Chapter 3
Are Failures the Pillars of Success?

3.1 All Life Is Problem Solving

Engineering is one of the oldest and most characteristic examples of a problem solving enterprise. It is concerned with transformation or useful change, and change almost always occurs when there is a felt need or problem. Sometimes of course change is brought about through seeking an opportunity for improvement, even without a perceived problem. A key feature of engineering is design, which Christopher Alexander (1964) has described as the ‘elimination of misfits’—i.e. ‘misfits’ between a current solution and its context.

Change is frequently associated with risk. A person who takes no risks will cause little change. Part of this risk refers to the chances of not achieving what one sets out to do. Another part is the risk of unforeseen effects or unintended consequences. Thus, in the process of solving problems engineers can create new problems too. A good example is how technology is blamed for environmental degradation, both in terms of pollution and resource depletion. However, such problems can be seen as fresh ‘grist for the mill’; many engineering activities are now directed towards conserving the environment. This solving of problems that gives rise to new problems and challenges is highly reminiscent of Sir Karl Popper’s (1902–1994) cyclic scientific methodology. This chapter builds on the pioneering paper of Blockley and Henderson (1980) in applying Popper’s ideas to engineering (see also Dias 2007).

3.2 Popper’s Problem Solving Methodology

Karl Popper was one of the most dominant and influential philosophers of science in the 20th century. Scientists can perform exceptionally well without being aware of any philosophies of science (Lipton 2005); but most practising scientists would operate as Popperians, whether consciously or not. Popper (1968) considered that the main philosophical problem to be solved was that of the question concerning

P. Dias, *Philosophy for Engineering*, SpringerBriefs in Applied
Sciences and Technology, https://doi.org/10.1007/978-981-15-1271-1_3

knowledge and its growth. He sought to understand the growth of knowledge in general by studying the growth of scientific knowledge, which he considered as having the fastest rate of growth. His work focused also on the scientific *method* (Magee 1973), held by him to be of crucial importance to the growth of knowledge. Other philosophers have downplayed the importance of 'method' (Feyerabend 1975), but practising scientists and engineers would largely agree that method is very important.

The popular view about method, prior to Popper's influence, was that science grew through a process of what could be called *inductive generalization*. The inductive process starts from making a succession of observations or conducting many experiments; and ends by making generalizations or arriving at theories, based on the results of those observations or experiments. It can therefore also called be an *empirical* (or practical) method. For example, we observe that a metal expands every time it is heated; also that this property is displayed by more than one metal. We can therefore make a generalized tentative hypothesis that "all metals expand when heated". We then subject this to verification in order to prove or disprove the hypothesis. Good inductivists will test a wide range of metals under different initial temperatures and ranges, and ensure that no observation violates the hypothesis, before pronouncing that the hypothesis has been 'proved'.

David Hume (1711–1776), although being an empiricist, saw that inductive generalization was not strictly logical. He pointed out that repetitions of 'particular' (or specific) observations could not logically give rise to universal theories. Any future expectations we had based on past regularities were *psychological* rather than *logical*. Theories could never be verified logically, because there would always be a chance that the sequence of regularity could cease or change. As put by Magee (1973), "from the fact that all past futures have resembled past pasts, it does not follow that all future futures will resemble future pasts".

In addition, one of the main problems with induction is its focus on *verification*. Popper (1989) argued that a more self-critical approach was required for the growth of knowledge; this would also restore a sense of humility to scientists. He proposed the following scientific methodology for replacing inductive generalization (Popper 1999; Magee 1973): (i) (old) problem; (ii) proposed tentative trial solution—a conjecture; (iii) deduction of crucial testable propositions; (iv) critical testing—attempted refutations; (v) (new) problem(s). The new problem will not arise unless and until the proposed solution or conjecture has been disputed.

The important thing in the above scheme is the recognition that science starts with a problem, and not through the 'disinterested' observation of entities. These problems could typically be gaps or anomalies in existing theories—e.g. their lack of comprehensiveness, or correspondence with observations. The above scheme is cyclic as well, in that the new problems will require new conjectures and so forth—hence, it would encourage the growth of knowledge. Furthermore, we see that the first step towards solving the problem is not observation or experimentation, but rather a proposed trial solution or hypothesis. Even if we did set out on some initial observations or experimentation, Popper said that we had, even sub-consciously, some half formed or tentative solution that we were trying out—in other words, a *conjecture*. Such conjectures could be based on our background knowledge; but imagination or aesthetics could be allowed to shape them too.

Once a conjecture or hypothesis was stated, some implications of this hypothesis could be arrived at by the process of *logical deduction*. The deductions made were not to be trivial ones, but those that were crucial for testing the hypothesis or extending its scope. Such deductions could then be tested by observation or experiment. So the movement here is from theory to experiment—the opposite of induction. The approach is also very self-critical, because Popper said that such testing should constitute attempted *refutations* of conjectures, or *falsifications* of hypotheses. We see from this that Popper is promoting falsification rather than verification. He was against verification, first because it was logically erroneous. No amount of confirming instances of tests could 'verify' a theory, because it could always fail such a test in the future; on the other hand, even a single failed test could falsify it. There was thus an 'asymmetry' between verification and falsification (Popper 1983). Also, a focus on verification would not promote growth in knowledge, whereas the replacement of a theory by a better one would.

Let us move from the *overthrowing* of theories to another way in which knowledge can grow. This is by the *improvement* of theories. Such improvement too could be assisted by a falsificationist outlook. Magee (1973) gives a good example of this. Suppose we state the hypothesis that "water always boils at 100 °C". If we had a verificationist outlook, we would merely be content to find many confirming instances of water boiling at 100 °C. However, a falsificationist would try to devise critical and novel methods of trying to falsify this hypothesis. Such a person would probably discover that water does not boil at 100 °C at elevated altitudes or in closed vessels. The hypothesis would then need to be framed in a more comprehensive and fundamental manner, and perhaps give rise to the idea that "water boils when its saturated vapour pressure is equal to that of the surrounding atmosphere"—thus resulting in a growth of knowledge.

It should be noted that Popper (1968) also used the concept of '*falsifiability*' as a criterion of demarcation to judge whether a body of knowledge could be called 'scientific' or not. In other words, for a discipline to call itself a 'science', its theories had to be enunciated in a way that it was possible to test and falsify them. On this basis, he refused to admit that the social sciences (in particular Marxism) and psychoanalysis were sciences, because their proponents tended to 'explain away' disconfirming instances; or expand their theories arbitrarily to accommodate such disconfirmations, rather than changing them.

3.3 Extending the Methodology

Solving a problem by first positing a conjecture was a scheme that Popper said applied to all knowledge. Popper broadened his theory of scientific knowledge to encompass our entire evolutionary history, which to him was the growth of knowledge through problem solving. He drew parallels between the 'random' genotype variations in

Darwinian evolution and the ‘bold’ conjectures in his scientific methodology, for which an element of ‘irrationality’ was virtually indispensable (Popper 1968); also between the ‘survival of the fittest’ at the phenotype (or organism) level as a result of a harsh environment and the critical testing of propositions for refuting theories in his methodology. He also called this process ‘error elimination’ (for both species and knowledge evolution). Popper compared the now discredited Lamarckian theory of evolution (where changes in species were supposed to accumulate at the phenotype level) to the idea of knowledge accumulation through induction, which he strongly disputed. The other feature of importance, whether of biological or scientific evolution, was the crucial ingredient of feedback (Popper 1972). A cyclic methodology such as Popper’s strongly emphasized learning from feedback. It was such feedback that resulted in error elimination and hence progress. Popper considered that the growth of knowledge formed a seamless web “from the amoeba to Einstein”, the amoeba being eliminated by evolution when it *makes* mistakes so that more robust species can evolve; whereas Einstein *looks* for mistakes in order to improve or even discard his theories in favour of better ones (Popper 1999).

