MISKOLCI EGYETEM

GÉPÉSZMÉRNÖKI ÉS INFORMATIKAI KAR

Automatizálási és Infokommunikációs Intézet

Mérnökinformatikus (BSc) alapszak

GYÓGYSZERIPARI INFORMATIKAI RENDSZER VALIDÁLÁSA

Szakdolgozat

TÓTH LEVENTE

YRBNIF

Miskolc, 2024

Miskolci Egyetem
Gépészmérnöki és Informatikai Kar
Mérnökinformatikus (BSc) alapszak

Szám: **2024-GE-BIL-YRBNIF**
Automatizálási és
Infokommunikációs Intézet
3515 Miskolc-Egyetemváros

SZAKDOLGOZAT FELADAT

Tóth Levente

BSc Mérnökinformatikus jelölt részére

A tervezés tárgyköre: *IT rendszer validálása*

A szakdolgozat címe: *Gyógyszeripari informatikai rendszer validálása*

A feladat részletezése:

1. Mutassa be a gyógyszeriparban alkalmazott számítógépes rendszerek szerepét és jelentőségét, ismertesse az informatika és automatizálás integrációját a kutatástól a gyártásig és minőségellenőrzésig.
2. Ismertesse a gyógyszeripari szabályozási környezetet, különös tekintettel az FDA 21 CFR Part 11 és EU GMP Annex 11 előírásaira!
3. Részletezze a számítógépes rendszer validálás (CSV) célját, életciklusát és típusait, mutassa be a GAMP® 5 módszertan alapelveit, rendszerkategóriáit és kockázatalapú megközelítését!
4. Végezze el egy ICP-OES berendezéshez kapcsolódó informatikai rendszer validálási folyamatának Installation Qualification részét!
5. Ismertesse a rendszer technikai követelményeit és beállításait (pl. hardver, operációs rendszer, hálózat, hozzáférések, adatmentés)!
6. Értékelje a validálás során elért eredményeket, és fogalmazza meg a tanulságokat a szabályozói megfelelés, adatbiztonság és működési megbízhatóság szempontjából!

Tervezésvezető(k): **Dr. Varga Attila Károly** egyetemi docens
ME-GÉIK, Automatizálási és Infokommunikációs Intézet

Konzulens(ek):

A szakdolgozat kiadásának időpontja: 2024.03.12.
A szakdolgozat beadásának határideje: 2024.05.03.

Miskolc, 2024.03.12.

Dr. Trohák Attila
egyetemi docens
intézetigazgató

1. *A* szakdolgozat *módosítása:* *szükséges (a módosítást külön lap tartalmazza)*
   nem szükséges (a megfelelő rész aláhúzandó)

   Miskolc, 2024.05.03.

   tervezésvezető aláírása

2. *A tervezést ellenőriztem:* *(1)* *2024.03.18.*
   (2) *2024.04.12.*
   (3) *2024.04.26.*
   (4) *2024.05.02.*

   tervezésvezető aláírása

3. *A* szakdolgozat *beadható*
   nem adható be

   Miskolc, 2024.05.03.

   konzulens aláírása *tervezésvezető aláírása*

4. *A* szakdolgozat *52 szövegoldalt,*
   18 db rajzot,
   - egyéb mellékletet tartalmaz.

5. *A* szakdolgozat *bírálatra* *bocsátható*
   nem bocsátható

   A bíráló neve: Sitku Ádám György, SAP Developer, MOL IT & Digital GBS HU Kft.

   Miskolc, 2024.05.10.

   intézetigazgató aláírása

6. *Osztályzat:* *a bíráló javaslata: ……..*
   az intézet javaslata: ……..
   a Záróvizsga Bizottság döntése: ……..

   Miskolc, ……..

   a Záróvizsga Bizottság elnökének aláírása

EREDETISÉGI NYILATKOZAT

Alulírott **Tóth Levente** (Neptun-kód **YRBNIF**) a Miskolci Egyetem Gépészmérnöki és Informatikai Karának végzős mérnökinformatikus szakos hallgatója ezennel büntetőjogi és fegyelmi felelősségem tudatában nyilatkozom és aláírásommal igazolom, hogy

GYÓGYSZERIPARI INFORMATIKAI RENDSZER VALIDÁLÁSA

című szakdolgozatom saját, önálló munkám; az abban hivatkozott szakirodalom felhasználása a forráskezelés szabályai szerint történt.

Tudomásul veszem, hogy szakdolgozat esetén plágiumnak számít:

- szószerinti idézet közlése idézőjel és hivatkozás megjelölése nélkül;
- tartalmi idézet hivatkozás megjelölése nélkül;
- más publikált gondolatainak saját gondolatként való feltüntetése.

Alulírott kijelentem, hogy a plágium fogalmát megismertem, és tudomásul veszem, hogy plágium esetén szakdolgozatom visszautasításra kerül.

Miskolc, 2024. év május hó 03. nap

……

Tóth Levente
hallgató

TARTALOMJEGYZÉK

KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretném kifejezni őszinte hálámat és köszönetemet a családomnak, akik mindvégig támogattak és biztattak a szakdolgozatom elkészítése során. Köszönöm a türelmüket, megértésüket és azt az érzelmi hátteret, amely lehetővé tette, hogy a tanulmányaimra koncentrálhassak.

Külön köszönöm a szüleimnek a folyamatos biztatást, valamint a nyugodt, stabil hátteret, amely nélkül ez a munka nem születhetett volna meg. Hálás vagyok a szeretetükért, támogatásukért és a belém vetett hitükért.

