Pavol Tomašov - Karol Rástočný - Jiří Zahradník *

ČASTI MODELU INFORMAČNÝCH A ZABEZPEČOVACÍCH SYSTÉMOV

PARTS OF MODEL OF INFORMATION AND SAFETY SYSTEMS

Modelovacie techniky pre rozsiahle a zložité systémy sa vyberajú s ohľadom na očakávaný výsledok modelovania. Pre rutinný postup syntézy vo väčšine prípadov postačí skúsenostný prístup. Model systému s exaktným opisom jeho atribútov vyžaduje aplikáciu niektorých teoretických záverov. Pre informačné a zabezpečovacie systémy je zvolený model, vychádzajúci z teórie informácií. Tento model možno ďalej precízovať pomocou systémovej a nakoniec obvodovej teórie. V predkladanom článku sú opísané dva nástroje aparátu teórie informácií pre spracovanie modelu systému. Ide o vyjadrenie nerovnosti pre spracovanie informácií a o kvantifikáciu chýb pri manipulácii s informáciou.

Úvod

Pri analýze a syntéze informačného a zabezpečovacieho systému existujú dva základné postupy:

- pre dohodnuté funkcie sa vyberá štruktúra technických a programových prostriedkov systému na základe skúseností projektanta z predošlých aplikácií. Výber je závislý od technologickej úrovne komponentov systému a od celkovej sumy, ktorú je odberateľ ochotný zaplatiť. Úloha riadenia systému je zložená zo „štandardných elementov“,
- podrobne sa špecifikujú požadované funkcie systému vo väzbe na riadený systém bez ohľadu na budúcu skladbu HW a SW komponentov. V ďalšom kroku sa vytvorí model funkcií, na ktorom sa definuje úloha riadenia ako čiastková úloha radenia primárneho procesu. Pri tvorbe modelu funkcií možno zobrať za základ niektorý z referenčných modelov, ak ide o obvyklý sortiment služieb. Pre osobitný sortiment služieb treba vykonať podobný postup, aký sa použil pri tvorbe referenčných modelov. Účinným prostriedkom je vrstvenie funkcií. Tento postup umožňuje rozklad úlohy syntézy na jednoduchšie moduly (vrstvy funkcií). Ak sa vyrieši spolupráca vrstiev, možno pri syntéze použiť postup, známy z objektového programovania. Na realizáciu funkcií vrstiev sa v poslednej fáze vyberú HW a SW komponenty. Charakteristiky vykonávania funkcie vrstiev (časové, objemové, spoľahlivostné, bezpečnostné, ...) sú závislé od tech-

Modelling techniques for large and composite systems are chosen with regard to the expected result of modelling. For routine procedure of synthesis the empirical method is sufficient in most cases. System model with exact description of its attributes demands application of some theoretical conclusions. For information and safety systems a model derived from Information theory is selected. This model can then be specified with the help of the system and, eventually, circuit theory. In the presented paper two tools of Information theory apparatus for model system processing are described. They express information processing inequality and quantification of faults occurring by information manipulation.

Introduction

When analysing and synthesising an information and safety system two ground lines exist:

- for denominated functions a structure of technical and program elements of the system is selected based on a designer's experience from the last application. The selection depends on technology level of system components and on general sums which the customer is willing to pay. The task of system control consists of "standard elements",
- the demanded functions of the system are thoroughly specified in connection with the controlled system regardless of the future composition of HW and SW components. In the next step the function model is created on the basis of which a control task is defined as a partial task of the primary process control. When creating a function model it is possible to use some of the reference models as a basis provided that a usual range of services is demanded. For a special range of services a similar procedure to the one used during the creation of reference models, has to be performed. The interleaving of functions is an effective tool. This procedure enables decomposition of synthesis responsibilities on simple modules (layers of the functions). Provided that the co-operation of the layers is solved, the procedure well-known from the object programming can be used in the synthesis. HW and SW components are chosen for

* [1]Prof. Ing. Pavol Tomašov, PhD., [2]Doc. Ing. Karol Rástočný, PhD., [3]Doc. Ing. Jiří Zahradník, PhD.
[1]University of Žilina, Faculty of Electrical Engineering, Veľký diel NF, SK-01026 Žilina, Slovak Republic,
Tel.: +42-89-5133262, Fax:+421-89-652241, E-mail: tomas@fpedas.utc.sk
[2]Tel.: +42-89-5655559, Fax: +421-89-652241, E-mail: rastoc@fel.utc.sk
[3]Tel.: +42-89-5655559, Fax: +421-89-652241, E-mail: zahra@fel.utc.sk

nologického stupňa použitých komponentov a od „šikovnosti“ vytvorenia modelu funkcií.

V mnohých aplikáciách je postačujúci prvý postup. V zložitých a rozsiahlych informačných systémoch sa niekedy vyžaduje osobitný sortiment služieb. Príkladom sú zabezpečovacie systémy, použité pri riadení kritických procesov. Typickým kritickým procesom je dopravný proces. Pri výskyte poruchy v riadení takého systému môže dôjsť k stratám na majetku, zdraví alebo živote. Porucha, ktorá vyvolá nebezpečný stav, môže byť aj produktom použitého systému. Je zrejmé, že funkcie takéhoto systému treba špecifikovať druhým z uvedených postupov. Skupinu funkcií v jednotlivých skupinách (vrstvách) treba zostaviť tak, aby bola zaručená stabilita, kauzalita a bezpečnosť. Výsledkom špecifikácie funkcií celého systému má byť „safety case“ pre konkrétnu aplikáciu.