The idea of feedback leads us to another area of Popper’s inquiry we shall look at—that of social change. Popper’s ideas of critical rationalism, error elimination and progress of knowledge in the evolutionary and scientific domains led to his arguing for an ‘open society’ in the political sphere. He was particularly opposed to shaping society based on predictions. “If it is possible for astronomy to predict eclipses, why should it not be possible for sociology to predict revolutions?” he asked (Popper 1960; Dias 2014); and proceeded to show why not. For one thing, he did not consider theories of society to be as dependable or testable as theories concerning science, since the former involved much greater complexity, including the essential unpredictability of human beings. It could be argued that such historical ‘laws’ were merely generalizations of trends and not really laws (Popper 1960). There are similarities between such ‘trends’ and the generalizations made in scientific induction to arrive at universal theories, a method rejected by Popper as we have seen. Induction can also be compared to generating a relationship between a dependent and independent variable by curve fitting after a series of observations. The best we can do through such fitting is to discover a *trend*, and not a *law* based on some genuine natural phenomenon, such as energy for example.

Popper was therefore opposed to shaping the long term future of society based on some grand utopian scheme, as espoused by Plato or Marx, both of whom he labelled as ‘enemies of the open society’. Popper argued that change had to be ‘engineered’ from a given situation, calling it ‘piecemeal social engineering’ (Popper 1960). This has similarities with starting from a problem situation in Popper’s scientific methodology, and with the idea that the growth of knowledge is evolutionary, with errors being eliminated through ‘feedback’ during each cycle of growth. How then could we ensure ‘error elimination’ in society? For one thing, Popper advocated that it be possible for those who rule to be removed periodically. He said therefore that the important question was not “Who should rule?” as raised and pursued by Plato and Marx, but rather the question of “How can rulers be removed?” (Popper 1999). For another, Popper valued a society with diversity. He considered the lack of a unifying

Table 3.1 Common themes from Popper across Evolution, Science and Society (from Dias 2007)

Domain →	Evolution	Science	Society
Problem domain (P)	Survival	Knowledge	Governance
Creativity of trial solution (TS)	Random variation in genotype	'Irrational' elements in hypothesis; also competing hypotheses	Pluralism in society
Error elimination (EE) method	Harsh environment (nature)	Critical testing (scientific community)	Public opinion (population)
Error elimination (EE) result	Extinction	Refutation	Change of rulers
Problem solving scheme	Natural selection (Darwinian)	Cyclic methodology: P_i → TS → EE → P_{i+1}	'Piecemeal social engineering'
Rejected alternative	Lamarckianism	Induction	Historicism
Result of alternative	–	Authoritarianism	Tyranny

idea in western democracies to be a strength rather than a weakness (Corvi 1997). Compare this to the diversity required in the gene pool for successful Darwinian evolution.

Table 3.1 presents Popper's remarkably unified ideas regarding problem solving in three distinct domains, namely evolution, science and society. All of them have a problem generating environment, and methodologies for proposing creative solutions and error elimination. The ingredients for incorporating creativity in solutions were considered by Popper to be very important; it was these elements that rescued his methodology from the bonds of induction. The critical approach to error elimination was equally or more important. The pluralism, public opinion and change of rulers required in the social sphere led Popper to argue for liberal democratic political systems. The problem solving scheme for the scientific domain consisted of his cyclic methodology of old problem → trial solution → error elimination → new problem. This had parallels in the other two domains too. Although his methodology was conceived for replacing the alternative of induction in science, similarly unsatisfactory parallels for induction were identified by Popper in the other two domains. Notturno (2000) has argued that an inductivist outlook could lead to authoritarianism in scientific institutions, while Popper himself was very clear about the link between sociological generalizations and social control, which led to tyranny.

3.4 Cyclic Engineering Processes

It is not only the *idea* of problem solving that makes Popper relevant to engineers; his *mode* of problem solving—i.e. a *cyclic* mode—is also something that is frequently used by engineers, especially in design. Engineers in design organizations would like to make design a linear process, i.e. to start with a set of specifications and end up with a solution. But in principle and often in practice, design is a circular process. Figure 3.1 presents the design cycle of specifications—synthesis—analysis—evaluation and compares them with the key elements of Popper's methodology. We shall consider each element in turn.

We start with the *specifications*, analogous to Popper's 'problem'. An engineering problem has to be formulated or defined through a set of specifications that have to be

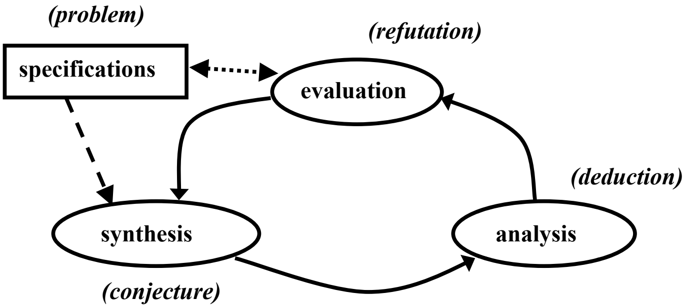

Fig. 3.1 Engineering design methodology and Popper's problem solving methodology (from Dias 2007)

satisfied by the design. Specifications can be seen as performance criteria or functions expressed in engineering terms. Conflicting specifications are often encountered in engineering; so the problem is not merely to satisfy the specifications, but also their conflicts. For example, an architect may want a beam not to exceed a specified depth so that the ceiling provided under the beam will have a sufficient clear height above the floor. On the other hand, the services engineers may want the air conditioning duct also placed within the ceiling. This is quite apart from the engineering specifications that the beam itself has to satisfy—i.e. that it should be strong enough to carry the loads imposed on it without deforming excessively.

The next step in design is to posit a solution, similar to a Popperian conjecture. This is called *synthesi*s. The step from specifications to synthesis is often a difficult one. This is where creativity in design comes into play, comparable to Popper's 'irrational element' that is required for a conjecture—for example proposing a beam with a pierced web in order to satisfy the architectural, services and engineering specifications described above. Factors such as memory (of *past* designs), perception (of the *present* context) and scenarios (of *future* usage or deterioration) are all required for synthesis (Blockley 1992). Synthesis is difficult to automate and in principle cannot be done via an algorithm or mathematical model. There is also the issue that design involves abductive reasoning or finding an 'inverse solution' (see Sect. 2.3)—where there may be more than one way to meet a single set of specifications. The managing of conflicting specifications via creative solutions (e.g. a pierced beam) is also part of synthesis.

If the design is a fairly routine one, experienced engineers will be able to make a guess at a good initial solution which may not even need to be changed subsequently. Younger engineers may be able to use 'rules of thumb' (frequently referred to in Chap. 2) that have been developed over the years. Nowadays they may be able to resort to Artificial Intelligence techniques (see Chap. 8); these can help us to propose solutions based on past experience (Dias 2002; Dias and Padukka 2005). Creative solutions can sometimes be generated using techniques of Artificial Life, an example of which is described at the end of this chapter—these techniques are often based on a Darwinian metaphor, giving us another link to Popper.

Once we have synthesized a solution, we can resort to the *analysis* of that solution. Analysis is well supported by mathematics and software. This constitutes, to a large extent, the engineering science component of the engineering process (see Fig. 2.2). For civil, structural and mechanical engineering it is underpinned essentially by Newtonian mechanics. The process of analysis can be compared to Popper's testable deductions, which are derived from the conjectured hypothesis.

The next step is to compare the results of our analysis with the specifications—a process of *evaluation*. If our original solution was either unsafe or too conservative, this comparison will show it up. This is the engineering parallel to Popper's idea of refutation. Engineers may think they are checking or trying to verify that the solution they proposed is satisfactory. But especially when trying to optimize their designs, a better way to think of evaluation is that it is a way to refute their proposed syntheses; or 'falsify' them, in Popperian language. Consider the design process for optimizing the form of the Tianjin CTF Finance Centre for wind loading using a wind tunnel (Cammelli 2018); a total of 17 different aerodynamic solutions were developed and tested in an interactive fashion. Another way to design is by comparing solutions that are proposed as candidates—for example the four alternatives tested for the Ridgeway Footbridge (Willoughby 1996). Both in optimizing and comparing alternatives we see that proposed solutions are in fact being rejected after critical testing. Trial and error procedures are very characteristic of engineering (Vincenti 1990), even during actual construction. For example, geotechnical design solutions are sometimes arrived at via feedback from monitoring the unfolding soil response (LeMasurier et al. 2006).

