Analýza rizika elektronických systémů za použití metody FMEA

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

Using FMEA Method for Risk Analysis of Electronic Systems

Abstract – **This article deals with reliability and safety assessment of the systems using highly structured systematic analysis FMEA (Failure Mode and Effect Analysis). The FMEA is one of the most commonly used qualitative methods of reliability analysis. This method is often perceived as a tool for managing and improving quality in pre-production stages. The paper describes the basic characteristics and the most important parts of the FMEA.**

Keywords – FMEA; Failure Mode and Effects Analysis; Risk; Qualitative Analysis.

I. Úvod

Základním nástrojem hodnocení spolehlivosti a bezpečnosti systémů jsou postupy a metody spolehlivostních analýz, které umožňují realizovat specifikované požadavky v jednotlivých etapách životního cyklu. Analýza systému je velmi důležitým krokem návrhu, mnohdy nezbytným, pokud se jedná o návrh systému, na který jsou kladeny požadavky na bezpečnost. Jednou z řady metod využívaných v prvotních fázích vývoje je analýza FMEA (Failure Mode and Effect Analysis), česky překládaná jako analýza způsobů a důsledků poruch.

I. Charakteristika analýzy FMEA

Při návrhu elektronických zabezpečovacích systémů se s metodou FMEA (či s dalšími analýzami např. HAZOP, FTA atd.) sekáme téměř bez výjimky. Jsou ale aplikace, kde požadavek na provedení rizikové analýzy není zákazníkem ani jinou legislativou požadován a je pouze na rozhodnutí vedoucího projektu, případně návrháři samotném, zda ve vlastním zájmu jakoukoli předvýrobní analýzu aplikuje. Z podstaty plyne, že odhalením chyby ještě ve fázi vývoje můžeme předejít závažným návrhovým nedostatkům vedoucích k přepracování systému. Čím je systém složitější a dražší na výrobu, tím závažnější dopady může chyba způsobit.

FMEA je metoda systematické analýzy možných druhů a důsledků poruchových stavů a jejich uspořádání podle stupně závažnosti. Rozšíří-li se metoda FMEA o hodnocení kritičnosti důsledků s uvážením pravděpodobností (nebo četností) jejich výskytu, jedná se pak o metodu zvanou Analýza druhů, důsledků a kritičnosti poruchových stavů (FMECA - Fault Modes, Effects and Criticality Analysis).

Analýzu FMEA je nutno chápat jako týmovou metodu. Jen velmi obtížně by ji mohl kvalitně provádět jeden pracovník, neboť by mu chyběly pohledy na problematiku z

dalších profesních oblastí. Při svém provádění musí být FMEA provázána s řídícími zásahy v podobě nápravných opatření vedoucích k odstranění příčin, které jsou identifikovány jako nejzávažnější potenciálně možné poruchové stavy. [2]

#	Item / Function / Objekt / funkce	Potencial Failure Mode(s) / Potenciální způsob poruchy	Potencial Local Effect(s) of Failure / Potenciální místní důsledek poruchy	Potencial Global Effect(s) of Failure / Potenciální konečný důsledek poruchy	SEV	Potencial Cause(s)/ Mechanism(s) of Failure / Potenciální příčiny / mechanizmy poruchy	PROB	Detection Method / Metoda detekce	DET	RPN	Recommended Action(s) / Doporučená opatření	Action Result / Provedená opatření
Napájecí zdroj												
1	D2	Zkrat	Zkrat +pólu baterie na -zem	Vybití baterie "vrať se domů pěšky"	10	Vnitřní vada - průraz materiálu	3	Hodnocení a validační zkoušky bezporuchovosti	1	30		
2	D2	Přerušení	Žádná ochrana proti přepólování	Nezasluhuje pozornost	2	Vnitřní vada - vada kontaktování nebo prasklina v polovodiči	3	Hodnocení a validační zkoušky bezporuchovosti	2	12		
3	C7	Zkrat	Zkrat +pólu baterie na -zem	Vybití baterie "vrať se domů pěšky"	10	Vnitřní vada - průraz dielektrika nebo prasklina	3	Hodnocení a validační zkoušky bezporuchovosti	1	30		
4	C7	Přerušení	Žádná filtrace proti elmag. Rušení	Provoz oběktu mimo specifikaci	2	Přerušení kontaktu mezi přívodem a polepem, netěsnost, dutina či prasklina	2	Hodnocení a validační zkoušky bezporuchovosti	1	4		
5	L1	Přerušení	Žádné napětí - V1	Objekt je nefunkční - žádné varování	9	Vnitřní vada - Prasknutí materiálu	2	Hodnocení a validační zkoušky bezporuchovosti	1	18		
6	R5	Přerušení	Žádné napětí pro spínasí obvod	Objekt je nefunkční - žádné varování	9	Vnitřní vada - Přerušení vodivého spojení nebo materiálu	2	Hodnocení a validační zkoušky bezporuchovosti	1	18		