1. BEVEZETÉS

1.1 A gyógyszeripar és a technológia elválaszthatatlan kapcsolata

A gyógyszeripar, mint a globális gazdaság és a társadalom egyik alappillére, alapvető küldetése az emberi egészség megőrzése, a betegségek megelőzése, diagnosztizálása és hatékony kezelése új, biztonságos és hatásos terápiák kifejlesztésén és gyártásán keresztül. E felelősségteljes feladat ellátása napjainkban elképzelhetetlen a fejlett technológiák, különösen az informatika és az automatizált rendszerek mélyreható integrációja nélkül. A gyógyszerekkel szemben támasztott rendkívül magas minőségi és biztonsági elvárások, a kutatási és gyártási folyamatok növekvő komplexitása, különösen a biológiai gyógyszerek esetében, a hatalmas mennyiségű adat kezelésének szükségessége, valamint a szigorú globális és helyi szabályozói követelmények mind hozzájárultak ahhoz, hogy a számítógépes rendszerek a gyógyszeripar szinte minden szegmensében nélkülözhetetlenné váljanak.

Ez a technológiai áthatolás már a legkorábbi fázisokban, a kutatás és fejlesztés során megmutatkozik, ahol az elektronikus laboratóriumi naplók segítik a kísérletek precíz dokumentálását. A következő lépcsőfokon, a klinikai vizsgálatok során, az elektronikus adatrögzítő rendszerek és a klinikai vizsgálat menedzsment rendszerek biztosítják az adatok pontosságát és a komplex folyamatok átláthatóságát, melyek a betegek bevonását és a vizsgálati készítmények elosztását koordinálják.

A gyártási területen talán még látványosabb a számítógépesítés mértéke, a gyártásirányítási rendszerek felügyelik a teljes termelési folyamatot, biztosítva az elektronikus gyártási jegyzőkönyvek létrehozását és a nyomon követhetőséget. A folyamatvezérlő és adatgyűjtő rendszerek a kritikus paraméterek valós idejű ellenőrzését és irányítását végzik. Ehhez szorosan kapcsolódnak az épületfelügyeleti rendszerek, amelyek a gyártási környezet stabilitását garantálják, amelyek a minőség folyamatos ellenőrzését teszik lehetővé.

A minőség-ellenőrzés sem maradhat ki ebből a körből, ahol a laboratóriumi információs és menedzsment rendszerek a minták kezelésétől az eredmények rögzítésén át a minőségi tanúsítványok kiállításáig terjedő teljes munkafolyamatot támogatják, gyakran

együttműködve a kromatográfiás adatfeldolgozó rendszerekkel és más műszerspecifikus szoftverekkel.

A technológiai fejlődés túlmutat a gyártás és minőség-ellenőrzés határain, a teljes ellátási láncot és a vállalati működést is áthatja. Az átfogó vállalatirányítási rendszerek integrálják a pénzügyi, logisztikai és gyártási adatokat, a raktárirányítási rendszerek optimalizálják a tárolási és anyagmozgatási folyamatokat, a szerializációs és aggregációs nyomon követési megoldások pedig a termékhamisítás elleni küzdelem kulcsfontosságú eszközei. Mindezek mellett a szabályozási megfelelőséget és a gyógyszerbiztonságot támogató rendszerek, mint a dokumentumkezelő rendszerek, az elektronikus törzskönyvezési eszközök és a farmakovigilanciai adatbázisok szintén elengedhetetlenek.

Fontos hangsúlyozni, hogy ezek a rendszerek nem csupán elszigetelt entitások, hanem egy komplex, gyakran szorosan összekapcsolt ökoszisztémát alkotnak, ahol az adatok és információk folyamatosan áramlanak a különböző funkcionális területek között. Ez a magas szintű integráció és az általuk kezelt adatok, illetve irányított folyamatok kritikus jellege – amelyek közvetlenül befolyásolják a termékminőséget és a betegbiztonságot, hiszen egy rendszerhiba súlyos következményekkel járhat – teszi megkerülhetetlenné működésük megbízhatóságának és pontosságának szisztematikus, dokumentált igazolását. Ez az igény vezet el minket a számítógépes rendszer validálásának alapvető fontosságú témaköréhez.

1.2 A számítógépes rendszer validálás jelentősége és aktualitása a gyógyszeriparban

Az előző fejezetben leírt technológiai komplexitás és a rendszerek kritikus szerepe miatt a gyógyszeriparban elengedhetetlenné vált a számítógép vezérelt rendszerek használata. Ez a folyamat nem csupán egy technikai ellenőrzés, hanem egy formális, dokumentált bizonyítási eljárás, amely magas fokú biztonsággal igazolja, hogy egy adott számítógépes rendszer – beleértve a hardvert, a szoftvert és a kapcsolódó eljárásokat – következetesen és megbízhatóan az előre meghatározott felhasználói követelményeknek, specifikációknak és minőségi jellemzőknek megfelelően működik a teljes életciklusa során. A számítógépes rendszer validálás elsődleges célja tehát annak biztosítása, hogy a rendszer pontos, megbízható és alkalmas a tervezett feladat ellátására, garantálva ezzel a folyamatok konzisztenciáját, az adatok integritását és a végső soron előállított termék minőségét.