In Fig. 3.1, the comparison with the specifications is shown with a double-headed dotted line. Normally, the specifications are held as the standard against which a design has to be measured, and failure to comply will demand a fresh synthesis (i.e. a new conjecture). However, if the specifications have been defined too tightly or with conflicting constraints, they may need to be changed or relaxed. Clearly this has to be done with the consent of the client, while taking into account the safety of the public.

It should be noted that the specifications are not really part of the main cycle in Fig. 3.1, especially in the more routine design situations where specifications are not changed after evaluation. The core engineering design cycle is synthesis—analysis—evaluation. Some authors (Coyne et al. 1990) denote this cycle as analysis—synthesis—evaluation. The analysis referred to by them is problem analysis, inclusive of defining specifications. It requires broad engineering knowledge and an appreciation of the 'big picture'. In Fig. 3.1 this type of analysis is subsumed under 'synthesis' (and perhaps specifications). The 'analysis' referred to in Fig. 3.1 on the other hand is the narrower type of analysis that can be tackled by engineering science techniques (e.g. mathematical models); but it also includes the creative envisaging of future scenarios for which the synthesis has to be analyzed.

It may also be noticed that the synthesis, analysis and evaluation cycle refer mostly to activities rather than states, with the arrows between them in Fig. 3.1 merely serving as links between activities. The design cycle can be depicted using states too; then it is the arrows linking them that will denote activities or transformations. In order to do this, we shall build on the well-known triad of ‘function—structure—behaviour’; and use the following symbols, after Umeda et al. (1990) and Hybs and Gero (1992):

F: function
S: structure (i.e. synthesized design object)
P: product (i.e. fabricated object)
Be: behaviour that is expected (based on specifications)
Bs: behaviour of the design object in an appropriate (mathematical) model
Ba: behaviour that is actually exhibited by the fabricated product

The following transformations can be identified:

F → Be: specification
Be → S: synthesis
S → Bs: analysis
Bs ↔ Be: evaluation
S → P: fabrication
P → Ba: operation
Ba ↔ Be: diagnosis

The transformations involved in the activities of specification, synthesis, analysis and evaluation are made explicit here. In addition, the wider cycle of the *world* in which the design object is realized, becomes evident (see Fig. 3.2). The role played by the behaviours is of crucial importance. They are the means by which comparison and correction are carried out—note the double headed arrows above. We saw earlier that comparison within the design cycle was called evaluation; this leads to improved design objects through repeated syntheses. On the other hand, comparison in what we shall call the *world cycle* can be called *diagnosis*; this should lead to improvements in the entire design cycle, or the ‘calculation procedure model’ (Sect. 2.3), as it has been called by Blockley and Henderson (1980). Diagnosis could indicate shortcomings in fabrication or operation too, but the sensitive designer should try to design against as many fabrication and operational errors as possible with an ‘idiot-proof’ design (Dias 1994).

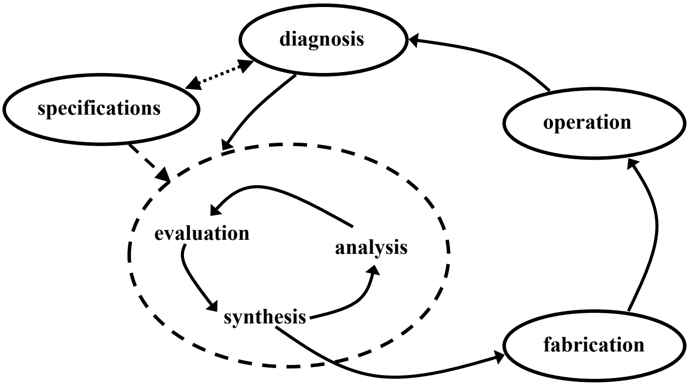

Fig. 3.2 Design cycle embedded within world cycle (from Dias 2007)

We are now in a position to compare the two cycles, i.e. the design cycle and the world cycle, with Popper's cyclic methodology for the growth of scientific knowledge—see Table 3.2. The problems (both old and new) for the two cycles differ, being the specifications for the design cycle and a failure in the 'calculation procedure model' (CPM) for the world cycle. The crucial difference is in the conjecture. In the design cycle, it is the synthesized design object that is the conjecture (analogous to a scientific theory), which is subjected to refutation through evaluation. In the world cycle, it is the entire design cycle or CPM (which is a closer analogy to a scientific theory) that is being tested (by diagnosis) with respect to its performance in the world (inclusive of construction and operation in that world). The world cycle is therefore a much wider and longer term one—since failures may not show up for a long time—and embeds within it the design cycle (Fig. 3.2). The knowledge generated through the world cycle is long term and industry-wide in nature; whereas in the design cycle it is project-specific and short term—i.e. in the process of trying to test our design object against various failure modes through a CPM. In the design cycle, we generally do not question the validity of the CPM. It is the *design object* that is being tested for fitness. In the world cycle on the other hand, *the entire CPM*, inclusive of all mathematical and heuristic models used, is being judged.

Learning through feedback in cyclic processes is very much a part of management practice today (Senge 1992; Checkland and Scholes 1990), for example as embodied in the art of reflective practice (Blockley 1992; Schon 1983; Dias and Blockley 1995). Recall that engineers are more managers than scientists (Sect. 2.3). Consider the representation of an organizational or even industry-wide activity. Although it can be seen as a linear process of converting inputs to outputs and waste, as in Fig. 3.3a, it is probably more realistic and helpful to view it as a circular process, as in Fig. 3.3b. The latter representation portrays the idea that the organization does not remain static during its operations—it changes too; and hierarchically nested reflection can lead to improvements, at one level through learning by reflecting on the transformation process, and at a deeper level by reflecting on and evaluating the

Table 3.2 Popper's cyclic methodology compared with the design cycle and world cycle (from Dias 2007)

		Design cycle	World cycle
Popper's categories	(Old) problem	Specifications	Failure
	Conjecture/hypothesis	Synthesis or design object	Calculation procedure model or design cycle
	Testable deductions	Analysis	Fabrication and operation
	Refutation/testing	Evaluation	Diagnosis
	(New) problem	Specifications	Failure
Nature of growth in knowledge	Extent	Project-specific	Industry-wide
	Duration	Short-term	Long-term