Obrázek I. **Příklad části FMEA analýzy**

II. VSTUPNÍ INFORMACE, POTŘEBNÉ PRO ANALÝZU

Aby mohla být provedena analýza systému metodou FMEA případně FMECA, je nezbytné stanovit přesné podmínky jejího provedení a shromáždit všechny potřebné vstupní údaje. Analytik by měl mít k dispozici především tyto podmínky a informace:

A. Účel a cíle analýzy

Musí být přesně vymezeno, k jakému účelu je analýza prováděna. Následující seznam uvádí nejčastější důvody k provádění analýzy:

- Prokázání, že výrobek splňuje požadavky na bezpečnost.
- Vyspecifikování kritických prvků systému z hlediska nepříznivých důsledků jejich poruch pro plnění základních funkcí systému.
- Prokázání splnění požadavků na spolehlivost.
- Poskytnutí vstupní informace pro návrh optimálního systému technické údržby a diagnostiky.

Požadavek na provedení analýzy může být kombinací výše uvedených účelů a cílů, případně jiných specifických důvodů pro konkrétní aplikaci.

B. Technický popis systému

Konstrukční uspořádání a použité technické řešení by mělo být popsáno slovním popisem, doplněným o podrobnou výkresovou dokumentaci, schémata, vývojové grafy apod.

C. Definice funkcí systému a jeho prvků

Jednou ze vstupních informací je definice všech důležitých funkcí systému a prvků, které musí být podrobeny analýze. Jednotlivé funkce musí být definovány tak, aby bylo možné modelovat jejich vzájemné souvislosti, posloupnost a vazby na provozní podmínky systému. Z jejich definic musí být možné jasně odvodit závažnost důsledků

jejich neplnění, možnosti jejich jednotlivého oddělení apod. V daném systému nebo prvku může být pouze jedna funkce. Většinou je však funkcí několik a v takovém případě se pro každou definovanou funkci provádí účelově zaměřená analýza.

D. Funkční členění systému

Funkční členění musí korespondovat s předchozím bodem. Definuje se, do jakých funkčních subsystémů se systém člení a to až do požadované hloubky analýzy. Je nutné odlišovat funkční členění od konstrukčního, které může být shodné, ale není to pravidlem. Toto rozdělení je důležité, protože systém jednoho konstrukčního uspořádání může plnit celou řadu odlišných funkcí a tomu musí být přizpůsobeno i odpovídající funkční členění.

E. Definice rozhraní systému

Musí být přesně vymezeny hraniční body a prvky, kde dochází ke vzájemné interakci mezi sousedními subsystémy nebo s vnějším okolím systému. Na tomto rozhraní jsou vymezeny tzv. okrajové podmínky pro analýzu systému s cílem vyloučit průniky jevů více systémů, aby se neopakovaly stejné analyzované jevy v různých systémech.

F. Údaje o prvcích systému

S ohledem na hloubku požadované analýzy musí být pro všechny prvky systému k dispozici alespoň následující informace:

- jednoznačná identifikace prvků (čísla výkresů, katalogová čísla, čísla prvků na schématech a výkresech apod.);
- popis funkcí prvků;
- popis možných způsobů poruch prvků;
- popis důsledků poruch prvků;
- pravděpodobnosti jednotlivých způsobů poruch prvků;

Poslední bod o pravděpodobnosti (intenzitách) poruch prvků je nutné mít k dispozici v případě, že je požadováno provedení kvantitativní analýzy.

