DESCRIPTION OF SAFETY MANAGEMENT SYSTEMS IN TRANSPORTATION

Tomáš Kertis, Dana Procházková

Czech Technical University in Prague, Faculty of transportation sciences;
Konviktska 20, 100 00 Praha 1, kertitom@fd.cvut.cz, prochazkova@fd.cvut.cz

Abstract: The work deals with analysis of different transportation domains in horizontal and vertical meaning. It looks for conformity in approaches and terms. It loans to concept of integral safety, i.e. a tool for ensuring the human security; it covers next engineering areas, for instance dependability management, functional safety, security of cyber-physical systems, technical and physical security, surveillance, occupational safety, safe place, human safety etc. Recent professional approaches of safety management and risk engineering are compared with current trends in transportation. It is clear that advanced professional procedures are needed for planned Smart Cities and Industry 4.0 in transportation domain practice; this work contribute to building the unified experts´ language from various transportation domains.

Key words: human security, integral safety, transportation system, system of systems, risk management, safety management.

1. Introduction

Each transportation mode has proper specifics in infrastructure, levels of management and in criticality in dependence on area characteristics and transportation goals. Therefore, the work deals with analysis of different transportation domains in horizontal and vertical levels. It looks for conformity in approaches and terms. The integral safety concept is used because it ensures human security and development. It also includes another engineering areas as the dependability management, the functional safety, the security of cyber-physical systems, the technical and physical security, the surveillance, the occupational safety, the safe place etc. Transportation systems in the context of various modes are denoted as systems of systems, cyber-physical systems related to informational technologies and socio-technical systems related to human aspects. A purpose of this work is also comparison of recent approaches of safety management and risk engineering, which improve the mentioned systems safety with current trends in transportation.

Safety is comprehended as the set of measures and activities, which are performed by humans owing to they ensure their security and sustainable development [1]. Because world dynamic development it is reality that safety management is the right tool. Therefore, we focus on safety, risks and criticality and their relations in transportation domains.

© 2017 Tomáš Kertis & Dana Procházková. This is an open access article licensed under the Creative Commons Attribution-NonCommercial-NoDerivs License (http://creativecommons.org/licenses/by-nc-nd/3.0/).
2. Human security and integral safety

The United Nations (UN) has defined the human security as a concept that means: “.. to protect the vital core of all human lives in ways that enhance human freedoms and human fulfilment. Human security means protecting fundamental freedoms – freedoms that are the essence of life. It means protecting people from critical (severe) and pervasive (widespread) threats and situations. It means using processes that build on people’s strengths and aspirations. It means creating political, social, environmental, economic, military and cultural systems that together give people the building blocks of survival, livelihood and dignity.” [2].

It mainly means to change the approach from only protection of State against enemy forces to the approach, which focuses on human lives and protection of people against all disasters. In accordance with UN [2], the common areas of human security and their threats are also the following items: economic security (persistent poverty, unemployment); food security (hunger, famine); health security (deadly infectious diseases, unsafe food, malnutrition, lack of access to basic health care); environmental security (environmental degradation, resource depletion, natural disasters, pollution); personal security (physical violence, crime, terrorism, domestic violence, child labour); community security (inter-ethnic, religious and other identity based tensions); political security (political repression, human rights abuses).

From the economy viewpoint the human security concept emphasises the needs on rehabilitation of transportation and traffic routes. The transportation is necessary for accomplishment of targets in particular domains of security. It could also be affected by inherent errors and weaknesses. It appears that transportation and the transportation system on one side are the most important for humans, and on the other side they are the sources of new threats as pollution, direct influence to human healthy and lives, and their property.

**Integral safety** is a complex tool for ensuring the human security. For aims reaching, it uses many techniques, methods and technologies. The famous tools are: reliability management; functional safety; security of cyber-physical systems; technical and physical protection; surveillance; guard; safe work procedures; safe place protection; human safety rules etc. The integral safety deals with more assets considered in system concept. It means that it considers the assets’ interactions, superordinate and subordinate systems, and activities in the system vicinity [1]. Integral safety management is based on integral risk management.

