Механика Транспорт Комуникации

Научно списание

ISSN 1312-3823

том 11, брой 3, 2013 г.

статия № 0788

http://www.mtc-aj.com

ВЪЗ ОСНОВА НА КОИ КРИТЕРИИ ПРИЕМАМЕ РИСКОВЕТЕ В ОБЛАСТТА НА ТРАНСПОРТА

Мария Антова
mantova@gmail.com

БЪЛГАРИЯ

Ключови думи: *безопасност, управление, оценка и критерии за приемливост на риска, транспорт*

Резюме*: Транспортът е многофакторна отворена система, която е изложена на множество вътрешни и външни рискове с различен вид и произход (технически, организационен, човешки, природен и т.н.). Видът на рисковете често е фактор, който играе голяма роля в решението за това как да оценим риска и в преценката ни за това кога той е приемлив за нас. От друга страна, историческото развитие на различните видове транспорт в техническо, организационно и географско отношение също е важен фактор, допринасящ за разнообразните практики по отношение на управлението и оценката на рисковете. Затова ролята на международно приети закони и стандарти, съдържащи изисквания за оценката и приемливостта на риска, е изключително важна. Такива документи са например семейството от международни стандарти IEC 61508, ARP 4754/ED 79, DO-178/ED 12B, DO-254/ED 80, ISO 26262, а така също и други международни стандарти и документи.*

Тази статия има за цел да представи кратък преглед на съвременните практики в някои видове транспорт по отношение на критериите за приемливост на риска. Понастоящем в международен план много от аспектите свързани с тези критерии все още нямат решение. От гледната точка на автора тази статия има за цел представи кратък обективен обзор, който да допринесе за дискусиите и да провокира по-нататъшни разговори, анализи и научна дейност по дадената тема.

1. УВОД

Дефинирането на критерии за приемливост на риска е задача трудна сама по себе си във всяка област на човешкия живот. Личният опит на автора в областта на дефинирането и хармонизирането на международно ниво на критерии за приемливост на риска мотивират тезата на автора, че е в общ интерес възможно повече актьори да разбират добре принципите на дадения проблем и да имат желание и достатъчно познания да дискутират върху него, да извършват научна дейност по него и така да достигат до общи критерии за приемливост на риска – тема, която е особено актуална в железопътния транспорт. Настоящата статия представя кратък преглед на критерии за приемливост на риска, които съществуват в различните сфери на транспорта.

2. ДЕФИНИЦИИ

За да разберем достатъчно добре разглежданата тема, то е нужно да започнем с дефинициите. Нужно е да споменем, че поради различното историческо развитие, а така също и поради различните нужди, то често различните транспортни сфери работят с различни дефиниции. В рамките на тази статия, авторът смята, че дефинициите, използвани в железопътния транспорт са удобни за постигане на целите.

- **"Риск"** означава комбинацията на честотата на възникване на произшествия и инциденти, водещи до нежелани последици (причинени от дадена опасност) и степента на тежест на тези нежелани последици;
- **"Критерии за приемливост на риска"** са отправните точки за сравнение (забележка на автора: "the terms of reference"), с помощта на които се оценява приемливостта на конкретен риск; тези критерии се използват за определяне дали нивото на риска е достатъчно ниско, за да не е необходимо да се предприемат непосредствени действия за допълнителното му намаляване.

Основата на тези дефиниции може да бъде намерена в Европейския регламент за оценка на риска в областта на железопътния транспорт 352/2009/ЕО [1], а така също и в неговото изменение от 2012 година [1]. Те не отговарят съвсем точно на българския превод на регламента, защото автора смята, че българският превод е неточен.

Важно е да отбележим, че дефиницията на понятието „риск" не се отнася до произведението, сумата, или някакъв друг вид математическа формула, на двете компоненти на риска – честотата на възникване и тежестта на последиците – а се отнася до тяхната „комбинация". В такъв смисъл, комбинацията може да бъде и произведение, и сума, и някакъв друг вид формула. За целите на тази статия, точната формула не е от значение.