A validálás jelentősége a gyógyszeriparban több kulcsfontosságú tényezőből fakad. Mindenekelőtt a betegbiztonság áll, hiszen egy nem megfelelően működő, validálatlan rendszer – legyen szó gyártást irányító, adagolást vezérlő vagy minőség-ellenőrzési adatokat kezelő alkalmazásról – közvetlen kockázatot jelenthet a betegekre nézve, akár hibás termék kibocsátása, akár helytelen adatok alapján hozott rossz döntések révén. Szorosan kapcsolódik ehhez a termékminőség biztosítása, a validált rendszerek elengedhetetlenek a gyártási folyamatok állandóságának fenntartásához és annak garantálásához, hogy a gyógyszerek minden egyes gyártási tétele megfeleljen a szigorú előírásoknak. Nem elhanyagolható szempont a szabályoknak való megfelelés sem. A nemzeti és nemzetközi gyógyszerügyi hatóságok, mint az amerikai FDA (Food and Drug Administration) a 21 CFR Part 11 rendelettel, vagy az Európai Unió az EU GMP (Good Manufacturing Practice) Annex 11 iránymutatásával, kötelezővé teszik a GxP (Jó Gyakorlatok – pl. GMP, GCP, GLP) környezetben alkalmazott számítógépes rendszerek validálását. Ezen előírások megsértése súlyos következményekkel járhat, a hatósági figyelmeztetésektől és bírságoktól kezdve a gyártási engedély felfüggesztésén át egészen a termékvisszahívásokig és a vállalat jó hírnevének csorbulásáig. A validálás továbbá központi szerepet játszik az adatintegritás fenntartásában, amely a hatóságok kiemelt figyelmét élvezi, és az ALCOA+ (Attribútumokhoz köthető, Olvasható, Egyidejűleg rögzített, Eredeti, Pontos + Teljes, Következetes, Tartós, Elérhető) elvek betartását követeli meg a megbízható adatok és az azokon alapuló döntések érdekében. Végül, bár a validálás erőforrás-igényes folyamat, hosszú távon üzleti és működési hatékonysági előnyökkel is jár, mivel csökkenti a rendszerhibákból, adatvesztésből, utólagos javításokból és nem tervezett leállásokból származó kockázatokat és költségeket.

A számítógépes rendszer validálás témakörének aktualitását napjainkban számos tényező erősíti. A gyors technológiai fejlődés folyamatosan új kihívások elé állítja a validálási szakembereket, a felhőalapú szolgáltatások, a mesterséges intelligencia és gépi tanulás alkalmazása, a Big Data analitika, valamint az Internet of Things (IoT) eszközök elterjedése mind új megközelítéseket és szempontokat igényelnek a validálás során. Ezzel párhuzamosan a gyógyszeriparban zajló digitális transzformáció és az Ipar 4.0 törekvések tovább növelik az integrált, komplex rendszerek szerepét, és még inkább előtérbe helyezik azok megbízhatóságának és validált állapotának fontosságát. A szabályozói elvárások is

folyamatosan fejlődnek, egyre nagyobb hangsúlyt fektetve a kockázatalapú megközelítésekre (amelyet például a GAMP® 5 iparági útmutató is támogat), az adatintegritás proaktív biztosítására és a validálás teljes életciklusra való kiterjesztésére, beleértve a rendszeres felülvizsgálatokat és a változáskezelést. A globalizáció és a komplex ellátási láncok szintén növelik a validálás jelentőségét, hiszen biztosítani kell a konzisztens minőséget és megfelelést a különböző régiókban és a partnerek által üzemeltetett rendszerek esetében is. Végezetül pedig a növekvő kiberbiztonsági fenyegetések miatt az adatvédelem és a rendszerek biztonságos működésének garantálása is egyre inkább a validálási tevékenységek szerves részévé válik.

1.3 A szakdolgozat célja

A számítógépes rendszerek validálásának fentebb vázolt komplexitása és kiemelt iparági jelentősége alapján jelen szakdolgozat célja, ennek a szemléletmódnak a bemutatása egy konkrét számítógépes rendszer validálásán keresztül, különös tekintettel az Installation Qualification (IQ) szerepére és annak megfelelő végrehajtására.

E célkitűzés mentén a szakdolgozat a következő központi kutatási kérdésekre keresi a választ:

Milyen GxP-követelmények érvényesek az ICP-OES berendezéshez kapcsolt számítástechnikai rendszerre, és ezek hogyan határozzák meg az IQ folyamatát?

Mi az Installation Qualification (IQ) szerepe a számítógépes rendszerek validálásában, és hogyan valósítható meg hatékonyan egy ICP-OES berendezés esetében?

Milyen számítógépes beállítások, rendszerkövetelmények és technikai konfigurációk szükségesek ahhoz, hogy a validálás megfeleljen az elvárt minőségi és biztonsági szinteknek?

2. A SZABÁLYOZÁSI KÖRNYEZET ALAPJAI A GYÓGYSZERIPARBAN

A gyógyszeriparban használt számítógépes rendszereknek meg kell felelniük a szigorú hatósági előírásoknak, amelyek célja a termékminőség, a betegbiztonság és az adatintegritás garantálása [1][2][5][6][7][8]. Két mérföldkőnek számító szabályozás határozza meg ezen a területen az elvárásokat:

1. FDA 21 CFR Part 11 – Electronic Records; Electronic Signatures (USA) [7]
2. EudraLex - Volume 4 - Good Manufacturing Practice (GMP) guidelines, Annex 11: Computerised Systems (Európai Unió) [8]

Bár eltérő régiókra vonatkoznak, céljaik és alapelveik sok tekintetben hasonlóak, és a globálisan működő gyógyszergyáraknak gyakran mindkét szabályozásnak meg kell felelniük [5] [6] [7] [8].

