Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 14, брой 3/2, 2016 г.
Научно списание **http://www.mtc-aj.com** **статия № 1401**

БАЗОВА КОНЦЕПЦИЯ И ТАКСОНОМИЯ НА ПРОБЛЕМИТЕ И ПОНЯТИЯТА В КРИТИЧНИ ПО БЕЗОПАСНОСТ СИСТЕМИ

Мария Христова, Христо Христов, Пламен Атанасов
mhristova@vtu.bg, cac@vtu.bg, p.atanasov.90@gmail.com

Висше транспортно училище „Тодор Каблешков”
София 1574, ул. „Гео Милев” № 158
БЪЛГАРИЯ

Ключови думи*: надеждност, сигурност, таксономия, критични по безопасност системи, критичен по безопасност софтуер, отказоустойчивост.*

Резюме: *Направени са проучвания в научната литература, фирмени материали и реално работещи системи, които позволяват да се обобщят и класифицират понятията и проблемите на релевантни по безопасност системи. Установени, изведени, обобщени и класифицирани са понятията и проблемите в критични по безопасност системи и са дефинирани йерархичните релации между тях. Използван е подходът на таксономията като наука за класификацията и систематизацията на сложни системи. Намерено е системното място и взаимната връзка между грешките, неизправностите и произтичащите от тях откази, както и техните следствия за безопасността на системите. Систематизирани са средствата за откриване на отказите и стопиране на тяхното опасно въздействие (fail-safe) както и средствата за толериране (fault tolerance) на отказите, чрез които се повишава отказоустойчивостта на системата. В предложената класификационна схема е показана и йерархията на различните видове тестове, хомогенното и диверситетното резервиране, включително различни форми на диверситета като средства за постигане на по-висока надеждност или по-добра идентификация на отказите.*

1. ПОСТАНОВКА

Критична по безопасност система (**S**afety **C**ritical **S**ystems - SCS) е система, от правилното функциониране на която зависи безопасността на човека. SCS системи управляват особено отговорни технологични процеси (в транспорта, авиацията, енергетиката, медицината и т.н.), чиито откази могат да доведат до загуба на живот, на големи човешки ценности. Предназначението на SCS налага особености при съставяне на спецификацията, при тяхното структуриране, изграждане, програмно осигуряване, следотказово поведение, както и до необходимостта да се спазват стандарти, адресирани към този клас системи.

По SCS има множество публикации ([1], [2], [3], [4] и др.), включително такива, в които се въвеждат термини, дефинират се понятия, извеждат се проблеми и се предлагат решения. Авторски принос към проблема е и монографията [5], където се предлага класификация на понятията в проблемното поле на софтуера.

Целта на настоящата статия е да се направи опит от литературните проучвания да се извлекат концепциите, да се установят, обобщят и класифицират понятията и проблемите в SCS и се дефинират йерархичните релации между тях.

2. ПРОБЛЕМИ В РЕЛЕВАНТНИ ПО БЕЗОПАСНОСТ СИСТЕМИ

От направените проучвания в литературните източници за проблемите на SCS могат да се извлекат и обобщят проблемните групи в хронологична последователност на тяхното решаване при изграждане на една критична по безопасност система:

- Съставяне на *рисково базирана спецификация*, съобразена с възможните опасности както при функционирането, така и след откази на SCS;
- *Синтез* и *структуриране* на системата в съответствие със спецификацията;
- Избор на *език за програмиране,* най-подходящ за критичен за безопасността софтуер;
- Методи и средства за откриване и отстраняване на *грешките при създаването и експлоатацията на системата;*
- Количествено оценяване на *влиянието на грешките* върху интензивността на отказите, надеждността и безопасността на системите;
- Методи и алгоритми за *толериране на грешките* и потискане на влиянието им.
- Сертификация на системата и *проследимост* на софтуера.

Във всяка проблемна група се използват общоприети и специфични термини, за класификация на които по-долу е използвана методологията на *таксономията.*

3. ТАКСОНОМИЯ

Таксономията е учение за принципите на класификацията, теория за систематиката на сложно организирани области, обикновено с йерархична структура**.** В контекста на управлението на знанията, таксономията е *йерархично структуриран набор от термини, който се използва за класификация и навигация* [6]. Тя включва правила, методи и приложението им. Отделените за изследване елементи и групи обекти и подсистеми се наричат *таксони*. Съгласно правилата класификацията се прави по съществени, а не по случайни акцидентални свойства.