Činnosť informačného aj zabezpečovacieho systému môže byť rozložená na štyri základné druhy služieb: získavanie, úschova, prenos a transformácia relevantných, aktuálnych a garantovaných informácií (obr. 1). Každá z čiastkových služieb je spojená so štruktúrou HW a SW prostriedkov, ktoré vykonávajú „technológiu“ príslušných operácií. Aby systém poskytoval požadovaný sortiment služieb, musia byť elementy služieb zostavené do sekvencií, ktorých vykonávanie je riadené. Charakteristiky vykonávania funkcií sú silne závislé aj od spôsobu riadenia. Už pri zostavovaní sekvencie čiastkových služieb musí byť zohľadnený technologický stupeň elementov systému. Napríklad výkonnosť počítačovej siete ovplyvňuje distribuovanosť DB systémov, spôsob a intervaly aktualizácie replík DB, atď. Jadrom tejto tézy je vytvorenie riadiaceho postupu, ktorý začína rozkladom služieb systému na primitívy, a končí špecifikáciou protokolu a stanovením príslušného formalizmu na jeho konštrukciu.

Za jadro problému analýzy a syntézy informačných a zabezpečovacích systémov s osobitným sortimentom služieb možno považovať zostavenie modelu, ktorý pokryje čo najväčšie množstvo funkcií a stavov systému. V predkladanom článku je pokus o jednotiaci prístup k modelovaniu takých systémov s využitím niektorých prvkov teórie informácií.

Výber nástrojov pre modelovanie úlohy riadenia

Výber modelovacích techník pre doterajšie technologické stupne informačných a zabezpečovacích systémov vychádza zo skúsenostného postupu. Tento prístup pokrýval takmer všetky požiadavky na riešenie úloh syntézy a analýzy. Išlo napríklad o modely funkcií, model dátových tokov, entitno-relačný model, protokolový model, model porúch a ďalšie modifikované modely. Tieto modely sa dajú zvládnuť špecializovanými programovými balíkmi, takže sú v praxi aj dostatočne efektívne. Majú však aj spoločnú nevýhodu, ktorá obmedzuje ich použitie a efektívnosť pre informačné a zabezpečovacie systémy posledného technologického stupňa. Touto nevýhodou je fakt, že v reťazi: Teória informácií, Teória systémov, Teória riadenia, Teória obvodov, vynechávajú závery teórie informácií, teórie systémov a niektoré aj závery teórie

the realisation of layer functions in the last phase. Characteristics of layer functions execution (up to date, performance, reliability, safety, ...) depend on a technological degree of service components and on the skill of function model creation.

In many applications the first procedure is sufficient. Sometimes a special range of services is demanded in the composite and extensive information systems. An example is the safety systems used for critical processes control. Transportation process is a typical critical process. When a failure occurs in the control of such a system, it may lead to the loss of property, health, or life. The failure that invokes a danger state can be a product of the used service system, too. It is evident that functions of such a system need to be specialised by the second procedure. The function group in single groups (layers) has to be formed in such a way that it guarantees stability, causality and safety. The result of function specification of the whole system has to be the „safety case“ for concrete application.

The activity of information and safety system can be divided into four basic kinds of services: *obtaining, safekeeping, transmission and transformation* of relevant, current and guaranteed information (Fig. 1). Each of the partial services is connected with the structure of HW and SW means performing competent operation “technology“. To enable the system to offer the required range of services the service elements have to be formed into sequences, whose execution is controlled. Characteristics of functions execution are strongly dependent on the kind of control, too. Even when forming the partial services sequence the technological degree of system elements has to be respected. For example the efficiency of computer network is influenced by the level of distribution of DB system, the way and time interval of actualisation of DB replicas, etc. The core of this thesis to create a control procedure, which begins by with decomposition of system services to primitives, and ends by with protocol specification and with estimating the competent formalism on its construction.

Formation of the model that covers the greatest possible number of functions and system states is considered to be the main problem of analysis and synthesis of information and safety system with special range of services. In our paper we try to present a unifying approach to modelling such systems using some elements of information theory.

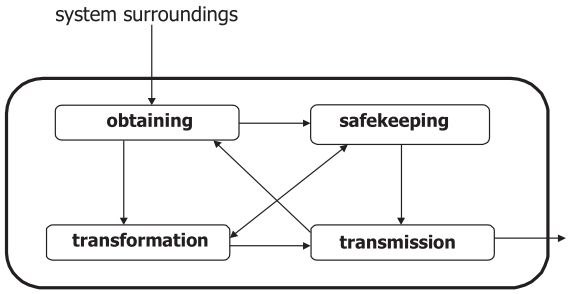
Selection of tools for modelling of control task

The selection of modelling techniques for up to present technological degrees of information and safety systems is based on empirical method. This approach covered almost all of the requirements for solution of synthesis and analysis tasks. Examples include: function models, data flow model, entity-relational model, protocol model, failure model and further modified models. These models can be managed by special software packets, and thus they are sufficiently effective even in praxis. However they all have a shared disadvantage which limits their application and effectiveness for information and safety systems of the last technological degree. In the chain of the Information theory System theory Control theory Circuit theory, all mentioned models fall to

riadenia. Pre rozsiahle a zložité systémy by sa mali modelovacie techniky doplniť najmenej o informačný model. Informácia je pre všetky takéto systémy primárnym „substrátom“, s ktorým sa v systéme manipuluje. Informačný model má preto ambície byť jednotiacim pre doterajšie jednoúčelové modely.

Zabezpečovací systém je podmnožinou informačného systému. Jeho úlohou je narábanie s informáciou (akvizícia, transformácia, prenos a úschova) osobitným spôsobom, odlišne od ostatných podobných činností v informačnom systéme. Otázky štruktúry a správania zabezpečovacieho systému možno rozložiť na riešenie jeho základných procesov.

Na opis systému (štruktúra a správanie) bez započítania dynamiky jeho stavov možno použiť statickú štrukturálnu funkciu. Ak je systém zložený z nezávislých a nekorelovaných elementov, ide o monotónnu štrukturálnu funkciu. Opis systému platí pre vybranú dvojicu jeho stavov (napríklad prevádzkový bezpečný stav a stav s nebezpečnou poruchou).



Obr. 1 Základné operácie pri manipulácii s informáciou
Fig. 1 Basic operations at manipulating with information

Od štrukturálnej funkcie možno prejsť jednoducho k pravdepodobnostnej funkcii, ktorá opisuje pravdepodobnosť jednotlivých stavov systému v niektorom bode časovej osi.

