UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

MAGISTRSKO DELO

OBLIKOVANJE SISTEMA KAKOVOSTI VALIDACIJE RAČUNALNIŠKIH SISTEMOV V FARMACEVTSKI INDUSTRIJI

Ljubljana, avgust 2014 TOMAŽ SALLUBIER

IZJAVA O AVTORSTVU

Spodaj podpisani TOMAŽ SALLUBIER, študent Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtor magistrskega dela z naslovom OBLIKOVANJE SISTEMA KAKOVOSTI VALIDACIJE RAČUNALNIŠKIH SISTEMOV V FARMACEVTSKI INDUSTRIJI, pripravljenega v sodelovanju s svetovalcem red. prof. dr. BORUTOM RUSJANOM.

Izrecno izjavljam, da v skladu z določili Zakona o avtorskih in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo zaključne strokovne naloge/diplomskega dela/specialističnega dela/magistrskega dela/doktorske disertacije na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem
    - poskrbel(-a), da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v zaključni strokovni nalogi/diplomskem delu/specialističnem delu/magistrskem delu/doktorski disertaciji, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
    - pridobil(-a) vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisal(-a);
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predložene zaključne strokovne naloge/diplomskega dela/specialističnega dela/magistrskega dela/doktorske disertacije dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne _____ Podpis avtorja:_____

KAZALO

KAZALO TABEL

KAZALO SLIK

UVOD

V današnjem času se na vseh področjih vedno pogosteje srečujemo z vse strožjimi predpisi, kar še posebej velja za farmacevtsko industrijo, ki je pod nenehnim nadzorom regulatornih organov. Od farmacevtskih podjetij se pričakuje zagotavljanje sledljivosti na vseh nivojih, ki so povezani s proizvodnimi in podpornimi procesi v združbi, kot tudi postavljen sistem kakovosti na vseh nivojih združbe (MetricStream, 2014). Področje, s katerim se ukvarjam v svojem magistrskem delu, so računalniški sistemi v farmacevtski industriji, kjer je integriteta podatkov ključnega pomena (Ranbaxy Laboratories Limited, 2014, str. 1–20), saj dandanes skoraj ni proizvodnega procesa, ki ne bi bil nadziran in krmiljen s strani enega ali več računalniških sistemov. Da bi zagotovili integriteto podatkov, je potrebno računalniške sisteme validirati skladno z zahtevami regulatornih organov (European Commission 2013, 2013a; U.S. Food and Drug Administration, 2013a, 2013b). Ker je pojem validacije zelo širok in zajema praktično vse nivoje v združbi, se bom v svoji nalogi posvetil področju validacij računalniških sistemov. Vodilna regulatorna organa v svetu, ki postavljata minimalne pogoje in omejitve tako v splošnem kot tudi na področju računalniških sistemov v farmacevtski industriji, sta ameriška organizacija Food and Drug Administration (v nadaljevanju FDA) in evropske medicinska agencija (angl. *European Medicines Agency*, v nadaljevanju EMA). Mnoge od teh regulatornih zahtev pa predstavljajo tudi precejšnje izzive za združbo, ki v farmacevtski industriji deluje. Največja izziva, s katerima se sooča nekdo, ki vzpostavlja sistem kakovosti na področju računalniških sistemov, sta predvsem nepravilna interpretacija in poenostavljenje regulatornih zahtev, ki jih predpisujejo regulatorni organi, ponavadi pa celo oboje. Mnogokrat pride tudi do bistvenih vsebinskih napak ali neskladij z zahtevami regulatornih organov zaradi nerazumevanja pojmov računalnik, aplikacija, računalniški sistem in/ali zaradi nepoznavanja dejanskega delovanja računalniških sistemov. Zahteve regulatornih organov so v osnovi zelo splošne, za pravilno oblikovanje in postavitev pa sta ključnega pomena pravilno razumevanje in interpretacija regulatornih zahtev v kombinaciji s poznavanjem in delovanjem računalniških sistemov, za uspešno validacijo računalniškega sistema pa moramo dodatno razumeti še procese dela.

Namen magistrskega dela je prikazati vzpostavitev sistema kakovosti na področju računalniških sistemov v farmacevtski industriji. Sistem kakovosti se vzpostavlja na osnovi zahtev regulatornih organov, ki pa so napisani v splošni obliki in jih ne moremo neposredno prenesti v združbo, temveč je vsako zahtevo potrebno interpretirati, interpretacijo formalizirati v postopke ter poskrbeti za izvajanje aktivnosti v združbi glede na interpretacijo in uvedene postopke. V tem magistrskem delu je poudarek na eden od delov sistema kakovosti, in sicer na področju računalniških sistemov.

Ciljev tega magistrskega dela je več. Prvi cilj je prikazati, kaj predstavlja sistem kakovosti v splošni obliki, interpretirati, kaj pomeni validacija v splošnem pomenu, ter v kombinaciji sistema kakovosti in validacije v splošni obliki potegniti vzporednice s farmacevtsko industrijo in predstaviti del sistema kakovosti – področje računalniških sistemov. Drugi cilj

je predstaviti regulatorne zahteve na področju računalniških sistemov v farmacevtski industriji dveh največjih regulatornih organov, ameriškega in evropskega. Tretji cilj je tudi pregledati in preučiti strokovno literaturo ter izluščiti ključne informacije, ki nam bodo koristile pri oblikovanju modela in vzpostavitvi sistema kakovosti na področju računalniških sistemov v farmacevtski industriji. Del spoznanj magistrskega dela pa temelji tudi na avtorjevih lastnih izkušnjah.

Ker je eden od poudarkov tega magistrskega dela poleg oblikovanja modela in vzpostavitve sistema kakovosti tudi na validacijah računalniških sistemov v farmacevtski industriji, je v sami nalogi prikazan tudi krajši primer validacije računalniško podprtega proizvodnega sistema v farmacevtski industriji iz prakse, ki temelji na le nekaj uporabniških zahtevah in katerega namen je doseči temeljitejše razumevanje povezanosti regulatornih zahtev in same izvedbe v praksi na podlagi predhodno postavljenega sistema kakovosti, ki je v nalogi tudi ustrezno razložen.

Ločeval sem med tremi pojmi na področju računalniških sistemov v farmacevtski industriji. Prvi je oblikovanje modela kakovosti, kjer preidemo iz regulatornih zahtev v prve osnutke in okvire, kaj sploh moramo zagotavljati na področju računalniških sistemov v farmacevtski industriji. Iz teh osnutkov preidemo na drugi korak, to so splošni postopki, ki podrobneje interpretirajo regulatorne zahteve, posledično pa iz njih nastane sistem kakovosti na področju računalniških sistemov, ki je ključna obravnavana tematika tega magistrskega dela. Sledi validacija računalniških sistemov na podlagi vzpostavljenega sistema kakovosti na področju računalniških sistemov v farmacevtski industriji, s prikazom na krajšem primeru iz prakse.

Magistrsko delo kot celota vsebuje poglobljen teoretsko-analitični pregled strokovne literature na področju kakovosti, regulatornih zahtev v farmacevtski industriji in regulatornih zahtev v farmacevtski industriji na področju računalniških sistemov ter validacij računalniških sistemov v farmacevtski industriji. V delu so obravnavane tudi znanstvene razprave, raziskave in članki predvsem tujih strokovnjakov na področju obravnavane tematike. Pri izdelavi magistrskega dela sem prav tako uporabil znanja, ki sem jih pridobil s študijem informatike, organizacije in managementa ter ekonomije. Uporabil sem tudi praktična znanja s področja validacije računalniških sistemov, ki sem ga in ga še vedno pridobivam kot ekspert za kakovost na področju računalniških sistemov in IT aplikacij v farmacevtski industriji.

V prvem delu magistrske naloge bom s pomočjo literature predstavil validacijo računalniških sistemov in zahteve regulatornih organov ter povzel, kako so regulatorni organi prišli do sklepa, da je potrebno računalniške sisteme v farmacevtski industriji regulirati. Opisana je krovna delitev računalniških sistemov, njihove podobnosti ter ključne razlike, ki jih je potrebno pri validaciji upoštevati. S pomočjo literature sem interpretiral regulatorne zahteve ter izpostavil pričakovanja regulatornih organov, ob tem pa tudi

navedel možne in najpogostejše modele, ki jih je potrebno vkomponirati v sistem kakovosti in ki se lahko uporabijo pri validaciji računalniških sistemov.

V drugem delu sem oblikoval in gradil sistem kakovosti na področju računalniških sistemov v farmacevtski industriji skladno z interpretacijo regulatornih zahtev, ki sem jih interpretiral znotraj t. i. splošnih postopkov. Za osnovno izhodišče sem uporabil V-model pristopa k validaciji, ki je na področju validacij računalniških sistemov v farmacevtski industriji najbolj razširjen. Cilj omenjenega modela je izboljšati kakovost računalniškega sistema, minimizirati tveganja na projektu, uveljaviti življenjski cikel sistema in dokumentacije ter izboljšati komunikacijo med vsemi sodelujočimi na projektu.

V tretjem delu magistrskega dela se dotaknem operativne rabe računalniških sistemov, retrospektivnih in ponovnih validacij računalniških sistemov v farmacevtski industriji, do katere pride predvsem zaradi staranja sistema kot celote na eni strani ter zaostrovanja regulatornih zahtev v farmacevtski industriji na drugi strani. Kam in kako s podatki, ki jih kot elektronske zapise moramo hraniti, kam in kako obravnavati računalniški sistem po sami uporabi in kako računalniški sistem upokojiti, vsa ta vprašanja smo vzeli pod drobnogled in skušali nanje podati vsaj delne odgovore.

Magistrsko delo sem zaključil s povzetki in komentiranjem ključnih dejavnikov, ki predstavljajo največje izzive pri oblikovanju in vzpostavitvi sistema kakovosti ter posledično tudi pri validacijah računalniških sistemov v farmacevtski industriji.

1 DEFINICIJA RAČUNALNIŠKEGA SISTEMA

1.1 Računalniški sistem

Kot ugotavlja Riganati (2012), je računalniški sistem sistem z namenom. Ko govorimo o računalniku, je govora o strojni in programski opremi, torej računalniku in aplikacijah. Ko govorimo o računalniškem sistemu, pa govorimo o skupku funkcij in operacij, ki so integrirane v računalniški sistem, ki ga upravljajo ustrezno usposobljene osebe.

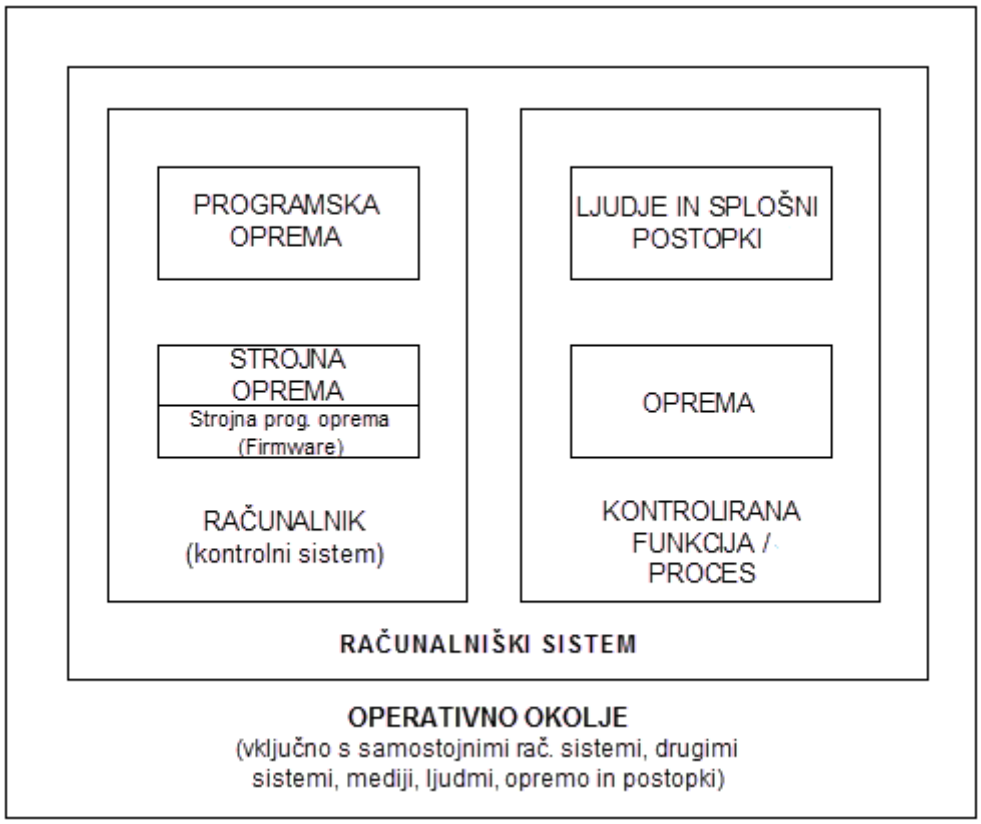
Riganati (2012) deli računalniški sistem na:

- računalniški sistem, ki kontrolira funkcije (procese in operacije),
- funkcije (procesi in operacije), ki so kontrolirane s strani računalniškega sistema.

Kot je razvidno s Slike 1, je računalniški sistem veliko več kot le računalnik. Računalniški sistem je sestavljen iz več elementov (McDowall, 2009):

- strojna oprema (npr. komponente računalnika, omrežne komponente ...),
- programska oprema (npr. operacijski sistemi, podatkovne baze, aplikacije ...),
- IT omrežje in infrastruktura (npr. domensko okolje, strežniki za varnostno kopiranje in arhiviranje ...),
- proizvodna in laboratorijska oprema (npr. tehtnice, tabletirke, oblagalne naprave ...).

Slika 1: Povezave med komponentami računalniškega sistema in operativnim okoljem



Vir: Prirejeno po PIC/S, Pharmaceutical Inspection Co-Operation Scheme Guidance – Good Practices For Computerised Systems In Regulated Gxp Environments, 2007, str. 8, International Society for Pharmaceutical Engineering - ISPE, GAMP 5: A Risk-based Approach to Compliant Gxp Computerized Systems, 2008, str. 21.

Računalniški sistem je kot celota torej skupek več med seboj povezanih elementov, računalnikov in pripadajoče programske opreme, ki izvaja uporabniške programe in upravlja s podatki, vključno z aritmetičnimi in logičnimi operacijami. Računalniški sistem je lahko samostojen ali sestavljen iz več povezanih računalniških sistemov.

V farmacevtski industriji in drugih reguliranih združbah se uporablja veliko število različnih tipov računalniških sistemov, ki variirajo od preprostih samostojnih sistemov do velikih, zelo kompleksnih sistemov (PIC/S 2007, str. 8), zato je računalniške sisteme zaradi lažjega obvladovanja smiselno razdeliti na:

- Računalniško podprte proizvodne sisteme

  To so sistemi, ki s svojim delovanjem (nadzorom, krmiljenjem) podpirajo proizvodnjo, npr. naprave, kot so granulirna naprava, tabletirka, oblagalna naprava, tehtnice, ki imajo lastno krmiljenje, in računalniški sistem za nadzor proizvodnih procesov in zbiranje podatkov (angl. *Supervisory Control and Data Aquisition*, v nadaljevanju SCADA). Med računalniško podprte proizvodne sisteme spadajo tudi sistemi za obvladovanje pogojev okolja (angl. *Heating, Ventilation, Air Conditioning*/Sistem za ogrevanje, prezračevanje in klimatizacijo, v nadaljevanju HVAC) in alarmiranja (angl. *Alarm Monitoring System*, v nadaljevanju AMS). V to kategorijo uvrščamo proizvodne informacijske sisteme in računalniške sisteme za avtomatizacijo procesov.

- Računalniško podprte laboratorijske sisteme

  Med računalniško podprte laboratorijske sisteme uvrščamo podatkovne sisteme, sisteme, ki so v omrežju in povezani z drugimi sistemi in/ali laboratorijskimi inštrumenti, računalniško krmiljene inštrumente in merilne naprave, ki so krmiljene z mikroprocesorjem ali krmilnikom in/ali procesirajo in hranijo elektronske zapise ali izvajajo manipulacije s podatki. Med računalniško podprte laboratorijske sisteme spadajo na primer naprave za podporo laboratorijskih analiz, recimo sistem za visoko ločljivo tekočinsko kromatografijo (angl. *High-Performance Liquid Chromatography*, v nadaljevanju HPLC), sistem za ultra ločljivo tekočinsko kromatografijo (angl. *Ultra-Performance Liquid Chromatography*, v nadaljevanju UPLC), sistem za plinsko kromatografijo (angl. *Gas Chromatography*, v nadaljevanju GC) ipd.

Kot primer enostavnega računalniškega sistema lahko vzamemo proizvodno opremo, ki ima svojo strojno programsko opremo (angl. *firmware*), na podlagi katere sistem prikazuje podatke in omogoča obvladovanje stroja.

Kompleksnejši sistem pa predstavlja denimo programabilni logični krmilnik (angl. *Programmable Logic Controller*, v nadaljevanju PLC) s uporabniškim vmesnikom (angl. *Human Machine Interface*, v nadaljevanju HMI).

Med še kompleksnejše računalniške sisteme štejemo npr. SCADA sistem, ki ga je možno prilagoditi lastnim potrebam glede na proces in funkcionalnosti (prilagoditev okolja/aplikacije podjetja General Electric Intelligent Platforms, nameščena na SCADA sistem, ki ji pravimo Proficy iFix ali le iFix). Najkompleksnejši sistemi pa so sistemi, v celoti zgrajeni po meri oz. naročilu.

Vse računalniške sisteme dodatno delimo še na zaprte računalniške sisteme in odprte računalniške sisteme.

Kot navaja U.S. Food and Drug Administration (2013b), predstavljajo zaprti računalniški sistemi okolje, kjer so dostopi do sistema upravljani s strani osebe, ki je odgovorna za elektronske zapise na sistemu in odprti računalniški sistemi okolje, kjer dostopi do sistema niso upravljani s strani osebe, ki je odgovorna za elektronske zapise na sistemu.

Lahko torej rečemo, da so zaprti računalniški sistemi tisti sistemi, do katerih ni mogoče dostopati brez ustreznih varnostnih mehanizmov (npr. uporabniškega imena in gesla) in kjer je kontrola dostopa znotraj združbe, ki ima nad računalniškim sistemom skrbništvo, odprti računalniški sistemi pa so tisti, kjer za skrbništvo računalniškega sistema skrbi dobavitelj. Nadzor nad elektronskimi zapisi (podatki) na računalniškem sistemu pri odprtih sistemih zaupamo dobavitelju, pri zaprtih sistemih ima nadzor nad elektronskimi zapisi združba sama.

2 VALIDACIJA RAČUNALNIŠKIH SISTEMOV

2.1 Kaj je validacija in kdo jo predpisuje

Validacija je dokumentiran postopek preizkušanja in potrjevanja, da vsi procesi, materiali, oprema in sistemi v vseh fazah (razvoj, proizvodnja, kontrola, distribucija) dosegajo predpisane in želene rezultate (Velkovrh - Remec, 2007 in Silva, 2013, str. 6). Verifikacija je ocena ali izdelek, storitev ali sistem, skladen z regulatornimi zahtevami, zahtevami uporabnika in specifikacijami (Project Management Institute, 2013, str. 566).

Termina »verifikacija« in »validacija« sta ločena že v standardu ISO 8402:1994, po drugi strani pa v inženirskih znanstvenih člankih med tema dvema terminoma v večini primerov ne razlikujejo, temveč uporabljajo kar izraz verifikacija, validacija in testiranje (v nadaljevanju VV&T), (U.S. Food and Drug Administration, 2002, str. 6). Termina validacija in verifikacija hodita z roko v roki in kot navajata Rao in Sastri (2011, str. 1232), se pri verifikaciji vprašamo, ali vzpostavljamo sistem na pravi način, pri validaciji pa, ali gradimo pravi sistem.

Validacijo računalniških sistemov v farmacevtski industriji v evropskem prostoru predpisuje Evropska agencija za zdravila, za vse izvoznike v Združene države Amerike pa tudi ameriški regulatorni organ FDA.

Dejstvo je, da smo v t. i. papirnem svetu lahko verjeli tistemu, kar smo videli, v današnjem svetu, ko operiramo z elektronskimi zapisi, pa temu več ni tako. Možnosti za spreminjanje ali kopiranje vsebin elektronskih zapisov, ne da bi to bilo mogoče dokazati, je izjemno veliko. Že sama funkcija kopiranja namreč ne pušča nobenih vidnih sledi.

Kot navaja European Compliance Academy (2011e, str. 8), regulatorni organi želijo le zagotovilo, da tudi ob uporabi računalniških sistemov zagotavljamo integriteto podatkov skozi zanesljive sisteme, sisteme, ki odkrijejo in prikažejo napake ter sisteme, ki zagotavljajo integriteto podatkov.

Kar želi industrija, pa je ravnati v skladu z regulatornimi predpisi in hkrati ohraniti inovativnost, zanesljive sisteme in sprejemljive stroške.

2.2 Zgodovina validacije računalniških sistemov

Zgodovina validacije v farmacevtski industriji v splošnem seže v konec sedemdesetih let, ko so v Združenih državah Amerike v farmakopejo zapisali testiranje sterilnih produktov. Temu je botroval predvsem incident, povezan s talidomidom leta 1962, ter incident, povezan s sepso, v sedemdesetih letih prejšnjega stoletja, ko je bila ugotovljena nesterilnost infuzij, kar se je odrazilo v 410 primerih resnih obolenj in 54 smrtnih primerih. FDA je tako leta 1976 uvedla spremembe v dobri proizvodni praksi (angl. *Good Manufacturing Practices*, v nadaljevanju GMP) s poudarkom na postopkih sterilizacije in čiščenja. V tem času je bila tudi prvič uradno uporabljena terminologija validacija, protokol in kvalifikacija (Biometrix, 2008, str. 2–7).

Zgodovina validacije računalniških sistemov sega v osemdeseta leta, k temu pa so pripomogli predvsem incidenti na računalniških sistemih Apolla – NASA ter incident v krvni banki v Connecticutu v ZDA, ko je pri prenosu podatkov prišlo do napake.

Posledično je bila kri, ki je prišla na trg oz. v obtok, HIV pozitivna (European Compliance Academy, 2011a, str. 4).

Zametki potrebe po validaciji računalniških sistemov izvirajo iz sedemdesetih let prejšnjega stoletja, ko so regulatorni organi postopoma začeli postavljati regulatorne zahteve za medicinske pripomočke. Terminologija, ki je bila tedaj v rabi, je bila besedna zveza proizvodno-validacijski koncept, danes to imenujemo validacija procesa.

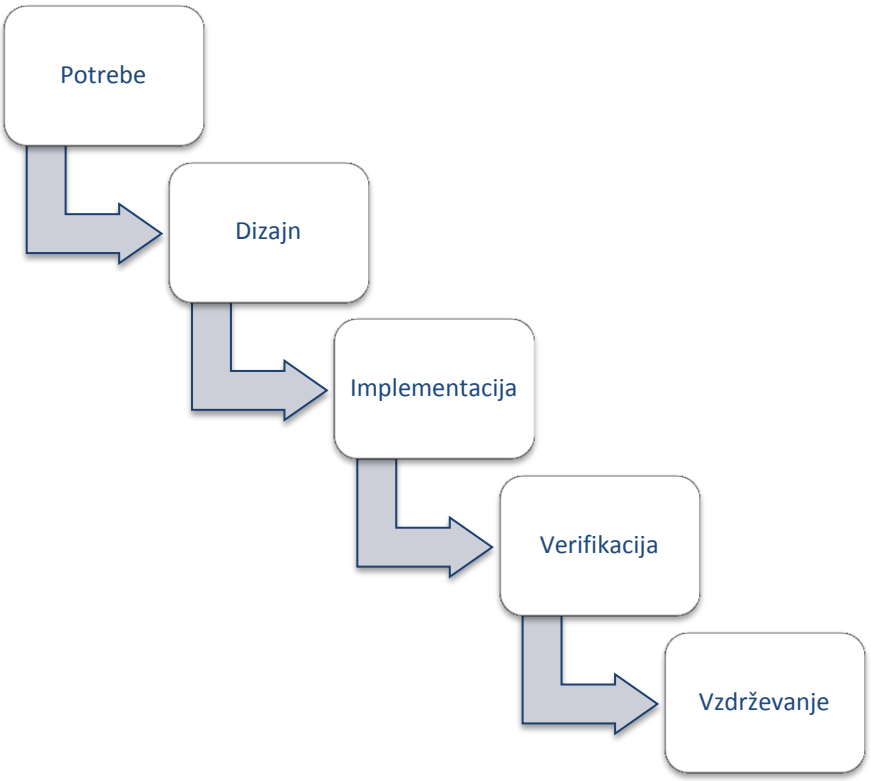
V poznih osemdesetih letih prejšnjega stoletja se v proizvodno-validacijskem konceptu pojavijo izrazi kvalifikacija inštalacije (angl. *Installation Qualification*, v nadaljevanju IQ), kvalifikacija obratovanja (angl. *Operational Qualification*, v nadaljevanju OQ) in kvalifikacija delovanja (angl. *Performance Qualification*, v nadaljevanju PQ) testiranja računalniških sistemov (Budihandojo, Coates, Huber, Matos, Schmitt, Stokes et al., 2007, str. 88).

2.3 Modeli validacije računalniških sistemov

V literaturi je moč najti več modelov oz. pristopov k validaciji računalniških sistemov (V-model, 4Q Lifecycle model, spiralni model, zaporedni oz. slapovni (angl. *waterfall*) model ipd.), vendar bomo tukaj podrobneje opisali le V-model validacije, ker je kot model validacije računalniških sistemov najbolj razširjen, poznan in tudi sprejemljivejši kot na primer 4Q Lifecycle model.