Таксономията се изгражда по известна методика, включваща: изследване на текстови корпуси с цел установяване и извличане (анотиране) на най-често срещаните и общоприети понятия; създаване на контролиран речник на извлечените класове от понятия; определяне на йерархичните релации между класовете. Класификацията се илюстрира графично с две различни схеми: дендритообразно (дървовидно), известно в логиката като класификационно, или във формата на вложени един в друг кръгове, олицетворяващи таксони.

4. ТАКСОНОМИЯ НА ПОНЯТИЯТА И ПРОБЛЕМИТЕ

Основни таксони са *надеждност*та, *безопасността* и *сигурност*та.

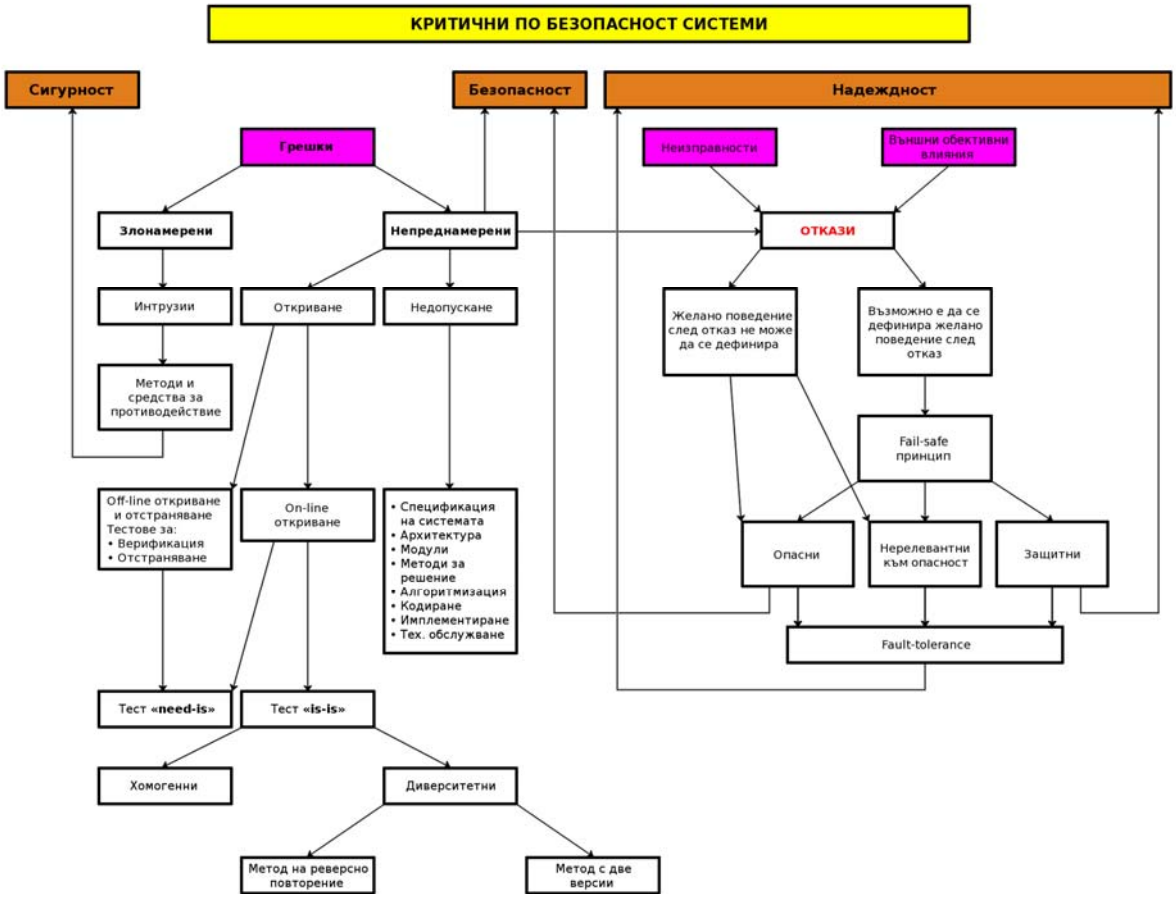
Надеждността (най-общо) е способност на обекта да запазва качеството си на съответствие в течение на отработката (времето за работа) при зададени ограничения.

Безопасността (safety) S(t) е съхранимост, отсъствие на недопустим риск. Рискът е мярка за възможните загуби от нежелани събития, чието настъпване е вероятно.

Сигурността (Security) е способността на системата да се защищава (да противостои, да противодейства) на външни дестабилизиращи фактори и въздействия, както и на вътрешни изменения, които могат да доведат до опасност.

Стремежът е да се постигнат високи нива на надеждност, безопасност и сигурност.

