Proceedings of ICAD2002
First International Conference on Axiomatic Design
Cambridge, MA – June 10-11, 2002
ICAD 022

DESIGN FAULT PREVENTION THROUGH ACTIVE USE OF DATABASE

Yotaro Hatamura
hatamura@hnl.t.u-tokyo.ac.jp
Kogakuin University
1-24-2 Nishi-shinjuku, Shinjuku-ku, Tokyo, 163-8677

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

Kenji iino (corresponding author)
kiino@sydrose.com
SYDROSE LP
475 N. 1st St., San Jose, CA 95112, USA

ABSTRACT

Japan has launched a national project for collecting and making active use of case information of design faults. The project involves the government, its agents, schools, and industry of Japan and cooperation from several overseas organizations. The process not just collects fault information but applies scenario analysis to each case. This scenario based analysis will clarify, the mechanism of design faults, from small mistakes to those leading to catastrophic accidents.

Our early studies show that design faults occur when the design matrix [Suh, 1990, 2001] or design constraint contains error or is incomplete. This paper introduces our first stage studies of how design faults occur and how we plan to reduce their frequency and seriousness.

Keywords: design error, fault, failure prevention, database

1 INTRODUCTION

The Japanese economy has been long struggling with recession, and, at the moment there seems to be no way out. Adding to the situation, the society recently faced a number of catastrophic accidents that have put the people in even lower spirits.

Several years ago, the authors wrote [Hatamura ed., 1996] about analyzing faults (or failure), primarily in the field of mechanical design and, described how we should analyze the faults and document them. Our method has emphasis on how to record the experience for positive use, by others and later generation, to prevent similar faults from occurring and avoid letting them grow into large-scale accidents. Since then, we further advanced our discussion and published the methodology in a book geared for the general public and analyzed some of the classic and recent accidents [Hatamura, 2001].

The book made its way to a national best seller and caught the attention of the government. A study group has been formed and efforts are being made to put our practice into a much larger scale project. Japan Science and Technology Corporation (JST) is organizing the “Fault Database Construction Project” that involves the government, schools, and large to small size corporations [JST, 2001]. Some overseas institutes are also providing help with the project.

This paper describes the mechanism of faults, how we recommend recording them, and what we can do to turn them around to produce positive value for the society.

We will also discuss that faults occur when the design matrix [A] of {FR} = [A] {DP} or the constraint vector {C} is incomplete or contains error. The outcome of our efforts shall produce computer tools to aid the designer in design and, at the same time, enhance the quality of the design equation representation for product design.

2 STUDY OF FAULTS

For our "Study of Faults" we define a fault as: "A human act that did not accomplish the original purpose," or alternatively, "When a human made an act it produced an undesirable and unpredicted results." The keywords for our purpose are "human" and "undesirable".

The actual faults we experience vary in size from small ones to large ones and in type. A designer may produce machines that fail to meet the original intention because of the designer's lack of knowledge or carelessness. We repeat small faults daily that do not quite cause inconvenience or damage to others. On the other hand, there are occurrences when a small fault causes the next one and eventually leads to a fatal accident or a catastrophe. Accidents or disasters that horrify people often start from small faults like careless mistakes.

In the following subsections, we will discuss the characteristics of faults that make it difficult to analyze them, how they grow into disasters especially in the modern society, how we recommend recording faults to make the best use these negative experiences, and what are the most effective ways of training people to prevent repetition and growth of faults.

2.1 SIX OBSTACLES IN FAULT ANALYSIS

Most modern fields of natural science advanced by first making observations, theorizing rules that describe the findings, and then applying the rules to new discovery. Making accurate observations or communicating the facts to other people are, thus, among the most important in the early stage of research.

Fault information, however, from its negative impact to the society and individuals, is difficult to transfer. There are six characters of fault information that describe this difficulty:

i. decays over time and space
ii. hides
iii. simplifies
iv. changes
v. turns into a myth
vi. localizes

This subsection describes these tendencies of fault information with some examples.

i. Fault information decays over time and space

Fault information quickly degrades with time and its travel through various passages. Fault information transmits well to the person next to the one who experienced it, however, it does not convey well to the second person. Not to mention, transfer across generations often almost destroys the information in its way from grandparents to grandchildren.

