Prof. Nancy Leveson

Aeronautics and Astronautics Dept.
MIT, Room 33-334
77 Massachusetts Ave.
Cambridge, MA 02142

Telephone: 617-258-0505 (MIT)
Email: leveson@mit.edu
URL: http://sunnyday.mit.edu

Dr. Nancy Leveson is a professor of Aeronautics and Astronautics at MIT. She has worked in system safety engineering for over 35 years. One common element in her work is an emphasis on applying systems thinking to complex systems and integrating humans and social systems with engineering considerations. She consults extensively on the ways to prevent accidents and has served on numerous national and international committees and accident investigations. She was an expert consultant for the Columbia Space Shuttle Accident Investigation Board, the Presidential Commission on Deepwater Horizon, the Baker Panel on the Texas City oil refinery explosion, and other lesser known losses.

Captain Shem Malmquist
Visiting Professor, Florida Institute of Technology
274 E. Eau Gallie Blvd. 252, Indian Harbour Beach, FL 32937
smalmquist2012@fit.edu

Captain Shem Malmquist is a visiting professor at the Florida Institute of Technology, an experienced accident investigator and an active current B-777 Captain. His work includes Automation and Human Factors lead for the Commercial Aviation Safety Team's Joint Safety Implementation Team, Loss of Control working group, the Aircraft State Awareness working group and the Joint Implementation Measurement and Data Analysis Team. He is an elected Fellow of the Royal Aeronautical Society, a full member of ISASI, REA, AIAA, HFES, IEEE, FSF and SAE's Flight Deck and Handling Quality Standards for Transport Aircraft working group.

Updating the Concept of Cause in Accident Investigation

Prof. Nancy G. Leveson, Aeronautics and Astronautics, MIT
Capt. Darren Straker, Air Accident Investigation Authority, Hong Kong
Capt. Shem Malmquist, Florida Institute of Technology

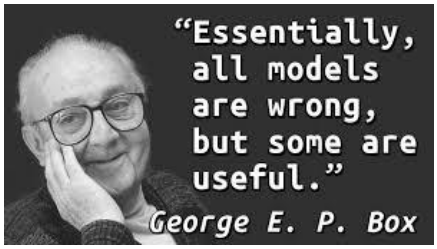
Traditional accident investigation practices are being challenged by the introduction of advanced technology. The increasing complexity of today's systems, enabled by the increasing and almost universal use of automation, is making the current approach to determining cause in accident investigation less useful. In this paper, we argue that we can no longer learn enough from accidents in aviation systems if we continue to limit ourselves to a linear view of causality.

The paper first examines how causality models impact our understanding and prevention of accidents. It then argues that linear causation models, such as the traditional chain-of-events (COE) model, are outdated and limit what is learned from accidents about how to prevent future occurrences. Finally, an alternative is suggested.

Causality Models

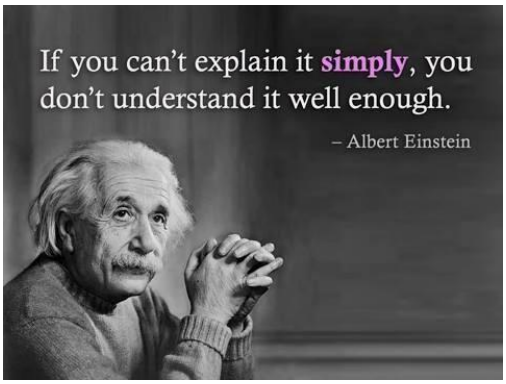
The goal of a causality model is to enhance understanding of causation, namely, how things work, and therefore a prediction about how things will behave in the future. We use models in design and development to better achieve our design goals for the system, in operations to more effectively operate and manage the use of the systems, and in accident investigation to understand why the loss occurred and to learn how to prevent future losses. All accident analyses and prevention efforts are based on the model of causality we are using. We may not be aware that we are using one, but we are. The question considered in this paper is whether we are learning enough from the current causality model used in accident investigation today or whether the current model or conception of causality is inhibiting our learning and prevention activities for the increasingly complex systems we are building and operating.

Models are not right or wrong, they only have comparative effectiveness. George Box famously argued that "All models are wrong; some models are useful." That is, all models are incomplete as they leave out something. They are an abstraction placed on a messy world to make it appear less "messy." By definition, an abstraction leaves out something---otherwise it is not a model (i.e., abstraction) but the thing itself. We hope that the model does not omit anything important with respect to our goals for the use of the model.

