Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra informačních technologií

Studijní program: Aplikovaná informatika

Obor: Informatika

Zlepšování procesů při vývoji medicínského softwaru

SEMESTRÁLNÍ PRÁCE

KURZ: 4IT421 ZLEPŠOVÁNÍ PROCESŮ BUDOVÁNÍ IS

Vypracovali: Bc. Václav Nejedlý

Bc. Martin Jenšík

Přednášející: doc. Ing. Alena Buchalcevová, Ph.D.

LS 2015

Obsah

1 Úvod

Tato semestrální práce se zabývá popisem procesů ve společnostech zabývajících se vývojem softwaru (dále jen SW) pro medicínské účely. Tato oblast patří mezi tzv. **safety-critical** oblasti, což znamená, že na těchto SW mohou záviset lidské životy nebo zdraví osob.

Hlavním cílem práce je rešerše metodik, které jsou využívány při vývoji medicínského SW.

K napsání těchto rešerší byl využit hlavně osobní překlad knihy **Software Process Improvement and Capability Determination** (Software Process Improvement and Capability Determination, 2012), která představuje sborník z 12. mezinárodní konference o zlepšování procesů pří vývoji SW, která se uskutečnila v roce 2012 na Mallorce. Dále posloužili další odborné texty v anglickém jazyku na internetu a knihách. Pouze jeden český zdroj (ČVUT, 2014) doplňuje zdroje v anglickém jazyce.

Seminární práce je celkem rozdělena do pěti kapitol, kromě úvodu a závěru jsou obsahem práce tři hlavní kapitoly. Kapitola 2 se nazývá Safety-critical SW, která obecně popisuje co to je oblast safety-critical a čím jsou specifické systémy a SW v této oblasti. Stěžejní kapitolou je kapitola 3 - Přehled metodik a standardů pro vývoj medicínského SW, která je rešerší hlavních metodik a standardů pro vývoj medicínského SW. V kapitole 4 je detailněji rozepsána „metodika metodik pro vývoj medicínského SW“ – MEDI SPICE.

Výstupem této práce by mělo být seznámení ostatních studentů kurzu 4IT421 Zlepšování procesů budování IS se základními metodikami pro vývoji medicínského SW. Jedná se o uvedení do oblasti vývoje medicínského SW a tak by tato práce mohla do budoucna sloužit jako základ pro další práci, která by na tuto práci navazovala.

2 Safety-critical (SW) systémy

Safety-critical je oblast ve které hrají hlavní roli rizika ohrožení lidských životů, zdraví, ztráty nebo poškození věcí anebo poškození životního prostředí. Do safety-critical spadají oblasti veškeré dopravy, medicína či jaderný průmysl a další.

V těchto oblastech se vyskytuje celá řada systémů. Tyto systémy jsou označovány jako safety-critical systémy nebo také life-critical systémy. V této práci využíváme prvního pojmenování.

Pro příklad uvádíme jednu z definic Safety-critical sytému.

Safety-critical systém obecně: „*Safety-Critical systémy jsou takové systémy, jejichž selhání by mohlo mít za následek ztráty na životech, významné poškození majetku nebo poškození životního prostředí.“* (Proceedings of the 24th International Conference on Software Engineering ICSE 2002: May 19-25, s. 547-550, 2002)

V naší práci nás bude více zajímat definice safety-critical systému z technologického hlediska.

Safety-critical systém z technologického hlediska: „*Počítač, elektronický nebo elektromechanický systém, jehož selhání může mít za následek zranění nebo smrt člověka.“* (Safety-critical system, 2010)

Do této definice můžeme zahrnout i safety-critical SW, jenž je pro nás stěžejní v této semestrální práci.

Žijeme v době kdy naše bezpečí a životy jsou závislé na těchto safety-critical systémech. U těchto systémů musí být kladen vysoký důraz na spolehlivost.

Vývoj těchto systémů je vysoce náročný, jak časově, tak finančně. Proto se organizace snaží najít co nejvíce cenově výhodné metody, které jsou schopné se vypořádat s velikostí a složitostí těchto systémů a zároveň respektovat pravidla a zásady, které jsou schopné zajistit potřebu bezpečnosti těchto systémů. (LARRUCEA, Xabier, Annie COMBELLES a John FAVARO, 2013) Zajímavostí je že při návrhu těchto systému se počítá se ztrátou životů menší než jedna při biliónu operačních hodinkonkrétního systému. (ČVUT, 2014)

V důsledku toho jsme svědky vzniku bezpečných metodik na podporu řízení vývoje těchto safety-critical softwarů. Vývojáři mají zájem využívat opětovný model řízení vývoje těchto safety-critical softwarů v průběhu jejich celých životních cyklů. Z tohoto důvodů se začaly tvořit metodiky pro vývoj medicínského SW. (LARRUCEA, Xabier, Annie COMBELLES a John FAVARO, 2013)

V této práci se zabýváme jen a pouze medicínskými safety-critical systémy (SW) a hlavně jejich vývojem a k němu využívaných metodik a standardů.

