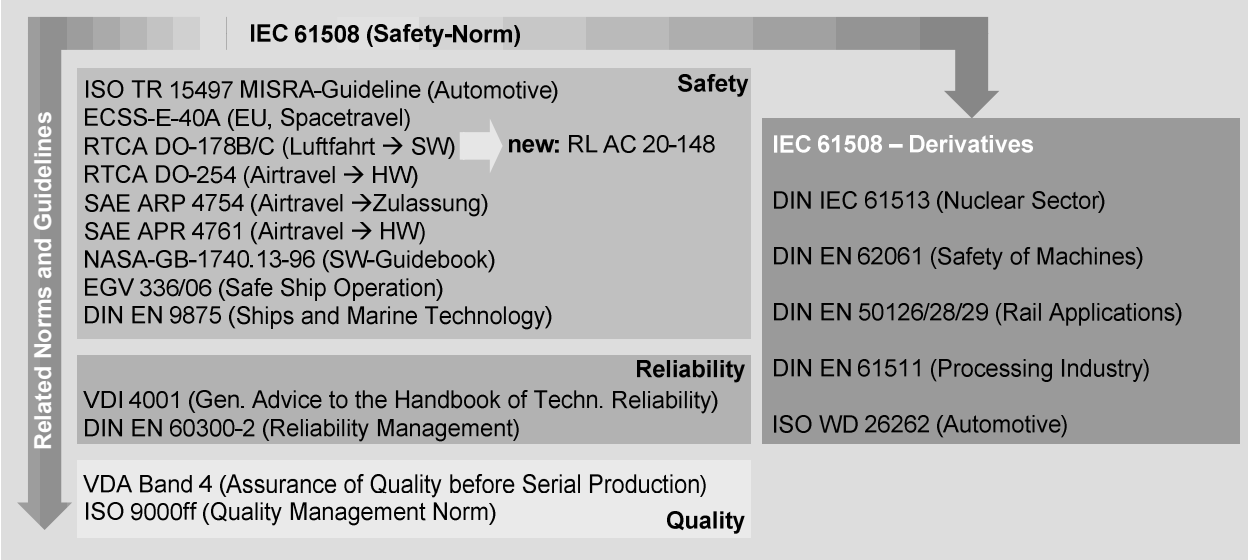
32. FISITA World Automotive Congress (14.-19.09.2008 in Munich)

Title of the paper	Safety Standards in Transportation Systems – Effort, Benefit and Challenges
Author	Dipl.-Ing. Tobias Ständer
Co-authors	Dr.-Ing. Uwe Becker Prof. Dr.-Ing. Dr. h.c. E. Schnieder
Contact Information	Institute for Traffic Safety and Automation Engineering (TU BS) Langer Kamp 8, 38106 Braunschweig phone 0531/391-7668 fax: 0531/391-5197 {t.staender | u.becker | e.schnieder}@tu-bs.de
Abstract (300-500 words)	see below
Relevant topic	International Standardisation (Electronics)
Keywords	Safety, Risk analysis, carrier, Standardisation, technical committee
Details of any previous papers published on the same subject	Becker, U. Ständer, T. *Derivate der Sicherheitsgrundnorm IEC 61508* TÜV-Tagung „Risikomanagement in der Automobilbranche 2006“, Stuttgart Becker, U., Ständer, T. *Eine vergleichende Betrachtung globaler Sicherheitsstandards für Verkehrssysteme* Auotomotive – Safety & Security 2006, Stuttgart Schnieder, E., Slovak, R., Wegele, S. *New and Conventional Measures for Quantifying Risk in Rail Transport* Journal of System Safety, 41(1) Jan./Feb. 2005 Schnieder, E. *Traffic safety and availability – Contradiction or attraction* In: Möhlenbrink, W.; Englmann F. C.; Friedrich, M.; Martin, U.; Hangleiter, U., Ed..: Proceedings of the 2nd International Symposium of Networks for Mobility - Fovus / Stuttgart, 2004 Schnieder, E. *Control for traffic safety – safety of traffic control* In: Tsugawa, S.; Aoki, M., Ed..: CTS 2003 - Preprints, S. 1-13, Tokyo, Japan, August 2003. 10th IFAC Symposium on Control in Transportation Systems/Tokyo, Japan

