Learning from failures through feedback to design

A. Labib
Portsmouth Business School, University of Portsmouth, UK

Abstract

The paper attempts to define the concept of learning from failures through feedback to design. This is demonstrated through case studies where analytical tools have been incorporated to facilitate problem structuring and analysis. We provide a framework on how to analyze case studies of learning from major disasters. We then provide examples of tools and techniques that are capable of analyzing the rare event of high impact.
Keywords: learning from failures, design, feedback, fault tree analysis, reliability block diagrams.

1 Introduction

In this paper generic lessons are identified based on the root causes of major problems and an understanding of how those problems unfold over time for organizations to use to avoid major failure.

Previous research of analyzing disasters has identified ten generic lessons for learning from failures [1]. In this paper we focus on three out of the ten lessons that are related to design and extend them. A brief account is provided about these lessons drawing on some similarities with other disciplines such as the maintenance function. We then provide a framework as a model for analysis using a case study to illustrate the concept.

It has been argued that lessons gained from major failures have not really been learnt by the very same organizations involved in those disasters and this is evidenced by recent reported case incidents of major organizations such as BP, NASA, and Toyota which are examples of this trend [1]. So what does 'learning' actually mean in the context of disasters? In response to this question, the same authors have proposed a model of the meaning of 'learning' in the context of

WIT Transactions on The Built Environment, Vol 134, © 2013 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE130581

disasters which is based on feedback to design, using advanced techniques and interdisciplinary generic lessons. In this paper, we focus on the feedback to design issue.

2 Design related generic lessons of learning from failures

The following three lessons have been chosen from the ten generic lessons provided by Labib and Read [1]. They were chosen as they are the most related to design issues. Here design is defined from a totality point of view to include design of organization structure, culture, information systems and procedures.

Lesson 1: The "I operate, you fix" attitude. In old-fashioned maintenance, a prevailing concept among operators is 'I operate, you fix'. In other words, maintenance is the responsibility of the maintenance department and operators should deal only with the operation of their own machines. When dealing with a disastrous situation this attitude frequently means most people feel the responsibility for dealing with a disaster lies with someone else. But it is important everybody, especially top management, is aware that a disaster is not just 'another issue' and that their direct involvement is necessary. The analogy of the maintenance function compared to safety function is an interesting one. For example, in Figure 1, one can see a comparison between old-fashioned attitudes

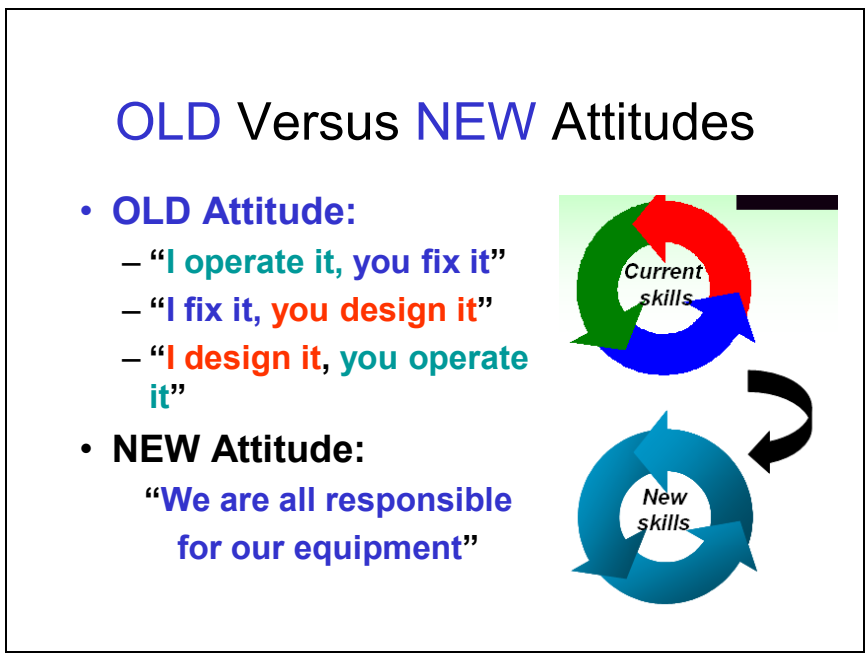


Figure 1: Old versus new attitude in maintenance (but can also apply to safety).

in maintenance (which used to be the prevailing attitude in the West) compared to the new attitudes promoted by the Japanese Total Productive Maintenance (TPM) philosophy. In old-fashioned maintenance, skills are fragmented and depicted in different colors in the figure. So the operator would claim '*I operate, you* [means maintenance people] *fix it*'. Then the maintenance engineer would claim in return '*I fix it, but you* [means designers] *design it*'. Finally, the designer would respond '*I design it, but you* [means operators] *operate it'*. We notice here that the prevailing culture is about shifting responsibility, and lack of ownership which leads to going in circles of shifting the blame to someone else, or to another function in the business. On the other hand, the new attitude should be pictured as all in one colored circle, which basically implies a culture of '*we are all in one ship, so we are all responsible*', and if it sinks we all drown. No attitude of 'them' and 'us', and ownership is shared among the whole team members. It is all about responsibilities.

