Security by Design with CMMI for Development, Version 1.3

4IT421 - Zlepšování procesů budování IS
Bc. Michal Vodrážka (xvodm12)
přednášející: doc. Ing. Alena Buchalcevová, Ph.D.
ZS 2013/2014

Obsah

1. Úvod

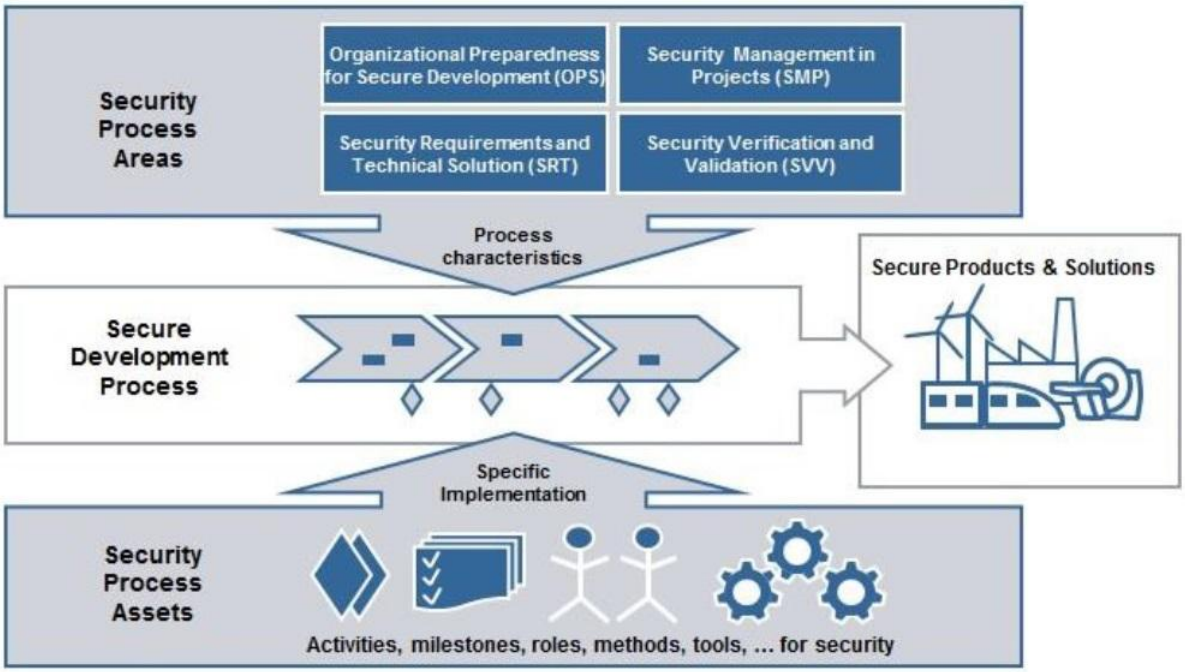
Nejprve bych rád uvedl, proč jsem si zvolil téma práce „*Security by Design with CMMI for Development, Version 1.3*“.
Toto téma považuji jednak za velmi zajímavé a taky především aktuální z pohledu současných bezpečnostních hrozeb. Rovněž bych rád nabyl znalosti o bezpečnosti coby aspektu návrhu (Security by Design), jelikož jsem se s tímto pojmem dosud nesetkal.
Cílem mé práce je popsat bezpečnost coby aspekt návrhu (Security by Design) a blíže popsat vztah bezpečnostní procesní oblasti Security Verification and Validation (SVV) s procesními oblastmi Verification (VER) a Validation (VAL) z Integračního modelu zralosti pro vývoj verze 1.3 (Capability Maturity Model Integration for Development, version 1.3 = CMMI-DEV v1.3) a jejich srovnání.
Budu se tedy ve své práci přednostně zabývat touto jednou bezpečnostní procesní oblastí z důvodu dodržení rozsahu práce. Bezpečnostní procesní oblast Security Verification and Validation (SVV) jsem si zvolil z přesvědčení, že se jedná o nejdůležitější bezpečnostní procesní oblast pro vývoj softwaru ze všech čtyř bezpečnostních procesních oblastí v rámci bezpečnosti coby aspektu návrhu (Security by Design).

Abych cíle dosáhl, využiji teoretické poznatky ze studia odborných materiálů a své již nabyté znalosti během studia. Stěžejní část této semestrální práce je rozčleněna na část týkající se tří bezpečnostních procesních oblastí a část týkající se bezpečnostní procesní oblasti Security Verification and Validation (SVV), přičemž se bezpečnost coby aspekt návrhu (Security by Design) sestává právě z těchto čtyř bezpečnostních procesních oblastí. U každé bezpečnostní procesní oblasti uvedu charakteristiku, její strukturu a v případě bezpečnostní procesní oblasti Security Verification and Validation (SVV) i její vztah k relevantním procesním oblastem v rámci CMMI-DEV v1.3.

2. Security by Design

Integrační model zralosti pro vývoj verze 1.3 (CMMI-DEV v1.3) je společně s Integračním modelem zralosti pro akvizice verze 1.3 (CMMI-ACQ v1.3) a s Integračním modelem zralosti pro služby verze 1.3 (CMMI-SVC v1.3) součástí Integračního modelu zralosti verze 1.3 (CMMI v1.3) z roku 2010, jehož první verze vznikla v roce 2000 v Institutu pro softwarové inženýrství (Software Engineering Institute = SEI), který sídlí v areálu Univerzity Carnegie Mellon v Pittsburghu (USA). Integrační model zralosti pro vývoj verze 1.3 (CMMI-DEV v1.3) je referenčním modelem procesů, který pokrývá celý životní cyklus softwarového produktu, přičemž definuje 22 procesních oblastí rozdělených do čtyř kategorií. Těmito čtyřmi kategoriemi jsou: Řízení procesu (Process Management), Řízení projektu (Project Management), Inženýrství (Engineering) a Podpora (Support).[1, s. 102];[2, s. 22]

