Българска академия на науките. Bulgarian Academy of Sciences
Аерокосмически изследвания в България. 14. Aerospace Research in Bulgaria
София. 1998. Sofia

Моделиране и оценка на безопасността на функциониране на системи за управление

*Антонио Андонов, Зоя Хубенова**

Висше военно транспортно училище, София

** Институт за космически изследвания, БАН*

Проблемът за надеждността, устойчивостта и безопасността на системите за управление в реално време на подвижни обекти в авиацията, космонавтиката, релсовия транспорт и др. рязко нарасна с повишаването на тяхната сложност. За решаването на поставения проблем е необходимо в допълнение на общоизвестните методи за обезпечаване на надежност да се използва при разработката им т.нар. безопасна технология, за да се изключи възможността за поява на изхода на системата на опасни съобщения или сигнали. По такъв начин, в допълнение на понятията надежност и експлоатационна готовност е въведено понятието безопасност като вероятност за появата в конкретния процес на управление на отказ (или дефект), който може да има катострофални последствия. Но в предварително зададена система е необходимо да се установи минимално необходимото ниво на безопасност, т.е. максимално допустимата вероятност за отказ. Например в авиацията действат следните изисквания:

– вероятността за катастрофален отказ в системите трябва да бъде по-малка от 10^{-7} на един час летателно време;

– вероятността за критичен отказ в системите трябва да бъде по-малка от 10^{-5} на един час летателно време.

Между влака и самолета има съществено различие в схемите за обезпечаване на безопасността. В самолетите няма устройства за безопасност, подобно на железопътните системи. Неговата безопасност се определя от отказоустойчивостта на всеки от елементите и може да бъде достигната само за сметка на високото ниво на надежност, което се обезпечава от конструктивните характеристики или чрез резервиране. Същевременно безопасността на влаковете се обезпечава не чрез наличието на отказоустойчивост на техните системи, а чрез прекратяване на движението им в

[1] Разработката е финансирана от НФ "Научни Изследвания" при МОНТ, съгласно дог. № 536/95.

случай на каквито и да е откази, в частност с помощта на задействане на осигурителните системи – системите за сигнализация и блокировка. Следователно в авиацията и в релсовия транспорт се използват различни стратегии за решаване на проблема за безопасността: чрез отказоустойчивост(fault-tolerance) и чрез безопасно след откази поведение на системата (fail-safe). Чрез тези две стратегии могат да се решат следните проблеми:

а) В системи, на които е необходима висока степен на безотказност за опазване на живота и околната среда, за управление на полети във въздушния и в космическия транспорт, за работа на комуникационни спътници и др., когато прекъсването за ремонт и възстановяване е недопустимо или опасно.

б) В системи на които е необходима висока готовност, като мощни изчислителни машини или мрежи от компютри (напр. в банковата система) с хиляди терминали, системи с осигурителна отговорност в релсовия транспорт и др., когато неработоспособност е допустима, но предизвиква големи загуби на живота или здравето на човека, на големи нематериални, духовни и природни ценности.

Проучванията показват, че има изобилие от публикации по тези проблеми. Въпреки това са нерешени или частично решени научно-теоретични и практически въпроси с голяма значимост:

1. Обикновено се търси решение на проблема за готовността, без да се поставя акцент на безотказността на система с откази, които се маскират чрез излишък;

2. На концептуално равнище няма единно разбиране за безопасността на системи за управление.

Конвенционалната теория на надеждността не се интересува от поведението на системата, в която са настъпили откази. Вследствие настъпването им системата може да предизвика големи загуби (напр. във въздушния транспорт). В повечето случаи в практиката обаче естеството на контролираното състояние или управлявания процес е такова, че поведението на системата не може да се раздели еднозначно на опасно или безопасно. В такива случаи за постигане на висока безопасност трябва да се търси висока отказоустойчивост, още повече, че ако всички откази са опасни, то безопасността се свежда до безотказност.

Съвременните подходи за анализ и синтез на системи за управление се основават на апарата на пространството на състоянията. При този подход понятието безопасност на системата за управление може да се определи по следния начин: Нека $У$ е множеството изходни сигнали на системата, $У_б$ – множеството безопасни изходни сигнали на системата, $У_{оп}$ – множеството опасни изходни сигнали на системата. Тогава $У_б \cup У_{оп} = У$, и условието за безопасност е $У_б \cap У_{оп} = 0$.

