SPECIFIKA CERTIFIKACE PODLE ČSN EN ISO 9001:2001 V ORGANIZACÍCH, KTERÉ SE ZABÝVAJÍ VÝVOJEM SOFTWARE

Václav Šebesta

Ústav informatiky Akademie věd ČR, e-mail: vasek@cs.cas.cz

Abstrakt
Jestliže ještě před několika lety platilo, že pro společnosti, zabývajícími se vývojem a dodávkami softwarových produktů, je certifikace systému jakosti marketingovou výhodou, platí dnes spíše obrácené pravidlo, že chybějící certifikace je dosti vážným nedostatkem, který může podstatně snížit prodejnost nabízených programových produktů, zejména při dodávkách do organizací státního sektoru. Při certifikačních i dozorových prověrkách podle normy ČSN EN ISO 9001:2001 se opakovaně setkáváme s některými nedostatky a nepřesnostmi aplikace této normy na konkrétní situaci v prověřované společnosti. Tento příspěvek se pokouší vysvětlit některá specifika aplikace této normy pro výrobce SW produktů a napomoci jim lépe se připravit na certifikaci nebo recertifikaci.

1. Úvod

Kromě všeobecně známých norem [1], [2] a [3] (včetně jejich starších verzí z roku 1994) jsou některá aplikační specifika vývoje programových produktů přehledně shrnuta v normě ISO 9000-3:1997 Směrnice pro použití ISO 9001:1994 při vývoji, dodávání a udržování SW. Při poslední revisi normy ISO 9000 z roku 2000 však tato pomocná norma nebyla aktualizována a ze seznamu inovovaných norem byla vypuštěna.

Tvorbu SW programů, ať už šitých na míru pro jednotlivé zákazníky, (tzv. „zákaznický SW“) nebo opakovaně prodávaných více zákazníkům (tzv. „krabicový SW“) musíme vždy považovat ve smyslu výše uvedené normy za vývoj nového výrobku. Vztahují se tedy na něj všechna ustanovení kapitoly 7.3 „Návrh a vývoj“ normy ISO 9001:2000. Naštěstí nejsou mezi požadavky staré a nové normy v této oblasti kromě změny struktury žádné další podstatné věcné rozdíly.

Stejně jako pro všechny ostatní certifikované vývojové činnosti společnosti musí být i pro návrh software:

- popsán odpovídající proces nebo procesy vývoje SW,
- specifikovány vstupy a výstupy každého vývojového projektu (zakázky),
- vedena agenda řízení neshodného výrobku,
- dokumentováno přezkoumání, ověření (verifikace) a validace vývoje,
- udržováno dokumentované řízení konfigurace, zvláště v případě krabicového SW, ale i pro opakovaný vývoj zákaznického SW,
- dokumentováno řízení změn při vývoji.

2. Procesy pro řízení návrhu SW

Popis návrhu software může být zpracován buď jako jeden proces nebo ve větších organizacích jako několik navazujících procesů. Každý proces musí mít specifikovány všechny náležitosti požadované normou, tedy vstupy a výstupy procesu, vlastníka procesu, měřitelné parametry (metriky) procesu, odpovědnosti za každý krok procesu, seznam a strukturu záznamů, které v průběhu vývoje programových produktů vznikají apod. Vstupem procesu bývá nejčastěji v případě krabicového SW rozhodnutí vedení organizace nebo pověřeného pracovníka o vývoji nového programu nebo nové verze programu, v případě zákaznického SW pak objednávka zákazníka. Výstupem procesu není jen sestavený, odladěný a otestovaný program ve zdrojovém i zaváděcím kódu, ale i veškerá programová, systémová, implementační, provozní a uživatelská dokumentace.