2.1 FDA 21 CFR Part 11: Electronic Records; Electronic Signatures

Az Amerikai Egyesült Államok Élelmiszer- és Gyógyszerügyi Hivatala (FDA) által kiadott 21 CFR Part 11 (Code of Federal Regulations Title 21, Part 11) azokat a kritériumokat határozza meg, amelyek alapján az FDA az elektronikus rekordokat és az elektronikus aláírásokat megbízhatónak, hitelesnek és a papíralapú rekordokkal, valamint a kézzel írott aláírásokkal egyenértékűnek tekinti [7]. Fontos megérteni, hogy a Part 11 önmagában nem kötelez az elektronikus rendszerek használatára, hanem feltételeket szab azok elfogadhatóságához, amennyiben egy cég úgy dönt, hogy elektronikusan teljesíti az FDA más szabályzataiban (az ún. „predicate rules” vagy alaprendeletek, pl. GMP, GCP, GLP előírások) megkövetelt dokumentációs vagy aláírási kötelezettségeket [7] [13].

2.1.1 Elektronikus rekordokhoz tartozó főbb követelmények

Validálás: Az elektronikus rekordok létrehozására, módosítására, karbantartására vagy továbbítására használt rendszereket validálni kell, hogy biztosítsák azok pontosságát,

megbízhatóságát, a következetes, rendeltetésszerű működést és a hamisíthatatlan rekordok létrehozásának képességét [6] [7] [13] [14].

Audit Trail (Naplózás): Biztonságos, számítógép által generált, időbélyegzővel ellátott audit trail-t kell létrehozni és megőrizni, amely függetlenül rögzíti az operátor által végrehajtott létrehozási, módosítási vagy törlési műveleteket az elektronikus rekordokon. Az audit trail-nek tartalmaznia kell a "ki, mit, mikor és miért (ha releváns)" információkat, és nem szabad, hogy felülírható legyen. Az audit trail-t a rekorddal együtt, annak teljes megőrzési ideje alatt kell tárolni és elérhetővé tenni a hatósági ellenőrzés számára [7] [10] [11].

Másolatok és Megőrzés: Képesnek kell lenni pontos és teljes másolatok generálására az elektronikus rekordokról, mind ember által olvasható, mind elektronikus formátumban, amelyek alkalmasak az ellenőrzésre, felülvizsgálatra és másolásra. A rekordokat védeni kell az adatvesztéstől és a jogosulatlan módosítástól, és biztosítani kell azok visszakereshetőségét a teljes megőrzési idő alatt [7] [9] [10] [11].

Hozzáférési Jogosultságok: A rendszerekhez való hozzáférést csak arra jogosult személyek számára szabad engedélyezni. Egyértelműen definiálni kell a jogosultsági szinteket (pl. adatrögzítés, módosítás, törlés, rendszeradminisztráció), és ezeket technikailag (pl. egyedi felhasználói azonosítók és jelszavak) és adminisztratívan (eljárások) is biztosítani kell [6] [7] [8] [10].

2.2 EU GMP Annex 11: Computerised Systems

Az EU GMP (Helyes Gyártási Gyakorlat) iránymutatásainak 11. melléklete (Annex 11) azokra a számítógépes rendszerekre vonatkozik, amelyeket a GMP által szabályozott tevékenységek részeként használnak (elsősorban gyógyszergyártás és minőség-ellenőrzés) [8]. Célja annak biztosítása, hogy ezek a rendszerek validáltak, megbízhatóak, és alkalmasak legyenek a tervezett felhasználásra, minimalizálva a betegbiztonságot, termékminőséget vagy adatintegritást érintő kockázatokat. Az Annex 11 alapelvei gyakran kiterjesztésre kerülnek más GxP területekre is az EU-ban [5] [6] [8] [11].

2.2.1 Az EU GMP Annex 11 főbb alapelvei és követelményei

Kockázatkezelés (Risk Management): Az Annex 11 kiemeli a kockázatkezelés fontosságát a rendszer teljes életciklusa során, a tervezéstől a kivezetésig. A validálási erőfeszítések mértékének és mélységének arányosnak kell lennie a rendszer komplexitásával, újdonságával és a betegbiztonságra, termékminőségre és adatintegritásra gyakorolt potenciális hatásával (kockázatalapú megközelítés) [6] [8] [12] [13].

Validálás: Minden GMP-releváns számítógépes rendszert validálni kell. A validálásnak bizonyítania kell, hogy a rendszer megfelel az előre meghatározott követelményeknek (URS - User Requirement Specification alapján). A validálásnak ki kell terjednie a releváns funkciókra, a beépített ellenőrzésekre, az adatátvitel pontosságára, a biztonságra és az audit trail funkciókra.

Személyzet (Personnel): Egyértelműen definiálni kell a felelősségi köröket a rendszer kezelésével, karbantartásával és validálásával kapcsolatban. A személyzetnek megfelelő képzésben kell részesülnie [5] [8].

Beszállítók és Szolgáltatók (Suppliers and Service Providers): A rendszerek vagy szolgáltatások (pl. felhő szolgáltatások) beszállítóit formális értékelésnek és auditnak kell alávetni. Világos szerződésekre és szolgáltatási szintekre (SLA) van szükség [6] [8] [11].

Adatok (Data): Kiemelt hangsúly van az adatintegritáson. Az adatokat biztonságosan kell tárolni, védeni kell a sérüléstől és elvesztéstől (pl. rendszeres biztonsági mentésekkel). Az adatmigrációt (adatok átvitele egyik rendszerből a másikba) szintén validálni kell. Az adatoknak pontosnak, olvashatónak és a teljes megőrzési idő alatt elérhetőnek kell lenniük [6] [8] [9] [10] [13].

