Safety-I and Safety-II: A White Paper on the Violations of Aviation Safety Management System Components

Research · June 2023

DOI: 10.13140/RG.2.2.36552.08962

CITATIONS
0

READS
476

1 author:

Brittany Glish
Embry-Riddle Aeronautical University
1 PUBLICATION **0** CITATIONS

SEE PROFILE

Safety-I and Safety-II: A White Paper on the Violations of Aviation Safety Management System Components.

Brittany Glish [a]

[a] Department of Aeronautics, College of Aviation, Aviation Safety and Human Factors, Embry-Riddle Aeronautical University, Daytona Beach, FL, 32114, USA, suncinb@my.erau.edu, https://orcid.org/0009-0003-4577-8174

Abstract

Modern aviation safety is saturated in Safety-I and Safety-II mindsets. When analyzing accidents or incidents, the typical focus of attention is based around analyzing human errors and human failures and many times, never thoroughly investigate process or system design. Many accident investigations are halted the moment it is discovered that a human violated procedure or made an error. In some accident investigations, the placement of blame is alleviated when an obvious manufacturer, mechanical, or other error is noticed. However, the old views of safety are designed to fail most people that are in any safety-sensitive in aviation role such as: pilots, mechanics, cargo loaders, or flight attendants. How organizations and regulators view safety and investigate accidents must shift from the Safety-I and Safety-II approaches - which violate all 4 components of aviation Safety Management Systems. Safety-III, provides a systems approach to safety, without the focus of human error or blame, and allows all 4 components of aviation Safety Management Systems to be incorporated when analyzing processes, systems, workflows, and accident investigations.

List of Acronyms

CAST – Causal Analysis Using Systems Theory

DFW – Dallas Fort Worth International Airport

MIT – Massachusetts Institute of Technology

NWS – National Weather Service

SMS – Safety Management Systems

STAMP – Systems Theoretical Accident Model and Processes

STPA – Systems Theoretical Process Analysis

WAI – Work-as-imagined

1. Safety Views

1.1. Safety-I

Safety-I is defined by Hollnagel as, "The system quality that is necessary and sufficient to ensure that the number of events that can be harmful to workers, the public, or the environment is acceptably low." [4]. Simply stated, safety is considered to be the prevention of errors and adverse effects. Adverse outcomes are things that go wrong. The explanation behind adverse events is when the assumed cause of the adverse event has been explained, contained, or eliminated [4].

A failure in Safety-I, is contributed to human error, which results in an unacceptable outcome. Hollnagel states that the starting point for safety management is that either something has gone wrong or that something has been identified as a risk [4]. Safety-I assumes that when work goes correctly, it is because people are doing the work as imagined. When things go wrong, it is because someone or something has failed [4]. Therefore, Safety-I assumes that the "Work-as-Imagined" (WAI) approach contributes to successful outcomes only. Under this mindset, the intent is to blame someone or something when and adverse event occurs. There is no ownership from an organization over faulty designed processes, software, or workflows. The Safety-I mindset also assumes that should any deviation from WAI occur, it will result in an unacceptable outcome. Countering the Safety-I approach is that deviation from processes happen in job roles every day without failures or accidents. Adaptive performance and variability are reflected based on the workers environment, duties, or responsibilities [3]. Eliminating variability based on the statement that WAI is the only correct approach assumes that everyone will perform the same task, the same way, every time. This assumption is inaccurately stated because people, places, and the environments in which work is performed change every day.

When a failure occurs – Safety-I tries to re-establish WAI [4]. The mindset behind Safety-I for an accident investigator only allows one outcome in an accident investigation: "not following procedures". Investigations in accidents labeled as "failure to follow procedure" usually stop the moment blame is placed and never usually identify, nor discover why the accident was caused. For example, on August 2nd, 1985, Delta Air Lines flight 191 crashed while on approach to runaway 17L at Dallas Fort Worth International Airport (DFW). While passing through rain and clouds directly underneath the thunderstorm, the aircraft entered a microburst, in which the pilots were unable to recover successfully. The aircraft struck the ground about 6,300 feet north of the approach of 17L at DFW. The aircraft hit a car on the highway and then struck two water tanks at the airport which caused the aircraft to break apart. Out of 163 passengers on board, 134 passengers and crew members were killed. There were 29 survivors [6]. The NTSB determined the cause of the accident:

"The flight crew's decisions to initiate and continue the approach into a cumulonimbus cloud which they observed to contain visible lightning."

