Variability: Threat or Curse?

Ale, Ben; Hartford, D.N.D.; Slater, D.H.

DOI
10.3850/978-981-11-2724-3_0184-cd

Publication date
2019

Document Version
Final published version

Published in
Proceedings of the 29th European Safety and Reliability Conference, ESREL 2019

VARIABILITY: THREAT OR CURSE?

Ben J.M. Ale
Technical University Delft, PO Box 5015, 2600 GA Delft, the Netherlands.E-mail: ben.ale@xs4all.nl
Des N.D. Hartford
BC Hydro, 6911 Southpoint Drive, Burnaby, BC, V3N 4X8, Canada.
David H.Slater
Cardiff University, School of Engineering, Queen's Buildings, 14-17 The Parade, Cardiff CF24 3AA, United Kingdom

In the philosophy of SAFETY-I variability is seen as a threat, because it brings with it the possibility of an unwanted outcome. Variability of hardware is curtailed by, amongst other things, precise specifications. Variability of human behavior is curtailed by inter alia regulations and protocols. In the philosophy of SAFETY-II variability is seen as an asset. In SAFETY-II, humans are seen as able to cope with the variability of technology circumstances to keep systems working. This capacity of coping has been designated resilience. Recently the meaning of resilience has been stretched to include the ability of restoring the operational state after an excursion into the realm of inoperability. The belief that humans will cope if an unexpected situation may arise, reduces the emphasis on preventive measures that limit the probability that the system may behave in an unsafe manner. The stretched meaning of resilience exacerbates this problem, because there is no real limit of what systems or society using these systems may bounce back from. The philosophies behind resilience engineering promote safety by exploiting the ingenuity of humans to keep systems within the desired operating envelope. Unfortunately the errors that may be introduced by over-relying on humans correctly assessing situations may also be fatal or catastrophic: maybe not for society as a whole, but surely for an individual, a group of individuals, or a company.

Keywords: SAFETY II, Resilience Human Error, Variability

1 Introduction

Variability has been the driving force behind the evolution of nature and mankind. Successful variations of species lead to improved survival characteristics. Unsuccessful variations become extinct. Variations on the other hand also lead to unpredictability and uncertainty. To promote chances of survival, predictability is a valuable tool. To know in advance when winter will end, when seeds can be sown and when crops can be harvested, has led to the development of astronomy and many of the other sciences. Uncertainty can be further reduced by following in other people's footsteps, along paths that have been proven to be safe; first literally, leading to worn out footpaths, carriage tracks and roads, later figuratively, by following examples. These examples were often coded into practices, notes, drawings. To prevent houses collapsing, for example, such codes were then converted into rules and regulations.

In military applications, multiple layers of defense were designed to cope with expected and unexpected breaches of any one of them. Systems of outer walls, moats with drawbridges, inner walls and keeps formed the "defense in depth" of many fortresses. The idea of building such elaborate defenses sometimes often survives beyond their useful life. The arrival of the airplane in the 20th century, made all these walls useless.

Over the centuries the emphasis has been swinging back and forth between curtailing variability and defense against external threats. But in their strategic thinking, there always has been a combination of the two. A fortress had walls, artillery, a guard inside to take care of intruders and a fire brigade to deal with stuff that was thrown over the walls.

2 SAFETY-I

In Safety-I variability is considered more of a threat. The development of machinery made it possible to harness energy on a larger scale. This in turn led to an increase in the number of situations where the force of the machinery exceeded the resistance of the human body. There had always had been injuries and deaths during work on farms, in construction and accidents

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio

Published by Research Publishing, Singapore.
ISBN: 978-981-11-2724-3; doi:10.3850/978-981-11-2724-3_0184-cd

caused by trips and slips; but now the deaths were more localized, as in a single factory, with an identifiable owner. It is therefore no surprise that the owners put the blame on the workers themselves. This however did not last. The owners of the factories themselves were held responsible. In this context, it is not surprising that the design of protective safety measures became another branch of the engineering profession. This led to the design and addition of guards, barriers, kill-switches and other devices that should prevent personnel being killed, or injured. The philosophies behind these designed defenses, however, were not new at all. If a system needs to be safe and if one of the safety systems can fail, introduce redundancy and defense in depth.

These developments made systems safer, but also more complex. Assuring safety slowly became detached from assuring functionality. Nevertheless the development of tools for the analysis of failure was originally meant to "assure" operators that systems would work. Fault-tree analysis for example, was introduced to make sure that the Minuteman missile would actually arrive at its target, which would happen if nothing went wrong. To construct a fault-tree or perform a FMEA anecdotal and analytical information is sufficient. In ancient times it was sufficient to know that the artillery of the enemy could penetrate a 10 feet wall. No further analysis was needed to decide to make the walls 15 feet thick.

