

Pavel Turjanica, Petr Burian, Jan Bartovský

Obvody FPGA v aplikacích se zvýšenými nároky na bezpečnost

Technická zpráva

Pracovní balíček:

9 – Bezpečnost

Rok řešení:

2013



**FAKULTA
ELEKTROTECHNICKÁ
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI**

2013

Pracoviště: RICE

Výzkumná zpráva č.: 22190-073-2013

Obvody FPGA v aplikacích se zvýšenými nároky na bezpečnost

Druh úkolu: Vědecko-výzkumný

Řešitelé: Pavel Turjanica, Petr Burian, Jan Bartovský

Vedoucí úkolu: Pavel Turjanica

Počet stran: 18

Datum vydání: prosinec 2013

Revize: 2

Anotace

Tento dokument se zabývá určitými aspekty návrhového procesu elektronických systémů s nároky na zvýšenou bezpečnost (tzv. safety-critical application). Pozornost je primárně věnována návrhu s využitím obvodů FPGA od společnosti Altera Corp. Jsou diskutovány možnosti implementace interní konektivity uvnitř obvodu FPGA s ohledem na proces certifikace. Na tuto problematiku navazuje popis balíčku Functional Safety Data Package; který se věnuje především obecné normě IEC 61508 a proto je v závěru dokumentu provedena stručná komparace této normy s normami pro drážní zařízení. Předkládaný dokument si klade za cíl podat základní přehled problematiky konektivity uvnitř FPGA obvodů (Programovatelná hradlová pole) od společnosti Altera Corp. **Zvláštní zřetel je věnován návrhovému prostředí Quartus II se standardními nástroji SOPC Builder resp. Qsys System Integration Tool s ohledem na jejich využití v aplikacích se zvýšenými nároky na bezpečnost (SIL1 a vyšší).**

Seznam symbolů a zkratek

CPLD	Complex Programmable Logic Device
FPGA	Field Programmable Gate Array
NoC	Network-on-Chip
SIL	Safety Integrity Level

Obsah

1	VÝVOJOVÝ PROCES SYSTÉMŮ SE ZVÝŠENÝMI NÁROKY NA BEZPEČNOST	4
2	KONEKTIVITA V RÁMCI FPGA.....	6
3	REFERENČNÍ DESIGN	9
4	ON-CHIP REDUNDANCY	10
5	ALTERA FUNCTIONAL SAFETY DATA PACKAGE	10
6	REFERENCE	13
7	KOMPARACE IEC 61508 A EN 50126/8/9	13
8	ZÁVĚR.....	15

1 Vývojový proces systémů se zvýšenými nároky na bezpečnost

Napříč všemi průmyslovými segmenty (výroba, automatizace, řízení pohonů, doprava atd.) se zvyšují požadavky na funkční bezpečnost elektronických zařízení/systémů. S těmito nároky se mění pohled na celý návrhový proces. Nároky na bezpečnostní opatření musí být vnímány jako integrální součást systému a jsou zohledňovány od samého počátku vývojového cyklu. Obecně je nevýhodné dodávat bezpečnostní opatření do systému později, taková řešení jsou ve výsledku finančně náročnější a méně flexibilní. Pro úspěšné zvládnutí vývoje systémů se zvýšenými nároky na bezpečnost je nutné zavést potřebnou metodologii, definovat bezpečnostní koncept, vybudovat potřebný projektový management, zavést systém pro uchovávání dat, dokumentace atd. Všechny tyto požadavky představují dodatečné náklady k samotnému vývojovému procesu a musí být brány v potaz.

Zaměříme-li se na běžný návrhový proces, můžeme ho rozdělit do několika základních fází. Nejprve se obvykle zvolí vhodná architektura systému. V této fázi definujeme základní části systému; v případě řízení pohonu například systém rozdělíme na část systémového řízení, real-time řízení motoru a část zajišťující komunikaci s okolním prostředím. V následné fázi vybíráme vhodné komponenty pro navrhovaný systém. Například definujeme použití procesorů či obvodů FPGA. Následně se přistupuje k implementaci jednotlivých modulů definovaných dle architektury. Po implementaci modulů dochází k jejich integraci, verifikaci a validaci systému jako celku. V případě kladných výsledků může být vývojový proces ukončen.