**The integral safety improving** is based on the process and project management principles, the target of which is the continuous improving the quality, i.e. the building-up or at least preservation of certain rate of system safety at the dynamically changing conditions of real world (surrounding physical conditions, linkages with next systems, change of culture and manner of persons or groups of people etc.). In the Middle Europe conditions, the project management of Total Quality Management (TQM) type is used for reaching the mentioned aims [3, 4]. The ISO standards (such as 9000, 1400) were created for the TQM successfulness. The TQM approach lies on the requirement that in the process of quality improvement, i.e. in the process of increasing the integral safety, in which there are participated all employees, from ordinary ones up to top management. The TQM also involves the principles and the attitudes for management of soft socio-technical systems, with simple idealized targets, so these might be understandable to the personal, respectively, also to the citizens in the considered area [3]. From the view of safety, the TQM introduces the Total Safety Systems (TSS), which have three basic elements [3,4]:

1. Safety of workplace (plant layout; environmental control – noise and other emissions; emergency procedures; firefighting arrangements; first aid facilities; lighting, rest-room and other facilities).
2. Safety of processes (physical guarding; electro-mechanical emergency stops; fail-safe systems; perimeter fencing).
3. Safety of human resources (safety training, personal protective equipment, supervision, medical checks).

The set of requirements in the TQM and the TSS significantly exceeds the Europe and national legislation requirements. Main prerequisite for improving the safety it is the risk reduction based on introducing the proactive programme with the continual measuring and elimination of so-called near-misses. The near-misses are the observed events, which finished without losses owing to certain random conditions, i.e. either the operator intervention or the fortunate coincidence of conditions (without them it leads to an incident or an accident) [1, 3].

**The safety management systems** are the systems of process and project management based on the mentioned TQM principles. The safety management systems are possible to divide into three categories [3, 4]:

- vertical one – problem solution level: political; strategic; tactical; operative; and technical,
- horizontal one - problem solution domain: mode of transport; type of infrastructure; nature of the system under consideration; other domains,
- conditions of operation - criticality level: normal conditions (concentration to prevention); abnormal conditions (vigilance, readiness); critical conditions (response and recovery).

So the safety management system might be effective, it shall be introduced in all mentioned levels and domains. For illustration, we give an example of safety management system that considers three levels of criticality of entity that is affected by disaster with different size.

In the model on Figure 1 it is shown the top level management on strategic level that on the outcomes from the risk management process establishes the requirements and criteria for the safety management on lower levels, i.e. in selected critical entities and areas. On the entity level there are applied the safety management systems on the basis of knowledge from lower levels of problem solution, i.e. there are established the plans for management of safety with measures, which are implemented within appropriate level of safety management system in the Defence-In-Depth approach [5]. The feedback to the top management is in the form of monitoring and continual assessment and improving, for which it is necessary inter sectoral communication through various fields [3, 6], is also shown there.

Present trends in the area of safety science and risk engineering are based on the above mentioned principles, namely with considering the system complexity that follows from the nature, properties and uncertainties of socio-technical and cyber-physical systems [1, 3, 6, 7].
3. Relation among safety, risks and criticality

Term of safety has various meanings in the present practice. Safety in transportation systems is related to: human protection without considering connections with a system; system resiliency against disruption of any adverse event (disaster), or against internal errors. Safety related to protection systems is meant as so-called functional safety, i.e. execution of any function or process in the case of desired situation [8]. Indeed, these conceptions have common base, i.e. to protect human health and lives and to ensure human society development. It means that the integral safety involves all mentioned meanings and it merges them into one concept. In the integral safety concept, the system safety means that the systems are protected against internal and external disasters including the human factor, i.e. the system has sufficient resiliency and adaptability against desired conditions. Moreover, the system shall not endanger its surrounding nor under own critical conditions, Figure 2 [9, 10]. Possible impacts, which are shown in Figure 2, are reflected as disasters for other systems in their surroundings. In this case, the cascade effects of disasters can origin. Each real system is complex system of systems with certain rate of complexity [8]. Therefore, ensuring the complex system safety is difficult process that involves sub-processes for: assets identification, assets criticalities determination, reduction of main risks, the most important assets protection, managing the relevant risks, coping with risks, etc.
The concept targeted to safety, i.e. increasing the human security and other public assets on which people depend, has higher goal than just reduction of risk, is shown in Figure 3. Safety and risk are somehow related each other, but they are not complementary variables (complementary variable to safety is for instance criticality) [1, 11].