3 Přehled metodik a standardů pro vývoj medicínského SW

V této kapitole se zabýváme stručným přehledem metodik a standardů v oblasti vývoje zdravotnických zařízení. Za účelem dosažení očekávané standardizace a lepšího řízení implementace SW zdravotních zařízení, publikovalo FDA (US Food and Drug Administration) CDRH (Center for devices and radiological health) řídící dokumenty, které zahrnují aktivity založené na riziku při validaci SW, postupy před uvedením výrobku na trh nebo situace kdy použít typový SW v oblasti zdravotních zařízení. Ačkoliv CDRH poskytuje v dokumentech potřebné informace, které SW aktivity mají být použity, Nepřikazují a nevynucují žádnou specifickou metodu, která má být použita.

V této kapitole se budeme zabývat následujícími normami a standardy:

- ISO/IEC 12207:1995/2008 - Systems and software engineering - Software life cycle processes a AAMI SW 68 - Medical device software - Software life cycle processes
- AAMI/IEC 62304:2006 - Medical device software – software life cycle processes
- ISO 14971:2007 - Medical devices - Application of risk management to medical devices
- MDD (1993/42/EEC) a MDD (2007/47/EC) – European Council directive
- ISO/IEC 15504-5 - Information technology — Process assessment

V kapitole 4 se podrobně zabýváme další metodikou, kterou je metodika MEDI SPICE.

3.1 Mezinárodní standard ISO/IEC 12207:1995/2008 a Standard AAMI SW 68

V oblasti zdravotních zařízení byla rozhodnutí z počátku realizována na základě tohoto standardu ISO/IEC 12207:1995, což je standard hlavního životního cyklu SW inženýrství a byl vhodný pro vývoj SW zdravotnických zařízení. Standard obsahuje procesy, činnosti a úkoly, které mají být použity při pořízení systému, který obsahuje SW, samostatný SW produkt nebo SW služby.

V roce 1995 byla vydána první verze tohoto standardu, která se dále vyvíjela až k dnešní nejnovější verzi mezinárodního standardu ISO/IEC 12207:2008. Standard stanovuje také procesy a činnosti používané při získání a nastavení služeb systému. K dispozici je ve

verzi 1995, 23 procesů, 95 aktivit, 325 úkolů a 224 výstupů, nová verze 2008 definuje 43 systémových a SW procesů.

Standard je založen na dvou základních principech: modularitě a odpovědnosti. Modularita znamená minimální zdvojování procesů a maximální soudržnost. Odpovědnost je za každý proces a také za zajištění aplikování standardu v projektech. Soubor procesů lze upravit dle daného projektu a tyto procesy jsou rozděleny do 3 typů: **Základní, Podpůrné a Organizační**. Podpůrné a Organizační existují nezávisle na organizaci a vykonání projektu a základní jsou instancemi dle situace.

Primární cyklus procesů obsahuje jádro procesů zapojených do vytváření SW produktů a tyto procesy jsou rozděleny do šesti základních fází:

1) Získávání
2) Dodávka
3) Vývoj
4) Provoz
5) Údržba
6) Odstavení

Každá fáze v rámci základních procesů může být rozdělena do různých aktivit. Níže uvádíme různé činnosti pro každý proces primárního životního cyklu.

Získávání

Zahrnuje všechny činnosti spojené se zahájením projektu. Tato fáze je rozdělena do několika činností jako Zahájení, Definování systémových požadavků, Definice globálních SW požadavků, Zhodnocení dalších možností, Definice přijatelnosti kritérií, Příprava návrhu apod. Dále samozřejmě definování způsobu projektu dle standardu a případné změny.

Dodávka

Na předchozí fázi navazuje fáze dodávky, ve které se připravuje smlouva a připravuje se výběrové řízení na dodavatele. Na základě požadavků a výběrového řízení jsou vybráni dodavatelé a je vypracován plán projektu. Tento plán obsahuje informace o projektu jako např. milníky apod. A je využit při další fázi, kterou je vývoj.

Vývoj

Ve vývojové fázi je SW produkt navržen, vytvořen a otestován tak aby byl připraven pro doručení k zákazníkovi. Metoda vývoje, která se používá v mnoha projektech má tzv. V-model. Techniky, které se používají při vývoji, jsou UML pro návrh a TMAP pro testování. Nejdůležitějšími kroky V-modelu jsou např. Definování funkčních požadavků (Shromáždění funkčních požadavků a požadavků na výrobek), Vytvoření vysoké úrovně designu (Základní uspořádání produktu, Nastavení a komunikace modulů), Návrhový modul (Podrobný popis modulů), Kódování, Provedení testu modulů (Testování funkčnosti jednotlivých modulů, Případný návrat k navržení modulu a oprava chyb), Test integrace (Test komunikace mezi moduly, případný návrat k designu a oprava chyb), Test systému (Kontrola přítomnosti funkčních požadavků)

Provoz

Fáze provozu a údržby probíhají současně, fáze provozu se skládá z aktivit na pomoc uživatelům při práci s vytvořeným SW produktem apod.

Údržba

Předposlední fází, na kterou navazuje již jen fáze odstavení, která nebude dále rozšiřována, je fáze údržby. Ta se skládá z údržby činností, obecných vylepšení, změn a dodatků, které mohou být vyžadovány od koncových uživatelů.

Nicméně po zkoušce ISO/IEC 12207, SW výbor asociace pro pokrok zdravotnického vybavení rozhodl, že je nutné vytvořit standard pro vývoj SW pro zdravotnická zařízení. Asociace používá ISO/IEC 12207:1995 jako základ pro nový standard AAMI SW68, SW zdravotních zařízení – Životní proces SW. V roce 2006 byl publikován nový standard AAMI/IEC 62304 jehož základem je právě zmíněný AAMI SW68.