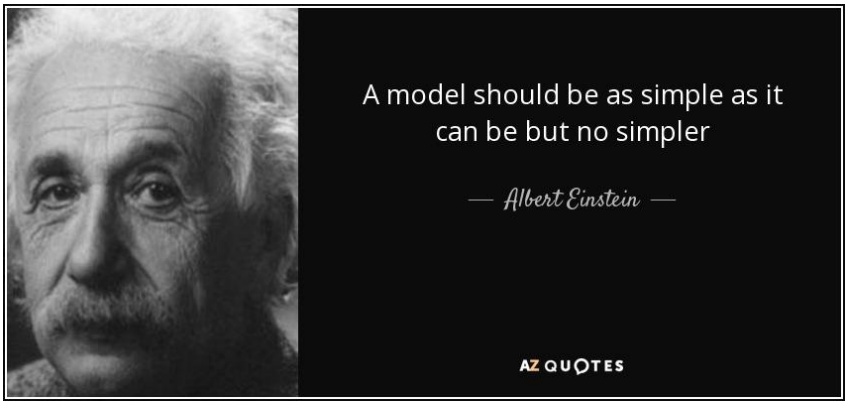


So rather than being "right" or "wrong," models simply differ in terms of usefulness. One model may be a better predictor of the future and allow us more control over future events than others.

We like simple models, and a simple model that is useful is indeed a good thing. Einstein said:



But at the same time:



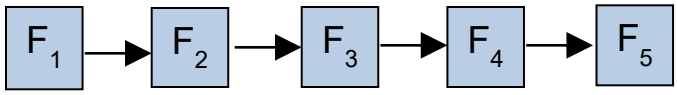
Simplicity is not the only criterion for a good model of causation. The model must also be useful. The outcome of an accident investigation is safety recommendations, so the usefulness of the causation model to help generate them is key. In ICAO Annex 13, a safety recommendation is defined as:

> *'Safety recommendation. A proposal of an accident investigation authority based on information derived from an investigation, made with the intention of preventing accidents or incidents and which in no case has the purpose of creating a presumption of blame or liability for an accident or incident…'*

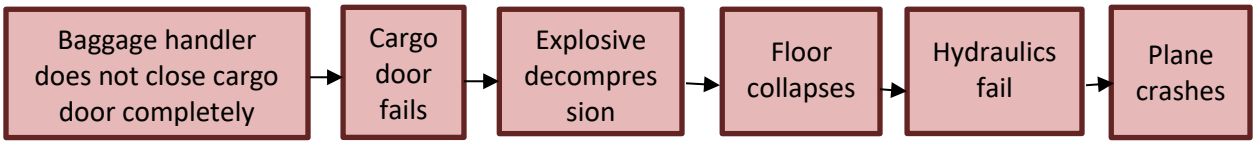
The Chain-of-Events (COE) model

The traditional model of causality used today assumes that accidents are caused by chains of failure events. This model is very simple and easily understood. It actually dates back hundreds of years. The important question is whether, for today's complex systems, it is too simple, i.e., whether it omits the most important causal factors important in accident investigation.

The COE model assumes that accidents result from chains of failure events.



Each event in the chain is the direct result of the preceding one. If F_1 does not occur, then by definition F_2 will not. More formally, F_1 is necessary and sufficient for F_2 to occur. The events identified are almost always system component failures until the final event, which is the system failure. As an example, consider the chain of events in the Turkish Airlines DC-10 loss over Paris in 1974, one of the deadliest crashes in aviation history (and used here because a lot of information about causes has been surfaced, with little remaining argument):



In this model of the chain of events, the cargo door handler did not shut the cargo door completely, the aircraft took off with the door not completely sealed, which resulted in explosive decompression, the collapse of the floor, the failure of the hydraulics (the cables all went through the floor), and the loss of the aircraft. We could easily choose more events to include in the chain or even a different subset of events (e.g., the light in the cockpit indicating the door had been properly closed when it had not could be added) and still argue, correctly with respect to the COE model, that we have identified the cause of the accident.

One event in the chain is usually identified as the "root" or, sometimes, "probable" cause of the final loss event. Any event could be labeled as the root cause: It is completely arbitrary which one is chosen. For example, the baggage handler might be labeled as the root cause (and in fact he was arrested immediately after the accident) or the failure of the hydraulics could be labeled as the root cause. Labeling the first failure in the chain as the root cause does not solve the problem as more prior events could always be added to the chain.