There are however two problems with this fault centered and fault eliminating approach.

- Accidents happen because systems do not conform to regulations.
- Accidents happen despite systems conforming to regulations.

The latter is more problematic than the former, especially when systems conforming to regulations are declared safe to the extent that "nothing bad can happen".

2.1 *Deviations*

There are many reasons why a system may not behave as expected. Some of these are real surprises, but these are rare indeed. Most deviations are caused by non-compliance with rules, regulations, or codes of practice; in short, by not fully applying the lessons from the past. These deviations are predominantly associated with human behavior; by error, on purpose or just because humans are variable.

The problem with this focus on deviations is that most of the data about deviations are derived from analyses of failure. What is largely unknown is how many deviations do not lead to failures. Therefore what really needs to be known is whether the deviation is more common in the population of systems, or people that have an accident, than in the population that does not have an accident (Ale et al, 2006a; Roelen et al, 2011). This information is very difficult to acquire, as was demonstrated in the development of the Occupational Risk Model (ORM) (Ale, 2006; Bellamy et al, 2011; Papazoglou and Ale, 2011) and of the Causal Model for Air Transport Safety (CATS) (Ale et al, 2006b).

These investigations led to insights into what deviations were more important than others, and which deviations had been of consequence so far. This should not lead to the conclusion that these deviations should be allowed to persist. If these deviations mainly pertained to secondary and tertiary defenses and the primary defense is mostly effective, the probability of these defenses to be challenged may be small, but there has been a decision at some point that these defenses were nevertheless necessary. Moreover, allowing non-compliance and the persistence of deviations is contagious. Postponing a paint job on a white storage tank allowing a little rust to persist may seem harmless until some years later everybody seems to be used to this tank to be brown.

2.2 *Human actions*

In the 18th, 19th and 20th centuries, the golden age of engineering relied on the seemingly immutable laws of Newton and his descendants, to specify how systems would work: and humans were trained to operate them and expected to behave in a similarly specified way. The operator was thus an add-on, an extension of the engineering design (Besnard and Hollnagel, 2007).

Since, in the mind-sets of the designers of these relatively simple systems, humans were a problem, it became logical to ascribe the "cause" of malfunctions of the systems to the most unreliable part, the human factor. It is then a very human response to "blame" the human for the results (Heinrich, 1931; Swuste et al 2011). It is also very convenient. It eliminates the need for

further thought about the intrinsic properties of a system and it avoids the need for protection measures that cost money. In this line of thought the variability of human behavior needed to be curtailed. Interpreting human error as operator error, however, ignored what emerged to be a deeper problem, which is the circumstances created by supervisors and managers and the decisions they take. Unfortunately, bending the rules is often necessary to keep things moving, as is demonstrated time and again when industrial actions are attempted by following the letter of all of the regulations. The question then is, what is the right balance to allow for human ingenuity, on the one hand, and defending against human fallibility at the other, in order to make things work.

3 SAFETY-II

In the approach taken in SAFETY II, variability is considered an asset. The sheer complexity of these modern systems made it difficult to understand how all the personnel and functions fitted together to make them work. Systems became and are still becoming increasingly more intractable, which makes an "à priori" analysis of what might go wrong increasingly impossible.

Having identified the nature and significance of some of the factors causing difficulty in operating large complex systems satisfactorily and reliably, many safety professionals have become convinced that we may need to address these issues from a different perspective, if we want to continue to operate ever more complex systems "safely'. Some of these are triggered by the perceived incomprehensibility of low probability – high consequence events. Some of these again, are triggered by the notion that analysis of causality seems to have no end; and some by the more legalistic discussion on whether a probabilistic progression of a sequence of events should lead to a negation of the certainty of the cause after the fact. The matter of causality is a highly philosophical question (Ale et al, 2009; Russel, 1946). In the case of accidents, rare extremes of independent variables can occur simultaneously by chance, such as in the – sometimes referred to as typically Dutch – problem of assessing the possibility and probability of extreme flood conditions (Gelder 2007).

Increasingly decision makers and scientists seem of the opinion that analyses of these extremes have no value for systems that are too complicated to be understood completely. Rather than making systems simpler, they prefer to look at the system as an organic creature, which may behave in unexpected and unforeseen ways. In this line of thinking, humans need to cope with these behaviors and rectify them, when they are unwanted, or unsafe. "Adapt and adjust" during operation and managing changes is a paradigm shift, which explains why, in the past, we have managed to make even the most challenging systems work. This approach however is not without its own challenges.