Audit Trail (Naplózás): Kockázatértékelés alapján kell eldönteni, hogy szükséges-e audit trail, és milyen mélységű. Ha van, annak rögzítenie kell minden GMP-releváns adat létrehozását, módosítását vagy törlését (ki, mit, mikor, miért). Biztonságosnak, időbélyegzővel ellátottnak, rendszeresen felülvizsgáltnak és a megőrzési idő alatt elérhetőnek kell lennie. Az Annex 11 expliciten említi az audit trail rendszeres felülvizsgálatának szükségességét [8] [9] [10] [11].

Biztonság (Security): Fizikai és logikai biztonsági intézkedéseket kell alkalmazni a jogosulatlan hozzáférés megakadályozására. Az adatok biztonságát is garantálni kell [8] [10].

Elektronikus Aláírások (Electronic Signatures): Használatuk esetén biztosítani kell, hogy ugyanolyan szintű biztonságot és jelentést hordozzanak, mint a kézzel írott aláírások [7] [8].

Tétel Felszabadítás (Batch Release): Ha számítógépes rendszer használatával történik a gyártási tétel felszabadítása, annak a rendszernek teljes mértékben validáltnak és biztonságosnak kell lennie [6] [8].

Üzletmenet-folytonosság (Business Continuity): Rendelkezni kell tervekkel a rendszer meghibásodása esetére (pl. katasztrófa-elhárítási terv, adat-visszaállítási eljárások), hogy a kritikus folyamatok ne vagy csak minimálisan sérüljenek [5] [8].

Archiválás (Archiving): Az elektronikus adatokat a vonatkozó előírásoknak megfelelő ideig kell megőrizni, biztosítva olvashatóságukat és integritásukat [8] [10] [11].

2.3 Összehasonlítás és Szinergiák

Bár a két szabályozás eltérő fókusszal és részletességgel rendelkezik bizonyos területeken (pl. az Annex 11 erősebben hangsúlyozza a kockázatkezelést és a beszállítói menedzsmentet), alapvető céljaik közösek: a számítógépes rendszerek megbízhatóságának, az elektronikus adatok integritásának és a betegbiztonságnak a garantálása a szabályozott gyógyszeripari környezetben. Mindkettő megköveteli a rendszerek validálását, a biztonságos audit trail funkciót, a hozzáférések szabályozását és az elektronikus aláírások megbízhatóságának biztosítását. A globális piacon működő vállalatok számára a gyakorlatban gyakran e két szabályozás követelményeinek együttes figyelembevételével kialakított validálási stratégia a célravezető [5] [6] [7] [8] [9] [10] [11] [13].

3. A SZÁMÍTÓGÉPES RENDSZER VALIDÁLÁS (CSV) ALAPELVEI ÉS FOGALMAI

A számítógépes rendszer validálása (Computerized System Validation) egy formális, dokumentált folyamat, amely bizonyítja, hogy egy adott számítógépes rendszer (beleértve a hardvert, szoftvert, perifériákat és a kapcsolódó eljárásokat) következetesen és megbízhatóan megfelel az előre meghatározott specifikációknak és minőségi követelményeknek, és alkalmas a tervezett felhasználásra a szabályozott gyógyszeripari környezetben. Nem csupán egy egyszeri tesztelésről van szó, hanem egy teljes életciklust átfogó megközelítésről [6] [13] [14].

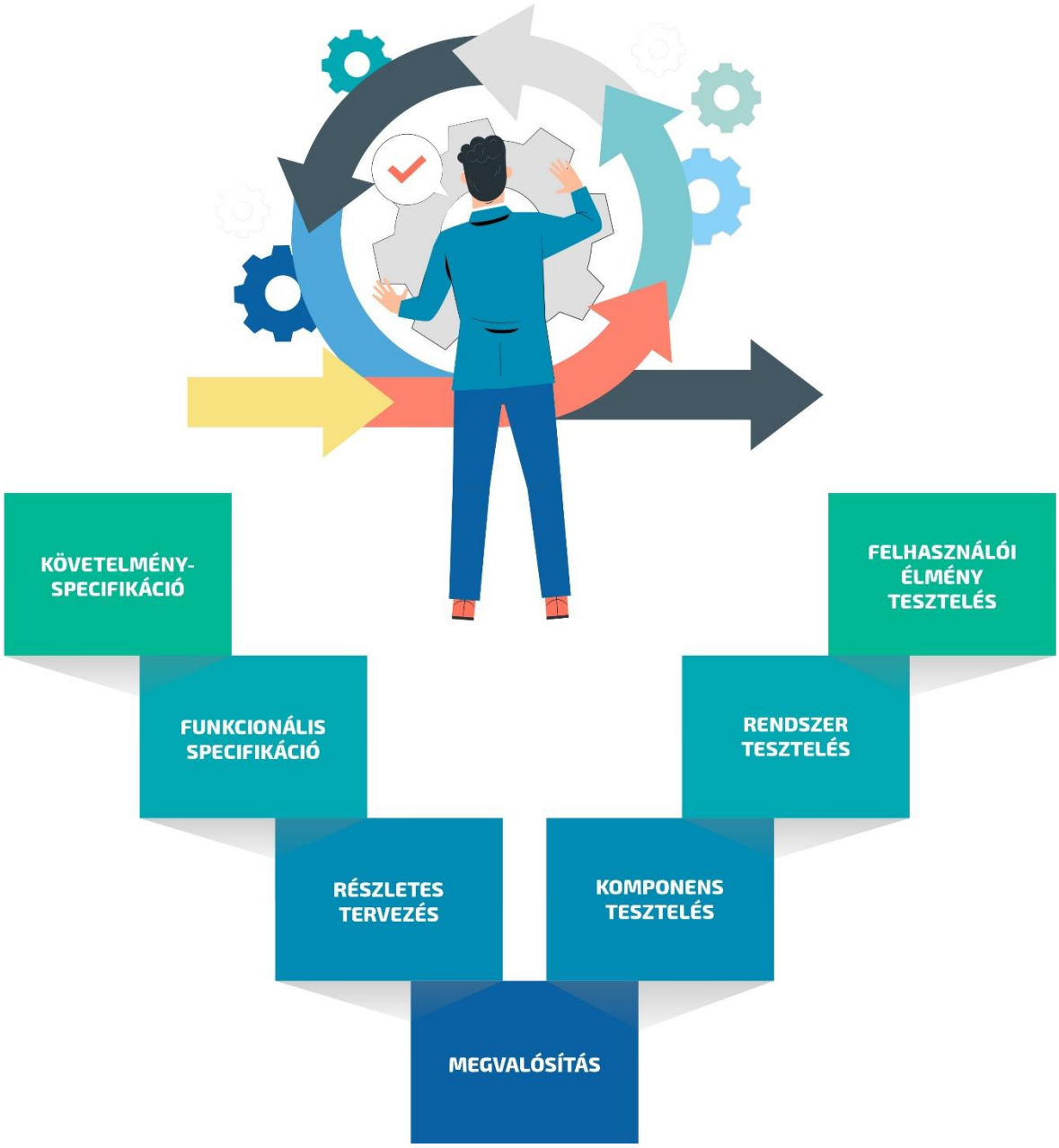
3.1 A számítógépes rendszer validálás céljai