Lesson 2: Solving a crisis is a forgotten experience. It is often the case that solving a problem does not get recorded or documented, but it is beneficial to both organizations and individuals to be able to easily access databases of mistakes or near misses. For example, in old-fashioned maintenance, it is often the case that solving a breakdown problem does not get recorded or documented. The reason is that it is often considered a bad experience that is usually forgotten. An analogy here is to imagine that you ask several applicants for a job to write their CV. It is most likely that they will all write about their achievements and none of the applicants will attempt to write about their bad experiences or any failures they had in their career; socially or academically. Nobody would be proud to mention them. On the other hand, modern maintenance techniques stress that a crisis is an opportunity for investigation, and failures should be well documented for future analysis. Unfortunately, in many near misses situations, organizations, and people, do not reveal their experiences with potential failing equipment or mistakes. One reason for that might be the fear of losing lawsuits and insurance claims. A good example is in the healthcare system [2]. It would, however, be beneficial to both organizations and individuals to be able to easily access databases of mistakes or near misses [3]. In this context, it is about communicating failures or near misses and responsibility to store and access lessons learnt. So in nutshell, a crisis is not the worst of failures, but not have tried to learn from it is the true failure, and hence failure can be regarded as success when we learn from it.

Lesson 3: Skill levels dilemma. In the maintenance function, the designer of the machine is not usually the one who fixes it, and surprisingly, might not even have the ability to do so. For example, skills needed to restore particular equipment include functions such as diagnostics, logic fault finding, disassembly, repair and assembly. Depending on the level of complexity of particular equipment, as well as on the level of complexity of the function that needs to be carried out, the necessary skill level can be determined. According to a survey conducted by McDonald [4] of aircraft maintenance technicians, approximately in one third of the tasks the technicians reported that they did not follow the procedure according to the maintenance manual. The technicians

reported that there were better, quicker, and even safer ways of doing the task than following the manual to the letter. McDonald [4] argues that manuals themselves are not an optimum guide to task performance as they have to fulfill other criteria, such as being comprehensive, and up to date. The question is: How to bring operator requirements to the forefront of the design process? Or How to feedback the knowledge, skills and experience of the operator, who is day in and day out in front of the machine, to the designer?

In a crisis, skill levels, and type, constitute a major dilemma because disasters tend to be multi-disciplinary problems as it can span various fields such as information systems, maintenance, decision making, and crisis and risk management and hence there is a need for a synchronized multidisciplinary team approach [5]. In summary, it is about communicating failures back to design and responsibility to store and access stored information.

3 Lessons learnt from maintenance and its application to disasters

The term 'drifting into failure' is a metaphor coined by Dekker [6] for the slow, incremental movement of systems operation toward (and eventually across) the boundaries of their safety envelope. In examining the maintenance domain, one can characterize the drift into failure as per the point of failure curve (abbreviated as the P-F curve) as shown in Figure 2.