Term risk has different and ambiguous meaning in many areas. Some definitions of risk are built on probability, other ones on inconvenient value, uncertainty and indeterminacy [12]. In terms of project management and system management, the risk has been defined as “an effect of uncertainty on objectives” [13]. The effect of uncertainty can have negative but also positive behaviour when it is realized [13]. In engineering domains such as risk management of systems, reliability management and management of risk related to safety, the term risk expresses the probable size of adverse / unacceptable impacts (losses, damage or harm) of disaster with size of hazard (i.e. normatively determined disaster size) normed to time unit and area unit [12].

Sources of risks are: natural phenomena, man-made technologies, huge human interventions to environment, adverse events and conflicts in human society. It means risks for people, their property, environment, critical infrastructure and last but not least for the State. Risks can be sorted according to which assets are considered for risk assessment and whether one assets, set of assets, or set of assets and interdependences are considered (i.e. particular, integrated or integral risks). Risks are then sorted according to which disasters resp. sources of disasters are considered (whether just some disasters, part of their scenarios or all relevant disasters etc.). In practice, in transportation systems, particular or integrated risks are considered. They are mostly expressed as product of probability of disaster (resp. incident) occurrence, or frequency of occurrence and its impacts (losses, damage, harm) related to the entity or selected set of entities under consideration.

Variables for risk calculation might be so many in the observed area, but most of them are product of both mentioned above. In most cases, it is the third component, e.g. assets’
vulnerabilities (e.g. in the automotive field). We can observe a lot of differences in the understanding risk. It is common that risk follows from fear of an uncertain feature [12]. For ensuring safe area, respectively bigger technological areas or facilities, there is necessary to calculate with comprehensive risk, i.e. integral risk based on system conception of reality [1].

The total entity integral risk is connected with more protected assets including the human life, health and security, their property, welfare, environment, technologies and infrastructures. It also includes the influences of interdependences among the mentioned protected assets [12, 14]. For all disasters in an area, the integral risk R is expressed by the following relationship [12]:

\[
R = \sum_{k=1}^{m} R_k
\]

where \( R_k \) is the risk related to \( k^{th} \) disaster:

\[
R_k = \sum_{i=1}^{n} P_k \cdot D_{i,k}.
\]

where \( P_k \) expresses the occurrence probability of \( k^{th} \) disaster, \( D_{i,k} \) expresses the impact of \( k^{th} \) disaster on the protected asset. Such relationships are also valid for the integral risk, but in the integral risk context \( D_{i,k} \) includes both, the direct \( DD_{i,k} \) and indirect impacts \( Di_{i,k} \) (secondary, tertiary and more), according to [12] their relationships are following:

\[
\begin{align*}
DD_{i,k} &= \int_S Z_{i,k} \cdot V_i \, dS; \\
Di_{i,k} &= \int_S I_{i,k} \cdot V_i \, dS
\end{align*}
\]

here \( V_i \) is value of the protected asset; \( S \) is the observed area or object; \( Z_{i,k} \) is vulnerability of \( i^{th} \) protected asset in case of \( k^{th} \) disaster; \( I_{i,k} \) is function of interdependences. The interdependences depend on appropriate structure of the protected assets in the observed area, it then depends on appropriate interconnections among the protected assets and on the disaster, i.e. according to [12]:

\[
I_{i,k} = f(u(VD_k, VP_{i,k}))
\]

\( VD_k \) is rate’s characteristic of \( k^{th} \) disaster that influences impacts on the protected assets. \( VP_{i,k} \) is rate’s characteristic of interconnections among the protected assets in the observed area. Establishment of \( VP_{i,k} \) is purpose of detailed research based on Boolean logics or it is based on methods of the operational analysis [10, 12].