Je-li však při návrhu kladen důraz na zvýšené nároky na bezpečnost, celý návrhový proces se značně komplikuje a může být rozdělen do následující fází. Pro FPGA design použitý jako součást systému platí obdobná pravidla bezpečného návrhu, jako pro celý systém:

- Zahájení projektu a risková analýza
 - Určení požadovaného stupně SIL pomocí formálních metod
 - Risk analýza poskytuje základ pro opatření, která musí být splněna při procesu vývoje
 - Strukturální členění dokumentace, která je uplatňována na komponentní i systémové úrovni
- Návrh architektury
 - Návrh architektury s ohledem na funkční i bezpečnostní hledisko

- Specifikování způsobu validace
- Jsou kladeny zvýšené požadavky na dokumentaci
- Specifikace bezpečnostních nároků
 - Specifikovat „nebezpečné“ události a reakce na tyto události
 - Specifikace časové odezvy
 - Informace pro nadřazený systém
- Validací a verifikační plán
 - Způsob testování chybových stavů (Failure On Demand)
 - Ověření parametrů a vlastností systému
 - Monitoring vnitřních stavů systému
- Výběr komponent, IP jader a vývojových nástrojů s ohledem na stupeň způsobilosti pro danou aplikaci
 - Výpočet spolehlivostních parametrů
 - Způsobilost je třeba doložit dokladem (často obtížně získatelné) či “proven in use”
- Implementace
 - Diversifikace a redundance kritických funkčních bloků na základě spolehlivostních parametrů
 - Složité funkce v FPGA, velká IP jádra apod. musí být způsobilá pro aplikace se zvýšenými nároky na bezpečnost (tedy rovněž dostatečně analyzována, testována)
- Bezpečností a diagnostické funkce
 - Doimplementování bezpečnostních a diagnostických funkcí
 - Diagnostické funkce, např.: sledování napětí, kvality hodinového signálu, sledování a analýza PWM signálů
 - Funkce, které automaticky rozpoznají selhání a uvedou systém do bezpečného stavu
 - Základní funkce se musí vypořádat například s porušením integrity dat v paměti z důvodů externího zásahu, selhání systémových hodin či s nekorektní činností napájecích zdrojů
- Integrace a testování
 - Po integraci jednotlivých komponent se verifikuje jak funkčnost, tak i bezpečnostní funkce
 - Každý chybový stav musí být systémem pokryt
 - Důkladné testování bezpečnostních funkcí (nesmí selhat, aniž by o tom byl celý systém informován)
- Bezpečnostní validace, certifikace, vydání
 - Nutnost spolupráce s hodnotitelem

Celý proces návrhu může být usnadněn, pokud spolupracujeme s dodavatelem použitých komponent a ten nám dodává například doklady o spolehlivosti polovodičů (u FPGA od společnosti Altera Corp. jsou tyto údaje k dispozici), o certifikaci vývojových nástrojů atd. Důležitá jsou i doporučení, která můžeme obdržet od jednotlivých výrobců.

2 Konektivita v rámci FPGA

Vzhledem k tomu, že nynější obvody FPGA umožňují díky velkému počtu logických elementů budovat velmi rozsáhlé systémy, je nutné dbát na hierarchický a modulární design. Ten sám o sobě umožňuje lepší management projektu, zjednoduší testovatelnost a validaci návrhu. Nezanedbatelný je fakt, že správná modularita systému je jeden z požadavků pro aplikace se zvýšenými nároky na bezpečnost; **požadavky na modulární návrh jsou přímo předepsány příslušnou normou** (viz IEC 61508-2, příloha F, tabulka F.2, Ref 11; podrobněji vysvětleno v IEC 61508-7, příloha E, odstavec E.12).

Jednotlivé funkční moduly FPGA návrhu by měly být propojeny **unifikovaným komunikačním rozhraním** a přímá komunikace mezi moduly, implementovaná mimo toto jasně definované rozhraní, musí být omezena na minimum. Je tedy nutnost implementovat vhodný „propojovací“ (interconnect) systém, který obstará vzájemnou konektivitu jednotlivých modulů.

