Resilience Engineering and the Fifth Age of Safety

Dr (Capt) Suresh Bhardwaj, *fics,fni,fcmmi*

PhD (Denmark & UK), Master Mariner

Resident Director& Principal, MASSA Maritime Academy, Chennai, India.

Introduction

This paper challenges some traditional fundamental concepts of accident dynamics, accident prevention, and accident analysis. The purpose is to emphasize that improvement analysts need to understand the theoretical bases of safety management and accident analysis, and the practical application of Integrated Safety Management framework. The increasing complexity in highly technological systems is leading to potentially disastrous failure modes and new kinds of safety issues. Traditional accident modelling approaches are not adequate to analyse accidents that occur in modern socio-technical systems, where accident causation is not the result of an individual component failure or human error.

The Contemporary Understanding of Accident Causation

Safety science today views serious accidents not as the result of individual acts of carelessness or mistakes; rather they result from a confluence of influences that emerge over time to combine in unexpected combinations enabling dangerous alignments, sometimes catastrophically. The accidents that stimulated the new safety science are now indelibly etched in the history of safety: Challenger and Columbia, Three Mile Island, Chernobyl, Bhopal, Piper-Alpha, and Deepwater Horizon, as identified in the DOE Handbook on *Accident and Operational Safety Analysis* (2012). These accidents have introduced new concepts and new vocabulary: normal accidents, systems accidents, practical drift, normal deviance, latent pathogens, organizational factors, and safety culture.

Within complex systems, human error does not emanate from the individual, but is a bi-product of the ever-present latent conditions built into the complexity of organizational culture and strategic decision-making processes. The triggering or initiating error that releases the hazard is only the last in a network of errors that often are only remotely related to the accident. Accident occurrences emerge from the organization’s complexity, taking many factors to overcome systems’ network of barriers and allowing a threat to initiate the hazard release.

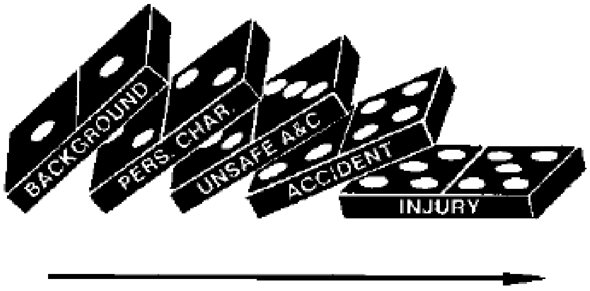
Accident Models

A Basic Understanding

What investigators look for when trying to understand and analyze an accident depends on how it is believed an accident happens. A model, whether formal or simply what one may believe, is extremely helpful because it brings order to a confusing situation and suggests ways one can explain relationships. However, the model is also constraining because it views the accident in a particular way, to the exclusion of other viewpoints and this must be kept in mind.

Sequence of Events Model

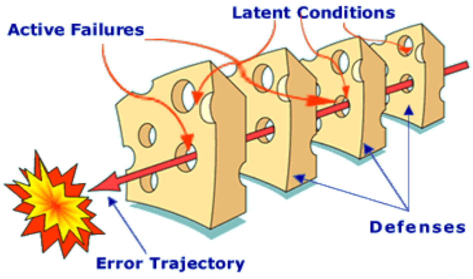
This is a simple, linear cause and effect model where accidents are seen as the natural culmination of a series of events or circumstances, which occur in a specific and recognizable order. It is generally represented by a chain with a weak link or a series of falling dominos. In this model, accidents are prevented by fixing or eliminating the weak link, by removing a domino, or placing a barrier between two dominos to interrupt the series of events.



The sequential model is limited because it requires strong ‘cause and effect’ relationships that typically do not exist outside the technical or mechanistic aspect of the accident. In other words, true cause and effect relationships can be found when analyzing the equipment failures, but causal relationships are extremely weak when addressing the human or organizational aspect of the accident. For example: While it is easy to assert that “time pressure caused workers to take shortcuts,” it is also apparent that workers do not always take shortcuts when under time pressure.

Epidemiological or Latent Failure Model

This is a complex, linear ‘cause and effect’ model where accidents are seen as the result of a combination of active failures (unsafe acts) and latent conditions (unsafe conditions). These are often referred to as epidemiological models, using a medical metaphor that equate the latent conditions to pathogens in the human body that lay dormant until triggered by the unsafe act. In this model, accidents are prevented by strengthening barriers and defences. The “Swiss Cheese” model developed by James Reason is an example of the epidemiological model.



Latent Failure Model – differences from Sequential

Performance Deviation – The concept of unsafe acts shifted from being synonymous with human error to the notion of *deviation from the expected performance.*

Conditions – The model also considers the contributing factors that could lead to the performance deviation, which directs analysis upstream from the worker and process deviations.