Tsunami is a phenomenon caused by earthquakes, broken glaciers or rocks falling into the ocean which produces waves that travel along the water face and grow into massive waves until they hit the coast. Sanriku coastline is not only deeply indented, but it also faces the Japan Deep, a hotbed of earthquakes. As so, it is known as the world's most frequent area of Tsunami attacks and has suffered many damages.

If we walk along the town of Sanriku coastline we notice stone monuments reminding us of the presence of past Tsunami. They are erected every time a large scale Tsunami attacks, and in the old days, when there were lots of casualties, they also served as memorials. Some of the monuments were built to teach lessons. They were at locations where the waves had reached and many of them were engraved with words saying, "Do not build houses lower than here."

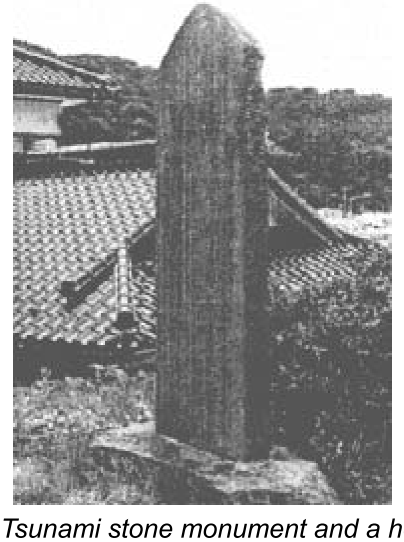


Figure 1. Tsunami stone monument and a house built underneath it

The stone monument in Figure 1 tells not to build houses on lower ground, but there is a house standing right under its nose. This shows that any valuable lesson we learned is useless when we are more concerned with convenience in our daily lives.

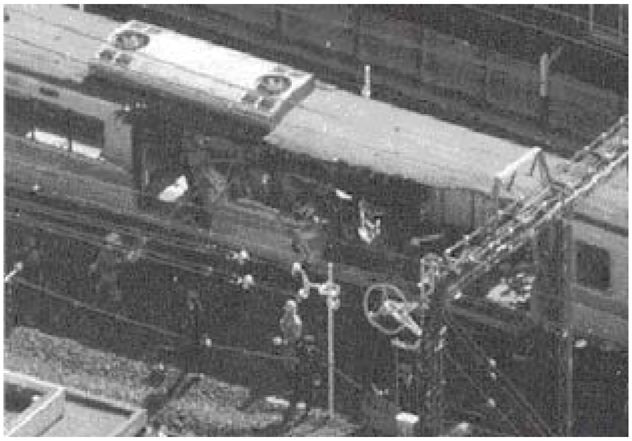
In the past, there were times when old lessons completely vanished from peoples minds, and one day a large scale Tsunami washed away the entire village. Even such experiences have traces on the monuments, but convenience forces some people to live close to the coast.

It is not rare for people to forget a fault experience in short time periods and repeat the fault again. The past incidents in the frequent Tsunami attack area of Sanriku coastline clearly represents the characteristics of fault information that "Fault is hard to transmit to people." and "Fault information degrades as it is passed along."

ii. Fault information hides

On March 8th, 2000, an eight car train derailed at a sharp turn near Nakameguro station of Eidan Subway Hibiya-line. The derailment turned into a disaster when the train collided with an oncoming train, killing 5 passengers and injuring 60. The accident is said to be caused by "derailment from gradual lifting" that can occur at sharp curves.

Eidan later announced that similar accidents took place in October and December of 1992. When Hanzomon-line cars passed a sharp curve at a switching point in a depot, cars number 4 and 5 derailed in the first accident and cars 9 and 10 in the second.



(Photo by Kyodo News)

Figure 2. Subway Hibiya line derailment and collision

After the two accidents the company formed a special team to investigate them, however, they could not identify the cause. At the end, the company took no special measures for other cars or lines, and did not report the accidents to the Ministry of Transport, which administers railways in Japan.

As we see this sequence, the Hibiya line accident was doomed to happen. In other words, a feature of fault information that avoids exposure to people or public, "fault information tries to hide" was in the background of this accident.

iii. Fault information simplifies

We know the teaching, "In case of fire, put out the flames." This comes from our lesson learned from the Great Kantoh Earthquake which killed many people in fires that broke out shortly after the earthquake. It is one of the brilliant phrases that made its way throughout our society by converting a past fault experience into knowledge. But if one literally follows these words and tries to put out any flames as soon as an earthquake hits, he will end up suffering from burns.