Bezpečnost coby aspekt návrhu (Security by Design, doprovodný dokument byl vytvořen v roce 2013) vychází z předpokladu, kdy organizace chtějí úspěšně vyvíjet bezpečné produkty pomocí ustálených procesů, které zahrnují využití zkušeností, schopností a bezpečnostních technik. Cílem je tedy vytvořit komponenty procesního modelu, které poslouží k vytvoření a zlepšování těchto procesů. K definici charakteristik pro proces vývoje poslouží čtyři bezpečnostní procesní oblasti, přičemž dvě tyto oblasti pokrývají bezpečnostní aspekty inženýrství, jedna oblast se týká řízení bezpečnosti v projektech a jedna oblast se zabývá organizačními tématy týkající se bezpečnosti. Implementací těchto bezpečnostních procesních oblastí organizace přizpůsobuje pracovní postupy (workflows), procesy a procesní aktiva (process assets). Příkladem je zavedení nových nebo změna stávajících procesních aktivit, milníků, rolí, metod nebo nástrojů. Pomocí těchto aktivit organizace vytváří produkty, které jsou bezpečné díky návrhu.[3, s. 3]



Obrázek 1a - Znázornění vlivu bezpečnosti coby aspektu návrhu (Security by Design) na proces bezpečného vývoje produktu či řešení.[3, s. 3]

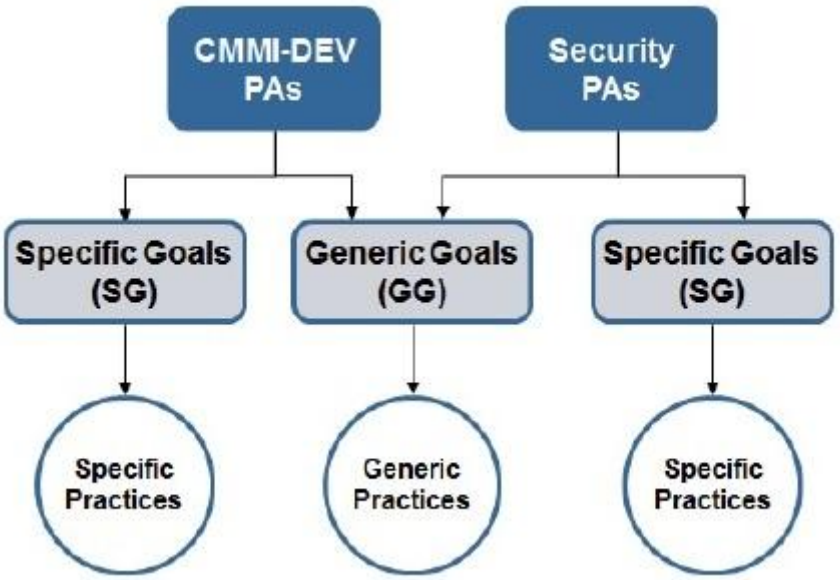
Bezpečnostní procesní oblasti mají stejnou strukturu jako procesní oblasti v rámci CMMI-DEV v1.3. Sestávají se tedy z obecných cílů a následně ze specifických cílů, od kterých se odvíjejí obecné praktiky, resp. specifické praktiky. Bezpečnostní procesní oblasti a procesní oblasti v rámci CMMI-DEV v1.3 mají stejné obecné cíle a obecné praktiky.[3, s. 9]

Souhrn obecných cílů a obecných praktik:

1.1) Obecný cíl: Dosáhnout specifických cílů
1.1.1) Obecná praktika: Provádění specifických praktik

1.2) Obecný cíl: Institucionalizovat proces jakožto řízený proces
1.2.1) Obecná praktika: Zřízení organizační politiky
1.2.2) Obecná praktika: Plánování procesu
1.2.3) Obecná praktika: Zajištění zdrojů
1.2.4) Obecná praktika: Přiřazení odpovědností
1.2.5) Obecná praktika: Vyškolení lidí
1.2.6) Obecná praktika: Kontrola pracovních produktů
1.2.7) Obecná praktika: Identifikace a začlenění relevantních vlastníků
1.2.8) Obecná praktika: Monitoring a kontrola procesu
1.2.9) Obecná praktika: Objektivní vyhodnocení dodržení politiky
1.2.10) Obecná praktika: Zhodnocení stavu s nadřízeným vedením

1.3) Obecný cíl: Institucionalizovat proces jakožto definovaný proces
1.3.1) Obecná praktika: Zřízení definovaného procesu
1.3.2) Obecná praktika: Získávání relevantních zkušeností



Obrázek 1b - Znázornění podobnosti struktury procesních oblastí CMMI-DEV v1.3 a struktury bezpečnostních procesních oblastí.[3, s. 9]

Bezpečnostní procesní oblasti rozšiřují procesní oblasti v rámci CMMI-DEV v1.3 ve třech kategoriích: Řízení procesu (Process Management), Řízení projektu (Project Management) a Inženýrství (Engineering).

Kategorie procesních oblastí Řízení procesu (Process Management) zahrnuje činnosti spojené s řízením procesů na úrovni celé organizace.
V rámci kategorie Řízení procesu (Process Management) jsou ze strany CMMI-DEV v1.3 procesní oblasti Organizational Process Definition (OPD) a Organizational Training (OT) rozšířeny bezpečnostní procesní oblastí Organizational Preparedness for Secure Development (OPSD).

Kategorie procesních oblastí Řízení projektu (Project Management) zahrnuje oblasti, které pokrývají činnosti řízení projektu.
V rámci kategorie Řízení projektu (Project Management) jsou ze strany CMMI-DEV v1.3 procesní oblasti Project Planning (PP), Supplier Agreement Management (SAM) a Integrated Project Management (IPM) rozšířeny bezpečnostní procesní oblastí Security Management in Projects (SMP).