V-model se je v osnovi razvil iz waterfall modela, ki je prikazan na Sliki 2. Waterfall model že upošteva razvoj življenjskega cikla validacijske dokumentacije, vendar se je sčasoma iz njega razvil današnji V-model (Budihandojo, et al., 2007, str. 90).

Slika 2: Grafični prikaz zaporednega oz. slapovnega (waterfall) modela



Vir: Prirejeno po W. W. Royce, Managing the development of large software systems: concepts and techniques, 1970, str. 328–330.

Nobeden izmed naštetih modelov ne zajema faze upokojitve računalniškega sistema, 4Q model pa dodatno ni primeren za sisteme, ki so potrebni dodelave s strani npr. lokalnega integratorja (Huber, 2012).

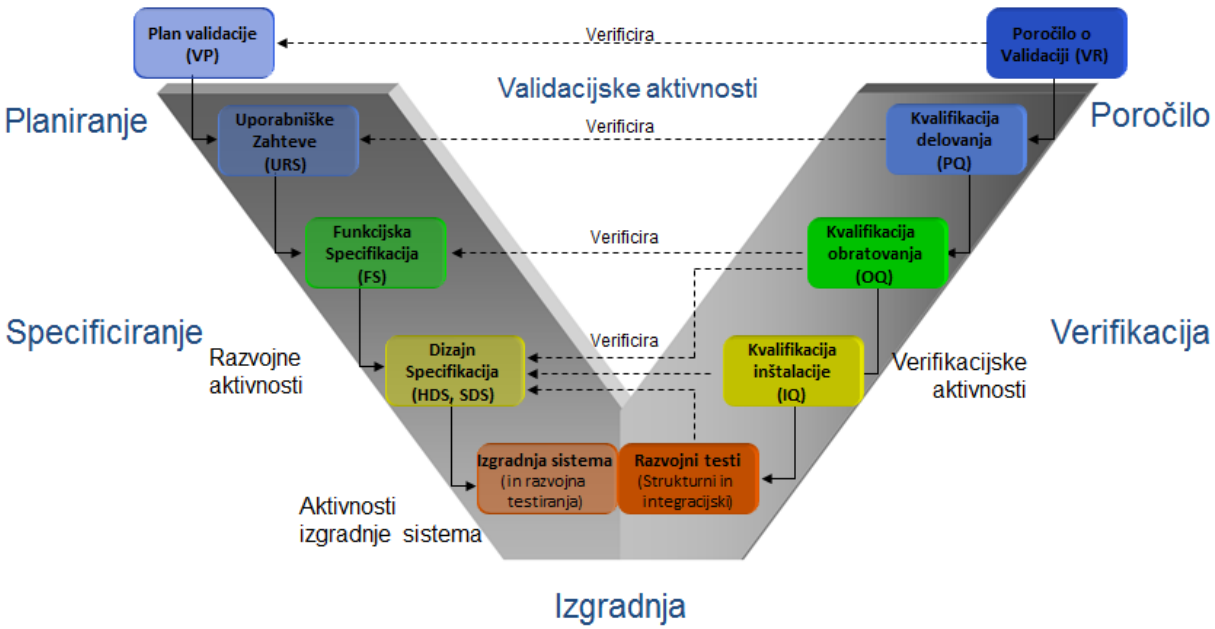
Primer takega sistema je denimo HMI/SCADA, ki deluje na osnovni platformi Proficy iFix, ki jo je možno prilagoditi lastnim potrebam oz. potrebam procesov v združbi. To spremembo na sistemu lahko izvede lokalni integrator, izmed modelov za validacijo tovrstnega posega pa je najbolj razširjen V-model validacije.

2.4 V-model

Prvi zametki V-modela, kot ga poznamo danes, so razvili v Nemčiji pod imenom V-Modell (prva različica je bila predstavljena avgusta 1992) in od leta 2005 predstavlja uradno metodologijo projektnega vodenja za IT sisteme nemške vlade pod imenom V-Modell XT (Industrieanlagen-Betriebsgesellschaft - IABG, 2006a). V-model je sicer podoben metodologiji projektnega vodenja v kontroliranih okoljih (angl. *Projects in Controlled Environments 2*, v nadaljevanju PRINCE2), vendar je V-model tesneje povezan z razvojem programske opreme.

V-model (Slika 3) predstavlja življenjski cikel razvoja in validacije računalniškega sistema in/ali IT aplikacije. Najlažje ga je razumeti, če je prikazan grafično in presekano na levi in desni del, pri čemer so predstavljene načrtovalne aktivnosti na levi in verifikacijske aktivnosti na desni strani. V-model povzema ključne korake in sekvence, ki morajo biti izvedene ob gradnji in validaciji sistema, ki ga razvijamo. Vendar pa ne pridejo vedno v poštev vsi koraki V-modela. Kot navaja več avtorjev, med drugim tudi avtorji priročnika GAMP5 (International Society for Pharmaceutical Engineering - ISPE, 2008, str. 3–63), je validacija in vzdrževanje validiranega stanja računalniškega sistema odvisna od rizikov in kompleksnosti računalniškega sistema.

Slika 3: Grafični prikaz V-modela



Vir: Prirejeno po International Society for Pharmaceutical Engineering - ISPE, GAMP 5: A Risk-based Approach to Compliant Gxp Computerized Systems, 2008, str. 27–37.

Kot navaja Industrieanlagen-Betriebsgesellschaft - IABG (2006b), je namen V-modela nuditi oporo pri planiranju in validaciji sistema ter:

- Minimizaciji rizikov projekta

  Povečata se obvladovanje in transparentnost projekta glede na pričakovane rezultate ter definirane vloge pri projektu, kar pomeni zgodnje odkrivanje odstopanj od planov, kar posledično vodi v manjša tveganja pri projektu.

- Izboljšanju kakovosti

  Model zagotavlja, da rezultati izvedenih aktivnosti dosegajo želeno kakovost, kar se lahko že sprotno preverja, predefinirane predloge pa zagotavljajo boljše razumevanje in lažje preverjanje pravilnosti.

- Zmanjšanju stroškov projekta

  Vire, potrebne za razvoj, proizvodnjo, uporabo in vzdrževanje, je na podlagi standardiziranega modela možno izračunati, predvideti in posledično tudi kontrolirati. To pomeni manjšo odvisnost od dobavitelja ter lažjo delitev aktivnosti in odgovornosti na projektu.

- Izboljšanju komunikacije med vsemi udeleženci projekta

  Vsi elementi modela so standardizirani in opisani tako, da vsi vpleteni v projekt razumejo svojo vlogo in vlogo ostalih sodelujočih pri projektu, rezultat česar je boljše medsebojno razumevanje.

Pri sami validaciji računalniških sistemov in IT aplikacij pa V-model uporabljamo predvsem za namen minimizacije rizikov (na kakovost) računalniškega sistema oz. IT aplikacije ter izboljšanje kakovosti.

Kot navaja International Society for Pharmaceutical Engineering - ISPE (2008, str. 27–37) v priročniku A Risk-Based Approach to Compliant GxP Computerized Systems, ključne točke V-modela (Slika 3) predstavljajo sledeče faze življenjskega cikla znotraj projekta (validacije računalniškega sistema):

- Planiranje

  Faza planiranja naj zajema krovno oceno rizika sistema, kompleksnost računalniškega sistema z vidika izgradnje in komponent sistema ter rezultate oz. oceno presoje dobavitelja (v primeru, da nam računalniški sistem razvija zunanji dobavitelj ali integrator). V tej fazi se kreirajo uporabniške zahteve (v nadaljevanju URS), ki morajo biti jasne do te mere, da je možno planirati potek validacijskih aktivnosti skozi V-model. Validacijo računalniškega sistema planiramo na podlagi dokumenta plan validacije (v nadaljevanju VP), ki ga potrdijo ključne osebe ter ekspert zagotavljanja kakovosti.

- Specificiranje in izgradnja

Dizajn in specifikacije sistema najpogosteje izdela dobavitelj in morajo temeljiti na podanih URS. Pomembno je, da naročnik oz. uporabnik ter vsi, ki so sodelovali pri pisanju URS za računalniški sistem, temeljito pregledajo specifikacije dizajna, ki so lahko razdeljene na funkcijsko specifikacijo (v nadaljevanju FS), programsko dizajn specifikacijo (v nadaljevanju SDS) in strojno dizajn specifikacijo (v nadaljevanju HDS), njeno pravilnost ter skladnost z URS. Le tako lahko pričakujemo, da bo sistem imel vse zahtevane funkcionalnosti in da bo deloval kot specificiran v dizajn dokumentih FS, HDS, SDS. Ko je dizajn dokumentacija s strani uporabnika oz. naročnika potrjena, dobavitelj začne z izgradnjo sistema skladno s specifikacijami.

- Verifikacija

  Z verifikacijo sistema potrdimo, da je sistem zgrajen skladno s specifikacijami in da so vsi postavljeni kriteriji doseženi. To dosežemo s pomočjo naslednjih vrst testiranja:

  - IQ, s katero testiramo dizajn dokumentacijo programske SDS in strojne opreme HDS,
  - OQ, s katero testiramo vso dizajn dokumentacijo, vključno s FS, saj večji del testiramo funkcionalnosti računalniškega sistema,
  - PQ, s katero (v večini primerov na produkcijskem okolju) testiramo URS oz. končni uporabnik izvaja serijo testov, ali računalniški sistem ustreza njegovim zahtevam (ki jih je podal v URS).

  Poznamo tudi več vrst/tipov testnih specifikacij – pozitivne teste, negativne teste, testiranje ponovljivosti, performančne teste, strukturne teste ipd.

- Poročilo

  Ko so glede na osnovni VP vse validacijske aktivnosti zaključene in če ni bilo odstopanj pri izvedbi testiranj oziroma so bile v sklopu testiranj vse pomanjkljivosti odpravljene, se to potrdi s poročilom o validaciji (angl. *Validation Report*, v nadaljevanju VR), s katerim sistem spustimo v produkcijsko/operativno rabo.

Kot že omenjeno, si je V-model smiselno predstavljati v dveh delih – levi in desni del, pri čemer levi del predstavlja načrtovanje sistema, desni del pa verifikacijo skozi testne procedure.

Dokumentacija, ki nastane pri validaciji računalniškega sistema, zajema več dokumentov, kot je prikazanih na Sliki 3 (grafični prikaz V-modela), kjer so zajeti le glavni (povezovalni) dokumenti, ki so nosilci V-modela.

3 REGULATIVA IN REGULATORNE ZAHTEVE

3.1 Evropska regulativa in regulatorne zahteve

Regulatornih organov ter posledično regulatornih zahtev je skoraj toliko, kolikor je držav na svetu, vendar so si med seboj v bistvu precej sorodne. Regulatorne zahteve so si med seboj podobne, največ pa je govora o ameriški FDA in evropski regulativi, obe skupaj pa

predstavljata temelje regulatornih zahtev po celem svetu. Zato v naslednjih dveh poglavjih opisujem le evropsko in ameriško regulativo.
Trenutna evropska regulativa dobre proizvodne prakse GMP temelji na osnovi treh odstavkov (direktiv), 8, 9 in 10, torej gre za tri temeljne odstavke (direktive) od devetnajstih odstavkov (direktiv) EU (European Commission, 2003, str. 24).

Navajam odstavke (direktive), poimenovane kot »Article 8«, »Article 9« in »Article 10«:

- Kvalifikacija in validacija opreme (Article 8)
    - (Proizvodna) oprema mora biti dizajnirana, konstruirana, prilagojena, vzdrževana in locirana tako, da ustreza uporabi, za katero je namenjena.
    - (Proizvodna) oprema mora biti dizajnirana in uporabljena na način, da se minimizira rizike napak, da je omogočeno normalno vzdrževanje in čiščenje opreme, z namenom, da se izognemo kontaminaciji, kros-kontaminaciji in v splošnem vidiku kakršnim koli posledicam, ki bi se lahko odrazile na padcu kakovosti izdelka.
    - (Proizvodna) oprema mora biti za vse proizvodne operacije, ki so kritične z vidika kakovosti izdelka, podvržena primerni kvalifikaciji in validaciji.

- Dokumentiranje (Article 9)
    - Proizvajalec mora imeti vzpostavljen dokumentni sistem, v katerem mora hraniti tipe dokumentov, kot so specifikacije, recepture, navodila, procesi ipd. Dokumenti morajo biti napisano jasno, brez napak in morajo odražati dejansko stanje (specifikacij, procesov, navodil ...). Dokumenti morajo biti hitro dostopni, enako pa velja za dokumente proizvedenih serij ter uvedbe sprememb zaradi zagotavljanja sledljivosti in možnosti raziskav. Dokumentacijo za farmacevtske izdelke je potrebno hraniti še vsaj eno leto dlje, kot je rok njihove uporabe, ali vsaj pet let po certifikaciji, skladno z direktivo EU 2001/83/EC, Article 51(3). Dokumentacijo kliničnih študij je po zaključku le-teh potrebno hraniti še vsaj pet let.
    - V primeru hrambe elektronskih zapisov, ki so uporabljeni namesto papirnih zapisov/poročil, mora proizvajalec zagotoviti, da so ti sistemi ustrezno validirani, da zagotavljajo integriteto podatkov. Elektronski zapisi morajo biti na voljo za prikaz regulatornim organom na njihovo zahtevo v berljivi obliki. Sistemi, ki hranijo zapise, da ohranijo integriteto podatkov (zapisi, zgodovina dogodkov ipd.), morajo biti redno varnostno kopirani.

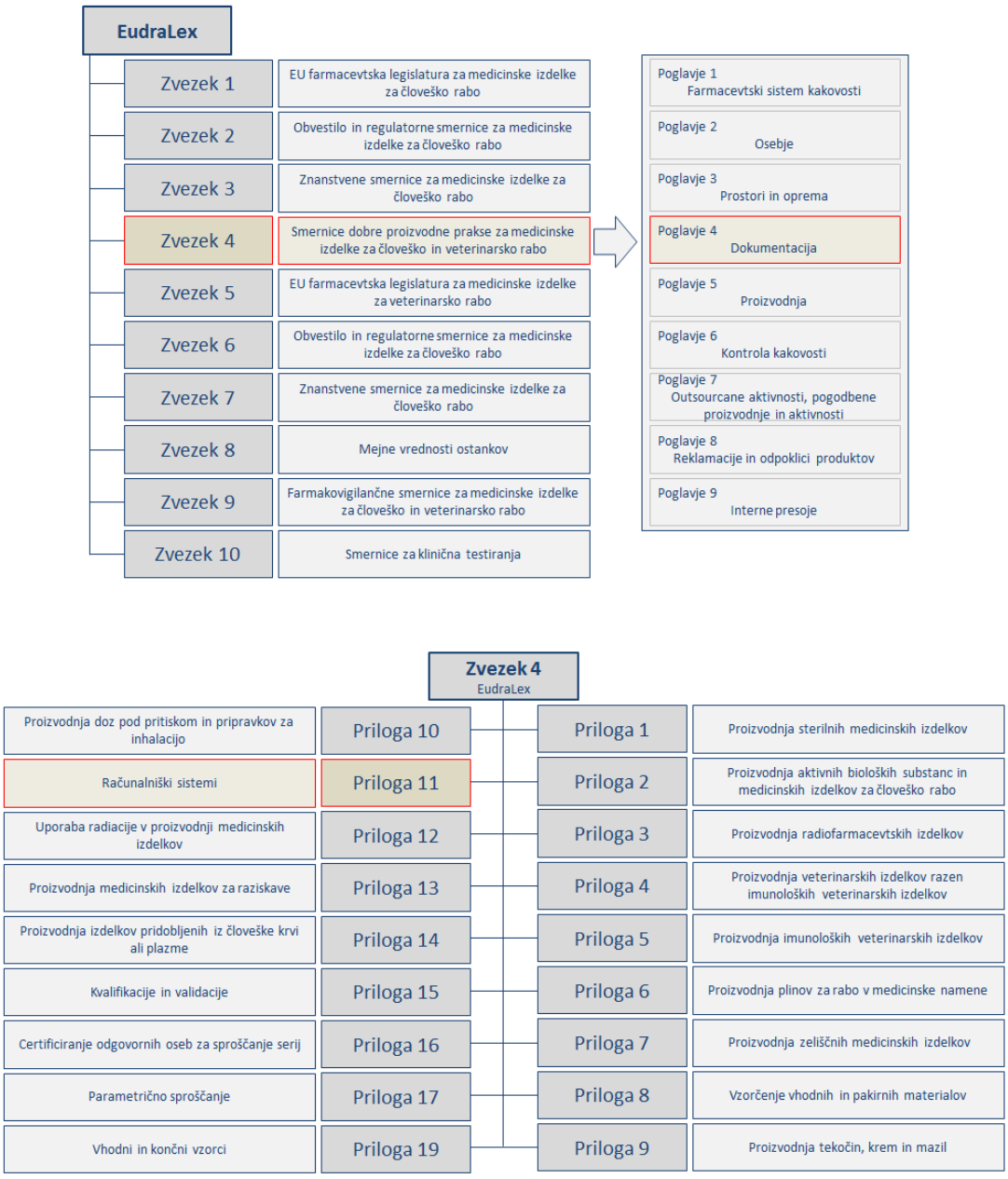
- Proizvodnja (Article 10)
    - Proizvodne operacije morajo biti izvedene sladno s potrjenimi splošnimi postopki in navodili ter skladno z dobro proizvodno prakso. Prav tako mora biti na voljo dovolj virov za medprocesno kontrolo. Odstopanja od dobre proizvodne prakse morajo biti ustrezno dokumentirana in temeljito raziskana.
    - Primerni tehnični in organizacijski predpisi morajo biti postavljeni tako, da ne pride do kros-kontaminacije ali zamenjave učinkovin in izdelkov (»mix-up«).
    - Vse večje spremembe morajo biti podvržene validaciji, kritične faze procesa proizvodnje pa morajo biti periodično revalidirane.
    - Vsi procesi morajo biti v celoti validirani v odvisnosti od faze izdelka (vsekakor pa vsi kritični procesi, kot je denimo sterilizacija). Celoten dizajn in razvoj proizvodnega procesa morata biti v celoti dokumentirana.

Ko govorimo o trenutni evropski regulativi, se opiramo na zbirko smernic regulatornih zahtev na področju zdravil in medicinskih pripomočkov v Evropski uniji, ki se imenuje EudraLex.

Smernice EudraLex sestavlja 10 zbirk, za računalniške sisteme pa je pomemben četrti zvezek (angl. *Volume 4*), ki predpisuje dobro proizvodno prakso GMP. V omenjenem zvezku je več poglavij in prilog (angl. *Annex*), vendar se bomo za validacijo računalniških sistemov omejili le na četrto poglavje (angl. *Chapter 4*), ki govori o dokumentaciji, ter na prilogo 11 (angl. *Annex 11*), ki govori o računalniških sistemih (European Commission, 2013a). Annex 11 je bil prvič predstavljen leta 1992, osvežitev na področju računalniških sistemov pa je doživel šele leta 2011 (Roemer & Lopez, 2011, str. 42). O kvalifikacijah in validacijah na splošno pa govori Annex 15.

Slika 4 prikazuje smernice evropske regulative v grafični obliki. Smernice, relevantne za validacijo računalniških sistemov, so na Sliki 4 obarvane z rdečo barvo.

Slika 4: Prikaz obravnavanih smernic evropske regulative



Vir: Prirejeno po European Commission, EudraLex – Volume 4 Good manufacturing practice (GMP) Guidelines, 2013a, European Commission, EU Legislation – Eudralex, 2013a.

Kot je navedeno v Zvezku 4 EudraLex (angl. *Volume 4*) v 4. poglavju (angl. *Chapter 4*) (European Commission, 2011a, str. 2), je obvladovanje dokumentacije ključni del zagotavljanja kakovosti in delovanja v skladu z dobro proizvodno prakso, vsi računalniški sistemi pa zapadejo tudi pod smernico Annex 11.

Annex 11 se navezuje na vse tipe računalniških sistemov, ki so klasificirani kot GxP, kar pomeni sisteme, vezane na dobre prakse, kjer črka »x« predstavlja spremenljivko. Tako lahko pomeni kratica GxP tudi GMP ali dobro laboratorijsko prakso (angl. *Good Laboratory Practices*, v nadaljevanju GLP) ipd. V ta sklop so zajete tudi IT aplikacije in IT infrastruktura, ki morajo biti podvržene kvalifikacijam. Uporaba računalniških sistemov namesto ročnih operacij ne sme negativno vplivati na kakovost izdelka, kontrolo procesa ali zagotavljanje kakovosti, prav tako pa ne sme biti povečanih tveganj, vezanih na celoten proces (European Commission, 2011b, str. 2).

Kot navaja European Compliance Academy (2011a, str. 9), so ključne točke 4. poglavja za upoštevanje pri validaciji računalniških sistemov elektronski zapisi (podatki na računalniškem sistemu), identifikacija izvornih (primarnih) podatkov ter dejansko potrebni ključni elektronski zapisi glede na sam proces dela ter določitev periode hrambe teh zapisov, dovoljena realno-časovna uporaba podatkov za sproščanje izdelkov – vendar so za to potrebni predpogoji, na primer zagotavljanje integritete podatkov ter zagotovljen dnevnik dogodkov opreme oz. sistema.

V Annexu 11 so zajeta sledeča poglavja, ključna za validacijo računalniških sistemov, ki jim dodajam kratek opis (glej tudi preglednico 1 – Primerjava Annexa 11 in 21 CFR Part 11):

a. Splošno

1. Obvladovanje rizikov/tveganj
   Analiza rizikov računalniškega sistema mora zajemati vplive na varnost pacienta, integriteto podatkov in kakovost izdelka.
2. Osebje
   Definirane morajo biti odgovornosti za vsak posamezni sistem, osebe morajo imeti ustrezne kvalifikacije in morajo biti ustrezno izobražene.
3. Dobavitelji in sistemski integratorji
   Imeti morajo pogodbe, v katerih so jasno določene odgovornosti, prav tako pa morajo s strani združbe, s katero bodo sodelovali, biti presojani.

b. Projektna faza

4. Validacija
   VP in VR morata pokrivati ključne korake validacije sistema, kot tudi vsa odstopanja, ki so nastala v obdobju validacije sistema. Dizajn sistema se mora ujemati z URS, ki se nato na podlagi ustreznih metod tudi potestira. Za faze validacije je potrebno imeti dokazila.

c. Operativna faza

5. Podatki
   Sistemi, ki so povezani z drugimi sistemi, morajo omogočati zanesljiv prenos podatkov med njimi.
6. Preverba točnosti (vnosa podatkov)
   Če se kritični podatki v računalniški sistem vpisujejo ročno s strani pooblaščene osebe (npr. operaterja na proizvodni liniji), je potreben sekundarni pregled vnosa s strani druge pooblaščene osebe.
7. Hranjenje podatkov in elektronskih zapisov
   Tako papirni kot tudi elektronski zapisi morajo biti ustrezno hranjeni, da ne pride do izgub, potrebno pa je skrbeti tudi za izdelavo varnostnih kopij in arhiviranja podatkov ter periodične preglede zapisov.
8. Tiskani dokumenti
   Sistemi, ki hranijo elektronske zapise, morajo biti zmožni le-te tiskati v berljivi obliki.
9. Zgodovina dogodkov
   Sistem mora omogočati zgodovino dogodkov za vse GMP relevantne spremembe.
10. Obvladovanje sprememb in konfiguracij

Vse spremembe na računalniških sistemih morajo biti ustrezno obvladovane.

11. Periodična evalvacija
    Računalniški sistemi morajo biti periodično pregledani in ocenjeni, ali so še v ustreznem (validiranem) stanju.
12. Varnost
    Računalniški sistemi morajo biti fizično in/ali logično zaščiteni.
13. Obvladovanje incidentov
    Vsi incidenti morajo biti ustrezno zapisani, vodeni in po potrebi raziskani.
14. Elektronski podpis
    Elektronski zapisi so lahko podpisani tudi z elektronskim podpisom, vendar le pod določenimi pogoji.
15. Sproščanje serij
    Serije lahko sprošča le za to odgovorna in certificirana oseba.
16. Neprekinjeno delovanje
    Računalniški sistemi, ki podpirajo kritične procese, morajo imeti postopek neprekinjenega delovanja (angl. *business continuity*), da lahko tudi med izpadom računalniškega sistema proces nemoteno deluje.
17. Arhiviranje
    Arhivirani podatki morajo biti preverjani glede dostopnosti, branja ter integritete kot celote.

Kot navaja European Compliance Academy (2011a, str. 11), so ključne točke iz Annexa 11 za upoštevanje pri validaciji računalniških sistemov:

- opisani principi veljajo za celoten GxP in ne samo za GMP,
- na vseh področjih je potreben pristop na osnovi ocene analize rizikov,
- elektronski podpisi so sprejemljivi,
- poudarek je na preverjanju dizajna sistema ob validaciji,
- zajeti so tudi zunanji dobavitelji GxP relevantnih IT sistemov,
- mejnik med fazo validacije in operativno fazo IT sistemov mora biti jasen.

3.2 Ameriška regulativa in regulatorne zahteve

Ameriški regulatorni organ je FDA, regulative pa najdemo v sekciji Code of Federal Regulations (v nadaljevanju CFR). Za validacijo računalniških sistemov sta pomembni 21 CFR Part 211 in 21 CFR Part 11.

Število 21 predstavlja sekcijo prehrane in zdravil, Part 211 pa predstavlja trenutno dobro proizvodno prakso (v nadaljevanju cGMP), medtem ko Part 11 predstavlja elektronske zapise in elektronske podpise (U.S. Food and Drug Administration, 2013a, 2013b).