Mentioned knowledge above and regarding the system complexity appear that integral safety can be improved only with consideration and management of integral risks, which enhance the sum of the parts (particular risks) with consideration of their interconnections and flows. As it has been mentioned above, although safety and the risk are related each other, they are not complementary quantities. For safety the complementary quantity is the criticality. The criticality is the threshold value that is complementary to the safety, i.e. higher criticality rate means lesser safety rate. Decreasing the criticality means improving the safety of observed entity. For safety management reasons, the asset criticality is understood as the result of scoring the asset importance and the asset vulnerability [15]:
Criticality of asset to certain disaster is expressed by the relationship:

\[ C = S \times O \times B, \]

where \( S \) is the highest disaster impact severity, \( O \) is the event occurrence probability and \( B \) is the conditional probability that the most severe impact is occurred [11].

4. Safety management systems in transportation domain

Safety management systems in the transportation domain are particularly defined by European guidelines and then by appropriate national legislative. The legislative is divided for each mode of transportation domain and it is mostly brief or unclear, because they are too much generic or they consider only particular risks.

In industrial domains and in terms of safety management, especially quality management systems based on process and project management (TQM) has been introduced including the processes of risk analysis, respectively it is based on standard ISO 9001 [16] enhanced with requirements on quality and safety of products in the domain.

For electrical, electronic and programmable devices (E/E/PE) in industry domain, international standard IEC 61508 [17] on functional safety has been introduced. Mentioned approaches and standards of management systems are then refined and enhanced with specific standards described in following paragraphs for each appropriate industrial domain.

Only very short group of subjects are assigned to critical infrastructure. In this case the subject need to introduce at least basis principles of crisis management and it has duty to create plans of crisis readiness based on crisis plan of related area (municipality).

Part of safety management systems also includes the information security management system and tasks of cyber security. Process of information security ensuring is based on protection of important assets of cyber (information) system by the way that the required level of Confidentiality, Integrity and Availability (CIA) might be ensured for important information [18]. In information technologies the CIA according to [18] means: information is not available or cannot be revealed by unauthorized individuals, entities or processes (Confidentiality); property describing the accuracy and completeness (Integrity); accessibility and usability of information on the request of authorized entities (Availability) [19]. Just some subjects have duty to introduce the information security management system, such as subjects which are selected by owners or operators of critical informational infrastructures or operators of critical infrastructures.

Above mentioned facts imply the claim that current transportation systems are mainly secured in terms of functional safety, but the fact is not considered there that inconvenient events over designed size can occur, i.e. cyber-attack or other disasters can lead the system under consideration into abnormal and critical conditions, which severe endanger its surrounding, see Figure 2.

In automotive resp. road transportation, no legislative demands on introducing comprehensive safety management systems are defined. For improving safety, particular technical and organizational requirements are established. Automotive industry introduces quality management system based on standard ISO/TS 16949 [20] or it applies German quality standard for automotive industry VDA [21]. In terms of E/E/PE the management requirements are then extended with standard ISO 26262 [22] on functional safety. The
standard is based on mentioned industrial standard on E/E/PE functional safety [17] but it has different approach to establishment of function criticality, it is described below.

The automotive industry is focused on mass production. It needs high rate or modularity, i.e. usability vehicle components for more different car models in different configuration. Owing to space saving, arrangement of the components and their relationships, it is not always possible to make up separated units executing safety functions. Therefore, the safety related (protection) functions are integrated into parts that execute more diverse functions. It is not widely admitted in other domains, because there is needed to demonstrate functional independences of functions with different safety integrity levels. Such systems are so-called systems with integrated safety, whereupon external safety (protection) systems are preferred in other domains. The mentioned approach of integrated safety is also applicable in case where it is not possible to implement the system inherent safety by external system parts, there it is needed to ensure safety of the control system [23].

