THE ANSWERS HAVE CHANGED

The United Airlines Flight 173 crash in 1978 triggered an in-depth research of the recurring problem of a breakdown in cockpit management and teamwork when there is aircraft systems malfunction in flight. **Michael R. Grüninger** **and Capt. Andreas Grauer** **investigate safety solutions to these problems**

PAST
30 years ago, there were always two pilots, an engineer and a navigator in the cockpit.

Safety: The Question

Student: Dr. Einstein, aren't these the same questions as last year's physics final exam?

Dr. Einstein: Yes; but this year the answers are different.

The same applies to the question of safety.

How is safety achieved? This is the question. The answers change with maturity.

Traditionally, safety is regarded as the absence of accidents. In the meantime though, new answers are sought after by many safety practitioners and researchers.

One aircraft accident in particular has triggered well known answers to the safety question.

When at about 18:15 Pacific Standard Time on December 28, 1978, United Airlines Flight 173 crashed into a wooded, populated area of suburban Portland, Oregon, during an approach into Portland International Airport, it triggered an in-depth investigation.

Below, four approaches to finding a safety answer to this accident are presented.

Safety I Answer

Erik Hollnagel has introduced the term "Safety I" to indicate the traditional approach to safety and safety management as laid out by the ICAO SMS framework. Accidents are the end of a chain of events. Along the chain of events, each event is the cause for the one following.


United DC-8 crashes at E. Burnside, 157th; 10 killed, 175 survive

The Oregonian

Therefore, in the logic of Safety I, the standard answer states that safety is achieved by creating reliable components of a process or system. Since our standard model on safety instructs us to see safety as the result of the interaction of these components functioning without failures. As long as components and people are reliable, no accidents should occur.

In line with this logic, the investigators of the Flight 173 accident concluded that a "contributing factor to the accident was the failure of the copilot and flight engineer either to fully comprehend the criticality of the fuel state or to successfully communicate their concern to the captain."

The investigators dissected the accident into its components, such as weather, technical components, crew and so on. Then they analyzed each component to discover which one had actually failed and by failing caused the accident.

The Portland United Flight 173 accident sequence started with a green gear down indication light not illuminating after gear was selected down. The flight crew became concerned, forgot about the actual flying and spent such a long time analyzing the problem that eventually they ran out of fuel and crashed.

The cause of the accident was, ultimately, identified as a lack of communication between the flight crew members and their leader, the captain. The unreliable component was identified as the communication patterns of the flight crew.

Therefore, to prevent such an accident from happening again, communication between flight crew members had to be fixed. United Airlines pioneered the introduction of Cockpit Resource Management, later called Crew Resource Management, and such an accident should have never occurred again. However, similar accidents happened again.

Safety II Answer

Safety II, in contrast to Safety I, does not focus on linear causality and "Safety I: Avoiding That Things Go

Wrong". Safety II focuses on "Enforcing What Goes Right". While linear causality-based analytical models might work when studying mechanical systems, they do not when studying people. People do not either function or fail, but adapt to the situation. They do not function as a machine. Such adaptations are variable, often not repeated and often unique. Observable outcomes, such as the accident of United Flight 173, might be due to transient phenomena or conditions that existed at a particular point in time and space.

On the other hand, how many times was a gear light unserviceable and it did not result in an accident? Reaction patterns of humans are not always the same. One time the crew saves the day, the other time they fail to do so. As James Reason once put it: The pilot is the hazard and the pilot is the hero.

It is therefore not so obvious to see the 1978 investigators stating "the accident was the failure of the copilot and flight engineer (…) to (…) communicate their concern to the captain."

STAMP Answer

The aviation community has moved forward and it now understands that reliable components alone are not sufficient to achieve safety. Nancy Leveson, an MIT professor with considerable experience in aircraft and aerospace accident investigation, denies that reliability of components necessarily leads to safe outcomes. High reliability is neither necessary nor sufficient for safety. In fact, accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately.

Leveson reasons that the most basic concept in STAMP is not an accident, but a constraint. In systems theory, emergent properties, such as safety, arise from the interactions among the system components. The emergent properties are controlled by imposing constraints on the behavior of and interactions among the components. Safety then becomes a control problem where the goal of the control is to enforce the safety constraints.

