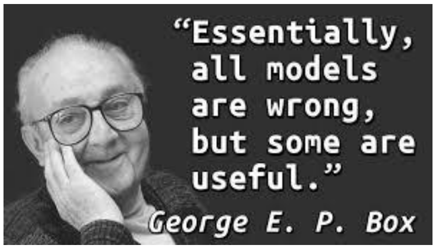
The Chain of Events Model Has Outlived its Usefulness
(or The Probable Cause is Probably Improbable)

Prof. Nancy G. Leveson
Aeronautics and Astronautics
MIT

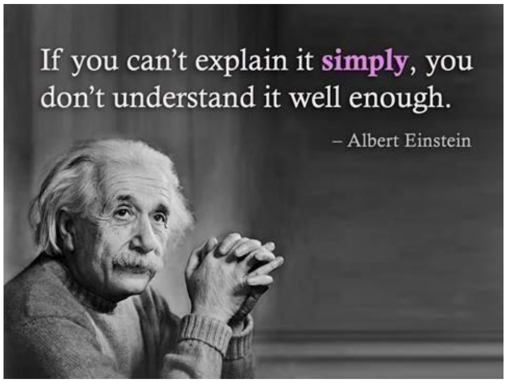
With the B737 MAX accidents has come lots of talk about the chain-of-events (COE) model[1]. The goal of the COE model is the same as any model, namely, to provide understanding of causation (how things work) and therefore prediction about how things will behave. We build models when designing systems in order to prevent or to create future events, depending on the goal of the model. The Napier-Stokes equations help us to design aircraft. Models of human behavior assist in designing human-automation behavior in a way that improves the results. Models of social behavior explain why societies behave the way they do and how to design them to change or control behavior.

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.



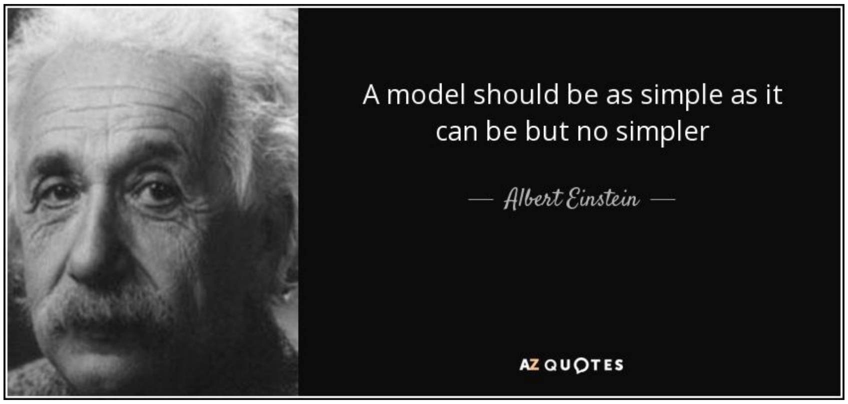
So rather than being "right" or "wrong," models simply differ in terms of usefulness. One model may be a better predictor of the future and allow us more control over future events than others.

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


If you can't explain it simply, you
don't understand it well enough.
– Albert Einstein

[1] Note that the so-called "bow-tie" model is just a chain of events model drawn in a particular way and given a "cutesy" name. It is not unique in any respects. The Domino and Swiss Cheese models are simply a chain of events model using different real-world analogies, i.e., dominos and Swiss cheese slices. All are different names for the same thing.

But at the same time:



A model should be as simple as it can be but no simpler

— Albert Einstein —

The COE model is a very simple and easily understood model. The crucial question is whether it is useful. But that depends on what your goal or potential use is. It is very useful as a way to assign blame when the goal is to limit the factors for blame, i.e., find one thing or person to blame for an adverse event (accident) and then get on with life. It is very useful for lawyers who are searching for something or someone other than their client to be blamed for a loss. It helps to direct our focus after accidents on blame. It is much less useful for learning from accidents and using the resulting understanding to prevent more accidents in the future.

The COE model is often used to deflect blame 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. In fact, the selection of events to include in the chain is completely arbitrary—we can easily include more events or delete some and still argue, correctly, that we have created the chain of events that led to the accident.

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 model at all. That helps us avoid the spotlight entirely. That’s usually easy to accomplish when only direct or simple relationships are iincluded 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 or the pilot-vehicle interface? And an argument is simple to make essentially says that since not everyone made a mistake when presented with those circumstances, those circumstances not a cause. For example, other pilots flew the 737 MAX in a flight before the Lion Air crash, and they were able to overcome the design flaws. Therefore, the design flaws cannot be the “cause” of the accident. What is being argued here is that only direct causes exist and are important, not indirect ones. 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 simply because it’s a lot easier for us to understand and to build agreement by 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 “low-level of control and low-on-the-totem-pole” person, such as a nurse or technician in a hospital or a maintenance worker or control room operator in a chemical plant.

