To appear in Proceedings of the ASME 2014 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference IDETC/CIE 2014
August 17-20, 2014, Buffalo, New York, USA
DRAFT DETC2014-34577

RECONSTRUCTING THE DESIGNERS INTENTION FOR REUSING FAILURE INFORMATION

Kenji Iino
SYDROSE LP
San Jose, California, USA

Masayuki Nakao
The University of Tokyo
Tokyo, Japan

Michelle L. Ota
SYDROSE LP, Tokyo Office
Tokyo, Japan

ABSTRACT

The functional-structural (F-S) diagram expresses the high-level structure of a design. It is often used in the early stage of conceptual design and serves as the starting point for a number of design tools like quality function deployment, failure mode and effects analysis, and more. On the other hand, for significant risk products whose failure can result in serious damage to the quality of human health, or the society, the designer often use tools like failure mode and effect analysis or fault tree analysis to detect weaknesses in design before the products are shaped. Failures, nonetheless, take place and cause negative impact to the society. It is then that the designer or other experts review the failure analysis to find flaws in the analysis tree or find elements or links in the graph that the designer overlooked. In other words, pre-manufacture failure analysis is limited to the designer's knowledge and insight. This paper proposes a way to make use of failure knowledge with past accident cases by constructing the F-S diagram for the failed products and storing the information in a failure database. Designers can then compare the F-S diagram for new products with linked representation of past failure cases and realize scenarios of failure he did not recognize or have to design carefully.

1. INTRODUCTION

Failures of machines vary from small-scale ones, e.g., like a broken off rubber cover for a smart phone interface jack, or catastrophic ones like the recent accident with the Fukushima-1 nuclear power plant [1], although amazingly this one did not cause any fatality from radiation overdose.

Some failures are blamed on the user who may have repeatedly pulled the rubber cover too strongly in disengaging it from the phone body, but if it had come off after only several times of pulling, the user will probably go back to the store to look for a replacement. When the frequency of this failure results in too many returns to the manufacturer, the cause is more likely to be a design flaw than a clumsy user. The designer will be blamed for the damage to the company that is not just limited to the cost of replacing the bad products but also the negative market image that may pose threat to the market presence of the company.

The responsibilities with more serious accidents are sometimes disputed among the design, maintenance, and use. We showed a fatal accident case with a roller coaster in an amusement park which was quickly attributed to the park owner for poor maintenance that overlooked a crack in the wheel axel, but there remains some questions about the vehicle design [2].

In the world of litigations and critiques, the responsible phase of the product life, whether it is design, maintenance, or use, depends on a number of factors that measure the state of the society at the time; whether similar accidents have occurred in the past, if other products have countermeasures against such accidents, or in expert opinion, if the failure was foreseeable or not.

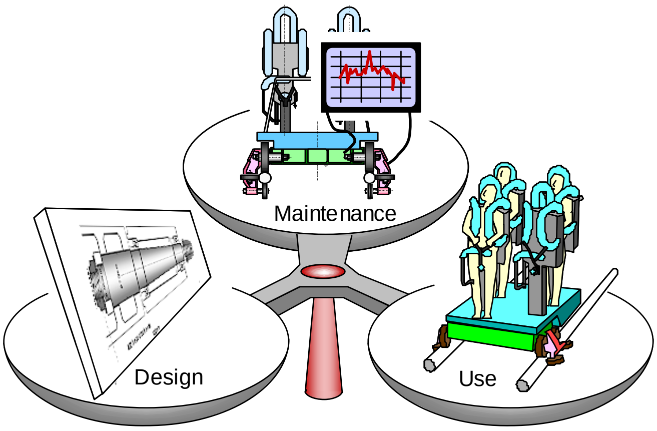

Fig. 1 What is responsible for an accident?

The criteria for deciding what phase, or in many cases, who is responsible for an accident, change with time. For example, an 1879 elevator accident in Chicago, Illinois, killed a 60-year-old female who fell on the threshold when the stopped car started to descend with the door open. The jury blamed the elevator boy who stepped out of the passenger’s way and failed to hold the shipper rope when the car started to move for an unknown reason [3], in other words, the user was held responsible.

Then in 1921, the first A17 Safety Code for Elevators was written, revised in 1925, and adopted as an American Standard in 1931 [4]. Since then, any elevator accident caused by a violation of this code was the responsibility of the design.