Asi za najdôležitejší model možno považovať ten, ktorý opisuje zabezpečovací systém v procese jeho starnutia. Takýto model musí dovoliť výber rozdelenia pravdepodobnosti výskytu príslušného náhodného parametra (poruchy) a výpočet pravdepodobnosti výskytu zvoleného stavu v potrebnom časovom intervale.

Zabezpečovací systém je súčasťou (subsystémom systému riadenia železničnej dopravy. Pri riadení dopravného procesu možno rozlíšiť tri hierarchické úrovne: procesnú, operatívnu a manažérsku. Riziko vzniku nebezpečenstva je najväčšie na procesnej úrovni. Na tomto riziku sa podieľajú všetky časti systému riadenia dopravy. Zabezpečovací systém má v tomto ohľade významný podiel, pretože stanovuje („vypočítava“) väčšinu povelov na zmenu stavu dopravného procesu. Ak je povel korektný, ide o prevádzkový stav. Ak z nejakých príčin dôjde k nesprávnemu vytvoreniu alebo interpretácii povelu na zmenu stavu, ide o poruchový stav. Tento stav môže, ale nemusí viesť k realizácii ohrozenia, pri ktorom vznikajú škody na majetku, zdraví, živote a životnom prostredí.

Úroveň bezpečnosti preto musí byť odvodená od prípustnej (akceptovateľnej) miery ohrozenia dopravného procesu. Táto úroveň je závislá od chránenej hodnoty a od intenzity dopravného procesu.

Predpokladajme v prvom priblížení, že existuje mechanizmus rozdelenia rizika medzi zabezpečovací systém a ostatné subsystémy riadenia dopravy. Potom možno hovoriť o úrovni bezpeč-

include the conclusions of Information theory System theory and some of them even the conclusions of Control theory. Modelling techniques for large and composite systems should be enlarged by the data model at least. For all information is such systems the primary “sub-slope“ which the system manipulates with. Information model has therefore an ambition to be the unifying one for present special purpose models.

Safety system is a subset of the information system. Its task is to handle the information (acquisition, transformation, transmission and safekeeping) in a specific way, different from other similar activities in the information system. Questions of the structure and behaviour of the safety system can be divided into solution of its basic processes.

Stationary structural function can be used to describe the system (structure and behaviour) without including dynamics of its states. If the system contains independent and non correlated elements, it is a monotonous structural function. Description of the system is valid for a chosen pair of its states (the safe operating state and dangerous failure state).

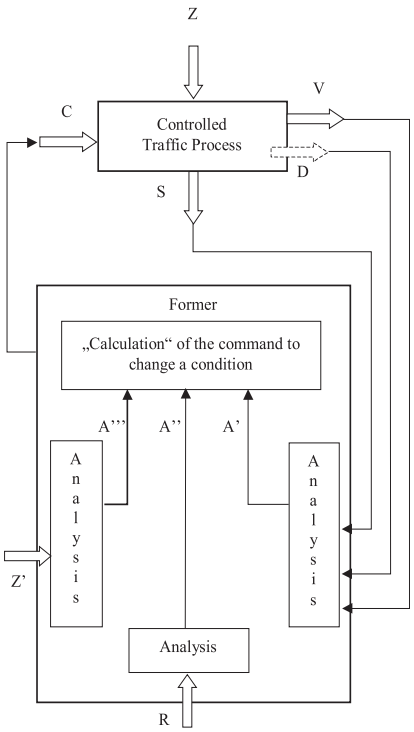
It is simple to pass from structural function to probability function, which describes the probability of single system state at some point of the time axis.

As the most important model can be regarded the one that describes the safety system in its ageing process. Such a model has to permit the selection of probability distribution of occurrence of competent random parameter (failure) and calculation of appearance probability of a chosen state in the necessary time period.

The safety system is a part (subsystem) of the railway traffic control system. In the control of the traffic process three hierarchical levels can be distinguished: procedural, operational and managerial. The highest risk of hazard occurrence exists on the procedural level. This risk is shared by all parts of the traffic control system. A significant role is played by the safety system since it sets (“calculates“) most of the commands given to change the conditions of the traffic process. Provided the command is correct, it results in an operational state. The state is considered faulty if for any reason the command given to change the condition is made incorrectly or misinterpreted. Such a condition can lead (but not in all cases) to an accident which damages property, health, lives and environment. The safety level must therefore be derived from the acceptable hazard rates for the traffic process. This level depends on the protected value and on the traffic process intensity.

Let us first assume that there is a mechanism of risk distribution between the safety system and other subsystems of the traffic control. Then the safety level of the safety system can be regarded as the level of risk of incorrect production and

nosti zabezpečovacieho systému ako o miere, ktorou sa dá vyjadriť riziko nesprávneho vytvorenia a nesprávnej interpretácie tých povelov, ktoré vytvára zabezpečovací systém. Za nesprávne vytvorenie povelu sa pritom považuje aj vytvorenie povelu správnym postupom, ale na podklade nesprávnych vstupných veličín pre jeho vytvorenie. Základná schéma jednostupňového riadenia procesu je na obr. 2.



Legend:
C – the space of control quantities
Z – the space of external effects
V – the space of output quantities
S – the space of state quantities
D – the space of diagnostic quantities
A – the space of the output quantities of the analyser
R – the space of order quantities
Z’ – the space of interference quantities

Obr. 2 Základná schéma jednostupňového riadenia procesu.
Fig. 2 The principal scheme of one-stage control process

Pre úlohy analýzy a syntézy systému s definovanou úrovňou bezpečnosti treba stanoviť postupy na zaistenie správania sa systému vo všetkých jeho predvídateľných stavoch. Tieto postupy sa realizujú cez ochranné mechanizmy zabezpečovacieho systému. Ochranné mechanizmy systému musia zaistiť, že aj v prípade výskytu poruchy systém vykonáva svoje funkcie presne podľa vopred definovaného algoritmu. Opatrenia na zaistenie takéhoto správania sa systému možno aplikovať na systémovej úrovni a na úrovni funkčných jednotiek a prvkov systému. Na systémovej úrovni ide predovšetkým o voľbu vhodnej štruktúry systému. Opatrenia na úrovni funkčných jednotiek a prvkov sú zamerané najmä na detekciu poruchy a negáciu jej účinkov.

