Uloga računarstva u farmaceutskoj industriji i validacija računalnih sustava prema 21 CFR Part 11 normi

Lončar, Matej

Master's thesis / Diplomski rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:908060

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

zir.nsk.hr

Image not found or type unknown

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

ULOGA RAČUNARSTVA U FARMACEUTSKOJ INDUSTRIJI I VALIDACIJA RAČUNALNIH SUSTAVA PREMA 21 CFR PART 11 NORMI

Diplomski rad

Matej Lončar

Osijek, 2016. godina.

SADRŽAJ

1 UVOD 2
1.1 Zadatak diplomskog rada 3
2 RAČUNALNI SUSTAV 4
2.1 Informacijski sustav 5
2.2 Laboratorijski sustav 6
2.3 Procesni sustav 8
2.4 Što nije računalni sustav 9
3 VALIDACIJA RAČUNALNOG SUSTAVA 10
3.1 Odgovornosti 10
3.2 Zašto je potrebno validirati računalni sustav? 11
3.3 Kada je potrebno validirati računalni sustav? 11
3.4 Kako validirati računalni sustav? 12
3.5 Kako odrediti opseg validacije? 12
3.6 Validacijska dokumentacija 17
3.7 Održavanje sustava u validiranom stanju 20
3.8 Validacija prema 21 CFR part 11 normi 21
4 ZAKLJUČAK 25
LITERATURA 26
SAŽETAK 27
ABSTRACT 28
ŽIVOTOPIS 29
PRILOG 30

1 UVOD

Kako navodi IBM, poznata američka tvrtka u razvoju računarstva i informacijskih tehnologija, u jednom od svojih članaka, u današnje vrijeme razvoj modernih lijekova praktički je nemoguć bez moderne IT tehnologije. IT sustavi prate sve procese tijekom cjelokupnog životnog vijeka lijeka, od njegovog istraživanja, registracije, proizvodnje pa sve do njegovog plasiranja na tržište i same prodaje, stoga imaju važnu ulogu u farmaceutskoj industriji.

Pravila koja vrijede za IT sustave i pohranjene podatke mijenjala su se tijekom godina. U zadnje vrijeme sve se veća pozornost posvećuje sigurnosti tih podatka. Tako je Američka agencija za hranu i lijekove (Food and Drug Administration - FDA) u kolovozu 1997. izdala prve naputke vezane za elektroničke sustave i podatke u farmaceutskoj industriji, 21 CFR Part 11, u kojima su opisana pravila vezana uz elektroničke zapise i elektronički potpis. Pravila se odnose na računalne sustave koji izrađuju, mijenjaju, održavaju, pohranjuju, pretražuju ili prenose podatke u elektroničkom obliku, a njihovom primjenom minimalizira se mogućnost lažiranja podataka. Time se štite lijekovi i medicinski proizvodi, a u konačnici i pacijenati.

Pravila naputaka 21 CFR Part 11 proširena su u lipnju 2011. kada u primjenu ulazi i Annex 11: računalni sustavi – Annex 11: Computerized Systems [1], koji je dodao mnoga poglavlja koja se odnose na same računalne sustave, sigurnost, backup podataka te na sustave za oporavak nakon havarije. Annex 11 također stavlja više odgovornosti na pojedince koji su zaduženi za poslovne procese i održavanje sustava. To je učinjeno kako bi se i menadžment uključio u praćenje usklađenosti kritičnih sustava, kao i u preuzimanje odgovornosti čime je dodatno stavljen naglasak na izuzetnu važnost informatičke podrške i IT sustava u farmaceutskoj industriji. [2]

Kroz daljnja poglavlja pobliže su opisani računalni sustavi, kao i njihovi podsustavi: što su, od čega se sastoje i koja je njihova uloga u samom sustavu. Također je opisan sam proces validacije, navedene su odgovornosti, zašto, kada i kako validirati, kako odrediti opseg validacije i kako sustav održavati u validiranom stanju. U praktičnom dijelu rada, kao primjer validacije računalnog sustava, izvršena je kvalifikacija sustava za kontrolu prolaza FALCON u tvrtki Yasenka d.o.o. koja se bavi proizvodnjom farmaceutskih pripravaka.

1.1 Zadatak diplomskog rada

Zadatak rada je obraditi ulogu računarstva u farmaceutskoj industriji i objasniti validaciju sustava prema normi 21 CFR Part 11.

2 RAČUNALNI SUSTAV

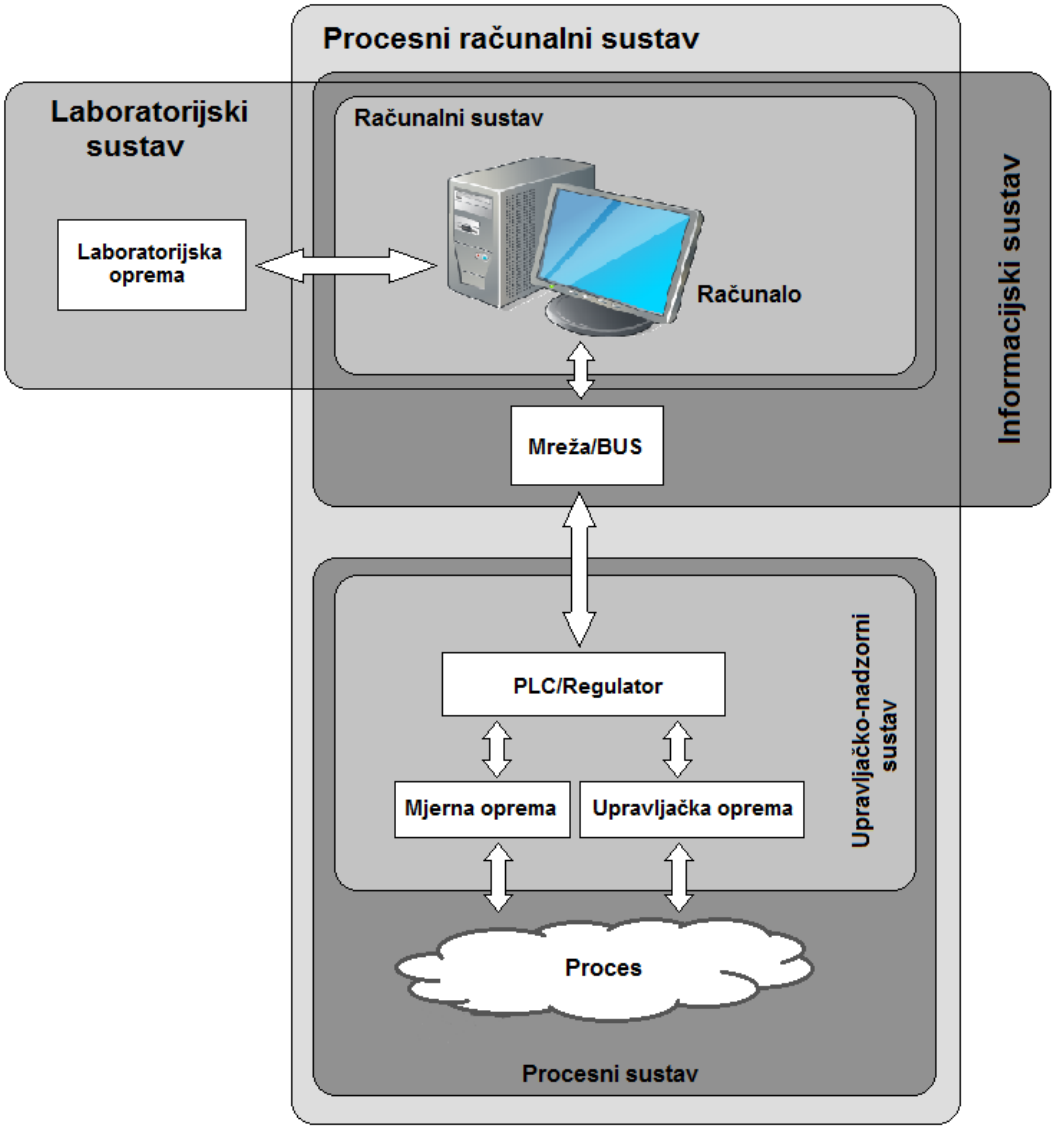
Prema definiciji [3], računalni je sustav zapravo sustav međusobno povezanih računala koja dijele centralni sustav za pohranu podataka i razne periferne uređaje. Svako računalo spojeno u sustav može raditi samostalno, ali može komunicirati i s ostalim uređajima i računalima spojenim u sustav.