Една класификация на основните понятия и проблеми, базирана на *таксономията*, е показана в дървовидната версия на таксономията на SCS (фиг. 1).На най-високо ниво в структурно-класификационната схема стоят таксоните: *грешки*, *неизправности* и *външни влияния*.



фиг. 1 Таксономия на понятията в критични по безопасност системи

Грешката е отклонение от възприетия критерий за вярност. Грешките при създаването на системата и нейното поддържане в експлоатация са *непреднамерени случайни* и *пред(зло)намерени*. **Преднамерените (злонамерени) грешки** са резултат от неоторизирани умишлени прониквания (интрузии) и извличане и/или промяна на информацията в системата. Те са свързани със сигурността и защитата на SCS. **Непреднамерените грешки** влияят върху надеждността и безопасността, а те са ключово важни характеристики на SCS. Затова се прилага стратегия за перфектност (недопускане на грешки) – съвкупност от подходи, методи и средства за съставяне на безгрешни: рисково базирана спецификация, синтез и структуриране на системата, архитектура на софтуера, изграждане на модулите, алгоритмизация и кодиране.

Откриването и отстраняването на неизправностите и грешките става off- или on-line. Off-line тестването (преди пускане в експлоатация) е силно развита наука и практика и обхваща известни подходи, методи и средства, по които има публикации, монографии и дисертации. On-line тестването (по време на работа) се прилага с цел откриване на грешките и/или неизправностите и своевременни реакции на работещата система. Тези реакции могат да са два вида: спиране до отстраняване на откритата грешка или неизправност; превключване към резерв, ако такъв има.

За on-line откриване на грешките и неизправностите се прилагат различни методи, но най-ефективният от тях е **диверситетът.** Диверситетът [5, 8, 9] е метод за решаване на задача (математическа, логическа, техническа и пр.) по два (А и В) различни начина при еднакви входни данни. Когато двете решения, модулите, са идентични (антиномни на диверситета), чрез сравнение на резултатите могат да се откриват неизправности, но не и грешки. Откриват се само хардуерните повреди, които са независими в двата модула и нямат свойството да се мултиплицират.

Когато модулите са диверситетни, грешките при конструирането и технологията на изработването им, при алгоритмизацията и кодирането на програмите им, са независими. Вече

могат да се открият, защото водят към различни резултати от решенията. За целта най-често се прилагат две версии, решаващи една и съща задача по различни методи, алгоритми и програми, разработени от различни екипи. Авторско предложение е да се използва (т. нар. от авторите) метод на реверсното повторение [10], който позволява и двете версии да се изпълнят от един и същи програмист.

Случайните непреднамерени грешки, заедно с неизправностите на хардуера и външните влияния, предизвикват **откази.** Отказите са събития, които водят до нарушаване на работоспособността на системата.

Има отговорни технологични процеси (ОТП), някои от нарушенията на които не са опасни. Когато управляващата система след отказ може да заема предварително дефинирано безопасно състояние или да има желано поведение, отказите се подразделят на **защитни** или **опасни**. Ако след отказ поведението на системата противоречи на дефинирания критерий за безопасност, отказът е опасен, а ако му съответства – защитен. Такива са случаите в жп сигнализацията, охранителната техника и др. В системите от този клас може да има откази, нерелевантни на безопасността, които нямат опасни последици, тъй като засягат други системни функции без отношение към безопасността. Те касаят само надеждността.

Ако пък ОТП е от такова естество, че всеки отказ на управляващата го система е опасен (във въздушния транспорт, в животоосигуряващи системи в медицината и др.), единственият подход да се постигне безопасност е отказоустойчивостта (*fault-tolerance*). Отказът се маскира, толерира, надеждността нараства - толкова повече, колкото по-голям е делът на толерираните откази. Но потискането на отказите зависи от наличието на излишък (*redundancy*) - структурен, функционален, времеви и др. Когато той се изчерпи, системата отново започва да отказва. Изчерпването на излишъка зависи от неговата дълбочина, а тя има функционални и икономически измерения.