Kategorie procesních oblastí Inženýrství (Engineering) pokrývá činnosti vývoje a údržby v různých inženýrských disciplínách a týká se vývoje produktu nebo služby.
V rámci kategorie Inženýrství (Engineering) jsou ze strany CMMI-DEV v1.3 procesní oblasti Requirements Development (RD) a Technical Solution (TS) rozšířeny bezpečnostní procesní oblastí Security Requirements and Technical Solution (SRTS).
V rámci kategorie Inženýrství (Engineering) jsou ze strany CMMI-DEV v1.3 procesní oblasti Verification (VER) a Validation (VAL) rozšířeny bezpečnostní procesní oblastí Security Verification and Validation (SVV).[2, s. 22];[3, s. 15]

Obrázek 1c - Znázornění vztahů mezi bezpečnostními procesními oblastmi a procesními oblastmi v rámci CMMI-DEV v1.3.[3, s. 15]

3. Bezpečnostní procesní oblasti

V této kapitole uvedu tři bezpečnostní procesní oblasti: Organizační připravenost pro bezpečný vývoj (Organizational Preparedness for Secure Development), Řízení bezpečnosti v projektech (Security Management in Projects) a Bezpečnostní požadavky a technické řešení (Security Requirements and Technical Solution).

3.1. Bezpečnostní procesní oblast: Organizational Preparedness for Secure Development (OPSD)

První bezpečnostní procesní oblastí je Organizační připravenost pro bezpečný vývoj (Organizational Preparedness for Secure Development).
Cílem této bezpečnostní procesní oblasti je stanovit a udržovat schopnosti vyvíjet bezpečné produkty a reagovat na reportované nedostatky zabezpečení.[3, s. 4]

V rámci kategorie Řízení procesu (Process Management) jsou ekvivalentem ze strany CMMI-DEV v1.3 procesní oblasti Organizational Process Definition (OPD) a Organizational Training (OT), které tato bezpečnostní procesní oblast rozšiřuje.

Souhrn specifických cílů a specifických praktik:

2.1) Specifický cíl: Zavést schopnost organizace vyvíjet bezpečné produkty
2.1.1) Specifická praktika: Získat závazek managementu a sponzorství pro bezpečnost a zabezpečení obchodních cílů
2.1.2) Specifická praktika: Zavést standardní procesy a jiná procesní aktiva pro bezpečný rozvoj
2.1.3) Specifická praktika: Vytvořit povědomí, znalosti a dovednosti pro bezpečnost produktu
2.1.4) Specifická praktika: Vytvořit bezpečnostní standardy pracovního prostředí
2.1.5) Specifická praktika: Stanovení zranitelnosti při manipulaci[3, s. 18-27]

3.2. Bezpečnostní procesní oblast: Security Management in Projects (SMP)

Druhou bezpečnostní procesní oblastí je Řízení bezpečnosti v projektech (Security Management in Projects).
Cílem této bezpečnostní procesní oblasti je stanovit, identifikovat, plánovat, a řídit činnosti související s bezpečností v rámci životního cyklu projektu a řídit rizika bezpečnosti produktů.[3, s. 4]

V rámci kategorie Řízení projektu (Project Management) jsou ekvivalentem ze strany CMMI-DEV v1.3 procesní oblasti Project Planning (PP), Supplier Agreement Management (SAM) a Integrated Project Management (IPM), které tato bezpečnostní procesní oblast rozšiřuje.

Souhrn specifických cílů a specifických praktik:

3.1) Specifický cíl: Připravit a řídit projektové aktivity v rámci bezpečnosti
3.1.1) Specifická praktika: Zavést integrovaný projektový plán pro bezpečnost projektů
3.1.2) Specifická praktika: Plánovat a provést bezpečnostní školení
3.1.3) Specifická praktika: Zvolte bezpečného dodavatele a komponenty třetích stran
3.1.4) Specifická praktika: Určit základní příčiny zranitelnosti

3.2) Specifický cíl: Řídit bezpečnostní rizika produktu
3.2.1) Specifická praktika: Zavést plán řízení bezpečnostních rizik produktu
3.2.2) Specifická praktika: Provedení posouzení bezpečnostních rizik produktu
3.2.3) Specifická praktika: Plán pro zmírňování vzniku rizik bezpečnosti produktu (Product Security) [3, s. 28-40]

3.3. Bezpečnostní procesní oblast: Security Requirements and Technical Solution (SRTS)

Třetí bezpečnostní procesní oblastí jsou Bezpečnostní požadavky a technické řešení (Security Requirements and Technical Solution).
Cílem této bezpečnostní procesní oblasti je stanovit bezpečnostní požadavky a bezpečný návrh a zajistit implementaci bezpečného produktu.[3, s. 4]

V rámci kategorie Inženýrství (Engineering) jsou ekvivalentem ze strany CMMI-DEV v1.3 procesní oblasti Requirements Development (RD) a Technical Solution (TS), které tato bezpečnostní procesní oblast rozšiřuje.

Souhrn specifických cílů a specifických praktik:

4.1) Specifický cíl: Vypracovat bezpečnostní požadavky zákazníků a bezpečnou architekturu a návrh
4.1.1) Specifická praktika: Vypracovat bezpečnostní požadavky zákazníků
4.1.2) Specifická praktika: Provedení výrobku podle bezpečné architektury a bezpečnostní zásady pro návrh
4.1.3) Specifická praktika: Vyberte odpovídající technologie, které využívají bezpečnostní kritéria
4.1.4) Specifická praktika: Stanovit normy pro bezpečnou konfiguraci produktu

4.2) Specifický cíl: Implementace bezpečného návrhu (Secure Design)
4.2.1) Specifická praktika: Použijte bezpečnostní normy pro implementaci
4.2.2) Specifická praktika: Zahrnout bezpečnost do dokumentace v rámci podpory produktu[3, s. 41-50]

4. Bezpečnostní procesní oblast: Security Verification and Validation (SVV)

Poslední bezpečnostní procesní oblastí je Bezpečnostní verifikace a validace (Security Verification and Validation).
Cílem této bezpečnostní procesní oblasti je zajistit, aby vybrané pracovní produkty splňovaly své specifikované bezpečnostní požadavky a prokázaly tak, že produkty nebo jejich součásti naplňují očekávání zabezpečení pro zamýšlené provozní prostředí, do kterého budou umístěny.[3, s. 4]

V rámci kategorie Inženýrství (Engineering) jsou ekvivalentem ze strany CMMI-DEV v1.3 procesní oblasti Verification (VER) a Validation (VAL), které tato bezpečnostní procesní oblast rozšiřuje.