21 CFR Part 211 je, podobno kot evropska regulativa, sestavljena iz 11 podpoglavij (»subpart«), kot prikazuje Slika 5 (relevantna poglavja so obarvana rdeče).

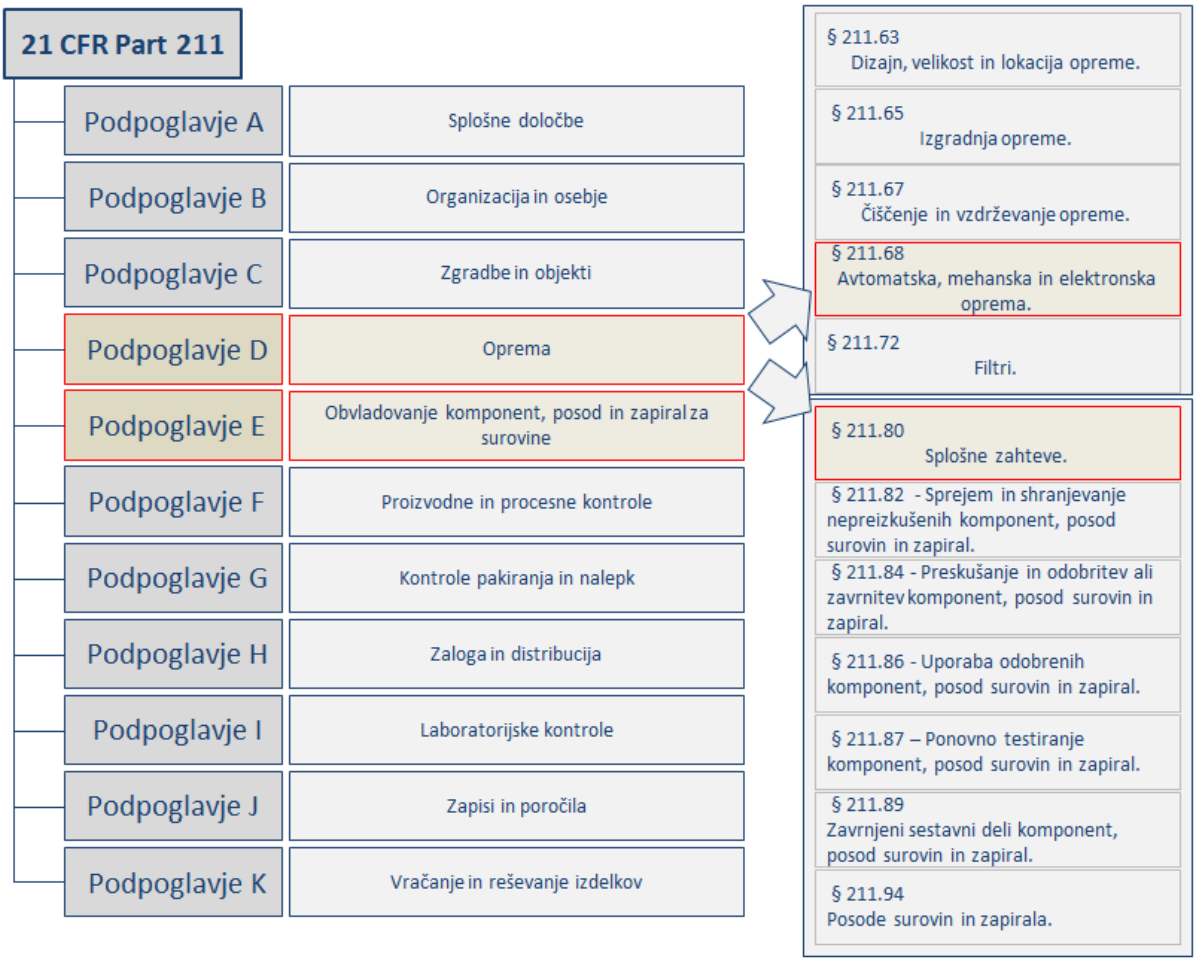
Kot navaja European Compliance Academy (2011a, str. 18), sta za upoštevanje pri validaciji računalniških sistemov iz FDA 21 Part 211 ključni sekciji:

- 211.68, podpoglavje D – Oprema; predpisuje regulatorne zahteve avtomatske, mehanske in elektronske opreme.

- Računalniški sistemi morajo biti rutinsko pregledani, da se zagotovi njihovo ustrezno delovanje.
- (Proizvodna) oprema mora biti rutinsko pregledana in kalibrirana.
- Ključne aktivnosti lahko izvajajo le pooblaščene osebe.
- Zapisi in konfiguracija, ki omogočajo nemoteno delovanje sistema, morajo biti pregledani in varnostno kopirani.

- 211.80, podpoglavje E – Obvladovanje komponent in posod, ki se uporabljajo v proizvodnji farmacevtskih izdelkov; predpisuje splošne zahteve obvladovanja komponent.

Slika 5: Prikaz obravnavanih poglavij ameriške regulative 21 CFR Part 211



Vir: Prirejeno po U.S. Food and Drug Administration, CFR – Code of Federal Regulations Title 21, Volume 4 – Part 211 Current Good Manufacturing Practice for Finished Pharmaceuticals, 2013a.

Ključnega pomena pri validaciji računalniških sistemov z vidika ameriške regulative je FDA 21 Part 11, kot prikazuje Slika 5 (relevantna celota obarvana rdeče), ki govori o elektronskih zapisih in podpisih, kar zajema (U.S. Food and Drug Administration, 2013b):

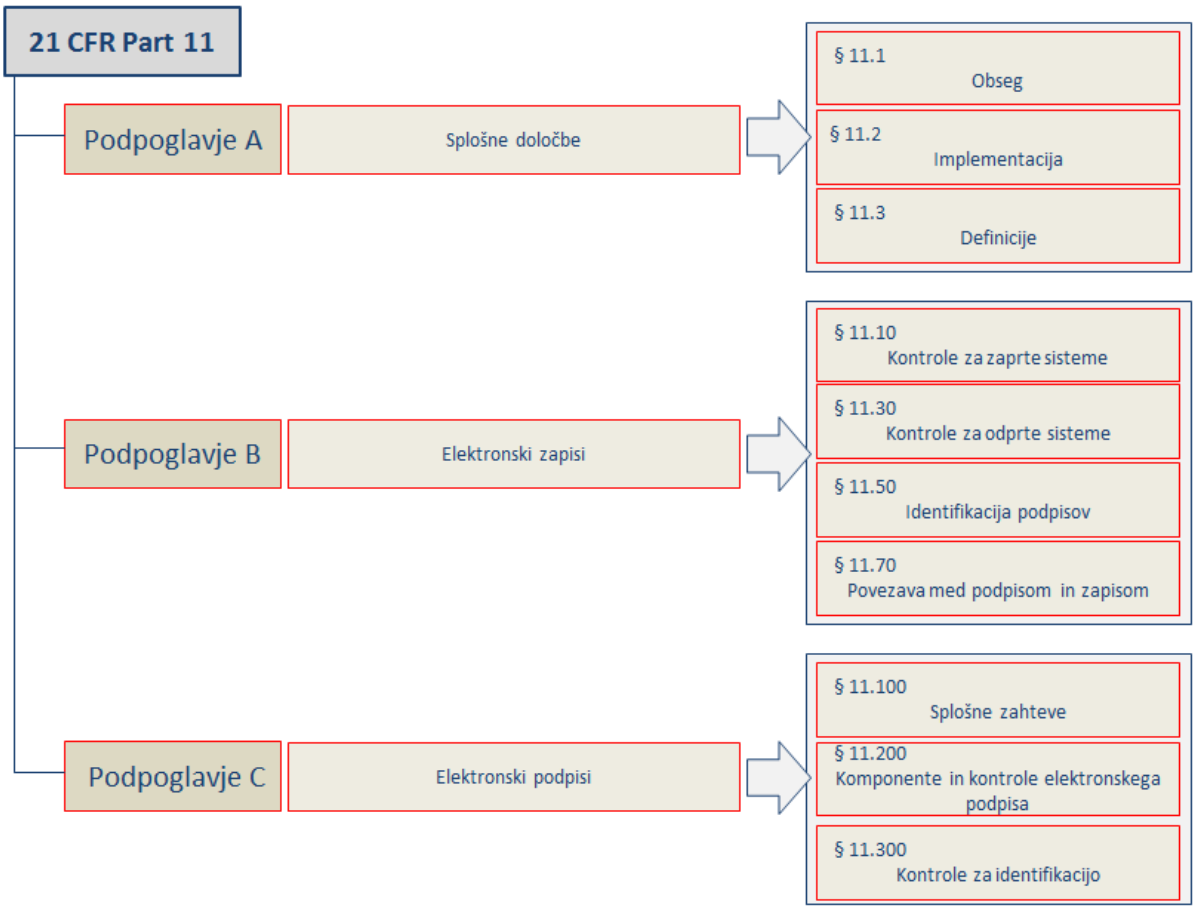
- kontrole sistemov (zaprti, odprti tip računalniškega sistema) – validacija sistema, zaščita elektronskih zapisov, zaščita pred nepooblaščenim dostopom, obvladovanje sprememb sistema ipd.,
- kontrolo elektronskih podpisov – identifikacija podpisnika, časovni žig, odgovornost (npr. avtor, pregledal, odobril),
- povezave med elektronskim podpisom in elektronskim zapisom,

- identifikacijo uporabnikov – biometrična identifikacija, uporabniško ime in geslo, administracija uporabnikov ipd.

Pomembno se je zavedati, da pod regulativo 21 CFR Part11 zapadejo tudi računalniški sistemi, ki hranijo elektronske zapise in so bili v uporabi, še preden je 21 CFR Part11 stopil v veljavo, vendar le, če so bili po uveljavitvi 21 CFR Part 11 podvrženi spremembi (U.S. Food and Drug Administration, 2003, str. 7), kar lahko predstavlja precejšen izziv v smislu, da starejše sisteme, ki jih zaradi različnih razlogov nismo obravnavali kot 21 CFR Part 11 relevantne (pa bi jih morali), spravimo na nivo, ki ga zahteva regulativa. Veliko je primerov, ko starejši računalniški sistemi enostavno niso skladni z vsemi točkami 21 CFR Part11, zato je v takih primerih potrebno uvesti organizacijske predpise, s katerimi zagotavljamo skladnost sistema z zahtevami 21 CFR Part11.

Slika 6 prikazuje relevantna poglavja iz 21 CFR Part 11 za validacijo računalniških sistemov. V poštev pridejo rdeče obarvana poglavja, v tem primeru je to celota.

Slika 6: Prikaz obravnavanih poglavij ameriške regulative 21 CFR Part 11



Vir:Prirejeno po U.S. Food and Drug Administration, CFR – Code of Federal Regulations Title 21, Volume 4 – Part 11 Electronic Records; Electronic Signatures, 2013b.

3.3 Razlika med Annexom 11 in FDA 21 CFR Part 11

Kot navaja tudi Lopez (2012), imamo v osnovi na voljo dva temeljna vira regulatornih zahtev na področju validacije računalniških sistemov: ameriški FDA 21 CFR Part 11 in evropski Annex 11. S to trditvijo se v celoti strinjam, kajti po dosedanjih izkušnjah regulatorne zahteve organov držav, ki ne delujejo v sklopu evropske ali ameriške

regulative, povzemajo bistvo svojih zahtev iz že definiranih evropskih ali ameriških, lahko pa tudi kombinacijo obeh. Viri in avtorji s tega področja, med drugimi Lopez (2012), dodatno navajajo, da se zahteve 21 CFR Part 11 nanašajo predvsem na tehnične in proceduralne kontrole v primereh elektronskih zapisov (kreiranje, modificiranje, hramba, arhiviranje, prenos, obnova) in elektronske podpise. Annex 11 pa zajema celoten sklop, potreben za validacijo računalniških sistemov. Do enakega sklepa lahko pridemo tudi sami, če primerjamo zahteve regulativ 21 CFR Part11 in Annex 11. Toda da je validacija računalniškega sistema lahko izpeljana v celoti, moramo upoštevati širše področje, torej tudi 21 CFR Part 211 (za računalniške sisteme predvsem podpoglavji D (§211.68) in E (§211.80), kot prikazuje Slika 5.

Poudariti je treba, da so zahtevam 21 CFR Part 11 podvržena farmacevtska (in druga regulirana) podjetja, ki delujejo v Združenih državah Amerike, oz. vsa podjetja, ki želijo pridobiti dovoljenje za prodajo od FDA, ne glede na to, kje v svetu so locirana. Zahteve EMA Annex 11 so aplikabilne za območje Evropske unije, vendar morajo aneks upoštevati tudi vsa podjetja zunaj Evropske unije, ki želijo dovoljenje od EMA.

V preglednici 1 navajam primerjavo med Annexom 11 in 21 CFR Part 11, v preglednici 2 pa povezave med obema obravnavanima regulativama – Annexom 11 in 21 CFR Part 11.

Tabela 1: Primerjava med Annexom 11 in 21 CFR Part 11

Regulativa **Namen**	**Annex 11**	**21 CFR Part 11**
Kaj zajema?	GxP relevantne računalniške sisteme, vključno z validacijo aplikacij in kvalifikacijo IT infrastrukture.	Vse GxP relevantne elektronske zapise in podpise za vse s strani FDA regulirane aktivnosti.
Fokus	Pristop k validaciji računalniškega sistema temelji na podlagi ocene tveganja (angl. *»Risk based approach«*).	Uporaba elektronskih zapisov in podpisov v zaprtih in odprtih računalniških sistemih.
Cilj	Uporaba računalniških sistemov mora zagotavljati enako kakovost in najmanj enako stopnjo tveganja kot neračunalniški sistemi.	Elektronski zapisi in podpisi morajo biti zanesljivi in verodostojni v enaki meri kot papirni zapisi in ročni podpisi.

Vir: Prirejeno po EduQuest, Comparison of FDA's Part 11 and the EU's Annex 11, 2011, str. 1.

Tabela 2: Povezave med Annexom 11 in 21 CFR Part 11

Annex 11 Številka poglavja	**Annex 11 Naslov poglavja**	**Part 11 Naslov poglavja**	**Part 11 Številka poglavja**
/	Principi	Implementacija Validacija	**11.2(b)** **11.10(a)**
1	Obvladovanje tveganj	/	/
2	Osebje/zaposleni	Osebje/zaposleni	**11.10(i)**
3	Dobavitelji in integratorji	/	/
3.1	Sporazumi/pogodbe	/	/
3.2	Presoje dobaviteljev	/	/
3.3	Pregled dokumentacije za aplikacije, ki jih ni moč spreminjati	/	/
3.4	Dosegljivost poročila o presoji dobavitelja	/	/
4	Validacija	Validacija	**11.10(a)**
4.1	Življenjski cikel	/	/
4.2	Obvladovanje sprememb in odstopov	Obvladovanje dokumentov	**11.10(k)**
4.3	Seznam sistemov	/	/
4.4	Uporabniške zahteve	/	/
4.5	Sistem kakovosti	/	/
4.6	Proces validacije	/	/
4.7	Dokaz pravilnosti testnih scenarijev in metod	/	/
4.8	Validacija migracije podatkov	Veljavnost vhodnih podatkov	**11.10(h)**
5	Podatki	Preverba delovanja sistema Kontrole odprtih sistemov	**11.10(f)** **11.30**
6	Preverba točnosti vnosa	Preverba delovanja sistema	**11.10(f)**
7	Hranjenje podatkov	Zaščita podatkov	**11.10(c)**
7.1	Zaščiteni in dostopni	Omejeni dostopi do sistemov Zaščita zapisov Avtorizacije/dostopi	**11.10(d)** **11.10(e)** **11.10(g)**
7.2	Varnostno kopiranje	/	/
8	Izpisi	/	/
8.1	Jasni izpisi zapisov	Generiranje točnih in celovitih kopij	**11.10(b)**

se nadaljuje

nadaljevanje

Annex 11 Številka poglavja	**Annex 11 Naslov poglavja**	**Part 11 Naslov poglavja**	**Part 11 Številka poglavja**
8.2	Spremembe ob sproščanju serij	/	/
9	Zgodovina dogodkov	Zgodovina dogodkov Obvladovanje dokumentacije	**11.10(e)** **11.10(k)**
10	Obvladovanje sprememb in konfiguracij	Omejeni dostopi do sistemov Zaščita zapisov	**11.10(d)** **11.10(e)**
11	Periodične evalvacije	Periodični pregledi Obvladovanje dokumentacije	**11.300(b, e)** **11.10(k)**
12	Zaščita	Zaščita zapisov	**11.10(c)**
12.1	Fizična/logična zaščita	Omejeni dostopi do sistemov Avtorizacije/dostopi Biometrična preverba Edinstven ID Preprečitev neavtorizirane uporabe	**11.10(d)** **11.10(g)** **11.200(a, b)** **11.300(a)** **11.300(b)**
12.2	Zaščita glede na kritičnost sistema	/	/
12.3	Zapis sprememb – uporabniki	Preverba identifikacije	**11.300(b, c)**
12.4	Zgodovina dogodkov	Kontrole zaprtih sistemov	**11.10(e)**
13	Obvladovanje incidentov	/	/
14	Elektronski podpisi	Elektronski podpisi	**11.50**
14a	Enakovrednost ročnim podpisom	Obseg Definicije Certifikacija	**11.1(a)** **11.3(b)** **11.100(c)**
14b	Sledljivost na zapis	Sledljivost na zapis	**11.70**
14c	Datum in čas	Zgodovina dogodkov (sistemski datum in čas)	**11.10(e)**
15	Sproščanje serij	/	/
16	Neprekinjeno delovanje	/	/
17	Arhiviranje	Zaščita podatkov za obnovo	**11.10(c)**

Vir: European Commission, EudraLex – Volume 4 Good Manufacturing Practice Medicinal Products for Human and Veterinary Use, Annex 11: Computerized Systems, 2011b, str. 1–5, U.S. Food and Drug Administration, CFR – Code of Federal Regulations Title 21, Volume 4 – Part 11 Electronic Records; Electronic Signatures, 2013b, prirejeno po EduQuest, Comparison of FDA's Part 11 and the EU's Annex 11, 2011, str. 2–5.

3.4 Interpretacija regulatornih zahtev

Kot je razvidno iz prejšnjih poglavij, je regulativa po eni strani zelo splošna, po drugi pa precej jasno navaja, kaj od združbe zahteva. Kot navaja Velkovrh Remec (2007), zakonodaji FDA in EU zahtevata validacijo vseh kritičnih postopkov, procesov in sistemov

ter izobraženost vseh posameznikov v procesu. S strani regulatornih organov so podana tudi številna priporočila za izvajanje validacij posameznih sistemov. Poznamo več vrst validacij, ena od njih je validacija računalniških sistemov, ostale pa so, kot navaja Pharmacists Pharma Journal (2010), validacija čiščenj, validacija procesov in validacija analitskih metod.

V nadaljevanju magistrskega dela bo prikazan model in postavitev sistema kakovosti za validacijo računalniških sistemov v farmacevtski industriji glede na regulativo in regulatorne zahteve, zatem pa še potek validacije računalniškega sistema na praktičnem primeru.

Na področju validacije računalniških sistemov v farmacetvski industriji je skozi čas nastal stroki dobro poznan priročnik International Society for Pharmaceutical Engineering - ISPE GAMP5, ki regulatorne zahteve na področju validacije računalniških sistemov dobro interpretira in nudi pomoč pri postavitvi sistema kakovosti za validacijo računalniških sistemov.

Farmacevtske in ostale združbe, ki delujejo v regulirani panogi, pa imajo na področju validacij (validacije čiščenj prostorov/opreme, validacije računalniških sistemov, validacije procesov ...) zaposlene strokovnjake, ki so eksperti na področju delovanja (validacij), ki ga pokrivajo. To so eksperti za zagotavljanje kakovosti (angl. *Quality Assurance*, v nadaljevanju QA managerji) in strokovnjaki, ki poleg obvladovanja osnovnih principov validacij delujejo tudi na področju elektronskih zapisov in podpisov (angl. *eCompliance managerji*). Vlogi QA in eCompliance sta običajno združeni.

4 VZPOSTAVITEV SISTEMA KAKOVOSTI ZA VALIDACIJO RAČUNALNIŠIH SISTEMOV

4.1 Interni standardi in splošni postopki

Za oblikovanje modela in postavitev sistema kakovosti za validacijo računalniških sistemov je potrebno upoštevati regulatorne zahteve in jih v celoti implementirati v sistem kakovosti. Prav tako se pričakuje, da ima združba v osnovi enoto kakovosti ločeno od proizvodnje oz. mora biti funkcija enote kakovosti neodvisna funkcija, razen izjemoma (U.S. Food and Drug Administration, 2006, str. 6).

Večje farmacevtske združbe postavljajo sistem kakovosti na globalni ravni, ki ga morajo podrejene združbe implementirati. Obstaja več mehanizmov preverjanja, ali so združbe uspešno implementirale sistem kakovosti, predpisan s strani matične združbe, na primer letne ocene skladnosti, kjer organizacije znotraj združbe na podlagi predefiniranih vprašalnikov podajo samooceno z utemeljitvijo in medorganizacijske presoje, kjer združba, ki postavlja globalni sistem kakovosti, izvaja presoje glede ustreznosti implementacije globalnega sistema kakovosti.

Za uspešno vzpostavitev sistema kakovosti je potrebno izdelati navodila ali pravilnike, ki povzemajo dele regulatornih zahtev, teh pa se potem držijo vsi zaposleni v organizaciji. Imenujmo jih splošni postopki.

Splošni postopki, ki so namenjeni večini aktivnosti in poslovnih procesov v združbi in jih potrebujemo za zadostitev regulatornim zahtevam ter validacijo računalniških sistemov, so naslednji:

- postopki dobre dokumentacijske prakse, kot to opisuje naslednje poglavje;
- postopki, ki govorijo o načinu in časovni periodi hrambe različnih tipov zapisov, tako v elektronski kot papirni obliki, kar je pomembno zaradi dostopnosti zapisov, potrebni pa so predvsem v primerih odpoklicev izdelkov s trga, raziskav odstopanj od dobre proizvodne prakse, lahko pa služijo le kot dokazilo o pravilnosti izvedbe procesov (npr. proizvodnih, laboratorijskih);
- postopki, ki predpisujejo izobraževanja, frekvenco in način izobraževanja. Z vidika računalniškega sistema je to pomembno, ker se ob izgradnji ali spremembi funkcionalnosti računalniškega sistema posledično spremenijo tudi navodila za delo s sistemom, gledano z vidika regulative pa to pomeni, da morajo vsi uporabniki sistema biti ustrezno izobraženi o zadnjih veljavnih navodilih za delo s sistemom;
- postopek, ki predpisuje izvajanje internih presoj v združbi;
- postopek, ki predpisuje izvajanje presoj dobaviteljev glede ustreznosti sistema kakovosti ter poznavanja regulatornih zahtev (za dobavitelje računalniških sistemov je zaradi specifik lahko postopek tudi ločen in napisan eksplicitno za obvladovanje dobaviteljev računalniških sistemov);
- postopek, ki predpisuje obvladovanje odstopov od dobrih praks, postopek lahko vsebuje tudi navodila, kako izvajati raziskave odstopov oz. odstopanj;
- postopek, ki predpisuje obvladovanje dobaviteljev in pogodb.

Poleg naštetih splošnih postopkov, ki podpirajo več poslovnih procesov v združbi, potrebujemo za validacijo računalniških sistemov dodatno tudi specifične predpise oz. splošne postopke, ki so potrebni za validacijo računalniških sistemov. Teh postopkov je običajno več, našteti in opisani so v naslednjih poglavjih.

Struktura splošnih postopkov mora biti definirana vnaprej, najbolje, da ima združba predpis glede strukture poglavij splošnih postopkov ali predlogo, na podlagi katere se splošni postopki izdelujejo. Temeljna poglavja vsakega splošnega postopka so:

- namen postopka, kjer se pojasni, čemu splošni postopek sploh služi,
- odgovornosti za izvajanje, kjer so pojasnjene odgovornosti,
- obseg, kjer so razjasnjene meje in omejitve splošnega postopka,
- definicije, kjer se definira terminologija, uporabljena v splošnem postopku,
- vsebina splošnega postopka.

Splošni postopki kot dokumenti morajo biti podvrženi obvladovanju sprememb, kar lahko obvladujemo ročno ali skozi validiran elektronski dokumentni sistem.

4.1.1 Načela dobre dokumentacijske prakse

V farmacevtski industriji je vedno potrebno upoštevati načela dobre dokumentacijske prakse, še posebej pa to velja pri kvalifikacijskih in validacijskih aktivnostih, kot je denimo validacija računalniškega sistema. Potrebno je imeti splošni postopek, ki definira, kaj sploh je dobra dokumentacijska praksa, kaj zajema in kako se lotiti zapisov, predpisov in dokumentacije nasploh.

- Splošne zahteve dobre dokumentacijske prakse:
    - tip in naziv predpisa,
    - nadzor nad različicami glede na spremembo, datum izdelave, datum pregleda,

- predpisana oblika in format dokumenta,
- definiran dostop do zapisov in predpisov, nadzor nad tiskanjem in kopiranjem,
- način varovanja, hrambe in arhiviranja zapisov ter predpisov (tako veljavnih kot neveljavnih),
- skladnost z zahtevami 21 CFR Part 11.

- Dobre prakse izdelave dokumentov:

  - primerno izdelane predloge dokumentov, da se ob uporabi vršijo nedvoumni vnosi v te predloge, zagotovljen mora biti ustrezen nadzor nad uporabo dokumentacije, da se prepreči uporaba starejših različic dokumentov, ipd.;
  - dokumenti morajo biti definirani glede na vrsto (npr. VP, letni pregled, analiza rizikov, testna specifikacija ...), naslov dokumenta, verzijo, enoto veljavnosti dokumenta, datum izdelave, pregled in odobritev dokumenta;
  - način uporabe in izpolnjevanja validacijske dokumentacije za informacijske sisteme;
  - način uporabe in pisanje zapisov, pregledovanje zapisov ter njihova hramba.