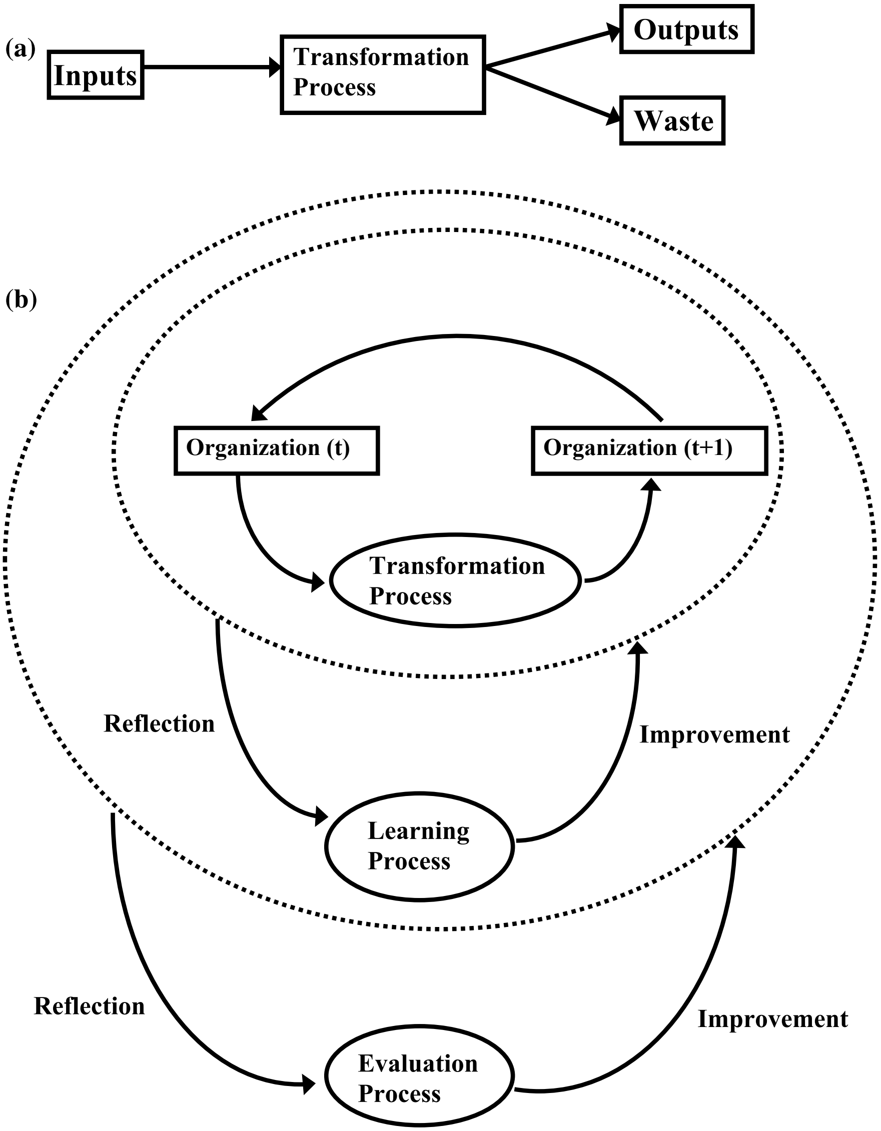

Fig. 3.3 Organizational process viewed as **a** linear and **b** circular (from Dias 2007)

learning process itself. Learning within organizations can be promoted by asking the question "*What* did we learn from our experience?" from time to time; while evaluation can be a more structured exercise carried out periodically (e.g. annually) by asking the question "*How* did we learn during our experiences?" or "*How* can we improve our learning process?".

3.5 The Role of Failure in Engineering

Popper's great innovation was that a theory could only be falsified, as opposed to being verified. If we consider the design cycle, where the synthesized design object corresponds to Popper's conjecture, we have seen that falsification is precisely what we actively try to do. Engineering is steeped in a culture of safety. This means that we are always trying to identify modes of failure, in order to design against them. Henry Petroski's book *To Engineer is Human*, is subtitled *The role of failure in successful design* (Petroski 1969); one of its chapters is called 'Success is foreseeing failure'. For the structural engineer, the 'ultimate' failure is collapse. However, a structure, or any other engineering product, can fail in many other ways.

The ultimate limit state (i.e. the point beyond which failure would occur) is certainly the most *important* one in structural engineering. However, a serviceability limit state—i.e. a point beyond which a structure would not be useable (e.g. by exhibiting excessive cracking or deflection)—could be more *critical*, in that it could be the criterion that governs the design. This is very common in prestressed concrete structures and water retaining concrete structures, where the amount of steel wires or bars required for the limiting of crack widths to below a desired value is often greater than the steel required for preventing collapse. What happens in practice is that engineers make the initial synthesis based on their background knowledge regarding what the critical limit state is. If the design checking satisfies the criteria for that limit state, the chances are that all other limit states, when subsequently checked, would be satisfied by that solution as well. The difficulty is in obtaining a good initial solution, so that it will not need to be changed many times. Design can indeed be seen as cyclic, and the fact that many analyses and design checks need to be done reflects that cyclic nature. However, designers would prefer not to make changes in the synthesis or design object after each test. The choice of good initial solutions depends on accumulated engineering knowledge and reflection thereon (Dias and Blockley 1995); this can be based on an engineer's own experience or that of his company or even that of the entire industry. Later on in the book (Chap. 8) we explore how Artificial Intelligence techniques can capture and process such experience.

An important aspect of foreseeing failure is that we try to design not only for the 'normal', but also for the 'abnormal'. There are two ways in which we can deal with unforeseen disasters. The first is to build redundancy into the system. In structural engineering this is equivalent to providing alternative load paths—i.e. ensuring that there can be sharing of the load that is shed if one element fails accidentally. The other is to make sure that failure takes place safely; in other words, to provide *fail-safe* mechanisms (Dias 1994). In structural engineering, this is achieved through ductile failure modes. We design structures so that if there is unanticipated overload, the elements will exhibit cracking and deflection prior to collapse. This will provide warning for inhabitants to take remedial action or vacate the building. Ductility is also required for redistributing any loads shed by failed members to alternative load paths.

We could even think of ‘ductility’ at the structural level, by trying to arrange for members ‘higher up’ in the load chain to fail first. In addition to providing warning as before, this will prevent the catastrophic failure of more heavily loaded members ‘lower down’ the chain by reducing the load on them—i.e. the load previously carried by the failed member (Dias 1994). For example, there is a documented failure of a 32 m span prestressed concrete girder at a cement works due to dust accumulation on the roof (Dias et al. 1994). The load from the dust accumulation was transferred to the girder first via roofing sheets that spanned just 1.2 m between concrete purlins, that in turn spanned 9 m between the girders. If the sheets or the purlins had failed first, the large scale failure could have been avoided. The concept here is like the electrical engineer’s fuse in an electrical circuit; in order to prevent the failure—i.e. melting of the wires in the circuit due to an unforeseen electrical overload—a predesignated element, i.e. the fuse, will melt first because its thermal capacity is made to be lower than that of the wires. If such failure occurs, we merely replace the small fuse rather than having to re-wire the entire circuit; the ‘failure’ is much smaller and easily managed. Micro circuit breakers have now replaced fuses, making failure even easier to deal with.

So we see that within the design cycle, the aim is to actively falsify our conjecture (in the form of a design synthesis), in order to improve on it—very much a Popperian objective. One of the ways in which such falsification takes place in science is if there are *alternatives*. This is true in engineering design too—especially of large or novel products or systems. More than one solution to the specifications will certainly be generated at least at the conceptual design stage in the design cycle. The alternative that does better in the design checks (tests) is the one adopted for fabrication in the world cycle—see also Sect. 3.4.

How about the world cycle? Can we seek active falsification there too? Recall that our conjecture here is the design cycle or the calculation procedure model (CPM)—see Table 3.2. It would be nice to find ways to test the accuracy of the CPM; in other words, can we build a structure and subject it to failure, to check how accurate our CPM is? Automobile manufacturers try to do this by their ‘crash tests’. This is because an automobile is a mass produced artefact and testing a few to failure can be tolerated in order to fine-tune the associated CPM—although here too the actual performance during or after prolonged use cannot be tested. Buildings and bridges are however one-off artefacts; each one is unique, at least with respect to the ground it is founded on. Especially in structural engineering therefore, we cannot actively seek failure in the world cycle, because engineering is carried out within a social matrix. If such engineering products are fabricated to test the ‘truth’ of the CPM by testing them to ‘failure’, the public would be greatly inconvenienced, if not incapacitated or even killed. Technology underpins the entire fabric of our society. We have to make sure, as far as possible, that there are no breakdowns.