Aktivity Bezpečnostní verifikace a validace se provádějí za účelem zjištění bezpečnostních nedostatků produktu nebo jeho součástí a otestování odolnosti proti zákeřným útokům. Kromě ověření, že pracovní produkty splňují stanovené bezpečnostní požadavky, je také nezbytné použít perspektivu útočníka jako zdroj pro validační procedury s cílem zajistit bezpečnost produktu nebo jeho součástí pro zamýšlené provozní prostředí, do kterého budou umístěny.

Výsledky bezpečnostní verifikace jsou zaznamenány a použity se jako základ pro určení nápravných opatření. Výsledky bezpečnostní validace jsou analyzovány a jsou přijata příslušná opatření (např. na přehodnocení v souladu s bezpečnostním plánem řízení rizik produktu a vymezení plánů pro snížení rizik). Implementace nápravných opatření je předpokladem pro ušetření značných nákladů na opravy spojené s potížemi nebo „patch“ managementem. Bezpečnostní zranitelnosti v produktivním prostředí (tj. výrobek v provozu) můžou také vést ke značné finanční ztrátě nebo k problémům s odpovědností v případě bezpečnostních incidentů. [3, s. 51]

Bezpečnostní verifikace a validace nenahrazuje, ale rozšiřuje "standardní" Verifikaci a Validaci.

Souhrn specifických cílů a specifických praktik:

1) Specifický cíl: Provést bezpečnostní verifikaci

1.1) Specifická praktika: Připravte se na bezpečnostní verifikaci
Příklady pracovních produktů:
1. Procedury bezpečnostní verifikace
2. Kritéria bezpečnostní verifikace
3. Seznam technik a nástrojů bezpečnostního testování
4. Bezpečnost prostředí verifikace
5. Procedury pro nezávislé hodnocení softwarového kódu odborníky využívající statickou a dynamickou analýzu

Příklady typů pracovních produktů určených pro bezpečnostní verifikaci:
Specifikace architektury a návrhu
Softwarové komponenty
Dokumentace podpory bezpečnosti produktu (Security product support documentation)
Dokumentace k instalaci a nasazení

Příklady zdrojů pro kritéria bezpečnostní verifikace:
Bezpečnostní požadavky produktu a součástí produktu
Bezpečnostní politiky organizace
Standardy bezpečné architektury a návrhu
Standardy bezpečné konfigurace
Standardy bezpečné implementace
Parametry pro kompromis mezi bezpečností a náklady na testování
Návrhy a dohody

1.1.1) Subpraktika: Identifikovat pracovní produkty pro bezpečnostní verifikaci.
1.1.2) Subpraktika: Identifikovat a definovat metody verifikace použité pro každý vybraný produkt práce.
1.1.3) Subpraktika: Definovat procedury a kritéria pro bezpečnostní verifikaci.
1.1.4) Subpraktika: Stanovit a udržovat prostředí pro bezpečnostní verifikaci.

1.2) Specifická praktika: Proveďte bezpečnostní verifikaci
Příklady pracovních produktů:
1. Výsledky verifikace
2. Reporty verifikace
3. Report o analýze
4. Zprávy o vadách
5. Požadavky na změnu
6. Plán snížení rizik

1.2.1) Subpraktika: Proveďte ověření zabezpečení vybraných pracovních produktů vůči jejich bezpečnostním požadavkům.
1.2.2) Subpraktika: Zaznamenejte výsledky bezpečnostní verifikace.
1.2.3) Subpraktika: Analyzovat výsledky činností bezpečnostní verifikace a způsobených bezpečnostních rizik.
1.2.4) Subpraktika: Zahájit nápravná opatření.

2) Specifický cíl: Provést bezpečnostní validaci

2.1) Specifická praktika: Připravte se na bezpečnostní validaci

Příklady pracovních produktů:

1. Procedury bezpečnostní validace
2. Kritéria bezpečnostní validace
3. Seznam technik a nástrojů bezpečnostního testování
4. Bezpečnost prostředí validace

Příklady typů produktů nebo součástí produktu určených pro bezpečnostní validaci:

Architektura a návrh
Komunikační modul
Webová aplikace
Databáze
Šifrovací mechanismy
Autentizační a autorizační mechanismy
Session Handling
Administrativní rozhraní
Dokumentace podpory bezpečnosti produktu (Security product support documentation)

Příklady zdrojů pro kritéria bezpečnostní validace:

Bezpečnostní požadavky produktu a součástí produktu
Akceptační kritéria zákazníků
Posouzení rizik bezpečnosti produktu
Databáze zranitelností a hrozeb (např. výčtový seznam častých slabých stránek)
Standardy pro bezpečné kódování a podnikovou bezpečnost technických implementačních pokynů

Příklady typů testovacích případů pro bezpečnostní validaci:

Zkontrolujte, zda bezpečnostní dokumentace může být implementována.
Zkontrolujte, zda autentizační mechanismy lze obejít pomocí útoku hrubou silou.
Zkontrolujte, zda uživatelé (oprávnění i neoprávnění) mohou provádět funkce, které jim nejsou určeny.
Zkontrolujte, zda jsou útoky denial-of-service (zabránění přístupu ke službám) jsou úspěšné.
Zkontrolujte, zda může být injekce kódu (code injection) úspěšně provedena (např. Java Script ve webových aplikacích).
Zkontrolujte, zda lze manipulovat s příkazy SQL (SQL injection)
Zkontrolujte aktuální úrovně záplat komponent třetích stran.
Zkontrolujte, zda výrobek odolá škodlivému útoku sofistikovaného útočníka.

