Accident Investigations - Meeting the challenge of new technology

Established methods challenged by uncertain safety concepts and failure behaviour in new technology

Knut Rygh
kr@aibn.no
Chief engineer system safety
Accident Investigation Board Norway

Keywords: Safety, Accident investigation, Transport system, Digital system, STAMP, Barrier, Safety concept, Root causes, Safety constraints, Accident causation

Abstract New technology and new organisational concepts are being introduced at a pace that does not allow enough time to demonstrate control of possible residual risk by means of technical design and human performance. One area where this is becoming increasingly noticeable is the transport sector. Through identification of causal factors resulting from accident investigations, it may seem for digital systems that some transport sectors are facing challenges when ensuring documentation of safe operations. Operators and approval authorities are also facing a challenge in understanding the safe limitations and risk aspects involved when introducing new technology to transport systems The purpose of this paper is to demonstrate through lessons learned from accident investigations in the transport sector:

1) Why applied safety techniques to prevent accidents sometimes fail to show preventive effect in modern systems

2) Why a system for understanding the safety concept needed to investigate these transport systems has not been established.

It is becoming increasingly important to speed up the efforts to modernise techniques for accident prevention as these have been lagging behind the use of new technology in several sectors. Furthermore, this paper wishes to bring focus on the fact that the pace of introduction of digital automation systems to certain parts of modern transport systems during the last 15-20 years seems to have outstripped one's ability to assure and document safe operations. The fact that the safety of such systems cannot be assured in accordance with established and traditional methods and safety principles, combined with the fact that replacements are immature and unproven, calls for a more cautious and conservative approach with

regard to how this technology should be applied to safety- critical systems/operations.

1) Introduction

Innovation and new technology are found to provide a positive increase in wealth and way of living. The basis for accepting new technology into our lives lies in the fact that the risks are known and under control. Standards and established methods for engineering safety features into systems to prevent accidents are predominately based on handling failure of simple systems and physical components in chain or sequential events.

Digital technology has created a revolution in most fields of engineering, but system engineering and system safety engineering have not kept pace. One example among others is the introduction of a new safety system on board aeroplanes, Traffic Alert and Collision Avoidance System (TCAS), to give the pilot a warning and recommended action when two planes are on a collision course. This system operates isolated from air traffic controllers on the ground, which gives us two entities controlling the same airspace without communicating with each other. The extreme consequence of this was demonstrated in the Ueberlingen accident in Germany on 1st. July 2002 when a Tupolev TU 154M passenger aircraft had an in-flight collision with a Boeing B757-200 transport aircraft that resulted in 71 fatalities. The root cause, seen from a system perspective, was a severely deficient safety system where the airborne technical safety concept to avoid collisions did not correspond with the human ground-based air traffic controllers' collision avoidance system. (#1)

Digital systems introduce new "failure modes" that are changing the nature of accidents. Several approaches that worked on electromechanical components – such as replication of components to protect against individual component failure (i.e., redundancy) – are ineffective in controlling accidents that arise from the use of digital systems and software. Redundancy may even increase risk by adding complexity. (#2)

2) The safety concept – investigating the built-in safety features

Findings on the accident scene are usually a manifestation of a result that has its origin in systemic weakness and a failure, which symptoms ought to have been noticeable for some time. It is an accepted fact that a transport system's level of safety is determined by the safety concept for that transport system, which includes all safety features for prevention of any serious incident or an accident. It is also a proven fact that it is a weakness in one or more of these or the lack of safety features that allows an accident/incident to occur.

It is also an established practise, and therefore a continuing challenge for the accident investigation boards of the transport sectors, to document that