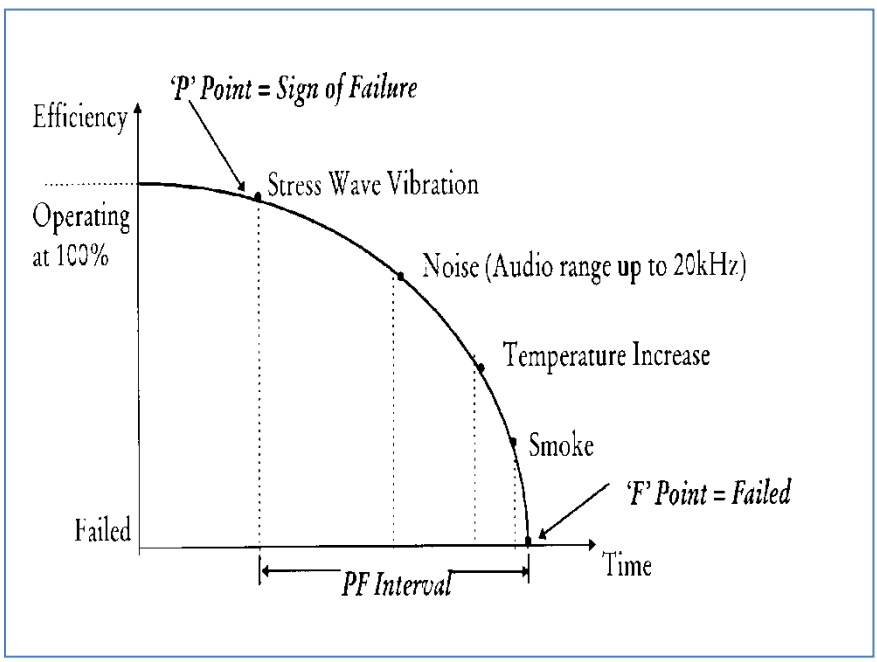


Figure 2: The P-F curve in maintenance.

The basic idea is that as failure propagates in time, the equipment is deteriorating in performance from the ideal 100% level of performance or efficiency, at the left of the curve and then over time as the equipment deteriorates in efficiency it is releasing some sort of energy in the form of a signal that can be captured if one has the sufficient monitoring capability. This signal is a form of energy, and according to Newton's law: energy does not disappear but transforms itself into different forms. So at the beginning the energy signal is in the form of wave that can be captured by a vibration analysis, then it is transformed into noise that can be captured by a monitoring device such as ultrasound, but then this energy creates friction that generates heat that can be captured by a temperature increase and so on. When a disaster happens there are usually some signals and it depends whether we have the ability to monitor such signals.

In the P-F curve one needs to be aware that the nearer one is from the P-point, which is the sign of failure, the more time one would have to act before a failure occurs and hence preventive measure can be taken, and vice versa the nearer we are towards the right where the F point (Point of failure) the less time we have to respond. On the other hand at the left of the curve the deterioration is incremental that one may in some cases confuse the signal with the noise.

Similarly, in a disastrous situation, there are some early warning signals but organizations vary at their capability to monitor and accordingly take sufficient action to prevent the realization of the complete failure.

The main challenge is about how can we implement a framework that facilitates the learning process from failures with respect to feedback to design.

In the area of decision making in maintenance, a model called the Decision Making Grid (DMG) was proposed by Labib [7] to facilitate selection of appropriate maintenance policies and process of feedback to design.

In the next section we attempt to introduce the DMG and adapt it into a framework for learning from failures and feedback to design.

4 The Decision Making Grid (DMG) model

The Decision Making Grid (DMG) model which was originated by Labib [7] has helped companies to select appropriate maintenance strategies. The DMG model has been used and reported by various researchers such as Fernandez *et al*. [8], Burhanuddin [9], Aslam-Zainudeen, and Labib [10], Shain *et al*. [11], and Tahir *et al*. [12]. All literature have reported considerable saving in terms of minimising downtime and significant maximisation of productivity without having to acquire any additional capacity.

The DMG acts as a map where the performances of the worst machines are placed according to multiple criteria. The model is illustrated in Figure 3. The objective is to implement appropriate actions that will lead to the movement of machines towards an improved state with respect to multiple criteria.

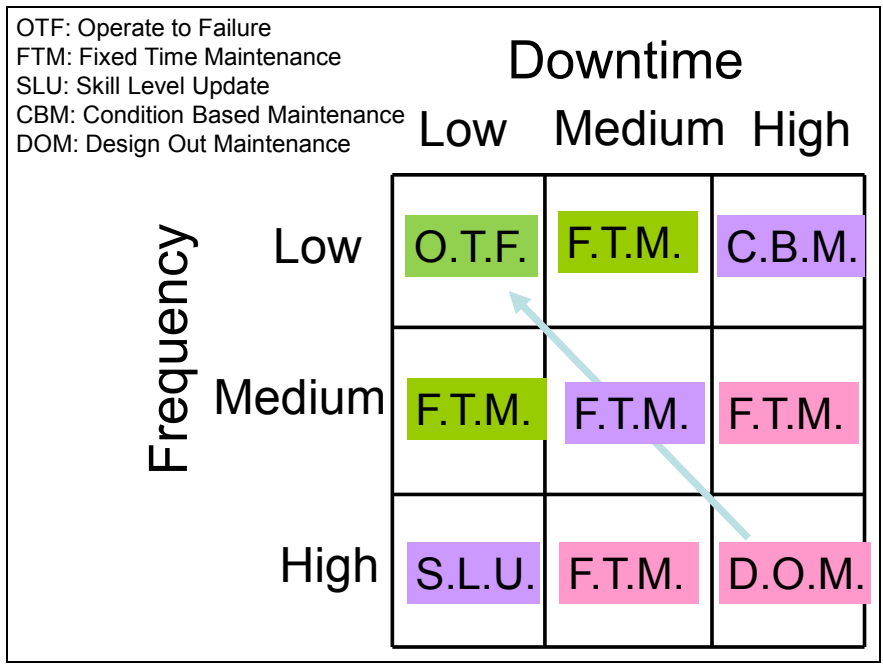


Figure 3: The Decision Making Grid (DMG).