After a while, it becomes established that pilots are to blame for most accidents because they always appear in the COE identified for an aircraft accident and are usually the focus of 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's not, of course, true 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 (recommendations) to prevent future accidents. There is not much we can do to eliminate pilots (and thus their contributions to accidents). Our only possibility is to substitute automation for humans, which simply shifts the spotlight to the engineers who create the automation. Automation probably will not eliminate accidents; it may actually contribute to human error (and all humans cannot be removed from systems). Besides, total automation is not feasible for any but the simplest conditions. So, 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.

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 cause of the crashes? That the design of MCAS had no impact on the losses? That the regulatory policies and practices also had no importance? Can we really explain the B737 MAX accidents with a simple chain of events, with the pilot actions highlighted 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.

It's time to "grow up" with respect to the model used to explain accidents. The COE events model is too simplistic and omits too many important causal factors. 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 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.

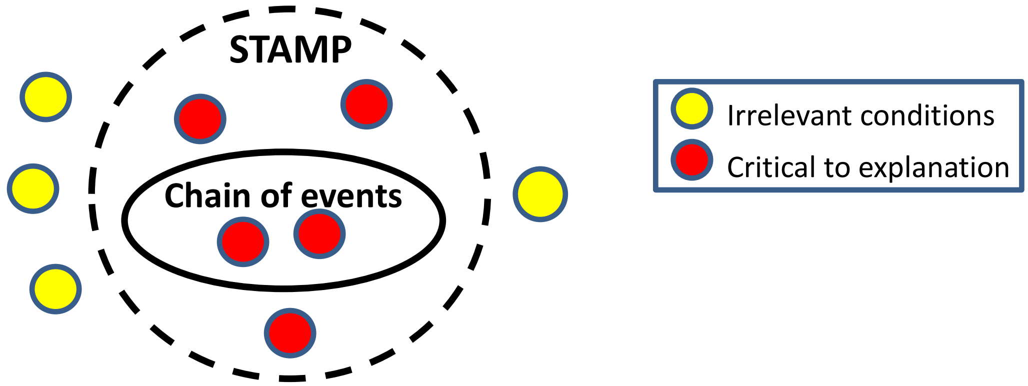
Is there something else we could use? I have suggested an alternative model that is based on systems theory. Systems theory was created about 60 years ago to deal more effectively with the types of complex systems we began creating after WW II.

My model is called STAMP (System-Theoretic Accident Model and Processes) and can be used, like the COE models (e.g., the domino, Swiss cheese, or bow-tie models), to explain the cause of accidents. It subsumes all the explanations provided by the COE model but provides a more comprehensive explanation for accidents.

STAMP starts from some basic assumptions:

- Events are not independent, as is assumed by the chain of events model. Multiple failures may have common influences, e.g., maintenance activities or the lack of them or creating maintenance facilities in third-world countries, which may in turn be influenced by competitive or financial pressures on a company.

- Events and behaviors may have subtle and indirect influences on each other. They also may 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 events model assumes that the events in the chain are independent and each event is only the direct result of the event(s) preceding it. Not only is this untrue in real life accidents, but which events are included in the chain is totally arbitrary.
- Accidents are not just caused by failures. The interactions among events are important in accident causation, not just the individual events themselves, which may include more than failures. 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, 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, which was perverted and altered over time by pressures on the company that have little to do with safety. It is this type of common process 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. Doesn't that provide as important a part of the causal explanation as "the pilot zigged when he/she should have zagged"?
- Accidents are the result of interactions among humans, physical things, established processes, social structures, and cultural factors. The events, and particularly the failure events, are only one small aspect of the cause. And it may be the least important in preventing future accidents.
- Accidents are a *control* problem. We need to control the interactions of the system components in order to prevent unsafe interactons. 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 events. They explain why the events occurred. These factors are not in the event chain.
- The COE model is a subset of STAMP. Everything in a COE model is included in STAMP.



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.

More about STAMP can be found in *Engineering a Safer World.*[2] There is an accident analysis method, called CAST (Causal Analysis based on System Theory), that can be used to more thoroughly investigate the cause of accident.[3]

Let's not let the response to these tragic losses be reduced to the usual legal wrangling and posturing as well as arguments about "root cause" using oversimplified causal models. We can't stop that from happening, unfortunately. But we <u>can</u>, as engineers, pilots, and users of these systems, insist on employing more sophisticated explanatory models to explain 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 safer systems for the future.

[2] You can download a free pdf version of this book from the MIT Press (the publisher) website. Just "google" the name of the book and the free copy comes up high on the list of results. Of course, you can also purchase a hard copy if you prefer.

[3] Nancy Leveson, CAST Handbook, to be available June 1, 2019.