The meaning implied in this phrase is, in case an earthquake hits, wait for the shaking to settle then extinguish any flames. This is a typical example of simplified fault information that hampers accurate knowledge transmission.

Any person who has experienced an earthquake should know the danger of trying to put out flames without hearing such an explanation. He can easily supplement, in his mind, the teaching of, "In case of fire, turn out the flames." to "In case an earthquake hits, wait for the shaking to settle then extinguish any flames."

This correction is possible because he has proper knowledge of an earthquake situation. Accurate analysis of a fault itself is important when making use of fault knowledge, and therefore, transferring fault information should include detail processes and causes without simplification.

iv. Fault information changes

When a fault occurs, especially when it took place in an organization, those higher in rank often try to place responsibility at lower levels. Medical malpractice is a good example. When the wrong medicine is given to a patient, the hospital, without any mention to administrative issues like management organization or workload to nurses, tends to explain the problem as a mistake by a nurse. This reveals the troublesome characteristic of fault information that "cause of fault tends to change".

Let's look at the Chernobyl nuclear power plant accident on April 26, 1986. It may not be well known that when the accident broke out the government of the Soviet Union, at the time, announced that the cause of the fault was the result of an operator violating the rules. This covered up the structural flaw in the reactor structure itself. The easy pursuit by the western world was partly responsible for this screening. Making much noise about the Chernobyl issue might have triggered more activity in anti-nuclear acts in their own countries. The governments thought the accident would only have a negative impact. For having national policies promoting nuclear power generation, they intentionally accepted the distorted fault information.

When we hear fault information, we have to decide if such an intentional filter or accessories are present to cope with the characteristic of fault information that "cause of fault tends to change".

v. Fault information turns into a myth

The world's largest battle ship, Yamato, built during World War II, hardly achieved anything and it departed to take part in the Okinawa battle with one way fuel only to sink in the ocean after repeated air raids by US fighter planes. This well known story gave birth to its name "Battleship of Tragedy" from its size and last battle.

There is no doubt that the fault of the battleship Yamato came from change in restrictions in war strategies. Nonetheless, we must not forget the core cause - that the war ship planners could not foresee the improvement of air fighters and submarines. We always need to find the real cause to turn fault information into knowledge and to teach to the next generation.

The phrase "XYZ of Tragedy" actually shows us the feature of fault information that they tend to turn into myths. The tragic story that has turned into a myth appeals to peoples' hearts and chivalrous spirits, and it is easier for the audience to understand and remember.

On the other hand, a myth beyond a certain extent blurs the essence of the information itself. In fact, Yamato would have been a great battleship in the older days when large ships and huge cannons were still effective in war. The ship turned into a tragedy as time changed and air fighters became the main force of war. The real cause of this tragedy was the military planners' misjudgment. They did not realize the change in effective weapons from large battleships and huge cannons to air fighters.

Fault information with a tragic story translates to a large audience as a myth, however, it tends to be singled-sided. The form of transfer is not ideal because it lacks preciseness as knowledge. The theory that "fault tends to turn into a myth" is not welcome by those that want to study the subject later.

vi. Fault information localizes

Fault that occurred in one place tends not to transfer to other places. This tendency is clear in modern organizations with tree structures. The structure itself tries to cut lateral connections by dividing roles among groups, and thus information of a fault in one group naturally does not transfer to others.

In addition to the structure itself, the reason for the tendency to localize fault information originates from the negative image of fault. If fault information within your own group transmits to another, most people are concerned that "This information lowers the evaluation of our group," or "It will place disadvantage on our work." Thus, when we face fault, it is natural for us to unintentionally hide the facts.

Nevertheless, this tendency to localize fault information is clearly a negative act when viewed from the organizational standpoint as a whole. Not sharing the information of fault in one group allows similar fault to take place in other groups. Repeating a fault that already occurred in another group is nothing but a waste, and the source of the waste is localization of fault information based on concerns with individual evaluations and images.