3.1 Functionality

Whereas it is usually clearly defined as to what constitutes a failure, what constitutes success is usually not clearly defined; and even more often, narrowly defined in terms of non-failure. A car that does not go has obviously failed. But can a car that still goes on a "donut" spare still be considered to function correctly, or a car, where the driver has to continuously correct for asymmetric steering behavior. In the latter case the driver makes things work, but can it be called a success?

For functionality one could distinguish three stages of performance (Ale et al, 2005): Functions as intended; functions but not as intended and does not function. Functionality can also be seen as an entity, of which the distribution ranges from normal functionality, through subnormal functionality, to failure; but the demarcations between the areas are not sharp. The apocryphal guy in the blue overalls with the oil can, who keeps the system going, may have been acceptable as an engineering solution for a steam locomotive, but regular intermittent halting of machinery, is not considered a valid engineering solution for airplanes. Functionality therefore is ill defined.

3.2. *Instruments*

The instruments associated with SAFETY-I can be grouped according to the well known "bow-tie" model (Nielsen, 1971): identification instruments which lead to the definition of the center event; fault-tree instruments to the left of the center event describe the events and processes leading up to that failure. Event-tree instruments

are used to evaluate the consequences of that failure. These instruments can be qualitative or quantitative and probabilities can be assigned to various events and branches of the tree when desired. As has been demonstrated elsewhere, there is no need for systems to behave linearly for these methods to be employed. The approaches employed in SAFETY-I, do lend themselves to quantification and therefore to a comparison of costs and benefits.

As in all analytical techniques, there is the problem of uncertainty. In most cases the values of parameters are only known with limited accuracy; and thus the results of cost-benefit evaluations are uncertain as well. The major uncertainty is whether all possibilities have been covered. There may always be surprises. This is also known as the "black swan" problem. There is no set limit on the extent of the failure tree to the left or the event tree to the right. The analysis can be as deep and as wide as is wanted. As a result the decision space can be expanded at will. It can be restricted to a single operation or piece of equipment. It can be expanded to the surroundings including the population in which it is located to evaluate and decide on the risks to properties and life.

The analysis tools associated with SAFETY-II, such as FRAM (Functional Resonance Analysis Model) (Hollnagel, 2012), the graphical implementation of which is a simplified version of SADT (Structural Analysis and Design Technique) (Marca and McGowan, 1987), are essentially qualitative. They can be used to describe the structure and behavior of a system and the way it is supposed to function, but for a quantitative analysis of the potential variations of the behavior of the system, a process simulator has to be put on top of these models. For SAFETY-II a cost benefit evaluation is more difficult if the methods employed are essentially qualitative; perhaps with the exception of the cases where success is defined as the absence of failure. In the latter case SAFETY-II in essence reverts to SAFETY- I.

4. Resilience

In SAFETY-II resilience has a special place. When resilience is interpreted as having redundant defenses and defenses in depth, resilience engineering reverts to SAFETY-I. When resilience is interpreted as assuming that any problems will be successfully solved by human ingenuity, when and if they arrive in the future, there is an immediate cost saving, as complicated in-depth analyses of potential faults and their consequences is no longer necessary. Another cost reduction results, because potentially costly measures to take away problems that could, or would, emerge from these analyses are not necessary either. Resilience engineering therefore is an attractive alternative to a SAFETY-I approach. Since the paradigms behind resilience engineering implicitly, or explicitly, assume that future problems will be solved successfully, the problem of "black swan" events disappears. In fact, many of the potential events that would be discovered by SAFETY-I analyses may now be future surprises.

A common argument in favor of the SAFETY-II approach is that if the SAFETY I approach is successful and no accidents occur, doubt will be raised as to whether the investment in safety was justified, while in the SAFETY II approach, investments are made that promote productivity and, as a consequence, also promote safety. This sounds like a praiseworthy ambition, but again like safety, although in a different way, this seems to be a label which covers a multitude of concepts; which range from the use of more effective or layers of barriers (defenses), to designing in some functionality to monitor, respond, adapt and learn from actual operational experiences. Again, inevitably, because this is applied without distinction to everything, from simple engineering systems to large organizations, it is difficult to get a consensus view as to exactly what it is. The unfortunate side effect of this line of thought is that it entices engineers to refrain from further analysis of possible deviations and their consequences; and use these analyses as a basis for design changes, or the incorporation of further protective measures: be it in the form of additional hardware at one end of the spectrum, to additional emergency protocols at the other. Fixed asset-capital intensive industries that are focused SAFETY I approaches run the risk of inadvertently drifting into a SAFETY II mode with reliance on the ability to cope if safety improvements are primarily decided on the basis of a favorable benefit:cost ratios. This can happen because typically, such organisations have always been able to cope with all eventualities and a culture of coping will have emerged that drives the thinking of engineers and managers with the