What is not included here are the things not included in the events, namely, *why* the events occurred. For example, the design of the door made it hard for the baggage handler to detect that the door had not actually closed. There was a flaw in the design of the latching mechanism in the door. The light in the cockpit indicated to the flight crew that the door had closed when it had not. The same event had happened during ground testing before certification but was ignored because it was considered to be a small problem with low probability of occurrence. Claims were made later about a cozy relationship between MDA and the FAA, leading to certification irregularities. A prior incident occurred (AA 96 over Windsor Ontario) but due to the skill of the pilots as well as the fact that not all the cables were severed, the aircraft was saved. However, nothing effective was done to solve the design problem and instead the prior Windsor accident was also blamed on the baggage door handler. After Flight 96, a service bulletin was issued to make changes to the door but was never implemented in the case of the Turkish Airlines aircraft, either due to oversight or fraud. Changes were made to the cockpit warning light switch mechanism after Flight 96, which had an unintended consequence that the warning light would go off even though the door latches were not fully in place. Another fix after Flight 96 was to add a peephole to assist the cargo door handler in determining that the latches were in place, but Turkish Airlines had never instructed the baggage handler in how to use this peephole. In addition, the instructions regarding the peephole were printed in English and Turkish but the baggage handler, who was fluent in three other languages, could not read either of these languages. Most of the readers of this paper are familiar with this accident and the conditions contributing to it, but are any of the factors listed above in the chain of events? And even if considered, which of them is the root cause?

COE models describe simple, direct relationships but omit more complex and indirect relationships. Note that the Domino, Swiss Cheese, and Bow Tie models are the COE events model using different real-

world analogies, i.e., dominos, Swiss cheese slices, and formal men's apparel. They are not different causal models, but simply different names and graphical representations for the same thing.

Again, the question is not whether a model is right or wrong. The COE model does provide an explanation for an accident. The question is whether it is the most useful explanation for the goals of accident causal analysis and prevention. The Navier-Skokes equations (model) provide a more complete explanation of air flow over the wings than the simpler Euler equations that preceded them. The Euler equations neglect the effects of the viscocity of the fluid, which are included in the Navier-Stokes equations. That doesn't mean that the Euler equations may not be useful in some circumstances.

Limitations of the COE Model

The COE model is an easily understood model, due in part to its inherent simplicity. The crucial question is whether it is still as useful and applicable as it once was for today's increasingly complex and software-intensive systems, both the technical and social aspects. The answer to that question is that it depends on what is your goal or potential use for the model

Four limitations are discussed here:

(1) The focus on a root or probable cause,
(2) The focus on failure
(3) Limitations on what is included in the model
(4) Promotion of hindsight bias

Focus on identifying a root or probable cause

John Carroll has coined the term "root cause seduction." We like having a root cause because it gives us the illusion of control. If we can identify a root cause that can be easily eliminated, then we can control future accidents. We don't want too many things that we have to eliminate, one identified cause is ideal. Usually the root cause selected is a human operator or technical component failure, which may only be a symptom of much deeper problems. Identifying and eliminating the superficial result of the deeper problems enhances our feelings of control over losses, but actually does little to prevent future losses.

The COE model can also be used to deflect responsibility from ourselves or to make sure that attention is not drawn to our decisions. Because the COE says that one event is the "root" or "probable" cause of the final loss event and the selection of that event is completely arbitrary, then we simply need to make sure that the event in which we ourselves were involved is not declared to be the root cause.

The best result, from our own perspective, is to make sure that nothing we did or nothing that was related to what we did is contained in the chain of events used to describe the cause of the accident. That helps us avoid the spotlight entirely, and its usually easy to accomplish when only direct or simple relationships are included in the chain. For example, it's difficult to chain backward from a human action to the design of the system that influenced that action. What "event" is involved in the design of the aircraft, the design of the pilot-vehicle interface, or competitive and productivity pressures?

In addition, it is usually simple to argue that because not everyone made a mistake when presented with the same circumstances, those circumstances cannot be the cause. For example, other pilots flew the 737 MAX before the Lion Air and Ethiopian Airlines crashes, and they were able to overcome the design flaws. Therefore, any aircraft design flaws cannot be the "cause" of the accident. The implication here is that only direct causes exist and are important, not indirect ones. Using the COE model, smoking does not cause lung cancer because not everyone who smokes gets lung cancer and not everyone who gets lung cancer smokes. We simplify the causal mechanism for our own purposes or perhaps because it's a lot easier for us to understand and to build agreement among everyone. Do you really believe,

however, that smoking has no relationship to getting lung cancer? Does denying this relationship, as the Tobacco Institute successfully did for many decades, lead to effective prevention measures?