In other words, we are not interested primarily in the *truth* of our CPM, but rather about whether it constitutes a *safe* and *dependable* method for fabricating products that will be operated in the world (Blockley 1980; Blockley and Henderson 1980). Science on the other hand is carried out within the confines of a laboratory, where theories can be put to the test and active falsification sought. This is why scientific knowledge grows so rapidly. These distinctions between scientific theories and engineering models are further described in the next chapter (Sect. 4.5). In ancient days, there were strict penalties that were imposed on builders who did not deliver safety, as exemplified in the code of Hammurabi, 6th king of Babylon (1792-50 BC) and cited in Petroski (1969):

> If a builder build a house for a man and do not make its construction firm and the house which he has built collapse and cause the death of the owner of the house, that builder shall be put to death.
>
> If it cause the death of the son of the owner of the house, they shall put to death a son of that builder.
>
> If it cause the death of the slave of the owner of the house, he shall give to the owner of the house a slave of equal value.
>
> If it destroy property, he shall restore whatever it destroyed, and because he did not make the house which he built firm and it collapsed, he shall rebuild the house which collapsed at his own expense.
>
> If a builder build a house for a man and does not make its construction meet the requirements and a wall fall in, that builder shall strengthen the wall at his own expense.

However, if and when engineering failures do occur, they provide invaluable opportunities for improving or even overthrowing our CPM, and thus for industry-wide growth in engineering knowledge. Engineers are therefore very interested in failures, since they provide scope for learning. It has been argued (see Fig. 2.2) that the CPM could be seen as having an engineering science core, surrounded by ‘shells’ of idealization, margins of safety, design philosophy, design context and engineering process. While the engineering science core is now mature and unlikely to grow very much, there is still much scope for learning in other aspects, as we shall see in the next section, which gives an example each of failure in the six components of the CPM. It must be appreciated that reflection on over-conservatism and unnecessary use of materials—i.e. the opposite of failure—also leads to changes in the CPM. The availability of powerful structural analysis programs for example, reduces to a large extent the need to make conservative idealizations. Also, the use of reliability theory has been used to reduce margins of safety, where they have been unnecessarily large (Beeby 1994).

3.6 Failures in Various Components of the CPM

We start with a defect in an *engineering science* theory described by Petroski (1992) and discussed by Dias and Blockley (1994). It has to do with Galileo’s wrong assumption that a cantilever behaved like a beam hinged at the bottom edge of its fixed end, with a uniform tensile stress σ across its section resisting the overturning moment caused by the load W at the end of the cantilever (see Fig. 3.4a). The maximum load that could be carried can then be obtained as $W = \sigma bh^2/2L$, where h, b and L are dimensions of the cantilever as in Fig. 3.4a. The correct stress distribution however

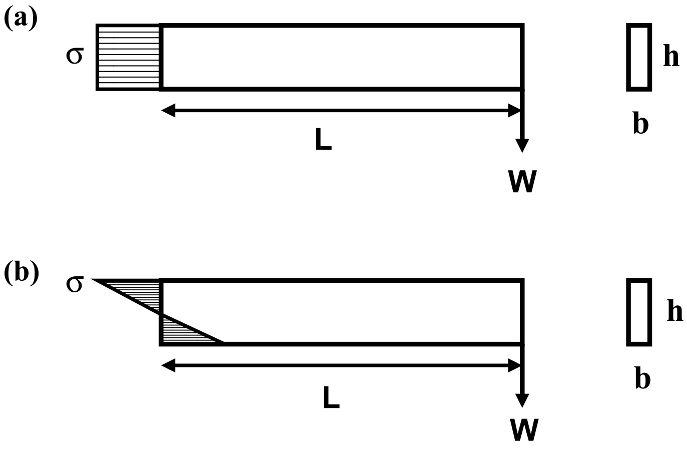

Fig. 3.4 Maximum longitudinal stress, σ, in cantilever beam: **a** as per Galileo; **b** actual (after Petroski 1992)

is shown in Fig. 3.4b, where σ is the maximum stress and the corresponding value of maximum load is $W = \sigma bh^2/6L$, which is three times lower than Galileo's estimate.

Even though Galileo's theory would have been used in real structures such as timber ships for example, given that Renaissance shipbuilders were likely to have used factors of safety in excess of 3, Galileo's error was not discovered. This shows that the safety of a structure does not guarantee the truth of the CPM. Blockley (1980) says that the CPM, as realized in most structures, is only 'weakly not falsified'. There may be components in the CPM, such as Galileo's hypothesis in this case, that are erroneous, even though structures based on it do not collapse. The great pity where Galileo's hypothesis is concerned however, is that it could have been falsified and corrected by careful and critical laboratory testing; for example by testing the beam in axial tension, in order to ascertain the value of σ. This example shows the importance of a critical and falsificationist approach towards our hypotheses, as advocated by Popper.

Figure 3.5 shows the schematic view of a roof truss with two end supports and a central one. In normal practice, such trusses are constructed with a (laterally) free or sliding end. This is to allow the truss to expand and contract with variations in temperature without setting up any internal stresses. Also, the assumption of fixed conditions at both ends would require full lateral restraint at end supports—a condition difficult to achieve in practice. The truss however, had been idealized during analysis as having both ends fixed, because it was to be rigidly welded to the tops of steel columns. The result of this is to change the structural action from the usual continuous beam to an arch; and the stress state in the bottom chord from the usual large tension at the two midspans (with large compression near the central support), to a small compression throughout. Therefore, the truss had been fabricated with a fairly small bottom chord section. However, the relatively slender columns to

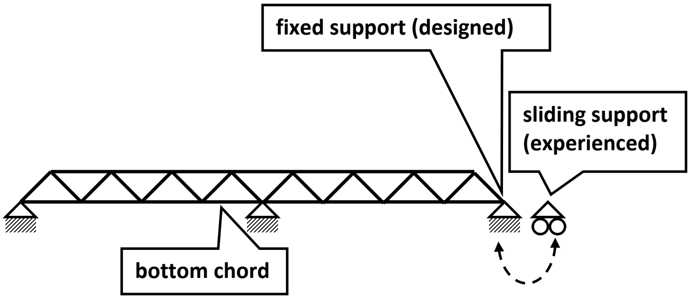

Fig. 3.5 Idealization of roof truss (after Anwar 1997)

which the truss was welded would have deflected laterally due to the truss loads; and the trusses actually behaved as continuous beams (and not like arches as idealized). This caused the bottom chord to fail either in compressive buckling near the central support or in tension at the site fabricated splices near the midspans (Anwar 1997).

This was clearly an error in *idealization*. Changes in boundary conditions can cause large differences in internal stresses, and such mistakes can very easily be made in today's design climate, where many easy-to-use computer software packages are available for structural analysis. This is a cautionary tale, not only with respect to the need for correct idealization, but also with respect to the proper use of software (MacLeod 1995). Idealization errors can occur for loads too—for example, idealizing snow loads as uniformly distributed ones may not capture the more onerous case of a varying load, and can cause collapse (Pidgeon et al. 1986).

A good example of a failure due to an inadequate *margin of safety* is the collapse of the Dee Railway Bridge in 1846, reported by Petroski (1994) and Sibly and Walker (1977). The Dee Bridge was made of cast iron girders. These were sized at the time based on a formula by Hodgkinson, which gave the central load that could be carried by such a girder of given length, depth, and area of tension flange. The emphasis was on the tension flange because cast iron was much weaker in tension than in compression; and cast iron girders were fabricated with a large tension flange but a small one in compression. By the time Robert Stephenson designed the Dee Bridge, around 15 years of construction using such girder bridges had elapsed; and spans had increased from around 25 feet to the 98 foot spans of the Dee Bridge. Although it was common practice to use global factors of safety of around 3–4, Stephenson chose to use one of only 1.5, since he thought that he was also strengthening the girders with wrought iron trussing (see Fig. 3.6). One of the three bridge spans collapsed when a train was crossing it.

