0 & X & 0 & 0 & 0 & 0 & 0 & 0 \\
FR5 & 0 & 0 & 0 & X & 0 & 0 & 0 & 0 & 0 \\
FR6 & 0 & 0 & 0 & X & 0 & 0 & 0 & 0 & 0 \\
FR7 & 0 & 0 & 0 & 0 & X & X & 0 & 0 & 0 \\
FR8 & 0 & 0 & 0 & 0 & 0 & X & 0 & 0 & 0 \\
FR9 & 0 & 0 & 0 & 0 & 0 & 0 & X & 0 & 0 \\
FR10 & 0 & 0 & 0 & 0 & 0 & 0 & X & X & 0
\end{pmatrix}
\]

(2)

The DM in Equation (2) consists of elements 0 and X, where 0 indicates that the corresponding DP has no effect on the FR and X that the DP affects the FR to some level without quantitative indication.

When a design is uncoupled in AD, its DM is diagonal. When this condition holds for a design, its DRG has all its arcs across the functional space and physical space show one to one correspondence and they form a ladder like structure.

3. Two accident cases

This section discusses a consumer product, a bicycle recall case that caused major injuries but luckily no fatalities, and part of a catastrophic accident that still has residual effects on us, the Fukushima Nuclear Power Plant (NPP) accident.

3.1. Bicycle recall case

First is a design problem with our first subject, a bicycle. A major bicycle manufacturer in Japan introduced a new model in 2003 with a device to lock the rotation of the steering shaft when the user parks the bike and locks the rear wheel. The company named the mechanism “single action double lock” to have it stand out in the market where its competitors had models with separate steering locks that required the riders to engage them separately from the actions of locking the rear wheels. Figure 2 shows a photo of the recalled model. The red circles identify the rear wheel and steering shaft locks.

Figure 2 Recalled bicycle
The purpose of the rear wheel lock is to stop the rear wheel from rotating while the bicycle is parked, that is to prevent theft. Locking the steering shaft is a recent development for bicycles. One of the purposes is to prevent it from toppling over when parked on sloped surfaces, and another function, favored by parental riders, is to keep a stable position while seating a child in a child seat.

Figure 3 Parts of single action double lock

Figure 3 shows parts of the single action double lock mechanism [5]. The steering shaft lock is housed inside in a diecast case, seen as an oversized gray box in the right-hand upper photo in figure 2, with a window to show the status of the lock.

Figure 4 shows how the single action double lock works. The figure on the left shows when the lock is disengaged, and the one on the right when engaged. The movements numbered 1 through 5 in the right figure happen at the same time; the numbers are for easier understanding of the mechanism.

Figure 4 How single action double lock works
Figure 5 is the DRG for this bike locking system. All the arcs that cross the boundary between the functional space and physical space have one to one mapping indicating that the design is uncoupled in AD.

![Figure 5 DRG of “Single action double lock” for a bicycle in parked mode](image)

So far, we discussed how “single action double lock” works in parking a bike. The primary function of a bike, however, is not in parking it, but rather in riding it. Figure 6 next shows a typical DRG for the primary function of riding a bike without the detail of the braking system for simplicity. The two nodes with heavy lines and pink background show where the FE-PE relation failed when the locking system failed as we describe later.

![Figure 6 DRG of a bicycle in riding mode](image)

Note that the designer is not very concerned about the locking system. One may add the function of “keep the bike locked when parked” with a corresponding mechanism of “locking system,” or for a deliberate functional analysis the designer may add the contents of figure 5 into figure 6.

Knowing that this “single action double lock” led to the recall, we will take a closer look at the locking system when the user is riding the bike. Figure 7 shows the DRG in this mode.

![Figure 7 DRG in riding mode](image)
Note that with the mechanism working in the other direction, the parts change their functions shown with colored nodes in Fig. 7. What causes the locking block to engage into (parked mode) and retract from (riding mode) a pinion gap is the balance among the torsion spring, block spring, and force from the pushing rod. In riding mode, the pushing rod does not push up the receptor, and spring force from the torsion spring overcomes the block spring force. On the other hand, in parked mode, the pushing rod gains upward force that overcomes torque from the torsion spring and block pressing tab moves to the left to allow the block spring to push the locking block into a gap of the pinion.

The locking block in riding mode has the function of retracting itself from the pinion gap it engaged in parked mode. The torsion spring in riding mode, in the meantime, must constantly keep its spring force on the pushing force receptor to keep the locking block retracted.

The recall was due to cracking of the diecast case of the steering handle lock assembly. Ministry of Economy, Trade and Industry (METI) had a news release [5] showing photographs of a normal and a cracked case. Figure 8 shows the illustration that accompanied the photos and comparing it with the photo of the steering shaft lock in figure 2 clearly shows the problem.