The pilots are almost always in the COE for an aircraft accident. We can arbitrarily pick something a pilot did as the root or probable cause, and then deflect attention away from anything non-pilots did that contributed. For "pilot" we can substitute any non-management role, such as a maintenance worker or air traffic controller.

After a while, it becomes established that pilots are the cause of most accidents because they always appear in the COE identified for an aircraft accident and are usually the focus of potential blame arguments. The cause of the accident being the pilot then becomes simple and easier to prove for future losses. After a while, pilot behavior becomes the only thing we need to focus on. An hour after the crash, the newspapers can declare the cause was pilot error.

It is not, of course, usually the case that pilots have nothing to do with aircraft accidents. And their contributions may be major. The problem is that by oversimplifying causation, we miss the opportunity to find more contributors and therefore make more comprehensive changes to prevent future accidents. Substituting automation for pilots simply shifts the spotlight to the engineers who create the automation. It can also lead us to incorrect conclusions. Once we accept that pilots are the problem, it would appear that the solution is to eliminate pilots or introduce automation to take over more of their functions. In fact, this is the stated impetus (often listed before cost) behind some of the current efforts by several manufacturers to argue for fully automated aircraft. In reality, automation probably will not eliminate accidents but merely change the causal factors we encounter and shift the spotlight to the engineers who create the automation or to the pilots that monitor it: Automation design can contribute to human error, and all humans cannot be removed from systems. Besides, total automation is not feasible for any but the simplest conditions. Today, however, what typically occurs is that we declare the pilot as the cause—or spend endless time in useless arguments about whether the pilot was the cause—and miss the opportunity to have a major impact on the occurrence of future accidents.

It is also not much help to tell pilots not to make mistakes or to train them to follow procedures when the procedures do not handle the conditions that actually occur or are not the right thing to do in that particular case.

Human behavior is always affected by the context in which it occurs. We are building systems today that are so complex that even the engineers do not understand all the potential system behavior, the so-called "unknown unknowns." Why would pilots be better able to identify a flawed design or flawed automation behavior and respond correctly under stressful and time-limited conditions? It is remarkable that pilots do as well as they do under extreme circumstances (e.g., the QF32 uncontained engine failure or the QF72 uncommanded pitch over). We are designing systems today in which operator error is inevitable and then blame the results on the operators. In fact, one could argue that human error is a symptom of a system that needs to be redesigned. To eliminate human errors, we need to change the system design.

Another example: Does anyone really believe that competitive pressures on Boeing with respect to the Airbus A320neo had absolutely no influence on Boeing management decision-making with respect to factors that impacted the Lion Air and Ethiopian accidents? Was it really just that foreign pilots are not well trained or are less competent than American and European pilots (a current popular argument)? Or that changes in the behavior of the B737 MAX aircraft had no influence on the pilot behavior and thus the losses? Was the fact that redundancy was not used for the sensor simply a random mistake by a design engineer at Boeing that was unrelated to the lack of a systems view of the operation of the aircraft as a whole and the procedures used to certify aircraft today? That the design issues that occurred in MCAS were not related to the system engineering processes and procedures used and will never occur again? That the regulatory policies and practices and their changes over time

to give more autonomy to Boeing also had no importance? Can we really explain the B737 MAX accidents with a simple chain of events, with the pilot actions highlighted along with perhaps the MCAS design as the only actions worthy of attention? Competitive pressures, regulatory policies, basic design features are not 'events' so they don't appear in the chain of events and therefore can be dismissed without consideration by those who find it convenient to ignore these factors.

As could be predicted, the B737 MAX accidents have led to lots of talk about the COE model. For example, on June 26, 2019, Boeing Chairman and CEO Muilenburg addressed Lion Air Flight 610 and Ethiopian Airlines Flight 302 crashes at the Aspen Ideas Festival 2019. "Anytime there is an airplane accident, it involves a chain of events and we are spending time with investigators to understand every dimension of that," adding that MCAS, being "one of the items" in this chain of events, "added to the workload" of the pilots. Boeing also announced that it "could break the chain of events that led to both crashes by developing a software fix that would limit the potency of that stabilization system." Is creating a fix for the MCAS software to prevent the specific events in the Lion Air and Ethiopian Airlines accidents really the solution for the B737 MAX problems and, indeed, those of other new aircraft being designed today? Already, new problems with the B737 MAX design are being uncovered [Bloomberg 2019; Flight Global 2019; Financial Times 2019;], none of which will be fixed by a simple update to the MCAS software to limit its authority. While the software needs to be fixed, the real causes of the accidents that need to be tackled go much deeper than that and they are not only at Boeing.