Системата за управление се нарича идеално безопасна само в този случай, когато за произволен отказ f, $f \in F$, където F е множеството повреди на системата, нейният изходен вектор удовлетворява условието $У_f \in У_б$. Идеалната безопасна система винаги осигурява безопасни изходни сигнали, дори когато се намира в неизправно състояние.

Изключително важно място в общия проблем, свързан с изграждането на ефективни, надеждни и с безопасно при откази поведение системи, заема проблемът за оперативна идентификация на динамичните им характеристики [1, 2]. Познаването на текущата информация за динамичното състояние на функциониращата система позволява от една страна да се организира оптимално управление с адаптация относно изменящите се външни условия,

а от друга, позволява да се вземат правилни и своевременни решения при възникване на нарушения във функционирането на системата. Така например в [2] е предложена структура на адаптивна система за автоматично управление с идентификация на динамичните характеристики, използваща комбиниран принцип на управление: адаптивно управление при относително бавно изменение на параметрите вследствие на параметрични смущения и изменение на структурата на управляващата част на системата при скокообразно изменение на параметрите, вследствие на откази с оглед осигуряване на безопасно поведение на системата. Тук понятията надеждност и безопасност се интерпретират като трета и четвърта степен след понятията устойчивост и качество на управлението, които изграждат представите ни за изискванията към системата за управление. Под надеждност на управлението се разбира свойството на алгоритъма на управление и съответстващата структура на управляващата част на системата да съхранява приемливо качество на системата при отказ на отделни подсистеми. Съдържанието на такъв принцип за построяване на системи е търсене и реализиране на такава конфигурация на алгоритъма на управление и на управляващата част, която да минимизира загубите в качеството на управление, обусловени от отказите. С оглед на безопасността на функциониране на системата, при нарастване на загубите над дадено ниво, основната задача, която трябва да реши системата от разглеждания клас е в привеждане на обекта на управлението в определена област или точка в пространство на състоянията. С други думи в този случай системата за управление изпълнява функции и на *осигурителна* система. Във връзка с това при проектиране на система за автоматично управление при този подход е необходимо да се изпълнят следните етапи:

1. Да се определят променливите на състоянието на автоматизирания обект;
2. Да се построи математичен модел на управляемото движение на обекта в пространство на състоянията.
3. Да се формулират изискванията по отношение на безопасността във вид на конкретни ограничения върху стойностите на променливите на състоянието, да се апроксимират във вида на линейни неравенства и да се построи изпъкнал многоъгълник на ограниченията в пространство на състоянията.
4. Да се определи функционалът на качеството на системата и неговата чувствителност по отношение на ограниченията;
5. Да се синтезират ограничаващите управления, препятстващи развитието на функционални нарушения.
6. Да се определи производителността на управляващата ЕИМ необходима за реализация на управляващите въздействия върху автоматизирания обект.

Казано с други думи, още при проектиране на системата, от гледна точка на безопасността възниква задачата за удържане на вектора на променливите на състоянието в зададена област $X_{доп}$ от пространство на състоянията X, при възникване на откази.

Днес, във връзка с внедряването на компютърна техника в системите за автоматично управление, методите на т.нар. безопасна технология широко се използват в различни отрасли на промишлеността при управление на отговорни технологични процеси. Разработени и изпитани са различни безопасни микропроцесорни системи за управление. За изпълнението на зададени функции при осигуряване на надеждност и безопасност структурата на системата се състои от две нива, едното от които не е свързано с безопасността, а другото е безопасно. Безопасното ниво се изгражда от блокове

с по-висока надеждност и по- високи характеристики на безопасността. В този аспект може да се разгледа системата за управление . В общия случай системата за управление се състои от две основни части -- обект на управлението и управляваща част - регулатор. Съвкупността от критерии и правила, в съответствие с които функционира регулатора, преследвайки целите на управлението, представлява алгоритъма на управлението. При това представяне на системата, безопасността й на функциониране може да се постигне по пътя на въвеждане на различни видове излишък: апаратен, информационен, програмен, времеви и др. Може да се въведе понятието елементарна система [1,2], т.е система без излишък. Като се вземе предвид, че структурата на произволна ситема е съставена от технически устройства в съответствие с нейната функционална схема и множество връзки между тях, осигуряващи функционирането й в съответствие с определен алгоритъм, то елементарната система може да се определи като система, която е работоспособна само при отсъствие на откази в нейните технически устройства и връзки между тях. Тогава способите за обезпечаване на безопасност при функциониране се свеждат до:

– резервиране, т.е. добавяне на технически устройства и връзки към елементарната система, така че нейният алгоритъм на управление да е неизменен;

– алгоритмично обезпечаване, т.е. възможно преобразуване на структурата на елементарната система чрез добавяне на устройства и връзки по такъв начин, че да се измени алгоритъмът на управление.

За редица системи, включително и в транспорта, високата степен на апаратен излишък е нежелателна, а в някои случаи (авиация, флота) е недопустима. Затова разработването на методи за алгоритмично осигуряване на безотказност , позволяващи да се намали апаратният излишък, е особено актуално.

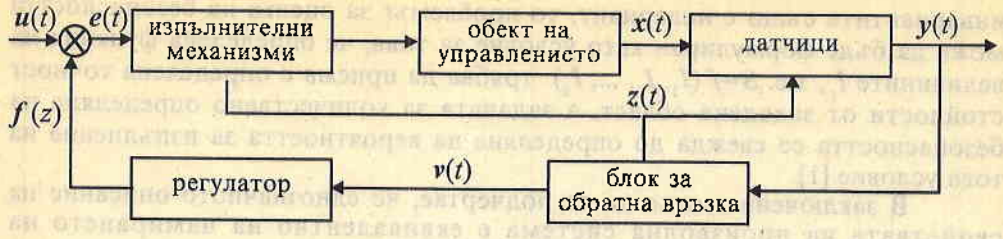
Да разгледаме система, съставена от обобщен обект, включващ обекта на управление, изпълнителните органи и датчици, затворена чрез обратна връзка през регулатор, формиращ алгоритъма на управлението. Ще считаме, че обобщеният обект при номинален режим се представя с уравненията на състоянието:

$$x' = A(t)\, x + B(t)\, u\ ,$$
$$y = C(t)\, x\ ,$$

където $x \in R$ е векторът на състоянията на системата; $u \in R$ – векторът на външните въздействия, $A(t)$, $B(t)$, $C(t)$ са съответно преходната матрица на състоянието, матрицата на управлението и матрицата на наблюдението. Да предположим, че в системата могат да настъпят постепенни параметрични смущения в матрица $A(t)$, внезапни откази в изпълнителните органи (матрица $B(t)$) и внезапни откази в датчиците във вида на появата на допълнителен лъжлив сигнал в съответстващата компонента на вектора на наблюдението. Нека критерият за качество е зададен във вида [1]:

$$V[e(t), u(t)] = e^{T}(t)\, Qe(t) + \int f(z)dz,$$

където $e(t)=y(t)-y^{0}(t)$ е сигналът на грешката, Q – симетрична, положително определена матрица, $f(z)$ – функция, описваща изходния закон на управлението, реализирана от регулатора, $z(t)$ – постъпващият в регулатора сигнал. Необходимо е да се определи структурата на регулатора, минимизиращ горния функционал върху множеството откази на системата, т.е. осигуряващ асимптотична устойчивост на решението. Структурата на системата, позволяваща да се реши поставената задача е показана на фиг.1.



фиг.1. Обобщена структура на отказоустойчива система

Блокът на обратната връзка формира управляващи сигнали $z(t)$ и $v(t)$, първият от които компенсира параметричните смущения върху обекта, а вторият осигурява изключване на отказали датчици и изпълнителни органи и включване на резервни. При това могат да бъдат решени следните три задачи:

1. В зависимост от сигнала на грешката $e(t)$ се установява фактът за наличие или отсъствие на отказ на системата, като нейното номинално състояние се възпроизвежда например чрез метода на наблюдателя на Люенбергер [1].

2. С помощта на алгоритъм за разпознаване се определя видът на отказа [3].

3. След диагностиране на системата [3,4] се осъществява компенсация на отказите, т.е . синтезират се управляващите сигнали $z(t)$ и $v(t)$, осигуряващи устойчивост на системата в пространство на състоянията.