Računalni sustav: hardversko-softverski koncept obuhvaća

- računalo s ulazno-izlaznim podsustavima
- programska rješenja (skup programskih instrukcija) za:
    - upravljanje radom hardverskih komponenata i povezivanje s korisničkim programima
    - rješavanje specifičnih zadataka

Računalni sustav: prošireni koncept obuhvaća

- računalo s ulazno-izlaznim podsustavima
- programska rješenja (skup programskih instrukcija) za:
    - upravljanje radom hardverskih komponenata i povezivanje s korisničkim programima
    - rješavanje specifičnih zadataka
- ljude – sudionike u interakciji s hardverom i softverom
- organizaciju
- podatke (u najširem smislu)



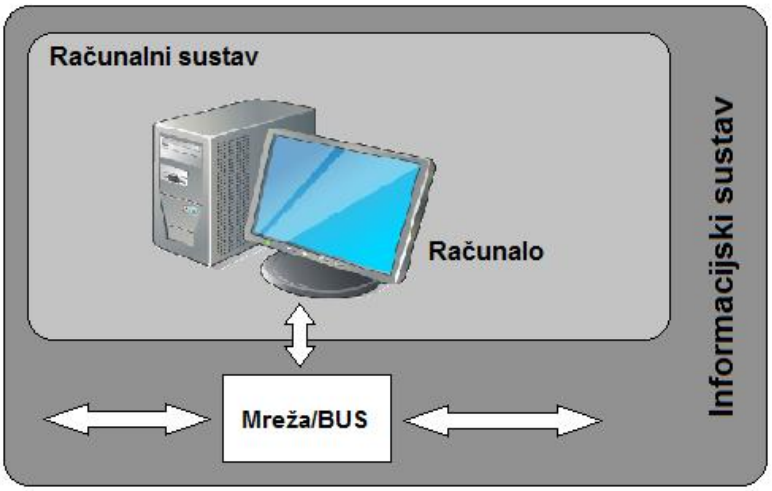
Slika 2.1. Procesni računalni sustav

2.1 Informacijski sustav

Informacijski je sustav naziv za računalni sustav čija je osnovna zadaća prikupljanje, memoriranje i obrada podataka, a rezultat njegova rada je informacija.

Informacije najprije trebaju biti prikupljene, odnosno zahvaćene iz izvora u kojemu nastaju. Potom ih je potrebno pohraniti, odnosno memorirati u ili na određenim prikladnim medijima kako bi bile raspoložive na duži rok ili trajno. Slijedi obrada ulaznih informacija koju je moguće opisati kao primjenu aritmetičko-logičkih postupaka, odnosno operacija, kojima se informacije pretvaraju (transformiraju) iz izvornog u neki drugi željeni oblik. Tako

preoblikovane informacije nerijetko će se pohranjivati odnosno memorirati iz razloga sličnih onima zbog kojih se to čini i s izvornim informacijama. Konačno, izlazne informacije potrebno je dostaviti, odnosno diseminirati korisnicima (konzumentima).

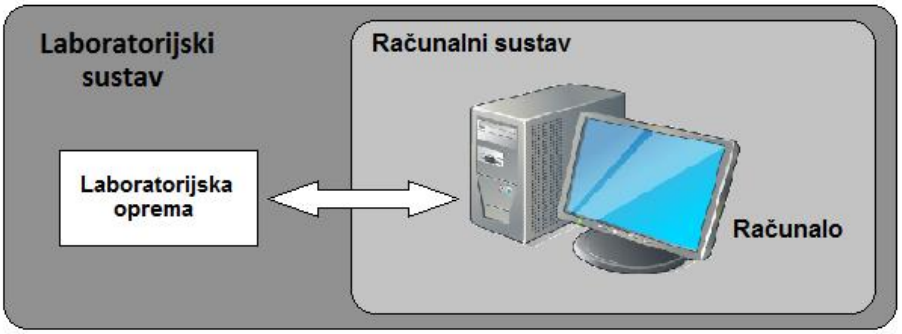


Slika 2.2. Informacijski sustav

Imajući u vidu sve navedeno, moguće je formulirati i šire određenje pojma informacijskog sustava: informacijski je sustav uređeni skup elemenata, odnosno komponenata koje u interakciji obavljaju funkcije prikupljanja, obrade, pohranjivanja i diseminacije (izdavanja na korištenje) informacija. U poslovnim sustavima, informacijski sustavi podržavaju i informacijski poslužuju poslovne procese i operacije, poslovno odlučivanje te razvijanje i implementaciju kompetitivnih strategija poslovanja. U tom smislu moguće je govoriti o poslovnim informacijskim sustavima (engl. Enterprise Information System, EIS).

2.2 Laboratorijski sustav

Laboratorijski je sustav naziv za automatizirani sustav zasnovan na računalnom sustavu i grupi međusobno povezanih uređaja namijenjenih provedbi analitičkih procesa nekog laboratorija.



Slika 2.3. Laboratorijski sustav

Laboratorijski informacijski sustav vrsta je opreme koja prima, procesuira i sprema informacije koje se dobivaju iz medicinskog ili istraživačkog laboratorija. Također bilježi rezultate pronalazaka u nekim laboratorijima diljem svijeta. LIS je visoko organizirana i prilagodiva aplikacija koja se koristi za spremanje nekoliko modela laboratorijskih radova istovremeno. Odluka o tome koju vrstu LIS-a kupiti vrlo je važan posao za svaki laboratorij. Većina većih laboratorija danas ima neki tip Laboratorijskog informacijskog sustava za spremanje svojih rezultata i informacija. Neki mali i srednji laboratoriji također istražuju i razmatraju korisnost integriranja laboratorijskog informacijskog sustava.