4.1.2 Obvladovanje odstopanj

Splošni postopek naj opisuje, kako se obvladujejo odstopi od dobrih praks – GxP. Odstop je definiran kot neskladnost izvajanja postopkov, specifikacij, protokolov ali procesov z dobro proizvodno prakso.

Sistem obvladovanja odstopov je ključen z vidika obvladovanja odstopov ter prispeva k stalnemu izboljševanju procesov razvoja, proizvodnje in kontrole izdelkov, s ciljem zagotavljanja njihove varnosti, kakovosti in učinkovitosti.

Postopek obvladovanja odstopov naj vsebuje:

- Opis postopka dela

  Kjer je zapisano, kaj storimo, ko pride do neskladja, kako reagiramo in koga vse je potrebno o neskladju obvestiti. Vprašati se moramo, ali imajo dostop do ključnih aplikacij za beleženje incidentov res vsi zaposleni ali le posamezniki, in temu primerno zagotoviti in predpisati eskalacije ob odstopu.

- Klasifikacija odstopov

  Pri tem razložimo, kako v združbi klasificiramo odstope ter na katere tipe odstopov.

- Proces obveščanja in eskalacije kritičnih odstopov.
- Reševanje odstopov

  Tukaj zapišemo, kako se lotimo reševanja odstopov glede na tip, kdo lahko izvaja raziskave odstopov ter kakšni so minimalni pogoji (npr. izobraževanja, potrdila), proces reševanja odstopov, časovne omejitve ipd.

- Korektivni ukrepi

Ti so lahko kot odgovor na odstop – korektivni, da se odstop več ne ponovi, ter kurativni, da se preprečijo enaki odstopi v prihodnje.

4.1.3 Elektronski zapisi in elektronski podpisi ter njihov način uporabe

Eden izmed temeljnih splošnih postopkov je postopek, ki definira, kako združba definira elektronske zapise, dodatno pa podaja splošne zahteve, ki jim morajo računalniški sistemi zadostiti, da dosegajo skladnost z regulativama 21 CFR Part 11 in EU Annex 11.

Splošni postopek mora jasno navajati:

- kriterije za elektronske zapise (da morajo biti računalniški sistemi validirani);
- klasifikacijo elektronskih zapisov, na primer
    - GxP relevantni,
    - GxP nerelevantni ipd.,
    - trajni in začasni elektronski zapisi;
- zaščito elektronskih zapisov (zagotavljanje integritete podatkov);
- zagotavljanje sledljivosti elektronskih zapisov (npr. skozi zgodovino dogodkov, ki beleži vsaj identiteto posameznika, časovno značko z datumom in časom ter spremenjene vrednosti parametrov);
- način hrambe elektronskih zapisov;
- obvladovanje sprememb v smislu, da ob spremembah na računalniškem sistemu elektronski zapisi ostanejo v obliki, da je omogočeno kronološko sledenje do originalnih vnosov oz. interakcij v računalniškem sistemu.

4.2 Temeljni postopki za validacijo računalniških sistemov

Poleg splošnih postopkov, naštetih v poglavju Interni standardi in splošni postopki, ki so namenjeni vsem poslovnim procesom znotraj združbe, je za validacije potrebno zagotoviti tudi posamezne postopke, ki so vezani na samo specifiko validacij. Na primer, za validacijo čiščenj je potrebno imeti predpisane dodatne splošne postopke, ki se podrobneje dotikajo le validacije čiščenj, enako velja denimo za področje validacije procesov. Prav tako pa to velja za validacije računalniških sistemov ter njihovo vzdrževanje v validiranem stanju. Ključni postopki za validacijo računalniških sistemov so našteti in opisani v naslednjih poglavjih. Vsi splošni postopki, vezani na validacijo računalniških sistemov, se medsebojno prepletajo in so v večini primerov tesno povezani.

4.2.1 Krovni splošni postopek, ki predpisuje validacijo računalniških sistemov

Združba mora razpolagati s splošnim postopkom, ki določa principe, načine, predpogoje in izvedbo validacije računalniških sistemov. Do tega sklepa pridemo, ko prebiramo regulatorne zahteve in ostale vire, ki se na regulativo naslanjajo (U.S. Food and Drug Administration, 2002, str. 1–34; U.S. Food and Drug Administration, 2003, str. 1–9; U.S. Food and Drug Administration, 2004, str. 7–8; U.S. Food and Drug Administration, 2006, str. 3–24; U.S. Food and Drug Administration, 2013a; U.S. Food and Drug Administration, 2013b; European Compliance Academy, 2011b, str. 7–22; European Compliance Academy, 2011c, str. 3–58; European Compliance Academy, 2011d, str. 3–28; European Commission, 2011a, str. 2–9; European Commission, 2011b, str. 2–5; European Commission, 2013; European Commission, 2013b; International Society for

Pharmaceutical Engineering - ISPE, 2008, str. 25–56; Schousboe, 2005, str. 20–30; PIC/S, 2007, str. 1–50) in ki od nas zahtevajo vzpostavljen sistem kakovosti v splošnem in tudi specifične postopke za validacijo računalniških sistemov.

Priporočljivo je imeti ločen postopek za validacijo IT aplikacij, računalniško podprtih proizvodnih sistemov ter računalniško podprtih laboratorijskih sistemov, ki je podrejen krovnemu postopku za validacijo računalniških sistemov. Vendar pa to ni pogoj, če krovni postopek za validacijo računalniških sistemov zajema validacijo vseh vrst sistemov in je to znotraj postopka jasno opredeljeno.

Vsebina postopka mora biti celovita in na primernem nivoju. Če se odločimo, da bo en splošni postopek zajemal vse vrste računalniških sistemov, ki jih združba uporablja, je smiselno, da splošni postopek opisuje splošne pristope k validaciji računalniških sistemov ter pristope k validaciji za vsak tip računalniškega sistema posebej (IT aplikacije, računalniško podprti proizvodni sistemi, računalniško podprti laboratorijski sistemi). V tem primeru je nivo splošnega postopka bolj podroben.

Če se odločimo za krovni postopek, ki opisuje validacije računalniških sistemov ter ločene postopke za vsak tip računalniškega sistema, je v krovnem splošnem postopku potrebno zajeti vsaj odgovornosti enot in zaposlenih, da vemo, kje so razmejitve. To je sicer smiselno definirati tudi v vseh ostalih splošnih postopkih.

Odgovorna oseba iz enote kakovosti je odgovorna v okviru predpisov predpisati kriterije in zahteve za validacijo računalniških sistemov, potrjuje tudi ključne dokumente v fazi validacije računalniškega sistema in odobri sistem za uporabo. Informacijska tehnologija je odgovorna za zagotavljanje funkcionalnosti, delovanje in validacijo IT aplikacij ter izvajanje operativnih aktivnosti in vzdrževanje sistemov (ko govorimo o računalniško podprtih proizvodnih ali laboratorijskih sistemih, se lahko te aktivnosti prenesejo na primernejše organizacijske enote in sistemske skrbnike), lahko pa je ena enota znotraj podjetja odgovorna za vse tipe računalniških sistemov. Vodstvo enot uporabnikov računalniških sistemov pa je odgovorno za zagotovitev, da uporabniki uporabljajo le validirane računalniške sisteme.

Poleg obsega splošnega postopka naj postopek vsebuje še definicije in vsebino, ki zajema:

- vodila in standarde, na podlagi katerih je postopek napisan,
- življenjski cikel računalniškega sistema,
- razvojne in validacijske aktivnosti,
- operativno delovanje sistema,
- razčlenitev računalniških sistemov (na primer kategorizacija po GAMP),
- upokojitev sistema,
- proces poteka validacije računalniških sistemov.

V krovnem postopku, ki predpisuje validacije računalniških sistemov, je smiselno poleg naštetega zapisati še odgovornosti in pogoje za zunanje izvajalce, ki delajo posege na računalniških sistemih združbe. Zunanji izvajalci morajo imeti dokazila, da razumejo regulatorne zahteve ter interne zahteve podjetja, v katerem delajo posege v računalniške sisteme. V primeru, da teh dokazil nimajo, je potrebno zagotoviti, da je med posegi prisotna v združbi zaposlena oseba, ki s temi dokazili razpolaga.

4.2.2 Izvedba krovne ocene analize rizika

Ker regulatorni organi vedno bolj poudarjajo pristope h kvalifikacijskim in validacijskim aktivnostim skozi analize rizikov oz. t. i. »Risk based approach« (U.S. Food and Drug Administration, 2006, str. 22), se validacijske aktivnosti računalniškega sistema vedno začnejo s krovno oceno analize rizikov (angl. *High Level Risk Assessment*, v nadaljevanju HLRA). Vendar pa to ni edini razlog, zakaj se je smotrno lotiti validacije sistema skozi analize rizikov; na podlagi analize rizikov lahko bistveno zmanjšamo stroške validacije sistemov (Ade, 2008), še posebej, če jo izvedemo, ko imamo potrjene URS in pred končno različico dizajn dokumentov (Woods & Beale, 2009, str. 54–58).

S pomočjo HLRA pridemo do rezultatov, ki predstavljajo osnovno izhodišče za definiranje obsega validacijskih aktivnosti računalniškega sistema. HLRA je eden izmed ključnih dokumentov pred začetkom validacije računalniškega sistema, zato je pomembno, da imamo enoten obrazec (najbolje formaliziran kot predlogo) za izvedbo krovne ocene analize rizika kot del splošnega postopka in ga uporabljamo za vse računalniške sisteme v združbi.

Vsebina postopka naj zajema proces izvedbe; izpolnjevanje, pregled in odobritev HLRA ter po odobritvi še vnos računalniškega sistema v seznam računalniških sistemov (če gre za nov računalniški sistem) in navodila za izpolnjevanje predloge HLRA.

Na podlagi HLRA vnesemo rezultate ocene sistema v seznam računalniških sistemov, če je bila HLRA izvedena retrospektivno, pa obstoječi sistem v seznamu računalniških sistemov le posodobimo.

HLRA naj opredeljuje vsaj:

- tip krovne ocene analize rizika:
    - nov sistem, sprememba na sistemu ali retrospektivna ocena,

- tip računalniškega sistema,
- kategorizacijo računalniškega sistema (na primer po GAMP),
- namen računalniškega sistema in katere procese podpira,
- GxP relevantnost računalniškega sistema:
    - ocena, v kolikšni meri sistem podpira GxP kritične procese (Schousboe, 2005, str. 26–27),

- 21 CFR Part 11 relevantnost računalniškega sistema,
- Sarbanes-Oxley Act (v nadaljevanju SOX) relevantnost sistema (v primerih, da gre za IT aplikacijo, ki se uporablja na primer v financah),
- ali bodo v sistemu hranjeni osebni podatki,
- vplive na zdravje, varnost in okolje (v nadaljevanju ZVO).

Pri tem pa ne smemo pozabiti na osnovne podatke o računalniškem sistemu, da definiramo lastnosti računalniškega sistema ter odgovorne osebe; ti so:

- različica programske opreme,
- kdo je lastnik sistema,
- kdo je sistemski skrbnik sistema,
- pod katero poslovno enoto spada računalniški sistem,

- kje se računalniški sistem nahaja ter
- kratek opis računalniškega sistema.

4.2.3 Ocena dobavitelja računalniškega sistema

Ocena dobavitelja računalniških sistemov je obvezna za vse dobavitelje GxP relevantnih računalniških sistemov, velja pa tudi za tiste dobavitelje oz. zunanje izvajalce, ki delajo spremembe ali posege na računalniških sistemih združbe.

V primeru nabave novega računalniškega sistema se napišejo URS, na podlagi katerih dobavitelj pripravi ponudbo, vendar kot združba v regulirani farmacevtski industriji lahko dobavitelju damo zeleno luč le v primeru, da uspešno prestane presojo.

Presojo dobavitelja izvaja strokovno usposobljena oseba, ki je običajno tudi odgovorna za sistem kakovosti računalniških sistemov v podjetju, torej QA manager danega področja. Dobavitelj mora razumeti zahteve farmacevtske industrije in mora poznati vsaj osnovne principe validacije računalniških sistemov, obenem pa imeti vzpostavljen svoj sistem kakovosti. Sicer ob presoji ne more pridobiti ustrezne ocene, posledično pa to pomeni, da ne more in ne sme posegati v GxP relevantne sisteme združbe.

Poleg namena, odgovornosti in definicij mora biti popisan proces poteka dela, pa tudi tip ocene dobavitelja. Razlikujemo presoje pri dobavitelju, poštne ocene dobavitelja s pomočjo vprašalnika, osnovno oceno dobavitelja glede na javno dostopne informacije o dobavitelju ali kombinacijo vseh naštetih ocen oz. presoj. Proces mora vsebovati informacije o odločitvi za tip ocene dobavitelja glede na kompleksnost in način uporabe računalniškega sistema, planiranje in izvedbo presoje, poročilo o presoji ter način spremljanja korektivnih ukrepov.

Pomembno je dejstvo, da presoja dobavitelja odraža trenutni posnetek stanja v času izvajanja nadzora. Odgovorne osebe za izvajanje presoje poročajo na podlagi dejstev, ki so bila razvidna na dan presoje, in ne na podlagi dobaviteljevih obljub.

4.2.4 Obvladovanje sprememb računalniških sistemov

Kot ugotavljajo Ali, Gonjare in D'souza (2012, str. 3706), je obvladovanje sprememb eden izmed ključnih stebrov sistema kakovosti. Neobvladovanje sprememb pomeni tveganje, da pridemo navzkriž z regulatornimi organi, saj ne dosegamo tistega, kar nam nalaga regulativa. Avtorji navajajo tudi ključne prednosti obvladovanja sprememb:

- strukturiran in konsistenten pristop k spremembam na sistemih,
- ustrezno dokumentiranje sprememb,
- obvladovanje rizikov, ki lahko ob spremembah nastanejo,
- jasno definiran proces, ki služi tudi obveščanju, in potrditev predlogov za spremembo s strani ključnih oseb,
- ustrezno dokumentiraje posega ob spremembah,
- obvladovanje seznama, vsebine sprememb in sledljivost izvedenih sprememb na sistemih,
- dokazilo regulatornim organom, da spremembe na sistemih v celoti obvladujemo.

Postopek obvladovanja sprememb naj bo usklajen s splošno politiko obvladovanja sprememb, kar zajema vrste računalniških sistemov, obvladovanje sprememb glede na

vrsto računalniških sistemov, način obvladovanja sprememb, opis procesa obvladovanja sprememb ter kategorizacijo sprememb, ki so lahko načrtovane in nenačrtovane ali nujne spremembe v operativni fazi uporabe računalniškega sistema. Kot navaja tudi PIC/S (2007, str. 21–23), mora splošni postopek obvladovanja sprememb zajemati vsakršno spremembo, ki ima vpliv na sistem, ter ločiti nujne spremembe od načrtovanih.

4.2.5 Obvladovanje dostopov in avtorizacij računalniških sistemov

Obvladovanje dostopov do sistemov je predpisano s strani regulatornih organov (EU Annex 11, 21 CFR Part 11), če govorimo o GxP relevantnem računalniškem sistemu.

Namen splošnega postopka obvladovanja dostopov in avtorizacij računalniških sistemov je predpisati in urediti proces obvladovanja dostopov do računalniških sistemov. To pomeni kontrolirano dodajanje novih uporabnikov v sistem, kontrolirano odvzemanje pravic uporabnikom in spreminjanje pravic dostopov do sistema obstoječim uporabnikom. V postopku je prav tako potrebno definirati odgovornosti za naštete aktivnosti.

V obsegu postopka za obvladovanje dostopov in avtorizacij računalniških sistemov definiramo, na katere tipe računalniških sistemov se postopek aplicira in v kolikšnem obsegu (GxP relevantni sistemi, GxP nerelevantni sistemi ipd.).

Postopek mora ločevati tudi med dostopi uporabnikov in dostopi administratorjev (sistemskih skrbnikov) do računalniškega sistema. Slednji imajo v večini primerov možnosti manipulacije z elektronskimi zapisi v sistemu in nastavitvami sistema, ki se po izvedenih kvalifikacijah ne bi smeli spreminjati. Prav tako imajo številni računalniški sistemi implementirane različne nivoje dostopov, ki so omejeni po funkcionalnostih, na primer:

- nivo 1 – Operater: vodenje osnovnih operacij procesa (najmanj pravic na računalniškem sistemu),
- nivo 2 – Tehnik: dodatne pravice k pravicam operaterja,
- nivo 3 – Tehnolog: vse pravice na sistemu, razen pravic sistemskih nastavitev in administracije,
- nivo 4 – Administrator: pravice sistemskih nastavitev in administracije, brez pravic tehnologa oz. vodenja procesa.

Vendar pa se pri računalniških sistemih pogosto pojavlja, da je na nivoju administratorja omogočeno delo s sistemom v celoti, tudi vodenje procesa, kar je s stališča regulatornih zahtev težje sprejemljivo. Zato je smiselno, da implementiramo računalniške sisteme, ki administratorjem ne omogočajo drugih pravic v sistemu kot pravice sistemskih nastavitev in administracije, če pa se temu ne moremo izogniti, pa to rešujemo z organizacijskimi predpisi, pri čemer nam je lahko v pomoč izjava administratorjev oz. sistemskih skrbnikov, da torej uporabniki z administratorskimi pravicami v računalniškem sistemu podpišejo izjavo, v kateri se zavezujejo, da bodo posege izvajali skladno z dobrimi praksami stroke ob upoštevanju politik, postopkov in navodil združbe (obvladovanje avtorizacij, obvladovanje sprememb na sistemu ipd.), da bodo sistemsko skrbništvo izvajali v okviru opisa delovnih nalog, da brez pisnega zahtevka ne bodo vpogledovali, spreminjali ali brisali podatkov na sistemih, da bodo skrbeli za varnost sistemov in podatkov na njih, da ne bodo delili svojih gesel ter da prevzemajo vso odgovornost ob kršitvi katere koli izmed naštetih zahtev.

Splošni postopek obvladovanja dostopov in avtorizacij računalniških sistemov mora prav tako imeti definiran proces izvajanja postopka.

4.2.6 Izvajanje varnostnih kopij, arhiviranja elektronskih zapisov in restavracije računalniškega sistema

Za vse vrste računalniških sistemov, ki hranijo GxP relevantne elektronske zapise, je potrebno imeti predpis, na kakšen način, kako frekventno in kam se elektronske zapise varnostno kopira in arhivira, da ne pride do izgub teh zapisov v primeru odpovedi sistema ali ob pojavu višje sile. Pri tem velja opomniti, da moramo v primeru izgube podatkov iz sistema imeti preverjen (potestiran) postopek, s katerim je sistemski skrbnik zmožen vzpostaviti sistem na predhodno, torej delujoče stanje, preden je prišlo do izgube podatkov oz. izpada celotnega sistema iz kakršnih koli razlogov.

Smiselno je torej imeti krovni splošni postopek, ki opisuje pristope k izvedbi varnostnih kopiranj, arhiviranj in nenazadnje tudi restavracije računalniškega sistema v splošnem smislu, dodatno pa ločen postopek za vse tipe računalniških sistemov. Nič pa ni narobe, če se celota zajame v en splošni postopek.

V obsegu postopka se pojasni, katere vrste podatkov, kot so denimo sistemske informacije (operacijski sistem), uporabniške informacije (uporabniški računi, mape ...) ipd., so predmet varnostnih kopij in arhiviranja. Postopek mora vsebovati še točen opis postopkov izvajanja varnostnih kopiranj in arhiviranj glede na tip sistema ter restavriranje podatkov, kjer se za vsak tip sistema predpiše način restavracije. Ob prvotni restavraciji je le-to smiselno potestirati in v tej fazi odpraviti morebitne pomanjkljivosti.

Nikakor pa ne smemo pozabiti na samostojne računalniške sisteme, kajti računalniški sistemi so lahko iz več razlogov izolirani iz omrežja združbe (stari sistemi, varnostna politika združbe ipd.). To je pomembno zlasti v primeru, ko združba razpolaga s centralnim računalniškim sistemom, ki služi za hrambo in arhiviranje podatkov iz vseh vrst in tipov računalniških sistemov. V takih primerih je skrbnik računalniškega sistema odgovoren za izvajanje varnostnih kopij in arhivov. Način, kako se teh posegov loti, pa mora temeljiti na analizi rizikov, kjer se ovrednoti, kateri elektronski zapisi sploh so GxP relevantni, ter določi najprimernejša frekvenca izvajanja varnostnih kopij na računalniškem sistemu.

Dodatno je potrebno izdelati navodila, po katerih se skrbnik sistema ravna ob izvajanju aktivnosti varnostnega kopiranja, arhiviranja in restavracije sistema, če je to potrebno. Restavracija sistema mora ob vzpostavitvi sistema biti potestirana, kar služi kot dokaz regulatornim organom, da so navodila za restavracijo ustrezna, da so elektronski zapisi sistema primerno hranjeni in dostopni ter da je način vzpostavitve sistema ob izpadu nazaj v operativno stanje ustrezen.

4.2.7 Neprekinjeno poslovanje in vzpostavitev računalniškega sistema

Sodobna združba ima običajno več računalniških sistemov, od katerih sta odvisna proizvodnja in poslovanje združbe. Za računalniške sisteme, ki so na podlagi HLRA z vidika nemotenega delovanja ocenjeni kot kritični, morajo združbe imeti predpis, na kakšen način zagotavljajo neprekinjeno poslovanje oz. proizvodnjo v primeru izpada računalniškega ali informacijskega sistema.

Ne smemo pozabiti na sisteme, brez katerih je poslovanje onemogočeno, saj proizvodnja obstane, dokler niso vzpostavljeni. Tak sistem je lahko na primer informacijski sistem za načrtovanje virov v združbi (angl. *Enterprise resource planning*, v nadaljevanju ERP), vendar je tudi za tovrstne sisteme potrebno imeti zapisan predpis, da se ob izpadu sistema proizvodnja ali poslovanje ustavi, dokler sistem ni vzpostavljen v predhodno stanje.

Postopek mora poleg samega obsega imeti v sklopu definicij pojasnjeno, kaj se smatra pod incident, nesrečo in kaj pod katastrofo. Za vsakega izmed možnih vzrokov (požar, voda, poškodba zgradbe, naravne nesreče (poplave, udari strel), potresi, izguba električne energije, sabotaže, poškodbe omrežij, odpovedi strojne opreme, teroristični napad, vojna, padec letala ipd.) se predpiše plan aktivnosti (scenariji), ki se jih (s simulacijo) testira, odgovorne osebe, nosilce določenih vlog pri varnostnih in drugih ukrepih, pa ustrezno izobrazi.

Postopek neprekinjenega poslovanja pa mora zajemati še pogoje za kritične računalniške sisteme, to so sistemi, ki morajo kljub nesreči ostati v delujočem stanju, na primer računalniški sistemi za hrambo varnostnih kopij, ki nam jih zagotavlja zunanji dobavitelj, podatkovni strežniki, omrežna infrastruktura. Pri procesih in sklopih računalniških sistemov se prav tako definirajo najdaljša možna časovna obdobja za nedelovanje računalniškega sistema. Za računalniške sisteme, ki so v upravljanju zunanjih dobaviteljev, poskrbimo s sklenitvijo temu primerne pogodbe.

4.2.8 Obvladovanje konfiguracij računalniških sistemov

Kot enega izmed dejavnikov moramo na računalniških sistemih obvladovati tudi konfiguracije. Sprememba konfiguracije vpliva na delovanje sistema in lahko se zgodi, da po uvedeni spremembi sistem preneha delovati v okviru funkcionalnosti, za katere je namenjen in tudi validiran. Ključnega pomena je, da vsakršno spremembo na sistemu obvladujemo s pomočjo procesa obvladovanja sprememb, enako velja tudi za obvladovanje konfiguracij. Vsaka sprememba v konfiguraciji se obravnava kot sprememba na računalniškem sistemu.

Ni potrebno, da ima vsak računalniški sistem dokument s konfiguracijami imenovan konfiguracijska specifikacija, angl. *Configuration Specification*, v nadaljevanju CS), le-te so lahko zajete tudi v dizajn dokumentih samega sistema. Je pa bistveno, da se predpiše način obvladovanja konfiguracij.

Poleg namena, odgovornosti, obsega, standardov in vodil ter opisa procesa obvladovanja konfiguracij je smiselno v splošni postopek napisati, kaj pod konfiguracijo računalniškega sistema sploh smatramo. Po International Society for Pharmaceutical Engineering - ISPE (2010, str. 87–99) je konfiguracija odvisna od tipa, kompleksnosti in kritičnosti računalniškega sistema. Med konfiguracijo računalniškega sistema štejemo programsko opremo in nastavitve, npr. programsko kodo, zaženljive datoteke, konfiguracijske datoteke, servisne pakete in njihove verzije, ostalo programsko opremo, npr. gonilnike, operacijske sisteme in njihove verzije, pa tudi specifični firmware programske opreme in verzije, strojno opremo, kot so PLC krmilniki in računalniki, strežniki, komunikacijske povezave, navodila in verzije navodil, npr. navodila za delo, navodila za vzdrževanje, podatkovne baze in verzije, nivoje uporabniških dostopov, varnostne popravke in ostale popravke. Pri kompleksnejših sistemih za nadzor/vodenje procesov, ki imajo večje število različnih komponent, pa lahko med konfiguracijo štejemo še module/sklope računalniškega sistema, verzije HMI modulov, povezave krmilnikov na druge sisteme, programsko kodo

krmilnikov, verzije programske opreme na krmilniku, navodila za delo in vzdrževanje, mehanske slike, elektro-shematske diagrame in podobno.