However, the *actual* cause of the accident was that there were no clear procedures given to pilots during that time on how to avoid or escape windshear, which was admitted in the accident report. Further, the aircraft weather radar in the Lockheed L-1011 was not able to detect severe thunderstorms over a level 3, as categorized by the National Weather Service (NWS). The storm at DFW was a level 4 [6]. There was a clear lack of ownership and responsibility by the FAA, until Delta 191 crashed, considering there had been 25 accidents previously due to low level windshear from 1964-1975 [7].

1.2. Safety-II

Recently, Safety-II has gained traction over the last few decades as terms like "Resilience Engineering" have gained popularity [3]. Safety-II, arguably, is the same approach and methodology as Safety-I, except the focus is on what went right. As stated previously, Safety-I assumes that when work goes correctly, it is because people are performing WAI [4]. Safety-II is written to be read almost the exact same as Safety-I, in that the focus is on what went correctly. Hollnagel states that under Safety-II, failures should not be treated as unique, individual events, but are to be seen as an expression of performance variability [4]. The methodology under Safety-II cites performance variability as the direct cause of failures – another attempt to re-establish WAI, just as stated in Safety-I.

Safety-II is defined by Hollnagel as "Proactive, continuously trying to anticipate developments and events." [4]. However, Massachusetts Institute of Technology Professor, Nancy Leveson, counters this statement by stating, "the definition of "reactive" in the dictionary states, "Acting in response to a situation, rather than creating or controlling it"." Leveson further states that because the concept of Safety-II does not address hazards, it cannot be an accurate description of a proactive system [5].

Safety-II is arguably a reassembled version of Safety-I. The only difference is that Safety-I is worded to seem positive and proactive by focusing on what goes right. However, it does not account for the situations in which variability still produces the desired outcome. Safety-II, additionally, is human-focused in terms of failure. As Leveson states, Safety-II organizations assume that human operators are primary responsibility for safety, rather than the overall design of the environment and the system by the organization itself [5].

2. Violations of Aviation Safety Management System Components

2.1. Safety-I and Safety-II Violations

In aviation, a Safety Management System (SMS) is defined by the Federal Aviation Administration as:

"A formal, top-down, organization-wide approach to managing safety risk and assuring the effectiveness of safety risk controls. It includes systematic procedures practices, and policies for the management of safety risk. SMS is a structured process that obligates organizations to manage safety with the same level of priority that other core business processes are managed." [1].

The FAA defines the 4 functional components and the definitions of SMS as [2]:

- Safety policy
- Safety Risk Management
- Safety Assurance
- Safety promotion

The definitions of the 4 components of SMS, as stated per the FAA, arguably, violate all 4 components under Safety-I and Safety-II.

Safety Policy is defined as:

"The commitment from an organizations' senior management to improve safety. This commitment defines the processes, methods, and organizational structure needed to meet that goal [2]."

Under a Safety-I and Safety-II mindset for analyzing processes, accidents, or workflows, neither one demonstrates a defined process or method to meet the goal to improve safety. The only focus for Safety-I and Safety-II is that the single point of failure is contributed to human error, while reinforcing WAI is the only correct method to avoid adverse outcomes. Therefore, Safety-I and Safety-II violate this component of SMS.

Safety Promotion is defined as:

"The inclusion of training and communication that builds and creates a positive safety culture for all levels of the workforce [2]."

Approaching safety under Safety-I and Safety-II, a positive safety culture will arguably be challenging to obtain. The focus on blame and human error as the single cause of failure when analyzing adverse events contributes to a lack of safety reporting culture. In doing so, fear is created in employees to speak up when safety concerns are identified. Therefore, Safety-I and Safety-II violate this component of SMS.

Safety Assurance is defined as:

"The evaluation of the continued effectiveness of implemented risk control strategies, which supports the new identification of new hazards [2]."

Safety-I and Safety-II approaches to safety do not address hazards and can therefore, not be considered as a method used to implement risk control, nor support the identification of new hazards, because current system hazards are not analyzed. Therefore, Safety-I and Safety-II violate this component of SMS.

Safety Risk Management is defined as:

"The need and adequacy of new or revised risk controls, based on the assessment of acceptable risk [2]."

Because Safety-I and Safety-II do not address hazards, they cannot be used as a method of revising or assessing risk [5]. In safety, you cannot have a risk, without first classifying a hazard. Therefore, Safety-I and Safety-II violate this component of SMS.