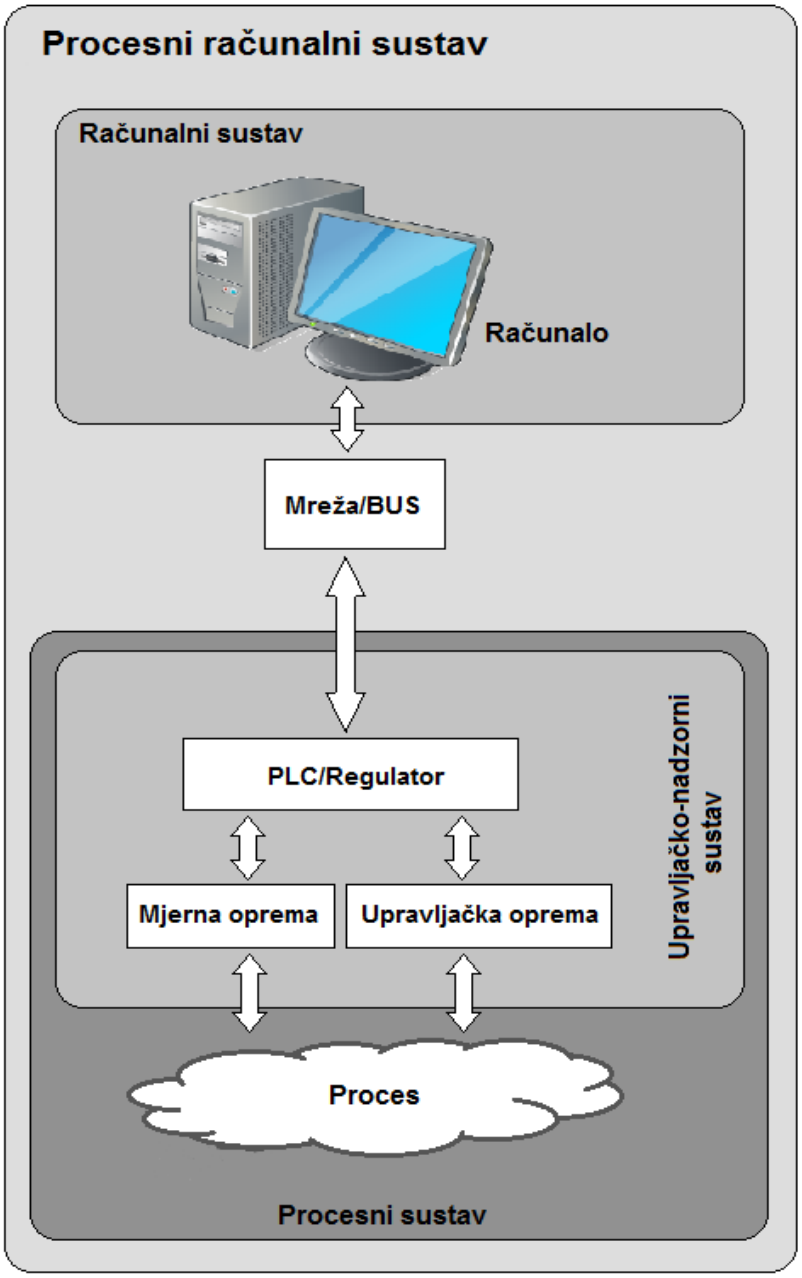
Laboratorijski informacijski sustav (LIS)

- u užem smislu:
  - program ili sustav programa
  - unos, obrada i pohrana podataka nastalih kao rezultat laboratorijskih pretraga
- u širem smislu:
  - računalna oprema
  - baza podataka
  - programi automatskih analizatora
  - program koji omogućuje komunikaciju između analizatora i LIS-a

2.3 Procesni sustav

Procesni računalni sustav naziv je za automatizirani sustav povezan s procesnom opremom u cilju upravljanja i/ili nadzora procesa, pri čemu se težište aktivnosti stavlja na promjene koje se događaju tijekom odvijanja samog procesa.

U ovisnosti o svojoj funkcionalnosti moguće ga je okarakterizirati kao mjerni, upravljački, nadzorni i sigurnosni sustav te sustav vizualizacije.



Slika 2.4. Procesni sustav

2.4 Što nije računalni sustav

Oprema ili komponente koje zadovoljavaju sve navedene kriterije:

- ne pohranjuje trajno podatke
- ne uključuje izmijenjen programski kod/ne može se izmijeniti program
- nije upravljan sa računalom ili PLC-om
- korisnik ne može mijenjati parametre sustava

Primjeri: računalo, operacijski sustav, analogna vaga, PLC...

3 VALIDACIJA RAČUNALNOG SUSTAVA

Validacija računalnog sustava predstavlja dokumentirani dokaz da je računalni sustav projektiran, instaliran i da radi za namijenjenu upotrebu, u skladu sa specificiranim zahtjevima korisnika, specifikacijom funkcionalnih zahtjeva te propisanim zahtjevima regulative.

Verifikacija i validacija podrazumijevaju sustavnu analizu i testiranje softvera tijekom razvoja radi povećanja pouzdanosti. Dok sam pojam "testiranje" često podrazumijeva provjeru ispravnosti gotovog proizvoda, verifikacija i validacija počinju istovremeno s razvojem sustava. Potrebno je utvrditi da softver obavlja upravo ono za što je sustav namijenjen i da ne ostvaruje nikakvu neželjenu funkciju, a proces podrazumijeva identificiranje i uklanjanje najrizičnijih problema u radu.

Verifikacija i validacija često se smatraju jednim objedinjenim procesom u svrhu kontrole sustava. [4]

3.1 Odgovornosti

Poslovni vlasnik sustava

Vlasnik aplikativnog dijela sustava (aplikacija i podaci) odgovoran je za procjenu sustava, njegovu poslovnu primjenu i održavanje sustava u validiranom stanju. Složeni sustavi, koji podržavaju više poslovnih procesa, mogu imati više poslovnih vlasnika sustava od kojih je svaki odgovoran za aplikativni dio sustava koji podržava njegov poslovni proces.

Tehnički vlasnik sustava

Vlasnik sistemskog dijela sustava (hardware i sistemski software) odgovoran je za isporuku sustava koji zadovoljava zahtjeve poslovanja, validaciju sustava te razvoj i održavanje sustava s tehničkog aspekta u skladu s propisanim procedurama i zahtjevom da sustav ostaje u validiranom stanju.

Osiguranje kvalitete

Odgovorno je za usklađenost poslovnih, tehničkih i korisničkih zahtjeva sa važećom regulativom. Osiguranje kvalitete pruža podršku kod kreiranja, pregledava i odobrava

pripadajuću dokumentaciju te osigurava neprekidnu usklađenost i validiranost sustava nakon puštanja sustava u rad.

Korisnik sustava

Osoba, educirana i ovlaštena za samostalno korištenje sustava, u cilju realizacije definiranih procesa i postizanja zadanih rezultata.

Administrator sustava

Osoba, educirana i ovlaštena za nadzor rada sustava, analizu sistemskih zapisa, identifikaciju potencijalnih problema na sustavu, održavanje korisničkih računa na sustavu, vođenje brige oko sigurnosti sustava, te kreiranje, izvođenje i upravljanje backup podacima.