3.2 Standard AAMI/IEC 62304:2006

Jak jsme již uvedli výše, standard IEC 62304 byl vyvinut na základě AAMI SW 68 a jedná se o standard, který specifikuje požadavky na životní cyklus pro rozvoj zdravotnického SW a SW v rámci zdravotnických prostředků. Je harmonizován v EU a USA a může být použit pro dosažení souladu s regulačními požadavky na obou těchto trzích.

Standard vysvětluje model rozhodování na základě rizikových situací a definuje požadavky na testování a podporu zdůvodnění proč měl být použit daný typ SW. Je zde několik hlavních rozdílů mezi IEC 62304 a AAMI SW68.

Do Standardu IEC 62304 byl přidán koncept klasifikace bezpečnosti SW. Byly identifikovány tři třídy bezpečnosti a výrobci jsou povinni připsat jednotlivé třídy bezpečnosti SW ke každému SW systému. Pro každou bezpečnostní třídu jsou požadovány specifické procesy a činnosti. Dalším rozdílem je, že ve standardu IEC 62304 není žádný rozdíl mezi základními a podpůrnými procesy, jako tomu je ve standardu AAMI SW68 resp. ISO/IEC 12207:1995/2008. Posledním důležitým rozdílem je, že nejsou v tomto standardu zahrnuty dva procesy, které byly v AAMI SW68. Jsou to procesy dokumentace a verifikace. Požadavky, které byly v těchto procesech, byly přesunuty do jiných procesů, kde jsou aplikovány.

IEC 62304:2006 je odvozena také ze standardu ISO/IEC 12207 vyvinuté Asociací AMMI (Association of Advancement of medical Instrumentation) a z již výše zmíněné AAMI SW68:2001. Zatímco ISO/IEC 12207 není oblastně specifikována, je velmi obsáhlá v postupech a odráží se od standardů jako ISO IEC 15504-5:2006 a ISO/IEC 90003.

Vyvíjený SW dle IEC 62304:2006 je založen na předpokladu, že SW je vyvíjen v souladu se standardem řízení kvality (ISO 13485:2006), standardem řízení rizik (ISO/IEC 14971) a standardem produktové úrovně (EN 60601-1).

IEC 62304:2006 definuje Model životního cyklu SW následovně:

Konceptuální struktura definuje životní cyklus SW dle definice požadavků na uvedení do výroby, které:

- Identifikují procesy, aktivity a činnosti zapojené do vývoje SW produktu
- Popisují posloupnosti a závislosti mezi aktivitami a činnostmi
- Identifikuje milníky, při kterých je ověřena úplnost uvedených výstupů

Tato definice je založena na definici dle standardu ISO/IEC 12207:1995.

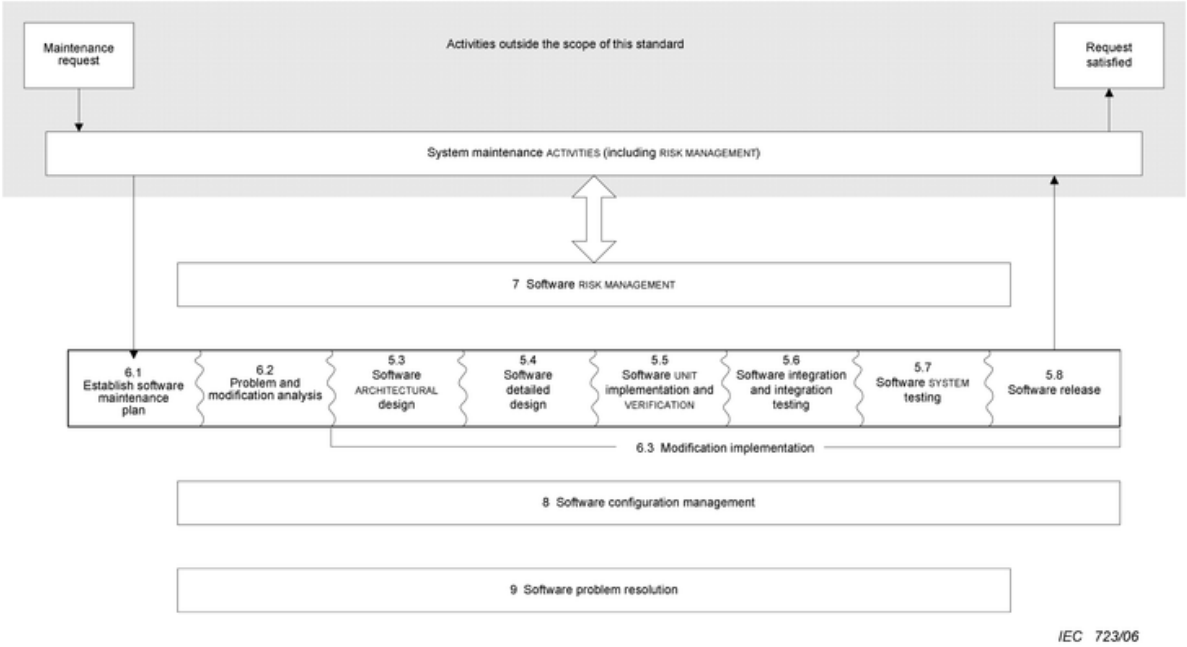
Standard poskytuje rámec pro procesy, aktivity a činnosti. Proces je rozdělen na aktivity a jednotlivé aktivity jsou rozděleny na dílčí činnosti. Procesy pro vývoj SW pro zdravotnická zařízení jsou dle standardu IEC 62304:2006 následující:

- Systém řízení kvality
- Klasifikace bezpečnosti SW
- Proces vývoje SW zahrnující:
    - Plánování vývoje SW
    - Analýza SW požadavků
    - Návrh SW architektury
    - Detailní návrh SW

- Implementace a verifikace SW jednotek
- Testování a integrace SW
- Systémové testování SW
- Vydání SW

- Proces údržby SW
- Proces řízení rizik
- Proces řízení konfigurace SW
- Proces řešení SW problémů

Níže je graficky znázorněno, jak tyto procesy zapadají do standardu IEC 62304:2006.



Obrázek 1 – Přehled procesů vývoje a aktivit SW, Zdroj: *O'CONNOR Rory V., ROUT Terry, MCCAFFERY Fergal, DORLING Alec, Software Process Improvement and Capability Determination*

Dle standardu IEC 62304:2006 je SW klasifikován dle závažnosti potenciálního ublížení a je dělen do jedné ze tří kategorií.

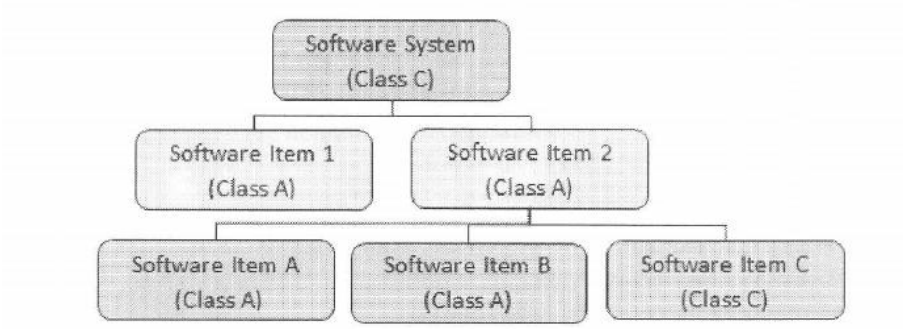
A. Není možné žádné zranění nebo poškození

B. Není možné žádné vážné zranění

C. Je možné vážné zranění nebo smrt

Toto rozdělení je předmětem standardu řízení rizik zdravotních zařízení ISO 14971:2007. Proces řízení rizik je tedy pokryt standardem ISO 14971:2007 a standard IEC 62304:2006 se na tento standard odkazuje.

Samostatný safety-critical SW může být rozdělen do položek běžících na rozdělených SW elementech s vlastní klasifikací bezpečnosti. Tento celý SW systém předpokládá nejvyšší klasifikaci obsaženou v každém SW elementu. Např. když systém obsahuje 5 SW částí (elementů), 4 z nich by byly klasifikovány jako třída A a jeden by byl klasifikován jako třída C, celý systém by měl být označen, jako třída C. Názorně to zobrazuje obrázek 2.



Obrázek 2 – Klasifikace SW položek a celého SW systému, Zdroj: *O'CONNOR Rory V., ROUT Terry, MCCAFFERY Fergal, DORLING Alec, Software Process Improvement and Capability Determination*

3.3 Standard ISO 14971:2007 a Standard EN ISO 13485:2003

Standard ISO 14971:2007 je standardem pro aplikaci řízení rizik na SW zdravotnických zařízení, na kterou se odkazuje již výše zmíněný standard IEC 62304:2006. Stanovuje požadavky na řízení rizik bezpečnosti zdravotních zařízení pro výrobce v průběhu celého životního cyklu SW.

Standard ISO 13485:2003 reprezentuje požadavky na komplexní systém řízení jakosti při návrhu i výrobě zdravotnických prostředků. Tento standard je harmonizován s normou ISO 9001 – Sytém řízení kvality, hlavním rozdílem je, že ISO9001 vyžaduje, aby organizace prokazovaly neustálé zlepšování, ISO 13485 vyžaduje pouze certifikaci organizací, že je systém jakosti zaveden a udržován.

Mezi další specifikace standardu patří např. Zaměření se na činnosti řízení rizik a kontrola aktivit v průběhu vývoje SW, Specifické požadavky na kontrolu implantabilních prostředků, požadavky na dokumentaci a ověřování postupů v oblasti sterilních zdravotních prostředků nebo zaměření na ověření účinnosti nápravných a preventivních opatření apod.

Shoda se standardem ISO 13485 a ISO 14971 je vnímána jako první krok k dosažení souladu s evropskými regulatorními požadavky. Dodržením těchto standardů je možné získat certifikát CE a povolení k prodeji lékařského zařízení v EU. Pro získání tohoto certifikátu je nutné dodržet také evropské direktivy pro zdravotnická zařízení (MDD), (1993/42/EEC) a MDD (2007/47/EC).