Velmi důležitým prvkem popisu procesu je i určení měřitelných parametrů (metrik) procesu, které budou ve stanovených intervalech (čtvrtletně, ročně) měřeny a vyhodnocovány, čímž vznikne jedna nebo několik časových řad, z jejichž trendů bude možné zjistit, zda a jak dobře proces návrhu SW funguje. Každý z těchto parametrů musí mít i deklarovanou cílovou hodnotu, kterou chce firma dosáhnout v nejbližším období. Praxe ukazuje, že je vhodnější k tomuto účelu používat spíše poměrové ukazatele (např. poměr mezi plánovanou a skutečnou dobou vývoje, poměr mezi plánovanými a skutečnými náklady, poměr mezi počtem zákaznických reklamací a počtem interně zjištěných neshod) než absolutní ukazatele. Náklady na vývoj, počet neshod v procesu vývoje, počet vyvinutých programů apod. mohou spíše sloužit za příklady nepříliš vhodně zvolených metrik, protože z jejich trendů nelze zpravidla posoudit kvalitu vývojového procesu. Na základě analýzy trendů metrik by měla být přijímána nápravná a preventivní opatření podle kapitoly 8.5 normy a tím uzavřena smyčka PDCA a splněn tak požadavek na kontinuální zlepšování.

V procesu návrhu musí být zpracován plán návrhu pro každý SW produkt nebo jeho novou verzi, ve kterém budou specifikovány etapy vývoje, časový harmonogram vývoje, odpovědnosti a pravomoci jednotlivých členů vývojového týmu, způsob testování vyvíjeného produktu, způsob řízení změn ve vývoji apod.

3. Dokumentace vývojových projektů

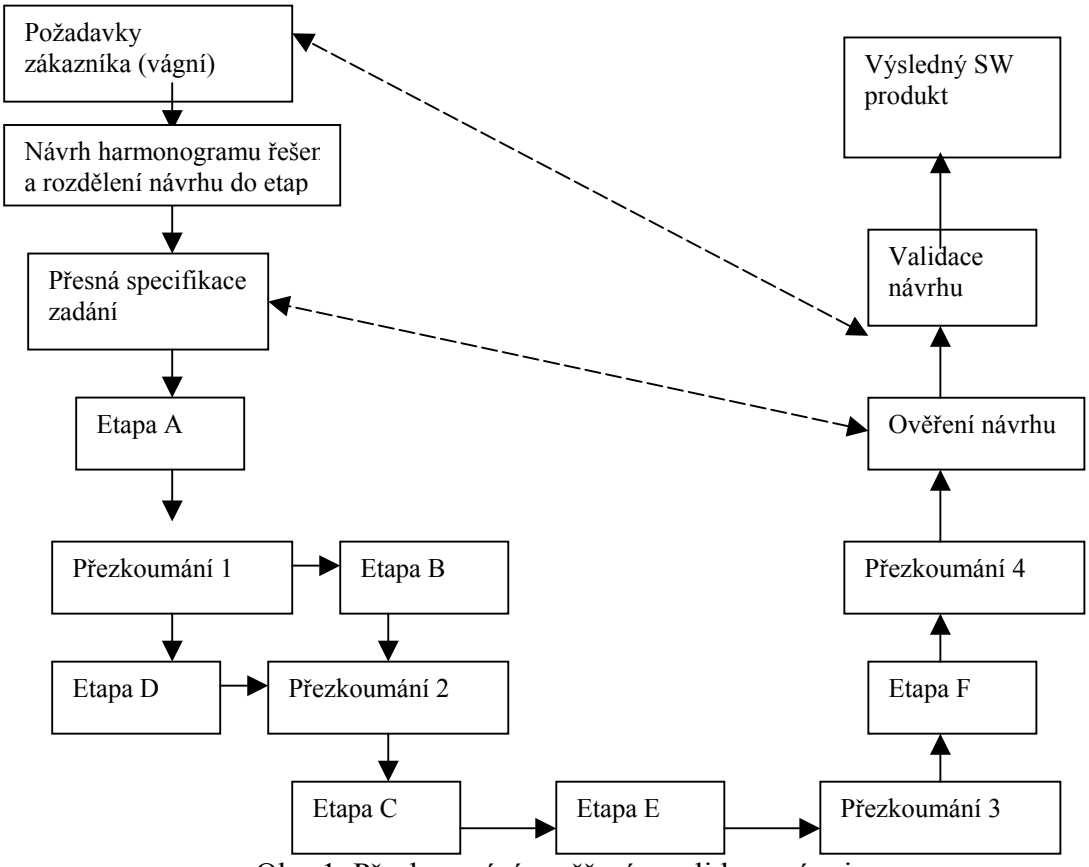
Podle výše popsaného procesu budou probíhat jednotlivé vývojové projekty. Záznamy o každém projektu by měly obsahovat:

- Specifikaci požadavků na výsledný SW produkt včetně uvedení příslušných zákonů, předpisů a norem. Zpravidla jsou první požadavky zadány zákazníkem (a z hlediska přesnosti bývají značně vágní). V dalších krocích procesu vývoje je podle nich (ve spolupráci se zákazníkem) nutno vypracovat podrobnou a dostatečně přesnou specifikaci funkčních požadavků a ostatních požadavků na provedení. Za základ je možno vzít popis vstupních požadavků např. podle normy ANSI/IEEE 830.
- Přesná specifikace výstupů vývoje, tj. v jaké formě bude vyvinutý produkt předáván k dalšímu zpracování, jaké záznamy a protokoly budou v procesu vývoje vznikat, jaká dokumentace uživatelská, programátorská, implementační, provozní apod.
- Záznamy o přezkoumání vývoje, tj. o kontrole výsledků na úrovni jednotlivých etap vývoje, např. jednotlivých programových modulů a dokumentované odstranění případných nedostatků.

- Záznamy o ověřování vývoje, tj. např. protokoly o provedení testů všech funkcí, které měl program provádět podle specifikace funkčních požadavků a dokumentované odstranění případných nedostatků.
- Záznamy o validaci vývoje, tj. záznamy o testování programového produktu v provozním prostředí a případné odstranění nalezených nesrovnalostí. Typickou validací vývoje krabicového SW jsou tzv. beta-testy, kdy je program předán vybrané skupině uživatelů k otestování a vyjádření připomínek. Validace zákaznického SW se zpravidla provádí zkušebním provozem u zákazníka. Validace musí být ukončena před předáním SW produktu zákazníkovi, pokud ve smlouvě mezi výrobcem SW a zákazníkem není stanoveno jinak. O připomínkách a jejich vypořádání musí být vedeny záznamy.
- Plánované přezkoumání, ověření a validace mohou tvořit plán jakosti výrobku.
- Záznamy o změnách v procesu návrhu. Každá změna nebo doplnění vstupních specifikací, změny termínů a harmonogramu vývoje, vývojových etap apod. musí být zaznamenána příslušnou formou, včetně schválení pracovníkem s odpovídající pravomocí.
- O nalezených nedostatcích (neshodách) při přezkoumání, ověřování a validaci je nutno vést v dokumentované formě evidenci, včetně způsobu jejich nápravy a odstranění nedostatků. V určených intervalech je nutno provádět analýzu těchto nedostatků a podle jejích výsledků se snažit zlepšovat proces návrhu.

4. Přezkoumání, ověření a validace vývoje SW

Velmi často není v certifikovaných organizacích zcela jasný vztah mezi přezkoumáním, ověřením a validací. Pokusme se vysvětlit si tyto pojmy na následujícím příkladu:



Obr. 1. Přezkoumání, ověření a validace vývoje

Uvědomíme-li si, že v naprosté většině případů jsou požadavky zákazníka formulovány velmi vágně nebo dokonce vznikají až v průběhu návrhu, bude rozdíl mezi ověřením a validací návrhu zcela zřejmý. V průběhu validace (nejčastěji při zkušebním provozu nebo připomínkami vybraných zákazníku při testování beta-verzí) je výrobce velmi často upozorňován na závady, které nemají oporu v počátečních požadavcích zákazníka na SW produkt. Závisí pak na marketingové a obchodní strategii výrobce, jak se s takovými případy vypořádá.