- **Megbízhatóság és Pontosság:** Annak biztosítása, hogy a rendszer következetesen azt teszi, amit elvárnak tőle, és pontos eredményeket szolgáltat [1] [2] [6] [13].
- **Adatintegritás:** Annak garantálása, hogy a rendszer által kezelt adatok teljesek, pontosak, megbízhatóak és védettek a jogosulatlan módosításoktól vagy elvesztéstől (ALCOA+ elvek) [6] [9] [10] [11].
- **Szabályozói Megfelelés:** A hatósági előírásoknak (pl. FDA 21 CFR Part 11, EU GMP Annex 11) való megfelelés bizonyítása [5] [6] [7] [8] [13].
- **Termékminőség és Betegbiztonság:** Közvetett módon hozzájárulás a konzisztens termékminőséghez és a betegbiztonság fenntartásához azáltal, hogy biztosítja a kritikus folyamatokat támogató rendszerek helyes működését [1] [2] [6] [13].
- **Üzleti Folyamatok Támogatása:** Annak igazolása, hogy a rendszer hatékonyan támogatja a tervezett üzleti folyamatokat [3] [6] [13].

3.2 A Validálási Életciklus Modell

A CSV általában egy strukturált életciklus-modellt (1. ábra) követ, amely biztosítja a követelmények, a tervezés és a tesztelés közötti nyomon követhetőséget. A modell célja, hogy ne csak a bevezetés pillanatában, hanem a rendszer teljes használati időtartama alatt

biztosítsa a szabályozói és minőségi megfelelést. Ez különösen fontos a gyógyszeriparban, ahol az adatkezelés, a minőség és a betegbiztonság kulcskérdés [1] [6] [9] [13].



1. ábra: Validálási életciklus modell

3.3 A rendszer validálás időzítés szerinti típusai

- **Prospektív Validálás:** A rendszer rutin használatba vétele előtt végzett teljes validálási folyamat. Ez a preferált és leggyakoribb megközelítés [6] [13].
- **Konkurens (Egyidejű) Validálás:** Kivételes esetekben, dokumentált indoklással végezhető validálás a rendszer rutin használatával párhuzamosan [6] [13].
- **Retrospektív Validálás:** Régebbi, már használatban lévő, de korábban nem validált rendszerek esetén alkalmazott megközelítés, amely a múltbeli adatok és a rendszer működésének elemzésén alapul. Ezt a hatóságok általában már nem fogadják el új rendszerek esetében, és csak nagyon korlátozottan alkalmazható [6] [13].

Összefoglalva, a CSV egy átfogó minőségbiztosítási folyamat, amely messze túlmutat a puszta szoftvertesztelésen. Magában foglalja a tervezést, a kockázatértékelést, a követelmények és specifikációk pontos meghatározását, a szigorú dokumentálást, a képzést, valamint a rendszer teljes életciklusa alatti felügyeletet és változáskezelést, mindezt a szabályozói elvárásoknak való megfelelés és a betegbiztonság garantálása érdekében [6] [9] [13] [14].

4. A GAMP® 5 MÓDSZERTAN BEMUTATÁSA

A GAMP® (Good Automated Manufacturing Practice – Helyes Automatizált Gyártási Gyakorlat) nem egy jogszabály vagy kötelező érvényű rendelet, hanem egy iparági útmutató, amelyet az ISPE (International Society for Pharmaceutical Engineering – Nemzetközi Gyógyszerészmérnöki Társaság) fejlesztett ki és tart karban [6]. A GAMP® célja, hogy gyakorlati, kockázatalapú megközelítést nyújtson a gyógyszeriparban és a kapcsolódó iparágakban használt automatizált és számítógépes rendszerek validálásához, segítve a vállalatokat abban, hogy megfeleljenek a hatósági elvárásoknak (mint pl. az FDA 21 CFR Part 11 és az EU GMP Annex 11) hatékony és eredményes módon [6] [7] [8] [13] [14]. A legutóbbi fő verziója a GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems, amelyet eredetileg 2008-ban adtak ki, de azóta frissítések és kiegészítő útmutatók jelentek meg hozzá, hogy lépést tartson a technológiai fejlődéssel és a szabályozói környezet változásaival.