Barriers – The consideration of barriers or defences at all stages of the accident development.

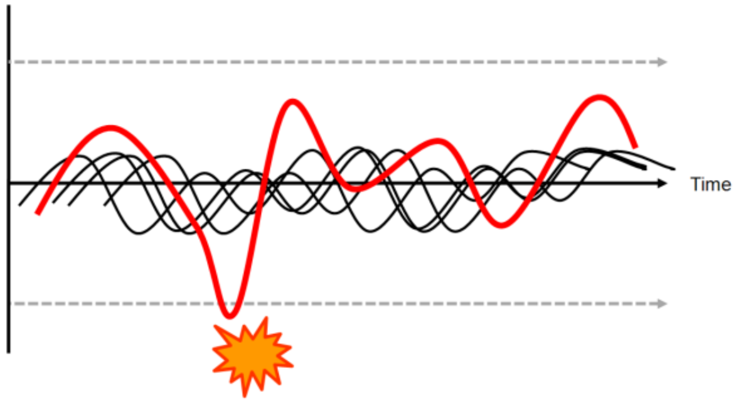
Latent Conditions – The introduction of latent or dormant conditions that are present within the system well before there is any recognizable accident sequence.

This model views the accident to be the result of long standing deficiencies that are triggered by the active failures. The focus is on the organizational contributions to the failure and views the human error as an effect, instead of a cause.

Systemic Model

New approaches to accident modelling as brought forward by Hollnagel (2004) in his book *Barriers and Accident Prevention,* adopt a systemic view which considers the performance of the system as a whole. In systemic models, an accident occurs when several causal factors (such as human, technical and environmental) exist coincidentally in a specific time and space. Systemic models view accidents as emergent phenomena, which arises due to the complex interactions between system components that may lead to degradation of system performance, or result in an accident.

This is a complex, non-linear model where both accidents (and success) are seen to emerge from unexpected combinations of normal variability in the system. In this model, accidents are triggered by unexpected combinations of normal actions, rather than action failures, which combine, or resonate, with other normal variability in the process to produce the necessary and jointly sufficient conditions for failure to succeed. Because of the complex, non-linear nature of this model, it is difficult to represent graphically. The Functional Resonance model from Erik Hollnagel uses a signal metaphor to visualize this model with the undetectable variabilities unexpectedly resonating to result in a detectable outcome.



Leveson (2004) in his seminal article *A New Accident Model to Engineer Safer Systems* in Safety Science journal explains the theory behind. Systemic models have their roots in systems theory. In a systems theory approach to modelling, systems are considered as comprising interacting components which maintain equilibrium through feedback loops of information and control. A system is not regarded as a static design, but as a dynamic process that is continually adapting to achieve its objectives and react to changes in itself and its environment. The system design should enforce constraints on its behaviour for safe operation, and must adapt to dynamic changes to maintain safety. Accidents are treated as the result of flawed processes involving interactions among people, social and organizational structures, engineering activities, and physical and software system components.

The perspective of Resilience Engineering

Viewing safety though the lens of complexity theory illuminates an understanding that it is the ability of people in organizations to adapt to the unexpected that produces resilient systems, systems in which safety is continually created by human expertise and innovation under circumstances not foreseen or foreseeable by technology designers.

Resilience Engineering is defined as ‘The intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under expected and unexpected conditions.’

For Resilience Engineering, 'failure' is the result of the adaptations necessary to cope with the complexity of the real world, rather than a breakdown or malfunction. The performance of individuals and organizations must continually adjust to current conditions and, because resources and time are finite, such adjustments are always approximate. This definitive new approach explores this groundbreaking new development in safety and risk management, where 'success' is based on the ability of organizations, groups and individuals to anticipate the changing shape of risk before failures and harm occur.

Erik Hollnagel, a pioneer of the Resilience Engineering perspective, has explained that accident investigation and risk assessment models focus on what goes wrong and the elimination of "error.” While this principle may work with machines, it does not work with humans. Variability in human performance is inevitable, even in the same tasks we repeat every day. According to Hollnagel, our need to identify a cause for any accident has coloured all risk assessment thinking. Only simple technology and simple accidents may be said to be “caused.” For complex systems and complex accidents we don't "find" causes; we "create" them. This is a social process which changes over time just as thinking and society change.

It is to be noted that it is not just to be able to recover from threats and stresses, but to respond appropriately to both disturbances and opportunities – a change from ‘protective safety’ to ‘productive safety’ – thereby leaving the sterile discussions and the stereotypes of the past behind. Resilience is about how systems perform, not just about how they remain safe. Hollnagel and other resilience thinking proponents see the challenge not as finding cause. The challenge is to explain why most of the time we do things right and to use this knowledge to shift accident investigation and prevention thinking away from cause identification to focus on understanding and supporting human creativity and learning and performance variability. In other words, understanding how we succeed gains us more than striving to recreate an unknowable history and prescribing fixes to only partially understood failures.