Също така полезно е да отбележим колко обща и „конвенционална" е дефиницията на понятието „критерий за приемливост на риска". Някои актьори смятат дефиницията за твърде обща и объркваща. Авторът смята, че дефиницията е изключително подходяща, тъй като е точно толкова описателна, колкото е нужно за да бъде изразена същността на понятието, а едновременно с това е и достатъчно обща, за да може да се отнася до критериите за приемливост на различни видове риск, които по същността си са също толкова разнообразни по вид, както и самите видове риск.

3. КАКВИ КРИТЕРИИ ЗА ПРИЕМЛИВОСТ НА РИСКА СЪЩЕСТВУВАТ В РАЗЛИЧНИТЕ ВИДОВЕ ТРАНСПОРТ?

Видът на критериите за приемливост на риска е често свързан с вида на риска, който е оценяван. В днешни дни, в областта на транспорта, ярко се открояват два главни вида рискове и критерии за тяхната приемливост:

1. Рискове и критерии, които са свързани с производствения процес на техническите системи.
2. Всички други рискове и критерии, които възникват в областта на транспорта извън областта на производството на техническите системи.

В тази статия ще се съсредоточим върху критериите свързани с производствения процес. Тези критерии са свързани с класифицирането на рисковете в различни категории (SIL, ASIL, DAL и т.н.). В последствие тези категории се свързват с различни мерки за контрол на риска, които са изразени в изисквания към процеса използван за проектирането, разработката и производството на системите. Така, в общия случай, производната съвкупност от изискванията за мерки и процеси за контрол на риска и от

категориите, в които рисковете попадат, представлява критериите за приемливост на риска.

В следващите точки накратко ще опишем по-ярко открояващите се критерии за приемливост на риска, които са свързани с производствения процес на техническите системи в различните видове транспорт. Поради ограничената рамка на тази статия, описанието е кратко, без да влиза в детайли свързани с начините, по които се определят и извеждат съответните критерии, а така също и без детайли свързани със съответните мерки и изисквания към съответния производствен процес. Тази статия няма за цел да бъде изчерпателна по отношение на всички съществуващи критерии.

4. КРИТЕРИИ СВЪРЗАНИ С ПРОИЗВОДСТВЕНИЯ ПРОЦЕС В АВИАЦИЯТА

В производствените процеси на авиацията има различни изисквания и критерии според вида на разглежданата техническа система. Най-общо, изискванията и критериите са различни според това дали те са свързани с дизайна на самолети, или са свързани с дизайна на системата за управление на въздушния трафик [2]. Не е възможно в рамките на тази кратка статия да бъдат описани в детайл и двата вида критерии, затова тук ще се съсредоточим върху критериите свързани с дизайна на самолетите.

Тези критерии, и изискванията за тяхното извеждане са описани в ARP 4754A/ED 79 [2]. ARP 4754A е ревизия А на ръководството, което описва процеса на разработка, свързан със сертифицирането на цивилни самолетни системи (Civil Aircraft Systems). Ръководството съдържа секция, която описва процеса за определяне на нивата за осигуряване на разработката (DAL - Development Assurance Level). Тези нива определят мерките за контрол на рисковете свързани със сложни хардуерни и софтуерни разработки, а така също и дейностите по тяхната верификация. ARP 4754A се използва заедно с ARP 4761 [4] - ръководството, свързано с процеса на оценка на безопасността на цивилни летателни системи и оборудване - и е подкрепяно от други два важни стандарта в авиацията - RTCA DO-178B [5] и DO-254 [6] - които се отнасят до изискванията свързани с разработката съответно на софтуера и на хардуера.

Връзката между тежестта на функционалните условия за отказ (functional failure conditions), количественото изискване за безопасност за функцията и нивото за осигуряване на разработката (DAL) е показана в **Таблица 1**. Тя е описана в ARP 4754.

Таблица 1

Failure condition class	Quantitative safety requirement for the probability (failures/h)	DAL (Development Assurance Level)
Catastrophic	$< 10^{-8}$	A
Hazardous	$< 10^{-7}$	B
Major	$< 10^{-5}$	C
Minor	None	D
No safety effect	None	E

Процесът на оценка и използване на тези критерии е сложен. Той е свързан с различни компоненти като FDAL (Functional DAL), IDAL (Item DAL) и т.н. Въпреки това, в голяма степен, по същността си той би могъл да бъде сравняван с процесите, използвани в другите видове транспорт и най-вече железопътния.