Dnešní trend se ubírá směrem tzv. NoC (Network-on-Chip) architektur, neboli budování „sítě na čipu“. Tyto „sítě“ mají oproti starším „non-NoC“ architekturám přínos především v ohledu na lepší nezávislost a oddělení jednotlivých vrstev FPGA návrhu a lepší možnosti optimalizace pro konkrétní aplikaci, snazší testovatelnost, jasně definované a unifikované rozhraní vede k úsporám při vývoji a testování jak komponent, tak celého designu (Např. není nutné v každém projektu opakovat modulární testy).

Uvažujeme-li obvody FPGA od společnosti Altera Corp., existuje několik možností, jak může být „propojovací“ systém implementován:

- **Architektura plně založena na „vlastním návrhu“:**
 - Designér navrhne vlastní způsob propojení a rozhraní funkčních bloků implementovaných v FPGA
 - **Výhody:**
 - Vyšší úspornost pro menší design

- **Nevýhody**
 - Ztížená možnost využívat IP jádra dalších subjektů
 - Z hlediska certifikačního řízení velmi náročné; subjekt musí prokázat vhodnost navrženého řešení a absenci systémových závad při každé modifikaci propojovacího systému, což představuje značnou časovou a finanční zátěž
 - Jedná se o archaické řešení, v moderních FPGA návrzích (SoC) se téměř nevyskytuje
 - Obtížné pro modifikaci
- **Architektura založena na rozhraní Wishbone:**
 - Tato varianta představuje návrh a implementaci (či převzetí již implementovaného) vlastního propojovacího systému. Jednotlivé IP jádra (moduly) využívají rozhraní Wishbone, které je využíváno především v „open source“ komunitě
 - **Výhody:**
 - Široká komunita uživatelů
 - **Nevýhody:**
 - Možnost certifikace je obdobná s předchozí variantou
 - Obtížné pro modifikaci
- **Architektura založena na nástroji SOPC Builder**
 - Nástroj firmy Altera Corp.
 - Založeno na IP jádrech s rozhraním Altera Avalon
 - **Výhody:**
 - Automatický návrh struktury pro propojení jednotlivých modulů
 - Vysoká modularita a efektivita
 - Lze rozlišit Master a slave komponenty
 - **Toto řešení je akceptovatelné orgánem TÜV a splňuje požadavky návrhu dle normy IEC 61508** (viz White Paper „Developing Functional Safety Systems with TÜV-Qualified FPGAs“ od společnosti Altera).
 - Určeno i pro aplikace se zvýšenými nároky na bezpečnost
 - **Využíváno lídry v oblasti řízení a drážních vozidel** (viz kapitola 6)
 - Vysoká kvalifikace v provozu (přes 10 tisíc uživatelů)
 - **Nevýhody:**
 - V současné době firma Altera končí s podporou tohoto nástroje, proto se nejeví jeho používání v začínajících projektech jako smysluplné

- **Architektura NoC založena na nástroji Qsys:**

- Nástroj firmy Altera Copr. Založeno na IP jádrech s rozhraním Altera Avalon. Vychází ze SOPC Builderu a je určen pro nové systémy jako jeho plnohodnotná náhrada. Stěžejní produkt společnosti Altera pro konektivitu v rámci FPGA. **V současné době probíhá certifikace orgánem TÜV dle normy IEC 61508,** ukončení procesu certifikace v prosinci 2013
- **Výhody:**
 - Větší datová propustnost v porovnání s SOPC Builderem
 - Zlepšená podpora pro hierarchický design
 - Bohatá podpora rozhraní (Avalon, AXI atd.)
 - Real-time systémový debugging
 - Široká podpora od výrobců IP jader
- **Nevýhody:**
 - Dosud bez širokého nasazení v SIL aplikacích (novum)