On these insights and further reasoning, mainly increased complexity and coupling, Leveson developed a new approach, complementary to Safety I reasoning, to understanding accidents and designing safe systems. She called it System-Theoretic Accident Model and Processes (STAMP). Leveson points out that ways to analyze and prevent accidents must reflect the reality of today's complex socio-technical systems and not oversimplify the causes of accidents

Leveson observes that we do not seem to be making much progress lately in reducing accidents in most industries. Major accidents that seem preventable and that have similar systemic causes keep occurring. Too often, we fail to learn from the past and/or make inadequate changes in response to accidents. More generally Leveson asks, why don't the approaches we use to learn from events, most of which go back decades and have been incrementally improved over time, work well in today's world?

Safety I and Safety II approaches may work well in certain well defined cases. However, when the problem is not any longer the failure of a mechanical component or the emergence due to adaptive behavior of individuals, new descriptions of the problem must be found. Leveson subverts the assumption "Most accidents are caused by operator error and rewarding 'correct' behavior and punishing "incorrect" behavior will eliminate or reduce accidents significantly".

Traditionally, human or pilot error is often cited as the cause of an accident. The investigators of the 1978 United Flight 173 accident concluded also that the human, or rather the humans in this case, have erred by not communicating assertively enough their concern about the fuel situation to the captain. But, as a US Air Force study of aviation accidents states, the designation of human error, or pilot error, is a convenient classification for mishaps whose real cause is uncertain, complex or embarrassing to the organization.

Nancy Leveson concludes that traditional event-based accident and risk models are particularly poor at dealing with human error and decision-making. Human error is usually defined as any deviation from the performance of a specified or prescribed sequence of actions. However, instructions and written procedures are almost never followed exactly, as operators strive to become more efficient and productive and to deal with time and other pressures.

In studies of operators, even in such highly constrained and high-risk environments as nuclear power plants, modification of instructions is repeatedly observed and the violation of rules appears to be quite rational, given the actual workload and timing constraints under which the operators must do their job.

Work-as-done is most likely not identical to work-as-imagined.

'Safety Differently' Answer

"Safety Differently" has become an approach to safety which looks at it, as the name suggests, differently. The key principles of Safety Differently are: Safety is defined as the presence of positives, such as the capacity to be successful in varying conditions (as opposed to the absence of negatives); People are the solution (as opposed to the problem to control); and Safety is an ethical responsibility to those who do the organization's risky work (as opposed to safety being a bureaucratic accountability to those up the hierarchy).

While Safety Differently is not renegading Safety I, Safety II or STAMP, it puts the focus on assuming that even if we eliminate all negatives, such as accidents or component failures, success is not guaranteed. This is not necessarily true because of how people adapt to deal with complexity, which leads to both success and failure, as Ron Gantt stated. Eliminating the causes of failure will also eliminate the causes of success. Safety thus becomes an enabler, not a pull on the organization.

If safety is an ethical responsibility, safety should be oriented towards supporting workers, not towards meeting bureaucratic and regulatory requirements. Nobody works to create an accident. Workers want to be successful and safe. The organization should ask workers what they need instead of asking them why they are not following the rules.

In the context of the analysis of the United Flight 173 accident, the introduction of CRM might still have been a valid Safety Differently answer.

CRM did indeed give flight crews a space in which variability and team-oriented decision-making became possible. But when CRM itself degenerates to a bureaucratic exercise, a tick in the box of the training list, its benefits are diminished.

Michael R. Grüninger *is Managing Director of Great Circle Services (GCS) Safety Solutions and* ***Capt. Andreas Grauer*** *is the Deputy Managing Director of GCS. GCS assists in the whole range of planning and management issues, offering customized solutions to strengthen the position of a business in the aviation market. Its services include interim and start-up management, training and auditing (IS-BAO, IOSA, EASA), consultancy, manual development and process engineering. GCS can be reached at www.gcs-safety.com and +41-41 460 46 60. The column Safety Sense appears regularly in BART International since 2007.*