CS računalniškega sistema spada med žive dokumente, zato mora biti vedno ažurna in mora odražati konfiguracijo sistema v trenutnem stanju.

4.2.9 Obvladovanje incidentov računalniških sistemov

Vsak incident, ki se nam na računalniškem sistemu pripeti, je potrebno skrbno obravnavati, celoten potek od odkritja, obravnave in odprave incidenta pa je potrebno dokumentirati skladno z dobro dokumentacijsko prakso. To je poleg same regulatorne zahteve še posebej pomembno v primerih, ko pride do eskalacije incidenta v odstop od dobre proizvodne (ali druge) prakse, saj je ob raziskavi odstopa potrebna vsakršna informacija, če želimo priti do samega vzroka in ga posledično tudi uspešno odpraviti. Prav tako pa periodični pregled računalniških sistemov od nas zahteva pregled incidentov na sistemu.

Najbolje je, da v sklopu splošnega postopka predpišemo tudi veljavne obrazce oz. predloge dokumentov, na katere se podatki o incidentu vnašajo, saj s tem pripeljemo uporabnika do aktivnosti in dokumentiranja tistega, kar je bistveno, ter da se ključne informacije o incidentu ne izpustijo, obenem pa s predpisano predlogo že zagotavljamo skladnost z dobro dokumentacijsko prakso (številčenje strani, verzioniranje dokumentov ipd.).

V postopku poleg namena in odgovornosti v obsegu postopka obvladovanja incidentov računalniških sistemov definiramo tudi, katere tipe računalniških sistemov bomo v ta postopek zajeli; ali so to vsi tipi računalniških sistemov ali samo računalniško podprti proizvodni in laboratorijski sistemi, IT aplikacije pa obvladujemo na kakšen drug način. Incidente lahko prav tako razdelimo v več kategorij, na primer na aplikacijski incident in infrastrukturni incident, določimo pa tudi prioritete incidentov, na primer nizka prioriteta, visoka prioriteta in nujno.

Ravnamo seveda v skladu z zahtevami regulatornih organov; International Society for Pharmaceutical Engineering - ISPE (2010, str. 63–64) navaja, kaj naj bi zapis o incidentu vseboval oz. katere informacije je potrebno podati, ko pride do incidenta na računalniškem sistemu; to so:

- enoznačen identifikator računalniškega sistema,
- uporabniško ime zaposlenega in kontaktni podatki,
- datum in čas incidenta,
- datum in čas prijave incidenta,
- ime sistema/aplikacije/infrastrukture, okolja ter modul, v katerem je prišlo do incidenta (ali ime strojne opreme ter tip napake),
- opis incidenta,
- nujnost/prioriteta incidenta,
- želeni odzivni čas za odpravo incidenta (razen če je incident kategoriziran z zelo visoko prioriteto),
- ime skrbnika sistema oz. osebe, ki je prevzela informacijo o incidentu (npr. klic), ter datum in čas,
- ali sistem/aplikacija deluje v okviru dokumentiranih zahtev in ali dosega/ne dosega uporabnikovih zahtev,
- ocena incidenta, ki vsebuje tudi:

- kakšen je GxP vpliv (vpliv na zdravje pacientov, varnost produktov, integriteta podatkov in poslovni del),
- kaj je incident povzročilo in zakaj.

Ta zapis je lahko evidentiran na papirju ali pa se za obvladovanje incidentov uporabi IT aplikacija.

Ko je bil incident zabeležen, se začne reševanje incidenta, kjer se zabeležijo osnovne informacije o reševanju incidenta; to so:

- ugotovitev vzroka za incident, ang. root cause, npr. zunanji vpliv – izpad električne energije itd.;
- edinstven identifikator številke poročila incidenta (ki je enak pripadajočemu zapisu o incidentu; s tem zagotavljamo sledljivost med zapisom in poročilom o incidentu);
- opis rešitve za odpravo incidenta oz. proces odprave incidenta;
- reference (npr. za splošne postopke, predloge za spremembo, odstop …),
- ali so potrebna izobraževanja,
- neizvedene aktivnosti, vezane na incident (npr. izobraževanje uporabnikov glede na posodobljene splošne postopke),
- zgodovina dogodkov (ang. Audit trail) aktivnosti (zapis mora vsebovati: kdo, kdaj, kaj, zakaj je izvajal določeno aktivnost, da je incident na računalniškem sistemu odpravil),
- končne ugotovitve glede ustreznosti odprave incidenta,
- zaprtje incidenta, odobreno vsaj s strani sistemskega skrbnika sistema.

Da zares obvladujemo incidente ter da se le-ti ne ponavljajo (kar posledično privede do odstopa na računalniškem sistemu), izvajamo periodične preglede incidentov na računalniških sistemih, kjer si postavljamo vprašanja, ali imamo vse incidente zabeležene, ali so vse odprte aktivnosti, vezane na incidente, zaključene, ali so se vse aktivnosti ob odpravi incidenta zabeležile v poročilo o incidentu, ali se pojavljajo trendi incidentov, ki so povezani z določenim računalniškim sistemom, kolikokrat in kako je bil v reševanje incidenta vpleten dobavitelj računalniškega sistema ipd. Da je pristop periodičnih pregledov incidentov za vse računalniške sisteme enak, formaliziramo vprašalnik v dokumentno predlogo, ki jo nato odgovorne osebe (sistemski skrbniki) ob periodičnem pregledu računalniškega sistema izpolnijo.

4.2.10 Obvladovanje seznama (inventarja) računalniških sistemov

Kot za ostale naštete postopke, tudi za seznam računalniških sistemov regulativa European Commission (2011b, str. 3) veleva, da mora biti ta seznam vzpostavljen in vsaj za GxP sisteme vedno ažuren. Možnosti, kako voditi evidenco računalniških sistemov, je več: lahko jo vodimo ročno ali s pomočjo IT aplikacije. V vsakem primeru pa je potrebno uvesti ustrezno kontrolo spreminjanja vsebine seznama, če uporabljamo IT aplikacijo, pa mora ta biti validirana.

Poleg namena, odgovornosti za izvajanje in obsega mora vsebina postopka zajemati predpis, katere informacije o računalniškem sistemu so minimalne v seznamu računalniških sistemov, na primer: ime sistema, identifikator računalniškega sistema – ID, tip računalniškega sistema, status validiranosti, datum validiranosti, GxP relevantnost ipd., popisati je potrebno potek dela, kjer se definira, kdaj se računalniški sistem na seznam vnese in kdaj se računalniški sistem kot inventar v seznamu posodobi. Potrebni so tudi periodični pregledi ažurnosti seznama računalniških sistemov, ki se lahko vrši samostojno

ali v sklopu drugih pregledov, na primer ob letnem pregledu računalniškega sistema se preveri tudi seznam računalniških sistemov in ali je predmetni računalniški sistem v seznamu ažuren.

4.2.11 Periodični pregledi računalniških sistemov

Kot navajata McDowall (2011a, str. 30) in International Society for Pharmaceutical Engineering – ISPE (2008, str 43–44), je cilj periodičnih pregledov zagotoviti vodjem procesa in vodstvu, da sistem obvladujemo v skladu s pričakovanji regulatornih organov ter da identificiramo nepravilnosti oz. neskladja in šibke točke računalniškega sistema ter jih odpravimo.

Z ugotovitvami omenjenega avtorja se v celoti strinjam, da pa to celovitost računalniškega sistema dosežemo, moramo izhajati iz kontrolnih točk, kar zajema (International Society for Pharmaceutical Engineering - ISPE, 2010, str. 112–113):

- pregled dokumentacije življenjskega cikla računalniškega sistema,
- pregled uporabniških pravic,
- pregled izobraževanj uporabnikov računalniškega sistema,
- pregled zgodovine dogodkov,
- pregled izvajanja preventivnih vzdrževalnih aktivnosti,
- pregled incidentov in odstopov na računalniškem sistemu,
- pregled ažurnosti računalniškega sistema v inventarju računalniških sistemov,
- pregled realizacije korektivnih ukrepov iz predhodnega periodičnega pregleda.

Periodični pregledi se morajo planirati letno, frekvenca periodičnih pregledov pa mora temeljiti na konkretnih utemeljitvah, najbolje na podlagi analize rizikov vsakega izmed računalniških sistemov.

Cilj periodičnih pregledov je torej preveriti, ali je računalniški sistem z vidika regulatornih zahtev primeren za uporabo v produkcijski rabi oz. se s periodičnim pregledom potrdi njegov status (International Society for Pharmaceutical Engineering - ISPE, 2008, str. 43–44). Za vse ugotovljene nepravilnosti oz. neskladja računalniškega sistema z internimi in regulatornimi predpisi je potrebno predpisati korektivne ukrepe in jih redno spremljati, da se ugotovljene vrzeli odpravijo, določiti rok za izvedbo ter odgovorne nosilce aktivnosti. Neskladja vrednotimo glede na kritičnost, kar navaja tudi McDowall (2011b, str. 27):

- manjše neskladje:
  ni vpliva na elektronske zapise, kakovost izdelka ali varnost pacientov;

- srednje neskladje:
  majhen vpliv na elektronske zapise, kakovost izdelka ali varnost pacientov;

- večje neskladje:
  sistemski odstop, ki ne vpliva na elektronske zapise, kakovost izdelka ali varnost pacientov, ter druga podobna neskladja;

- kritično neskladje:
  sistemski odstop, ki ima vpliv na elektronske zapise, kakovost izdelka ali varnost pacientov.

Priporočljivo je, da že sam splošni postopek poleg namena, odgovornosti in definicij zajema in opisuje tudi proces izvedbe periodičnega pregleda, dokumentiranje in obvladovanje korektivnih ukrepov.

5 ŽIVLJENJSKI CIKEL RAČUNALNIŠKEGA SISTEMA S PRAKTIČNIM PRIMEROM

5.1 Življenjski cikel računalniškega sistema

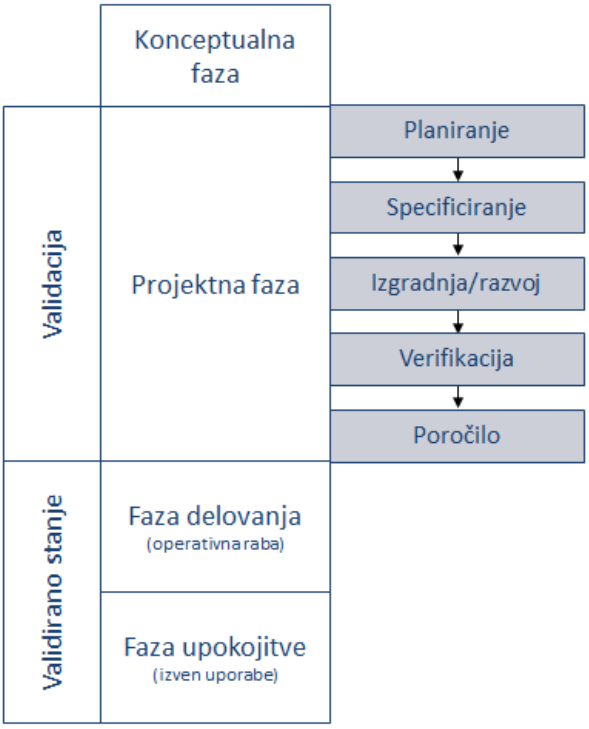
K življenjskemu ciklu pri validaciji računalniških sistemov lahko pristopimo na tri načine, ki se medsebojno razlikujejo po obsegu oz. se nadgrajujejo (Remén, 2005, str. 24). Kot navaj Remén (2005, str. 24) tako ločimo življenjski cikel razvoja računalniškega sistema, življenjski cikel implementacije računalniškega sistema in celotni življenjski cikel računalniškega sistema.

Da zagotovimo regulatorno skladnost in da računalniški sistem deluje znotraj zahtevanih specifikacij, moramo upoštevati življenjski cikel računalniškega sistema (PIC/S, 2007, str. 7), ki nam zagotavlja razumevanje zahtev, ki jih imamo glede računalniškega sistema, ter sistematičnost pri razvojnih aktivnostih, implementaciji, uporabi in upokojitvi računalniškega sistema.

Življenjski cikel računalniškega sistema sestavimo na logičen način glede na predpise regulatornih zahtev in strokovne literature (U.S. Food and Drug Administration, 2002, str. 1–34; U.S. Food and Drug Administration, 2003, str. 1–9; U.S. Food and Drug Administration, 2004, str. 7–8; U.S. Food and Drug Administration, 2006, str. 3–24; U.S. Food and Drug Administration, 2013a; U.S. Food and Drug Administration, 2013b; European Commission, 2011a, str. 2–9; European Commission, 2011b, str. 2–5; European Commission, 2013a; European Commission, 2013b; European Compliance Academy, 2011e, str. 2–12; European Compliance Academy, 2011f, str. 3–46; European Compliance Academy, 2011g, str. 3–31; International Society for Pharmaceutical Engineering - ISPE, 2008, str. 65–79; International Society for Pharmaceutical Engineering - ISPE, 2010, str. 17–19; PIC/S (2007, str. 1–50; Huber, 2012), ki nas že v osnovi omejita v okvire, znotraj katerih izdelamo koncept oz. način.

V tem poglavju bo opisan koncept življenjskega cikla računalniškega sistema kot celote, sestavljene iz štirih faz, kakor so navedene v priročniku GAMP5 (International Society for Pharmaceutical Engineering - ISPE, 2008, str. 26), in poglavitnih pet aktivnosti projektne faze/validacije računalniškega sistema – planiranje, specificiranje, izgradnja/razvoj, verifikacija in poročilo, kot prikazuje Slika 7.

Slika 7: Prikaz modela celotnega življenjskega cikla računalniškega sistema



- Konceptualna faza:

  V začetni, konceptualni fazi združba oz. zaposleni razmišljajo o ideji, nekem računalniškem sistemu za, denimo, avtomatizacijo proizvodnega procesa. V tej fazi nastane osnutek funkcionalnosti (zahtev), ki naj bi jih računalniški sistem omogočal, in se izpelje odločitev, ali se sploh lotiti, v našem primeru, projekta avtomatizacije procesa.

- Projektna faza:

  Projektna faza zajema planiranje in ocenjevanje oz. presojo dobavitelja glede ustreznosti. V tej fazi se izdela vsa dokumentacija, potrebna za izdelavo, ter izpelje celotna validacija računalniškega sistema:

  - planiranje,
  - specificiranje,
  - izgradnja/razvoj,
  - verifikacija,
  - poročilo.

Projektna faza je podrobneje prikazana in opisana s procesnimi diagrami v naslednjih odstavkih.

- Faza delovanja:

  je običajno najdaljša faza, torej ko je računalniški sistem v operativni rabi. V tej fazi je lastnik sistema odgovoren, da računalniški sistem ohranja v validiranem stanju. To pomeni, da je za sistem potrebno ustrezno skrbeti, torej so nujne aktivnosti obvladovanje sprememb na računalniškem sistemu, izvajanje

vzdrževalnih aktivnosti, izvedba periodičnih pregledov, zagotavljanje, da so navodila za delo in splošni postopki ažurni ter da so uporabniki o njih izobraženi, sem pa spada še skrb za nadzor dostopov do sistema ter za varnostno kopiranje in arhiviranje podatkov.

- Faza upokojitve:

  Do upokojitve pride, ko se odločimo, da računalniškega sistema več ne bomo uporabljali. Pri tem moramo biti pazljivi na to, kako izvedemo (in dokumentiramo) proces upokojitve in kaj naredimo z elektronskimi zapisi na sistemu.

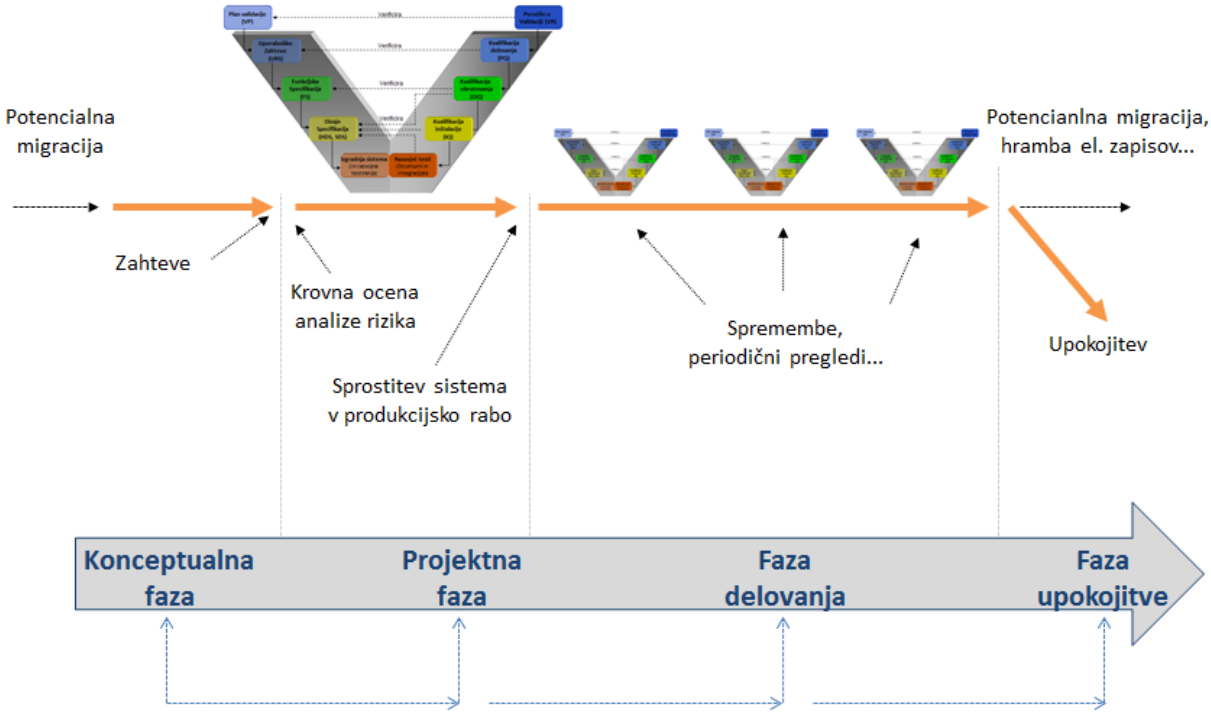
Podrobnejši pregled življenjskega cikla računalniškega sistema v enakih fazah kot Slika 7 prikazuje tudi Slika 8. Modra puščica na Sliki 8 prikazuje časovnico faz (konceptualna faza, projektna faza, faza delovanja, faza upokojitve), zgornji del slike (nad puščico) pa potek aktivnosti na računalniškem sistemu.

V konceptualni fazi se, kot že opisano, kreirajo URS za računalniški sistem in HLRA, s tem pa preidemo v projektno fazo. Projektna faza je podvržena celotni validaciji računalniškega sistema, kjer sledimo celotnemu V-modelu, kot je to razvidno s Slike 8. Ko se projektna faza zaključi, računalniški sistem preide v fazo delovanja, kar pomeni operativno rabo računalniškega sistema.

Ko je sistem enkrat v redni uporabi, lahko pride do zahtev uporabnika, da se računalniški sistem nadgradi, lahko pa pride tudi do spremembe procesa ali kakšne druge spremembe na računalniškem sistemu. Če gre za spremembe, ki ne vplivajo bistveno na delovanje računalniškega sistema, nam ni potrebno ponovno čez celoten proces validacije računalniškega sistema, temveč izvedemo le tisto, kar je na računalniškem sistemu spremenjeno – to na Sliki 8 prikazujejo manjši V-modeli (nad fazo delovanja).

Sčasoma, ko računalniški sistem več ne more služiti v polnem obsegu ali se ga iz kakršnih koli drugih razlogov odstrani iz operativne rabe, preidemo v fazo upokojitve, kjer je potrebno tak računalniški sistem upokojiti skladno s predpisanimi splošnimi postopki. Ob upokojitvi računalniškega sistema je treba največjo pozornost nameniti hrambi GxP relevantnih elektronskih zapisov (podatkov) na računalniškem sistemu, da le-ti ostanejo dostopni pooblaščenim osebam in v celoti berljivi še nadaljnjih nekaj let po upokojitvi računalniškega sistema (običajno je ta doba 10 let po upokojitvi). V primeru, da upokojeni računalniški sistem nadomestimo z novim računalniškim sistemom, lahko izvedemo migracijo podatkov v nov sistem in s tem zagotovimo dostopnost podatkov, obenem pa s tem dejanjem (migracijo) preidemo, kot prikazuje Slika 8, v konceptualno fazo novega računalniškega sistema, ki ga je potrebno validirati.

Slika 8: Faze življenjskega cikla – podrobnejši pogled



Vir: Prirejeno po International Society for Pharmaceutical Engineering - ISPE, GAMP 5: A Risk-based Approach to Compliant Gxp Computerized Systems, 2008, str. 26–37.

5.2 Validacijska dokumentacija skozi življenjski cikel računalniškega sistema

V tem poglavju bomo izpostavili življenjski cikel računalniškega sistema z vidika validacijske dokumentacije in kako zagotoviti skladnost računalniškega sistema kljub dejstvom, da je ta skozi svoj življenjski cikel podvržen mnogim spremembam.

Aktivnosti, ki so potrebne za izvedbo na računalniškem sistemu ob spremembi, so odvisne od kompleksnosti sistema, procesa in kritičnosti. Le stežka, če ne celo nemogoče bi bilo definirati neko splošno pravilo, katere aktivnosti je potrebno zajeti, da bomo po uvedeni spremembi na računalniškem sistemu lahko rekli, da le-ta deluje zanesljivo in v skladu s specifikacijami.

Za začetek je smiselno, da naštejemo vse dokumente, ki so potrebni za validacijo računalniškega sistema, in na kratko opišemo, čemu so namenjeni. Ti dokumenti predstavljajo »veliki« V-model, kot prikazuje Slika 3, v naslednjem koraku pa izpostavimo tiste dokumente, za katere moramo zagotavljati ažurnost in ki morajo biti podvrženi posodobitvi ob vsaki spremembi računalniškega sistema. Ti dokumenti so zajeti v »majhnem« V-modelu na Sliki 8, izvedbo teh aktivnosti pa od nas pričakujejo tudi regulatorni organi (Joshi, 2005, str. 64).

5.2.1 Dokumentacija ob prvotni validaciji (ali revalidaciji) računalniškega sistema

V tem odseku se bomo podrobno spustili v projektno fazo in podrejene aktivnosti (planiranje, specificiranje, razvoj, verifikacija, poročilo). Dokumentacija, ki v tej fazi nastane, zajema:

- Plan validacije – VP

- V VP definiramo obseg računalniškega sistema, razvojno metodologijo sistema, planirane validacijske aktivnosti in testiranja, prav tako predpišemo splošne postopke, ki so pomembni za delovanje sistema. Validacijske aktivnosti morajo imeti definirane nosilce in vloge, ki so skladne s predpisanimi splošnimi postopki združbe.

- URS

  - URS so temeljni dokument za validacijo računalniškega sistema (Stein, 2006, str. 79–81, in Culin, 2011, str. 32–33).
  - V URS se definirajo zahteve uporabnikov računalniškega sistema, kjer je potrebno poleg procesnih upoštevati tudi tehnične in regulatorne vidike računalniškega sistema. URS morajo pokrivati vsaj:

    - zahteve strojne opreme (arhitekturo sistema, delovno okolje, opremo, vmesnike ...),
    - zahteve programske opreme (funkcionalnosti aplikativnega dela računalniškega sistema, nivoje zaščite, obvladovanje elektronskih zapisov v primeru, da sistem hrani GxP relevantne elektronske zapise, nivoje zaščite/dostopa do sistema, ekranske prikaze, logično zaščito) ter ostale zahteve, ki jih predpisuje regulativa,
    - povezave z drugimi sistemi.

- FS

  - FS je dokument, ki definira, kaj bo sistem delal in katere funkcije lahko izvaja. FS odraža URS in mora biti z njimi skladna. Za orientacijo navajamo nekaj točk, ki jih lahko vsebuje FS računalniško podprtega proizvodnega sistema:

    - arhitektura sistema (nadzorni nivo, krmilni nivo, proizvodna oprema, način povezave ipd.),
    - seznam funkcionalnosti sistema,
    - opis krmilno-regulacijskih zank,
    - fizične (npr. interloki) in logične zaščite (npr. gesla) sistema,
    - vhodni in izhodni podatki iz sistema,
    - prenos parametrov na proizvodno opremo,
    - opis alarmov in sporočil,
    - zgodovina dogodkov (spremembe parametrov, alarmi, prijave/odjave iz sistema ...),
    - prikaz procesnih vrednosti na nadzornem sistemu (vizualizacija procesa),
    - ostali mehanizmi, ki so potrebni iz vidika regulatornih zahtev.

- HDS in SDS

  - HDS definira arhitekturo strojne opreme, na primer krmilnike, osebne računalnike, proizvodno opremo, povezave med posameznimi elementi.
  - SDS definira tehnične funkcije, ki opisujejo funkcionalnosti, zapisane v FS, na primer blok diagrame, diagrame stanj, logične tabele, strukturo podatkovne baze, standarde kodiranja, verzijo programske opreme ipd.

- Kvalifikacija načrtovanja (angl. *Design Qualification*, v nadaljevanju DQ)

    - Predpogoj za DQ so URS, FS, HDS in SDS.
    - Pri DQ pregledamo FS, SDS in HDS, ali so zajete in pravilno interpretirane URS. Rezultat pregleda formaliziramo. V primerih odstopanj je potrebno dizajn dokumentacijo ustrezno popraviti in posodobiti verzijo dokumentov, v primeru nekritične funkcionalnosti pa lahko popravimo tudi URS (in jim posodobimo verzijo).

