Механика Транспорт Комуникации

Научно списание

ISSN 1312-3823

брой 3, 2009 г.

статия № 0444

http://www.mtc-aj.com

ПРЕДЛОЖЕНИЕ ЗА МЕТОД ЗА ОЦЕНКА НА БЕЗОПАСНОСТТА НА СЪВРЕМЕННИТЕ ЖЕЛЕЗОПЪТНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ И КОНТРОЛ

Нели Стойчева, Бисер Минчев

nstoytcheva@vtu.bg , mbinchev@mtc.government.bg

ВТУ „Т. Каблешков”, 1574 София, ул. „Г. Милев” 158

БЪЛГАРИЯ

Резюме**: Европейската Железопътна Агенция (ERA) има задача да установи Общи Цели на Безопасността (CSTs) и Общи Методи за Безопасност (CSMs) за железопътните системи в Европа. Целта на тази статия е да предложи метод за оценка на безопасността на новата Европейска система за контрол. . Предложението интегрира колиествен и качествен подход.* ***В неговата основа са известни подходи и най-добрите практики в Европа.

***Ключови думи:** Безопасност, надежност, риск, ERTMS*

ВЪВЕДЕНИЕ

Стандартите *CENELEC* EN 50126 и EN 50129 дефинират ***безопасността*** като отсъствие на недопустимо ниво на риска. По този начин въпросът “каква безопасност е необходима?” се задава като “какво ниво на риска е допустимо?”. Ето защо трябва да бъдат дефинирани и използвани принципите за допустимото ниво на риска

Стандартите CENELEC обаче не помагат много при избирането на принципите определяне на допустимия риск. EN 50126 препоръчва да се използват основните приети принципи : ALARP, GAMAB, and MEM.

В контекста на анализа на риска се прилага избрания принцип, за да се идентифицитат на опасностите. Избраният принцип дава отговор на следните въпроси:

1. решава дали в устройството или функцията, отговорни за безопасността е необходимо или не правило за безопасност (ако това вече не е уредено чрез друга регулация);
2. определя безопасностното ниво на интегритет (SIL- Safety Integrity Level) за всички необходими безопасни устройства и функции;
3. определя други параметри, свързани с безопасността, например спирачна дължина, скорост и т.н.

Така избрания принцип има голямо влияние върху процесите на проектиране и качеството на крайната осигурителна система., може да подпомогне техническия прогрес. Избраният прионцип може да спести много усилия по контролиране на случайните хардуерни откази, системните грешки в спецификацията и операторските грешки по време на работа на системата.

За разработване на безопасни осигурителни системи има специални ограничения. В процеса по разработване на изискванията към спецификацията на системата са въвлечени три страни. Първата страна е железопътния мениджър. В България това е НК „ЖИ”. Тяхно задължение, съгласно стандартите, е подготовката на техническата спецификация. Много често изпълнението на тази задача се възлага пряко на (или в

сътрудничество) индустриални разработчици (производители)

Трета страна са наблюдаващите органи (органите по безопасност), които трябва да инспектират изискванията на спецификацията, осигурявайки съответствие със стандартите. В Република България този орган е Изпълнителна Агенция „Железопътна Администрация" към Министерството на транспорта. Европейската практика показва, че работата по инспектиране се възлага често на независим оценител, който е експерт в съответната приложна област.

След приемане на изискванията на техническата спецификация работата се предава на индустриалните разработчици, които правят реализацията на спецификацията в качеството си на доставчик.

ЦЕЛ НА СТАТИЯТА

В тази статия е предложен метод за анализ на риска съгласно стандартите EN 50126 I 50129 за ERTMS. Отправна точка за този анализ е определянето на нивото на допустимия риск.

В стандарта не се дават точни изисквания за провеждане на анализа на риска.

CENELEC дефинира риска като "отсъствие на недопустим риск"[50126]. Следователно критерият за допустим риск е отправна точка, касаеща допустимия граничен риск. Оттук, безопасността съществува, когато риска е допустимо малък, т.е. не по-голям от граничния риск.