5. КРИТЕРИИ СВЪРЗАНИ С ПРОИЗВОДСТВЕНИЯ ПРОЦЕС В АВТОМОБИЛНИЯ ТРАНСПОРТ

Критериите, които са свързани с производствения процес на техническите системи в автомобилната индустрия, могат да бъдат намерени в част 5, анекс G на ISO 26262 [7]. Кратко описание на тези критерии е поместено в **Таблица 2**.

Таблица 2

Random hardware failure targets	ASIL
$< 10^{-8}$ / h	D
$< 10^{-7}$/ h	C
$< 10^{-7}$ / h	B
$< 10^{-6}$ / h	A

ISO 26262 специфицира четири нива на Automotive SIL (ASIL от A до D). Те се отнасят до нужните изисквания към процесите за разработка и към мерките за безопасност, които позволяват избягването на ненужен остатъчен риск свързан със съставните части (items) и елементи на техническите системи. Количествените стойности свързани с ASIL нивата, са цели за случайни (random) хардуерни откази. Те са еднакви за ASIL B и C. Затова, за да бъдат получени по-високи изисквания за категорията, отговаряща на ASIL C, в сравнение с ASIL B, при разработването на системи, попадащи в категорията на ASIL C се прилагат допълнителни качествени мерки. Въпреки, че ISO 26262 е производен на IEC 61508 [7], процесът по определянето на ASIL нивата и мерките свързани с тях е по-различен от този, който е известен от IEC 61508, а така също и железопътните EN 5012x. За разлика от останалите стандарти, тук ASIL нивата и така наречените Safety Goals зависят не само от честотата на възникване и от последиците, а са производни и на оценката за възможността за установяване на контрол върху ситуацията от страна на човешкия оператор (шофьора). Честотата на възникване е променена във вероятност за излагане и може да включва и продължителността на изпадане на системата в даденото състояние.

6. КРИТЕРИИ СВЪРЗАНИ С ПРОИЗВОДСТВЕНИЯ ПРОЦЕС В ЖЕЛЕЗОПЪТНИЯ ТРАНСПОРТ

Най-широко използваните критерии, които са свързани с производствения процес на техническите системи в железопътния транспорт, могат да бъдат намерени в така наречените RAMS стандарти на CEN/CENELEC, които включват стандартите EN 50126 [9], EN 50128 [10], EN 50129 [11]. Тези критерии свързват така наречената приемлива честота на възникване на опасността (THR – Tolerable Hazard Rate) с така наречените интегрирани нива на безопасност (SIL – Safety Integrity Levels). SIL-нивата от своя страна са свързани с определени изисквания към използваните производствени процеси, а така също и с мерки за контрол на опасностите и рисковете до нива, които са приемливи. Кратко описание на връзката между THR и SIL е поместено в **Таблица 3**.

Таблица 3

THR (h^{-1})	SIL
$10^{-9} \leq THR \leq 10^{-8}$	4
$10^{-8} \leq THR \leq 10^{-7}$	3
$10^{-7} \leq THR \leq 10^{-6}$	2
$10^{-6} \leq THR \leq 10^{-5}$	1

Друг подобен критерий се намира в Европейския регламент за оценка на риска [1]. Той свързва така наречените "Катастрофални последици" („смъртни случаи и/или множество тежко пострадали, и/или големи щети на околната среда") с приемлива честота на възникване $\leq 10^{-9}$/h.

7. КРИТЕРИИ СВЪРЗАНИ С ПРОИЗВОДСТВЕНИЯ ПРОЦЕС В КОРАБОПЛАВАНЕТО

В сектора на корабоплаването съществуват различни видове критерии за приемливост на риска, които са свързани с дизайна на техническите системи.

Организацията IMO (International Maritime Organisation), която е специална агенция на Обединените Нации е специфицирала техника за формална оценка на безопасността (FSA - Formal Safety Assessment) [12]. Тази техника определя глобални цели за индивидуален риск и за обществен риск: „*максималният годишен риск за смърт за членове на екипажа трябва да бъде 10^{-3} и за пътници/общество 10^{-4}*". Извън рамките на този критерий е изискано да бъде проведена оценка на загубите и печалбите свързани с допълнителни мерки за намаляване на риска [2].