In 2003, 125 years after the accident in Chicago, an elevator accident in Houston, Texas decapitated a doctor by pinning his head in closing doors and running up with the doors open. The 2000 ASME Code A17.1 "Safety Code for Elevators and Escalators" had two additions, Ascending Car Overspeed, and Unattended Car Movement. The latter required a braking mechanism that stopped the car in case its doors were open, in addition to the main braking system [5]. The elevator in Houston had the right design in place, and it was later discovered that a maintenance staff had wired a line to a wrong terminal during his work. This discovery led to a settlement between the family of the victim and the maintenance company. In this case, maintenance was responsible.

Fig. 2 Second Braking Mechanism on an Elevator in the City of Houston Code Enforcement Building

As we see in this example of technological advancement, first a design provides a new function or its improvement to the society, then due to the immaturity of the design, accidents and trouble take place. The designer may be excused in early cases, however, as such problems become widely known to the world, the designer may be held responsible for failing to plan against “foreseeable” troubles.

With this mechanical product “elevator,” we illustrated the shift in responsibilities of users towards design. There have been number of design improvements during the 125 years that eliminated the “shipper rope” and even the elevator boy to operate the machine from inside the machine. Now the user interface and foolproof has improved and we can board an elevator and safely reach our intended floor.

The second elevator case we described above was attributed to poor maintenance, however, if we apply Poka-Yoke methods [6] to design, it can even eliminate such maintenance errors. The wires for the controller in the Houston accident were color-coded, but to further eliminate the chance of the careless mistake by the repairman, we can add color to the mating terminals, or even shape the wire ends and terminals so a wire cannot go onto a mismatching terminal.

Whether it is his efforts to avoid liability or out from his good-will mind to prevent accidents, the burden on the designer keeps growing as the society, not just the designer, gains more experience with the advancement of technology or in years of operating machines.

This paper reports our preliminary study in applying existing design tools in helping the designer, with continually growing responsibility, recognize troubles with his design from failure information available elsewhere. Section 2 discusses inherent limitations with existing tools for failure analysis (e.g., FMEA) for that purpose and another tool that we use for our proposal (F-S Diagram). Section 3 then explains how we apply these existing tools so they can cooperate for our purpose of notifying the designer about potential failure modes that he overlooked. Section 4 shows a sample run and Section 5 discusses what further studies have to take place for our future research. Section 6 concludes our report.

2. DESIGN TOOLS FOR ACCIDENT PREVENSION

As our world and the world for the designer devour more information readily available from the INTERNET and computer tools, it is starting to look ever more difficult for the designer to recognize potential troubles with his design without the help of the network. The designer used to rely on knowledge he acquired through his studies but after the industrial revolution, it became necessary to put the design through design reviews so any oversights are caught by his peers before production. At the same time, the designer no longer was able to hold all knowledge needed to finish his design and he would rely on standards, reference books, and textbooks. Anybody who has carried out mechanical design in the 80s has the experience of looking up CRC books or ASME standards. And now, after the explosive revolution in information processing, it is now necessary to rely on the network as a repository of information and it is our task to extract from it what we need.

The designer today wants to plan against possible troubles with his design and implement mechanisms to prevent them or at least make sure that he sends out some warning signal, in the form of alarms to the user or warnings in the user’s manual to avoid litigations against him.

Tools for helping the designer identify such troubles include fault tree analysis (FTA) and failure mode and effects analysis (FMEA) [7] so he can make modifications to avoid trouble. These methods identify the most damaging scenarios based on probability assessment of element events that lead to accidents. Leveson developed System Theoretic Process Analysis (STPA) [8] for handling more complex systems including human factor. Visnepolschi extended TRIZ into I-TRIZ [9] to find failure mechanisms that are hard to recognize by asking the designer “how can the system accomplish the failure?”

These tools intended for accident prevention, however, are based on the designer’s knowledge, experience, and insight in identifying what can go wrong with his design.

Iino et.al. proposed a way of expressing the essence of a failure with a chain of phrases which they called the failure scenario [10,11]. A failure scenario describes three components of a failure, namely, cause, progress, and results, in a single sequence of phrases. Each component starts from the high level to the detail, e.g. for cause, “Poor Planning” to “Missed Deadline.” The failure scenario, however, did not have good applications other than describing the event with a sequence of phrases.