В тази статия се дава процедурата за определляне на допустимия риск, адаптирана за ERTMS. Това изисква изясняването на следните въпроси:

1. Как може термина "риск" да бъде определен успешно и обхватно в този контекст?
2. Какъв риск е допустим в случай на ERTMS?

Тук се дават основните положения.

ОПРЕДЕЛЕНИЕ ЗА РИСК

В EN 50126 рискът се разбира като някаква средна стойност. В практиката действителния риск варира около тази средна стойност; прогнозираната средна стойност също липсва поради статистическата несигурност на началната стойност, използвана при оценката от експертите.

ДОПУСТИМ РИСК

След аргументите, представени в предишната секция е необходимо да се определи допустимия критерий за индивидуалния риск на пътниците. Няма универсално приет допустим критерий поради голямата разлика между различните компании.

Безопасността в EN се дефинира като отсъствие на недопустим риск. Степента на риска не трябва да превишава една допустима гранична стойност (**Tolerable Hazard Rate** – **THR**).

Така дефинирана, тя включва както техническите характеристики на осигурителната система (вероятността за възникване на опасни откази), така и параметрите на управлявания процес.

Различават се *индивидуален риск* и *колективен риск*.

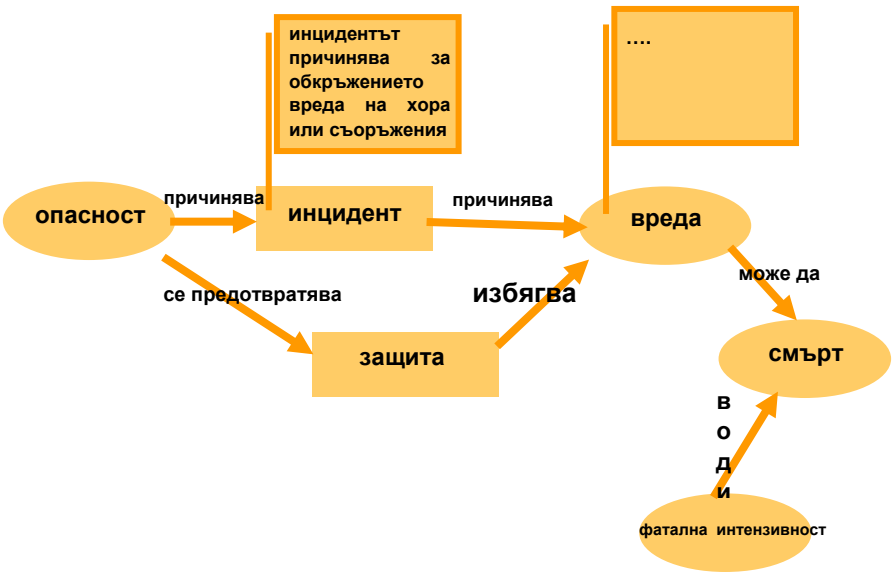
Индивидуалния риск се измерва с вероятността за възникване на произшествие със смъртен случай за една година:

R_I = Брой смъртни случаи за една година / Брой пътници.

Колективният риск се измерва с броя жертви за една година. Статистически средния индивидуален риск се получава като отношение на колективния риск и броя на индивидите в колектива. (Това е коректно при положение, че всички индивиди се държат еднакво спрямо процеса).

Съгласно европейските норми доказателството за безопасност е комплекс от документи, доказващи функционалната и безопасностна пригодност на изделието, доказващи и обезпечаването на качеството на изделието през целия му цикъл на живот.

Една примерна схема на подход за онтология на термините е показана на фиг.1.



Фиг. 1 . Примерен подход за онтология на безопасността

Примери на количествени критерии

Досега много малко критерии са публикувани. Най-добре познатия критерий в жп транспорт е MEM критерия.