Some producers focus on implementation of integral safety related to human security in the car, indeed it means the implementation more of security tools. Hereby, the term of integrated and integral safety in the automotive industry has different meaning than terms given above. Unlike functional safety in other domains, in the automotive industry another concept of risk and safety integrity levels (ASIL according to ISO 26262 [22]) are introduced. At the automotive industry, the safety integrity levels are derived by size of risk defined as:

\[ R = \text{severity} \times \text{exposure} \times \text{controllability}. \]

The Table 1 shows the derivation of special quantity ASIL. In Table 1 the following quantities are given: \( S \) means severity, \( E \) is exposure and \( C \) controllability. ASIL takes values A, B, C, D; the A denotes the smallest value and the D the biggest one. Higher ASIL value means the implementation of more protection measures within whole system life cycle. Value QM means that the safety is only ensured by standard techniques of quality management, i.e. no additional protection measures.

Table 1. ASIL determination from risks according to ISO 26262 [22].

<table>
<thead>
<tr>
<th>ASIL TABLE</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>E1</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>QM</td>
<td>A</td>
</tr>
<tr>
<td>S2</td>
<td>E1</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>QM</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>S3</td>
<td>E1</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>B</td>
<td>C</td>
</tr>
</tbody>
</table>

From the Table 1, it follows that the given approach is focused on safety control system. According to the system criticality, it is assigned into different levels, i.e. QM, ASIL A up to D. On the basis of these levels, the appropriate safety measures are applied within whole system life cycle.

strict documentation, assessment and justification it terms of safety influencing factors according to the CSM, i.e. risk management methods. Any rail operator is obliged to introduce the safety management system with considering the normal and abnormal conditions. Indeed, it does not consider the critical conditions according to the principles described in previous parts. The railway accidents shall be announced to national The Rail Safety Inspection that investigates accidents and proposes safety measures.

The system safety in the railway industry domain is based on high rate of quality assurance, i.e. standard IRIS that applies requirements on the system life cycle in accordance with EN 50126 [26]. Each change (i.e. technical, organizational and change in management system) in the railway system then subjects to risk evaluation, whether the change affects safety or not, outcomes of the evaluation serves to design of appropriate measures. Standard EN 50126 [26] defines railway system life cycle including the determination and demonstration RAMS (Reliability, Availability, Maintainability and Safety) properties and the life cycle costs (LCC) that take into consideration also the system operation, maintenance, renewal up to disposal.

The RAMS properties apply the system approach that divides the system into several layers. Each of such layer contains own functional subsystems, and on the basis of risk analysis it assigns the functions and safety functions. In terms of the railway domain, the risk is expressed by relationship:

\[ \text{Risk} = \text{frequency} \times \text{consequence}. \]

The risk mitigation is performed by ALARP / ALARA approaches [26]. Functions, the malfunctions of which, have severe impacts, or functions that mitigate the analysed risks are called the safety related functions. The safety related functions have assigned the safety integrity levels (SIL) from 1 up to 4 determined according to the tolerable hazard rate (THR), Table 2.

For the safety related functions the protection measures are applied, which are similar to measures recommended by the industrial standard EN 61508 [17]. The protection measures are expressed by requirements focused on HW (hardware) according to EN 50129 [27] or SW according to EN 50128 [28]. There are also requirements for the safety case elaboration. The safety integrity level 0 is used for SW (software) in the rail domain that is not related to safety, but minimal requirements for quality assurance are established.

Table2. Relationship of THR to safety integrity level according to EN 50129 [27].

<table>
<thead>
<tr>
<th>Tolerable Hazard Rate (THR) per hour, related to system function</th>
<th>Safety Integrity Level (SIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(10^{-9} \leq \text{THR} &lt; 10^{-8})</td>
<td>4</td>
</tr>
<tr>
<td>(10^{-8} \leq \text{THR} &lt; 10^{-7})</td>
<td>3</td>
</tr>
<tr>
<td>(10^{-7} \leq \text{THR} &lt; 10^{-6})</td>
<td>2</td>
</tr>
<tr>
<td>(10^{-6} \leq \text{THR} &lt; 10^{-5})</td>
<td>1</td>
</tr>
</tbody>
</table>

Avionic transportation is regulated by national law on civil aviation [29] that does not directly oblige all subject to introduce safety management systems. It imposes partial technical and organizational measures that can be implemented into the safety management system, but they are not making up the uniform system. Selected subjects, such as operators of aero ports or aviation facilities, persons entrusted with operation of air services, operators of air activities and other related to civil aviation, they are obligated to follow international regulations and guidelines of ICAO, Joint Aviation Authorities (JAA), European Aviation...
Safety Agency (EASA), i.e. Joint Avionic Requirements (JAR) and Parts, and Eurocontrol. The integrated safety management system is defined by International Civil Aviation Organization (ICAO) Annex 19 [30]. The regulation imposes the obligation to introduce safety management system to selected subjects [30]. Document Doc 9859 Safety Management Manual [31] then refine these requirements.