result is gradual deterioration in the risk position of the fixed assets that goes unnoticed until disaster strikes and a bridge collapses (http-1).
The expectation that problems will be dealt with when they arrive is common in politics and religion, but as Clausewitz (1832) explains, this is not a good idea if one contemplates to engage in warfare. The ultimate outcome of resilience engineering is continuous improvisation. Variability produces innovation, but in the end consistency sells the product, as Deming (1982) and Juran and Gruna (1988) have pointed out before.
A second problem with the SAFETY-II is that the definition of success requires the definition of the system under consideration, at the start of the analysis and decision making process. In SAFETY-II the focus is on continued successful functioning of a system. The demarcation of what is considered to belong to the system and what is a success can have profound ethical implications. As an example consider a system that requires the presence of a single human operator to operate successfully. For continued operation it is sufficient that this operator can be replaced, should the current operator be unavailable, or make an error, (i.e. is unreliable), just as any other replaceable component. In the context of the analysis it does not make any difference to the level of functionality of this system, if the operator fails to function, errs deliberately or because of inattention, or perhaps because he is killed on the job. However, the system is still resilient against disturbances in human operator availability, as long as he can immediately be replaced. The collateral damage may be that the operator is killed. One could even state that the society around the operator is resilient against this event if there is a burial service that disposes of the body quietly and efficiently. Indeed with a small addition of burial capacity to the FRAM diagram the system can be declared to continue to successfully operate with a considerable death rate under its human components.
The ethical and political problem gets even deeper when the collateral damage extends to third parties such the surrounding population or passengers on an airplane. The airfield of FARO was reopened within 24 hours after the crash of Martinair Flight 495, which killed 54 of the 340 people on board. The wreck was swept aside and only a few flights were diverted. From the point of view of resilience of the airfield the operation was a success. From the point of view of the passengers that were killed and their families it was a disaster. The SAFETY-II approach therefor has the intrinsic tendency to transfer risk to resources and people who are outside the system under consideration.
Resilience thus is also a matter of scale in distance and time. Society as a whole can be considered as extremely resilient. Even after large disasters, society keeps functioning. May be not at the location where disaster struck. The families involved in fires such a Paradise and Mati will mourn for the victims or have to find resources to rebuild their homes, but in a few decades also for those families it will be history. Similarly disasters such as the explosions in Beek (1976, http-2) and Flixborough (1975, http-3) are disappearing in the mist of time, while the explosion on the Deepwater Horizon (http-4) recently resulted in a Hollywood disaster movie. The ethical question remains though. Can accident and disasters be accepted and preventive measures be omitted because there is an expectation of short or longer term resilience.

5. Conclusion

Currently four main streams of thinking in safety engineering can be identified: SAFETY-I, SAFETY-II, Resilience Engineering and Precaution. Each of these try to deal with the effects of the variability of nature and of human behavior.
In SAFETY-I and Precaution the states of failure that are considered to be unsafe are defined a priori. The causes and the consequences emerge from analysis. The extent of the system, or the system of systems considered, depend on choices made by a decision maker and the analyst on the extent of the analysis.
In SAFETY-II and Resilience Engineering, it needs to be defined a priori, what system it is that it is desired to keep functioning. This means that collateral damage outside of the chosen system is not considered; and could even be used to support the continued functioning of the system. The continued functionality is not defined a priori; and the definition may change during the analysis.
SAFETY-I and Precaution designate variability as, in principle, unwanted. In SAFETY-II and Resilience Engineering it is desirable. However, the latter implicitly assumes that future variations

will stay within bounds and the system does not stray so far outside the safe operational envelope, that recovery is not possible. Resilience engineering is aimed at keeping a system working. Variability is accepted and should be controlled by the ingenuity of humans to work with and if necessary compensate for unwanted excursions.

The resilience approach has the inherent tendency to be blind to collateral damage; and therefore to support choices that put the damages outside the system to make them collateral.

In this light variability still is more a threat than an asset and should be reduced as far as reasonably achievable.