Příklady typů technik bezpečnostní validace:

Posouzení architektonických rizik
Hrozby a hodnocení rizik
Modelování hrozeb
Statické a dynamické analýzy bezpečnostního kódu
Automatické skenování zranitelnosti
Penetrační testování
Přátelské hackování (Friendly hacking)
Fuzzy testování
Re-play testování

Příklady typů nástrojů pro testování bezpečnosti:
Datové nebo síťové fuzzery (Data or network fuzzers)
BlackBox skenery
Skenery portů
Skenery zranitelnosti
Statické analyzátory softwarového kódu
Nástroje testování bezpečnosti dynamických aplikací
Síťové skenery
Analyzátory protokolů

2.1.1) Subpraktika: Identifikovat produkty nebo součásti produktů pro bezpečnostní validaci.
2.1.2) Subpraktika: Definovat procedury a kritéria pro bezpečnostní validaci.
2.1.3) Subpraktika: Identifikovat techniky bezpečnostní validace.
2.1.4) Subpraktika: Identifikovat a získat nástroje a zařízení bezpečnostní validace.
2.1.5) Subpraktika: Připravit prostředí pro bezpečnostní validaci.

2.2) Specifická praktika: Proveďte bezpečnostní validaci
Příklady pracovních produktů:
1. Report o posouzení bezpečnosti
2. Report bezpečnostní validace
3. Tovární akceptační test bezpečnosti
4. Problémy bezpečnostní validace
5. Bezpečnostní zranitelnosti
6. Bezpečnostní hrozby

2.2.1) Subpraktika: Proveďte bezpečnostní validaci produktů a součástí produktů.
2.2.2) Subpraktika: Zaznamenejte výsledky bezpečnostní validace.
2.2.3) Subpraktika: Analyzovat výsledky činností bezpečnostní validace a způsobených bezpečnostních rizik.
2.2.4) Subpraktika: Zahájit nápravná opatření. [3, s. 51-58]

4.1. Procesní oblast Verifikace (CMMI-DEV v1.3)

Souhrn specifických cílů a specifických praktik:

1) Specifický cíl: Připravte se na verifikaci

1.1) Specifická praktika: Vyberte pracovní produkty pro verifikaci

Příklady metod verifikace:
Evaluace architektury softwaru a vyhodnocení realizace shody
Testování pokrytí cest (Path coverage testing)
Testování zátěžové, hraniční zátěže a výkonnostní testování (Load, stress, and performance testing)
Testování na základě rozhodovací tabulky (Decision table based testing)
Testování na základě funkční dekompozice
Znovupoužití testovacího scénáře (Test case reuse)
Akceptační testování
Kontinuální integrace (tj. Agilní přístup, který brzy identifikuje integrační problémy)

Příklady pracovních produktů:
1. Seznamy pracovních produktů vybraných pro verifikaci
2. Metody verifikace pro každý vybraný produkt práce

1.1.1) Subpraktika: Identifikovat pracovní produkty pro verifikaci.
1.1.2) Subpraktika: Identifikovat požadavky, které musí být splněny každým vybraným pracovním produktem.
1.1.3) Subpraktika: Identifikovat metody verifikace, které jsou k dispozici pro použití.
1.1.4) Subpraktika: Definovat metody verifikace k použití pro každý vybraný produkt práce.
1.1.5) Subpraktika: Předložit k integraci s plánem projektu identifikaci pracovních produktů k verifikaci, požadavky, které mají být splněny, a metody, které mají být použity.

1.2) Specifická praktika: Stanovit prostředí pro verifikaci
Příklady pracovních produktů:
1. Prostředí verifikace

1.2.1) Subpraktika: Identifikovat požadavky na prostředí pro verifikaci.
1.2.2) Subpraktika: Identifikovat zdroje verifikace, které jsou k dispozici pro opakované použití nebo modifikaci.
1.2.3) Subpraktika: Identifikovat nástroje a zařízení verifikace.
1.2.4) Subpraktika: Získat verifikaci podporující zařízení a prostředí (např. testovací zařízení, software).

1.3) Specifická praktika: Zavést verifikační procedury a kritéria

Příklady zdrojů pro kritéria verifikace:
Požadavky produktu a součástí produktu
Standardy
Politiky organizace
Typ testu
Parametry testu
Parametry pro kompromis mezi kvalitou a náklady na testování
Typ pracovních produktů
Dodavatelé
Návrhy a dohody
Zákazníci hodnotí pracovní produkty ve spolupráci s vývojáři

Příklady pracovních produktů:
1. Procedury verifikace
2. Kritéria verifikace

1.3.1) Subpraktika: Generovat soubor komplexních, integrovaných procedur verifikace pro pracovní produkty a komerční běžně dostupné („podpultové“) produkty, jak je potřeba.
1.3.2) Subpraktika: Rozvíjet a zdokonalovat kritéria verifikace podle potřeby.
1.3.3) Subpraktika: Identifikovat očekávané výsledky, tolerované odchylky a další kritéria pro splnění požadavků.
1.3.4) Subpraktika: Identifikovat zařízení a komponenty prostředí potřebné pro podporu verifikace.

2) Specifický cíl: Proveďte vzájemná hodnocení

2.1) Specifická praktika: Připravte se na vzájemná hodnocení

Příklady pracovních produktů:
1. Plán vzájemného hodnocení
2. Kontrolní seznam vzájemného hodnocení
3. Vstupní a výstupní kritéria pro pracovní produkty
4. Kritéria pro vyžadování dalšího vzájemného hodnocení
5. Výukový materiál vzájemného hodnocení
6. Vybrané pracovní produkty, které mají být hodnocené

Příklady typů vzájemného hodnocení:
Kontroly
Strukturované návody (Structured walkthroughs)
Aktivní hodnocení (Active reviews)
Vyhodnocení implementace shodné architektury

Příklady položek, jimiž se zabývají kontrolní seznamy (the checklists):
Pravidla konstrukce
Obecné zásady návrhu
Úplnost
Správnost
Udržovatelnost
Běžné typy vad