The act of design, however, does not start from such mind activity of “what could go wrong?” but instead starts from defining the problem, and then ideating how he will meet the functional requirement (FR), i.e., the fun part of design. Another tool useful in this phase of conceptual design is the Functional-Structural diagram (F-S Diagram).

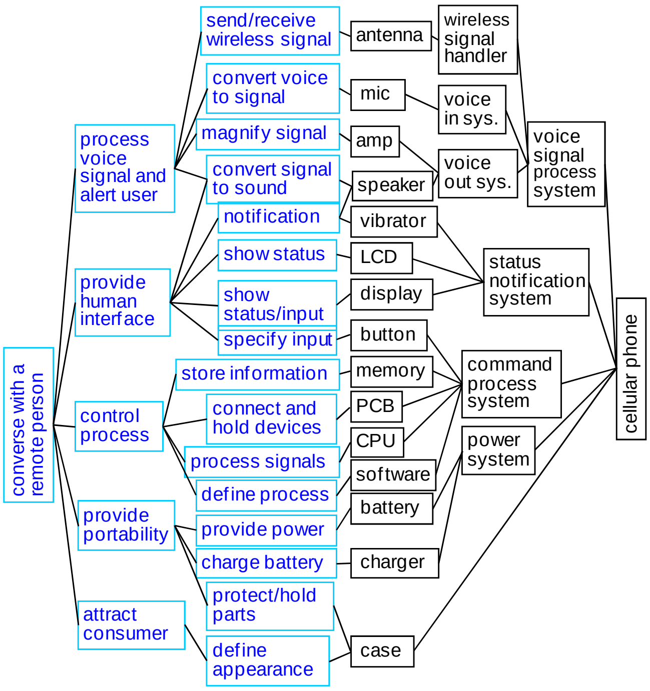

Fig. 3 F-S Diagram of a cellular phone (phone mode)

Although it is unclear to the authors who started F-S Diagrams, or even if there was a distinct starting point, design education at Stanford University [12, 13] and the University of Tokyo [14, 15] use this linked graph expression of functional and structural analyses in their design education. Fig. 3 shows a sample F-S Diagram for a cellular phone with the level of detail often used in university classes.

The F-S Diagram is a powerful tool in reaching a good solution given a clearly stated FR. We almost always use this tool for project/problem/design-based learning. In regular use, it proceeds from the left to the right, i.e., starts from the overall FR that iteratively decomposes to sub-FRs to element FRs that map to structural elements which then synthesize into sub assemblies and eventually to the overall solution.

This design tool does not help the designer in recognizing potential troubles with his design that he has overlooked either. It serves as the starting point of FMEA [13], however, in identifying the most damaging scenario out of all possible bad sequences of events that the designer can think about.

3. FAILURE PATH IN F-S DIAGRAM

Failure Path

A path in a linked graph is a route from one node to another. Instead of a failure scenario we suggested earlier for describing failure events, this paper proposes describing a failure event with the path it propagates in the F-S Diagram for the product. For example, with the cellular phone in phone mode with its F-S Diagram in Fig. 3, let’s say one of its buttons failed. The failure path in the F-S Diagram in this case is the path shown in Fig. 4.

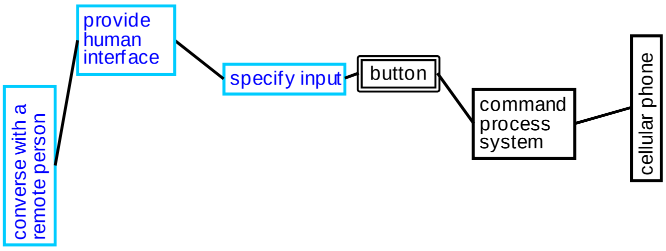

Fig. 4 Failure Path in the cellular phone F-S Diagram when a button fails

The path in Fig. 4 is taken out from Fig. 3 without straightening the links. There is no meaning to the geometric directions and lengths of the links other than they make it easier for the reader to identify the same path in Fig. 3.

Note the following for the failure path in Fig. 4:

- Failures in most cases start from a single point of failure with one of the structural elements in the F-S Diagram. In this example of cellular phone, it was the button noted with double lines in Fig. 4.
- There is at least a single path that passes through the above point of failure and connects the overall functional requirement ("converse with a remote person" in this case) and the product ("cellular phone").

A more common problem with cellular phones, and the same problem still persists with the newer smart phones, is the failure of the color display, or its partial failure of cracking. Fig. 5 shows the Failure Path for such troubles.