References

Ale, B.J.M , L.J. Bellamy, R. van der Boom,R.M. Cooke, L.H.J.Goossens, A.R. Hale, D. Kurowicka, P.H. Lin, O., Morales, A.L.C., Roelen, J., Cooper, J., Spouge. (2006b) *CATS final report*, Ministry of Transport and Water management, The Hague, The Netherlands, ISBN 10: 90 369 1724-7; ISBN 13: 978 90 369 1724-7 (2006b)

Ale, B.J.M. (2006) *The Occupational Risk Model*, TU-Delft/TBM RC 20060731, ISBN 90-5638-157-1, Delft.

Ale, B.J.M., L.J. Bellamy, A.L.C. Roelen, R.M. Cooke, L.H.J.Goossens, A.R. Hale, D. Kurowicka, E. Smith (2005) Development of a causal model for air transport safety, IMECE 2005, 79374, Proceedings of IMECE, 2005 ASME International Mechanical Engineering Congress and Exhibition, Orlando, Florida, nov 5-11, ISBN 0-7918-3769-6

Ale, B.J.M., L.J. Bellamy, R. van der Boom, J. Cooper, R.M. Cooke, L.H.J. Goossens, A.R. Hale, D. Kurowicka, O. Morales, A.L.C. Roelen, J. Spouge (2009), Further development of a Causal model for Air Transport Safety (CATS): Building the mathematical heart, *Reliability Engineering & System Safety, Volume 94, Issue 9*, pp 1433-1441.

Ale, B.J.M., L.J. Bellamy, R.M. Cooke, L.H.J. Goossens, A.R. Hale, A.L.C. Roelen, E. Smith. (2006a) Towards a causal model for air transport safety—an ongoing research project - *Safety Science 44 657–673*

Bellamy, L.J., B.J.M. Ale, J.Y.Whiston, M.L. Mud, H. Baksteen, A. Hale, I.A. Papazoglou, A. Bloemhoff , J.I.H Oh. (2006) The software tool Storybuilder and the analysis of the horrible stories of occupational accidents, Working on Safety, 12-15.

Besnard, Denis, Erik Hollnagel (2014) I want to believe: some myths about the management of industrial safety. Cognition, Technology and Work, Springer Verlag, 16 (1), pp.13-23. <10.1007/s10111-012-0237-4>. <hal-00720270>.

Clausewitz, Carl von, (1832) *On War*, translated by Howard, Princeton university press, 1992, ISBN 0691018545 (1992) (From Carl von Clausewitz, Zum Kriege, Ferdinand Dümmler, 1832

Deming, W. E.(1982) *Quality, productivity and competitive position,* Massachusetts Institute of Technology, Cambridge, ISBN 0911379002 (1982)

Gelder, Pieter van (2007) *Quantitative methods for flood risk management, statistical extremes and environmental risk*. Faculty of Sciences, University of Portugal, Lisbon, Portugal, February 15–17.

Heinrich, H., (1931) *Industrial Accident Prevention a Scientific Approach*, first ed. McGraw-Hill Book Company, London.

Hollnagel, E, (2012) *FRAM, The Functional Resonance Analysis Method*, CRC Press, ISBN 9781351935968.

http-1: https://www.nytimes.com/interactive/2018/09/06/world/europe/genoa-italy-bridge.html

http-2: http://www.hse.gov.uk/comah/sragtech/casebeek75.htm (last visited 06-01-2019)

http-3: http//en.wikipedia.org/wiki/Flixborough_disaster (last visisted 06-01-2019)

http-4: https://nl.wikipedia.org/wiki/Deepwater_Horizon (last visited 06-01-2019)

Juran, J. M. and Gryna, F. M. (Eds.) (1988) *Quality control handbook*, 4th. ed., McGraw-Hill, New York ISBN-10: 9780070331761 (1988)

Marca, D., C. McGowan (1987), *Structured Analysis and Design Technique,* McGraw-Hill, 1987, ISBN 0-07-040235-3

Nielsen, D., 1971. *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis*. Danish Atomic Energy Commission, Research Establishment Risø. Rapport Risø-M-1374.

Papazoglou Ioannis A. and Ben J.M. Ale (2007) A logical model for quantification of occupational risk, *Reliability Engineering & System Safety, Volume 92, Issue 6, Pages 785-803.*

Roelen, A. L. C., Lin, P. H., Hale, A. R. (2011), Accident models and organisational factors in air transport: The need for multi-method models. *Safety Science, 49, 5-10*

Russell, Bertrand (1946) *History of western philosophy*. London: George Allen & Unwin.

Swuste, Paul, Coen van Gulijk, Walter Zwaard, (2010) Safety metaphors and theories, a review of the occupational safety literature of the US, UK and The Netherlands, till the first part of the 20th century, *Safety Science 48, 1000–1018.*