    Pozitivni učinki izvedbe DQ so opazni tudi pri manj uporabljenih virih tekom projekta, saj odkrijemo neskladnosti že v zgodnji fazi projekta, kjer za aktivnosti za odpravo ugotovljenih vrzeli ne potrebujemo toliko virov, kot bi jih, če bi neskladja ugotovili v fazi izgradnje sistema ali v fazi delovanja (Rao & Sastri, 2011, str. 1235–1236).

- Izgradnja sistema na osnovi FS, HDS in SDS

    - Po potrjeni kvalifikaciji načrtovanja se lotimo izgradnje računalniškega sistema. Kot osnovo za razvoj vzamemo dizajn dokumentacijo.

- IQ

    - Namen IQ je pokazati, da sta strojna in programska oprema nameščeni skladno s specifikacijami proizvajalca ali dobavitelja. Posamezni sklopi IQ testiranj se lahko izvajajo pri dobavitelju, kar imenujemo Factory Acceptance Test (v nadaljevanju FAT). Drugi del je Site Acceptance Test (v nadaljevanju SAT) in se izvaja pri naročniku.

- OQ

    - OQ zagotavlja, da sistem deluje skladno s FS. Smiselno je, da so OQ testne specifikacije izdelane v kontekstu z navodili za delo. Zaželeno je, da se OQ testi izvajajo na realnem okolju, lahko pa se izvajajo tudi na testnem okolju.

- PQ

    - S PQ dokazujemo, da sistem deluje tako, kot je bil definiran v URS. Zato je smiselno, da PQ testiranja izvaja uporabnik, ki je sistem zahteval, saj sam najbolje ve, kakšne so bile njegove želje. Za razliko od OQ testiranj morajo biti PQ testiranja izvedena na produkcijskem okolju.

- VR

    - VR služi kot formalni dokument za odobritev sistema v produkcijsko rabo in preverja vse točke z naslova VP. VR mora vsebovati vsaj:

        - seznam validacijskih aktivnosti (reference na plane testiranj IQ, OQ in PQ),
        - povzetek rezultatov testiranj (reference na poročila o testiranjih IQ, OQ in PQ),

- poročilo, da so vsi potrebni postopki in navodila za delo posodobljeni oz. kreirani ter da so vsi uporabniki o njih ustrezno izobraženi,
- poročilo ostalih točk iz VP,
- izjavo, da je sistem primeren za uporabo v produkciji.

Poleg naštete dokumentacije je za celovito validacijo in zadostitev potrebam regulatornih zahtev potrebno izvesti še:

- CS,
- matriko sledljivosti (angl. *Traceability Matrix*, v nadaljevanju TM):

    - za lažji pregled, ali so vse funkcionalnosti sistema ustrezno potestirane, moramo zagotoviti sledljivost med URS, FS, HDS in SDS ter izvedenimi testi IQ, OQ in PQ. Zagotavljanje sledljivosti nam predpisuje regulativa, lahko pa jo vkomponiramo tudi v funkcionalno analizo rizikov (v nadaljevanju FRA), vendar le v primeru, ko točno vemo, kaj bomo kje (IQ, OQ, PQ) testirali.

5.2.2 Obvladovanje sprememb in validacijska dokumentacija računalniškega sistema

Ob spremembah na računalniškem sistemu moramo le-te voditi skladno s splošnim postopkom za obvladovanje sprememb, vendar ni dovolj zgolj dokumentiranje spremembe in izvedba testiranj. Potrebno je poskrbeti tudi za ostale dokumente, ki predstavljajo jedro računalniškega sistema. Validacijska dokumentacija mora biti v času življenja sistema vedno ažurna in mora prikazovati trenutno stanje računalniškega sistema (as built). Ključni dokumenti, ki to ponazarjajo, so »živi« dokumenti oz. dokumentacija življenjskega cikla (angl. *Life-cycle*) računalniškega sistema.

Problematika, ki se v praksi pogosto pojavlja, je, da se spremembe z dokumentacijskega stališča vodijo na sistemu za vsako spremembo posebej. Če ponazorimo s primerom, to pomeni, da se za spremembo na sistemu napiše nove URS, ki zajemajo le želene dodatne funkcionalnosti računalniškega sistema, namesto da bi posodobili že obstoječe (prvotne) URS in verzijo dokumenta. Iz te problematike sledi, da imamo tudi ostalo dokumentacijo življenjskega cikla le delno in neažurno oz. vezano le na uvedeno spremembo na računalniškem sistemu. Čez čas, ko se na računalniškem sistemu nabere več sprememb, smo vse bolj daleč od tega, da bi imeli ažurno dokumentacijo računalniškega sistema, dokumentirano imamo le začetno validacijo ter individualne spremembe.

To pa pomeni, da nismo skladni z regulatornimi zahtevami, ker nimamo ažurne dokumentacije življenjskega cikla računalniškega sistema, posledično pa ne moremo zagotavljati sledljivosti skozi celoten sistem. Rezultat neupoštevanja življenjskega cikla dokumentacije računalniškega sistema se lahko odrazi kot večje odstopanje ob inšpekciji regulatornih organov. V takih primerih je najučinkovitejši korektivni ukrep posodobitev Life-cycle dokumentacije ali revalidacija sistema, kar je ne samo časovno zamudno, temveč je potrebnih tudi veliko človeških virov, prav tako pa imamo težave v proizvodnji, če tak računalniški sistem nadzoruje in krmili kritične procese neprekinjeno (24/7).

5.3 Proces poteka projektne faze/validacije računalniškega sistema (s praktičnim primerom)

Projektno fazo sem se odločil podrobneje pojasniti, saj sem mnenja, da je ta faza ključnega pomena, če želimo računalniški sistem uspešno spraviti čez proces validacije. Skrbna preučitev regulatornih zahtev in strokovne literature (U.S. Food and Drug Administration, 2002, str. 1–34; U.S. Food and Drug Administration, 2003, str. 1–9; U.S. Food and Drug Administration , 2004, str. 7–8; U.S. Food and Drug Administration, 2006, str. 3–24; U.S. Food and Drug Administration, 2013a; U.S. Food and Drug Administration, 2013b; European Commission, 2011a, str. 2–9; European Commission, 2011b, str. 2–5; European Commission, 2013a; European Commission, 2013b; European Compliance Academy, 2011e, str. 2–12; European Compliance Academy, 2011f, str. 3–46; European Compliance Academy, 2011g, str. 3–31; International Society for Pharmaceutical Engineering - ISPE, 2008, str. 65–79; PIC/S (2007, str. 1–50; Huber, 2012) nas pripelje do sestave potek procesa projektne faze oz. validacije računalniškega sistema, kot je opisano v tem poglavju. Možne so seveda različne variacije, vendar veliko manevrskega prostora glede drugačnega pristopa vseeno ni. Predstavljen potek procesa projektne faze oz. validacije računalniškega sistema je odraz lastnega sklepanja na podlagi preučenih in analiziranih regulatornih zahtev.

Validacijo računalniških sistemov je smiselno opredeliti kot projekt (projektna faza), kot to prikazujeta Sliki 7 in 8, saj se validacija računalniškega sistema konča, ko slednji preide v fazo delovanja (operativno rabo). A da se validacije računalniških sistemov sploh lahko lotimo, je potreben predpogoj vzpostavljen sistem kakovosti (ki je vzpostavljen, ko so veljavni in implementirani vsi relevantni splošni postopki, kot je opisano v prejšnjih poglavjih).

V naslednjih procesnih diagramih je predstavljen zgrajen model kakovosti na praktičnem primeru poteka validacije proizvodnega računalniškega sistema SCADA skozi faze planiranja, specificiranja, izgradnje/razvoja, verifikacije ter poročil. S fazo poročila se projekt validacije računalniškega sistema zaključi in začne se faza delovanja, kar pomeni operativno rabo računalniškega sistema.

Da bo model kakovosti na primeru čim bolj realen, v naslednjih odstavkih podajam ključne informacije o računalniškem sistemu.

Tehnolog v proizvodnji farmacevtskega podjetja želi ročno vodeni proizvodni proces nadzorovati in krmiliti računalniško. V proizvodnem procesu mora tehnolog venomer paziti in nastavljati kritične procesne parametre, kot so denimo temperatura, hitrost in čas mešanja v proizvodnem procesu, da parametri ne gredo izven specificiranih meja. Tehnolog izvaja korake v sekvenci skladno z navodili v proizvodnem poročilu.

Tehnolog je v tem primeru uporabnik, ki začne s pisanjem URS za računalniški sistem. V našem primeru je to SCADA, saj nadzira in krmili proizvodni proces. Pri snovanju URS za nadzorno-krmilni sistem podajo svoje mnenje tudi QA manager na področju računalniških sistemov z vidika regulatornih zahtev, odgovorna oseba za ZVO, pooblaščenec za informacijsko varnost ter odgovorna oseba, ki bo z računalniškega vidika prevzela skrbništvo, torej sistemski skrbnik SCADA sistema. Vodja proizvodnega obrata je običajno v vlogi lastnika nadzorno-krmilnega sistema in je odgovoren, da se z računalniškim sistemom ravna skladno s predpisi (regulativo).

Računalniške sisteme za lažji pristop k validaciji uvrstimo v eno izmed GAMP kategorij, ki za računalniške sisteme v farmacevtski industriji predstavljajo neki standard.

Poenostavljeno rečeno, tehnolog v našem primeru torej potrebuje funkcionalnosti SCADA sistema, da mu na ekranskem prikazu (monitorju) prikazuje vse informacije, ki jih potrebuje za nemoteno delo, da lahko pogleda podatke o procesu za nek določen čas za nazaj v obliki grafa (x os: čas, y os: vrednosti kritičnih parametrov – npr. temperatura, hitrost mešanja, čas mešanja ...), potrebuje pa tudi možnost reguliranja temperature in hitrosti mešanja. Seveda pa ne bi bilo slabo imeti na SCADA sistemu shranjene še recepture, ki bi samodejno šla skozi sekvence (zaporedje) korakov in izvajala funkcije temperiranja, mešanja ipd., skratka vse, kar je potrebno za izvajanje proizvodnega procesa, popolnoma samodejno. Torej je zahteva uporabnika tudi to, da lahko proizvodni proces preko SCADA sistema vodi ročno ali pa da celoten proizvodni proces vodi SCADA samodejno, tehnolog pa le občasno preverja stanje in urgira po potrebi. Temu rečemo avtomatski režim delovanja SCADA sistema.

Kot prikazuje tabela 3, računalniške sisteme klasificiramo v štiri možne kategorije; računalniški sistem najlažje kategoriziramo po kompleksnosti, na primer glede na klasifikacijo računalniškega sistema po GAMP, kot to poleg International Society for Pharmaceutical Engineering - ISPE (2008, str. 128–132) in Tedstonea (2012) trdijo še McDowall (2010, str. 22–31) in drugi. Kar se tiče same kategorizacije SCADA sistema, smo ga v našem primeru (za nadzor in krmiljenje proizvodnje) umestili v GAMP4 kategorijo, to pa zato, ker gre za konfigurabilni računalniški sistem. Če kupimo na primer računalniški strežnik, nanj namestimo denimo aplikacijo Proficy iFix, ki je sicer v osnovi produkt podjetja General Electric, vendar je aplikacijo iFix za naše potrebe v proizvodnem procesu potrebno bistveno spremeniti (poleg aplikacije pa še dodelati krmilni nivo računalniškega sistema), za kar najamemo zunanjega dobavitelja, da nam računalniški sistem v celoti prilagodi skladno z našimi URS, je to konfigurabilni računalniški sistem. Ker imamo torej aplikacijo iFix, na kateri gradimo naš SCADA sistem, tega nadzorno-krmilnega sistema ne uvrščamo v GAMP5 kategorijo, saj se vanjo uvrščajo praktično iz nič (po meri) razvite aplikacije ali računalniški sistem kot celote, našega primera pa ne moremo uvrstiti niti v kategorijo GAMP3, kamor bi na primer uvrstili računalniški sistem ali aplikacijo, ki je kot take ne bi mogli prilagoditi našemu proizvodnemu procesu in bi jo vzeli táko, kot je – na primer določena proizvodna oprema z lastnim krmilnikom ali kupljena aplikacija, ki je ni moč spreminjati (angl. *Commerical of the Shelf*, v nadaljevanju COTS).

Tabela 3: Kategorizacija programske opreme po International Society for Pharmaceutical Engineering – ISPE – GAMP

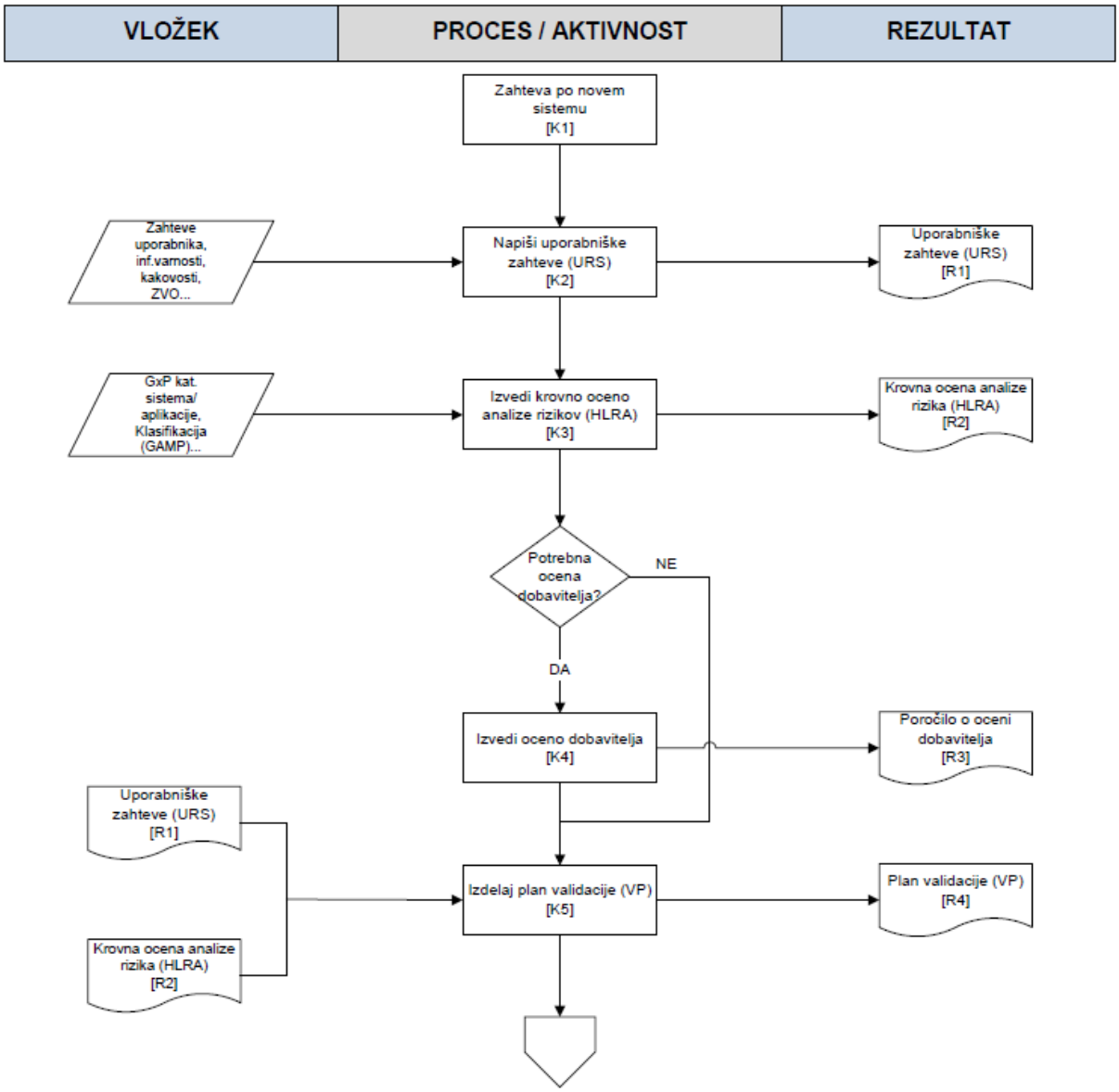
Kategorija	**Opis**	**Primer**
GAMP 1	Infrastrukturna programska oprema	Operacijski sistemi, podatkovne baze, strežniki za varnostno kopiranje in arhiviranje podatkov ...
GAMP 3	Nekonfigurabilne aplikacije/sistemi	Laboratorijska oprema s pripadajočo aplikacijo, proizvodna oprema s krmilnikom (PLC) ...
GAMP 4	Konfigurabilne aplikacije/sistemi	SCADA, ERP, MES ...
GAMP 5	Aplikacije/sistemi, razviti po meri	Računalniški sistemi in aplikacije, razvite posebej za potrebe združb v farmacevtski industriji (ki še ne obstajajo, jih ni).

Vir: International Society for Pharmaceutical Engineering – ISPE, GAMP 5: A Risk-based Approach to Compliant Gxp Computerized Systems, 2008, str. 128–132 in B. Tedstone Computer Systems Validation. Computer Systems Validation and Quality Assurance blog, 2012.

5.3.1 Planiranje

Slika 9 s pomočjo procesnega diagrama prikazuje, kako potekajo prve aktivnosti ob uvedbi novega računalniškega sistema.

Slika 9: Procesni diagram – Planiranje



V nadaljevanju podajam podrobnejši opis posameznih korakov v procesu.

[K1] Zahteva po novem sistemu
Uporabnik v proizvodnji razmišlja o novem računalniškem sistemu, ki bi mu podajal koristne informacije iz proizvodnega procesa in s katerim bi upravljal ter nadzoroval proizvodni proces. Uporabnik torej razmišlja o SCADA sistemu.

[K2] Napiši uporabniške zahteve (URS)
Uporabnik prenese svoje zamisli o računalniškem sistemu, v našem primeru SCADA sistemu, na papir. Vsaka zahteva ima svoj edinstven identifikator (npr. URS-01 ipd.), ki nam v nadaljnjih korakih validacije služi za sledljivost zahtev, da pri razvoju računalniškega sistema ne izpustimo katere izmed funkcionalnosti, ki jo želimo v sistemu imeti, hkrati pa s tem lažje preverimo, ali so vse funkcionalnosti računalniškega sistema bile testirane.

Ker tehnolog, ki je kot uporabnik SCADA sistema ekspert na področju vodenja proizvodnega procesa, običajno nima dovolj znanja o regulativi na področju računalniških sistemov, tukaj vstopi QA manager za kakovost na področju računalniških sistemov. V našem primeru bi QA manager na področju računalniških sistemov vsekakor dodal zahteve za obvladovanje integritete podatkov (onemogočen izbris podatkov, omejen dostop do podatkov, uporabniški nivoji dostopov ipd.), potrebne so tudi zahteve po alarmiranju, ne sme se pozabiti na verzioniranje in hrambo receptur na računalniškem sistemu, omogočena mora biti tudi zgodovina dogodkov, ki nam pove, kdo je delal na SCADA sistemu, kaj je delal, kdaj je delal in, ob določenih pogojih, zakaj je izvedel določen korak. Dodatno sledijo predpisi obvladovanja dostopov do SCADA sistema, periodični pregledi SCADA sistema, obvladovanje odstopanj od dobre proizvodne prakse, obvladovanje sprememb na računalniškem sistemu itd. Svoj delež prispevajo še odgovorna oseba ZVO, odgovorna oseba za informacijsko varnost (angl. *Information Security Officer*, v nadaljevanju ISEC) itd. Tako nastane dokument URS [R1]. Vsi podpisniki dokumenta URS so avtorji dokumenta. Avtor dokumenta URS je lahko tudi posameznik sam, vendar mora dokument URS v tem primeru kljub temu biti odobren s strani strokovno usposobljenih oseb na svojem področju (QA, ZVO, ISEC ...).

V preglednici 4 navajam primer URS dokumenta s tremi zelo enostavnimi zahtevami po funkcionalnosti računalniškega sistema, kjer v prvem stolpcu definiramo edinstven identifikator zahteve zaradi zagotavljanja sledljivosti, v drugem stolpcu navedemo zahtevo za računalniški sistem in v tretjem stolpcu kritičnost zahteve v smislu potreb po tej zahtevi. Lahko denimo rečemo, da je zahteva obvezna, pomembna ali želena.

Tabela 4: Primer URS – Funkcionalnosti v dokumentu URS

URS ID	Zahteva	Kritičnost
URS-x-01	…	Obvezno/pomembno/želeno
…	…	…
URS-F-49	Ekranski prikaz nadzornega sistema mora prikazovati celoten proizvodni proces v eni sliki na zaslonu s procesnimi vrednostmi.	Obvezno
URS-F-50	Nadzorni sistem mora na ekranskem prikazu prikazovati, kdo je v nadzorni sistem prijavljen, ter datum in čas.	Obvezno
URS-F-51	Nadzorni sistem mora beležiti vse procesne parametre v graf s časom na osi x in vrednostmi parametrov na osi y ter omogočati realnočasovni prikaz teh parametrov.	Obvezno
…	…	…
URS-x-n	Uporabniška zahteva – n	Obvezno/pomembno/želeno

[K3] Izvedi krovno oceno analize rizikov (HLRA)

S HLRA izvedemo prvotno klasifikacijo računalniškega sistema – GxP relevantnost računalniškega sistema, kategorizacijo računalniškega sistema/aplikacije (uporabimo GAMP kategorizacijo, kot prikazuje tabela 3). Kot je opisano, v našem primeru uvrstimo SCADA sistem v kategorijo GAMP4, saj gre za računalniški sistem, ki ga lokalni integrator oz. dobavitelj priredi našim potrebam na osnovi že obstoječe aplikacijske platforme iFix. Prav tako v HLRA determiniramo, ali je računalniški sistem 21 CFR Part11 relevanten (vprašamo se torej, ali bo sistem hranil elektronske zapise ali bomo uporabljali elektronske podpise). V našem primeru bo računalniški sistem hranil procesne podatke, ki so klasificirani kot GxP relevantni, zato sistem zapade pod 21 CFR Part11 regulativo. Elektronskih podpisov ne bomo uporabljali. Ovrednotimo tudi vpliv na ISEC, vpliv na ZVO ter vplive na občutljive osebne podatke. Na podlagi rezultata HLRA [R2] se

odločimo, katere validacijske aktivnosti računalniškega sistema so potrebne, da sistem ustrezno validiramo.

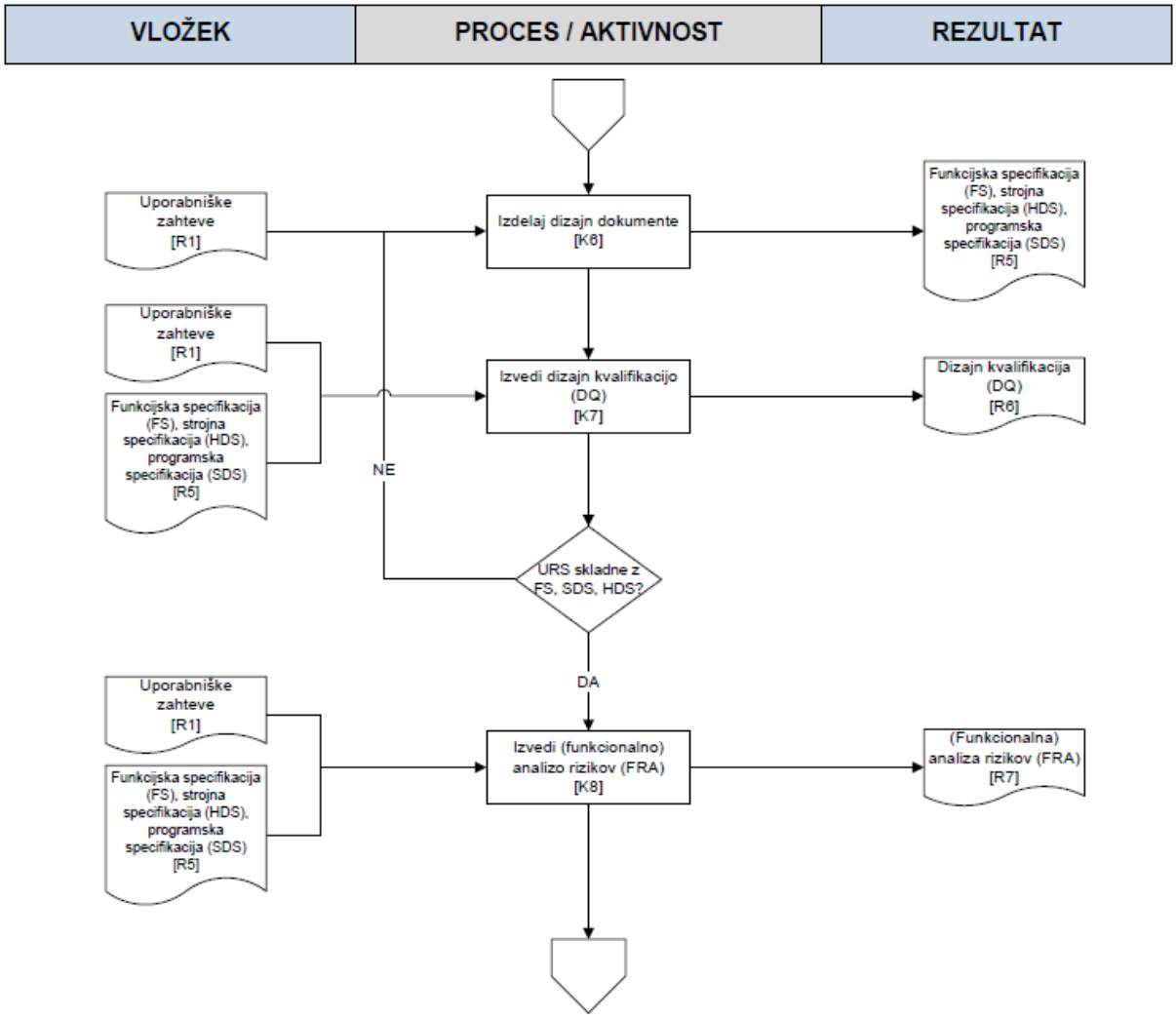
[K4] Izvedi oceno dobavitelja
Ker se URS [R1] pošljejo v našem primeru več integratorjem oz. dobaviteljem nadzornih računalniških sistemov, je potrebno pred izbiro dobavitelja izvesti presojo le-tega z namenom, da ocenimo, ali je sposoben razvijati računalniške sisteme skladno s standardi farmacevtske industrije in internimi standardi podjetja. V primeru, da se izkaže, da dobavitelj nima vzpostavljenega zadovoljivega sistema kakovosti, da bi presojo ustrezno prestal, se ga kot morebitnega integratorja računalniškega sistema izloči. Presoja se zabeleži v dokument Poročilo o oceni dobavitelja [R3]. V primeru, da smo v preteklosti (denimo zadnjih 5 let) dobavitelja oz. integratorja že presojali in je dobil ustrezno oceno, izvedba presoje ob validaciji novega računalniškega sistema/aplikacije ni potrebna. V tem primeru presojo izvedemo le, če je slednja bila izvedena pred več kot denimo 5 leti ali pa je pri dobavitelju prišlo do večjih organizacijskih sprememb.

