Architektury systémů pracujících se zvýšenými požadavky na bezpečnost

Luděk Elis, Kamil Kosturik
Katedra aplikované elektroniky a telekomunikací
Fakulta elektrotechnická
Západočeská univerzita v Plzni
ludaelis@kae.zcu.cz, kosturik@kae.zcu.cz

The Architectures of the Systems for Increased Safety Requirements

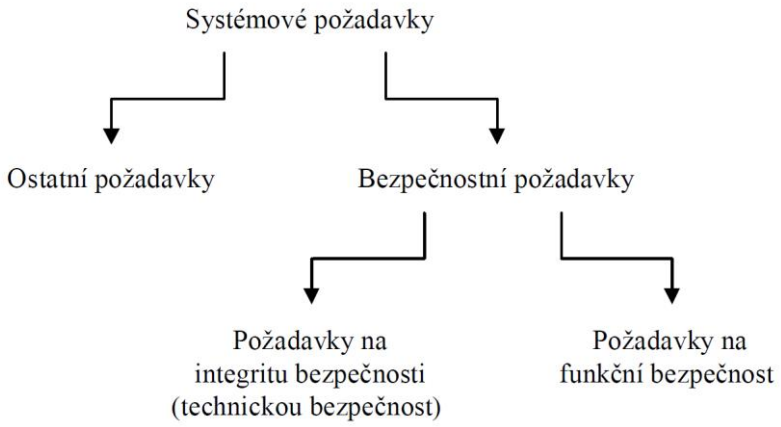
Abstract – **This paper deals with the structures and the architectures of the safety related systems. The assignment of architecture, which is related to the application of the system, belongs to one of the most important parts of the equipment design. The most used architectures 1oo2, 2oo2 and 2oo3 are briefly described. This article discusses the basic characteristics, features and abbreviated designation of mentioned architectures. The conclusion points out the difference of the abbreviated designation and meaning of individual structures.**

Keywords – Safety Requirements; Architecture; Safety System; 1oo2; 2oo2; 2oo3; Inherent Fail-Safety; Reactive Fail-Safety; Composite Fail-Safety; ČSN EN 61508

I. ÚVOD

Při návrhu systémů určených pro aplikace vyžadující zvýšené nároky na bezpečnost je nutné zohlednit řadu faktorů, které ovlivňují celkovou spolehlivost, pohotovost a především bezpečnost výsledného zařízení. Bezpečnost je nutné vztahovat k jednotlivým krokům vývoje a také k cílovému použití systému. Obecně lze říci, že čím jednodušší je navržené bezpečné zařízení pro konkrétní aplikaci, tím je účinnější.

Návrhu zařízení předchází koncept a také specifikace požadavků zahrnující požadavky na funkční a technickou bezpečnost, požadavky na integritu bezpečnosti a ostatní požadavky.



Obrázek I. **Rozdělení systémových požadavků**

Po schválení specifikace je vytvořen koncept systému. Koncept popisuje vyvíjený systém na úrovni blokových diagramů, definuje rozhraní uživatele a procesu, výkonové napájení, komunikační spoje mezi kanály, strukturu softwaru se stavovými diagramy, ale především určuje architekturu systému.

Architektura definuje vnitřní strukturu systému, neboli složení základních stavebních a funkčních částí tvořící jádro bezpečného systému. Obecná norma pro bezpečnost ČSN EN 61508 [1] definuje několik základních architektur, které se používají pro konkrétní aplikace, případně jejich kombinace nebo modifikace. Jelikož je na půdě ZČU rozsáhlá znalost zabezpečovací techniky, je zde uveden pohled na architektury definované normou pro zabezpečovací techniku ČSN EN 50129 [3].

II. STRUKTURY SYSTÉMŮ

Obecně je možné struktury systémů rozdělit do třech základních skupin. Toto rozdělení vychází především ze zabezpečovací techniky, která se v české republice řadí k těm více zkoumaným oblastem (viz například [2]).