Klasifikácia chýb

Zabezpečovací systém sa podieľa na týchto operáciách schémy riadenia podľa obr. 2.:
- získavanie veličín V, D, R, S,
- analýza veličín R, Z′, V, D, S,
- tvorba veličín C,
- prenos potrebných veličín medzi dvoma miestami.

Pri všetkých týchto operáciách môže vzniknúť chyba. Chyby vedú k nesprávnemu vytvoreniu riadiacej veličiny C (povelu na zmenu stavu), alebo k nesprávnej interpretácii riadiacej veličiny (prechod do nepríslušného stavu v priestore veličín S). Pre definovanie úrovne bezpečnosti treba tieto chyby klasifikovať a nájsť opatrenia na zaručenie akceptovateľného výskytu (pravdepodobnosti alebo intenzity) nezistených, alebo neošetrených chýb.

misinterpretation of the commands produced by the safety system. Commands resulting from a correct procedure but using incorrect input quantities are also considered incorrect commands. The principal scheme of the one-stage process control is shown in Fig. 2.

For the tasks of analysis and synthesis of the system with a defined level of safety the procedures ensuring the behaviour of the system in all its predictable states must be defined.

These procedures are realised through the defence mechanisms of the safety system. They have to ensure fulfilling of the demanded functions according to the pre-defined algorithm even in the case of failure. Precautions taken to ensure such system behaviour can be applied on the system level as well as on the level of functional units and system components. On the system level the choice of the appropriate system structure is involved above all. Precautions taken on the level of functional units and components aim mainly at fault detection and negation of fault effects.

Fault Classification

The safety system takes part in the following operations of the control scheme shown in Fig. 2:
- Obtaining V, D, R, S quantities
- Analysing R, Z′, V, D, S quantities
- Producing C quantities
- Transmission of required quantities between 2 places.

A fault may occur in all of these operations. Faults result in an incorrect production of the control C quantity (the command for a change of state) or in misinterpretation of the control quantity (transition to an unauthorised state in the area of S quantities). To define the safety level these faults must be classified and precautions that can guarantee acceptable occurrence (probability or rate) of unidentified or unattended faults must be taken.

Všetky časti zabezpečovacieho systému, ktoré získavajú veličiny V, D, R, S, analyzujú veličiny R, Z′, V, D, S, vytvárajú veličiny C a podieľajú sa na prenose všetkých veličín riadeného systému, možno takmer bez výnimky považovať za nejakú podobu konečného automatu (KA). Chyby, ktoré môžu vzniknúť v činnosti KA, možno klasifikovať do tried:

a) chyby v jazyku,
b) chyby v prenose zo vstupu na výstup KA,
c) chyby formátu,
d) chyby správania (kauzality vykonávania čiastkových funkcií),
e) chyby poskytovania služby vyššiemu systému (chyby kauzality služieb).

Na kompletný opis systému treba zostaviť model, ktorý okrem uvedených skutočnosti umožní zarátať aj účinky operačného prostredia, teda kombinovať dva a viac náhodných procesov, ktoré môžu mať rozdielny charakter rozdelenia pravdepodobnosti.

Ak predpokladáme, že stavy objektu sa dajú opísať ako náhodné premenné, potom možno s výhodou použiť aparát teórie informácií na vytvorenie charakteristík toku porúch (pri analýze), alebo na opis modifikácie takého toku (pri syntéze). Ide o nasledujúce časti informačnej teórie.

Stavy objektu ako náhodné premenné:

Nech sú stavy objektu považované za náhodné premenné X_1, X_2, ... X_n. Ich vlastnosti sú dostatočne opísané funkciou rozdelenia pravdepodobnosti $p(x_1, x_2, ... x_n)$. Premenné $X_1, X_2, ... X_n$ môžu byť identicky rozdelené podľa niektorého typu rozdelenia pravdepodobnosti. Môžu byť nezávislé, podmienene závislé, alebo štatisticky závislé. Pri známom rozdelení pravdepodobnosti náhodných premenných sa dá stanoviť entropia stavov objektu.

Entropia umožňuje opísať objekt v potrebnej forme, napríklad pri tvorbe kódu, ktorým je opísaný celkový stav objektu.

Opis stavov objektu pomocou nerovnosti pre spracovanie dát

Predpokladajme, že stavy objektu tvoria Markovovu reťaz. Nerovnosť pre spracovanie dát sa použije na demonštráciu, že žiadna „šikovná“ manipulácia s údajmi nemôže zlepšiť výpočet stavových charakteristík.

Definícia: Náhodné premenné *X*, *Y*, *Z* tvoria Markovovu reťaz v tomto poradí, ak podmienené rozdelenie *Z* závisí len od *Y* a je podmienene nezávislé od *X*. Premenné *X*, *Y*, *Z* tvoria Markovovu reťaz $X \rightarrow Y \rightarrow Z$, ak spoločná pravdepodobnostná funkcia sa dá napísať takto:

$$p(x, y, z) = p(x).\ p(y \mid x).p(z \mid y). \qquad (1)$$

Z toho vyplývajú niektoré jednoduché dôsledky:

- $X \rightarrow Y \rightarrow Z$ vtedy a len vtedy, ak *X* a *Z* sú podmienene nezávislé pre dané *Y*. Implicitne je v tom podmienená nezávislosť, pretože

All parts of the safety system that obtain V, D, R, S quantities, analyse R, Z′, V, D, S, quantities produce C quantities and take part in the transmission of all the controlled system quantities can be regarded (almost without exception) as a certain kind of the finite automaton. Faults that can occur in operation of the finite automaton may be classified into the following classes:

a) Language faults
b) Faults in transmission from the input to the output of the finite automaton
c) Format faults
d) Behaviour faults (faults in causality of performing partial functions)
e) Faults in providing services to the superior system (faults in service causality).