[K5] Izdelaj plan validacije (VP)
VP [R4] je dokument, ki opisuje način in principe validacije računalniškega sistema. Osnova za izdelavo VP so URS [R1] ter HLRA [R2]. Upoštevamo tudi poročilo o oceni dobavitelja [R3]. VP na visoki ravni opisuje, katere aktivnosti se planirajo za izvedbo ustreznega validiranja računalniškega sistema, katere interne predpise oz. splošne postopke je potrebno posodobiti, katera izobraževanja je potrebno izvesti in kdo se mora izobraziti, kateri dokumenti bodo med postopkom validacije računalniškega sistema kreirani, kdo bo njihov avtor, kdo bo dokumente pregledal in kdo (katera vloga oz. funkcija v podjetju) bo dokumente potrdil.

5.3.2 Specificiranje

Ko je osnova novega računalniškega sistema definirana in sta izdelana HLRA in VP, se lotimo izdelave funkcionalnosti in specifikacij računalniškega sistema na podlagi danih URS. Slika 10 podrobneje prikazuje ključne korake za izvedbo.

Slika 10: Procesni diagram – Specificiranje



V nadaljevanju podajam podrobnejši opis posameznih korakov v procesu.

[K6] Izdelaj dizajn dokumente
URS [R1] so osnova za izdelavo FS, SDS in HDS.

Dizajn dokumentacijo izdela dobavitelj računalniškega sistema, če gre za interni razvoj, pa jo izdela podjetje samo. V našem primeru gre za nadzorno-krmilni sistem SCADA, ki ga za nas razvija zunanji dobavitelj, zato nam slednji posreduje ta sklop dokumentacije v pregled. V sklop dizajn dokumentacije je lahko tudi deloma ali v celoti vključena CS računalniškega sistema, čepav je ta lahko tudi ločen dokument s popisom konfiguracij (nastavitev) računalniškega sistema.

Dobavitelj v svojih dizajn dokumentih opiše, kako si predstavlja in razume URS, ki jih je dobil od naročnika, hkrati pa je smiselno, da navede referenco na edinstven identifikator URS, kot to prikazuje tabela 5. Le tako je na pregleden način možno zagotoviti, da bo dobavitelj izdelal računalniški sistem skladno z URS. Prikaz je podan v FS, saj pri URS v preglednici 4 govorimo o funkcionalnosti sistema.

Tabela 5: Primer FS – Funkcionalnosti sistema v dokumentu FS

FS ID	Opis funkcionalnosti	Referenca na URS
FS-xx-01	…	URS-x-01
...	...	...
FS-EP-01	Ekranski prikaz nadzornega sistema vsebuje vse standardne elemente, prikaze in vmesnike za pregled in upravljanje proizvodnega procesa s celotnim tehnološkim postopkom, s prikazanimi vsemi potrebnimi parametri, vključno s časovno značko in identifikacijo prijavljenega uporabnika.	URS-F-49 URS-F-50
FS-HI-01	Prikaz zajetih podatkov v obliki grafa (histografija) je del aplikacije iFix, ki poleg drugih funkcionalnosti omogoča tudi realnočasovni prikaz vseh definiranih parametrov.	URS-F-51
...	...	...
FS-xx-n	…	URS-x-n

Ob pregledovanju FS vsa neskladja s podanimi URS zabeležimo in celoto formaliziramo v DQ. Če ob pregledu ni ugotovljenih neskladnosti, je to kljub temu potrebno dokumentirati in formalizirati v DQ.

[K7] Izvedi kvalifikacijo načrtovanja (DQ)
V našem primeru SCADA sistema smo na tej točki prejeli v pregled dizajn dokumentacijo s strani dobavitelja, torej FS, SDS in HDS [R5]. Ker je v našem interesu, da dobimo tak računalniški sistem, kot smo ga definirali v URS [R1], je v tej fazi potreben pregled, ali dizajn dokumentacija, ki nam jo je posredoval dobavitelj, dejansko zajema vse naše zahteve iz URS. Dobavitelj bo namreč računalniški sistem izgradil natanko tako, kot je to definiral v FS, SDS in HDS. Po zaključeni primerjavi med URS in FS, SDS ter HDS odgovorni nosilci podpišejo zapisnik, ki je nastal ob pregledu in ki ga formalno imenujemo kvalifikacija načrtovanja – DQ [R6]. V primeru, da so bila v DQ ugotovljena odstopanja glede na URS, mora dobavitelj posodobiti dizajn dokumentacijo tako, da bo le-ta zajemala vse URS, ali pa uporabnik omeji svoje zahteve glede računalniškega sistema in izdela nove URS.

Pomembno je poudariti, da se na računalniških sistemih v farmacevtski industriji lahko omejijo le tiste funkcionalnosti računalniškega sistema, ki nimajo vpliva na regulatorne zahteve, nikakor pa ne moremo omejiti zahtev, ki nam jih posredno predpisujejo regulatorni organi, saj v tem primeru že v osnovi validiramo računalniški sistem, ki ni skladen s predpisano regulativo.

[K8] Izvedi (funkcionalno) analizo rizikov (FRA)
Po potrjenih FS, SDS in HDS [R5] vzamemo še URS [R1] in na podlagi te dokumentacije izdelamo FRA [R7], v kateri ocenimo vsako izmed URS glede na GxP kritičnost posamezne funkcionalnosti računalniškega sistema (v našem primeru SCADA sistema), ocenimo možna tveganja, ki se nam ob napaki ali nedelovanju vsake posamezne funkcionalnosti lahko pripetijo, ocenimo, v kakšni frekvenci lahko do teh dogodkov pride, ocenimo kritičnost teh dogodkov z vidika vpliva na kakovost izdelka, ogroženosti pacientov, varnosti pri delu ipd. ter ocenimo možnosti, da nepravilno delovanje ali napako odkrijemo. Na podlagi rezultatov ocen vsake funkcionalnosti na računalniškem sistemu se odločimo, kakšen način testiranja bomo za vsako funkcionalnost izbrali. Testi so lahko enostavni ali kompleksni, vsako odločitev pa je ob vsaki funkcionalnosti potrebno obrazložiti in pojasniti, čemu smo izbrali tak način testiranja določene funkcionalnosti računalniškega sistema.

Sledita torej vrednotenje in opis rizikov v primeru, da računalniški sistem ne bi deloval skladno z, v našem primeru, funkcionalnostmi, navedenimi v FS. Kjer so riziki visoki, v fazi verifikacije računalniškega sistema izvedemo ustrezna IQ, OQ ter PQ testiranja.

Primer analize rizikov je razviden iz preglednice 6, kjer ocenimo GxP kritičnost funkcionalnosti računalniškega sistema (DA/NE), posledice napak oz. odstopanj, možnost nastanka napake ali odstopanja ter možnost neodkritja napake oz. odstopanja (V – visok vpliv, S – srednji vpliv, N – nizek vpliv).

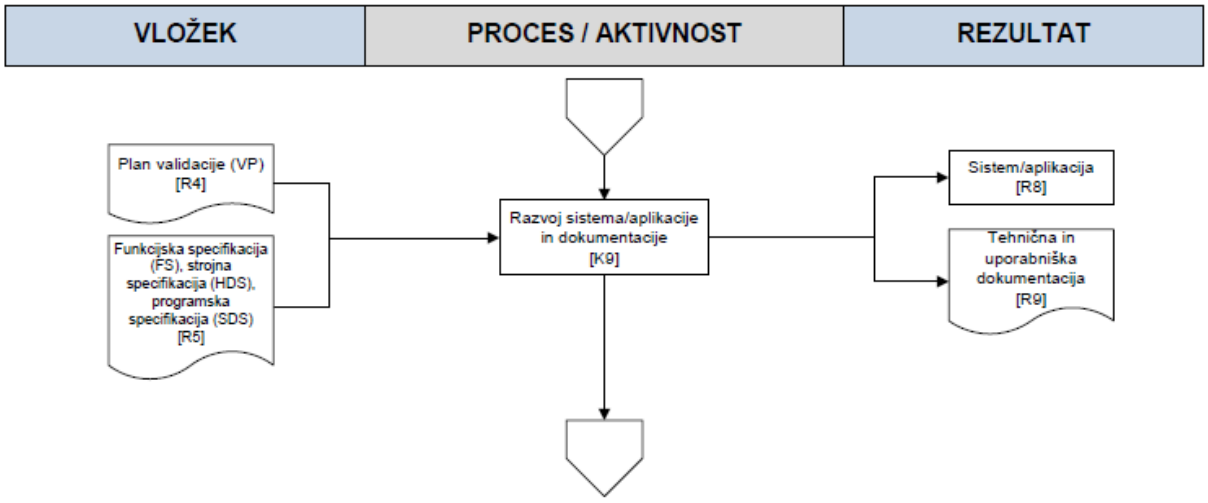
Tabela 6: Primer FRA

FS ID	Scenarij rizika/podrobnosti morebitne napake oz. odstopanja	GxP kritičnost funkcionalnosti	Vpliv/posledice napake/odstopa	Možnost nastanka napake/odstopa	Možnost neodkritja napake/odstopa	Opomba	Način testiranja
FS-EP-01	Neustrezno vodenje proizvodnega procesa; neustrezen izdelek.	DA	V	N	N	/	OQ test
FS-HI-01	Ni procesnih podatkov za pregled; ni možnosti pregledovanja procesnih podatkov; neskladnost z regulativami; raziskava odstopanj od dobre proizvodne prakse ni možna; izdelek ne more na trg.	DA	V	N	N	/	OQ test

5.3.3 Izgradnja/razvoj

Slika 11 prikazuje vložke, potrebne za izgradnjo računalniškega sistema, prav tako pa rezultat, ki sledi – razvit računalniški sistem ter pripadajoča tehnična in uporabniška dokumentacija.

Slika 11: Procesni diagram – Izgradnja/razvoj



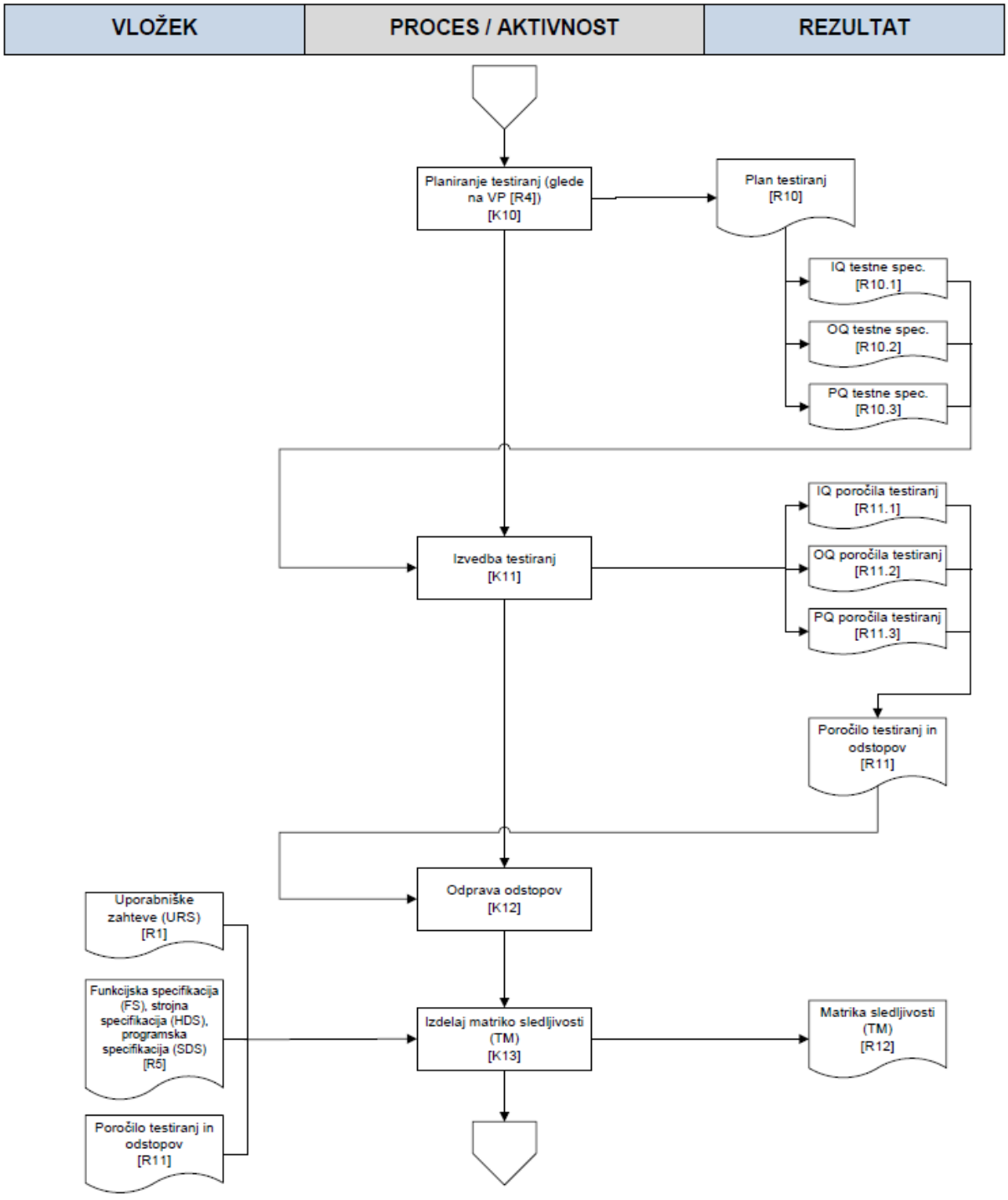
V nadaljevanju podajam podrobnejši opis posameznih korakov v procesu.

[K9] Razvoj sistema/aplikacije in dokumentacije
V tej fazi začnemo z izgradnjo računalniškega sistema (v našem primeru SCADA sistema). Pri razvoju je potrebno upoštevati osnovne principe razvoja, definirane v VP [R4], glavno dokumentacijo za razvoj pa predstavljajo FS, SDS in HDS [R5]. Rezultat je računalniški sistem, skladen z URS, prav tako pa je v našem primeru dobavitelj dolžan izdelati tudi tehnično in uporabniško dokumentacijo [R9], s katero se pred uporabo računalniškega sistema morajo vsi uporabniki seznaniti in ustrezno izobraziti.

5.3.4 Verifikacija

V sklopu verifikacije preverimo, ali računalniški sistem deluje skladno s pričakovanji uporabnika. Kot je razvidno s Slike 12, to preverimo z IQ, OQ in PQ testi.

Slika 12: Procesni diagram – Verifikacija



V nadaljevanju podajam podrobnejši opis posameznih korakov v procesu.

[K10] Planiranje testiranj (glede na VP [R4])
Ko imamo računalniški sistem razvit (v našem primeru je to SCADA sistem), mora prestati še testiranja, s katerimi dokazujemo, da računalniški sistem deluje brezhibno in skladno s specifikacijami. Obseg in metodologijo validacije računalniškega sistema predpisuje VP, plan testiranj [R10] pa podrobneje opisuje, katere IQ, OQ in PQ teste je potrebno na računalniškem sistemu izvesti. Ko imamo izdelan in odobren plan testiranj, napišemo IQ [R10.1], OQ [R10.2] in PQ [R10.3] testne specifikacije, kjer se definira, kaj testiramo, kako izvedemo testiranje ter kakšen je pričakovani rezultat.

[K11] Izvedba testiranj

Teste izvajamo skladno s planom testiranj [R10] na predodobrene testne specifikacije IQ [R10.1], OQ [R10.2] in PQ [R10.3], ki so osnovane na podlagi rezultatov iz FRA. Namestitev oz. inštalacijo računalniškega sistema testiramo z: IQ testom, ki je dokumumentirana verifikacija, da je računalnški sistem nameščen skladno s predodobrenimi specifikacijami (International Society for Pharmaceutical Engineering – ISPE, 2008, str. 209; International Society for Pharmaceutical Engineering - ISPE, 2014a); OQ testom, ki je dokumentirana verifikacija, da računalniški sistem deluje skladno s predodobrenimi specifikacijami v vseh navedenih območjih delovanja (International Society for Pharmaceutical Engineering - ISPE, 2008, str. 334; International Society for Pharmaceutical Engineering - ISPE, 2014b); in PQ testom, ki je dokumentirana verifikacija, da je sistem sposoben delovati in/ali kontrolirati (v našem primeru proizvodne) procese med delovanjem v produkcijskem okolju skladno s predodobrenimi specifikacijami (International Society for Pharmaceutical Engineering – ISPE, 2008, str. 284; International Society for Pharmaceutical Engineering - ISPE, 2014c). Izpolnjene testne specifikacije, ki jih dobimo po izvedenih testiranjih, se imenujejo poročila o testiranjih. Tako dobimo tri sklope – IQ testna poročila [R11.1], OQ testna poročila [R11.2] in PQ testna poročila [R11.3]. V primerih, kjer se je med testiranjem v testnih korakih pojavila napaka in testiranje ni bilo uspešno ali je bilo uspešno le delno, se to dokumentira kot odstopanje. Tako odstopi kot tudi ustrezna poročila o testiranjih so popisana v neke vrste zbirniku testov, ki ga imenujmo Poročilo testiranj in odstopov [R11].

Če si ogledamo nadaljevanje našega primera, je iz preglednice 6 razvidno, da je obe funkcionalnosti računalniškega sistema potrebno testirati z OQ testom. Sama testna specifikacija mora biti pred začetkom izvajanja testa odobrena, testne korake se po odobritvi testne specifikacije izvaja na kopiji odobrene testne specifikacije. Pričakovani rezultat, ustreznost in datum ter podpis se beležijo ročno v za to predvidena polja sočasno ob izvedbi testa. V našem primeru sem tekst, ki se ga vnaša ročno, v preglednici 7 obarval z modro barvo.

V preglednici 7 navajam primer OQ testne specifikacije obravnavanega primera. Slika 13 prikazuje, kako je v našem primeru videti priloga (dokazilo) testnega koraka 1 testne specifikacije OQ-2_test parametrov in zgodovine.

Tabela 7: Primer OQ testa

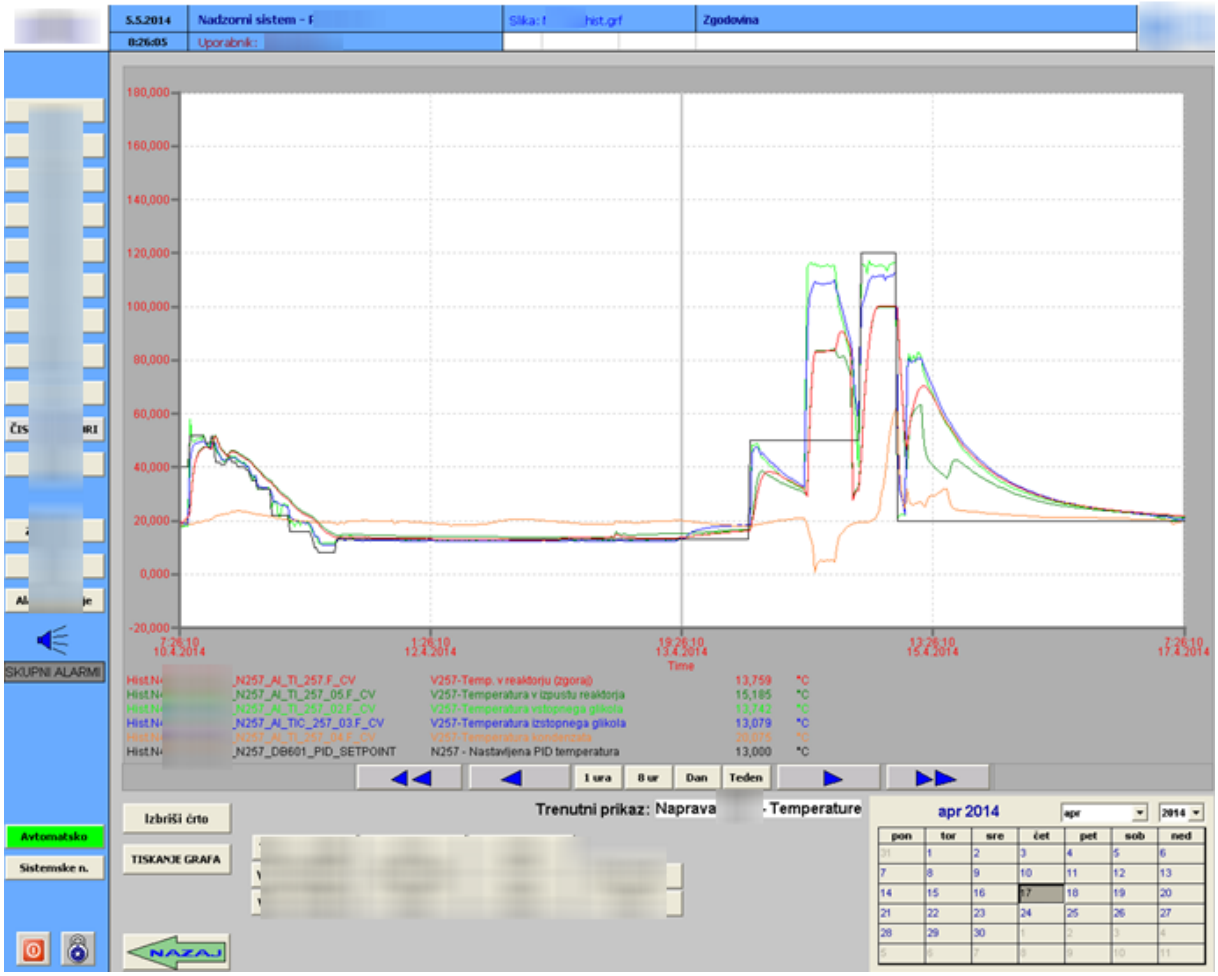
Ime testa: OQ-1_test ekranskega prikaza				**Predpogoj za izvedbo:** Odobrena FS in FRA			
Korak	**Ref. URS**	**Ref. FS**	**Opis testa za izvedbo**	**Pričakovani rezultat**	**Dejanski rezultat, referenca na prilogo**	**Ustreza?**	**Datum in podpis**
1	URS-F-49 URS-F-50	FS-EP-01	Zaženi in se prijavi v aplikacijo iFix. Preveri, ali je na zaslonu nadzornega sistema prikazan celoten proizv. proces, vključno s procesnimi vrednostmi, datumom in uro ter prijavljenim uporabnikom.	Na zaslonu je razviden celotni proizvodni proces, vključno s procesnimi vrednostmi, datumom in uro ter prijavljenim uporabnikom.	Skladen s pričakovanim.	DA	30.04.2014 *Janez Novak*

se nadaljuje

nadaljevanje

Ime testa: OQ-2_test parametrov in zgodovine				**Predpogoj za izvedbo:** Odobrena FS in FRA			
1	URS-F-51	FS-HI-01	V iFix odpri »zgodovino«. Preveri, ali nadzorni sistem realnočasovno beleži vse procesne parametre v graf.	Nadzorni sistem beleži vse procesne parametre v graf.	Skladen s pričakovanim. Priloga 1	DA	30.04.2014 *Janez Novak*
2	URS-F-51	FS-HI-01	V iFix odpri »zgodovino«. Preveri, ali ima graf na osi x čas in vrednosti parametrov na osi y.	Graf prikazuje vrednosti parametrov na osi y, čas na osi x.	Skladen s pričakovanim.	DA	30.04.2014 *Janez Novak*

Slika 13: Prikaz histografije SCADA sistema – Priloga 1 testa OQ-2_Test parametrov in zgodovine



[K12] Odprava odstopov

V primeru, da imamo po izvedenih testiranjih računališkega sistema v poročilu testiranj [R11] evidentirane odstope, moramo le-te odpraviti. Način odprave odstopanj je odvisen od same napake oz. odstopa na sistemu. Morebiti je potrebno v teh primerih popraviti tudi sam dizajn računalniškega sistema. Odstop je uspešno odpravljen, ko je ponovni test, v katerem je prišlo do odstopa, uspešno zaključen.