Сигналът, постъпващ на входа на регулатора, се формира във вида:

$$z(t) = \boldsymbol{K}^{\mathrm{T}} e(t),$$

където $\boldsymbol{K}^{\mathrm{T}}$ е векторът на параметрите. На базата на прекия метод на Ляпунов, за който в качеството на функция на Ляпунов се избира посочения по-горе функционал на качеството, може да се определи областта на допустимите стойности на $\boldsymbol{K}$, зависеща от отказа, и да се избере стойност от тази област.

В пространство на състоянията на системата отказът може да се свърже със загубата на устойчивост на системата. Тогава с оглед количествената оценка на безопасността, подобно на определянето на понятието информация в техническите системи като вероятност, с която заема известно състояние на физическа система, безопасността на системата може да се оцени чрез вероятността за това, че състоянието на системата ще принадлежи към множеството допустими състояния и едновременно ще се изпълняват условията, гарантиращи техния устойчив характер, т.е.:

$$p_{\text{без}}(t) = p\,(X \in X_{\text{доп}}\,,\ \text{Real}\ \rho_i < 0;\ i=1,\ldots,n)$$

където $X_{\text{доп}}$ е множеството от допустими състояния на системата, а Real $\rho_i < 0$ са условия, определящи устойчивостта на състоянията.

Както е известно, линейните преобразувания съответстват на вариации на структурата на системата, определена чрез матричен модел в пространство на състоянията. Инвариантите на матрицата на състоянието определят условията за физическа реализуемост. Съвкупността на инвариантите в определен момент характеризира напълно състоянието на системата. И съответно, на всяка траектория в пространство на състоянията отговаря съвкупност от стойности на инвариантите на матрицата на състоянията. Предложената оценка за безопасността може да се свърже с необходимите стойности на инвариантите I_i $(i=1,\ldots n)$. Но тъй като всяка функция на

инвариантите също е инвариант, то проблемът за оценка на безопасността може да бъде формулиран като условие за това, че определена функция на величините I_i, т.е. $S=f(I_1, I_2, ..., I_n)$ трябва да приема с определена точност стойности от зададена област, а задачата за количествено определяне на безопасността се свежда до определяне на вероятността за изпълнение на това условие [1].

В заключение може да се подчертае, че еднозначното описание на свойствата на произволна система е еквивалентно на намирането на съответните инварианти на съответния матричен модел в пространство на състоянията на системата. Инвариантите винаги отразяват реално съществуващите свойства и отношения, общи за цялото разнообразие от технически системи от даден тип. Във връзка с това изключително актуално е по-нататъшното развитие на теоретичните и приложните изследвания на задачата за алгоритмично осигуряване на отказоустойчивостта на системите за автоматично управление.

Литература

1. Андонов, А.В. Проблемът за функционалната устойчивост на системите за подвижна радиовръзка. С., ВВТУ, 1996. 128 с.

2. Андонов, А. В., З.В. Хубенова. Проблемът за безопасността на функциониране на автоматичните системи в техническата кибернетика. - В: Сб. Научни трудаве на ВВТУ, 1989.

3. Андонов, А. В. Диагностика на откази в микропроцесорни системи с високи изисквания за надеждност и безопасност при откази. IV научно-приложна конференция с межд. участие " Приложение на ЕИМ и микропроцесорна техника в ж.п. транспорт", 1987.

4. Гришин, Ю.В. Динамические системы устойчивые к отказам. М., Радио и связь, 1985.

5. Иванов, Е.Б. Основи на автоматиката и телемеханиката в ж.п. транспорт.С., ВВТУ, 1991.

Постъпила на 21. I. 1997 г.

Modelling and evaluation of the safety of the functioning of an electroninc system for a moving objects control

Antonio Andonov, Zoja Hubenova

(Summary)

In this paper the methds for providing the safety of the functioning of systems for a moving objects control in real time, in the aviation and the rail transport, are studied. The similarity and diferences among these sastems are analysed. A general method for modelling and evaluation of the safety is elaborated based on the contemporary automatic control theory (the methods of the states space). The condision and requirements concerning the automatic control systems are definited by making possible its functioning as a safety system. A proposal of a criterion for quantitative evaluation of the degree of safety in the systems functioning is made.