Příklady rolí:
Vedoucí (Leader)
Čtenář (Reader)
Zapisovač (Recorder)
Autor (Author)

2.1.1) Subpraktika: Určete typ vzájemného hodnocení, které má být provedeno.
2.1.2) Subpraktika: Definovat požadavky pro sběr dat v průběhu vzájemného hodnocení.
2.1.3) Subpraktika: Vytvořit a udržovat vstupní a výstupní kritéria pro vzájemné hodnocení.
2.1.4) Subpraktika: Vytvořit a udržovat kritéria pro vyžádání dalšího vzájemného hodnocení.
2.1.5) Subpraktika: Vytvořit a udržovat seznamy pro ujištění, že pracovní produkty jsou hodnoceny důsledně.
2.1.6) Subpraktika: Vypracovat podrobný plán vzájemného hodnocení, včetně termínů pro školení vzájemného hodnocení a pro případy, kdy budou k dispozici materiály pro vzájemná hodnocení.
2.1.7) Subpraktika: Ujistěte se, že pracovní produkty přednostně splňují vstupní kritéria vzájemného hodnocení před distribucí.
2.1.8) Subpraktika: Dodejte produkt práce (k vzájemnému hodnocení) a související informace účastníkům dostatečně včas pro adekvátní přípravu vzájemného hodnocení.
2.1.9) Subpraktika: Přiřaďte role pro vzájemné hodnocení podle potřeby.
2.1.10) Subpraktika: Připravte se přednostně na vzájemné hodnocení kontrolou produktu práce před vedením vzájemného hodnocení.

2.2) Specifická praktika: Proveďte vzájemná hodnocení
Příklady pracovních produktů:
1. Výsledky vzájemného hodnocení
2. Problémy vzájemného hodnocení
3. Data vzájemného hodnocení

2.2.1) Subpraktika: Aplikujte přidělené role vzájemného hodnocení.
2.2.2) Subpraktika: Identifikovat a zdokumentovat vady a jiné nedostatky pracovních produktů.
2.2.3) Subpraktika: Zaznamenat výsledky vzájemného hodnocení, včetně položek činností.
2.2.4) Subpraktika: Sbírat data vzájemného hodnocení.
2.2.5) Subpraktika: Identifikovat položky činností a komunikovat problémy s příslušnými vlastníky.
2.2.6) Subpraktika: Provést další vzájemné hodnocení v případě potřeby.
2.2.7) Subpraktika: Ujistěte se, že výstupní kritéria pro vzájemné hodnocení jsou splněna.

2.3) Specifická praktika: Analýza dat vzájemného hodnocení
Příklady pracovních produktů:
1. Data vzájemného hodnocení
2. Položky činností vzájemného hodnocení

Typické údaje jsou název produktu, velikost výrobku, složení týmu, typ vzájemného hodnocení, doba přípravy na jednoho recenzenta, délka hodnotící schůzky jednání (length of the review meeting), počet zjištěných závad, typ a původ závady atd.

Další příklady údajů vzájemného hodnocení, které mohou být analyzovány:
Fázová vada byla zneužita (Phase defect was injected)
Doba přípravy nebo rychlost ve srovnání s očekávanou dobou přípravy nebo rychlostí
Počet vad oproti očekávanému počtu vad
Typy zjištěných vad
Příčiny vad
Dopad vady
User stories a případové studie spojené s vadou
Koncoví uživatelé a zákazníci, kteří jsou spojeni s vadami

2.3.1) Subpraktika: Záznam údajů vztahujících se k přípravě, průběhu a výsledkům vzájemných hodnocení.
2.3.2) Subpraktika: Ukládání dat pro budoucí použití a analýzu.
2.3.3) Subpraktika: Ochrana dat pro ujištění, že data vzájemného hodnocení nemohou být nevhodně použita.
2.3.4) Subpraktika: Analyzovat data vzájemného hodnocení.

3) Specifický cíl: Verifikujte vybrané pracovní produkty

3.1) Specifická praktika: Proveďte verifikaci
Příklady pracovních produktů:
1. Výsledky verifikace
2. Reporty verifikace
3. Ukázky
4. Záznam výkonu procedur "as-run"

3.1.1) Subpraktika: Proveďte verifikaci vybraných pracovních produktů vzhledem k jejich požadavkům.
3.1.2) Subpraktika: Zaznamenejte výsledky verifikačních činností.
3.1.3) Subpraktika: Identifikace položky činností vyplývající z verifikace pracovních produktů.
3.1.4) Subpraktika: Zdokumentujte metodu verifikace "as-run" a odchylky od dostupných metod a procedur objevených v průběhu jejího vykonávání.

3.2) Specifická praktika: Analýza výsledků verifikace
Příklady pracovních produktů:
1. Report analýzy (např. statistické údaje o výkonu, kauzální analýza neshod, srovnání chování mezi reálným produktem a modely, trendy)
2. Reporty problémů
3. Změnové požadavky pro metody, kritéria a prostředí verifikace

3.2.1) Subpraktika: Porovnání skutečných výsledků s očekávanými výsledky.
3.2.2) Subpraktika: Na základě stanovených kritérií verifikace identifikovat produkty, které nesplňují požadavky nebo identifikovat problémy s metodami, procedurami, kritérii a prostředím verifikace.
3.2.3) Subpraktika: Analýza vadných dat.
3.2.4) Subpraktika: Zaznamenejte všechny výsledky analýz do reportu.
3.2.5) Subpraktika: Použijte výsledky verifikace k porovnání skutečných měření a výkonu s technickými výkonnostními parametry.
3.2.6) Subpraktika: Poskytnout informace o tom, jak lze nedostatky vyřešit (včetně metod verifikace, kritérií a prostředí verifikace) a zahájit nápravná opatření. [4, s. 401-411]

4.2. Procesní oblast Validace (CMMI-DEV v1.3)

Souhrn specifických cílů a specifických praktik:

1) Specifický cíl: Připravte se na validaci

1.1) Specifická praktika: Vyberte produkty pro validaci

Příklady produktů a součástí produktu, které mohou být validovány:
Požadavky a návrhy produktů a součástí produktu
Produkt a součásti produktu (např. systém, hardwarové jednotky, software, servisní dokumentace)
Uživatelská rozhraní
Uživatelské příručky
Školicí materiály
Procesní dokumentace
Přístupové protokoly
Formáty reportů výměny dat (Data interchange reporting formats)

Příklady metod validace:
Diskuse s koncovými uživateli v kontextu s formálním hodnocením
Demonstrace prototypu
Funkční demonstrace (např. systém, hardwarové jednotky, software, servisní dokumentace, uživatelská rozhraní)
Pilotní školicí materiály
Testy produktů a součástí produktu koncovými uživateli a dalšími relevantními zúčastněnými stranami (stakeholders)
Inkrementální dodávka fungujícího a potenciálně přijatelného produktu
Analýzy produktů a součástí produktu (např. simulace, modelování, uživatelské analýzy)

Příklady pracovních produktů:
1. Seznamy pracovních produktů vybraných pro validaci
2. Metody validace pro každý vybraný produkt práce
3. Požadavky na provádění validace každého produktu nebo jeho součásti
4. Omezení validace pro každý produkt nebo jeho součást

1.1.1) Subpraktika: Identifikujte klíčové principy, funkce a fáze pro validaci produktu nebo součásti produktu po celou dobu životního cyklu projektu.
1.1.2) Subpraktika: Určit, které kategorie potřeb koncového uživatele (operativní, údržba, školení nebo podpora) musí být validovány.
1.1.3) Subpraktika: Vyberte produkt a součásti produktu k validaci.
1.1.4) Subpraktika: Vyberte metody hodnocení pro validaci produktu nebo součástí produktu.
1.1.5) Subpraktika: Zhodnoťte výběr validace, omezení a metody s příslušnými vlastníky.

1.2) Specifická praktika: Stanovit prostředí pro validaci

Příklady typů prvků ve validačním prostředí:
Testovací nástroje propojené s produktem jsou validovány (např. rozsah, elektronické zařízení, sondy)
Dočasně integrovaný testovací software
Záznamové nástroje pro „dump" analýzy nebo další analýzy a jejich přehrávání
Simulované subsystémy a součásti (např., software, elektronika, mechanika)
Simulované propojené systémy (např. fiktivní válečná loď pro testování námořního radaru)
Skutečně propojené systémy (např. letadlo pro testování radaru se zařízeními sledujícími trajektorii)
Vybavení a zákazníkům dodávané produkty
Schopní lidé k provozování nebo užití všech předešlých prvků (Skilled people to operate or use all the preceding elements)
Vyhrazené počítačové nebo síťové testovací prostředí

Příklad pracovních produktů:
1. Prostředí validace

1.2.1) Subpraktika: Identifikovat požadavky pro prostředí validace.
1.2.2) Subpraktika: Identifikovat produkty dodávané zákazníkům.
1.2.3) Subpraktika: Identifikovat testovací zařízení a nástroje.
1.2.4) Subpraktika: Identifikovat zdroje validace, které jsou k dispozici pro opětovné použití a modifikaci.
1.2.5) Subpraktika: Naplánujte podrobně dostupnost zdrojů.

1.3) Specifická praktika: Zavést validační procedury a kritéria

Příklady zdrojů validačních kritérií:
Požadavky produktů a součástí produktů
Standardy
Akceptační kritéria zákazníků
Výkon v prostředí
Prahové hodnoty odchylek výkonu (Thresholds of performance deviation)

Příklady pracovních produktů:
1. Procedury validace
2. Kritéria validace
3. Testovací a hodnotící procedury pro údržbu, školení a podporu

1.3.1) Subpraktika: Zhodnoťte požadavky na produkt pro ujištění, že problémy ovlivňující validaci produktu nebo součástí produktu jsou identifikovány a vyřešeny.
1.3.2) Subpraktika: Zdokumentujte prostředí, operační scénář, procedury, vstupy, výstupy a kritéria pro validaci vybraného produktu nebo součásti produktu.
1.3.3) Subpraktika: Posoudit návrh z hlediska zralosti v souvislosti s prostředím validace a identifikace problémů validace.

2) Specifický cíl: Validace produktu nebo součástí produktu

2.1) Specifická praktika: Proveďte validaci

Příklady pracovních produktů:
1. Reporty validace
2. Výsledky validace
3. Validace referenční křížové matice
4. Záznam výkonu procedur "as-run"
5. Operační ukázky

2.2) Specifická praktika: Analýza výsledků validace

Příklady pracovních produktů:

1. Reporty o nedostatcích validace
2. Problémy validace
3. Změnové požadavky pro procedury

2.2.1) Subpraktika: Porovnání skutečných výsledků s očekávanými výsledky.
2.2.2) Subpraktika: Na základě stanovených kritérií validace identifikovat produkty, které nesplňují požadavky nebo identifikovat problémy s metodami, procedurami, kritérii a prostředím validace.
2.2.3) Subpraktika: Analyzovat data validace pro nedostatky.
2.2.4) Subpraktika: Zaznamenejte výsledky analýzy a identifikaci problémů.
2.2.5) Subpraktika: Použijte výsledky validace k porovnání skutečných měření a výkonu se zamýšleným použitím nebo provozními potřebami.
2.2.6) Subpraktika: Poskytnout informace o tom, jak lze nedostatky vyřešit (včetně metod validace, kritérií a prostředí validace) a zahájit nápravná opatření. [4, s. 393-400]