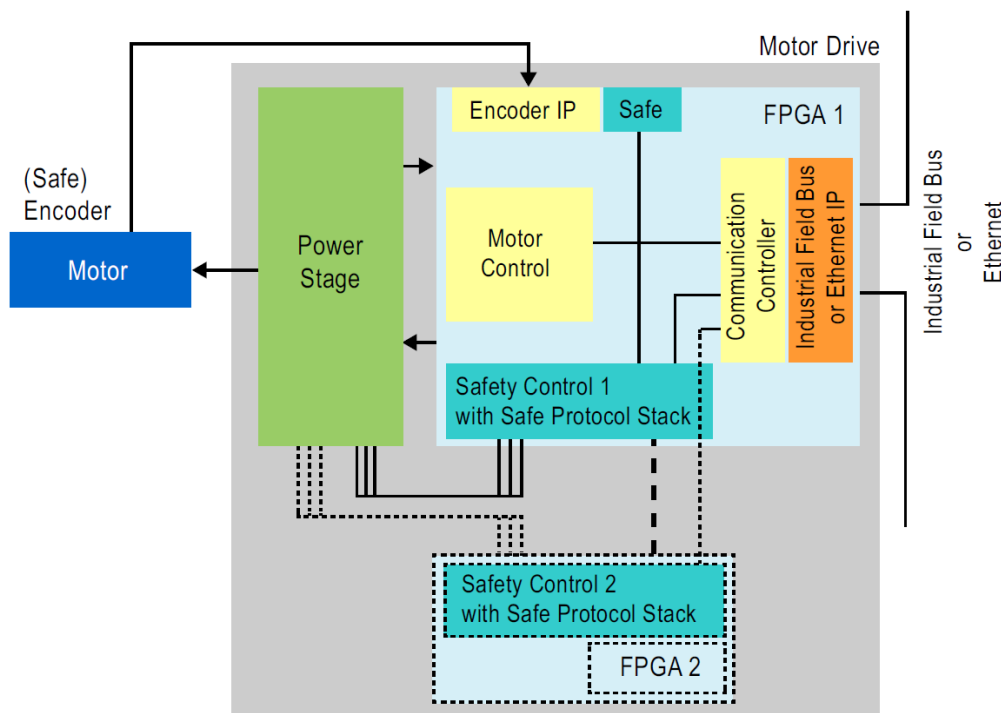
Shrneme-li výše uvedené varianty z hlediska možnosti certifikace, je zřejmé, že není nutné využívat žádné speciální nástroje pro podporu hierarchického a modulárního návrhu a i samotná propojovací architektura může být navržena *ad hoc* pro specifickou aplikaci. Je však nutné přihlédnout k jistým omezením této strategie, a to je především tíha prokázání vhodnosti implementovaného návrhu dle příslušné normy. Toto prokazování s sebou nese nejenom značnou finanční a časovou náročnost. Je nutné si uvědomit, že případné schválení propojovací architektury se vztahuje jen na jednu konkrétní implementaci. Připojení dalšího IP jádra nebo modulu k této architektuře či jiná případná jemná modifikace má za následek vznik *de facto* úplně nové implementace, na kterou se předchozí schválení nevztahuje, a subjekt je tak nucen znovu provádět celý proces schvalování. V případě, že propojovací architektura je založena na nástroji SOPC Builder tato nutnost odpadá. Společnost Altera spolupracovala na certifikaci nástroje SOPC Builder s orgánem TÜV a tak jsou výstupy tohoto nástroje „předschváleny“ dle normy IEC 61508. Situace s nástrojem Qsys je obdobná, avšak jak již bylo uvedeno, certifikace tohoto nástroje není ještě ukončena. Pokud ale certifikační řízení není plánováno dříve než počátkem roku 2014, je využití nástroje Qsys silně doporučeno – nástroj SOPC Builder v současné době končí a Qsys je jeho plným nástupcem. Samozřejmě je možné struktury generované pomocí obdobných nástrojů certifikovat i jiným způsobem. Generovaný zdrojový kód můžeme vnímat jako implementaci fixní struktury, kterou můžeme samostatně testovat, verifikovat a validovat. Můžeme tedy k této struktuře

přístupovat jako k obecnému zdrojovému kódu. Tento přístup ovšem přináší již zmíněná negativa, kdy musíme prokázat vhodnost daného návrhu.

3 Referenční design

Společnost Altera Corp. vydává ke svým produktům tzv. referenční design v různých oblastech. V současné době pracuje na návrhu referenčního designu za využití Qsys Integration Tool a FSDP. Již nyní je uvolněna ukázková koncepce moderního řízení pohonu založená na architektuře s dvěma obvody FPGA, jako příklad aplikace se zvýšenými nároky na bezpečnost (SIL3).

Architekturu systému tvoří několik částí, které jsou implementovány pomocí softwarových procesorů Nios II. Jeden procesor obstarává komunikaci, druhý implementuje (spolu s příslušnými IP jádry) real-time řízení motoru, a třetí procesor řídí celý systém jako celek. Druhý obvod FPGA implementuje redundantní řízení, které je nutné pro dosažení SIL3. Konektivita uvnitř FPGA, tzn. propojení jednotlivých IP jader a procesoru Nios II je implementována vývojným nástrojem Altera SOPC Builder a je založena na rozhraní Altera Avalon.