3.4 Evropská direktiva MDD (2007/47/EC)

MDD (2007/47/EC) je direktivou pro zdravotnická zařízení a je rozšířením direktivy MDD 1993/42/EC. Od března 2010 se stala povinnou pro získání CE certifikátu pro prodej zdravotnických zařízení. Tato direktiva je samozřejmě sladěna s množstvím standardů, mezi které patří např. EN ISO 14971:2009 nebo IEC EN 62304:2006.

Direktiva definuje Zdravotnické zařízení jako: *"jakýkoliv instrument, aparatura, spotřebič, SW, materiál nebo jiný výrobek, který je použit samostatně nebo v kombinaci, zahrnující SW od výrobců, pro použití specificky na diagnostiku a terapeutické účely a také pro vlastní aplikaci"*

Většina definic v direktivě MDD (1993/42/EEC) nebyla změněna s vydáním MDD (2007/47/EEC) avšak byla změněna definice MD (Medical device) se zvláštní referencí na samostatný SW, schopný být aktivním MD. Příklad SW jako aktivního MD je SW plánující dávky ozařování při léčbě rakoviny a kontrolující nastavení přístrojů při onkologické léčbě.

MDD (2007/47/EEC) řadí MD do jedné ze 4 kategorií:

- **Třída I** – Neinvazivní zařízení, pokud nejsou použity pro účely vyšetření krve, nebo tkáně nebo pokud nejsou úmyslně pro užití na rány na pokožce a mohou pouze léčit
- **Třída IIa** - Chirurgicky invazivní prostředky pro přechodné použití, pro kontrolu, diagnostiku, sledování nebo nápravu vad srdce a centrálního oběhového systému např. transfúzní zařízení nebo zařízení na skladování a přepravu dárcovských orgánů
- **Třída IIb** – Chirurgicky invazivní zařízení, implantabilní nebo určené pro dlouhodobé použití, pokud se dostanou do kontaktu se srdcem např. hemodialýza nebo nálevy k chronické ulceraci rozsáhlých ran
- **Třída III** – Zařízení pro podporu a udržení života a zařízení použitá v případě potenciálního rizika nepřiměřeného onemocnění nebo úrazu, např. kardiostimulátory nebo srdeční chlopně.

Toto rozdělení je založeno na rizicích pacientovi bezpečnosti, rozdělených od nejmenších po největší rizika. Čím vyšší je riziko pro pacienta, tím vyšší musí být úroveň klasifikace pro získání CE certifikace. Pokud je SW součástí zdravotnického zařízení, je předpokladem klasifikace pro celé zařízení. Pokud je samostatný SW aktivním zdravotním zařízením, je zařízení klasifikováno na základě rizika působení zařízení na pacienta nebo třetí osobou.

Direktiva 2007/47/EEC má velmi rozsáhlé důsledky, zařízení, která v minulosti nebyla klasifikována jako zdravotní zařízení, nebyla v souladu se standardy a nepodléhala jim,

jsou od publikace této direktivy klasifikována jako zdravotnická zařízení. To samozřejmě nastává v případě, že jsou zařízení připojena na aktivní zdravotní zařízení. Jako příklad můžeme uvést pouhou vizuální zobrazovací jednotku, která ukazuje výsledky ze zdravotních zařízení, tato jednotka je dle direktivy také brána jako zdravotnické zařízení a musí podléhat této direktivě.

3.5 Sada standardů ISO/IEC 15504-5

Sada standardů ISO/IEC 15504 Informační technologie – Posuzování procesu, známa také jako SPICE (Software Process Improvement and Capability Determination), je souborem standardů a dokumentů pro procesy vývoje SW a souvisejících funkcí řízení podniku. Tato sada standardů vznikla odvozením ze standardu ISO/IEC 12207, který je uveden výše v této práci. Zabývá se mimo jiné procesy, referenčními modely apod.

ISO/IEC 15504 obsahuje referenční model, který definuje rozměry procesů a dimenze schopností. Dále standard definuje prostředky pro ověření shody s referenčními modely. Procesní dimenze ISO/IEC 15504 rozděluje procesy do pěti kategorií:

- Zákazník/dodavatel
- Inženýrské
- Podpůrné
- Řídící
- Organizační

Pro každý proces standardu ISO/IEC 15504 definuje standard úroveň schopnosti (způsobilosti). Úrovně zobrazuje následující tabulka 1:

Tabulka 1 – Úrovně schopností, Zdroj: ***O'CONNOR Rory V., ROUT Terry, MCCAFFERY Fergal, DORLING Alec, Software Process Improvement and Capability Determination***

Úroveň	Název
5	Optimalizace procesů
4	Předvídatelné procesy
3	Založené procesy
2	Řídící procesy
1	Splněné procesy
0	Neúplné procesy

Způsobilost procesů se měří pomocí atributů těchto procesů. Standard vymezuje devět atributů pro jednotlivé procesy:

1. Výkon procesu
2. Řízení výkonnosti
3. Řízení práce na produktu
4. Definice procesu
5. Nasazení procesu
6. Postup měření
7. Kontrola procesu
8. Inovace procesu
9. Optimalizace procesu

Každý atribut se skládá z jedné nebo více generických praktik, které jsou dále zpracovány do praktických ukazatelů, podporujících hodnocení výkonnosti.