[K13] Izdelaj matriko sledljivosti (TM)

Kar smo od dobavitelja računalniškega sistema zahtevali v URS [R1] in to, kar smo dejansko dobili, je v FS, SDS in HDS [R5], morebitna odstopanja pa smo prav tako

pregledali in to dokumentirali v DQ [R6]. Vendar to ni dovolj. Zagotoviti je namreč potrebno še sledljivost, kjer je na pregleden način razvidno, ali so vse URS popisane v dizajn dokumentih (to preverimo že v DQ) ter v katerih testih (IQ, OQ, PQ) smo te zahteve testirali. Za začetek izdelave TM [R12] torej ni potrebno čakati na verifikacijo računalniškega sistema, temveč jo lahko začnemo sproti izdelovati že prej (med kvalifikacijo načrtovanja – DQ). S tem zagotovimo prvi del sledljivosti, in sicer med URS ter FS, SDS in HDS). Drugi del pa zagotovimo po IQ, OQ in PQ testiranjih, kjer dizajn dokumentacijo povežemo s testnimi poročili. Kot že omenjeno, vsako uporabniško zahtevo označimo z edinstvenim identifikatorjem, da potem lahko zagotavljamo sledljivost dizajn dokumentov in testov. Če ugotovimo, da smo izpustili testiranje katere izmed funkcionalnosti računalniškega sistema, je to potrebno dokumentirati in retrospektivno izvesti testiranje.

Ko s testiranji končamo, lahko v celoti sestavimo TM, s katero preverimo in zagotavljamo, da so vse v URS zahtevane funkcionalnosti s strani dobavitelja bile ustrezno upoštevane in testirane skladno z rezultati FRA. TM za naš primer je prikazana v preglednici 8.

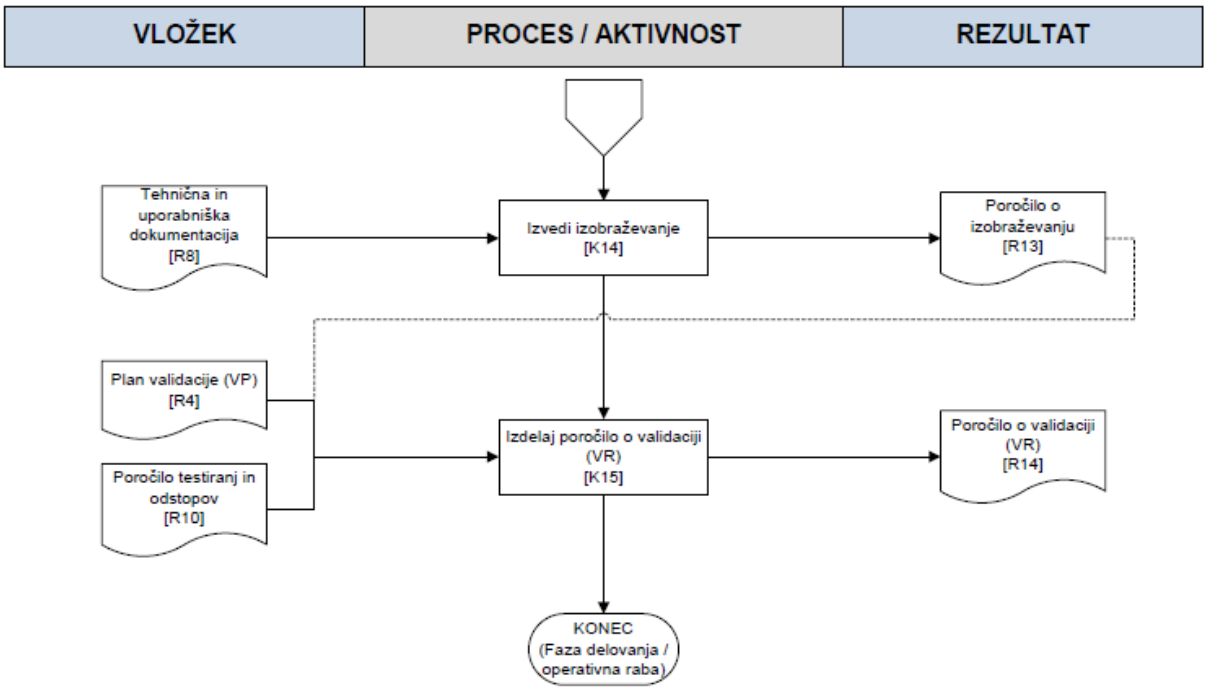
Tabela 8: Primer TM

URS	FS	SDS	HDS	IQ	OQ	PQ	Komentar
URS-F-49	FS-EP-01	/	/	/	OQ-1_test ekranskega prikaza – korak 1	/	Ustreza
URS-F-50	FS-EP-01	/	/	/	OQ-1_test ekranskega prikaza – korak 1	/	Ustreza
URS-F-51	FS-HI-01	/	/	/	OQ-2_test parametrov in zgodovine – korak 1, 2	/	Ustreza

5.3.5 Poročilo

Slika 14 prikazuje zadnje aktivnosti, ki so potrebne pred sprostitvijo računalniškega sistema v produkcijsko in operativno rabo.

Slika 14: Procesni diagram – Poročilo



V nadaljevanju podajam podrobnejši opis posameznih korakov v procesu.

[K14] Izvedi izobraževanja
Preden gre sistem v produkcijo in operativno rabo, je potrebno poskrbeti, da so vsi (bodoči) uporabniki računalniškega sistema izobraženi o tehnični in uporabniški dokumentaciji računalniškega sistema. Prav tako je uporabnike potrebno izobraziti o navodilih oz. postopkih podjetja, ki opisujejo proces in potek dela, ki opisujejo proces in potek dela in jih računalniški sistem krmili. Izobraževanje uporabnikov se dokumentira v poročilo o izobraževanju [R13], kot priloga poročilu je lahko priložen tudi test preverjanja.

[K15] Izdelaj poročilo o validaciji (VR)
Ko so vse aktivnosti, predvidene v VP [R4], ustrezno zaključene, to popišemo v VR [R14]. Potrjen VR pomeni, da je računalniški sistem (v našem primeru SCADA sistem) uspešno validiran in lahko gre v redno operativno rabo brez omejitev. Zadnji datum odobritve na VR pomeni datum validacije računalniškega sistema.

5.4 Izobraževanja

Preden gre računalniški sistem v produkcijsko rabo, morajo biti zaposleni, ki bodo s sistemom delali, izobraženi o zadnjih veljavnih splošnih postopkih in navodilih za delo. Navodila za delo s sistemom lahko zahtevamo od dobavitelja, ki nam je sistem razvijal. V tem primeru zahtevamo tudi, da dobavitelj izobrazi zaposlene ali vsaj ključne osebe (na primer vodje obrata), ki nato prenesejo svoje znanje naprej do svojih sodelavcev. Celoten proces mora biti dokumentiran skladno z dobro dokumentacijsko prakso.

V primeru funkcionalnih sprememb na sistemu, ki vplivajo na splošne postopke in/ali navodila za delo, je potrebno pred formalno zaključitvijo te spremembe ustrezno posodobiti ter izobraziti vse uporabnike sistema. Brez te aktivnosti sistema ne smemo spustiti v produkcijsko rabo.

5.5 Operativna raba sistema

V operativno fazo sistema oz. v fazo delovanja sistem stopi, ko je tudi formalno zaključen in odobren VR s strani odgovorne osebe upravljanja kakovosti. Da zagotavljamo validiranost računalniškega sistema v tej fazi, moramo zagotoviti stalni nadzor nad sistemom, kar zajema zaščito in administracijo sistema, obvladovanje varnostnega kopiranja in restavriranja, obvladovanje arhiviranja zapisov, obvladovanje sprememb, obvladovanje incidentov in GxP odstopov, obvladovanje konfiguracij, zagotavljanje ažurnosti podatkov o računalniškem sistemu v evidenci oz. na seznamu računalniških sistemov ter periodično pregledovanje računalniškega sistema.

5.6 Upokojitev sistema

Glede na obseg podatkov, ki jih računalniški sistem generira skozi svoje življenjsko obdobje oz. fazo delovanja, je lahko upokojitev računalniškega sistema zahtevna naloga. Zato je potrebno vzpostaviti ustrezne postopke za izvedbo upokojitve računalniškega sistema, ki jih mora predhodno odobriti odgovorna oseba za upravljanje kakovosti, izluščiti, katero dokumentacijo o sistemu je potrebno hraniti, izluščiti, kateri elektronski zapisi v sistemu so GxP relevantni in se morajo hraniti in za kakšno obdobje (lahko pa podatke migriramo na nov sistem), vzpostaviti nadzorovan dostop do arhiva in zagotoviti, da vsi podatki v času hrambe ostanejo dostopni in v berljivi obliki.

5.7 Retrospektivna in ponovna validacija sistema

V osnovi je potrebno ločiti retrospektivno validacijo in ponovno validacijo oz. revalidacijo računalniškega sistema.

Retrospektivne validacije sistema se poslužujemo v primerih, ko imamo starejše računalniške sisteme, vmes pa so se spremenile regulatorne zahteve; to je le eden od primerov. Pri retrospektivni validaciji običajno govorimo o starejših (t. i. Legacy) sistemih, ki imajo določen nivo validacijske dokumentacije, vendar ne zadostijo trenutnim regulativnim standardom. Taki sistemi so denimo tudi računalniški sistemi, ki so podpirali ne-GxP procese, sedaj pa bi jih radi uporabljali tudi za GxP relevantne procese (Comes compliance services, 2013, str. 1). Zato je pomembno, da se retrospektivne validacije lotevamo sistematično in s pravo mero razuma, obseg aktivnosti, ki si jih predpišemo, pa ovrednotimo in pojasnimo v izvedeni analizi rizikov.

Lucas (2004, str. 33) navaja kot aktivnosti retrospektivne validacije pregled zgodovine delovanja in dokumentacije, ki služi ugotavljanju vrzeli na računalniškem sistemu, izdelava VP, kjer definiramo pristop k validacijskim aktivnostim, izdelava URS, v katerih popišemo trenutno funkcionalnost sistema, izdelava FS, SDS, HDS (na podlagi URS), testiranje računalniškega sistema, obseg testiranj določimo na podlagi FRA, VR, v katerem povzamemo ključne korake validacije (osnovo nam predstavlja VP) ter operativna raba računalniškega sistema v produkcijskem okolju, kjer ohranjamo validirano stanje računalniškega sistema.

K tem točkam bi sam dodal še popis konfiguracije računalniškega sistema, če le-ta ni že vključena v samo dizajn dokumentacijo. Računalniški sistem je potrebno potestirati glede na to, kako je konfiguriran. CS nam v tem primeru služi tudi kot nujni dokument ob restavriranju računalniškega sistema in testiranju le-tega. Dodal pa bi tudi pregled obstoječih navodil za delo, jih po potrebi ažuriral in izobrazil vse uporabnike sistema.

Revalidacije sistemov se lotevamo v primerih, ko denimo ob periodičnem pregledu računalniškega sistema odkrijemo vrzeli v delovanju sistema in/ali validacijski dokumentaciji. Mnogokrat pride do teh vrzeli zaradi nezagotavljanja ažurnosti dokumentacije življenjskega cikla, kar posledično pomeni, da URS in dizajn dokumenti ne opisujejo računalniškega sistema v stanju, v kakršnem ta dejansko je z vidika delovanja in funkcionalnosti. Prav tako ne zadostimo regulatornim zahtevam z vidika zagotavljanja sledljivosti med funkcionalnostmi in izvedenimi testiranji na sistemu.

SKLEP

Zaradi vse kompleksnejših računalniških sistemov se počasi, a vztrajno zbujajo tudi regulatorni organi, ki so iz generacije v generacijo bolj izkušeni in sposobni obvladovati še tako kompleksne računalniške sisteme. To pa je tudi razlog, zakaj so v zadnjem času računalniški sistemi v farmacevtski industriji pravi hit.

Med vrstami inšpektorjev je vedno več takih, ki so odraščali z računalniki in zabavno elektroniko, svoje znanje pa nadgradili še z dodatnim zanimanjem in formalnim izobraževanjem v stroki. V zadnjih treh letih je prišlo do večjih premikov na področju računalniških sistemov in glede na trende, ki se kažejo predvsem na področju zagotavljanja integritete podatkov, bo teh premikov v prihodnosti še veliko več. Računalniški sistemi postajajo vse kompleksnejši, na voljo je množica novih tehnologij, ki jih lahko uporabimo, zato regulatorni organi ne počivajo in prav v tem trenutku razmišljajo, kako bolje obvladovati računalniške sisteme in ohranjati integriteto podatkov skozi regulatorne predpise.

Pomembno je, da se vsi dobavitelji in integratorji računalniških sistemov, ki sodelujejo s farmacevtskimi združbami na nivoju GxP relevantnih računalniških sistemov, zavedajo, da množica predpisov posledično velja tudi zanje in da morajo biti sposobni dokazovati, da delujejo skladno z regulatornimi zahtevami, dodatno pa tudi s predpisi in internimi standardi farmacevtske združbe, s katero sodelujejo. Farmacevtske združbe so namreč dolžne izvajati presoje dobaviteljev in integratorjev, s katerimi sodelujejo, in te presoje na področju računalniških sistemov postajajo vse strožje, sodelovanje med združbama se tako lahko hitro znajde na negotovih tleh.

Upam, da bo pričujoče magistrsko delo pripomoglo k razumevanju regulatornih zahtev in nenazadnje tudi k postavitvi modela sistema kakovosti na področju računalniških sistemov v farmacevtski industriji. Konec koncev računalniških sistemov ne validiramo zato, da bi prestali inšpekcije, temveč v prvi vrsti zato, da v celoti zagotovimo integriteto podatkov in posledično varna zdravila za vse nas. Lahko vzpostavimo odličen sistem kakovosti, vendar je od zaposlenih in kulture odvisno, v kolikšni meri bo sistem dejansko deloval.

LITERATURA IN VIRI

1. Ade, D. (2008). Software Validation Goes a Long Way. Najdeno 24. novembra 2013 na spletnem naslovu http://www.pharmaasia.com/article/software-validation-goes-a-long-way/7044

2. Ali, H., Gonjare, N., & D'souza, M. (2012). Change Management in Pharmaceuticals: The most critical element of Quality Management System. *Journal of Pharmacy Research, 5*(7), 3706–3708.

3. Biometrix. (2008). Biometrix History of Validation. Najdeno 24. decembra 2013 na spletnem naslovu http://www.scribd.com/doc/3437628/History-of-Validation

4. Budihandojo, R., Coates, S., Huber, L., Matos, J. E., Schmitt, S., Stokes, D. et al. (2007). A perspective on Computer Validation. *Pharmaceutical Technology, 31*(7), 86–93

5. Comes compliance services. (2013). The mysteries of retrospective computer system validation. Najdeno 19. oktobra 2013 na spletnem naslovu http://ccs-innovation.com/wordpress/wp-content/uploads/2013/09/CCS_-Retrospective-Computer-System-Validation_-2013_rev0.pdf

6. Culin, R. V. (2011). New Approach to System Validation. *Applied Clinical Trials, 20*(2), 32–37

7. EduQuest. (2011). *Comparison of FDA's Part 11 and the EU's Annex 11*. Hyattstown, MD: EduQuest Inc.

8. European Commission (2013b). *EU Legislation – Eudralex.* Najdeno 25. decembra 2013 na spletnem naslovu http://ec.europa.eu/health/documents/eudralex/index_en.htm

9. European Commission. (2003). *2003/94/EC* – Laying down the principles and guidelines of good manufacturing practice in respect of medicinal products for human use and investigational medicinal products for human use. Najdeno 25. decembra 2013 na spletnem naslovu http://ec.europa.eu/health/files/eudralex/vol-1/dir_2003_94/dir_2003_94_en.pdf

10. European Commission. (2011a). EudraLex – Volume 4 Good Manufacturing Practice Medicinal Products for Human and Veterinary Use, Chapter 4: Documentation. Najdeno 25. decembra 2013 na spletnem naslovu http://ec.europa.eu/health/files/eudralex/vol-4/chapter4_01-2011_en.pdf

11. European Commission. (2011b). EudraLex – Volume 4 Good Manufacturing Practice Medicinal Products for Human and Veterinary Use, Annex 11: Computerized Systems. Najdeno 25. decembra 2013 na spletnem naslovu http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf

12. European Commission. (2013a). EudraLex – Volume 4 Good manufacturing practice (GMP) Guidelines. Najdeno 25. decembra 2013 na spletnem naslovu http://ec.europa.eu/health/documents/eudralex/vol-4/

13. European Compliance Academy (2011a). *Introduction & Welcome. ECA Education Course – Computer Validation The GAMP5 Approach*. Vienna, Austria: Concept Heidelberg GmbH

14. European Compliance Academy (2011b). *Laws, Regulations and Guidelines for Computer and Control Systems. ECA Education Course – Computer Validation The GAMP5 Approach*. Vienna, Austria: Concept Heidelberg GmbH

15. European Compliance Academy (2011c). *The GAMP5 Approach to Computer Systems Validation. ECA Education Course – Computer Validation The GAMP5 Approach*. Vienna, Austria: Concept Heidelberg GmbH

16. European Compliance Academy (2011d). *Supplier Assessment. ECA Education Course – Computer Validation The GAMP5 Approach*. Vienna, Austria: Concept Heidelberg GmbH

17. European Compliance Academy (2011e). *Introduction to Requirements. ECA Education Course – Computer Validation The GAMP5 Approach*. Vienna, Austria: Concept Heidelberg GmbH

18. European Compliance Academy (2011f). *Validation Planning. ECA Education Course – Computer Validation The GAMP5 Approach*. Concept Heidelberg GmbH

19. European Compliance Academy (2011g). *Specifications, Design Review & Traceability. ECA Education Course – Computer Validation The GAMP5 Approach*. Vienna, Austria: Concept Heidelberg GmbH

20. Huber, L. (2012). Computer System Validation – Tutorial. Najdeno 18. januarja 2014 na spletnem naslovu http://www.labcompliance.com/tutorial/csv/

21. Industrieanlagen-Betriebsgesellschaft - IABG. (2006a) . *Willkommen auf den V-Modell-Seiten der IABG*. Najdeno 18. januarja 2014 na spletnem naslovu http://v-modell.iabg.de/index.php?option=com_content&task=view&id=10&Itemid=1

22. Industrieanlagen-Betriebsgesellschaft - IABG. (2006b). *Part 1: Fundamentals of the V-Modell, V-Modell XT, version 1.3*. Najdeno 18. januarja 2014 na spletnem naslovu http://v-modell.iabg.de/v-modell-xt-html-english/index.html

23. International Society for Pharmaceutical Engineering - ISPE. (2008). *GAMP 5: A Risk-based Approach to Compliant Gxp Computerized Systems*. Tampa, Florida: International Society for Pharmaceutical Engineering

24. International Society for Pharmaceutical Engineering - ISPE. (2014a). *ISPE Glossary of Pharmaceutical and Biotechnology Terminology*. Najdeno 26. aprila 2014 na spletnem naslovu http://www.ispe.org/glossary?term=Installation+Qualification+%28IQ%29

25. International Society for Pharmaceutical Engineering - ISPE. (2014b). *ISPE Glossary of Pharmaceutical and Biotechnology Terminology*. Najdeno 26. aprila 2014 na spletnem naslovu http://www.ispe.org/glossary?term=Operational+Qualification+%28OQ%29

26. International Society for Pharmaceutical Engineering - ISPE. (2014c). *ISPE Glossary of Pharmaceutical and Biotechnology Terminology*. Najdeno 26. aprila 2014 na spletnem naslovu http://www.ispe.org/glossary?term=Performance+Qualification+%28PQ%29

27. International Society for Pharmaceutical Engineering - ISPE. (2010). *A Risk-Based Approach to Operation of GxP Computerized Systems, A Companion Volume to GAMP 5*. Tampa, Florida: International Society for Pharmaceutical Engineering

28. Joshi, A. S. (2005). Prepare your computer system for inspection. *BioPharm International*, *18*(2), 18–27,64,71

29. Lopez, O. (2012). *For Life Science Professionals, Annex 11 and 21 CFR Part 11: Comparisons for International Compliance*. Najdeno 25. januarja 2014 na spletnem naslovu http://www.mastercontrol.com/newsletter/annex-11-21-cfr-part-11-comparison.html

30. Lucas, I. (2004). *Legacy Systems Validation-Managing the Unwanted Gift. Special Edition: Computer Validation VI.* Duluth, MN: Institute of Validation Technology, 29–39

31. McDowall, R. D. (2009). Automated systems and regulated environments. Najdeno 23. decembra 2013 na spletnem naslovu http://www.labautopedia.org/mw/index.php?title=Automated_systems_and_regulated_environments

32. McDowall, R. D. (2010). Understanding and interpreting the GAMP5 life cycle models for software. *Spectroscopy*, *25*(4), 22–31

33. McDowall, R. D. (2011a). Periodic Reviews of Computerized Systems, Part I. *Spectroscopy*, *26*(9), 28–38

34. McDowall, R. D. (2011b). Periodic Reviews of Computerized Systems, Part II. *Spectroscopy*, *26*(11), 20–29

35. MetricStream (2014). Systems Validation for 21CFR Part 11 Compliance. Najdeno 21. maja 2014 na spletnem naslovu http://www.metricstream.com/insights/sys_validation.htm

36. Pharmacists Pharma Journal (2010). Validation in Pharmaceutical Insdustry Types of Pharma Validation. *Pharmacists Pharma Journal*. Najdeno 5. maja na spletnem naslovu http://www.pharmacistspharmajournal.org/2010/03/validation-in-pharmaceutical.html#.U2dNoKJrVLN

37. PIC/S (2007). Pharmaceutical Inspection Co-Operation Scheme Guidance – Good Practices For Computerised Systems In Regulated Gxp Environments. Najdeno 23. decembra 2013 na spletnem naslovu http://www.picscheme.org/pdf/27_pi-011-3-recommendation-on-computerised-systems.pdf

38. Project Management Institute - PMI. (2013). *A Guide To The Project Management Body Of Knowledge (PMBOK Guide) 5th edition*. Project Management Insitute

39. Ranbaxy Laboratories Limited (2014). *Data Integrity*. Najdeno 21. maja 2014 na spletnem naslovu http://www.slideshare.net/skvemula/presentation-on-data-integrity-in-pharmaceutical-industry#

40. Rao, K. N., & Sastri, A. P. (2011). Overcoming Testing Challenges in Project Life Cycle using Risk Based Validation Approach. *International Journal on Computer Science & Engineering*, *3*(3), 1232–1239

41. Remén, J. (2005). *Lifecycle approach to Computer Systems Validation. Computer Systems and Software Validation – Proceedings Book*. Duluth, MN: Institute of Validation Technology

42. Riganati, D. (2012). What is a computerized system? Najdeno 23. decembra 2013 na spletnem naslovu https://www.ibm.com/developerworks/community/blogs/obidan/entry/what_is_a_computerized_system?lang=en

43. Roemer, M., & Lopez, O. (2011). Annex 11. *Pharmaceutical Technology Europe*, *23*(6), 42.

44. Royce, W. W. (1970). *Managing the development of large software systems: concepts and techniques*. Los Angeles: Proc. IEEE WESTCON, 1–9

45. Schousboe, M. (2005). Computer Validation Master Planning "Validation Strategies". *Pharmaceutical Technology*, 20–30.

46. Silva, E. J. (2013). Computer System Validation. Najdeno 23. decembra 2013 na spletnem naslovu http://www.slideshare.net/ericjsilva/computer-system-validation-17173238#

47. Stein, T. R. (2006). The Computer System Risk Management and Validation Life Cycle. Chico, CA: Paton Press

48. Tedstone, B. (2012). Computer Systems Validation. *Computer Systems Validation and Quality Assurance blog*. Najdeno 27. aprila 2014 na spletnem naslovu http://computersystemsvalidation.blogspot.com/2012/11/GAMP-Software-Category.html

49. U.S. Food and Drug Administration - FDA (2002). *General Principles of SoftwareValidation; Final Guidance for Industry and FDA Staff. U.S. Department Of Health and Human Services Food and Drug Administration*. Najdeno 24. novembra 2013 na spletnem naslovu http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf

50. U.S. Food and Drug Administration - FDA (2003). *Guidance for Industry Part 11, Electronic Records; Electronic signatures – Scope and Application. U.S. Department of Health and Human Services*. Najdeno 19. oktobra 2013 na spletnem naslovu http://www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm125125.pdf

51. U.S. Food and Drug Administration – FDA (2004). *Pharmaceutical cGMP's for The 21St Century, A Risk Based Approach, Final Report. U.S. Department Of Health and*

Human Services Food and Drug Administration. Najdeno 24. novembra 2013 na spletnem naslovu http://www.fda.gov/downloads/Drugs/DevelopmentApprovalProcess/Manufacturing/QuestionsandAnswersonCurrentGoodManufacturingPracticescGMPforDrugs/UCM176374.pdf

52. U.S. Food and Drug Administration - FDA (2006). G*uidance for Industry, Quality Systems Approach to Pharmaceutical CGMP Regulations*. Najdeno 1. februarja 2014 na spletnem naslovu http://www.fda.gov/downloads/Drugs/.../Guidances/UCM070337.pdf

53. U.S. Food and Drug Administration - FDA (2013a). *CFR – Code of Federal Regulations Title 21, Volume 4 – Part 211 Current Good Manufacturing Practice for Finished Pharmaceuticals*. Najdeno 26. decembra 2013 na spletnem naslovu http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?cfrpart=211

54. U.S. Food and Drug Administration – FDA (2013b). *CFR – Code of Federal Regulations Title 21, Volume 4 – Part 11 Electronic Records; Electronic Signatures*. Najdeno 26. decembra 2013 na spletnem naslovu http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?cfrpart=11

55. Velkovrh Remec, B. (2007). Validacije v farmacevtski industriji. Najdeno 1. novembra 2013 na spletnem naslovu http://www.scribd.com/doc/23022819/VALIDACIJE

56. Woods, P., & Beale, D. (2009). The benefits of risk-based analyses during system validation. *Pharmaceutical Technology Europe, 21*(9), 54–58