Accident investigation can be accusatory or explanatory. An accusatory accident report focuses on who to blame for the accident and what that person or thing did wrong. In contrast, an explanatory accident report focuses on what happened and why the loss occurred without trying to assign blame. That is the goal for the courts and lawyers, not for engineers.

The biggest problem with a focus on blame is that blame is the enemy of safety. If blame is a potential result, people stop reporting errors, information is hidden, finger pointing becomes a fundamental activity, and learning is inhibited

A focus on failures, especially operator "failures"

Because the COE contains primarily or only failure events, the focus is on failures when the COE is used to explain why an accident occurred. But accidents today are not simply caused by system component failures. Increasing complexity is leading to accidents in which nothing failed but were caused by unsafe interactions among the system components and system design flaws. Consider the A320 accident at Warsaw in 1993 [Warsaw 1993] where the software did not think that the aircraft had landed and prevented the pilots from activating the reverse thrusters. The specific odd conditions that occurred had not been considered, or at least had not been properly handled, by the engineers. Each component in the system, however, worked as it was designed to work. The did not fail: The design, including the interactions among the components, was unsafe.

The word "failure" is pejorative, that is, it is a judgement and assigns blame. The problem is that once blame has been assigned, there is no need to look further. Note the difference between the two statements about the cause of an accident:

(1) The captain's failure to reject the takeoff during an early stage when his attention was called to anomalous engine instrument readings.
(2) The captain did not reject the takeoff during an early stage when his attention was called to anomalous engine instrument readings.

The first statement is judgmental and a conclusion that the captain was responsible for the accident. The reader can stop there. The second encourages the reader to look further at the anomalous instrument readings and why they occurred because the pilot has not already been declared to be the primary problem.

The American Airlines B757 crash while trying to land at Cali, Columbia, in 1995 provides another example. There are four causes identified in the accident report, all identified as flight crew failure. Perhaps the most egregious is the fourth:

> "Failure of the flight crew to revert to basic radio navigation at the time when the FMS-assisted navigation became confusing and demanded an excessive workload in a critical phase of flight."

Note that the flight crew were blamed for confusion caused by using the automation they were told to use, which also demanded an excessive workload, resulting in distraction. Only in hindsight could the crew (or the investigators) know that the crew was confused. Focus should, in this case, be on changing the design of the automation and not on the fact that the crew used it. When the focus is on finding someone or something to blame, questions like "why did the pilot think it was the correct action at the time," which is the essence of avoiding hindsight bias (see below), are not emphasized.

Limitations in what is included in the model

Accident reports using COE models as the primary methodology invariably specify an event, usually a pilot "failure," as the root or probable cause. Often the contributory causes are also focused on pilot actions. Much less frequently are the reasons why the events occurred included. While they may be buried somewhere in the report contents, rarely are they listed in the report summary of the "cause" or even in the findings, and therefore they may not be used to generate safety recommendations.

The causal factors in an accident are not the basic events that occurred but the systemic factors that led to the events and disabled the protections built into the system to prevent them. The systemic factors are not events and therefore are left out of the chain of events model: examples include design of automation and the increasing amount and kind of automation itself (not just assisting but taking over and changing the role of pilots), corporate and industry culture, industrial competition and its impact on what types of systems are built, migration toward states of higher risk (e.g., reducing the type and amount of regulation after it is effective and drives down accident rates and therefore is no longer seen as necessary because accident rates are low), etc.

In addition, rarely are the interactions among the events in system behavior limited to simple causal chains. There may be complex interactions among the events and the causal factors may interact in non-linear ways. Linear chains are a small subset of the way that events and conditions interact in complex systems.

We need accident causation models that include the underlying causal factors and not the artifacts or events that resulted from these causes. They must also identify the complex interactions that result in unsafe conditions and events, with the view to introducing controls to mitigate future safety action to prevent a reoccurrence.

Promoting hindsight bias

After an accident or incident, it is easy to see what should have been done or avoided and easy to make judgments about missing a piece of information that turned out to be critical. This phenomenon is called *hindsight bias*. After the fact, the causal connections are firmly established in our minds, and it is almost impossible to go back and understand how the situation looked to somebody without knowledge of the outcome.