These are the six characteristics of faults that interferes with proper analysis. In addition, the hierarchical systems of the modern society multiply with these negative effects, and not only do they hinder proper evaluation, but they often keep seeds of faults untouched to eventually grow into catastrophic accidents.

2.2 GROWTH OF FAULTS

Many corporations and government bodies organize themselves in tree structures. The tree structure is most powerful in orchestrating a large group to move towards a unified goal.

Nonetheless, we have to be careful to know that the tree structure is a measure that simplifies the object so it is easier for people to understand, and that the actual concept or events are more complicated. In the real world, even nodes at ends of the structure, have invisible links, in other words, relations (Figure 3). If we think that we understand the entire structure, forgetting these invisible links, they can certainly come back to haunt us later.

In fact, our study of cause of faults shows that most cases have an underlying illusion of full understanding from this haunted tree structure. In other words, fault is a revelation of weakness of the tree structure.

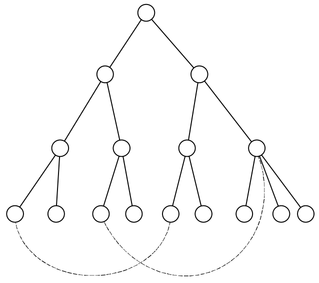


Figure 3. Hidden links in the tree structure

Most modern corporations have tree structures for their operations. A common problem with this type of organization is fault repeating in a group next to another group that has already made the same mistake. The fault could have been avoided if the fault information was transferred. Figure 4 sketches the situation.

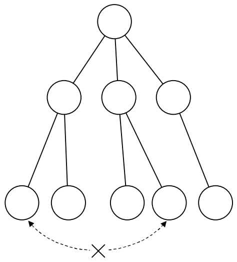


Figure 4. Fault information is hard to travel among different groups

Another cause that easily leads to design faults is hidden links. For example, in automobile manufacturing, each system, like engines or electronic systems, form an independent group, then work is performed within even smaller groups for individual parts. However, physical configuration defines invisible links among all parts and operation of one part may have a bad effect on others. Not recognizing hidden links or ignoring them leads to many faults.

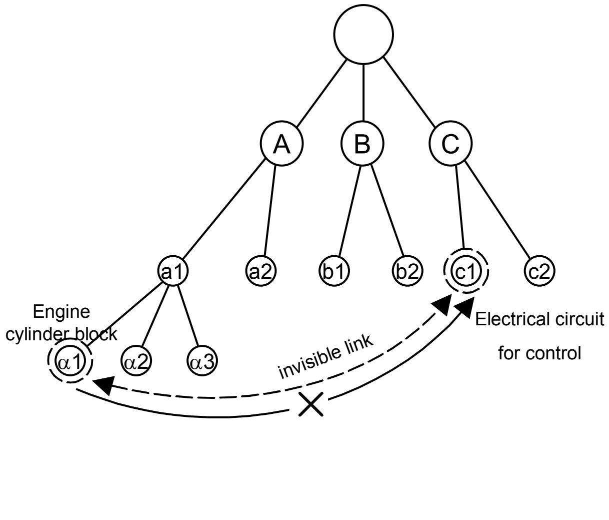


Figure 5. Hidden links can lead to faults

Say we have a trouble free engine. The heat from the piston area can cause a bad effect on the electronics control system and the machine can go out of control. The engine and its electronic controls have tight links between them in terms of temperature and heat, however, not recognizing these links and pursuing works of the engine and electronics separately would definitely cause fault and may eventually lead to a disaster.

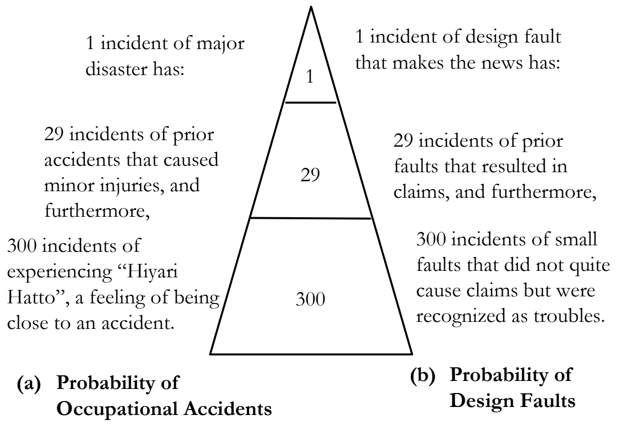
In terms of Axiomatic Design, these hidden links are hard to see constraints {C} that are actually there, but once the design team (or teams) headed out thinking they had an uncoupled design, and later could not discover the constraint turning into an active one due to a design change (in the automobile example, moving the control box closer to the engine). They can also appear as non-diagonal components of the design matrix [A] of the design equation {FR} = [A] {DP}, that is, what seemed insignificant at the beginning later turned out to have greater magnitude to affect the design.