3. Safety-III

Safety-III, known as Systems Theoretic Accident Model and Processes (STAMP), was created by Massachusetts Institute of Technology (MIT) professor, Dr. Nancy Leveson. STAMP is not a linear model nor does STAMP model losses as a chain of failure of events. STAMP is not an analysis method; it is a theoretical causality model based on systems theory. Systems theory was created after World War II when new technology and complexity began to arise in our engineered systems. Systems theory treats the system as a whole, not the sum of its parts [5]. There are multiple interactions to consider when analyzing complex, socio-technical systems, such as human-to-human interactions, human-to-system interactions, and system-to-system interactions. The interaction within these systems is incorporated in STAMP through the use of feedback loops to determine the impact of control actions and the controller's belief of the current system state [5].

There are two analysis methods built on STAMP, Systems Theoretic Process Analysis (STPA) and Causal Analysis using Systems Theory (CAST). STPA is the proactive hazard analysis used for the design, or re-

design of a new process or procedure. CAST is the reactive approach that is used to analyze an accident or loss to better improve the system, as a result of the loss [5].

To compare STAMP to the 4 components of SMS, Leveson states the following [5]:

Definition of Safety:

"The freedom from unacceptable losses as identified by stakeholders. The goal of STAMP is to eliminate, mitigate, or control hazards, which are the states that can lead to those losses."

Definition of Safety Management Principle:

"Concentrates on preventing hazards and losses; but learns from accidents, incidents, audits, of how the system is performing.

Accident Analysis:

"When analyzing accidents, the explanation is that accidents are caused by inadequate control over hazards."

Linear Causality:

"Linear causality is not assumed and there is no root cause, or single point of "failure". The entire socio-technical system must be designed to prevent hazards and the goal of the investigation is to determine why did the current system today, not prevent the loss."

Human Factors Principles:

"The system must first be designed so that human operators can be flexible, resilient, and handle unexpected events."

The Role of Performance Variability:

"To design the system so that performance variability is safe. Conflicts between productivity, achieving system goals, and safety are eliminated or minimized. System design should be so that when the performance of operators varies outside of safe boundaries, safety is still maintained."

3.1. Safety-lll compared to SMS

Comparing the definitions of STAMP to the 4 components of SMS, STAMP accurately demonstrates Safety Assurance by analyzing current system hazards to allow for continued effectiveness of implemented risk controls; and providing a model that supports the identification of new hazards [5].

STAMP accurately demonstrates Safety Risk Management by allowing the controlling of hazards as much as possible, which allow for controls of risk. The system is also designed under STAMP to be flexible and resilient to the operators [5].

STAMP accurately demonstrates Safety Promotion by not focusing on human error and removing blame. The safety culture, as stated by Leveson, is nurtured, and defined, with a carefully designed SMS structure [5].

STAMP accurately demonstrates Safety Policy by providing a framework and foundation that supports an organizational structure to overall improve safety from a defined method and process [5].

4. Conclusion

In conclusion, Safety-I and Safety-II approaches to safety violate the FAA's 4 components of SMS: Safety Policy, Safety Assurance, Safety Risk Management, and Safety Promotion. However, former views on Safety-I and Safety-II still exist today within many airlines, regulatory agencies, and organizations in the aviation industry. Safety-III supports the framework of SMS as defined by the FAA, and further provides structured methods for adequate analysis of investigations and incidents, as well as new process development or design.

References

[1] Federal Aviation Administration (FAA). (n.d.-c). Safety Management System (SMS). Safety Management System (SMS) | Federal Aviation Administration. https://www.faa.gov/about/initiatives/sms

[2] Federal Aviation Administration (FAA). (n.d.-b). Safety Management System. Safety Management System | Federal Aviation Administration. https://www.faa.gov/about/initiatives/sms/explained/components

[3] Ham, D.-H. (2020, December 2). Safety-II and Resilience Engineering in a Nutshell: An introductory guide to their concepts and methods.

[4] Hollnagel, E., Wears, R. L., & Braithwaite, J. (2015). From safety-I to safety-II: A White Paper. NHS England. https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-whte-papr.pdf

[5] Leveson, N. (2020, July 1). Safety lll: A Systems Approach to Safety and Resilience. MIT Engineering Systems Lab - Massachusetts Institute of Technology. http://sunnyday.mit.edu/safety-3.pdf

[6] NTSB. (1986, August 15). Aircraft accident report. https://www.ntsb.gov/investigations/AccidentReports/Reports/AAR8605.pdf

[7] Smith, M. (2010). Warnings the true story of how Science tamed the weather. Greenleaf Book Group Press.