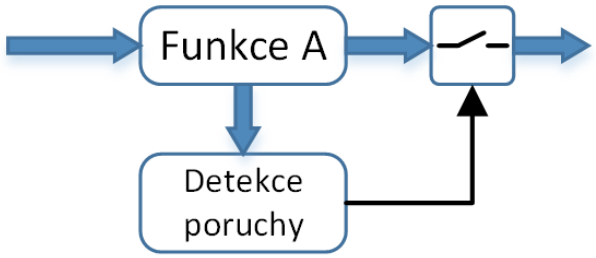
A. systémy s vnitřní bezpečností

Jak už samotný název napovídá, jedná se o zařízení, která jsou složena jen z několika málo prvků, nebo dokonce pouze z jediného prvku. Navíc nesmí žádná z uvažovaných poruch zařízení vyvolat hazardní stav. Lze tedy připustit, že v systému se mohou vyskytnout chyby, ale vždy musejí přejít do bezpečného stavu.

Typickým příkladem je relé 1. bezpečnostní skupiny, které tvoří základní stavební prvek železničních zabezpečovacích systémů s vnitřní (vestavěnou) bezpečností a jenž má zaručený odpad kotvy při poruše.

B. reakční systémy

V reakčních systémech jsou funkce související s bezpečností prováděny pouze jedním zařízením a samy o sobě nemusí plnit požadavky na bezpečnou konstrukci. Bezpečnost zařízení je zajištěna rychlou detekcí hazardního stavu a následným převedením výstupu do bezpečného, jak ukazuje následující obrázek.

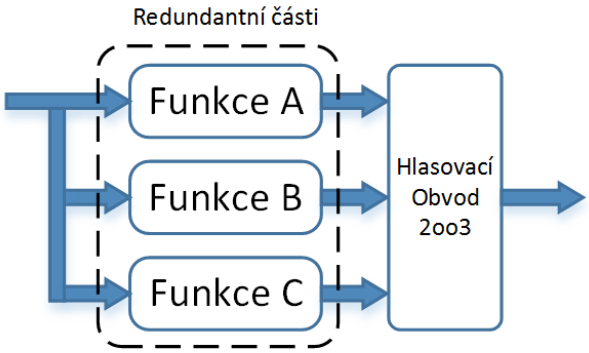


Obrázek II. **Struktura reakčního systému**

Pro detekci hazardních stavů lze použít různé diagnostické nástroje využívající kontinuální testy, různé způsoby kódování nebo několikanásobné výpočty s následnou komparací výsledků. Nevýhodou reakčních systémů je fakt, že na výstupu systému se na přechodnou dobu může objevit hazardní stav a je nutno s ním při návrhu počítat.

C. *Redundantní systémy*

Redundantní systémy zajišťují bezpečnost pomocí nadbytečnosti v části zpracování informace a následnou komparací všech výsledků.



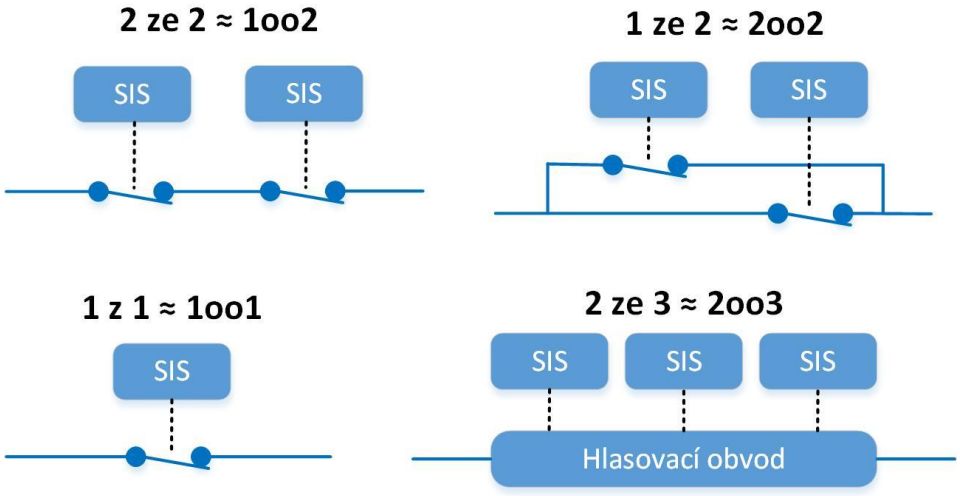
Obrázek III. **Redundantní struktura systému**

Redundance nemusí být nutně jen hardwarová, systém může využívat redundanci programového vybavení (software), redundanci datovou, informační atd. Přitom redundantní části nemusí být identické a navzájem se jednotlivé metody mohu kombinovat.