Cause and Effect Relationships - & pitfalls

Although generally accepted as the overarching purpose of the investigation, the identification of causes can be problematic. Causal analysis gives the appearance of rigor and the strenuous application of time-tested methodologies, but the problem is that causality (i.e., a cause-effect relationship) is often constructed where it does not really exist. Investigators look backwards with the undesired outcome (effect) preceded by actions, which is opposite of how the people experienced it (actions followed by effects).

A true cause and effect relationship must meet the requirements of (a) The cause must precede the effect (in time); (b) The cause and effect must have a necessary and constant connection between them, such that the same cause always has the same effect.

This second requirement is the one that invalidates most of the proposed causes identified in accident investigations. As an example, a cause statement such as "the accident was due to inadequate supervision" cannot be valid because the inadequate supervision does not cause accidents all the time. This type of cause statement is generally based on the simple "fact" that the supervisor failed to prevent the accident.

In a complex socio-technical system involving people, processes and programs, the observed effects are usually 'emergent phenomena' due to interactions within the system rather than 'resultant phenomena' due to cause and effect. Since accidents do happen, there are obviously many factors that contribute to the undesired outcome. These factors are often identified by missed opportunities and missing barriers which get miss-labelled as causes. The investigation should focus on understanding the context of decisions and explaining the event. In order to understand human performance, one must not limit oneself to the quest for causes. An explanation of 'why people did what they did' provides a much better understanding - and with understanding comes the ability to develop solutions that will improve operations.

Human Performance Considerations in the context of Work

According to the DOE Handbook on *Accident and Operational Safety Analysis* (2012), workers have knowledge, but the application of knowledge is not always straight forward because it needs to be accurate, complete and available at the time of the decision. Goals and knowledge combine together to determine the worker's focus. These influences and differences include:
Organization - actions taken to meet management priorities and production expectations;
Knowledge - actions taken by knowledgeable workers with intent to produce a better outcome;
Social – actions taken to meet co-worker expectations, informal work standards;
Experience – actions based on past experience in an effort to repeat success and avoid failure;
Inherent variability – actions vary due to individual psychological & physiological differences;
Ingenuity and creativity – adaptability in overcoming constraints and under specification.

The result is variable performance. From the safety perspective, this means that the reason workers sometimes trigger an accident is because the outcome of their action differs from what was intended. Conversely, successful performance and process improvement also arises from this same performance variability. Expressed another way, performance variability is not aberrant behaviour; it is the probabilistic nature of decisions made by each individual in the organization that can result in both success and failure - emerging from same normal work sequence. In accident investigations, performance variability needs to be acknowledged as a characteristic of the work, not as the cause of the accident. Rather than simply judging a decision as wrong in retrospect, the decision needs to be evaluated in the context in which it was made.

The Fifth Age of Safety

It has been suggested by Borys, Else & Leggett (2009) in *The Fifth Age of Safety: the Adaptive Age*, in the Journal of Health & Safety Research & Practice, that we are living in the fifth age of safety. The first was a technical age, the second a systems age, and the third a culture age. Metaphorically, the first may be characterized by engineering, the second by cybernetics and systems thinking, and the third by psychology and sociology. The fourth age, the "integration age," builds on the first three ages not abandoning them but blending them into a trans-disciplinary socio-technical paradigm, thus prompting more complex perspectives to develop and evolve. The fifth age is an "adaptive age." It does not displace the former, but rather transcends the other ages by introducing the notion of complex adaptive systems in which the roles of expertise, professional practice, and naturalistic observation attain primacy in resolving the duality of "work-as-imagined" versus "work as done."

The adaptive age embraces adaptive cultures and resilience engineering and requires a change in perspective from human variability as a liability and in need of control, to human variability as an asset and important for safety. Embracing variability as an asset challenges the comfort of management. However, the gap between work as imagined and work as performed and the failure of OHS management systems and safety rules to adequately control risk mean that a new perspective is required.

What is important to remember is not that individuals in organizations make mistakes, but that mistakes themselves are socially organized and systematically produced. The accidents have systemic origins that transcended individuals, organization, time and geography. Its sources are neither extraordinary nor necessary peculiar. Instead, its origins are in routine and taken for granted aspects of organizational life that create a way of seeing - that was simultaneously a way of not seeing.

The most important contribution of this new version is the reminder that tools are only mechanisms for collecting and organizing data. More important is the framework; the theory derived from research and practice, that is used for interpreting the data.

This version thus challenges future investigators to apply analytical tools and sound technical judgment within a framework of contemporary safety science and organizational theory.