The objective from the grid is to implement appropriate maintenance strategies that will lead the movement of machine toward an improvement machine status in the grid. In the next section we explain the suggested maintenance strategies and the equivalent safety measures in case of learning from failures and disasters.

Suggested strategies:

(i) **Operate to Failure (OTF), or Keep the Best Practice:** This strategy is implemented when the machine rarely fails as compared to others, and once failed the downtime is short. OTF also implies sustaining the best practice that already exists on this machine. In the safety domain, this region is about sustaining current practice with respect to the status quo, i.e. business as usual.

(ii) **Fixed Time Maintenance (FTM):** This strategy uses preventive maintenance schedule (some call it pre-determined maintenance), implemented when failure frequency and downtime are almost at the moderate cases. It the safety field, this is the region where we analyze our existing checks of systems, safety barriers, and back-up systems.

(iii) **Skill Level Upgrade (SLU):** Upgrading skill level of operator, because machine has been visited many times (high frequency) but can easily be fixed (low downtime). In the safety domain, here we

are addressing frequent incidents of low impact and the suggestion is to focus on training and awareness of how to implement safety measures and procedures in the most efficient way.

(iv) **Condition-Based Maintenance (CBM):** This is used to analyze the breakdown event and closely monitor its condition. It is when the machine does not breakdown often but take long time to fix. In the safety field, we are here addressing a high significant event that is also rare, which is a feature of a disaster. It the state where investigative strategy is being deployed, and the focus is to find the root cause and make recommendations with respect to how to monitor and analyze such an event in order to either eliminate its possibility of occurrence or mitigate its impact when it re-occurs.

(v) **Design Out Maintenance (DOM):** DOM is the most crucial area in the grid. Machines in this region are recommended to go for a major design out or overhaul project. This is because the machines experience high downtime and high frequency. In the safety field we are dealing here with a disastrous situation that has been repeated. It reminds us of examples such as NASA (Challenger, and Columbia), or BP (Texas, and Deepwater Horizon) cases. The strategy is to examine a situation that is currently not fit for purpose and hence a reconfiguration, or re-design strategy should be followed. Either to get rid of the status quo (for example stop the space shuttle program), or design a resilience strategy as a fundamental mechanism to prevent occurrence, minimize significance and increase ability to detect and monitor.

The methodology is implemented as follows: (i) Criteria analysis: Establish Pareto analysis of the criterion; (ii) Decision mapping: Mapped the criterion in the matrix; and (iii) Decision support: Identifying a focused action to be implemented.

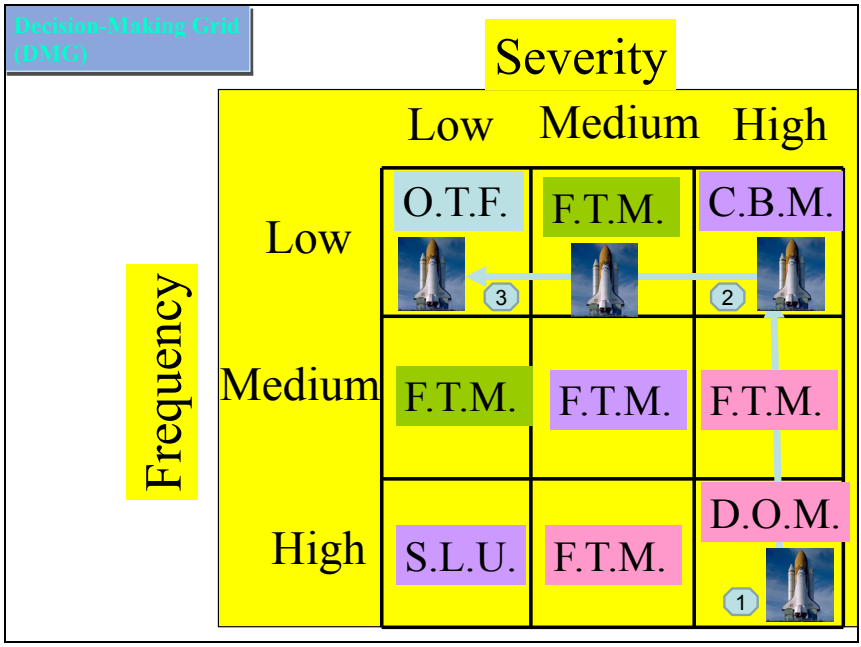
In a disaster situation one could have the two dimensions of ‘acute’ versus ‘chronic’ goals, instead of ‘downtime’ versus ‘frequency’ as in the traditional DMG.