Hodnocení výkonnosti lze zobecnit do několika kroků:

- Zahájení posouzení
- Výběr hodnotitele a týmu hodnocení
- Plánování hodnocení, včetně procesů a organizačních jednotek
- Sběr dat a ověřování dat
- Hodnocení procesů
- Oznámení výsledků hodnocení

Model hodnocení procesu, je podrobným modelem používaným ke zhodnocení reálného stavu procesu. Jedná se o vypracování referenčního modelu procesu a životního cyklu procesu. Tento model je založen na referenčním modelu procesu dle standardu ISO/IEC 12207 a ISO/IEC 15288.

Standard popisuje několik nástrojů na získávání hodnocení procesů. Nejjednoduššími jsou papírové “nástroje”, obecné ukazatelé praxe a generické ukazatele praxe. K dispozici jsou také SW nástroje a indikátory umožňující uživatelům zadávat rozsudky, poznámky a výsledné sestavy utříděných hodnocení.

Standard ISO/IEC 15504 může být použit ve dvou kontextech. Pro zlepšování procesů a stanovení “schopností” (hodnocení způsobilosti procesů dodavatele). V prvním případě se tedy jedná o zlepšování procesů v rámci organizace technologií, poskytnutím standardů

pro posouzení organizačních schopností v každé fázi procesu. Stanovuje také požadavky na zlepšení program a poskytuje návody pro plánování a vylepšení. Druhým kontextem je stanovení schopností dodavatele, což můžeme chápat jako stanovení cílových funkcí pro dodavatele na základě potřeb organizace a zhodnocení dodavatele na základě řady cílových procesů.

4 MEDI SPICE

Výše popsané standardy jsou dobrým začátkem při validaci SW. Zatímco tyto standardy jsou obecně přijímány a řazeny pod MDD (Medical device directive), obsahují nedostatky, které je obtížné aplikovat do samostatného SW jako aktivního zdravotnického zařízení. Např. v IEC 62304 neexistuje ustanovující standard pro validaci systémových prvků samostatného SW.

Ve zdravotnické oblasti je hodně standardů, které jsou orientovány přímo na dodržování právních předpisů. Výsledkem soustředění vývoje zdravotnického SW je spíše dodržování než zlepšování procesů. Proto byl vyvinut MEDI SPICE. Předmětem MEDI SPICE je poskytovat procesní přehled a vývojový model, který je specifický pro vývoj zdravotnického SW a zahrnuje dodržení právních předpisů.

MEDI SPICE je také schopen sjednocovat rozdílné standardy v oblasti SW zdravotnických zařízení a přináší best-practises vhodné pro různé standardy do jednoho prostředí, které je vhodné pro vývojáře při implementaci jejich požadavků, stejně jako příklady procesního vývoje. Výsledek MEDI SPICE ustanovení, může být použit na zjištění stavu praktik dodavatelů zdravotnického SW ve vztahu k právním předpisům v oblasti, a identifikaci oblastí procesního vývoje. Může být také použit jako kritérium pro výběr dodavatele. Autoři věří, že s publikací MEDI SPICE budou k dispozici konkrétnější pokyny k základům návrhu a hodnocení procesů v oblasti výroby zdravotnických zařízení.

V&V v MEDI SPICE (Validace a Verifikace)

Na základě výzkumu, který zahrnoval rozsáhlé literární zkoumání a konkurenční analýzu standardů v oblasti zdravotnických zařízení a dalších safety-critical oblastí, byly zjištěny následující skutečnosti, které zahrnují definici procesů ve vztahu k V&V v MEDI SPICE.

a. Z analýzy vyplývá, že termíny V&V jsou často zaměňovány. FDA pokyny rozlišují mezi validací a verifikací. Ačkoliv FDA pokyny jsou jasné v definicích v sekcích 4, 5 a 6 FDA GPSV (General Principles of Software Validation), které se zabývají provozními aktivitami, stále používají pouze termín validace a žádné odkazy na verifikaci. Návrh MDD 2007/47/EC zdůrazňuje důležitost validace a potřeby pro současný stav validace a verifikace.

b. Verifikace není popsána jako samostatný proces ani ve standardu IEC 62304 a verifikační praktiky jsou integrovány do jiných činností. Validace je považována za proces systémové úrovně a nespadá do úrovně IEC 62304, i když se systém skládá výhradně ze SW.

c. Automotive SPICE má V&V kritéria a V&V záznamy jako výstupy procesů. ISO/IEC 15504-5 nesahá do této úrovně detailů.

d. IEEE Standardy V&V SW stanovují, že klasická nezávislá verifikace a validace je obecně potřebná pro vývoj SW systémů považovaných za kritické. Nezávislost je důležitým faktorem, popsaným DO-178B. Stupeň nezávislosti je také popsán ve standardu ISO/IEC 15504-5 a Automotive SPICE. FDA GPSV Sekce 4.9 popisuje nezávislost a ponechává na uvážení vývojářů zařízení, jak ji dosáhnout. Nezávislost není popsána v části IEC 62304 a předpokládá se, že je tak učiněno v ISO 13485. Proto je v MEDI SPICE kladena zvláštní pozornost na nezávislost verifikačních a validačních procesů.

e. SW vyvinutý pro koncern zdravotnických zařízení, získává právní potvrzení místo toho, aby se soustředil na zlepšování procesů s cílem dosáhnout účinnějšího vývoje SW. Modely jako CMMI a ISO/IEC 15504-5 mají samostatné procesní oblasti pro validaci a verifikaci. Samostatné procesy pro oblast kritickou jako V&V umožňující organizacím porozumět jejich síle a slabosti detailním způsobem a může poskytnout pomoc při podnětech k zavedení zlepšení procesů.