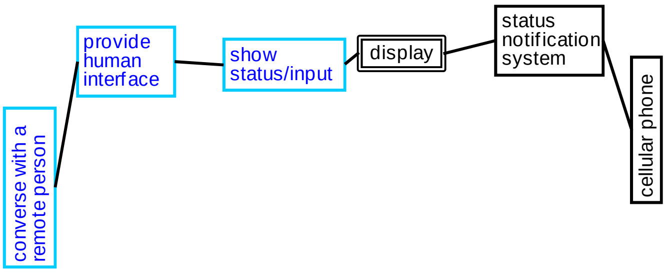

Fig. 5 Failure Path in the cellular phone F-S Diagram when the color display fails

Another sample with double paths is the failure of the speaker case (Fig. 6). The speaker on a phone has two functions of converting voice signals to sound that simulates human voice, and sending out a sound to notify an incoming call (if not in silent mode) and feedback beeps when buttons are depressed.

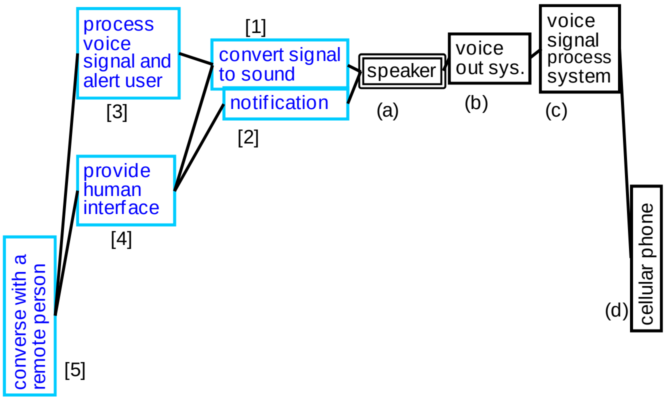

Fig. 6 Failure Paths in the cellular phone F-S Diagram when the speaker fails

Note the two links to the left of the origin node “speaker” and also to the left of one of the functional element nodes “convert signal to sound.” When we travel the paths to the left, we reach the overall functional requirement of “converse with a remote person.”

Altogether, there are three failure paths in Fig. 6 which are, from the left to right:

- [5] →[3]→[1]←(a)←(b)←(c)←(d)
- [5] →[4]→[1]←(a)←(b)←(c)←(d)
- [5] →[4]→[2]←(a)←(b)←(c)←(d)

The multiplicity of these paths, multiple parent child relations in both the function and structure sides, and where the structural elements meet the functional elements have to be noted because our design tool will automatically detect possible failures with conceptual designs.

Date Structure for Failure Path

As we saw in Fig. 6, links in failure paths are not necessarily one to one. The suitable data structure, therefore, is the same as that for F-S diagrams.

When we review Fig. 3 and try to record the details of the button failure, we notice that the link “specify input” to “button” can be further expanded. Fig. 7 shows the physical structure of the button and one level expansion of the F-S Diagram. Note that the failure of the button was caused by failure of the conductive pad; the pad wore out.

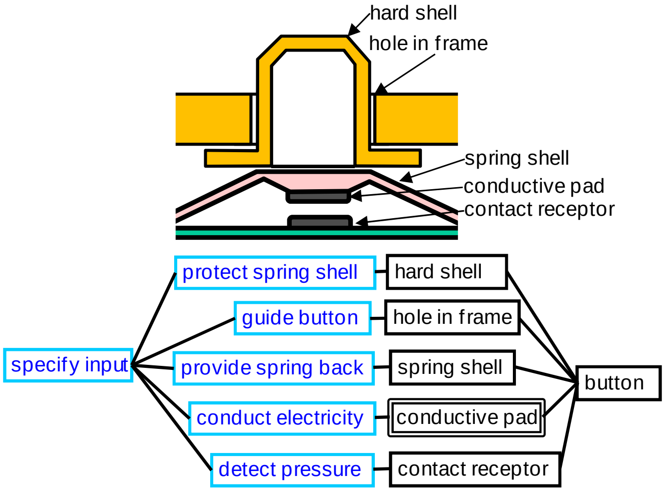

Fig. 7 Detail structure of button and part functions

The level of detail for an F-S Diagram is up to the person who is defining it. The level of the one in Fig. 3 is probably sufficient for the very early stage of conceptual design, however, the designer would want to define further detail as he proceeds to conceptualizing the detail. Also, note that different people draw different F-S Diagrams, i.e., there is no “correct” F-S Diagram for each mechanical product. Even the same person can draw diagrams with subtle differences on different days.