5 Case study of applying the DMG to a disaster analysis

In a near-miss disaster, NASA’s space shuttle, despite undergoing a Design-out phase, had to be repaired by an astronaut with the help of a robotic arm, based on discovering a misplaced piece which could have resulted a repeat of a catastrophic failure.

The question is how can one sketch the Decision Making Grid (DMG) model and place the different stages which the shuttle has gone through starting from the Design-Out (DOM) Stage.

An example of a possible solution:



The shuttle was redesigned (Design Out Maintenance DOM) after a disaster that has occurred in a previous mission. The DOM has resulted into installing cameras and remote monitoring devices, which is a condition based maintenance (CBM) strategy that were able to capture the disoriented part. When the situation happened again the reduction of significance, or severity through CBM, which had to be repaired by an astronaut with the help of a robotic arm, lead the shuttle to land safely in the Low Frequency Low Severity range, and the situation was back to normal and the repeat disaster was avoided, job well done. So in summary; this case study shows how the condition of the shuttle moved from stage 1 at DOM to stage 2 at CBM and ultimately to stage 3 at OTF. There might be other cases where the outcome of the DOM strategy may lead to the movement to SLU state and eventually to the favorable OTF state.

6 Conclusion

The case study demonstrates how the DMG can be used to model failures in terms of their acute and chronic dimensions. Running the DMG model over time shows that as long as the movement is from the DOM state is towards the direction of the OTF state, then this means that our resilience strategy is working well and hence the DMG can be used for detection and assessment as well decision support with respect to safety.

References

[1] Labib, A. and Read, M., Not just rearranging the deckchairs on the Titanic: Learning from failures through risk and reliability analysis. Safety Science, 51(1), pp. 397–413, 2013.
[2] Barach, P. and Small, S.D., Clinical review Reporting and preventing medical mishaps: lessons from non-medical near miss reporting systems. British Medical Journal (BMJ), pp. 759–763, 2000.
[3] Kim, J. Y. and Miner, A.S., "Vicarious learning from the failures and near-failures of others: Evidence from the U.S. commercial banking industry." Academy of Management Journal 50: 27, 2007.
[4] McDonald, N., Organizational Resilience and Industrial Risk, in Resilience Engineering Concepts and Precepts, Eds. Hollnagel, E., Woods, D.D., Leveson, N., Ashgate, England, 2006.
[5] Labib, A.W., The millennium problem versus the maintenance problem. Logistics Information Management, 12(3), pp. 254–258, 1999.
[6] Dekker, S., Resilience Engineering: Chronicling the Emergence of Confused Consensus, in Resilience Engineering Concepts and Precepts, Eds. Hollnagel, E., Woods, D.D., Leveson, N., Ashgate, England, 2006.
[7] Labib, A.W., A Decision Analysis Model for Maintenance Policy Selection Using a CMMS, Journal of Quality in Maintenance Engineering (JQME); MCB Press; Vol 10, No 3, pp 191–202, 2004.
[8] Fernandez, O., A.W. Labib, R. Walmsley, D.J. Petty, "A Decision Support Maintenance Management System: Development and Implementation", International Journal of Quality and Reliability Management, IJQRM, Vol 20, No 8, pp 965–979, 2003.
[9] Burhanuddin, M.A., An application of Decision Making Grid to improve maintenance strategies in small and medium industries, Proceedings of the 2nd IEEE Conference on Industrial Electronics & Applications, pp. 455–60, 2007.
[10] Aslam-Zainudeen, and Labib, Ashraf, Practical Application of the Decision Making Grid (DMG), Journal of Quality in Maintenance Engineering (JQME); MCB Press; ISSN: 1355-2511, volume 17, issue 2, pp 138–149, 2011.
[11] Shain, A, Ranjbar, M, and Abedi, S, ,Critical Discussion On The Relationship Between Failure Occurrence And Severity Using Reliability Functions, Management Science And Engineering , Vol. 5, No. 1, pp. 26–36, 2011.
[12] Tahir, Z., Burhanuddin, M.A., Ahmad, A.R., Halawani, S.M. and Arif, F., Improvement of Decision Making Grid model for maintenance management in small and medium industries, Proceedings of the International Conference of Industrial and Information Systems (ICIIS), Sri Lanka, pp. 598–603, 2009.