Heinrich [1980] stated that, for every major accident there are 29 minor injuries and 300 near misses. This is the so-called Heinrich's Law and it is an empirical relation of the probability of obvious occupational disasters among latent ones.

A phrase that well describes this law and alerts us what to look out for is "Hiyari Hatto". The origin of this phrase is "Hiyarito-shita (I felt the chills.)" and "Hatto-shita (I was startled.)", and it teaches latent danger and fault within these experiences. This interesting phrase also implies that taking proper measures can prevent the danger by recognizing it.

In the study of faults there is almost an identical law which we can call "Heinrich's law of fault". If we apply it to a business, it will be phrased, if there is a large fault that makes its way to the media, there were 29 minor claims (customer complaint) and 300 faults that employees recognized.

Taking proper countermeasures when we experience "Hiyari Hatto" can stop the growth of faults. If we leave them alone the number of incidents may be smaller, but we will certainly experience faults with larger effect like claims. If we do not take any countermeasure then the fault shows itself in a greater scale and it leads to a disaster that causes great damage to the surroundings. This is what "Heinrich's Law of Fault" teaches us. Large scale faults that cause accidents and troubles always have this type of structure in the background.


1 incident of major disaster has:
1
1 incident of design fault that makes the news has:
29 incidents of prior accidents that caused minor injuries, and furthermore,
29
29 incidents of prior faults that resulted in claims, and furthermore,
300 incidents of experiencing "Hiyari Hatto", a feeling of being close to an accident.
300
300 incidents of small faults that did not quite cause claims but were recognized as troubles.

(a) Probability of Occupational Accidents

(b) Probability of Design Faults

Figure 6. Heinrich's Law of Faults

If we have our antenna covering our world we can always recognize the signs of faults and, by taking appropriate measures, we can certainly prevent the occurrence of the large faults. In theory, it is one of the simplest methods of avoiding faults. The reality, however, leaves these signs of fault untouched. The reason is because faults are something to "avoid" and people would rather "not face them". As I mentioned earlier, human nature "does not see things that it does not want to". Precise investigation of a fault or accident to reveal the real cause leads us to prevent the next fault that occurs for the same reason, and, is often larger in magnitude.

2.3 RECORDING FAULT EXPERIENCE

Learning a lesson from a fault and making use of it to prevent future faults or to turn it into a creation requires two actions; one is to coherently describe the fault from events to conclusions, and the other is to "turn the fault into knowledge". Turning fault into knowledge means summarizing the fault into knowledge so that the person who caused the fault and others can use it. This is indispensable for properly transferring fault information.

Corporations and administrative offices archive reports that explain the process of fault in cases of accidents or troubles. The authors spend a great amount of effort writing these reports, however, in most cases, no one goes back to read them and they are just stored in the archive room. The biggest cause for us not using the reports is they are written only for the purpose of recording and not for future use. We should "Turn them into knowledge" after the recording process. Once they are turned into knowledge they become usable fault information.

When we turn a fault into knowledge we need to properly record the information regarding the problem. Records that are missing necessary information are not transferring the truth, and insufficient descriptions lead to distorted perception by the reader and hinder the positive use of the information. The reader only gets confused with the fault information and is better off without it.

Proper fault information includes descriptions for each item of "phenomena", "process", "cause (or its inference)", "countermeasure", and "summary". These items are not just picked out of air, but they come from our study of the human thinking pattern when we understand concepts and they are arranged to follow the pattern. Placing a title in the header of the report allows us to organize the fault information so anyone can take a glance to see the ingredients of a single fault sample. The sixth item that we should record is "knowledge" gained after examining and evaluating the former five items.