Na základě výzkumu, který zahrnoval rozsáhlé literární zkoumání V&V a konkurenční analýzu zlepšování modelů procesů a standardů bylo cílem popsat best practises v této oblasti a usnadnit zlepšování procesů. Cílem je také uspokojení požadavků pro relevantní standardy zdravotnických zařízení, zahrnující FDA GPSV, MDD, ISO/IEC 13485, IEC 62304, IEC TR 80002-1 a ISO14971. Pro dosažení cíle uspokojení požadavků standardů, bylo nutné je zahrnout do MEDI SPICE. K dosažení toho byly vyvinuty následující MEDI SPICE procesy se zvláštním důrazem na verifikaci a validaci.

1. SW konstrukce
2. SW integrace
3. SW testování
4. Verifikace
5. Validace

Na rozdíl od ISO/IEC 15504-5, kde nejsou požadavky na klasifikaci výstupů a procesů založených na bezpečnosti, to byla důležitá část, která se musela zahrnout do MEDI SPICE. Proto bylo použito klasifikační schéma poskytované IEC 62304, které je použito pro sdružení výstupů a specifických praktik s úrovní bezpečnosti SW, pro který jsou praktiky použitelné. Z praktik ISO/IEC 15504-5 a analýzy standardů ve stejných safety-critical oblastech bylo zjištěno, že by bylo vhodné použití Automotive SPICE jako odkaz, tak jak byl vyvinut pro popsání specifických požadavků na vývoj safety-critical SW. Výsledkem zkoumání bylo zahrnutí V&V jako samostatných procesních oblastí v MEDI SPICE. Pro-

ces validace zahrnuje mnoho doporučení, které byly vyprodukovány jako část výzkumu.

Souhrn V&V souvisejících procesů v MEDI SPICE

Pro splnění cílů analýzy, byl použit jako příklad proces SW testování v MEDI SPICE. Tento proces se vztahuje k IEC62304 SW system testing activity, která má 5 částí. Jako výstup analýzy byly zavedeny zvláštní praktiky (1-10) pro proces testování SW. Tyto praktiky a jejich mapování do relevantních standardů zdravotnických zařízení jsou ilustrovány v tabulce 2.

Oproti pěti částem, které IEC 62304 poskytuje, proces MEDI SPICE SW testing má 9 specifických praktik a 1 pod-praktiku. V souladu s good-practices k zajištění sledovatelnosti každé úrovně aktivity jak je pozorováno u ISO/IEC 15504-5, se MEDI SPICE zaměřuje na sledovatelnost každé aktivity, což je velmi důležité z pohledu verifikace. Kromě specifických praktik, je zde samostatná sub-praktika a další řízení implementace je poskytnuto v 10 poznámkách v procesu SW testování. Z tabulky 2 můžeme vyčíst, že specifická praktika – KONTROLNÍ AKTIVITY RIZIKOVÝCH ČINNOSTÍ, byla přidána jako část modelu.

Bylo tedy poskytnuto řízení aktivit přes MEDI SPICE dle ISO 14971 které vyžadují verifikace implementace kontroly rizik stejně jako verifikace redukce risku přes přijetí kontrolního mechanismu rizik.

Tabulka 2 – Praktiky testování SW podle IEC 62304 a MEDI SPICE, Zdroj: *O'CONNOR Rory V., ROUT Terry, MCCAFFERY Fergal, DORLING Alec, Software Process Improvement and Capability Determination*

IEC 62304 Reference	SUB Task/Doložka	MEDI SPICE REFERENCE	MEDI SPICE REFERENCE
5.7.1	Sestavení testů pro SW požadavky	ENG.8.SP1	Vývoj SW test strategie
		ENG.8.SP1.1	Sestavení sady testů
		ENG.8.SP2	Vývoj testovacích specifik pro SW testy
		ENG.8.SP4	Test integrovaného SW
5.7.2	Použití procesu řešení SW problémů	ENG.8.SP5	Záznam anomálií
5.7.3	Retest po změnách	ENG.8.SP9	Vývoj regresních strategií testování a provedení regresního testování
5.7.4	Verifikace systému SW testování	ENG.8.SP3	Verifikace test. Specifikací pro SW testování
		ENG.8.SP7	Verifikace SW testování

5.7.5	Záznam obsahu systému SW testování	ENG.8.SP6	Záznam výsledků SW testování
		ENG.8.SP8	Zajištění souladu a dvojstranné sledovatelnosti
		ENG.8.SP10	Kontrolní aktivity rizikových činností

Tabulka 3 ukazuje, jak byly popsány některé z typických činností SW testování s odkazy na FDA GPSV řídící dokument.