In comparison with other industrial and transportation domains, the Safety Management System (SMS) is the most expanded just in avionic domain. In avionic as well as in the railway domain, the SMS is based on TQM principles described above. Moreover, the system admits not only technical issues, but also human behaviour issues (human factor) and organizational faults (it admits organizational accidents). It is then based on building the safety culture. It attributes the potential accident to three factors: organization (management decision making and organizational processes); workplaces (working conditions); human being (human errors and disruptions); and protection (guidelines, training, technologies).

The mentioned order of factors is so-called the latent conditions trajectory for the accident occurrence, see Figure 4.

![Fig. 4. The concept of accident causation [31].](image)

The document [31] recommends to integrate the SMS into integrated management system that is more flexible for adjustment of guidance with more systems such as the quality management system (QMS), the Environmental Management System (EMS), the Occupational Health and Safety Management System (OHSMS) or the security management system (SeMS) that is also important in terms of integral safety. In terms of avionic, the SMS requirements are provided by ICAO Annex 17 on Security: Safeguarding International Civil Aviation Against Acts of Unlawful [30]. Unlike the ICAO Annex targeted to ensuring quality of security measures (focused on people, places, means of transport, cyberspace) and prevention against acts of unlawful, the coherent SeMS emphasizes the hazard and risk identification, their evaluation, prevention, and preparation of emergency and crisis plans [30].

Avionic industry, as well as automotive and railway industry, for electronic systems development apply inherent line of standards that ensures functional safety and security using life cycle from early development phases. The avionic industry applies standards mentioned above. Like the automotive domain, it focuses more on ensuring safe control system. Mostly, mainly when the aircraft is in air, it is not feasible to enforce approach of inherent safety, therefore it is not widely used.
The avionic standards do not define safety integrity levels, but they are focused on hazard level. According to the hazard level it establishes acceptable failure rate and Design Assurance Level (DAL) in case of software, Table 3. DAL is used for software according to DO-178 [33] to eliminate developers’ system errors in design, DAL E applies the least measures and DAL A applies the most measures.

Table 3. Safety assurance in the avionic industry according to [32, 33, 34].

<table>
<thead>
<tr>
<th>Hazard level</th>
<th>Failure rate</th>
<th>Design Assurance Level DAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>$10^{-9}$ per hour</td>
<td>A</td>
</tr>
<tr>
<td>Hazardous</td>
<td>$10^{-7}$ per hour</td>
<td>B</td>
</tr>
<tr>
<td>Major</td>
<td>$10^{-5}$ per hour</td>
<td>C</td>
</tr>
<tr>
<td>Minor</td>
<td>$10^{-3}$ per hour</td>
<td>D</td>
</tr>
<tr>
<td>No effect</td>
<td></td>
<td>E</td>
</tr>
</tbody>
</table>

5. Conclusion

The work provides overview of safety management and risk management issues from both, general layer and with focusing on three the most important transportation modes and their comparison. Recent professional approaches of safety management and risk engineering are compared with current trends in transportation. It is clear that advanced professional procedures based on integral risk management targeted to transportation safety are needed for planned Smart Cities and Industry 4.0 in transportation domain practice; this work contribute to building the unified experts’ language from various transportation domains.

Acknowledgement

Authors thanks to Czech Technical University in Prague for support (grant SGS2015-17).

References


[21] VDA. Qualitäts Management Center im Verband der Automobilindustrie e.V. Berlin, online: http://vda-qmc.de


[33] RTCA. DO-178C Software Considerations in Airborne Systems and Equipment Certification. RTCA 2011