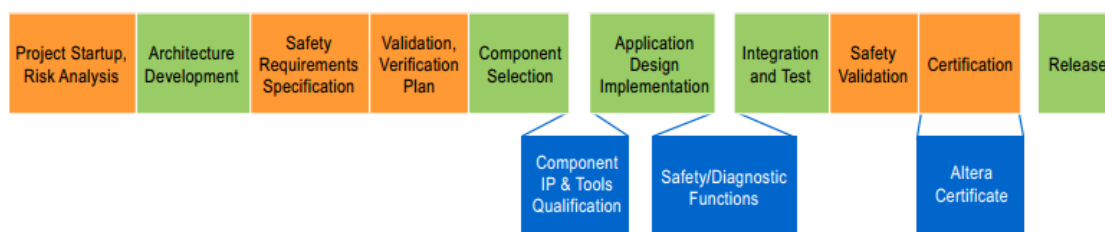
Obr. 1 - Moderní koncepce řízení pohonu

4 On-chip redundancy

Společnost Altera nyní pracuje na podpoře technologie „**on-chip-redundancy**“, která ve stávajících obvodech usnadní budování dvou-a více kanálové architektury na jednom čipu (FPGA obvodu). Průchodnost této architektury přes schvalovací autority bude v nejbližší době řešit. Podmínky použití a omezení (maximálně SIL3) tohoto typu redundance jsou nicméně uvedeny v normě IEC 61508-2 (edice 2, příloha E). Tento směr v sobě skrývá veliký potenciál, neboť omezí nutnost použití více čipů pro aplikace s vyšší bezpečností. Dle dostupných informací bude pro tuto architekturu a referenční design opět použit Qsys.

5 Altera Functional Safety Data Package

Speciální balíček Functional Safety Data Package (dále jen FSPD) je produkt společnosti Altera Corp., který vznikl po dlouhém vývoji ve spolupráci s certifikačním orgánem TÜV. Je určený pro partnery z oblasti průmyslu, kde je kladen důraz na zvýšenou bezpečnost. FSPD je soubor dokumentů, nástrojů, IP jader a metodologie, který umožňuje výrazně zkrátit (výrobce udává, že až o 18 měsíců) proces certifikace výsledné aplikace dle normy IEC 61508. Přínos FSPD se však samozřejmě vztahuje i k jiným normám, které jsou od IEC 61508 odvozeny, jmenujme například: automatizace procesů (IEC 61511), strojní automatizace (IEC 62061), drážní zařízení (EN 50128), lékařská technika (IEC 62304), „automotive“ systémy (ISO 26262), distribuce elektrické energie či doprava. Na Obr. 2 je modře naznačeno, ve kterých fázích návrhového procesu může být FSPD přínosný.