Održavatelj sustava

Osoba, educirana i ovlaštena za osiguravanje funkcionalne ispravnosti sustava i svih preduvjeta za odvijanje definiranih procesa sukladno važećem sustavu kvalitete.

3.2 Zašto je potrebno validirati računalni sustav?

Računalni je sustav potrebno validirati kako bi dokumentirano dokazali, uz visoku sigurnost, da je sustav prikladan za upotrebu kojoj je namijenjen te usklađen sa zahtjevima regulative.

3.3 Kada je potrebno validirati računalni sustav?

Validacija sustava se provodi u okviru svakog projekta vezanog za taj sustav:

- Početno uvođenje sustava
- Prelazak na novu verziju (upgrade)
- Značajne izmjene u sustavu (patch)
- Uvođenje novih lokacija (roll-out)
- Implementacija novih procesa

3.4 Kako validirati računalni sustav?

Validacijski pristup temelji se na provjeri njegovih ključnih elemenata koji jedan takav sustav čine drugačijim od ostalih sustava, pri čemu je validacijom potrebno obuhvatiti sve segmente životnog ciklusa računalnog sustava, a u ovisnosti od kompleksnosti i specifičnosti njegove realizacije uključiti faze planiranja, izrade specifikacija, programiranja, testiranja, puštanja u rad, dokumentiranja, rada sustava i praćenja izmjena.

3.5 Kako odrediti opseg validacije?

Opseg validacije sustava ovisi o:

- GAMP kategoriji sustava
- rizičnosti sustava određenoj na osnovu provedene procjene rizika
- namijenjenoj upotrebi (npr. Korištenje elektroničkog zapisa i elektroničkog potpisa)

a) Validacijski pristup prema GAMP kategorijama software-a

Tablica 3.1. Validacijski pristup prema GAMP kategorijama software-a

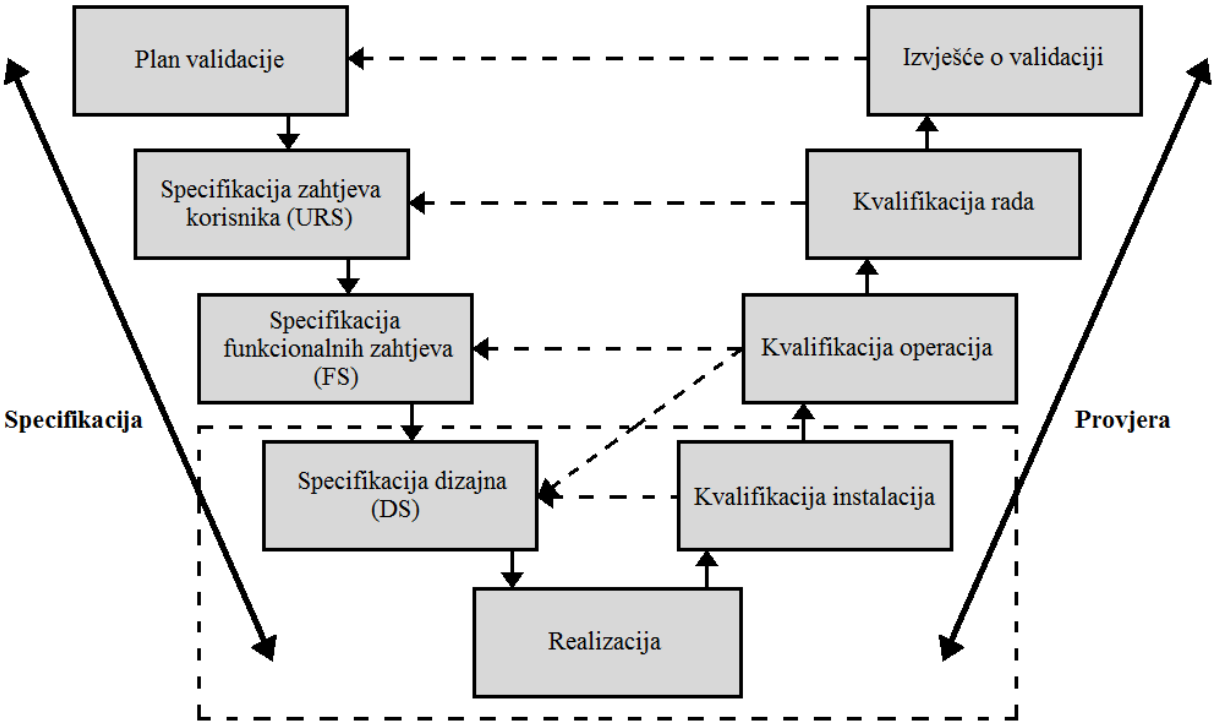
Kategorija software-a		Validacijski pristup				
		Faze V-modela				
Broj	Naziv	URS ↑ PQ	FS ↑ OQ	DS ↑ IQ	MS ↑ FAT	Napomene
1	**Infrastrukturni software** ***Osnovni SW*** (SW koji služi kao osnova za izradu aplikacije) i ***Infrastrukturni alati*** ; tipični primjeri su: Operacijski sustavi, platforme baza podataka, midleware, programski jezici, statistički paketi, proračunske tablice (Excel), nadzor mreže, sigurnosni SW, anti-virusni SW	√	×	×	×	- Kontrola izmjena
		×	×	√	×	
3	**Nekonfigurirani COTS (Commercial of the shelf) software-ski paketi** (SW koji nije moguće konfigurirati u svrhu prilagođavanja zahtjevima poslovnog procesa korisnika) Aplikacije na bazi, firmware, statistički analitički SW, SW za poslovne namjene, Office	√	√	×	×	- Kontrola izmjena - Dodatna kategorizacija: ● za konfiguriranje standardnih funkcija za korisnika → **4** ● za dodatni specijalni razvoj za korisnika → **5**
		√	√	√	×	
4	**Konfigurirani COTS software-ski paketi** (SW koji je moguće konfigurirati u svrhu prilagođavanja zahtjevima poslovnog procesa korisnika, no programski kod se ne mijenja) LIMS, SCADA, DCS, CDS, EDMS, ERP, BMS, MES, MRPII, HMI (Human Machine Interfaces)	√	√	√	×	- Audit dobavljača - Kontrola izmjena - Testiranje na testnom i produkcijskom okruženju - Dodatna kategorizacija: ● za dodatni specijalni razvoj za korisnika → **5**
		√	√	√	×	
5	**Posebno razvijeni software** (bespoke/custom-made SW, tj. SW dizajniran i kodiran u svrhu prilagođavanja zahtjevima poslovnog procesa korisnika) IT aplikacije, aplikacije za upravljanje procesima, Macro naredbe	√	√	√	√	- Audit dobavljača - Pregled dizajna i programskog koda
		√	√	√	√	