Hindsight bias is ubiquitous. Accident reports are filled with phrases like "X should have …" or "X could have …" or "if only X would have …"

Another example from the Cali Columbia accident is the cause listed in the accident report as "Failure of the flight crew to discontinue the approach into Cali, despite numerous cues alerting them to

the inadvisability of continuing the approach." Unfortunately, most of those cues were only obvious if one knew that continuing the approach would result in the aircraft flying into a mountain, i.e., after the accident.

Dekker has suggested that hindsight bias can be reduced by emphasizing not what the people involved did wrong, but why it made sense for them to do what they did [Dekker 2002]. We don't learn much from simply listing what people did wrong. We do, however, obtain important information for prevention from understanding why they did what they did and why it appeared to them to be the right thing to do at the time.

It's time to adapt our models of causation to include the most relevant causes related to the more complex aircraft designs and operations today. We need to expand our model of causation to provide better explanation, prediction, and prevention, that is, control over future events. The COE has had its day. It is simple, easy to understand, and easy to manipulate to serve our own sometimes selfish purposes, but not very useful in preventing future accidents. It is, to exploit the words of Einstein, too simple to serve the goal of protecting the general public.

The Alternative: Non-Linear, Systemic Causality Models and Investigation Methods

Arguments against the concept of probable or root cause, or in general limitations in the explanation of why an accident occurred are not new (see, for example, the ISASI papers by Miller 1991 and Rimson 1998). The continued use of overly simple and incomplete COE models and identification of root cause is likely because few alternatives have been available. This is no longer true. At least one alternative model has been proposed and others are possible. The problem is opening people's minds to change.

A non-linear causality model acknowledges that accidents are not just caused by a linear chain of events, but the concomitant occurrence of multiple factors that come together to produce the loss. Attention is not on the events but on why the events occurred and why the controls that were used to prevent such an occurrence were not effective. Accidents are explained not in terms of failure events but in terms of inadequate *control* over the events.

A systems or non-linear approach to modeling causality focuses on the design of the entire sociotechnical system as a whole, including the safety controls, and identifies weaknesses in the system design that led to the loss event. Examples are pilot mode confusion caused by introducing complex new software functions, management attempts to reduce maintenance costs by reducing or eliminating important activities, or changes to regulatory oversight.

Human decisions and behavior are not viewed as failures but rather as part of a flawed system that influenced the individual's behavior. Accidents are not viewed as a failure problem but a control problem. The solution is to fix the system as a whole.

Leveson's STAMP (System-Theoretic Accident Model and Processes) is an example of one such non-linear accident causality model [Leveson, 2012]. It is now being used in system design in most industries. STAMP is more powerful than the COE model; it includes complex interactions among humans, physical failures, environmental conditions, established processes, social structures, and organizational and industrial culture. The events, and particularly the failure events, are only one small aspect of the cause. And they may be the least important factor in learning from losses and preventing future accidents. To prevent the events, we need to prevent the conditions and behavior that led to the events.

Accidents are a *control* problem. Preventing "failures" is not enough as the most important factors in accidents are not failures but are instead the systemic conditions that impact or create the failures or other events. They explain why the events occurred. These factors are not in the event chain.

The assumptions underlying STAMP differ from those underlying the COE model. First, accidents are not just caused by failures or by simple chains of failure events. The interactions among events are important in accident causation, and these interactions are usually more complex than simple chaining relationships. There can be feedback loops and other types of interactive processes at work that dampen or heighten the way the system components behave. For example, one possible factor that can be hypothesized as being part of the cause of the B737 MAX losses is that the past success of Boeing in promoting safety and a lack of adequate resources provided by Congress helped to convince the FAA to relax the oversight in the DER process, essentially changing it into a self-certifying process for Boeing. This process was probably fine at first but degraded over time by pressures on the company that conflicted with safety. It is this type of change that usually precedes an accident—the system slowly and inadvertently changes to one where an accident is inevitable. Basically, the system migrates slowly toward a state of higher risk [Rasmussen 1997]. Doesn't that provide a more useful causal explanation than "the pilot zigged when he/she should have zagged"?