In the subsequent inquiry, contemporary engineers suggested factors of safety ranging from 3 to 7. The problem with Stephenson's factor of safety was not only that it was rather insufficient in itself, but that it was also clearly inadequate in the context of the level of understanding regarding the interaction between the wrought iron truss and the cast iron girders. It is likely that the prestressing effect of the wrought iron ties created additional bending and compression in the girders, causing

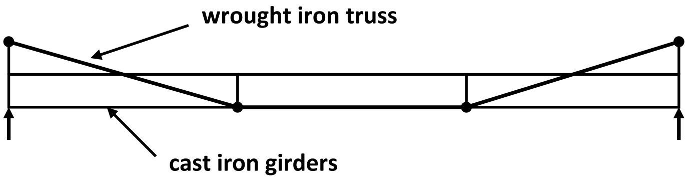

Fig. 3.6 Main structural elements in Dee Bridge (after Petroski 1994)

them to fail by lateral torsional buckling, given the small compression flange. This problem would have been exacerbated by the geometric imperfections in terms of out-of-straightness in Stephenson's long girders. Such imperfections and stress levels in shorter girders would not have been sufficient to cause failure by lateral torsional buckling. However, this second order effect became the critical mode of failure for the long spans of the Dee Bridge, especially with the reduced factor of safety. An undamaged girder from the Dee Bridge tested by Stephenson was found to fail at a load much lower than that predicted by the Hodgkinson formula. Given that the Dee Bridge was the longest of its kind to be constructed, it could be argued that a higher margin of safety should have been used, especially because the truss-girder interaction was not well understood. Hence we could say that the margins of safety component was falsified by this catastrophe.

One of the most significant structural failures of the 20th century was the partial collapse in 1968 of the 22 storey Ronan Point apartment block in Camden Town, East London in the U.K. (Levy and Salvadori 1992). The block had been constructed in the post war years using precast elements, which enabled the city to be reconstructed quickly after the war bombing. Both loadbearing walls and floors were made of precast concrete panels that were factory-cast and assembled on site. Early one morning at around 5:45 am, a resident on the 18th floor had attempted to light a gas stove; whereupon there was an explosion as a result of an unnoticed gas leak. The explosion pushed out some loadbearing walls on that floor. This caused the walls above that floor, and the slabs they supported, to collapse, since they had now lost their bearings. The resulting debris on the 18th floor kitchen slab caused that slab to collapse as a result of overloading, and precipitated similar collapses on all the lower floors. Four persons were killed, a number that could have been much greater had the explosion been at a later time of day. This brought into focus two issues with respect to *design philosophy*—one, the importance of structural integrity, and the other, the principle that the consequences of an accident should not be disproportionate to the cause. As expressed lucidly in a previous British code of practice (CP 110: 1972):

> The layout of the structure in plan, and the interaction between the structural members, should be such as to ensure a robust and stable design: the structure should be designed to support loads caused by normal function, but there should be a reasonable probability that it will not collapse catastrophically under the effect of misuse or accident. No structure can be expected to be resistant to the excessive loads or forces that could arise due to an extreme cause, but it should not be damaged to an extent disproportionate to the original cause.

As a result, designers today are very conscious of the above ideas. For example, in the subsequent British code of practice for concrete (BS 8110: 1997), all provisions for ensuring stability and robustness were highlighted in a flowchart. The main approach to ensuring robustness and preventing progressive collapse is to ensure that all concrete elements are properly tied by reinforcement. If they cannot be so tied, the designer has to assume that each untied element is 'lost' in turn, and ensure that the rest of the structure can still stand up, albeit under reduced loads and/or factors of safety. In fact, for structures designed against bomb explosions, elements are generally considered 'lost' in turn, whether or not they are tied to the rest of the structure.

We next consider a failure in design *context*. A part type plan for two storey school buildings in Sri Lanka is shown in Fig. 3.7. During the 2004 Indian Ocean tsunami, the oncoming and receding waves caused severe scoring in the corner column foundations in two such structures, causing collapse of the end bays. These buildings with two lines of parallel column and pad footings had thitherto performed well under a range of conditions. However, it failed in the context of some locations on the eastern Sri Lankan coast that directly faced the tsunami-generating Sumatran fault. Figure 3.7 shows how the introduction of a new column and infill walls in end bays could make the design more robust in such contexts (Dias et al. 2006).

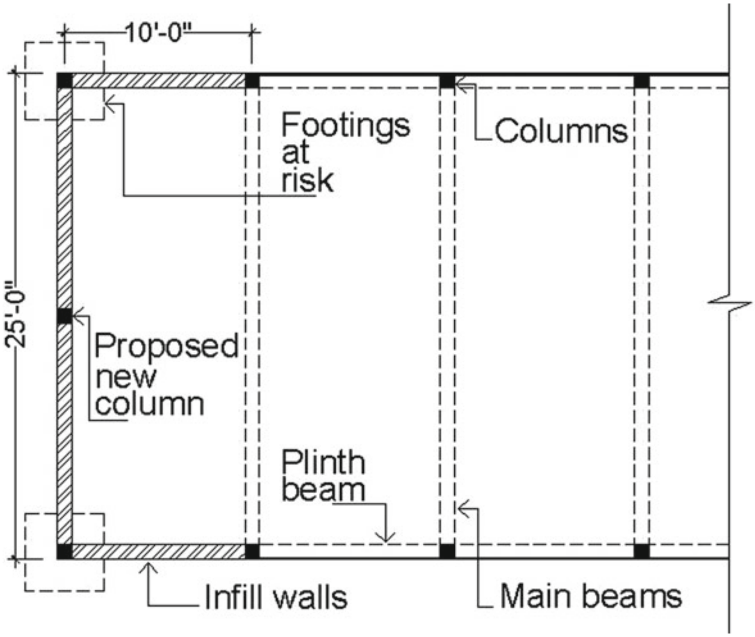

Fig. 3.7 Proposed new column and infill walls in type plan of school building to prevent failure in conditions where scouring is expected (after Dias et al. 2006)

Perhaps the most complex component of the CPM is the *engineering process*. This involves, among other things, unambiguous communication, especially of design intent. The failure that best illustrates this is the collapse of the suspended walkways at the Hyatt Regency Hotel in Kansas City, Missouri, U.S.A. in July 1981, shortly after it was constructed (Levy and Salvadori 1992). The 120 foot long walkways were at 2nd, 3rd and 4th floor levels, and enabled residents in the main residence block (with guest bedrooms) to access a function block (that housed meeting and dining rooms) without having to go down to the atrium. The walkways were suspended by hanger rods from the roof of the atrium. The 3rd floor walkway was on one side of the atrium; while the 2nd and 4th floor walkways were on the opposite side, with one hung under the other. During a well-attended dance competition in the atrium, which guests watched from the walkways as well, the 2nd and 4th floor walkways collapsed together into the crowded atrium, killing 144 persons and injuring over 200 more.

Upon investigation, it was found that the main cause of collapse was the fact that the walkways had not been hung as originally intended by the designer. The main structural elements of the walkways were two wide flanged beams that ran on both sides of a walkway along its length. These were supported, at 30 foot intervals, by transverse box beams, obtained by welding together two channel sections. Vertical holes were drilled through the ends of these box beams to pass the hanger rods. In the original design, the same hanger rod passed through both 2nd and 4th floor walkways, with nuts and washers below the beams holding the walkways to the hangers (see Fig. 3.8a). In the drawings submitted by the contractors however, this detail had been changed to that shown in Fig. 3.8b, where the lower 2nd floor walkway was carried not directly on a ‘through’ rod, but via a rod segment by the 4th floor walkway. The drawings had been stamped ‘Approved’ by the architects, and ‘Reviewed’ by the structural engineers. It transpired later that the change had never been checked,

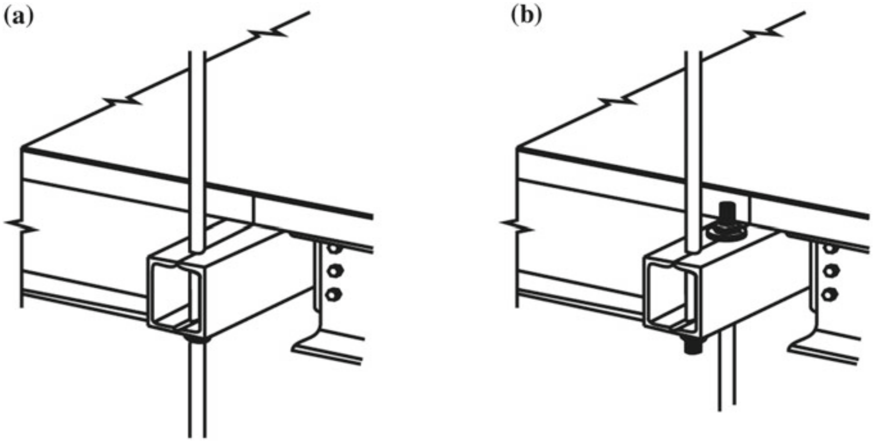

Fig. 3.8 Connection detail for Kansas Hyatt Regency walkways (4th floor): **a** as designed and **b** as constructed (after Delatte 2009)

presumably because it was considered a minor ‘detail’. As it happened, this change in detail completely changed the load carrying behavior of the walkway system.