Tabulka 3 – Typické činnosti SW testování, Zdroj: *O'CONNOR Rory V., ROUT Terry, MCCAFFERY Fergal, DORLING Alec, Software Process Improvement and Capability Determination*

FDA typické činnosti	MEDI SPICE REFERENCE
Plánování testů	Konstrukce SW
Identifikace případů funkčního testování	Konstrukce SW
Analýza sledovatelnosti	Konstrukce SW Integrace SW Testování SW
Jednotkové provádění testu	Konstrukce SW
Provedení integrace testu	Integrace SW
Provedení funkčního testování	Integrace SW
Provedení systémového testování	Testování SW
Hodnocení chyb	Testování SW
Finální test report	Testování SW

Požadavky FDA GPSV jsou jasně popsány MEDI SPICE tak, jak mohou být sledovány z plánování. Další, co je potřeba zaznamenat je, že činnost Přijetí provedení testu není popsána MEDI SPICE jako část procesu SW inženýrství. To je souvislostí s Automotive SPICE tak jako ISO/IEC 15504-5 kde přijetí testování je částí získávání skupin procesů.

Dále k definici nastavení procesních oblastí a přidružených praktik vztažených k V&V. Ty by měly být řízeny v organizacích na poli vývoje SW pro zdravotnická zařízení. Na základě získaných výsledků zpětné vazby od společností na poli vývoje SW pro zdravotnická zařízení, by měly být procesy hodnoceny a dále zlepšovány.

Jak V&V vstřebává významné množství projektového času, další výzkum by měl být proveden na praktiky, které mohou přinést snížení potřebného času na V&V aktivity ale ne na úkor kvality a bezpečnostních požadavků vyvíjených produktů.

Globalizace vývoje SW vedla k distribuovaným týmům pracujícím na stejném projektu v různých lokalitách. Pochopení problémů v globálně distribuovaném V&V v kontextu s vývojem SW pro zdravotní účely a další praktiky, mohou v těchto případech

jen přispět. Tyto praktiky se mohou stát poznámkami a dalšími sub-praktikami v další verzi MEDI SPICE.

5 Závěr

Je vidět, že metodiky se stále ještě vyvíjejí. MEDI SPICE je na dobré cestě stát se zastřešující metodikou pro vývoj medicínského SW, podle které by se mohl tento vývoj řídit dlouhá léta. Určitě je dobře, že tyto metodiky existují a vývoj safety-critical SW je nějakým způsobem řízený dle těchto metodik. Díky tomu můžeme více důvěřovat těmto systémům, které mají leckdy na starosti náš život.

Doufáme, že práce poskytla zajímavý úvod do vývoje medicínského SW a že mnoho ostatních studentů tento úvod do metodik zaujal natolik, že na naší práci někdo v budoucnu bude navazovat a bude se na ni odkazovat v rešerši konkrétní navazující práce. Dle našeho názoru byly cíle naplněny z jedné části již při průběžné prezentaci na kurzu 4IT421 Zlepšování procesů budování IS, kdy jsme ostatním studentům představili úvod do metodik a pokud to někoho zaujalo více, tak bude mít k dispozici tuto plnou verzi semestrální práce. Druhý cíl bude splněn, když tato práce v budoucnu poslouží jak základ pro další práce, které na tuto práci naváží a tuto oblast popíší více do hloubky.

Drobným omezení při psaní práce byl fakt, že téměř žádný zdroj nebyl v českém jazyce. Překlady zdrojů tak zvyšovaly časovou náročnost psaní této práce a občas se při překladech může stát, že se některé formulace přeloží jinak, než to bylo myšleno v původním cizojazyčném zdroji. Věříme však, že toto nebyl náš případ a že veškeré odstavce jsou přeloženy a přeformulovány do českého jazyka správně. Což může pojišťovat i průběžná prezentace v rámci kurzu 4IT421 Zlepšování procesů budování IS za dohledu odporného akademického dozoru.

Seznam zdrojů

Knižní zdroje

- **(Proceedings of the 24th International Conference on Software Engineering ICSE 2002: May 19-25, 2002)**
  Proceedings of the 24th International Conference on Software Engineering ICSE 2002: May 19-25, 2002, Orlando, Florida. New York: Association for Computing Machinery, c2002, xxiii., 744 s. ISBN 158113472x.

- **(Software Process Improvement and Capability Determination, 2012)**
  O'CONNOR Rory V., ROUT Terry, MCCAFFERY Fergal, DORLING Alec, Software Process Improvement and Capability Determination. Germany: Springer-Verlag Berlin and Heidelberg GmbH & Co. KG, 2012. 316 s. ISBN 9783642304385.

Internetové zdroje

- **(ČVUT, 2014)**
  ČVUT. Programové vybavení avionických systémů. In: *ČVUT v Praze* [online]. 2014 [cit. 2015-05-05]. Dostupné z: http://measure.feld.cvut.cz/groups/LIS/download/prednasky/EPS1/Programov%C3%A9%20vybaven%C3%AD%201%20.pdf

- **(LARRUCEA, Xabier, Annie COMBELLES a John FAVARO, 2013)**
  LARRUCEA, Xabier, Annie COMBELLES a John FAVARO. Safety-Critical Software [Guest editors' introduction]. In: *IEEE Software* [online]. 2013 [cit. 2015-05-02]. Dostupné z: http://www.computer.org/csdl/mags/so/2013/03/mso2013030025-abs.html

- **(Safety-critical system, 2010)**
  Safety-critical system. In: *Dictionary.com* [online]. 2010 [cit. 2015-05-02]. Dostupné z: http://dictionary.reference.com/browse/safety-critical+system

Seznam obrázků a tabulek

Seznam obrázků

Seznam tabulek