5. Závěr

Účelem bezpečnosti coby aspektu návrhu (Security by Design) s CMMI-DEV v1.3 je poskytnout strukturovaný rámec pro bezpečný vývoj produktů. Neklade si za cíl nahradit či upravit původní ustanovení v rámci CMMI-DEV v1.3.
Nutno podotknout, že doprovodný dokument k tomuto rozšíření má prakticky totožnou strukturu jako dokument týkající se CMMI-DEV v1.3, jelikož se na tvorbě obou těchto dokumentů podílela organizace CMMI Institute. Proto jsem se rozhodl v rámci analýzy vztahu mezi bezpečnostní procesní oblastí Security Verification and Validation a procesními oblastmi Verification a Validation znázornit jejich strukturu se všemi důležitými prvky (pracovní produkty, role, metody, zdroje, položky), které jsou nezbytné pro pochopení významu jednotlivých specifických subpraktik, praktik a posléze i cílů. Rozšíření v podobě bezpečnosti coby aspektu návrhu (Security by Design) zachoval stejné obecné cíle a praktiky, jako tomu je u ekvivalentních procesních oblastí v rámci CMMI-DEV v1.3.
Je patrné, že bezpečnostní procesní oblast Security Verification and Validation nijak nerozšiřuje druhý specifický cíl týkající se vzájemného hodnocení (Peer Reviews) v rámci procesní oblasti Verification. Vzájemné hodnocení (Peer Reviews) je definováno jako způsob kontroly, kdy si týmy vývojářů předloží navzájem své práce a zkontrolují. Dále je u rozšíření znát zjednodušení a zpřehlednění struktury specifických praktik a subpraktik včetně omezení počtu uváděných příkladů důležitých prvků (pracovní produkty, role, metody, zdroje, položky). To je způsobeno tím, že se jedná o rozšíření, které začíná tam, kde původní verze končí a přidává klíčovou hodnotu v podobě akcentu na doporučení užití libovolných bezpečnostních politik organizace, bezpečnostních standardů, bezpečnostních požadavků a nástrojů pro testování bezpečnosti. Myslím si, že patrně nejvýznamnější přínos rozšíření je zahrnutí práce (řízení, monitorování, zaznamenávání) s hrozbami, zranitelnostmi a riziky. Všechna tato rozšíření se vážou již na fázi návrhu produktu, aby byl okamžitě po dokončení vývoje bezpečný v prostředí, pro které je určen.

6. Seznam použité literatury a odkazovaných zdrojů

[1] BRUCKNER, Tomáš. *Tvorba informačních systémů: principy, metodiky, architektury*. 1. vyd. Praha: Grada, 2012, 357 s. Management v informační společnosti. ISBN 978-80-247-4153-6.

[2] BUCHALCEVOVÁ, Alena. *Metodiky budování informačních systémů*. Vyd. 1. Praha: Oeconomica, 2009, 205 s. Vysokoškolská učebnice (Oeconomica). ISBN 978-80-245-1540-3.

[3] CMMI INSTITUTE, Siemens AG, The Carnegie Mellon Software Engineering Institute. *Security by Design with CMMI for Development, Version 1.3: An Application Guide for Improving Processes for Secure Products*. Pittsburgh, 2013. Dostupné z: http://cmmiinstitute.com/wp-content/uploads/2013/05/Security-by-Design-with-CMMI-for-Development1.pdf

[4] CMMI INSTITUTE, The Carnegie Mellon Software Engineering Institute. *CMMI for Development, Version 1.3*. Pittsburgh, 2010. Dostupné z: http://www.sei.cmu.edu/reports/10tr033.pdf

7. Seznam použitých obrázků

8. Terminologický slovník

Terminologický slovník obsahuje abecedně seřazený přehled odborných termínů včetně českého překladu a vysvětlení významu.

CMMI-DEV v1.3
Capability Maturity Model Integration for Development, version 1.3 (Integrační model zralosti pro vývoj, verze 1.3)
Integrační model zralosti pro vývoj verze 1.3 (CMMI-DEV v1.3) je referenčním modelem procesů, který pokrývá celý životní cyklus softwarového produktu, přičemž definuje 22 procesních oblastí rozdělených do čtyř kategorií. Těmito čtyřmi kategoriemi jsou: Řízení procesu (Process Management), Řízení projektu (Project Management), Inženýrství (Engineering) a Podpora (Support).

Generic goal (Obecný cíl)
Obecné cíle jsou společné několika procesním oblastem na rozdíl od specifických cílů. K jejich naplnění slouží jim přidružené obecné praktiky.

Generic practice (Obecná praktika)
Obecné praktiky vedou ke splnění obecného cíle, kterému jsou přiřazeny, a jsou aplikovány na danou procesní oblast s cílem zlepšit procesy v této oblasti.

Process Area (Procesní oblast)
Procesní oblast je skupina navzájem spojených praktik, které pokud implementujeme kolektivně, naplní množinu cílů, jež jsou podstatné pro zlepšení dané oblasti.

Security by Design (Bezpečnost coby aspekt návrhu)
Jedná se o rozšíření vybraných procesních oblastí Integračního modelu zralosti pro vývoj verze 1.3 (CMMI-DEV v1.3) s akcentem na bezpečnost návrhu produktu.

Security Process Area (Bezpečnostní procesní oblast)
Bezpečnostní procesní oblast je skupina navzájem spojených praktik, které pokud implementujeme kolektivně, naplní množinu cílů, jež jsou podstatné pro zlepšení dané bezpečnostní oblasti.

Specific goal (Specifický cíl)
Každá procesní oblast má vždy definované specifické cíle, přičemž specifické cíle se týkají vždy pouze jedné procesní oblasti na rozdíl od obecných cílů. K jejich naplnění slouží jim přidružené specifické praktiky.

Specific practice (Specifická praktika)
Specifické praktiky vedou ke splnění specifického cíle, kterému jsou přiřazeny.

Validation (Validace)
Validace je ověření platnosti a jedná se o proces posouzení produktu nebo analytické metody, abychom se ujistili, že vyhovuje požadavkům, které jsou na produkt (metodu) kladené. Řeší tedy otázku, zda daný předmět (produkt, služba, metoda) je vhodný pro daný účel.

Verification (Verifikace)
Verifikace je ověření správnosti, pravosti a jedná se o proces posouzení produktu nebo analytické metody, abychom se ujistili, že splňuje požadavky, které jsou na produkt (metodu) kladené. Řeší tedy otázku, zda daný předmět (produkt, metoda) splňuje požadavky pro daný účel.