When the case is cracked, parts inside it lose tight positioning and the block pressing tab can lose its contact with the locking block. Figure 7 shows this origin of failure with the pink colored FE-PE mapping. The locking block and block spring also failed to meet their corresponding FEIs. Without force from the torsion spring, the block spring pushes the locking block into a pinion gap. Consequently, the steering handle locks while the user is riding the bike and that is a totally unexpected behavior that can cause the rider to fall on the road with the bike.

The recall covered about 3.4 million bicycles, and at the time of the METI press release on June 24, 2019 [6], there had been 6 serious injury cases. Consumer Affairs Agency (CAA) of the Government of...
Japan later reported that the number of accidents during April of 2019 to March of 2020 totaled 42 cases, and 11 during April to August 18, 2020 [7].

3.2. Accident of Unit 1 of Fukushima 1 NPP
The 2011 off the Pacific coast of Tohoku Earthquake broke out on March 11, 2011. It caused tsunami waves that attacked Fukushima Nuclear Power Plant-1 (Fukushima 1 NPP) about an hour later. The wave heights exceeded limits that Fukushima 1 NPPs were built for. The seawater flooded the basements of all six units at Fukushima 1 NPP, where most of all switchboards for units 1 to 4 were located. The four units were forced into station blackout, i.e., loss of all AC power [8]. Units 1 and 2 also lost all their DC power as well.

The earthquake caused all the units, running at the time, units 1, 2, and 3, to go through emergency insertion of their control rods. At the same time, all isolation valves on the main steam lines to the turbines and feedwater lines back from the condensers closed. The 3 reactors entered the state of core isolation. Since all the control rods succeeded in full insertion, main power of the cores stopped generating most of their powers. Nuclear fuel, however, even when they stop generating heat from nuclear chain reaction, continue to generate heat called decay heat.

Decay heat is only a few percent of full power (6.4% for unit 1 at the time of shutdown [9]), however, without removing this heat, the reactor will quickly boil the water inside and uncover the fuel. Once uncovered, the fuel will start to melt. Unit-1 had 78 minutes after station blackout to recover its lost core cooling function [9].

Unit 1, the oldest of all units that had started operation in March of 1971, had two Isolation Condenser (IC) systems, A and B, designed to remove the decay heat at time of core isolations. Figure 9 shows one of the systems at the time of core isolation.

IC is a simple condenser with a condensing chamber filled with cooling water and steam inlet pipes that connect to a high elevation of the reactor pressure vessel and water return lines to the recirculation piping that connects to a low elevation. This piping has 4 isolation valves; 2 AC valves inside the pressure containment vessel and 2 DC valves outside. During operation, the operator turns just the DC valve DC3 on and off to control temperature drop inside the pressure vessel and the remaining three valves are open all the time. Figure 10 shows the DRG for this IC system.
This IC system, however, had another mode of operation for safety. The piping that routes the steam through the cooling water to condense steam into water had a pressure sensor on it. The purpose of this steam sensor was to monitor any possible cracking on the piping. From figure 9, one can tell if the piping had a crack, steam with radiation can leak into the surrounding air by escaping through the crack to the condenser chamber and eventually through the steam outlet to the atmosphere.

This was IC piping failure mode that closes all the four IC isolation valves to avoid any radiation leakage from the IC. It is not very difficult to realize that this DC power operated instrument was designed to send out a leakage detection signal when it loses its DC power. It was a fail-safe design to assume leakage when the sensor lost its means of detecting the reality. Figure 11 shows the DRG of this safety feature.

It was ironic that at the time of station blackout, DC power (shown with pink background in Fig. 11) to this pressure sensor was first lost and the system sent out signals to close all the four IC isolation valves. In other words, the IC system entered a false piping failure mode. The operator was controlling the reactor temperature by opening and closing DCV3 on System A, thus, IC System B had its DCV3 fully closed. For this reason, the statuses of the other three valves on System B made no difference. The operator, without recognizing this safety feature, kept hitting the open and close switch of DCV3 on IC System A. He even went outside to observe steam from the two steam outlets outside the reactor building. He only saw a small amount of steam rising from the exhaust pipe but still was not sure if the IC was working. It was later pointed out that the plant had no experience of training about loss of DC power and the IC systems were tested only during plant startup, but never during the 40 years of operation that followed.
The consequence was meltdown of the core of Fukushima 1 NPP Unit-1 and the process generated hydrogen gas that leaked up inside the reactor building. The reactor building blew up in a hydrogen explosion a day after the station blackout.

4. Discussion

The previous section reviewed two accidents, one with a consumer product that caused a number of injuries to users and eventually was recalled, and the other about a major catastrophic accident of an NPP. Both accidents share the same difficulty in design that parts of the design had to operate in different manners for different modes of the products.