In STAMP, events are not assumed to be independent. Events and behaviors may have subtle and indirect influences on each other. And they may all be influenced by general conditions or factors in the system or its environment, called systemic factors, such as financial difficulties, competitive pressures, management and regulatory structures, poor cultural or value systems—such as the safety culture or value systems that influence decision making about safety—and so on. The COE model assumes that the events in the chain are independent and each event is only the direct result of the event(s) preceding it. This assumption is untrue in almost all real-life accidents.

To oversimplify somewhat, STAMP models accidents as resulting from inadequate control over the events, the conditions leading to the events (*why* they occurred), the behavior of individual system components, and the interactions among the system components and with the environment. When accidents occur, we need to identify why the controls did not work and improve them.

A new accident analysis method, called CAST and based on STAMP, has been created to guide accident investigation and identify the questions that should be asked during the investigation. CAST (Causal Analysis based on System Theory) provides a structured process that assists in producing a more thorough investigation of the cause of an accident.

As a brief example of CAST and treating safety as a control problem, consider the UPS CFIT (Controlled Flight into Terrain) accident at Birmingham-Shuttleworth International Airport on August 14, 2013. The only runway with a precision approach was closed at the time for ILS maintenance, so the Captain accepted a shorter runway with a nonprecision approach [Malmquist et.al. 2019]. The aircraft crashed a mile short of the runway.

The NTSB report on this accident [NTSB 2015] used the traditional COE approach and identified the following causes [Emphasis added]:

> Probable Cause: the flight crew's continuation of an unstabilized approach and their failure to monitor the aircraft's altitude during the approach, which led to an inadvertent descent below the minimum approach altitude and subsequently into terrain.
>
> Contributing Causes:
>
> 1. The flight crew's failure to properly configure and verify the flight management computer for the profile approach;
> 2. the captain's failure to communicate his intentions to the first officer once it became apparent the vertical profile was not captured;
> 3. The flight crew's expectation that they would break out of the clouds at 1,000 feet above ground level due to incomplete weather information;
> 4. The first officer's failure to make the required minimums callouts;

5. The captain's performance deficiencies likely due to factors including, but not limited to, fatigue, distraction, or confusion, consistent with performance deficiencies exhibited during training; and
6. The first officer's fatigue due to acute sleep loss resulting from her ineffective off-duty time management and circadian factors. [Emphasis added]

Responsibility for this loss is clearly assigned to the flight crew.

In contrast, CAST looks at causation as a control problem, not a failure problem, and examines the controls that have been created to prevent CFIT. CFIT has been an important safety problem in aviation for a long time. Much effort has gone into preventing it and lots of controls created including: airport physical structures such as ILS and PAPI, ground proximity warning systems (EGPWS), ATC systems including a minimum safe altitude warning (MSAW) and, in this case, weather information (ATIS), NOTAMs, aircraft navigation displays, airline dispatch communications, pilot training and procedures, etc. Rather than the goal of assigning responsibility for the loss, the focus in the CAST analysis is to understand why the existing CFIT controls did not prevent this loss and what changes might be made to strengthen the controls in the future.

For each of the controls and the controllers that implement them (such as the airport authority having control over the airport physical CFIT controls), the causal analysis provides information about whether the control was effective that day at BHM and, if not, then why it was not effective. For humans who did the wrong thing (in hindsight), emphasis is on why it made sense for them to do what they did given the information they had at the time (their mental model) and the context in which their actions and decision making took place. The goal is to understand why the accident occurred despite everyone trying to do the right thing. That information can be used to recommend changes to the system in order to prevent future CFIT losses during airport approach.

Looking only at one type of control as an example, i.e., the airport physical controls (ILS and PAPI), one goal of the CAST analysis is to determine why they were ineffective in this accident. The NTSB report does not mention them in the causal analysis as neither "failed." In this case, the runway on which the aircraft was landing did not have ILS installed. The runway with ILS glideslope control was closed for maintenance at the time and was scheduled to reopen 9 minutes after the UPS aircraft was scheduled to arrive. The CAST analysis process generates lots of questions with respect to the decisions related to ILS, the answers to which are omitted from the official accident report, perhaps because of the lack of direct causality. One question is why the airport did not have ILS on all runways; this decision probably involved cost or feasibility reasons. More interesting is why maintenance was performed on the primary runway during a time when large aircraft operations were scheduled. What types of Management of Change procedures are in place to analyze safety when making maintenance decisions? Could maintenance have been scheduled for a different time when large aircraft were not scheduled to arrive? This in turn generates questions about when and what type of information was provided to scheduled airlines about maintenance that night. What types of constraints are airports under (e.g., controls by the FAA Office of Airport Safety and Standards) in scheduling maintenance outage times? Is as much weight put on cargo aircraft safety as passenger aircraft? Large cargo operations at night are a relatively new practice. Could this change have happened slowly over time, resulting in decision making and practices not keeping up? Accidents often result from systems migrating toward states of higher risk over time under various types of pressures. Is decision making about airport maintenance procedures related to prevailing safety culture with respect to how airports treat cargo carriers? These and other questions need to be answered.