MEM принципа постулира, че техническата система- и включените в нея жп системи- не трябва да допускат по-голям риск от смъртни случаи от 10^{-5} за година.

Проблеми и процедури

Граничният риск, със всички инциденти, които могат да се случат по време на работата, не трябва да бъде превишен. Това включва инциденти, причинени от откази в инфраструктурата (напр. счупена релса), в превозните средства, в осигурителната система (централизацията и оборудването по контрола и управлението) и други компоненти, имащи връзка или човешките грешки.

При оценката в процедурата са въвлечени и техническите системи и човешките действия.

MEM може да се интерпретира по различни начини:

- положението, че "фатална опасност поради цялата техническа система" трябва да не надвишава минималната ендогенна смъртност "съдържа значителна степен на произволност".
- Няма отправна точка, в която да се казва какъв критерий за риска да се прилага към различните системи и инсталации- той е един и съща за всички и системата като цяло. Обаче, тук няма нито технически, нито статистически причини да се прави това.
- Съгласно EN 50126 не е ясно как става преминаването от MEM критерия, свързан с време на живот 1 година и извлечения критерий за един час, определен в MEM.
- Ако се избере година като отправна променлива, това може да доведе до безотговорно приемане на риск в случай на кратко, рядко или много опасно събитие.
- Ако се избере година пък за непрекъснато излагане на опасности , това може да доведе до нереалистични технически изисквания в случай на много кратки промеждутъци на излагане на риск.
- Дори, ако MEM критерия се приложи за целия жп трафик, въпросът е как рискът ще бъде разделен между различните му части .

Анализ на статистиката на инцидентите

За да се направи точен количествен анализ е нужна базата данни от статистическия анализ на железопътния мениджър. НК „ЖИ" има достатъчно добра база данни с такива събития и те ще бъдат използвани при следващи анализи от авторите.

АНАЛИЗ НА БЕЗОПАСНОСТТА

Безопасността на една система (част от система или блокове от нея) се оценява посредством анализ на риска съгласно стандартите CENELEC [34,35,36,50].

Анализът на безопасността е свързан с две цели:

1. Трябва да идентифицира всички опасности, присъщи на системата или свързани с нея.
2. Трябва да докаже, че вероятността за опасно събитие, достигната от системата, е по-малка от установения праг.

Стандартите дават известна свобода относно използвания метод за осъществяване на този анализ. В стандартите се препоръчва използването на Блок диаграми на надеждността, Дърво на отказите, Дърво на събитията, Марковски процеси, Мрежи на Петри, Анализ на вида и последствията от отказите (FMECA) и др.

Изборът на подходящ метод, или комбинация от методи, зависи от дадената свобода (изискванията на RAMS) и от специфичните аспекти на разглежданата система. Така *методите за анализ на риска трябва* да:

1. Допускат систематичен анализ на отклоненията и потенциалните опасности[1] ;
2. Допускат количествена оценка на риска[1];
3. Засягат всички аспекти на RAMS [1];
4. Да са с широко приложение (допускайки по-нататъшно използване)[2];
5. Бъдат модулни и разширяеми към съседни системи;
6. Допускат анализ чрез елементи или чрез функции на разглежданата система;
7. Бъдат стандартизирани и/или интернационално признати;
8. Бъдат органически (да засягат цялата система) - да дават общ поглед върху системата и да интегрира технически, човешки и експлоатационен аспекти.

Методите за анализ трябва или да:

- оценяват точно резултантния (индивидуален) риск или да определят приемливата степен на опасност чрез сравнение с работещи системи или познато ниво на техниката, посредством статистически или аналитични методи, или
- да определят приемливата степен на опасност от алтернативни качествени методи, ако те установяват като резултат една листа от опасности и съответния THR.