Given the above discussion, the designer would want to see the F-S Diagram with different levels of detail. This need is implemented with the user interface and that is not to be confused with the data structure. The F-S Diagram data structure stores all information to the level of detail as defined by the designer. The user interface shall expand and contract the tree representation as needed, e.g, the following tree in Fig. 8 is the same F-S Diagram as the one in Fig. 3, except it has contracted several levels from Fig. 3 for abstract conceptualization. The designer can then click, for example, the end of a link (circled red in Fig. 8. Note that it is not the link itself but one end of it.) to expand it. This will explode the part of the diagram one shown in the next Fig. 9.

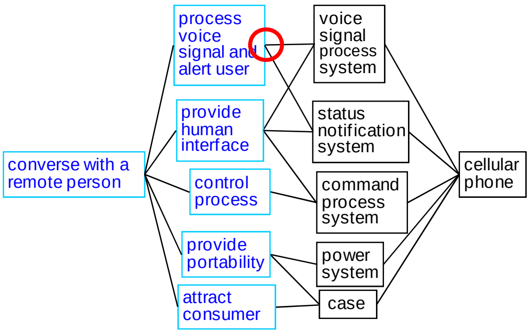

Fig. 8 Contracted F-S Diagram for cellular phone

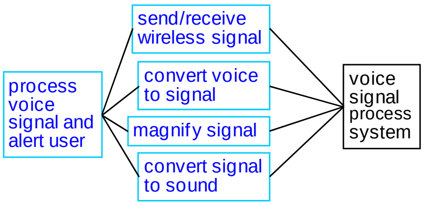
process voice signal and alert user
send/receive wireless signal
convert voice to signal
magnify signal
convert signal to sound
voice signal process system

Fig. 9 Contracted F-S Diagram for cellular phone (Part)

Such expansion and contraction is in the user interface and the data structure needed to store the F-S diagram is simply just the text in each node and who the parent of each node is. The special relation between a functional element and a structural element is defined by: "Functional element" realized by "Structural element" or "Structure" performs "Function."

4. SAMPLE CASE MATCHING

The TV Remote Case

To demonstrate the validity of our claim, we compared the case of button failure with the cellular phone with that on a TV remote. Fig. 10 shows the F-S Diagram for a TV remote. The diagram is much simpler, except the digital circuitry part has about the same complexity.

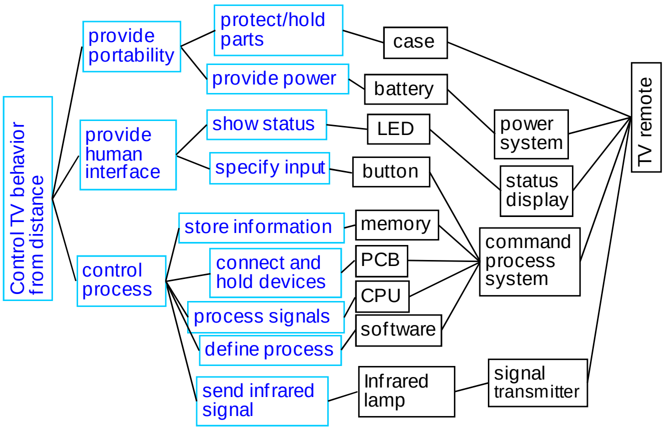

Fig. 10 F-S Diagram for a TV remote

Our search through failure cases with an F-S Diagram constructed for a specific product development proceeds as follows:

1) For every structural element in the F-S Diagram, search through the Failure Path base for matches at all levels.
2) If a match is found, look up the corresponding functional element in the Failure Path base.
3) If the corresponding functional element also matches that of the corresponding function for the structural element that started this round of search, the designer should study the failure case to see if his own design has a similar problem.

Going through this algorithm, the designer of the TV remote in Fig. 10 will find the matching failure path with a button failure in Fig. 4 for the structural element of “button” in Fig. 10.