4.1 A GAMP® 5 alapelvei

A GAMP® 5 öt kulcsfontosságú alapelvre épül, amelyek a következők [6] [13] [14]:

1. **Termék- és Folyamatismeret (Product and Process Understanding):** A validálásnak a termék és a támogatott üzleti/gyártási folyamat mély megértésén kell alapulnia. Ez teszi lehetővé a kritikus szempontok azonosítását és annak megértését, hogy a számítógépes rendszer hogyan befolyásolja a betegbiztonságot, a termékminőséget és az adatintegritást [6] [14].

2. **Életciklus Megközelítés (Lifecycle Approach within a QMS):** A validálási tevékenységeket a rendszer teljes életciklusa során alkalmazni kell, a kezdeti koncepciótól és tervezéstől kezdve a fejlesztésen, üzemeltetésen át egészen a rendszer kivezetéséig. Ezeket a tevékenységeket egy Minőségirányítási Rendszer (QMS) keretein belül kell végezni [6] [13] [14].

3. **Skálázható Életciklus Tevékenységek (Scalable Lifecycle Activities):** A validálási erőfeszítéseknek, a dokumentáció mélységének és a formális

követelményeknek skálázhatónak kell lenniük. Azaz, arányosnak kell lenniük a rendszer által jelentett kockázattal, a rendszer komplexitásával és újszerűségével. Nem szükséges minden rendszerre ugyanazt a maximális erőfeszítést fordítani [6] [13].

4. **Tudományos Alapú Minőségi Kockázatkezelés (Science-Based Quality Risk Management - QRM):** A minőségi kockázatkezelés (az ICH Q9 iránymutatás elvei alapján) központi eleme a GAMP® 5-nek. A QRM-et a teljes életciklus során alkalmazni kell a betegbiztonságot, termékminőséget és adatintegritást veszélyeztető kockázatok azonosítására, értékelésére, kontrollálására és felülvizsgálatára. A validálásnak a jelentős kockázatok csökkentésére kell összpontosítania [6] [12] [13] [14].

5. **Beszállítók Bevonása (Leveraging Supplier Involvement):** A GAMP® ösztönzi a beszállítókkal (szoftverfejlesztők, hardvergyártók, integrátorok) való szoros együttműködést. Lehetőség van a beszállítók tudásának, dokumentációjának és tesztelési eredményeinek felhasználására (leveraging) a validálási folyamat során, feltéve, hogy a beszállító minőségirányítási rendszere és fejlesztési gyakorlatai megfelelőek (ezt beszállítói értékeléssel kell igazolni). Ez különösen fontos a kereskedelemben kapható termékek esetében [6] [11] [13].

4.2 Kulcsfogalmak és eszközök a GAMP® 5-ben

- **Rendszerkategorizálás (GAMP® Software Categories):** Ez az egyik legismertebb GAMP® eszköz, amely segít a validálási stratégia és erőfeszítés skálázásában a szoftver típusa alapján. A fő kategóriák (a GAMP 5 Második Kiadásának értelmezése szerint is relevánsak a validációs stratégia szempontjából):
    - **3. Kategória: Nem konfigurált termékek (Non-configured Products):** Standard, "dobozos" szoftverek vagy firmware-ek, amelyeket a beépített funkciókkal használnak, és nem konfigurálják az üzleti folyamathoz. Például operációs rendszerek (bár ezek inkább infrastruktúra részét képezik), egyszerűbb műszerszoftverek. A validálás a megfelelő működés

ellenőrzésére és a konfigurációs beállítások dokumentálására összpontosít [6] [14].

- **4. Kategória: Konfigurált termékek (Configured Products):** Olyan szoftverek, amelyeket a beépített eszközökkel (konfigurációs beállításokkal, szkriptekkel) az adott üzleti folyamat igényeihez igazítanak, de maga a szoftverkód nem módosul. Ilyenek tipikusan a LIMS, MES, ERP, SCADA rendszerek. A validációnak ki kell terjednie a konfigurált funkciók és a standard funkciók együttes működésének alapos tesztelésére. Ez egy nagyon gyakori kategória [6] [13] [14].
- **5. Kategória: Egyedi alkalmazások (Custom Applications):** Kifejezetten egyedi igények alapján, egy adott vállalkozás számára fejlesztett szoftverek. Ezek hordozzák a legmagasabb kockázatot, ezért a legszigorúbb validálási megközelítést igénylik, amely lefedi a teljes szoftverfejlesztési életciklust (SDLC) a követelmények specifikálásától a kódoláson át a részletes tesztelésig [6] [14].

  (Megjegyzés: Az infrastruktúra elemeket, mint OS, adatbázisok, hálózat, a GAMP® szintén kezeli, de a validációs fókusz itt inkább a megfelelő telepítésre, konfigurációra és menedzsmentre irányul (Infrastructure Qualification).)

- **Hardver kategorizálás:** A GAMP® a hardvereket is kategorizálja (Standard és Egyedi), ami befolyásolja a szükséges kvalifikálási (IQ/OQ) tevékenységeket [6] [13].
- **Kockázatértékelési folyamat:** A GAMP® részletesen foglalkozik a kockázatértékelés módszertanával. Ez magában foglalja a potenciális hibák (mi romolhat el?), azok valószínűségének és súlyosságának (hatás a betegre/termékre/adatra) értékelését, valamint a kockázat elfogadhatóságának meghatározását. Az eredmények alapján határozzák meg a szükséges kontrollokat és a validálási tesztek mélységét [6] [12] [13].