Z obrázku je také zřetelněji vidět, proč je důležité dokumentované odstraňování neshod ve všech fázích vývojového procesu. Záznamy o neshodách i jejich odstranění jsou k dispozici ve všech dalších etapách návrhu a při provádění následných testů je potřeba zaměřit se kromě nových funkčních požadavků i na ty funkce programu, u nichž již v předcházejících testech byly odhaleny problémy.

Počet přezkoumání návrhu je závislý na počtu vývojových etap a lze doporučit, aby po každé etapě, kde vzniká nějaký reálný výstup, např. programový modul nebo součást dokumentace programového díla bylo provedeno nezávislé přezkoumání výsledku vývojové etapy (etap) osobou, která se nepodílela na vlastním naplňování příslušné etapy včetně zaznamenání nalezených neshod. Tento požadavek je samozřejmě v organizacích s velmi malým počtem programátorů (kteří často provádějí i testování) jen obtížně splnitelný.

Ověření návrhu je nezbytné provést na konci celého návrhového procesu, v některých případech může však být účelné provést částečné ověření po dokončení nějaké ucelené části SW produktu, jehož funkčnost může být testována samostatně. Validaci je vždy potřeba provádět v provozních podmínkách až na konci celého vývojového procesu. Jen zřídka je výrobce SW schopen tyto podmínky plně simulovat ve vlastním prostředí, zpravidla proto bývá validace prováděna u zákazníků. Validace musí být ukončena a případné nalezené nedostatky odstraněny ještě před předáním SW produktu zákazníkovi.

V případě návrhu velmi jednoduchých SW produktů může splynout přezkoumání a ověření návrhu (např. když nelze rozumně rozdělit proces návrhu do etap, celý vývoj proběhne v jediné etapě a není vytvářena žádná nová programová dokumentace.). Také ověření a validace mohou výjimečně splynout, jestliže zákaznická specifikace požadavků na produkt je dostatečně přesná a provozní podmínky se neliší od vývojového prostředí (je zřejmé, že k tomu dochází jen ve zcela výjimečných případech) a kdy se ověřování provádí dostatečně podrobně a po delší dobu.

5. Řízení konfigurace programových produktů

Vývoj programových produktů, které jsou dodávány více zákazníkům, nebo jednomu zákazníkovi ve více dodávkách, vyžaduje vedení záznamů o konfiguraci. Oporou tohoto požadavku je znění kapitoly 7.5.3. Identifikace a sledovatelnost.

Certifikovaná organizace musí mít záznamy o tom, kterou verzi každého programového produktu (samozřejmě pokud existuje více než jedna verze) má který zákazník, případně ze kterých verzí jednotlivých modulů je výsledná verze produktu sestavena. Dodržení tohoto požadavku je zvláště důležité při servisních a reklamačních zásazích, kdy je často potřeba zjistit přesnou konfiguraci dodaného programu konkrétnímu zákazníkovi. Tato konfigurace se navíc může i poměrně často měnit při automatickém nebo smluvním dodávání záplat nebo nových verzí programu. Pro řízení konfigurace je někdy postačující poměrně jednoduchá

tabulka se seznamem verzí programového produktu a seznamem zákazníků, jindy je žádoucí používat sofistikovanější programové produkty, které jsou dnes na trhu k dispozici. Řízení konfigurace je také předmětem několika mezinárodních norem, např. IEEE 1042.

Literatura:

1. ČSN EN ISO 9000:2000: Systémy managementu jakosti – Základy, zásady a slovník
2. ČSN EN ISO 9001:2001: Systémy managementu jakosti – Požadavky
3. ČSN EN ISO 9004:2001: Systémy managementu jakosti - Směrnice pro zlepšování výkonnosti. (Doplňuje a rozšiřuje normu ISO 9001)
4. ISO 9000-3:1997: Směrnice pro použití normy ISO 9001:1994 při vývoji, dodávání a udržování SW
5. ANSI/IEEE 830: Návod pro stanovení požadavků na programové vybavení
6. ISO EN 17799: Information security management systems – Specification with guidance to use
7. IEEE 1042: Směrnice pro řízení konfigurace SW