For a complete system description we need to create a model that, apart from the mentioned facts, enables to incorporate the effects of the operational surroundings as well- thus to combine two and more random processes, which can have different character of probability distribution.

Supposing that the object states can be described as random variables, the information theory apparatus can be conveniently used to create characteristics of fault flow (during analysis) or to describe the modification of such a flow (during synthesis). The following parts of information theory are involved.

Object states as random variables

Let the object states be regarded as the random variables X_1, X_2, ... X_n. Their characteristics are sufficiently described by the probability distribution function $p(x_1, x_2, ... x_n)$. Variables X_1, X_2, ... X_n can be identically sorted by some type of probability distribution. They can be independent, conditionally dependent or statistically dependent. When the probability distribution of the random variables is known, entropy of the object states can be estimated.

Entropy enables to describe the object in the necessary form, e.g. during the creation of the code, by which is the comprehensive object state described.

Let us suppose that object states create a Markov chain. The data processing inequality can be used to show that clever manipulation with the data cannot improve the computation of state characteristics.

Definition: Random variables *X*, *Y*, *Z* form a Markov chain in this order if the conditional distribution of *Z* depends only on *Y* and is conditionally independent from *X*. Specifically, variables *X, Y* and *Z* form a Markov chain $X \rightarrow Y \rightarrow Z$ if the joint probability mass function can be written as:

$$p(x, y, z) = p(x).\ p(y \mid x).p(z \mid y). \qquad (1)$$

Some simple consequences result:

- $X \rightarrow Y \rightarrow Z$ if and only if *X* and *Z* are conditionally independent for given *Y*. Markovity implies conditional independence because

$$p(x, y \mid z) = \frac{p(x, y, z)}{p(y)} = \frac{p(x, y)p(z \mid y)}{p(y)} = p(x \mid y).p(z \mid y) \quad (2)$$

Takto sú charakterizované Markovove reťaze, ktoré môžu byť rozšírené na definované Markovove polia. Sú to n-rozmerné náhodné procesy, v ktorých vonkajšok a vnútrajšok je nezávislý voči danej hranici.

- $X \rightarrow Y \rightarrow Z$ implikuje $Z \rightarrow Y \rightarrow X$. Tieto podmienky možno zapísať aj takto: $X \leftrightarrow Y \leftrightarrow Z$.
- Ak $Z = f(Y)$, potom $X \rightarrow Y \rightarrow Z$.

Teraz už možno dokázať dôležitú teorému, demonštrujúcu, že žiadne spracovanie Y (determinované alebo náhodné) nemôže zvýšiť informáciu, že Y vypovedá o X.

Teoréma 1: Ak $X \rightarrow Y \rightarrow Z$, potom $I(X;Y) \geq I(X;Z)$.

Dôkaz: Podľa reťazového pravidla môžeme rozšíriť vzájomnú informáciu dvoma spôsobmi:

$$I(X;Y,Z) = I(X;Z) + I(X;Y \mid Z) \quad (3)$$
$$= I(X;Y) + I(X;Z \mid Y). \quad (4)$$

Pretože X a Z sú podmienene nezávislé pre dané Y, je $I(X;Z \mid Y) = 0$. Pretože $I(X;Y \mid Z) \geq 0$, dostávame

$$I(X;Y) \geq I(X;Z). \quad (5)$$

Rovnosť platí vtedy a len vtedy, ak $I(X;Y \mid Z) = 0$, t. j. $X \rightarrow Y \rightarrow Z$ vytvára Markovovu reťaz. Podobne sa dá dokázať, že $I(Y;Z) \geq I(X;Z)$.

Dôsledok: Pre zvláštny prípad, ak $Z = g(Y)$, je $I(X;Y) \geq I(X;g(Y))$.

Dôkaz: $X \rightarrow Y \rightarrow g(Y)$ tvorí Markovovu reťaz. Funkcia $g(Y)$ nemôže zvýšiť informáciu o premennej X.

Dôsledok: Ak $X \rightarrow Y \rightarrow Z$, potom $I(X;Y \mid Z) \leq I(X;Y)$.

Dôkaz: Z rovnice (3) a (4) a použitím faktu, že $I(X;Z \mid Y) = 0$ a $I(X;Z) \geq 0$, dostávame $I(X;Y \mid Z) \leq I(X;Y)$

Závislosť X a Y je zmenšená (alebo aspoň nezmenená) pozorovaním „poklesu“ náhodnej premennej Z.

Všimnime si, že môže byť aj $I(X;Y \mid Z) \geq I(X;Y)$ vtedy, ak X, Y, Z netvoria Markovovu reťaz. Napríklad nech X a Y sú nezávislé lineárne náhodné premenné a nech $Z = X + Y$. Potom $I(X;Y) = 0$, ale $I(X;Y \mid Z) = H(X \mid Z) - H(X \mid Y,Z) = H(X \mid Z) = P(Z_{=1})$. $H(X \mid Z_{=1}) = 0{,}5$ bit.

Použitie chybovej nerovnosti pre analýzu bezpečnosti

Použitie chybovej nerovnosti je kľúčové pri rozbore bezpečnosti zabezpečovacieho systému a jeho elementov. Dá sa očaká-

$$p(x, y \mid z) = \frac{p(x, y, z)}{p(y)} = \frac{p(x, y)p(z \mid y)}{p(y)} = p(x \mid y).p(z \mid y) \quad (2)$$

This is the characterisation of Markov chains that can be extended to define Markov fields, which are n-dimensional random processes in which the interior and exterior are independent from the given values of the boundary.

- $X \rightarrow Y \rightarrow Z$ implies that $Z \rightarrow Y \rightarrow X$. Thus the condition is sometimes written $X \leftrightarrow Y \leftrightarrow Z$.
- If $Z = f(Y)$, then $X \rightarrow Y \rightarrow Z$.