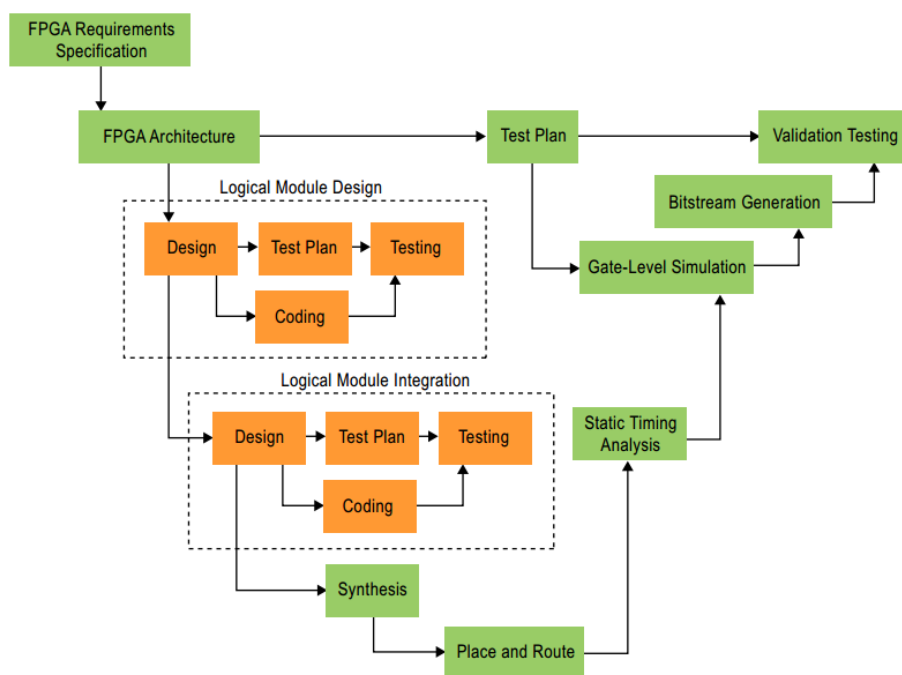


Obr. 2 - Vývojový proces s ohledem na zvýšenou bezpečnost

FSPD obsahuje tyto základní položky:

- Spolehlivostní reporty polovodičů (FPGA, CPLD, konfiguračních pamětí) – dostupné i mimo FSPD
- Doporučená metodologie pro návrh aplikací se zvýšenými nároky na bezpečnost
- Vývojové nástroje schválené dle normy IEC 61508 (Quartus II, SOPC Builder, TimeQuest)

- Komentář k normě IEC 61508
- „Safety“ IP jádra (kontrola konfigurační paměti, výpočet CRC, kontrola hodinového signálu)
- Podrobně popsany a doporučený V-model (viz **Chyba! Nenalezen zdroj odkazů.**; chválený orgánem TÜV, odvozen od IEC 61508)
- Příklady výpočtů spolehlivosti
- Formuláře akceptovatelné orgánem TÜV



Obr. 3 V-Model pro FPGA návrh

Obsah FSPD výrazně pomáhá plnit jednotlivé procesy nutné pro schvalovací proces. Například doporučuje, jaký nástroj a jaká metodika má být použita pro jednotlivé části V-modelu, samozřejmě jsou též připravené formuláře, které napomáhají k správnému procesu dokumentace a dodržování doporučených postupů.

Některé požadavky normy IEC 61508 jsou splněny automaticky díky dokumentům obsažených ve FSPD. Následující přehled shrnuje techniky a opatření normy, které jsou pomocí FSPD splněny (automaticky bez dalších zásahů). Jednotlivé techniky a opatření pro návrhový proces FPGA designu jsou uvedeny v normě IEC 61508-2, příloha F, tabulka F.2; tyto techniky a opatření jsou pak podrobně diskutovány v IEC 61508-7.

Zahájení návrhu

- *Ref 6 – Použití prostředí návrhu osvědčeného v provozu*
Používané návrhové prostředí je osvědčené v provozu, a to buď po dostatečně dlouho dobu, či velkým počtem uživatelů. Samozřejmostí je sledování nedostatků („bug list“), odezvy uživatelů atd.
- *Ref 7 – Aplikace osvědčené v provozu simulátorů (V)HDL*
Používaný simulátor jazyka VHDL či Verilog je osvědčený v provozu, a to buď po dostatečně dlouho dobu, či velkým počtem uživatelů. Samozřejmostí je sledování nedostatků („bug list“), odezvy uživatelů atd.
- *Ref 16a – Použití softwarových jader s potvrzenou platností*
Použitá softwarová jádra – IP cores – musí být ověřená na dostatečný stupeň SIL, minimálně tedy na takový stupeň, který má být dosažen pro celý výsledný systém. Je nezbytné k použitému jádru doložit veškeré potřebné dokumenty dokazující jeho „způsobilost“.

Syntéza

- *Ref 17 – Zkoušky vnitřní konzistence*
Viz Ref 6.
- *Ref 23 – Použití prostředí syntézy osvědčených v provozu*
- *Ref 24 – Použití knihoven /CPLD technologií osvědčených v provozu*

Obdoba viz Ref 6, avšak pro knihovny využité při syntéze.

Umístění, směrování, zkušební vzorky

- *Ref 30 – Použití prostředí návrhu osvědčeného v provozu, použití buněk knihoven osvědčených v provozu*

Viz Ref 6.