Abstract

The technical and economical relevance of safety and reliability in transportation systems - in all branches of transport - has long been increasing. This has partly been a result of the increasing number of systems critical to the assurance of safety in modern vehicles. According to current standards, a risk analysis must be conducted for every new transportation system before its employment can commence. The goal of this analysis is to identify and quantify all possible risks, or events that could potentially lead to dangerous situations, as related to the operation of the system. The degree of fulfillment of this safety standard must then be properly documented and kept as a proof of safety for the system.
This article compares the norms, standards and guidelines of various certification methods for manufactures and operators for air, rail and road transportation, and reveals existing weak points in their usability.



The most important norm in the extensive landscape of standards is surely still the IEC 61508. This very generally formulated norm describes the standards that electrical, electronic and programmable systems related to the safety of a transportation system are required to meet. Among the operations under the umbrella of this norm are today's transportation systems and their subsystems (i.e. driver assistance systems, etc.).
A comparison of the main transportation modes - roads, rails and air - clearly demonstrates that the degree of fulfillment of several parts of the standard depend heavily upon the varying intrinsic properties of the mode of transportation and thus should be viewed accordingly. Differing modes of transportation may therefore require more detailed, branch-specific norms in order to be properly assessed for certification.

Transportation mode	Air	Automotive	Rail
Movement	3D (Space)	2D (Plane)	1D (Line)
Pilot/Driver	i. g. 2 (Pro's)	1 (Amateur or Pro)	1 (Pro [+Integrated Safety System (Sifa)])
Weather	All, without Visibility	All, with Visibility	All, without Visibility
Operation Phases	Takeoff, Rise, Free Flight, Sink/Approach, Landing	City, Highway, Country, Parking	Train Station, Free Track
Lot size (in Europe)	10^3 (Tendency Falling)	10^6 (Tendency Rising)	10^3 (Tendency Falling)
Costs (Electronics)	ca. 10,000 €/kg	ca. 1,000 €/kg	ca. 1,600 €/kg (i.e. PZB 90; 25,000 €/15kg)
Frequency of Model Change	ca. 20 Years	ca. 2 Years	ca. 40 Years
Accident Investigation	Very extensive, but usually well documented	Less extensive	Very extensive, documentation improving
Maintenance, Repair	Only certified operations	Everyone	Small as well as large operations
Person-kilometers (2002 in Germany)	ca. 43 Billion/Year	ca. 76 Billion/Year	ca. 71 Billion/Year
Deaths (2002 in Germany)	ca. 120 Lives/Year	ca. 6,800 Lives/Year	ca. 200 Lives/Year

In light of this, various committees from the automotive and railroad industries are at work adopting the IEC 61508 in order to optimally regulate the certification process as concerning safety and risk analysis for their specific branch of the transportation sector.
The rail sector has, in the last few years, made a more or less large step in the direction of an industry-wide standardization of course of action with the formulation of the European CENELEC norm 5012x. Even though the EN 50126 norm addresses the rail industry and its suppliers with a method of consequently employing safety management, it is doubtful whether its usability is improved as compared with the IEC 61508, which builds its foundation.
Likewise, in the automotive industry there have been aspirations for some time to standardize safety-related hardware and software. In the mid 90's, for example, MISRA drafted development guidelines designed to facilitate the standardization of safe software in the automotive sector. Building on that, the FAKRA drafted an adapted version of the IEC 61508 for the automobile sector, in order to drive the standardization of safety-influencing activities. This draft (ISO/WD 26262) was presented to the ISO in November 2005 with the goal of standardization. […]
The purpose of the contribution is to give a clear and well structured overview on existing standards supporting the development of safety relevant transportation systems.