We can now prove an important and useful theorem demonstrating that no processing of Y, deterministic or random, can increase the information that Y states about X.

Theorem 1: If $X \rightarrow Y \rightarrow Z$, then mutual information $I(X;Y) \geq I(X;Z)$.

Proof: According to the chain rule, we can expand mutual information in two different ways

$$I(X;Y,Z) = I(X;Z) + I(X;Y \mid Z) \quad (3)$$
$$= I(X;Y) + I(X;Z \mid Y). \quad (4)$$

Since X and Y are conditionally independent for the given Y, $I(X;Z \mid Y) = 0$. Since $I(X;Y \mid Z) \geq 0$, we get

$$I(X;Y) \geq I(X;Z). \quad (5)$$

Equality is valid if and only if $I(X;Y \mid Z) = 0$, i.e. $X \rightarrow Y \rightarrow Z$ forms a Markov chain. Similarly can be proven that $I(Y;Z) \geq I(X;Z)$.

Corollary: In specific case, if $Z = g(Y)$, we get $I(X;Y) \geq I(X;g(Y))$.

Proof: $X \rightarrow Y \rightarrow g(Y)$ forms a Markov chain. Function $g(Y)$ cannot increase the information about variable X.

Corollary: If $X \rightarrow Y \rightarrow Z$, then $I(X;Y \mid Z) \leq I(X;Y)$.

Proof: From (3) and (4), and using the fact that $I(X;Z \mid Y) = 0$ by Markovity and $I(X;Z) \geq 0$, we get $I(X;Y \mid Z) \leq I(X;Y)$

Thus the dependence of X and Y is decreased (or remains unchanged) by the observation of the decrease of random variable Z.

Note that it is also possible that $I(X;Y \mid Z) \geq I(X;Y)$ when X, Y and Z do not form a Markov chain. For example, let X and Y be independent linear random variables, and let $Z = X + Y$. Then $I(X;Y) = 0$, but $I(X;Y \mid Z) = H(X \mid Z) - H(X \mid Y,Z) = H(X \mid Z) = P(Z_{=1})$. $H(X \mid Z_{=1}) = 0{,}5$ bit.

Application of error inequality for analysing the safety

The application of error inequality is key-important when analysing safety system and its components. The estimation of X

vať, že odhad X (vybraného stavu objektu) je možný s malou pravdepodobnosťou chyby len vtedy, ak podmienená entropia $H(X|Y)$ je malá (Y je vyjadrenie pozorovaného stavu X cez prostredníka, ktorým môže byť signál na výstupe obvodu). Chybová nerovnosť túto myšlienku kvantifikuje.

Rozšírime dôkaz kódov s nulovou pravdepodobnosťou chyby aj na kódy s malou pravdepodobnosťou chyby. Novou zložkou bude chybová nerovnosť, ktorá stanovuje spodnú hranicu pravdepodobnosti chyby v pojmoch podmienenej entropie.

Index W je rovnomerne rozdelený na množine $W = \{1, 2, ..., 2n^R\}$ a sekvencia Y^n je pravdepodobnostne zviazaná s W. Zo sekvencie Y^n odhadujeme vyslaný index W. Nech je odhad $\hat{W} = g(Y^n)$. Definujme pravdepodobnosť chyby

$$P^{(n)}_e = Pr(\hat{W} \neq W). \tag{6}$$

Ďalej definujme

$$E = 1, \text{ak } (\hat{W} \neq W), \tag{7}$$
$$E = 0, \text{ak sa } \hat{W} = W.$$

Použijeme reťazové pravidlo pre entropiu na rozšírenie $H(E,W|Y^n)$. Dostaneme:

$$H(E,W|Y^n) = H(W|Y^n) + H(E|W,Y^n) \tag{8}$$
$$= H(E|Y^n) + H(W|E,Y^n). \tag{9}$$

Pretože E je funkciou W a $g(Y^n)$ musí byť $H(E|W,Yn) = 0$. Tiež $H(E) \leq 1$, pretože E je binárna náhodná premenná. Posledný termín $H(W|E,Y^n)$ možno ohraničiť takto:

$$H(W|E,Y^n) = P(E=0)H(W|(Y^n,E=0) + P(E=1)H(W|Y^n,E=1) \tag{10}$$
$$\leq (1-P^{(n)}_e\,(E=0) + P^{(n)}_e \log(W-1) \tag{11}$$
$$\leq P^{(n)}_e\, nR, \tag{12}$$

pretože pri danom $E = 0$, $W = g(Y^n)$ a keď je $E = 1$, môžeme dostať hornú hranicu podmienenej entropie. Kombinovaním týchto výsledkov dôjdeme k chybovej nerovnosti:

$$H(W|Y^n) \leq 1 + P^{(n)}_e\, nR \tag{13}$$

Pretože pre pevný kód je $X^n(W)$ funkciou W, platí

$$H(X^n(W)(Y^n) \leq H(W(Y^n)). \tag{14}$$

Lema: (chybová nerovnosť): Pre diskrétny kanál bez pamäti s kódovou knihou ξ a s rovnomerne rozdelenými vstupnými správami nech platí: $P^{(n)}_e = Pr(W \neq g(Y^n))$.

Potom je

$$H(X^n|Y^n) \leq 1 + P^{(n)}_e\, nR. \tag{15}$$

Teraz dokážeme túto lemu, ktorá ukazuje, že kapacita kanála na jeden prenos sa nezvyšuje, ak použijeme diskrétny kanál bez pamäti viackrát.

(chosen object state) with small error probability is possible only if the conditioned entropy $H(X|Y)$ is small (Y is the observed state of X expressed through an intermediary, which can be a circuit output signal). Error inequality quantifies this idea.

We now extend the proof that was derived for zero-error codes to the case of codes with very small error probability. The new ingredient will be error inequality, which defines a lower boundary of the error probability in terms of the conditional entropy.