Výroba

- *Ref 32 – Použití technologie osvědčené v provozu*
- *Ref 33 – Použití sériových řad osvědčených v provozu*
- *Ref 34 – Výrobní proces osvědčený v provozu*
- *Ref 35 – Řízení kvality výrobního procesu*
- *Ref 36 – Vyhovující zařízení po kontrole kvality*
- *Ref 37 – Vyhovující zařízení po kontrole funkce*
- *Ref 38 – Normy kvality*
- *Ref 39 – Management kvality*

6 Reference

Vzhledem k tomu, že společnost Altera je jedním ze dvou hegemonů (tržní podíl přes 40%) v oblasti výroby obvodů programovatelné logiky, jsou produkty této společnosti používány i průmyslovými lídry napříč obory. Jmenujme například Siemens, Alstom či Deuta. Tyto firmy se věnují vývoji mimo jiné drážních zařízení a úspěšně nasazují obvody FPGA do aplikací s certifikací SIL2 i vyšší.

V rámci rešeršních prací v této oblasti bylo osloveno několik firem s žádostí o potvrzení využívání obvodů a vývojových nástrojů (Quartus II, SOPC Builder/Qsys Integration Tool, TimeQuest atd.) firmy Altera v drážních zařízeních:

„...We are using Altera FPGA/Tools (namely SOPC Builder) in SIL-certified railway-related products...”

Michael Gronemeyer
Siemens AG
Infrastructure & Cities Sector
Mobility and Logistics Division

„...We are using an Altera FPGA (Cyclone III and Cyclone IV) and the certified Altera design environment for our IconTrust product design.....we have a SIL 2 certified product and currently we are working on a similar SIL 3 certified product...”

Ulrich Angenendt
Deuta Werke GmbH

7 Komparace IEC 61508 a EN 50126/8/9

Norma IEC 61508 je obecným standardem pro funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů (E/E/PE) souvisejících s bezpečností. Hlavním cílem této normy je usnadnit tvorbu aplikačních norem a zároveň stanovuje všeobecné požadavky na systémy E/E/PE, kde žádné aplikační normy nejsou k dispozici. Pro drážní aplikace, CENELEC vytvořil sadu norem EN 50126/8/9, které pokrývají funkční bezpečnost drážních aplikací. EN 50126/8/9 mohou být chápány jako aplikační deriváty IEC 61508.

EN 50126 je hlavní normou definující bezporuchovost, pohotovost, udržitelnost a bezpečnost (RAMS) celého drážního systému. Dále definuje proces řízení RAMS v podobě životního cyklu, konceptu rizik, integrity bezpečnosti a poruch. EN 50129 definuje požadavky na

elektronické systémy a vyžaduje předložení dokumentu „důkaz bezpečnosti“. EN 50128 se zabývá specifickými aspekty softwaru pro dva výše zmíněné standardy.

Posouzení shody těchto tří drážních norem s „obecně bezpečnostní“ IEC 61508 je místy složité vzhledem k faktu, že stejný koncept se může objevovat pod různými jmény a zároveň shodná jména mohou skrývat různé koncepty. Srovnání EN 50126 s IEC 61508-1 ukazuje odlišné životní cykly, co se týče počtu a pojmenování fází. To přirozeně vede k nutnosti přizpůsobení aktivit návrhu systému, přestože základní myšlenka obou životních cyklů je velice podobná. Oba dva standardy vyžadují systematický a detailně dokumentovaný proces návrhu obsahující přesně definovanou specifikaci, analýzu rizik, požadavky bezpečnosti a její potvrzení. Shodný je taktéž zvolený V-model, kdy návrh je veden metodou „top-down“, ale validace je dělána strategií „bottom-up“.

Při srovnání EN 50129 s IEC 61508-2 a EN 50128 s IEC 61508-3 je zřejmá velká podobnost. Vzhledem k faktu, že všechny svazky IEC 61508 jsou provázány a velmi často se odkazují na obecné požadavky v první části (IEC 61508-1), je i zde formální rozdílnost mezi životními cykly návrhu uvedených výše. Určitá odlišnost se nachází v tom, že EN 50128 explicitně definuje úroveň integrity bezpečnosti (SIL) softwaru, ale IEC 61508 uvažuje pouze SIL celého testovaného zařízení, tudíž software i hardware.