От проучванията може да се направи изводът, че проблемите на SCS са в две пространства:

- **Функционално.** Функциите на различните по предназначение системи са описани в техните спецификации, стандарти и др. съпътстващи документи. На тази основа учени, изследователи и проектанти - професионалисти с експертен опит в съответната сфера (транспорта, авиацията, енергетиката, медицината и т.н.) - създават техническите средства. Специализирани програмисти разработват софтуер, който изпълнява дефинираните от тях изисквания. Функционалността е свързана с безопасността. Ако те не се спазили принципите и правилата, ако не всички условия за безопасност са предвидени, ако не са намерени правилните реакции, системата може да е опасна и когато работи нормално, както е зададено от създателите.
- **Надеждностно-безопасностно.** Това пространство е общо за всички системи, независимо от тяхното предназначение и функционалност. В него се влиза като се предположи, че спецификацията, по която системата е изпълнена, е перфектна. Когато SCS е работоспособна, тя изключва опасните управляващи въздействия. Опасностите се създават само след откази. Проблемите в това пространство са свързани с: нормите за допустим риск, най-често определен в международни стандарти; методите за изграждане и структурите на fail-safe и fault-tolerance SCS; методите за изграждане на безгрешен софтуер; оценката за опасността след отказ; методите, с които тя може да се намали; вероятностните модели на надеждността и безопасността на съответната структура, оценяващи влиянието на грешките на софтуера и др.

ЗАКЛЮЧЕНИЕ

Като са използвани правилата на таксономията е направен опит да се систематизират понятията и проблемите на критичните по безопасност системи и се дефинират йерархичните релации между тях. Построена е класификационна схема, която претендира да обхваща основната част от термините и тяхното понятийно покритие. В хронологична последователност са дефинирани проблемите от функционалното и надеждностно-безопасностно пространство,

които трябва да се решат при създаване на критични по безопасност системи. Получените резултати са основа за анализ и насоки за бъдещи изследвания в областта.

ЛИТЕРАТУРА:

[1] Avizienis A., J.C. Laprie, B. Randell, Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, vol.1, 2004

[2] Knight J. C., Safety critical systems: challenges and directions, Proceedings ICSE '02, pp. 547-550, ACM, NY, USA ©2002

[3] Ben Swarup Medikonda and Seetha Ramaiah Panchumarthy. An Approach to Modeling Software Safety in Safety-Critical System, Journal of Computer Science 5 (4), Science Publication 2009

[4] A.Castañeda, I. Romera, F. Bernard, P. Dahlen, B.Todd, D. Willeman, M. Zerlauth, The use of Software in Safety Critical Interlock Systems of the LHC, Proceedings of EPAC08, Genoa, Italy, 2008

[5] Христова, М. Софтуер за критични по безопасност системи. Изд. ВТУ „Т. Каблешков", 2016

[6] Bailey, S. Do you need a taxonomy strategy?, 2002, http://www.ikmagazine.com/xq/asp/sid.0/articleid.E4F31EEC-FB65-413A-A24B-13AA6AC DD12D/qx/display.htm

[7] Шаталкин А.И., Таксономия. Основания, принципы и правила. Изд. Товарищество научных изданий КМК, 2012 г. http://ashipunov.info/shipunov/school/books/shatalkin2012_taksonomija.pdf.

[8] Popov G., Failures Detection Methodology In Non Recovery Computer Systems Based On Diversity Modeling, International Journal of Computing, 2014, www.computingonline.net

[9] Popov G., Modelling Diversity as a Method of Detecting Failures in non Recovery Computer Systems, Information Technologies and Control, 2005, 2,pp15-19/

[10] Христова М., Обнаружение ошибок программного обеспечения посредством метода реверсного повторения, Proceedings of the IInd International Scientific and Practical Conference "Methodology of Modern Research", UAE, "World science", ISSN 2413-1032, 4(8), vol. 4, 2016.

BASIC CONCEPTION AND TAXONOMY OF THE PROBLEMS AND CONCEPTS IN SAFETY CRITICAL SYSTEMS

Mariya Hristova, Hristo Hristov, Plamen Atanasov
mhristova@vtu.bg, cac@vtu.bg, p.atanasov.90@gmail.com

Todor Kableshkov University of Transport
1574 Sofia, Geo Milev str. 158
BULGARIA

Key words: *reliability, security, taxonomy, safety critical systems, safety critical software, fault tolerance*

Abstract*: The article includes studies in the scientific literature, corporate materials and real working systems that allow for a summarization and classification of the notions and problems in critical systems by relevancy of safety. Issues and concepts in critical safety systems are established, derived, summarized and categorized, and the hierarchical relations between them are defined. The approach of taxonomy as a science of classification and systematization of complex systems has been used. The systematic place and the relationship between errors and faults, resulting failures and their consequences for the safety systems, has been found. The means to detect failures and stopping their dangerous effects (fail-safe) and the means of tolerance (fault tolerance) of refusals by which increases fault tolerance of the system have been systematized. The hierarchy of the different types of tests, the homogeneous and diversity reserve as a means to achieve greater reliability and better identification of failures is shown in the proposed classification scheme.*

Тази статия е написана като резултат от работата по научноизследователски проект 1232/11.05.2016 г. във ВТУ „Т. Каблешков".