The search was successful, however, we must recognize that if there was a case of, e.g., a button failure with a bigger machine, say an elevator with mechanical springs and metal contact, the corresponding functional element will probably be the same “specify input” thus the designer will be forced to look at this failure case as well. In other words, if the F-S Diagram the designer prepared is not at a detailed level, the designer will have to evaluate more failure cases than necessary. It is, therefore, advantageous to expand the F-S diagram to enough details, and for the same reason, the failure paths for known accident cases will be more helpful if they are expanded to a reasonable level of detail.

I-90 Connector Tunnel in Boston vs. Sasago Tunnel

Late at night on July 10, 2006, a section of concrete slabs in the ceiling of the I-90 connector tunnel en route to Logan Airport suddenly fell on a passenger car killing the 38-year-old wife in the passenger seat. The husband driver survived the accident [16].

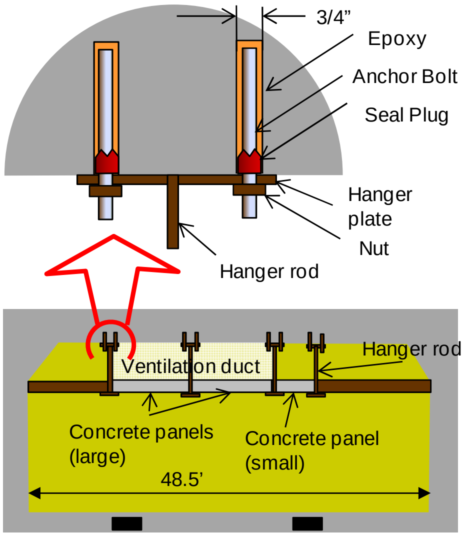

Fig. 11 Cross Section of I-90 Connector Tunnel

Fig. 11 shows the structure of the failed tunnel. The 2 rows of large concrete panels, each panel weighing about 4,700 pounds, that formed the bottom of the ventilation duct fell [17]. The support beam structure suspending the large concrete panels where the two rows meet fell with the concrete taking the threaded anchors with them. The National Transportation Safety Board reported [17] that a wrong type of fast drying epoxy glue was used and with the difficulty of injecting glue upwards without introducing bubbles the epoxy failed.

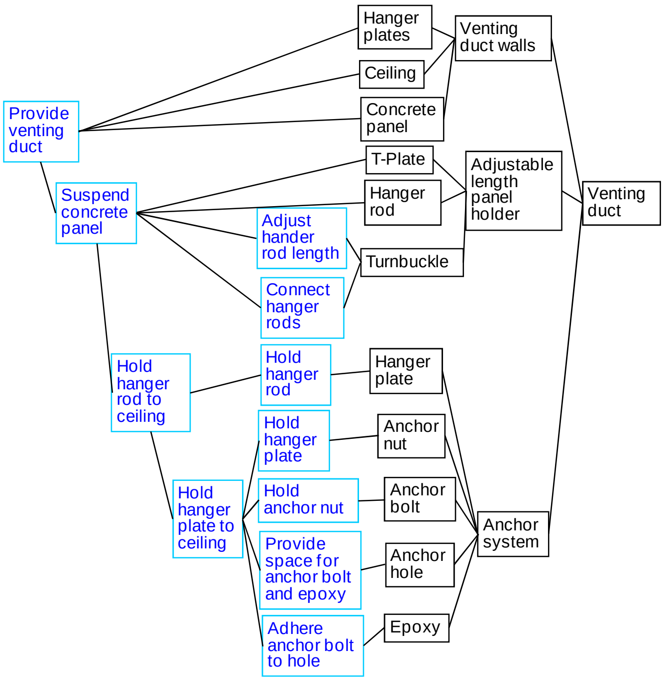

Fig. 12 F-S Diagram of the Venting Duct Sub-System

Fig. 12 is the F-S Diagram of the venting duct sub-system of the I-90 connector tunnel. The whole tunnel has a larger diagram with roads, lightings, shoulders, and walkways. Since the initial failure was attributed to the epoxy, we can extract the failure path as shown in Fig. 13

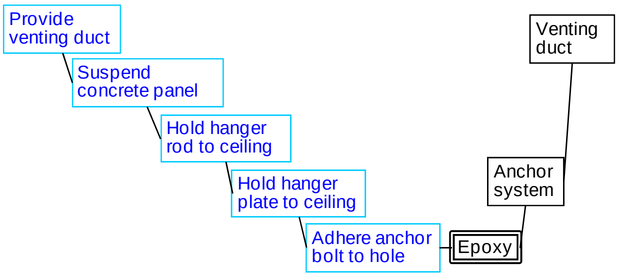
Provide venting duct
Venting duct
Suspend concrete panel
Hold hanger rod to ceiling
Anchor system
Hold hanger plate to ceiling
Adhere anchor bolt to hole
Epoxy

Fig. 13 Failure Path of the I-90 Tunnel Ceiling Collapse Accident

On Dec. 2, 2012, about 6 years and 5 months after the accident in Boston, ceiling panels in Sasago tunnel fell over a section of about 140m crushing 3 cars that were passing the tunnel. 2 of the crushed cars caught fire. The accident killed 9 people and injured 2 [18].