The index W is uniformly distributed on the set $W = \{1, 2, ..., 2n^R\}$, and the sequence Y^n is probabilistically related to W. From Y^n, we estimate the index W that was sent. Let the estimation be $\hat{W} = g(Y^n)$. Let us define the error probability

$$P^{(n)}_e = Pr(\hat{W} \neq W). \tag{6}$$

Next, we define

$$E = 1, \text{ak } (\hat{W} \neq W), \tag{7}$$
$$E = 0, \text{ak sa } \hat{W} = W.$$

Then using the chain rule for entropies to expand $H(E,W|Y^n)$. we get

$$H(E,W|Y^n) = H(W|Y^n) + H(E|W,Y^n) \tag{8}$$
$$= H(E|Y^n) + H(W|E,Y^n). \tag{9}$$

Now, since E is a function of W and $g(Y^n)$, inevitably $H(E|W,Yn) = 0$. Also $H(E) \leq 1$, since E is a binary valued random variable. The remaining term, $H(W|E,Y^n)$, can be bounded as follows:

since by given $E = 0$, $W = g(Y^n)$, and when $E = 1$, we can get the upper boundary of the conditional entropy. Combining these results, we obtain error inequality:

$$H(W|Y^n) \leq 1 + P^{(n)}_e\, nR \tag{13}$$

Since for a fixed code $X^n(W)$ is a function of W,

$$H(X^n(W)(Y^n) \leq H(W(Y^n)). \tag{14}$$

Lema: (error inequality). For a discrete memoryless channel with a codeboock (and the input messages uniformly distributed, let $P^{(n)}_e = Pr(W \neq g(Y^n))$.

Then

$$H(X^n|Y^n) \leq 1 + P^{(n)}_e\, nR. \tag{15}$$

We will now prove this lema which shows that the channel capacity per one transmission is not increased if we use a discrete memoryless channel many times.

Lema: Nech Y^n je výsledok prispôsobenia X^n na diskrétny kanál bez pamäti. Potom

$$I(X^n;Y^n) \leq nC, \text{ pre všetky } p(x^n). \tag{16}$$

Dôkaz:

$$I(X^n;Y^n) = H(Y^n) - H(Y^n \mid X^n) \tag{17}$$

$$= H(Y^n) - \sum_{i=1}^{n} H(Y_i \mid Y_1, ..., Y_{i-1}, X^n) \tag{18}$$

$$= \sum_{i=1}^{n} H(Y^n) - \sum_{i=1}^{n} H(Y_i \mid X_i), \tag{19}$$

pretože podľa definície diskrétneho kanála bez pamäti Y_i závisí len od X_i a je podmienene nezávislé od všetkých ostatných. Pokračovaním série nerovností je:

$$I(X^n;Y^n) = H(Y^n) - \sum_{i=1}^{n} H(Y_i \mid X_i) \tag{20}$$

$$\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i \mid X_i) \tag{21}$$

$$= I(X_i;Y_i) \tag{22}$$

$$\leq nC, \tag{23}$$

kde (21) vyplýva z faktu, že entropia súboru náhodných premenných je menšia ako súčet ich individuálnych entropií. Výsledok (23) vyplýva z definície kapacity. Tým je lema dokázaná.

Teraz treba dokázať konverziu kódovacej teorémy.

Dôkaz: Máme ukázať, že akákoľvek sekvencia $(2^{nR},n)$ kódov so $\lambda^{(n)} \to 0$ musí mať $R \leq C$.

Ak sa maximálna pravdepodobnosť chyby blíži k nule, potom priemerná pravdepodobnosť chyby pre sekvenciu kódov sa tiež blíži k nule, t. j. $\lambda^{(n)} \to 0$ implikuje $P^{(n)}_e \to 0$, kde $P^{(n)}_e$ je definovaná ako priemerná pravdepodobnosť chyby pre kód (M,n): $P^{(n)}_e = \frac{1}{M} \sum_{i=1}^{M} \lambda_i$ Nech je pre každé n zobrazené W podľa rovnomerného rozdelenia cez $\{1, 2, ..., 2^{nR}\}$. Pretože W má rovnomerné rozdelenie, je $P^{(n)}_e = Pr(\hat{W} \neq W)$.

Preto je

$$nR = H(W) = H(W \mid Y^n) + I(W;Y^n) \tag{24}$$

$$\leq H(W \mid Y^n) + I(X^n(W);Y^n) \tag{25}$$

$$\leq 1 + P^{(n)}_e nR + I(X^n(W);Y^n)\, P^{(n)}_e \tag{26}$$

$$\leq 1 + P^{(n)}_e nR + nC \tag{27}$$

Po vydelení n bude:

$$R \leq P^{(n)}_e R + \frac{1}{n} + C \tag{28}$$

Pre $n \to \infty$ idú prvé dva členy na pravej strane k nule a preto

$$R \leq C. \tag{29}$$

Lema: Let Y^n be the result of passing X^n through a discrete memoryless channel. Then

$$I(X^n;Y^n) \leq nC, \text{ pre všetky } p(x^n). \tag{16}$$

Proof:

$$I(X^n;Y^n) = H(Y^n) - H(Y^n \mid X^n) \tag{17}$$

$$= H(Y^n) - \sum_{i=1}^{n} H(Y_i \mid Y_1, ..., Y_{i-1}, X^n) \tag{18}$$

$$= \sum_{i=1}^{n} H(Y^n) - \sum_{i=1}^{n} H(Y_i \mid X_i), \tag{19}$$

since by the definition of a discrete memoryless channel, Y_i depends only on X_i and is conditionally independent from everything else. Continuing the series of inequalities, we get

$$I(X^n;Y^n) = H(Y^n) - \sum_{i=1}^{n} H(Y_i \mid X_i) \tag{20}$$

$$\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i \mid X_i) \tag{21}$$

$$= I(X_i;Y_i) \tag{22}$$

$$\leq nC, \tag{23}$$

where (21) follows from the fact that the entropy of a collection of random variables is less than the sum of their individual entropies, and (23) follows from the definition of capacity. Thus we have proved that using the channel many times does not increase the information capacity in bits per transmission. We are now in position to prove the conversion to the channel coding theorem.