Drážní normy EN 50126/8/9 jsou obecně chápány jako aplikační (drážní) interpretace normy IEC 61508. Požadavky pro návrh elektronických systémů a podklady pro vytvoření dokumentace (např. analýza rizik) pro certifikaci dle obou norem jsou ve své podstatě shodné. Avšak v detailech a v samotné požadované dokumentaci jsou obě normy mírně rozdílné, drážní normy lze považovat za rozšíření obecnější IEC 61508.

8 Závěr

Předkládaný dokument jasně naznačil, že problematika splnění zvýšených bezpečnostních nároků je velmi komplexní odvětví.

Společnost Altera Corp., na rozdíl od svého největšího konkurenta firmy Xilinx (ten vydání „bezpečnostního“ balíčku teprve plánuje), nabízí přímou podporu pro návrh systémů se zvýšenými nároky na bezpečnost a to v podobě produktu *Functional Safety Data Package*. Společnost dlouhodobě spolupracuje s certifikačním orgánem TÜV a ve svých dokumentech deklaruje využití svých obvodů a vývojových nástrojů pro aplikace certifikovatelné na SIL2 a SIL3. Toto potvrzuje i reakce oslovených firem Siemens a Deuta, kdy obě společnosti využívají tyto FPGA obvody a příslušné vývojové prostředí v oblastech drážních zařízení.

Nabídka společnosti Altera se pravděpodobně bude v této oblasti dále rozšiřovat a to například o podporu technologie „**on-chip-redundancy**“, která ve stávajících obvodech usnadní budování dvou-a více kanálové architektury na jednom čipu (FPGA obvodu). Podmínky použití a omezení (maximálně SIL3) tohoto typu redundance jsou uvedeny v normě IEC 61508-2 (edice 2, příloha E). Tento směr v sobě skrývá veliký potenciál, neboť omezí nutnost použití více čipů pro aplikace s vyšší bezpečností. Dle dostupných informací opět bude pro tuto architekturu a referenční design použit Qsys.

Pozornost byla věnována i způsobům pro implementaci interní konektivity v rámci FPGA. Zde se jeví jako nejvýhodnější využít nástroj, který je již certifikovaný a automaticky generuje propojovací strukturu s unifikovaným rozhraním. **V současné době je tímto nástrojem SOPC Builder (součást Quartus II), jehož použití pro drážní aplikace je potvrzeno například firmou Siemens.** V souvislosti s tímto nástrojem tedy nebyla objevena žádná skutečnost vyvracející možnost jeho použití. Jediným negativem tohoto nástroje tak zůstává fakt, že společnost Altera Corp. v současnosti končí s jeho podporou a přechází na produkt *Qsys System Integration Tool*, který se dočká certifikace dle IEC 61508 až koncem roku 2013. Z tohoto plyne, že **pro nové projekty, či pro projekty, které budou certifikovány od příštího kalendářního roku, je jednoznačně nejvýhodnější využívat Qsys System Integration Tool.** Tento nástroj se stává klíčovým elementem společnosti Altera Corp. a veškeré nové technologie (integrované procesorové jádra, transceivery, řadiče pamětí atd.) budou spojovány právě s tímto nástrojem. Výhody jeho použití byly diskutovány v předchozích kapitolách.

Literatura

- [1] IEC (ČSN EN) 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems (Funkční bezpečnost elektrických/ elektronických/ elektronických programovatelných systémů souvisejících s bezpečností).
- [2] IEC (ČSN EN) 50128: Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Software pro drážní řídicí a ochranné systémy
- [3] IEC (ČSN EN) 50129: Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Elektronické zabezpečovací systémy
- [4] IEC (ČSN EN) 50126: Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržitelnosti a bezpečnosti (RAMS)
- [5] A Validated Methodology for Designing Safe Industrial Systems on a Chip, Altera, 03/2013
- [6] 8 Reasons to Use FPGAs in IEC 61508 Functional Safety Applications, Altera, 10/2013

Seznam obrázků

Obr. 1 - Moderní koncepce řízení pohonu	9
Obr. 2 - Vývojový proces s ohledem na zvýšenou bezpečnost	10
Obr. 3 V-Model pro FPGA návrh	11

Historie revizí

Rev.	Kapitola	Popis změny	Datum Jméno / Odd.
1	Vše	První verze dokumentu	12.7.2013 PT/PB RICE
2	Vše	Review, finální úpravy	20.12.2013 PT/PB RICE