b) Validacijski pristup prema GAMP kategorijama hardware-a

Tablica 3.2. Validacijski pristup prema GAMP kategorijama hardware-a

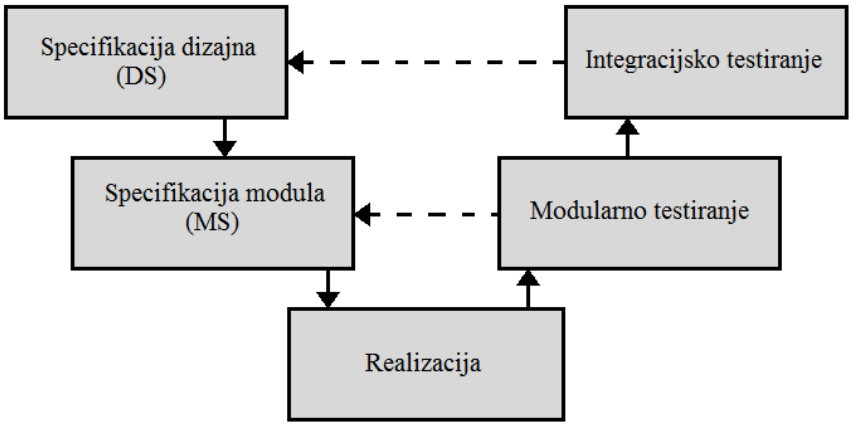
Kategorija hardware-a		Validacijski pristup				
		Faze V-modela				
Broj	Naziv	URS ↑ PQ	FS ↑ OQ	DS ↑ IQ	MS ↑ FAT	Napomene
1	**Standardne hardware-ske komponente**	√	×	×	×	- Kontrola izmjena
		×	×	√	×	
2	**Posebno razvijene hardware-ske komponente** (bespoke/custom-made)	√	×	√	×	- Audit dobavljača - Kontrola izmjena
		×	×	√	√	

c) V-model validacijskog pristupa



Slika 3.1. V-model validacijskog pristupa

U slučajevima kada je implementiran software kategorije 5, V-model validacijskog pristupa proširuje se sukladno sljedećem prikazu:



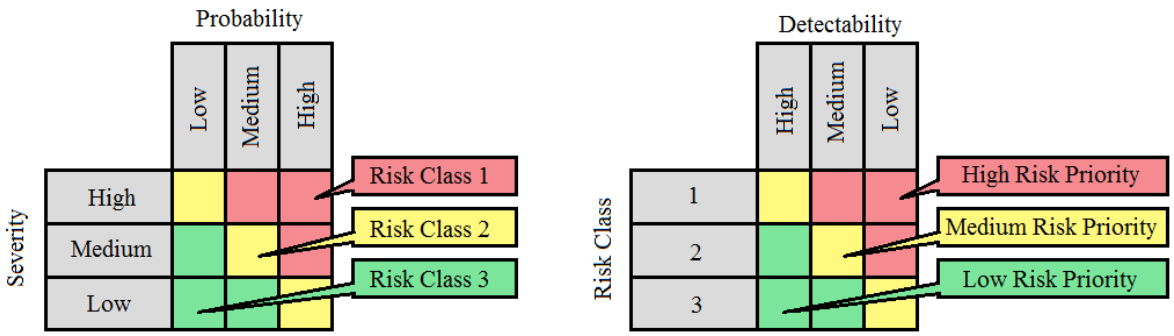
Slika 3.2. Prošireni V-model validacijskog pristupa

d) Procjena kritičnosti i rizičnosti korištenja sustava – procjena rizika

- Inicijalna procjena rizika
  - provodi se u fazi planiranja
  - određuje se kritičnost sustava prema kritičnosti poslovnih procesa koje taj sustav podržava da bi se moglo odrediti do koje mjere sustav mora biti usklađen s regulatornim zahtjevima i na osnovi toga provesti odgovarajuće validacijske aktivnosti
  - određuje se razina rizika korištenja sustava
- Razine rizika korištenja sustava
  - visoku razinu rizika imaju kritični sustavi čija se funkcionalnost za odvijanje poslovnih procesa ne može zamijeniti drugim sustavom ili ručnom procedurom.
  - srednju razinu rizika imaju kritični sustavi čija se funkcionalnost za odvijanje poslovnih procesa može zamijeniti drugim sustavom ili ručnom procedurom.
  - nisku razinu rizika imaju sustavi koji nisu kritični i čija se funkcionalnost za odvijanje poslovnih procesa može zamijeniti drugim sustavom ili ručnom procedurom.

- Funkcionalna procjena rizika
    - provodi se u fazi izrade specifikacija
    - određuju se rizici koji se mogu pojaviti tijekom rada sustava, te mogući rizici koji nastaju kao posljedica nepostojanja tražene funkcionalnosti sustava koja se proceduralno nadomješćuje
    - određuje se veličina rizika koja može biti visoka, srednja ili niska. U slučaju visokog rizika moraju se provesti odgovarajuće aktivnosti kojima će se rizik eliminirati ili smanjiti na veličinu koja će biti prihvatljiva za procjenjivani sustav
- Veličina rizika

  Određuje se na osnovi:
    - vjerojatnosti nastanka rizika (Risk Probability): mala, srednja, visoka
    - utjecaja rizika (Risk Severity): mali, srednji, visoki
    - vjerojatnosti otkrivanja rizika (Risk Detectability): mala, srednja, visoka



Slika 3.3. Veličina rizika

- Vjerojatnost nastanka rizika
    - visoka - funkcionalnost sustava prilagođena je izmjenom programskog koda (development, customizing)
    - srednja - funkcionalnost sustava prilagođena je konfiguracijom sistemskih parametara i/ili opcija
    - niska - koristi se standardna funkcionalnost sustava

- Utjecaj rizika
    - visoki - funkcionalnost sustava podržava kritične poslovne procese
    - srednji - funkcionalnost sustava podržava značajne poslovne procese
    - niski - funkcionalnost sustava podržava manje značajne poslovne procese
- Vjerojatnost otkrivanja rizika
    - visoka – postoji automatska provjera ulaznih podataka i izlaznih rezultata i automatsko detektiranje pogrešaka
    - srednja – postoji ručna provjera ulaznih podataka i izlaznih rezultata (dvostruka provjera podataka)
    - niska – ne postoji nikakva provjera ulaznih podataka i izlaznih rezultata
- Mogući načini smanjenja veličine rizika
    - izmjena procesa ili izmjena dizajna računalnog sustava
    - revizija projekta (uključiti kvalifikacije i iskusnije djelatnike, povećati edukaciju)
    - izmjena validacijskog pristupa i proširenje testiranja
    - eliminacija rizika, odnosno odustajanje od ponuđenog načina implementacije

e) Procjena dobavljača računalnog sustava

- audit dobavljača (obavezan za software kategorije 5)
- procjena upitnikom
- certifikat o uspostavljenom sustavu kvalitete

Način procjene dobavljača određuje se na osnovu procjene kritičnosti i rizičnosti sustava.

f) Provjera usklađenosti sustava sa zahtjevima FDA 21 CFR Part 11 norme

Za sustave koji koriste elektroničke zapise i potpise validacijskim aktivnostima potrebno je obuhvatiti provjeru zahtjevima navedenim u FDA 21 CFR Part 11 normi.

3.6 Validacijska dokumentacija

a) URS/FS – User Requirement specification/Functional Specification

Specifikacija zahtjeva korisnika za opremu (URS/FS), prostore, energente ili sustave dokument je u koji su ugrađeni ključni elementi i kvalitete i svaki rizik smanjen na prihvatljivu razinu.