Анализът на безопасността е необходим за много технологични области. Този анализ има за цел да обслужи две цели. Първо, трябва да идентифицира всички опасности, които са присъщи на системата или свързани с нея. Второ, трябва да се покаже, че вероятност за опасно събитие, достигната от системата, е по-малка от установения праг. Тази философия използва вероятностни причини и се използва в различни вариации в различни области. Основните методи обаче остават същите, независимо от областите на приложение.
Въпреки, че не е точно споменато в RAMS процедурите, описани в EN 50126, трябва да се отбележи, че анализът на риска е итерационен процес, който налага успешното внедряване на данните за опасностите. Обаче, EN 50126 позволява относителна свобода относно средството и метод, използван за осъществяване на този анализ. По-специфични препоръки се откриват в EN 50129 нормата, но те се прилагат по-скоро за електронното оборудване, отколкото за големи функционални системи

ОБЩ МОДЕЛ НА АНАЛИЗ НА БЕЗОПАСНОСТТА НА ERTMS

Моделирането на ERTMS системата може да бъде осъществено на три етапа :

- Системата се моделира на етап “анализ на изискванията“ към нея, на етап “функционално проектиране” и на етап “техническо проектиране”.
- До техническо изпълнение на системата се стига след (1) моделиране, (2) Функционален синтез и общо моделиране на надеждността и (3) технически синтез и локално (на ниво подсистема) моделиране на надеждността.
- Извършва се идентификация на опасните ситуации, анализира се модела, задават се общите изисквания за безопасност, анализира се модела на подсистемите и се прави обща оценка на безопасността преди да се пристъпи към техническо изпълнение на системата.

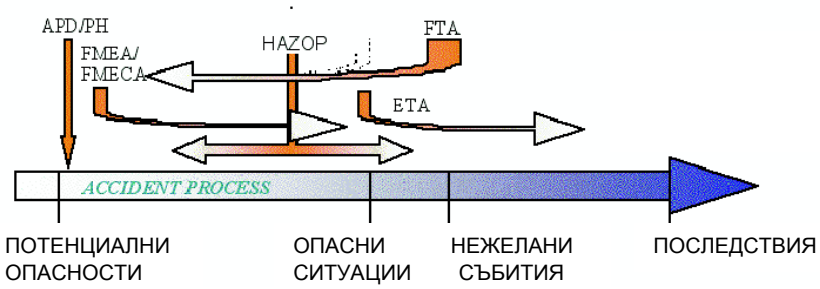
[1] изрично изискване на CENELEC стандартите
[2] нужно в контекста на изследването

Някои от тези класически методи за анализ на риска с голямо приложение са представени на фиг.2. Те се различават чрез тяхната <<входна точка>>, <<посока на изследване>>(индуктивна, дедуктивен) и чрез причинно-следствената им логика.

За да се анализира системата, е необходимо да се създаде модел във форма на FMECA структура. Адаптираният модел е по-скоро функционален, давайки на FMECA йерархията, която отразява не непременно физическата структура на системата. Функционалния подход се съобразява с факта, че повечето елементи на системата имат няколко функции, които работят на различни йерархични нива.

От функционална гледна точка, най-високата функция на системата е оптималното маршрутизиране на трафика. Съгласно FMECA метода, то е това ниво, където разпространените откази ще се появят като "макроскопични" последствия за системата. Тези последствия могат да бъдат вреда за хората, за оборудването или за работата на системата.

Необходимо е да бъдат разработени автоматизирани системи за инженерна дейност, отговарящи на нарасналата сложност на новите системи, увеличаващата се миграция на оборудването и неговата интероперативност. Нормата EN 50128 подсказва използването на формални методи.



Фиг. 2. Класически методи за анализ на риска

ЗАКЛЮЧЕНИЕ

Основната задача на ERTMS е да осигури безопасен железопътен трафик. Този процес трябва да бъде свободен от недопустим риск, който се дефинира като вероятност на нежелано събитие или състояние, получено при случайна повреда. За оценка на риска на съответната опасна ситуация, процесът, който се контролира от ERTMS, трябва да бъде анализиран още на първия етап при проектирането на системата. Трябва да бъде приложен подходящ модел на процеса, за да бъдат идентифицирани нежеланите събития и за оценка на интензивностите им на появяване, съобразно и честотата на трафика.