Proof: (conversion to channel coding theorem). We have to show that any sequence of $(2^{nR},n)$, codes with $\lambda^{(n)} \to 0$ must have $R \leq C$.

If the maximal probability of error is close to zero, then the average probability of error sequence of codes also goes to zero, i.e., $\lambda^{(n)} \to 0$ implies $P^{(n)}_e \to 0$, where $P^{(n)}_e$ is defined as average probability of error for an *(M,n)* code: $P^{(n)}_e = \frac{1}{M} \sum_{i=1}^{M} \lambda_i$.For each n, let W be drawn according to a uniform distribution, $P^{(n)}_e = Pr(\hat{W} \neq W)$.

Hence

$$nR = H(W) = H(W \mid Y^n) + I(W;Y^n) \tag{24}$$

$$\leq H(W \mid Y^n) + I(X^n(W);Y^n) \tag{25}$$

$$\leq 1 + P^{(n)}_e nR + I(X^n(W);Y^n)\, P^{(n)}_e \tag{26}$$

$$\leq 1 + P^{(n)}_e nR + nC \tag{27}$$

Dividing by n, we obtain

$$R \leq P^{(n)}_e R + \frac{1}{n} + C \tag{28}$$

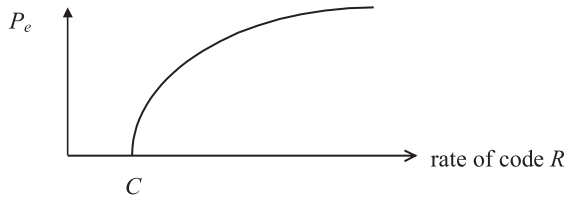
Now letting $n \to \infty$, we can see that the first two terms on the right hand side go to 0, and hence

$$R \leq C. \tag{29}$$

Takže po prepísaní (28) je

$$P^{(n)}_e \geq 1 - \frac{C}{R} - \frac{1}{nR}. \qquad (30)$$

Táto rovnica ukazuje, že ak $R > C$, pravdepodobnosť chyby sa vzdiaľuje od nuly so zväčšujúcim sa n. Preto sa pri takých rýchlostiach nedá dosiahnuť ľubovoľne malá pravdepodobnosť chyby (obr. 3).



Obr. 3 Dolná hranica pravdepodobnosti chyby
Fig. 3 Lower boundary of the error probability

Táto konverzia je slabou konverziou kódovacej teorémy. Dá sa dokázať aj silná konverzia, ktorá tvrdí, že pri zvyšovaní rýchlosti nad hodnotu kapacity sa pravdepodobnosť chyby blíži exponenciálne k 0,5. Hodnota kapacity je hraničným bodom, v ktorom sa pravdepodobnosť chyby mení.

Záver

V závere je formulovaný postup pre opis bezpečnosti z hľadiska pravdepodobnosti nebezpečnej poruchy ako pravdepodobnosti výskytu náhodnej premennej X_{ij}. Pravdepodobnosť $P(X_{ij})$ pritom znamená pravdepodobnosť prechodu objektu zo stavu i do stavu j. Stav X_i patrí do množiny bezpečných stavov, stav X_j patrí do množiny nebezpečných stavov. Pre obidve množiny stavov možno použiť aj jemnejšie delenie, pričom sa použije stromová štruktúra zobrazenia stavov do náhodných premenných.

- Bezpečnosť sa opisuje štruktúrou stavov. Túto štruktúru možno použiť na opis stavov celého objektu, alebo v hierarchickom usporiadaní na opis stavov jednotlivých prvkov , alebo funkcií objektu.
- Pre jednotlivé typy objektov (zabezpečovacích systémov, alebo dopravnej cesty ako celku) sa stanoví druh závislosti stavov, ktoré sú reprezentované náhodnými premennými. V prvom priblížení sa dá predpokladať, že náhodné premenné (stavy objektu) tvoria Markovovu reťaz.
- Pri manipulácii s náhodnými premennými treba rešpektovať fakty, vychádzajúce z nerovnosti pre spracovanie dát.
- Miera bezpečnosti objektu je závislá od pravdepodobnosti chybného odhadu náhodnej premennej X na základe znalosti premennej Y. Využitím chybovej nerovnosti sa dajú stanoviť požiadavky na logickú reprezentáciu zabezpečovacích funkcií.

Recenzenti: P. Peniak, L. Skyva

We can rewrite (28) as

$$P^{(n)}_e \geq 1 - \frac{C}{R} - \frac{1}{nR}. \qquad (30)$$

This equation shows that if $R > C$, the error probability is moving away from 0 for sufficiently large n. Hence we cannot achieve an arbitrarily low error probability at rates above capacity. This inequality is illustrated in Fig. 3.

This conversion is a weak conversion of the channel coding theorem. It is also possible to prove a strong conversion, which states that for the rates above capacity, the error probability nears exponentially to 0,5. Hence, the capacity is a very clear dividing point in which the error probability is changing.

Conclusion

In the conclusion a procedure for description of safety from the point of dangerous error probability as a probability of random variable Xij appearance is formulated. Probability P(Xij) means the probability of transition of the object from state i to state j. State Xi belongs to the set of safe states, state Xj belongs to the set of hazardous states. For both sets of states a more precise division can be used, by which a tree-type structure of displaying states into random variables is used.

- safety is described by the states structure. This structure can be used to describe states of the whole object, alternatively in hierarchical order to describe the state of single elements, or object functions.
- for individual object types (safety system, or transport route as a whole) a state dependency type is determined (of the states represented by random variables). In the first approach it can be assumed, that random variables (object states) create Markov chain.
- when manipulating with random variables, facts concluding from data processing inequality have to be respected.
- the rate of object safety depends on the probability of a wrong estimation of the random variable X based on knowing the variable Y. By using the error inequality the requirements for logical representation of safety functions can be estimated.

The paper was elaborated with the support of grants VEGA 1/5230/98 and 1/5255/98.

Reviewed by: P. Peniak, L. Skyva