2.4 LEARNING THROUGH FAULTS

The basic theme in the "Study of Fault" is "Why should people learn from fault?" Through teaching students at school we learned that we should never take faults negatively. Also, what is needed for education is not only to communicate the correct knowledge, but also to have the students experience the knowledge to learn without the fear of fault. One cannot master the real usable knowledge without such feelings or hands on experience.

A student studying mechanical engineering is a novice engineer, and if we give an assignment to a novice engineer without a sample model, everyone fails to produce anything that works. It is not any different with a beginner designer or economist who can never make a meaningful design or investment plan from no knowledge and no sample model.

In this case, the novice who possesses a stronger desire to learn feels more "pain", "suffering", and "loss" with greater frustration. We can avoid such frustration by providing a model and having the student follow it, guiding the student down the shortest path to the correct answer, however, the student in this case hardly gains anything.

In contrast, a student who experienced frustration at the beginning and felt the real need for knowledge can acquire actual knowledge that can be applied in any situation. This method of learning is clearly different from what students are familiar with. Studying for exams by learning the quickest path to answers to given questions is indeed rational, however, this method alone does not let students acquire knowledge in the real sense. You may gain superficial knowledge that does not grow roots in the deep parts of the mind and thus you cannot use it as your own knowledge.

To fill this gap it is necessary to learn by experience, accompanied with physical feel, and to actively use fault experience without frowning on it. In fact, in educating children, daring them to make mistakes so they learn themselves is the only way to increase their ability to make judgements.

As an example, we have been teaching children to be careful handling knives. There are hardly any chances now for children to use knives. The reason is "safety" and children no longer cut their hands with knives. However, in this case, children are deprived their chance to experience small fault of cutting their hands. It is possible that a child that never experiences cutting a hand with a knife grows without the proper knowledge of how dangerous a knife really is.

We should learn that "avoiding small faults imprudently is just preparing for larger faults to come."

Another effective way in teaching lessons from faults is to provide detailed information that can lead to having virtual experience. Here is an example;

One way is to state "Never touch hydrofluoric acid with his bare hands because when it contacts the skin, hydrofluoric acid penetrates the skin without harm and directly dissolves the bone. It is an extremely dangerous substance."

A more effective way is to give the whole story: "A careless student wiped hydrofluoric acid with his bear hands. An instructor saw the even and instructed him to consult with a medical doctor, an expert on hydrofluoric acid injuries. The student was confronted with the choice of losing his fingers or injecting calcium from under his nails. Nobody wants to have his fingers cut off, but also piercing a needle under the fingernail is a torture, and the student stood there with a pale face. The treatment took 2 months before he was fully recovered."

3 CONCLUSION

- This paper reported our initial studies about making use of fault information that triggered a national project.
- We have identified six key items that need to be recorded when documenting fault cases. Unlike conventional reports, we recommend documenting detailed information and, moreover, evaluation results that serve as "knowledge".
- Our efforts of clarifying causes of faults will have mutual effects with axiomatic design of increasing the accuracy of the design matrix [A] and constraints {C}.
- The national project is in the first stage of collecting case information, but in a way consistent with our methodology so that the information and evaluation will serve the purpose of preventing catastrophic accidents and repetition of the same faults.

4 ACKNOWLEDGMENTS

The authors thank MEXT and JST for their support of our research.

5 REFERENCES

[1] Hatamura Y, *The Study of Faults*, Kodansha Ltd., 2000. ISBN4-06-210346-X (in Japanese).

[2] Heinrich, HW., Peterson, D.,& Roos, N., *Industrial Accident Prevention: A safety management approach (Fifth Addition)*, New York: McGraw-Hill, Inc. 1980.

[3] Panel for Practical Use of Lessons Learned from Faults, MEXT, "Report - For Practical Use of Fault Experience", Ministry of Education, Culture, Sports, Science and Technology (MEXT), 2001.

[4] The Practice of Machine Design Study Group, *The Practice of Machine Design -Vol. 3*, Hatamura Y. (ed.), The Nikkan Kogyo Shimbun, Ltd., 1996. ISBN4-526-03922-5 (in Japanese).

[5] Suh N.P., *The Principles of Design*, New York: Oxford University Press, 1990. ISBN 0-19-504345-6

[6] Suh N.P., *Axiomatic Design*, New York: Oxford University Press, 2001. ISBN 0-19-513466-4