URS sadrži zahtjeve za opremu i njezinu funkcionalnost kako bi mogli biti korišteni za namjeravanu upotrebu u proizvodnji, kontroli kvalitete, čuvanju i rukovanju proizvodima koji podliježu GMP regulatornim zahtjevima.

URS treba biti referentna točka kroz validacijski životni ciklus.

b) DQ – Design Qualification / Matrica sljedivosti (Traceability matrix)

Kvalifikacija dizajna je element kvalifikacije opreme, prostora, energenata ili sustava, kojim se treba demonstrirati i dokumentirati usklađenost dizajna s GMP zahtjevima. Zahtjevi definirani u URS-u trebaju biti verificirani kvalifikacijom dizajna.

Matrica sljedivosti je dio protokola za kvalifikaciju dizajna, a sastoji se od tablice s listom zahtjeva koje je potrebno verificirati ili testirati, a spadaju u skupinu instalacija, operacija i rada.

c) FAT/SAT – Factory Acceptance Test / Site Acceptance Test

Oprema, posebno ako je u nju ugrađena nova ili kompleksna tehnologija, može biti evaluirana, ako je primjenjivo kod dobavljača, prije dostavljanja.

Prije instalacije, potrebno je potvrditi sukladnost opreme sa URS/FS na lokaciji dobavljača, ako je primjenjivo.

Gdje je to primjenjivo i opravdano, potrebno je provesti pregled dokumentacije i nekoliko testova prilikom FAT-a ili u drugim fazama, bez potrebe ponavljanja *on site* prilikom IQ/OQ, ako je moguće dokazati da transport i instalacija opreme nisu ilmali utjecaj na funkcionalnost opreme.

FAT može biti nadopunjen provedbom SAT-a prilikom zaprimanja opreme na mjestu proizvodnje.

d) IQ – Instalation Qualification / KI – Kvalifikacija instalacija

Kvalifikacija instalacija (KI) dokumentirani je postupak kojim se verificira da je oprema izrađena, promijenjena te instalirana u skladu s projektnom dokumentacijom, preporukama proizvođaća te zahtjevima korisnika opreme.

KI treba biti provedena na opremi, prostorima, energentima ili sustavima. [5]

KI uključuje sljedeće aktivnosti:

- verifikaciju da su komponente, instrumentacija, oprema, cijevi i usluge ispravno instalirane prema inženjerskim nacrtima i specifikacijama
- verifikaciju ispravne instaliranosti prema predefiniranim kriterijima
- sakupljanje i razvrstavanje operativnih i radnih postupaka dobavljača i zahtjeva održvanja
- kalibracija mjernih instrumenata
- verifikaciju materijala izrade

e) OQ – Operational Qualfication / KO – Kvalifikacija operacija

Kvalifikacija operacija (KO) dokumentirani je postupak kojim se dokazuje da instalirana, nabavljena ili izmjenjena oprema, unutar definiranog radnog područja, konzistentno i dosljedno ostvaruje funkcionalne zahtjeve prema definiranoj namjeni.

KO uključuje (ali nije ograničena) sljedeće:

- testove koji moraju biti razvijeni na bazi znanja o preocesu, sustavu ili opremi kako bi se osiguralo da sistem radi kako je dizajniran
- testove koji potvrđuju donju i gornju granicu operativnih vrijednosti, i/ili *worst case* uvjete

f) PQ–Perfomance Qualification / KR – Kvalifikacija rada

Kvalifikacija rada (KR) dokumentirani je postupak kojim se, neutralnim materijalom (placebo) ili stvarnim proizvodom, dokazuje da je unutar definiranog radnog područja instalirana, nabavljena ili izmjenjena oprema, zajedno sa svim pomočnim sustavima, u stanju konzistentno i dosljedno davati očekivani rezultat u skladu s definiranim procesom i/ili specifikacjom proizvoda.

KR treba uključiti (ali nije ograničeno) sljedeće:

- testovi, upotrebljeni proizvodni materijali, kvalificirani zamjenski ili simulirajuči proizvodi, dokazano da ima ekvivalentno ponašanje pod normalnim operativnim uvjetima s *worst case* veličinom serije
- učestalost uzorkovanja upotrebljena da potvrdi kontrolu procesa treba biti opravdana
- testovi trebaju pokriti operacijski raspon predviđeog procesa, osim postojanja dokumentiranih dokaza iz razvojne faze koji potvrđuju operacijske raspone

g) Završno izvješće

Nakon provedene kvalifikacije opreme, izrađuje se Izvješće o kvalifikaciji opreme u kojim se na osnovi provedenih zadataka zaključuje može li se oprema smatrati kvalificiranom i koristiti u redovnoj proizvodnji. [5]

Izvješće o kvalifikaciji opreme treba sadržavati sljedeća poglavlja:

- Uvod
- Analiza rezultata
- Odstupanja
- Preporuke za daljni rad
- Zaključak
- Prilozi

3.7 Održavanje sustava u validiranom stanju

- Ugovor o održavanju sustava i pružanju podrške
- Izrada sigurnosnih kopija, vraćanje sigurnosnih kopija i arhiviranje podataka
- Zaštita i informacijska sigurnost sustava
- Periodički pregled ovlaštenja za rad na sustavu (1x godišnje ispisivati popis ovlaštenja)
- Alternativni način rada i Plan poslovnog kontinuiteta
- Plan oporavka u slučaju havarije (što učiniti ako sustav nije dostupan neko vrijeme)
- Kontrola izmjena
- Upravljanje incidentima
- Periodički pregled sustava (1x godišnje)

Svrha periodičkog pregleda jest potvrditi da je sustav ostao u validiranom stanju nakon zadnje kvalifikacije.

Periodička pregleda sustava provodi se na temelju izjave u izvještaju za prethodnu kvalifikaciju ili najviše 3 godine nakon zadnje kvalifikacije.

Periodički pregled sustava obuhvaća:

- pregled svih izmjena provedenih na sustavu nakon zadnje kvalifikacije
- pregled odstupanja i provedenih korektivnih akcija nakon zadnje kvalifikacije
- pregled provedenih audita i zadanih korektivnih akcija
- pregled validacijske dokumentacije
- pregled procedura za održavanje sustava i evidencije incidenata

3.8 Validacija prema 21 CFR part 11 normi

Organizacije koje koriste računalne sustave u okolišu koji je reguliran od strane FDA moraju dokumentirati operacije koje čini sustav, konfiguraciju koja je potrebna da bi sustav ispravno radio te izvršiti testiranje koje će demonstrirati da sustav radi u skladu sa specifikacijama. Ovaj proces se naziva validacija.

Sec. 11.10 Kontrola za zatvorene sustave.