The Ministry and Land, Infrastructure, Transport and Tourism (MLIT) reported the accident was a result of combination of multiple causes, namely, insufficient bolt strength, epoxy degradation in the anchor, and poor inspection and maintenance.

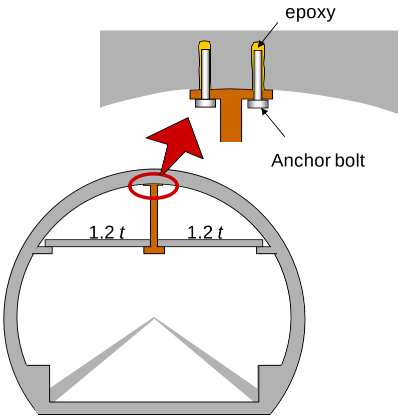

Fig. 14 Cross Section of Sasago Tunnel

Fig. 14 shows a simplified cross section of Sasago tunnel. As you can see, there is a striking resemblance to the I-90 Connector Tunnel in the basic structure. So if the designer of Sasago tunnel, or the maintenance company of it constructed the F-S diagram for the tunnel including its venting duct system, and worked out a fair amount of details when the F-S diagram lists epoxy as one of its structural elements, our proposed method will find the failure path and alert the designer to review the design.

Even if the designer of Sasago tunnel was at a very early stage, and constructed a simple F-S diagram like the one in Fig. 15, he will catch the failure path in the Boston accident when he searches the failure path base with the structural element “anchor system.”

We must note here, however, that we need to control the phrases the designer use for functional element. A creative designer who calls the “anchor system,” with a different name, say for example, “hanger to ceiling fixer” then the change of him catching the problematic failure path is slim. This concern is addressed in Section 5-1).

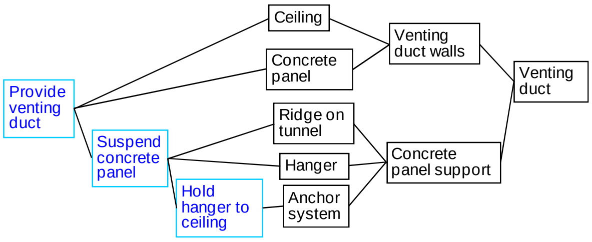

Fig. 15 Simplified F-S Diagram of Sasago Tunnel

5. FUTHER STUDIES

Our study has shown that we can effectively and automatically point out possible design flaws or areas that a designer has to pay attention to for avoiding accidents or failures with his design. He can do so by building a F-S Diagram for his conceptual design, and comparing its structural element list with those in a failure path base and see if the matches in the list have the same corresponding functional element with the design. If so, that part of the design calls for the designer’s attention.

There are a number of further efforts we have to make in polishing this system up for general use.

1) Standardization of words

The structural part of an F-S diagram consists of noun phrases. Standardizing phrases in this part, that is to use the same word for the same part seems reasonable. For example, a bolt is a bolt, and even if is a small one, use the word bolt instead of calling it a screw.

The functional part is more challenging. Phrases in this area usually take the form “verb + object.” We need to standardize the concept, e.g., of tighten, fasten, fix, and so on. A feasible solution will be to allow the user to define his functional phrase if he does not see it in the list of available ones and stick it onto the list of available functional phrases.

2) Large Failure Path base
We will need to construct a large database of failure paths from accidents that have taken place in the past. Fortunately, we have our hands on text data of accidents [19, 20, 21]. Our next phase is to define the failure paths for the cases listed in these databases.

6. CONCLUSION

When an accident breaks out, the criteria of whether the fault lies in the design, maintenance, or use phase varies over time. As the society gain more experience with new developments, and just more experience with existing machines, the responsibility that the design phase has to cover expands.