4.1. Bike recall case

The two modes for the bicycle were parking and riding. When we think of safety, the riding mode obviously has higher priority over the parking mode. Imaginable failure of the parking mode is theft or falling over. Theft is a definite loss to the user and falling may cause damage to the product, however, there is no way of getting injured with these failures. Users have voiced the convenience of steering shaft lock when they need to lift their children into the child seats, however, it is just “easier” and users used to do so without the steering shaft lock with added carefulness for seating their children.

In fact, the bike manufacturers no longer have the single action double lock features in their new products and instead, placed an independent steering shaft lock that the user must engage manually. The designer in applying AD or DRG to design tends to write out part names for DPs. That can easily lead to oversight if the design requires conflicting operations of the part in different modes. We have to analyze all modes of a product and pay special attention if the same part has different functions or different configurations in different modes. For the case of the bike, trouble with the part integrity let the “Locking block” slide into a different posture while in a mode where safety was more important.

4.2. Nuclear plant case

The purpose of our analysis in this paper with regards to Fukushima 1 NPP Unit 1 was not in pointing out responsibilities, but rather it was for revealing how easy it is for the designer to overlook conflicts in detail design.

It is, in fact, easy to point out design deficiencies after the trouble. However, in the case of Fukushima, among many reasons that can lead to core isolation, station blackout was definitely one that needed consideration. Moreover, before the Fukushima accident, even the Japanese design guideline stated that station blackouts would be short, and the practice was to assume 30 minutes or less [10]. Probably this minor concern with loss of power led to overlooking that the IC systems would shut down upon a station blackout closing all the IC valves, while they needed to be kept open to keep the shutdown core from melting.

5. Conclusion

We looked into two accidents where parts of the product needed to behave differently in different modes. When we apply AD or DRG in analyzing our design, we need to write out how the design expects the parts to behave. If we just write down the part names, it is easy to overlook conflicting behaviors of the parts in different modes. We further see the need to execute design analysis of products in all modes of their operations and find out what triggers the products from shifting from one mode to another.

In case of the bicycle, the two modes were “parked” and “ridden.” The “locking block” designed to lock the steering shaft turned loose and interfered with the function of safely riding the bike by allowing the rider to steer the handle into the desired direction. It was an interference of a secondary function with one of the crucial ones for safety.

In case of Fukushima 1 NPP Unit 1, the two modes were “IC piping failure” and “core isolation” and the designers overlooked consequences of the serious event of a station blackout. When this event happened, instrumentation first lost its DC power supply and enforced the safety function of closing all isolation valves on the IC systems. It was at the time of “core isolation” when cooling was needed for
the isolated core and the reactor without means for releasing decay heat of the core headed into core meltdown.

Designers must review all modes of operation of products and acknowledge the priorities among different modes. In case of the bike, “safe riding” had priority over “stable parking” and in case of the NPP, “cooling during core isolation” had priority over “preventing possible radiation leakage.” The designer must be careful in adding features that can possibly damage FRs of modes with higher priority.

References
[1] “How many parts is each car made of?” Toyota Motor Corporation, 1995 [https://www.toyota.co.jp/en/kids/faq/d/01/04/]
[2] Ullman D G The Mechanical Design Process Fourth Edition, McGraw-Hill, 2010, New York, NY
[3] Iino K, Nakao M, Design Record Graph and Axiomatic Design for creative design education, PROCIR-D-16-00377, Proceedings of ICAD 2016
[4] Suh N P, Axiomatic Design, Advances and Applications, Oxford University Press, 2001
[5] Accident talks: Design to notify trouble triggers accident/Recall of 3.43 million bikes with “Single action double lock” NIKKEI MONOZUKURI, Dec. 2019 (in Japanese).
[6] Recall of Bicycles and Electric Power Assisted Bicycles with Built-in Locking Mechanism Simultaneously Working Handlebar Lock and Circle Lock (Free Product Inspection and Repair), METI News Release, June 24, 2019 (https://www.meti.go.jp/english/press/2019/0624_003.html)
[7] Announcing serious product caused accidents by a consumer product, CAA News Release, August 18, 2020 (https://www.caa.go.jp/notice/assets/consumer_safety_cms202_200818_01.pdf in Japanese)
[8] Hatamura Y, Abe S, Fuchigami M, Kasahara N., The 2011 Fukushima Nuclear Power Plant Accident, Woodhead Publishing, 2015
[9] Iino K., Yoshioka R, Fuchigami M, Nakao M, Precautions at Fukushima That Would Have Suppressed the Accident Severity, Journal of Nuclear Engineering and Radiation Science, ASME, February 2018
[10] Report: A comparison of U.S. and Japanese regulatory requirements in effect at the time of the Fukushima accident, NRC, November 2013 (https://www.nrc.gov/docs/ML1332/ML13326A991.pdf)