Shifting attention to the PAPI, they were operational and operated as designed at the time of the accident. However, they were not visible to the pilots due to a combination of aircraft height and low cloud ceilings. The PAPI were designed for height group 3 aircraft but the A300 is a height group 4

aircraft. The accident report says that the PAPI indicators would have been visible for less than 1 second before being obscured by rising terrain. It is clear why they were not an effective control in this case. What is unanswered is why large aircraft are allowed to use runways for which navigational equipment is not effective and whether the FAA provides guidance for the navigational equipment to be installed on particular runways or restrictions on their use. Are such restrictions necessary?

Each of the controls would be analyzed similarly in CAST, including the role of UPS dispatch, ATC, EGPWS, the FAA, the aircraft instrumentation, NOTAMs, ATIS, etc. The pilots are, of course, included but the analysis of the role played by the pilots does not focus on what, in hindsight, they did wrong but why they thought that what they did was the right thing to do. What kinds of information did the flight crew have in making their decisions and how did the context in which the decisions were made affect their decision making? In summary, while both the CAST and official NTSB report use the same data, the questions asked, the answers generated, and the conclusions reached are very different.

CAST is described in more detail and an example provided in another paper presented at this same meeting. More about STAMP and CAST can also be found in *Engineering a Safer World* [Leveson 2012] and the new CAST Handbook [Leveson 2019].

Let's not let the response to the most recent and future tragic losses be reduced to the usual wrangling and posturing as well as arguments about "root cause" using oversimplified causal models. Instead, we can, as engineers, pilots, and users of these systems, insist on employing more sophisticated explanatory models as to why accidents occur and increase our learning from these tragedies. After we have a more complete explanation of an accident, we can use what has been learned to create significantly safer systems for the future.

References

[Bloomberg 2019] Benjamin Katz and Alan Levin, Boeing 737 Max's Autopilot has a Problem, European Regulators find, retrieved from https://www.bloomberg.com/news/articles/2019-07-05/europe-sets-out-demands-for-boeing-before-max-can-fly-again

[Dekker 2002] Sidney Dekker, *The Field Guide to Understanding Human Error*, Ashgate Publishers, 2002.

[Flight Global 2019] FAA Finds Issue with 737 MAX trim recovery procedure, retrieved from: https://www.flightglobal.com/news/articles/faa-finds-issue-with-737-max-trim-recovery-procedure-459331/

[Financial Times 2019] Europe asks Boeing to fix safety issues on 737 Max retrieved from: **https://www.ft.com/content/b98ccbfa-9f27-11e9-b8ce-8b459ed04726**

[Leveson 2012] Nancy Leveson, *Engineering a Safer World*, MIT Press, 2012.

[Leveson 2019] Nancy Leveson, A CAST Handbook, downloadable from http://psas.scripts.mit.edu/home/materials/

[Malmquist 2019] Shem Malmquist, Nancy Leveson, Gus Larard, Jim Perry, and Darren Straker, Increasing Learning from Accidents: A Systems Approach Illustrated by the UPS Flight 1354 CFIT Accident, downloadable from: http://sunnyday.mit.edu/UPS-CAST-Final.pdf

Miller 1991] C.O. Miller, Down with 'Probable Cause,' *Int. Soc. Of Air Safety Investigators Seminar*, Canberra, Australia, November 7, 1991.

[NTSB 2015]. *UPS 1354 DCA13MA133.* Retrieved from: https://www.ntsb.gov/investigations/Pages/2014-Birmingham-AL.aspx

[Rasmussen 1997] Jens Rasmussen, Risk Management in a Dynamic Society: A modeling problem. *Safety Science* 27(2/3):183-213, 1997.

[Rimson 1998] Ira Rimson, Investigating 'Causes,' *Int. Soc. Of Air Safety Investigators International Seminar*, Barcelona Spain, Oct. 20, 1998

[Warsaw 1993] Main Commission Aircraft Accident Investigation Warsaw, "Report on the Accident to Airbus A320-211 Aircraft in Warsaw on 14 September 1993.