To develop a way to alert the designer about possible design flaws that he may not be aware of, we evaluated the following scheme:

1) Accident cases are collected in a database and each accident is described with a set of Failure Paths.
2) A Failure Path is a path in a F-S diagram from the overall functional requirement to the product and one that passes through the structural element that triggered the accident.
3) Once we have a large enough database of failure paths, the designer can build the F-S Diagram for his own design and look up the failure path database for all the structural elements in his F-S Diagram.
4) If a match is found and the corresponding functional element in the failure path is the same as the one in the designer’s F-S Diagram, the designer is alerted of a possible design flaw and will be forced to review the case to analyze his own design.
5) There is ambiguity in the detail level of an F-S Diagram and failure paths defined in the failure path database, thus, each structural element of the F-S Diagram is compared with all the structural elements and their higher level structural entities in the paths.
6) Building detail F-S diagrams will help the designer, and providing detail description for the failure paths in the accident and failure database will narrow the search and make it more effective.

REFERENCES

[1] R.Yoshioka and K.Iino, Technical Report: Fukushima Accident Summary, 2011, Association for the Study of Failure, Tokyo, Japan.

[2] K.Iino and M.Nakao, A Fatal Accident Case and Lessons for Entertainment Engineering, 2013, Proceedings ASME IDETC 2013, DETC2013-12133

[3] L.E.Gray, “A History of the Passenger Elevator in the 19th Century” 2002, Elevator World, Inc.

[4] K.Iino, Loss of a Gold-Headed Cane, 2009, Association for the Study of Failure [www.shippai.org/eshippai/html/index.php?name=news460]

[5] Elevator Escalator Safety Foundation, History of Elevators [www.eesf.org/education/public_2/elevator.html/title/history-of-elevators]

[6] Nikkan Kogyo Shimbun, “Poka-Yoke: Improving Product Quality by Preventing Defects”, 1987, translated 1988 by Productivity Inc.

[7] ASME International, Failure Analysis [www.asminternational.org/portal/site/www/SubjectGuideItem/?vgnextoid=0f97f5e96349d210VgnVCM100000621e010aRCRD#7]

[8] N.G.Leveson, “A New Approach to Ensuring Safety in Software and Human Intensive Systems”, MIT and Safeware Engineering, Inc., (www.acq.osd.mil/se/webinars/2009-07-07-SECIE-Safety-in-Software-and-Human-Intensive-Systems-Leveson-brief.pdf)

[9] S. Visnepolschi, How to Deal with Failures (The Smart Way), 2008, Innovation Systems, Inc.

[10] K.Iino et.al., Scenario Expression for Characterizing Failure Cases, Proceedings of the 2003 IDETC, ASME Chicago IL

[11] Y.Hatamura et.al., Structure of Failure Knowledge Database and Case Expression, Y.Hatamura, K.Iino, K.Tsuchiya, T.Hamaguchi, 2003, Annals of the CIRP

[12] P.Leung, K.Ishii, J.Benson, Modularization of work tasks for global engineering, 2005, Proceedings of IMECE2005, ASME, IMECE2005-82137

[13] K.Ishii and K.Iino, Value Creating Design (in Japanese), 2008, Yokendo, Tokyo, Japan

[14] Y.Hatamura, Decision-Making in Engineering Design, 2006, Springer-Verlag, London, originally published in Japanese, Koshite Kimeta, 2002, The Nikkan Kogyo Shimbun, Tokyo Japan.

[15] M.Nakao, Study of Creative Design (in Japanese), 2003, Maruzen, Tokyo, Japan

[16] To Forgive Design, H.Petroski, 2012, Belknap Harvard

[17] National Transportation Safety Board, Ceiling Collapse in the Interstate 90 Connector Tunnel, Boston, Massachesetts, July 10, 2006,
[www.ntsb.gov/doclib/reports/2007/HAR0702.pdf]

[18] “About the Ceiling Slab Fall Accident in Sasago Tunnel on Chuo Highway” Dec. 12, 2012, MLIT, (in Japanese)
[www.mlit.go.jp/road/ir/ir-council/pdf/3.pdf]

[19] Failure Knowledge Database
[www.sozogaku.com/fkd/en/index.html]

[20] M.Nakao, 100 Failure Cases (in Japanese), 2005, Morikita, Tokyo, Japan

[21] M.Nakao, Sequel to 100 Failure Cases (in Japanese), 2010, Morikita, Tokyo, Japan