III. VÝKLAD OZNAČENÍ ARCHITEKTUR

V předchozí kapitole byly popsány základní struktury, se kterými je možné se u bezpečných systémů setkat. Poslední zmíněná struktura (redundantní) je běžně označována ve formátu „*n* z *m*“ nebo „*noom*“ (viz obrázek III). Toto označení je odvozeno od hlasovacího obvodu, který rozhoduje o povolení či blokování výstupních bezpečnostně relevantních signálů.

Při rozboru označení „*n* z *m*“ je možné z pohledu zabezpečovací techniky definovat *m* jako celkový počet redundantních kanálů zpracovávajících informace a *n* jako minimální počet kanálů, potřebných pro zajištění bezpečnostní funkce systému. Systém na obrázku III s označením 2 ze 3 je tedy složen ze třech redundantních kanálů a je schopen zajišťovat svoji bezpečnostní funkci i v případě poruchy jednoho kanálu. Porouchaný kanál je izolován a systém dále pracuje jako 2 ze 2. Tato struktura v sobě kombinuje vysokou spolehlivost a bezpečnost.



Obrázek IV. **Architektury bezpečných systémů**

V případě použití tohoto výkladu pro strukturu 1 ze 2 by znamenalo, že systém je složený ze dvou redundantních kanálů a je schopen zajišťovat svou bezpečnostní funkci i v případě poruchy jednoho z kanálů. Lze si to představit jako paralelní spojení dvou jednokanálových systémů. Systém struktury 1 ze 2 zvyšuje spolehlivost zařízení, ale bezpečnost nezvyšuje. Stejný výklad pro strukturu 2 ze 2 říká, že pro zajištění provádění bezpečnostní funkce systém vyžaduje oba kanály a takový systém má vysokou bezpečnost, ovšem na úkor spolehlivosti. Proto se v zabezpečovací technice struktura 1 ze 2 téměř nepoužívá.

Norma ČSN EN 61508 používá podobné znační jednotlivých struktur a to ve formátu „*n*oo*m*“ (*n* out of *m*). Toto značení je používáno v zahraniční literatuře a odborných článcích. Význam tohoto označení je podle normy ovšem od výše uvedeného „*n* z *m*“ pro některé struktury odlišný.

Pod označením 2 ze 3 lze v normě ČSN EN 61508 nalézt shodnou strukturu 2oo3 (tříkanálová redundantní architektura s hlasovacím obvodem viz obrázek III). Významově se 2 ze 3 a 2oo3 od sebe neliší a lze je chápat jako ekvivalentní označení.

Významový rozdíl je ovšem u dvoukanálových struktur. Zde je označení jednotlivých struktur odlišné. V zabezpečovací technice označení 2 ze 2 významově odpovídá označení 1oo2 dle normy ČSN EN 61508 a naopak označení 1 ze 2 odpovídá 2oo2.

Náhled na jednotlivé architektury je shodný v obou případech, liší se však jejich označení, které je matoucí. Proto je důležité v konceptu systému detailně architekturu popsat a nejlépe doplnit o blokové schéma.

IV. ZÁVĚR

V průběhu návrhu bezpečného systému je důležité zvolit vhodnou strukturu. Je nutné, aby byla architektura systému zvolena tak, aby byla schopná naplnit všechny body dle specifikace požadavků na bezpečnost. Struktura systému definovaná pomocí obrázku je zcela jednoznačná. To nelze říci o způsobu označení jednotlivých struktur. Jak již bylo zmíněno, výklad a především význam označení může být podle různých zdrojů jiný. Architektura musí být detailně popsána a nelze se spoléhat jen na označení formou zkrácených výrazů.

PODĚKOVÁNÍ

Tento článek vznikl za podpory interního projektu na podporu studentských vědeckých konferencí SVK-2016-006 a projektu SGS-2015-002: Moderní metody řešení, návrh a aplikace elektronických a komunikačních systémů. Rád bych také poděkoval vývojovým pracovníkům RICE za užitečné informace a cenné připomínky.

LITERATURA

[1] ČSN EN 61508 ed.2. Funkční bezpečnost E/E/EP systémů souvisejících s bezpečností. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Třídící znak 180301.

[2] Železniční zabezpečovací technika, Chudáček, V. a kol., Praha: ČD - VÚŽ, 2005.

[3] ČSN EN 50129. Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Elektronické zabezpečovací systémy. Brno: Český normalizační institut, 2003. Třídící znak 342675.