Може да бъде получена допустима вероятност на появяване на нежеланите събития на база на подходящ критерий за безопасност ALARP, GAMAB или MEM. Неговото сравнение с получената от оценката на модела стойност ще направи възможна оценката на риска на ERTMS.Тя е решаваща за по-нататъшното проектиране на ROCS и за техническото изпълнение на анализа на безопасността.

За да бъде моделирана подходящо железопътната осигурителна система, трябва да се използва подходящ формален език за моделиране. В конструирания модел трябва да се опише функционалното поведение на системата и поведението и след отказ и да се направи качествен и количествен анализ.

Главният проблем при моделирането на безопасността на ERTMS е необходимостта от описание на не-детерминистичното поведение на системата, което е причинено от стохастичния характер на обкръжението на системата и процеса на деградация на системата. Целта на безопасностния анализ е да се оцени нивото на безопасността по време на функционалното и техническото проектиране на ERTMS. Актуалните в момента Европейски стандарти изискват отчитане на

потенциалните човешки жертви и на вредите, причинени от бъдещата работа на системата.

Приемливо предсказване на нежеланото поведение на поведението на системата може да бъде получено само чрез вярно описание на влиянието на стохастичния процес върху коректното функциониране на системата. Тук се отнася, от една страна описанието на стохастичния характер на контролирания транспортен процес, който директно влияе на честотата на опасните ситуации, водещи до фатални последици, и от друга страна, възможна неизправност на компонент на техническата система трябва да се има пред вид, също както и вероятността за погрешно човешко решение, които могат да доведат системата в опасно състояние.

Необходими са изследвания и експерименти, касаещи моделирането на железопътни осигурителни системи, водещи до реални и с практическа стойност резултати. Необходими са сравнителни експерименти между резултатите от аналитичното моделиране и различни реално работещи и използвани в практиката системи в лабораторни условия.

Настоящата статия не претендира за изчерпателност на проблема, но дава насоката на бъдещата работа на авторите в тази област.

ЛИТЕРАТУРА:

1. CENELEC, EN 50126: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). 1998.
2. CENELEC, EN 50128: Railway applications –Communications, signalling and processing systems – Software for railway control and protection systems. 2000.
3. CENELEC, EN 50129: Railway applications – Safety-related electronic systems for signalling. 2002.
4. CENELEC, EN 50159-1/-2: Railway applications - Communication, signalling and processing systems - Safety-related communication in open/closed communication systems. 2001.
5. Иванов, Е., Н.Стойчева, Европейските норми в осигурителната техника, Списание "Железопътен транспорт", стр.37-40,10 брой, 2004
6. http://europa.eu.int/comm/energy_transport/library/lb_com_2001_0370_en.pdf
7. Strategic Rail Research Agenda – Technical Annex, ERRAC, 2002, http://www.errac.org/docs/ERRAC_SRRA_Tech_Annex.pdf
8. http://europa.eu.int/comm/transport/rail/era/doc/wp2005.pdf

A PROPOSAL FOR A SAFETY ASSESSMENT METHOD FOR RAILWAYS CONTROL SYSTEMS

Nelly Stoytcheva, Biser Minchev

nstoytcheva@vtu.bg, mbinchev@mt.government.bg

Higher School of Transport, 1574 Sofia, 158 Geo Milev str.

BULGARIA

Key words. *Safety, Reliability, Risk, ERTMS*

Abstract: *The European Railway Agency (ERA) has the challenges task of establishing Common Safety Targets (CSTs) and Common Safety Methods (CSMs) throughout Europe. The purpose of this paper is to provide a proposal for safety assessment method for the new European control systems. The proposal integrates quantitative and qualitative approaches. It is based on existing best practices in the railway supply industry across Europe.*