Osobe koje koriste zatvorene sustave za stvaranje, izmjenu, održavanje ili prijenos elektroničkih zapisa bi trebale upotrijebiti postupke i kontrole dizajnirane kako bi se osigurala autentičnost, integritet i, kada je to prikladno, povjerljivost elektroničkih zapisa te osigurati da potpisnik ne može lako odbaciti potpisani zapis kao da nije originalan. Takvi postupci i kontrole trebaju uključiti sljedeće:

(a) Validaciju sustava kako bi se osigurala točnost, pouzdanost, dosljedan i planiran učinak te sposobnost raspoznavanja nevažećih ili izmijenjenih zapisa.
(b) Mogućnost stvaranja preciznih i potpunih kopija zapisa koji su čitljivi i u elektroničkom obliku koji je prikladan za provjeru, pregled i kopiranje. Potrebno je kontaktirati agenciju ukoliko postoje pitanja u vezi mogućnosti agencije za provođenje provjere i kopiranja elektroničkih zapisa.
(c) Zaštita zapisa kako bi se osigurala preciznost i spremnost za preuzimanje kroz period čuvanja podataka.
(d) Ograničavanje pristupa na autorizirane osobe.
(e) Korištenje sigurnih, kompjuterski generiranih privremenih pristupa s pečatom vremena za neovisno bilježenje datuma i vremena unosa i akcija koje stvaraju, modificiraju ili brišu elektroničke podatke. Promjena podataka ne smije oštetiti prethodno zapisane informacije. Dokumentacija o takvim pristupima mora se zadržati barem toliko dugo koliko je potrebno za elektroničke zapise koji se pregledavaju i treba biti dostupna za nadzor i kopiranje agencije.
(f) Korištenje provjeravanja operacijskog sustava za osiguravanje dopuštenog slijeda koraka i događaja.
(g) Korištenje provjere prava pristupa kako bi se osiguralo da samo osobe s pravom pristupa imaju mogućnost korištenja sustava, elektroničkog potpisivanja zapisa, pristupanja operacijama ili uređajima za unos i ispis podataka, mijenjanja zapisa ili direktno izvršavanje operacija.

(h) Provjeriti korištenja uređaja (npr. terminala) za otkrivanje validnosti izvora podataka ili operacijskih instrukcija.

(i) Utvrditi da osoba koja razvija, održava ili koristi elektroničke zapise ili potpise ima potrebnu edukaciju, trening i iskustvo za obavljanje zadataka.

(j) Ustanoviti i držati se zapisanih pravilnika na temelju kojih su pojedinci odgovorni za djela koja su pokrenuta njihovim elektroničkim potpisom kako bi se odbilo falsificiranje zapisa i potpisa

(k) Korištenje prikladnih kontrola nad dokumentacijom sustava uključujući:

- prikladne kontrole nad distribucijom, pristupom i dokumentacijom operacija i održavanja sustava
- pregled i promjenu kontrolnih procedura za održavanje pristupa koji dokumentira vremenski poredani razvoj i modifikaciju dokumentacije sustava

Sec. 11.30 Kontrole za otvorene sustave.

Osobe koje koriste otvorene sustave za kreiranje, modificiranje, održavanje ili prijenos elektroničkih zapisa trebale bi koristiti procedure i kontrole koje su osmišljene za osiguravanje autentičnosti, integriteta i povjerljivosti elektroničkih zapisa od trenutka kreiranja do trenutka prihvaćanja. Takve procedure i kontrole trebaju uključivati one predviđene u 11.10 te dodatne mjere, poput enkripcije dokumenata, kao i korištenje prikladnog standarda digitalnog potpisa kako bi se osigurala autentičnost, integritet i povjerljivost zapisa što je neophodno u ovim uvjetima.

Sec. 11.50 Prikazi potpisa.

(a) Potpisani elektronički zapisi trebaju sadržavati određene informacije povezane s potpisivanjem koje jasno pokazuje sljedeće:
   - ispisano ime potpisnika
   - datum i vrijeme kada je zapis potpisan
   - značenje (poput pregleda, odobrenja, odgovornosti ili autorstva) povezano s potpisom

(b) Stavke propisane u paragrafima (a) (1), (a) (2) i (a) (3) ove sekcije trebaju podlijegati istim kontrolama kao elektronički zapisi i trebaju biti uključene kao dio svakog čitljivog formata elektroničkih zapisa (poput elektroničkog prikaza ili ispisa).

Sec. 11.70 Povezivanje potpisa/zapisa.

Elektronički potpisi i ručni potpisi izvedeni na elektroničkim zapisima trebaju biti povezani s navedenim zapisima kako bi se osiguralo da potpisi ne mogu biti premješteni, kopirani ili drugačije preneseni u svrhu falsificiranja elektroničkih zapisa uobičajenim sredstvima.

Podjeljak C—Elektronički potpisi

Sec. 11. 100 Općeniti zahtjevi.

(a) Svaki elektronički potpis treba biti unikatan za jednog pojedinca i ne smije se koristiti ili prebaciti na nekog drugog.
(b) Prije nego što organizacija ustanovi, dodijeli, certificira ili drugačije postupi prema elektroničkom potpisu pojedinca ili bilo kojem elementu takvog elektroničkog potpisa, mora potvrditi identitet pojedinca.
(c) Osobe koje koriste elektroničke potpise trebaju prije ili u vrijeme korištenja potvrditi agenciji da su elektronički zapisi u njihovom sustavu, koji se koriste na ili nakon 20. kolovoza 1997., namijenjeni kao zakonski povezani ekvivalent tradicionalnog ručnog potpisa.
(1) Certifikacija mora biti dostavljena u papirnom obliku, i biti potpisana tradicionalnim ručnim potpisom, u ured regionalnih operacija (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.
(2) Osobe koje koriste elektronički potpis trebaju, na zahtjev agencije, pružiti dodatnu certifikaciju i svjedočiti da je određeni elektronički potpis legalno i obvezujuće sredstvo ekvivalentno ručnom potpisu.

Sec. 11. 200 Komponente i kontrole elektroničkog potpisa

(a) Elektronički potpisi koji nisu osnovani na biometriji trebaju:
(1) sadržavati barem dvije posebne identifikacijske komponente poput identifikacijskog koda i lozinke

- kada pojedinac potpisuje niz dokumenata u jednom kontinuiranom periodu pristupa sustavu, prvi se potpis mora izvoditi koristeći sve komponente elektroničkog potpisa; daljnja potpisivanja moraju biti izvedena korištenjem barem jedne komponente koja može biti izvršena od strane pojedinca čime će biti ostvarena mogućnost da se njom služi jedino pojedinac

- kada pojedinac provodi jedan ili više potpisa koji se ne izvode u jednom kontinuiranom periodu pristupa sustavu, svaki potpis treba sadržavati sve komponente potpisa

(2) Koristiti samo njihovi pravi vlasnici.

(3) Biti administrirani i provedeni kako bi se osiguralo da pokušaj korištenja nečijeg elektroničkog potpisa od strane nekoga tko nije pravi vlasnik zahtijeva suradnju dviju ili više osoba.

(b) Elektronički potpisi koji su bazirani na biometriji trebali bi biti dizajnirati tako da bi se osiguralo da samo pravi vlasnici mogu koristiti potpis.

Sec. 11.300 Kontrole za identifikaciju kodova/lozinki.