The original design was analogous to two men hanging one under another on the same rope. The change corresponded to the lower man hanging on the upper man. The grip of the upper man on the rope now becomes all important, and would be the weakest link. The strength of the rope is not the critical issue. In the same way, failure was initiated in the walkway system (as discovered in subsequent testing), by the nut at the bottom of the 4th floor walkway box beam punching through its hole. It was also discovered that there was no redundancy built into the design. Once a connection was broken, other hanger rods did not have the capacity to carry the extra load, despite the fact that the number of people on the walkways was well below the design loading. In addition, it was found that the capacity of the nut and washer connection was only 60% of the prescribed value.

This failure teaches us many lessons, for example that more than one error was involved in the failure; and also the importance of details. However, the main lesson it teaches us is the importance of proper communication. The contractor did not understand the significance of hanging both walkways on the rods independently. And most outrageously, the designer did not see the implications of the change in detail made by the contractor. Also, the contractor may have made the change because constructing to the original detail could have been very difficult. It would have involved very long hanger rods, and may have necessitated cutting threads in those rods all the way from the 2nd floor to 4th floor level, quite apart from threading nuts through that length. This shows that perhaps the designer was not designing for constructability. All of this is part of the design cycle. So, in this failure, above all it was the engineering process component of the CPM that was falsified. There is much greater emphasis now on improving the design process and promoting teamwork among different players in that process.

3.7 The Genetic Algorithm for Optimization and Design

Popper’s evolutionary scheme involved not only a cyclic process, but also an element of *randomness*, especially when he brought Darwinian evolution also into his general theme of ‘error elimination’. Here too, there are parallels in engineering, particularly through its embodiment in the genetic algorithm. The use of genetic algorithms is not confined to engineering although its pioneers, Holland (1975) and Goldberg (1989) were both engineers. There are two broad areas in which the genetic algorithm has been used, the first for optimization and the second for generating novel solutions in design.

Both optimization and design can be considered as *search* problems. In both cases there is the problem of having a large number of parameters, each of which could have a large number of values or states. In optimization, the problem is how to search this vast multi-dimensional space so that an optimal or near optimal solution is obtained. In design, the problem is how to select combinations of parameters that will constitute novel or creative designs. It should be noted that cycling through the design and world cycles, as described before, will probably result only in incremental changes, or changes from one known solution to another. Many researchers have been interested in finding schemes to generate novel solutions, and a genetic approach seems promising because that appears to be the way that novelty has been introduced in nature too.

What then are the basic principles and steps of the genetic algorithm (GA)? There are three aspects to the scheme, mirroring the natural selection process, i.e. (i) survival, (ii) reproduction/crossover and (iii) mutation. In addition, there are analogies between the 'phenotype' and the physical solution on the one hand; as well as the 'genotype' and a low level representation of the solution (generally as binary strings) on the other. The binary string comprises concatenated (i.e. joined up) bit strings, each of which represents a particular state of a variable. So if a variable has 8 discrete states that need to be checked, each state can be represented by a binary number that ranges from 000 to 111; only 3 bits are required to represent the 8 states of that variable. If there are 3 such variables whose values define the solution, each of the variables with only 8 discrete values, then an entire solution can be represented by a $(3 \times 3 =)$ 9 bit binary string comprising the three separate bit strings for each variable. The trial solution that is represented by such a concatenated string can be tested with respect to an objective—e.g. minimizing the self-weight of a load carrying structure defined by the values of the 3 variables. These strings correspond to the genotypes in Darwinian evolution.

We could start off with a given population of strings, say around 50 for example, with the bits of the strings (i.e. the ones and zeros) assigned purely randomly. The solutions that are represented by each string can then be evaluated, after mapping the binary states back to the variable space. The trial solutions correspond to the phenotypes (or species) in Darwinian evolution. We can now rate the 50 solutions with respect to their 'fitness'. If this is a weight minimization problem, small values of the objective function (i.e. weight of a given solution) will be assigned a higher fitness—this can be done in some arbitrary way, but desirable solutions must be assigned with higher numerical values of fitness. Constraints will also need to be imposed—e.g. to ensure that a solution does not violate stress limits. We then have to ensure that the phenotypes 'survive' in proportion to their fitness. This should be done in a probabilistic fashion, for example by using a 'weighted roulette wheel' (Goldberg 1989). Phenotypes with larger fitness will probably be chosen many times, while those with smaller fitness may not be chosen at all. The total population size must remain the same as before—i.e. 50 in our case. This is the GA's version of the 'survival of the fittest'.

The next process is 'reproduction' or 'crossover', this time at the level of the genotype, where parts of strings are combined with those of others. This could cause better candidates to be generated than merely the strings that survived the fitness test. In design, it could cause novel solutions to be generated. The reproduction or crossover process is carried out by choosing partner strings for mating; selecting a point in the string for splitting the strings; and combining the first part of one string with the second part of its 'partner'. The choice of partners for 'mating' and the point of crossover are chosen randomly. It should be noted that only the strings corresponding to solutions which have high fitness in the first generation are allowed to reproduce. Crossover would hence result in a new and hopefully fitter population of strings. Mutation is a process (again effected randomly but with a much lower frequency) where a single bit is changed—i.e. from 1 to 0 or vice versa.

The above process is allowed to continue for many generations. The end point of the process is considered to be when incremental improvement in fitness becomes small. This may be slightly inadequate for a strict definition of searching for an optimum, but would suffice for most practical engineering purposes. GAs combine randomness (in the probabilistic rules) with directedness (through the fitness function). It is this combination that makes the scheme analogous to Darwinian evolution, where random variations in the genotype give rise to creative solutions, while the harsh environment ensures error elimination (see Table 3.1). Two good examples of this method are its use (i) to find a minimum weight truss (Jenkins 1991), which is an example of optimization and (ii) to generate house plans (Rosenman 1997), which is an example of novel design.

It may be argued that Darwinian evolution is ‘blind’ in that it is not goal directed—as reflected in the title of a book by Richard Dawkins (1986)—whereas the GA has a very definite goal, i.e. the fitness function, to aim at. When considered in this light, evolution and GAs may look conceptually quite different. However, it is argued in some quarters that Darwinian evolution too is characterized by ‘convergence’ of some sort (Conway Morris 2006), as in GAs. Furthermore, if we treat both processes as ones of competitive adaptation to a harsh environment, through the generation of ‘novelty’ and the elimination of ‘weakness’, they can be seen as conceptually similar. They also resonate with Popper’s thesis that scientific knowledge advances as its bold conjectures are subjected to critical testing.

3.8 Summary

- Two of Karl Popper’s most significant contributions to the philosophy of science were his cyclic problem solving methodology and his focus on falsification.
- Engineering processes can be seen as cyclic in nature, whether in a design project or in the wider growth of engineering knowledge. These processes either envisage failure modes or learn from examples of failure. As engineers we can look to Popper for a philosophical underpinning of such processes and approaches.
- Envisaging failure modes in the *design cycle* leads to better design solutions. In the *world cycle* however, we can improve our calculation procedure models, not by actively seeking real world failures, but by learning from failures when they do occur.
- An examination of historical real world failures can help us to identify which component of the calculation procedure model has been falsified—i.e. whether it is the engineering science core; or the outer shells of idealization, margins of safety, design philosophy, design context or engineering process.