III. POSTUP PROVÁDĚNÍ ANALÝZY FMEA

Realizace metody představuje provedení jisté logické posloupnosti kroků, které lze rozdělit na tři základní části:

A. Přípravná část analýzy

Obsahem této části je nashromáždění všech potřebných informací a podkladů, upřesnění cílů a stanovení základních pravidel. K základním informacím, které jsou k provedení analýzy nezbytné, patří zejména: *cíle a termíny; požadavky na spolehlivost a bezpečnost; informace o struktuře, funkcích a provozních podmínkách systému; podmínky prostředí*.

Na základě těchto informací je zpravidla sestaven strukturální (funkční) diagram, který znázorňuje vztahy mezi jednotlivými prvky systému. Je nutné určit nejnižší úroveň, která je předmětem sledování. Všechny objekty na této úrovni jsou pro účely analýzy považovány za dále nedělitelné prvky a lze si je představit za jakési „černé skříňky“, jejíž vnitřní struktury a funkce již nejsou předmětem analýzy.

B. *Vlastní FMEA jednotlivých prvků systému*

Při vlastní analýze jsou postupně všechny prvky systému (na zvolené nejnižší úrovni) podrobeny systematickému zkoumání. V rámci zkoumání se přiřazují *způsoby poruch, jejich důsledků a pravděpodobných příčin, identifikují se metody a opatření k detekci a izolaci poruch*, případně se posuzují i *kvalitativní významnosti poruch* (FMECA).

Výstupem FMEA jednotlivých prvků je *kvalitativní* hodnocení úrovně spolehlivosti a bezpečnosti zkoumaného systému a to v podobě výčtu všech předvídatelných poruch, problémových míst v konstrukci a jejich důsledky pro funkci systému.

C. *Vyhodnocení analýzy*

Výsledky analýzy se vždy porovnávají s požadavky schválených technických podmínek pro vývoj, výrobu a provoz výrobku. Na základě výsledků z porovnání a dalších poznatků při realizaci analýzy se navrhnou konkrétní nápravná opatření vedoucí k úplnému odstranění příčiny poruchy, nebo snížení pravděpodobnosti jejího vzniku na přípustnou mez.

Pro přehlednost analýzy se běžně používají pracovní formuláře. Neexistuje však žádný závazný předpis upravující obsah nebo formu, pouze doporučení např. viz [1]. Vždy by měl ale obsah a uspořádání odpovídat specifickým cílům analýzy a charakteru systému.

IV. ZÁVĚR

Obsah a rozsah jednotlivých částí analýzy závisí na celé řadě faktorů a může se případ od případu lišit jak formou, tak obsahem. Proto také neexistuje žádný univerzální ani závazný návod, který by jednoznačně a detailně určoval, jak analýzu provádět. Existují standardy a odborné publikace, které se této problematice věnují. Zpravidla v nich najdeme jen výčet základních principů metody a doporučení k jejímu provádění. Praktické uplatnění těchto principů a doporučení je vždy ovlivňováno specifickými vlastnostmi zkoumaného systému, podmínkami jeho provozu, účelem analýzy, nebo dohodou mezi kompetentními partnery.

PODĚKOVÁNÍ

Tento článek vznikl za podpory interního projektu na podporu studentských vědeckých konferencí SVK-2017-008 a projektu SGS-2015-002: Moderní metody řešení, návrh a aplikace elektronických a komunikačních systémů.

LITERATURA

[1] ČSN EN 60812 Techniky analýzy bezporuchovosti systémů - Postup analýzy způsobů a důsledků poruch (FMEA) Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Třídící znak 010675.

[2] A. Mykiska, P. Votava, *Princip a možnosti aplikace metody FMEA/FMECA*, Praha (Česká Republika): Úloha a aplikační možnosti metody FMEA při zabezpečování spolehlivosti, 2001.

[3] R. Holub, Z. Vintr, *Spolehlivost letadlové techniky*, Brno (Česká republika), VUT FST, 2001. Elektronická učebnice.