IMO е дефинирала и други критерии за приемливост на риска, които са част от международния кодекс за високоскоростни плавателни съдове [13]. Този кодекс включва цели на системно ниво, които са близки до тези в авиацията [2].

Таблица 4

Failure mode effect	Acceptable probability of occurrence per hour	Probability of occurrence description
Catastrophic	$P < 10^{-9}$	Extremely improbable
Hazardous	$10^{-9} \leq P < 10^{-7}$	Extremely remote
Minor	$10^{-5} \leq P < 10^{-3}$	Extremely improbable

8. ИЗВОДИ И ЗАКЛЮЧЕНИЯ

В настоящата статия накратко се запознахме с различни видове критерии за приемливост на риска, които съществуват в сферите на авиацията, на автомобилния, железопътния транспорт и на корабоплаването. Тази статия не би могла да бъде изчерпателна, но тя представя един добър, стегнат обзор на някои от критериите. Като цяло, в научните кръгове цари мнението, че в същността си тези критерии са сравними по цел, а така също и в много частични отношения. За съжаление, те не са сравними в детайл, тъй като исторически се основават на различни дефиниции и на комбинации от различни други изисквания. И все пак - частичните сравнения са нужни и полезни.

ЛИТЕРАТУРА:

[1] "Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council"; "Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009"

[2] Final report of the study on "Risk Acceptance Criteria for Technical Systems and Operational Procedures", issued by the European Railway Agency, prepared by Det Norske Veritas Ltd., Revision 02, 22/01/2010

[3] "Guidelines for Development of Civil Aircraft and Systems", EUROCAE ED-79A и SAE Aerospace Recommended Practice ARP 4754A, 21/12/2010

[4] "Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment", EUROCAE ED135 and SAE Aerospace Recommended Practice ARP 4761, 12/1996

[5] “Software considerations in airborne systems and equipment certification”, EUROCAE ED-12 и RTCA DO-178, issue B, 1/12/1992
[6] “Design Assurance Guidance for Airborne Electronic Hardware”, EUROCAE ED-80 and RTCA DO-254, 4/2000
[7] “Road vehicles – Functional safety” ISO 26262 Parts 1-9, first edition, 2011-11-15 ISO/FDIS 26262, Part 10, 20/07/2011
[8] “Functional safety of electrical/electronic/programmable electronic safety-related systems IEC 61508 Parts 1-7, Edition 2.0, 4/2010
[9] “EN 50126:1999 - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)”
[10] “EN 50128:2001 - Communications, Signalling and Processing Systems - Software for Railway Control and Protection Systems”
[11] “EN 50129:2003 Railway Applications - Communication, signalling and processing systems - Safety Related Electronic Systems for Signalling”
[12] “International Maritime Organisation, Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule Making Process”, T1/3.02, T5/1.01, 05/04/2002
[13] “International Code of Safety for High-Speed Craft (HSC Code) (resolution MSC.36 (63)”, which was developed following a revision of the “Code of Safety of Dynamically Supported Craft (resolution A.373(X))”.

BASED ON WHICH CRITERIA DO WE ACCEPT RISKS IN THE FIELD OF TRANSPORT

Maria Antova
mantova@gmail.com

BULGARIA

Key words: *safety, management, evaluation and criteria for risk acceptance, transport*

Abstract: *The transport is a multifactor open system, which is a subject of many external and internal risks of different types and origins (technical, organisational, human, nature, etc.). The type of the risks is often a factor, which plays a big role in decision how to assess the risk and in our evaluation on whether it is acceptable for us. On the other hand side, the historical development of the different types of transport with their different technical, organisational and geographic aspects, is also an important factor, which contributes to the variety of practices with regards to the management and the evaluation of the risks. Therefore, the role of internationally accepted laws and standards, which include requirements towards the assessment and the acceptance of the risk, is very important. Such documents are for example the family of international standards IEC 61508, ARP 4753/ED 79, DO-178/ED 12B, DO-254/ED 80, ISO 26262, as well as other international standards and documents.*

This article aims to present a short overview of the present practices within some types of transport with regards to the criteria for risk acceptance. Presently, at an international level, many of the aspects, related to these criteria do not yet have a solution. From the point of view of the author, this article has the aim to present an objective overview, which would contribute to the discussions and provoke further conversations, analyses and research on the above subject.