– Two relatively recent problem solving approaches also fall squarely within this cyclic paradigm. One of them, the genetic algorithm (GA) technique for optimization and design, embodies elements of randomness and error elimination in a cyclic manner. The other, reflective practice systems, encourages us to learn from our experience through reflection at progressively deeper levels. Above all, we must see engineering and our involvement in it as a learning experience, leading to continuous improvement.

Acknowledgements Adapted from *The Structural Engineer 85*(2), 32–37, Engineering as cyclic problem solving—some insights from Karl Popper by W. P. S. Dias, 2007, published by the Institution of Structural Engineers, London.

References

C. Alexander, *Notes on the Synthesis of Form* (Harvard University Press, Cambridge, 1964)

N. Anwar, *Structural Design Review: Bowling and Theater Roof Truss—Central Rama III* (ACECOMS, Asian Institute of Technology, Bangkok, 1997)

A.W. Beeby, Partial safety factors for reinforcement. Struct. Eng. **72**(20), 341–343 (1994)

D.I. Blockley, *The Nature of Structural Design and Safety* (Ellis Horwood, Chichester, 1980)

D.I. Blockley, Engineering from reflective practice. Res. Eng. Des. **4**, 13–22 (1992)

D.I. Blockley, J.R. Henderson, Structural failures and the growth of engineering knowledge. Proc. Inst. Civ. Eng., Part 1 **68**, 719–728 (1980)

BS 8110: 1997. *Structural Use of Concrete* (British Standards Institution, London, 1997)

S. Cammelli, Tianjin CTF financial centre: wind, form and structure. Struct. Eng. **96**(9), 14–21 (2018)

P. Checkland, J. Scholes, *Soft Systems Methodology in Action* (Wiley, Chichester, 1990)

S. Conway Morris, Darwin's compass: how evolution discovers the song of creation (The Boyle Lecture 2005). Sci. Christ. Belief **18**(1), 5–22 (2006)

R. Corvi, *An Introduction to the Thought of Karl Popper* (Routledge, London, 1997)

R.D. Coyne, M.A. Rosenman, A.D. Radford, M. Balachandran, J.S. Gero, *Knowledge Based Design Systems* (Addison-Wesley, Reading, 1990)

CP 110: 1972. *The Structural Use of Concrete* (British Standards Institution, London, 1972)

R. Dawkins, *The Blind Watchmaker* (Longman, London, 1986)

N.J. Delatte, *Beyond Failure: Forensic Case Studies for Civil Engineers* (ASCE Press, Reston, 2009)

W.P.S. Dias, Structural failures and design philosophy. Struct. Eng. **72**(2), 25–29 (1994)

W.P.S. Dias, Reflective practice, artificial intelligence and engineering design: common trends and inter-relationships. Artif. Intell. Eng. Des. Anal. Manuf. (AIEDAM) **16**, 261–271 (2002)

W.P.S. Dias, Engineering as cyclic problem solving—some insights from Karl Popper. Struct. Eng. **85**(2), 32–37 (2007)

P. Dias, The disciplines of engineering and history: some common ground. Sci. Eng. Ethics **20**(2), 539–549 (2014)

W.P.S. Dias, D.I. Blockley, Discussion on "Galileo's confirmation of a false hypothesis: a paradigm of logical error in design by Henry Petroski". Civ. Eng. Syst. **11**, 75–77 (1994)

W.P.S. Dias, D.I. Blockley, Reflective practice in engineering design. ICE Proc. Civ. Eng. **108**(4), 160–168 (1995)

W.P.S. Dias, U.A. Padukka, AI techniques for preliminary design decisions on column spacing and sizing. Paper presented at the 8th international conference on the application of artificial intelligence to civil, structural and environmental engineering, Rome, 30 Aug–2 Sep 2005 (2005)

W.P.S. Dias, A.D.C. Jayanandana, M.C.M. Fonseka, A.A.D.A.J. Perera, Distress in prestressed concrete roof girders at cement plant. ASCE J. Perform. Constr. Facil. **8**(1), 6–15 (1994)

P. Dias, R. Dissanayake, R. Chandratilake, Lessons learned from tsunami damage in Sri Lanka. ICE Proc. Civ. Eng. **159**, 74–81 (2006)

P. Feyerabend, *Against Method: Outline of an Anarchistic Theory of Knowledge* (New Left Books, London, 1975)

D.E. Goldberg, *Genetic Algorithms in Search, Optimisation and Machine Learning* (Addison-Wesley, New York, 1989)

J.H. Holland, *Adaptation in Natural and Artificial Systems* (University of Michigan Press, Ann Arbor, 1975)

I. Hybs, J.S. Gero, An evolutionary process model of design. Des. Stud. **13**(3), 273–290 (1992)

W.M. Jenkins, Structural optimization with the genetic algorithm. Struct. Eng. **69**(24), 418–422 (1991)

J. LeMasurier, D.I. Blockley, D. Muir Wood, An observational model for managing risk. ICE Proc. Civ. Eng. **159**(6), 35–40 (2006)

M. Levy, M. Salvadori, *Why Buildings Fall Down* (W.W. Norton & Co., New York, 1992)

P. Lipton, The truth about science (The Medawar Lecture 2004). Philos. Trans. R. Soc. Lond. B **360**, 1259–1269 (2005)

I.A. MacLeod, A strategy for the use of computers in structural engineering. Struct. Eng. **73**(21), 366–370 (1995)

B. Magee, *Popper* (Fontana, London, 1973)

M.A. Notturno, *Science and the Open Society: The Future of Karl Popper's Philosophy* (Central European University Press, Budapest, 2000)

H. Petroski, *To Engineer Is Human: The Role of Failure in Successful Design* (St. Martin's Press, New York, 1969)

H. Petroski, Galileo's confirmation of a false hypothesis: a paradigm of logical error in design. Civ. Eng. Syst. **9**(3), 251–263 (1992)

H. Petroski, *Design Paradigms: Case Histories of Error and Judgment in Engineering* (Cambridge University Press, Cambridge, 1994)

N.F. Pidgeon, D.I. Blockley, B.A. Turner, Design practice and snow loading—lessons from a roof collapse. Struct. Eng. **64A**(3), 67–71 (1986)

K.R. Popper, *The Poverty of Historicism*, 2nd edn. (Routledge and Kegan Paul, London, 1960)

K.R. Popper, *The Logic of Scientific Discovery*, 2nd edn. (Hutchison, London, 1968)

K.R. Popper, *Objective Knowledge: An Evolutionary Approach* (Oxford University Press, Oxford, 1972)

K.R. Popper, in *Realism and the Aim of Science: Postscript to the Logic of Scientific Discovery*, vol. 1, ed. by W.W. Bartley III (Hutchison, London, 1983)

K.R. Popper, *Conjectures and Refutations: The Growth of Scientific Knowledge*, 5th edn. (Routledge, London, 1989)

K.R. Popper, *All Life is Problem Solving* (Routledge, London, 1999)

M.A. Rosenman, An exploration into evolutionary models for non-routine design. Artif. Intell. Eng. **11**, 287–293 (1997)

D.A. Schon, *The Reflective Practitioner: How Professionals Think in Action* (Temple Smith, London, 1983)

P.M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization* (Century Business, New York, 1992)

P.G. Sibly, A.C. Walker, Structural accidents and their causes. Proc., Inst. Civ. Eng., Part 1 **62**, 191–208 (1977)

Y. Umeda, H. Takeda, H. Yoshikawa, T. Tomiyama, Function, behaviour and structure, in *Applications of Artificial Intelligence in Engineering V, Vol. 1—Design*, ed. by J.S. Gero (Computational Mechanics Publications, Southampton, 1990), pp. 177–193

W.G. Vincenti, *What Engineers Know and How They Know It: Analytical Studies from Aeronautical History* (Johns Hopkins, Baltimore, 1990)

S.B. Willoughby, The Ridgeway footbridge. Struct. Eng. **74**(5), 79–83 (1996)