Osobe koje koriste elektroničke potpise bazirane na korištenju identifikacijskih kodova u kombinaciji s lozinkama trebaju koristiti kontrole za osiguravanje sigurnosti i integriteta. Takve kontrole trebaju uključivati:

(a) održavanje jedinstvenosti svake kombinacije identifikacijskog koda i lozinke tako da dva pojedinca ne mogu imati istu kombinaciju identifikacijskog koda i lozinke

(b) osiguravanje da se identifikacijski kod i lozinka periodično provjeravaju, prozivaju i pregledavaju (npr. pokrivanje događaja starenja lozinke)

(c) praćenje procedura pri gubitku kako bi se elektronički uklonila autorizacija s izgubljenih, ukradenih ili drugačije potencijalno kompromitiranih tokena, kartica i drugih uređaja koji sadrže ili generiraju identifikacijski kod ili lozinku te izdavanje privremenih ili trajnih zamjena koristeći prikladne rigorozne kontrole

(d) korištenje transakcijskih zaštita kako bi bilo spriječeno nedopušteno korištenje lozinke i/ili identifikacijskih kodova te kako bi bili otkriveni i prijavljeni takvi pokušaji na brz i žuran način sigurnosnoj jedinici sustava i, kako je primjereno, organizacijskom menadžmentu.

(e) incijalno i periodično testiranje uređaja, poput tokena i kartica, koji sadržavaju ili generiraju identifikacijski kod ili lozinku kako bi bilo osigurano ispravno funkcioniranje te spriječeno mijenjanje na nedopušten način. [6]

4 ZAKLJUČAK

Kako računalni sustavi mogu izravno utjecati na zdravlje pacijenata, zbog toga moraju prolaziti poseban proces implementacije. Implementacija sustava u Dobroj proizvođačkoj praksi(DPP) i kritičnom okruženju sastoji se od pripremne faze (faza dizajna i izrade URS-a i/ili FS-a), faze implementacije te kontrole rada (IQ, OQ i PQ testiranje – validacija), najbolje se ilustrira tzv. V modelom. Validacija se provodi prema uputama i procedurama koje su opisane u GAMP-u 5. Validacija IT sustava provodi se kako bi se dokazalo da sustav radi u skladu s postavljenim zahtjevima. Nakon implementacije IT sustava u DPP okruženju, svaka promjena na takvom sustavu mora biti provedena kroz postupak kontrolirane izmjene (IT Change Control). Svaka promjena prolazi sličan put kao i kod implementacije: analiza rizika promjene, validacija te konačno implementacija uz svu potrebnu dokumentaciju.

Kao primjer validacije računalnog sustava izvršena je Kvalifikacija sustava za kontrolu prolaza FALCON u tvrtki Yasenka d.o.o., koja se bavi proizvodnjom farmaceutskih pripravaka. U suradnji s odgovornom osobom za validacije i kvalifikacije, napisan je protokol koji je iskorišten za kvalifikaciju istog. Kako je procjenom rizika ispitano, računalni sustav ne utječe na zdravlje pacijenata te je time i smanjen obujam kvalifikacije (IQ, OQ). Temeljem završene kvalifikacije računalnog sustava, dokazano je kako sustav radi u skladu sa postavljenim zahtjevima.

LITERATURA

[1] The Rules Governing Medicinal Products in the European Union, Good Manufacturing Practice Medicinal Products for Human and Veterinary Use, Annex 11: Computerised Systems

http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf (kolovoz 2016.)

[2] IBM blog: IBM, farmaceutska industrija i informacijska tehnologija, od A do Ž

https://www-304.ibm.com/connections/blogs/IBM.Talking_about/entry/farmaceutska_industrija_i_it_od_a_do_%25c5%25be?lang=en_us (lipanj 2016.)

[3] Business Dictionary

http://www.businessdictionary.com/definition/computer-system.html (kolovoz 2016.)

[4] GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems

[5] EU Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use, Annex 15: Qualification and Validation

http://ec.europa.eu/health/files/eudralex/vol-4/2015-10_annex15.pdf (kolovoz 2016.)

[6] CFR - Code of Federal Regulations Title 21

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1 (kolovoz 2016.)

SAŽETAK

U ovom je radu dan pregled rada računalnog sustava koji se koristi u farmaceutskoj industriji, kao i njegovih podsustava (informacijski, laboratorijski i procesni sustav). Dan je pregled kako se i zašto moraju validirati pojedini računalni sustavi. Također, prikazan je postupak validacije računalnog sustava (prema GAMP-u 5) i svih njezinih dijelova: Specifikacija zahtjeva korisnika (URS), Kvalifikacija dizajna (DQ), Kvalifikacija instalacija (IQ), Kvalifikacija operacija (OQ) i Kvalifikacija rada (PQ). Objašnjeno je i kako održavati računalni sustav u validiranom stanju. Ukoliko je potrebno validirati računalni sustav, potrebno je to učiniti prema 21 CFR Part 11 gdje su dane smjernice koji zahtjevi moraju biti ispunjeni kako bi se zadovoljio FDA standard. U praktičnom dijelu rada prikazan je postupak validacije računalnog sustava u farmaceutskoj industriji koji, u ovom slučaju, nema utjecaj na zdravlje pacijenta.

Ključne riječi:21 CFR Part 11, farmaceutska industrija, GAMP5, računalni sustav, validacija

ABSTRACT

Role of Computer Science in Pharmaceutical Industry and Validation of Computer Systems According to 21 CFR Part 11 Standards

In this paper, a review of computer system used in pharmaceutical industry is given, as well as its subsystems (informational, laboratory and process system). It is reviewed how and why specific computer systems are validated. It also shows a procedure of computer system validation (according to GAMP 5) and all its parts, and those are: User request specification (URS), Design qualification (DQ), Installation qualification (IQ), Operation qualification (OQ) and Performance qualification (PQ). It is explained how to keep computer system in validated state. If computer system needs to be validated according to 21 CFR part 11 you can find guidelines on requests that need to be fulfilled to satisfy FDA standard. In practical part of this paper I have shown a procedure for validation of computer system in pharmaceutical industry which in this case does not affect patient health.

Key words:21 CFR Part 11, computer system, GAMP 5, pharmaceutical industry, validation

ŽIVOTOPIS

Matej Lončar rođen je 27.3.1990. godine u Vinkovcima. Odrastao je i živi u Privlaci sa svojim roditeljima, ocem Radoslavom, majkom Dubravkom i braćom Ivanom i Tinom.

Školovanje je započeo 1997. godine u osnovnoj školi Stjepana Antolovića u Privlaci. Kroz sve razrede osnovne škole bio je odličan učenik. Godine 2005. upisao je opću gimnaziju u Vinkovcima. Sve razrede završio je s vrlo dobrim uspjehom, kao i maturu. Nakon uspješno riješenog prijemnog ispita i vrlo dobrog uspjeha u srednjoj školi, 2009. godine, upisuje Elektrotehnički fakultet u Osijeku, smjer računarstvo. Godine 2013. završava preddiplomski studij računarstva, te upisuje diplomski studij procesnog računarstva.

Potpis:

PRILOG

Na optičkom disku koji se nalazi u prilogu ovog rada nalazi se diplomski rad u digitalnom obliku i dokument Validacijska_dokumentacija.pdf u kojemu je prikazan postupak validacije računalnog sustava, odnosno Kvalifikacija sustava za kontrolu prolaza FALCON u tvrtki Yasenka d.o.o.. Također isti dokument je ispisan kao prilog ovoj tiskanoj verziji.