- **Specifikáció és verifikáció:** Megerősíti a V-modell szerinti, hangsúlyozva, hogy a specifikációk részletessége és a verifikáció (tesztelés) mélysége a kockázattól és a rendszer kategóriájától függ [6] [13] [14].

- **Beszállítói értékelés:** Részletes útmutatást ad a beszállítók kiválasztására és értékelésére, beleértve a minőségirányítási rendszerük, fejlesztési módszertanuk és dokumentációs gyakorlataik felmérését [6] [11] [13].

- **Üzemeltetési fázis (Operational Phase):** A GAMP® nemcsak a projekt fázisra koncentrál, hanem részletes útmutatást ad a validált állapot fenntartásához szükséges operatív tevékenységekre is (változáskezelés, időszakos felülvizsgálat, incidenskezelés, biztonsági mentés és visszaállítás, üzletmenet-folytonosság, archiválás, kivezetés) [6] [14].

4.3 A GAMP® 5 alkalmazásának előnyei

- **Hatékonyság:** A kockázatalapú megközelítés lehetővé teszi az erőforrások (idő, pénz, emberi erőforrás) fókuszálását a legkritikusabb területekre, potenciálisan csökkentve a validálás költségeit és időigényét [6] [14].

- **Megfelelőség:** Strukturált keretrendszert biztosít, amelyet a hatóságok széles körben elfogadnak a szabályozói követelmények teljesítésére [6] [7] [8] [13].

- **Konzisztencia:** Segít egységes validálási gyakorlat kialakításában egy szervezeten belül [6] [14].

- **Egyértelműség:** Gyakorlati útmutatást, példákat és sablonokat kínál a validálási folyamat támogatására [6] [13] [14].

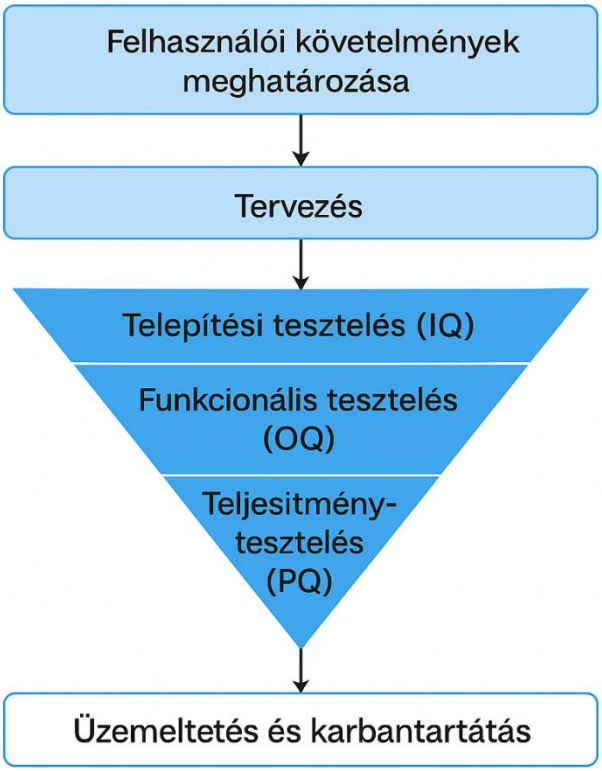
Összefoglalva, a GAMP® 5 egy nélkülözhetetlen útmutató a gyógyszeriparban dolgozó validálási szakemberek számára. Segít eligazodni a komplex szabályozói környezetben, és egy jól bevált, kockázatalapú módszertant kínál a számítógépes rendszerek megbízható, követelményeknek megfelelő és hatékony validálásához a teljes életciklus során.

4.4 A kockázatalapú validálás elveinek és alkalmazásának elemzése

A kockázatalapú validálás (Risk-Based Validation - RBV) egy olyan megközelítés a validálási folyamatokban, amely a hangsúlyt a rendszerek és folyamatok által jelentett kockázatokra helyezi. Ahelyett, hogy mindenre egyformán kiterjedő validálást alkalmaznánk, az RBV lehetővé teszi a szervezetek számára, hogy erőforrásaikat a kritikusabb területekre összpontosítsák, ezáltal hatékonyabbá és költséghatékonyabbá téve a validálási tevékenységeket. A kockázatalapú validálás egy elengedhetetlen megközelítés a modern validálási gyakorlatban. Lehetővé teszi a szervezetek számára, hogy hatékonyabban és költséghatékonyabban biztosítsák termékeik és szolgáltatásaik minőségét és biztonságát azáltal, hogy a validálási erőfeszítéseket a legkritikusabb területekre összpontosítják. A helyes alkalmazása hozzájárul a szabályozási megfelelőséghez és a folyamatos javuláshoz [6] [12] [13] [14].

A validációs tervezés (VP) és a követelmény specifikáció (URS) két kritikus dokumentum a validálási folyamatban. Mindkettő elengedhetetlen a sikeres validáláshoz, de különböző célokat szolgálnak és eltérő információkat tartalmaznak [6] [13] [14].

5. A SZÁMÍTÓGÉPES RENDSZER VALIDÁLÁS FOLYAMATA A GYÓGYSZERIPARBAN



2. ábra: Számítógépes rendszer validálási folyamata

5.1 Követelmény Specifikáció (User Requirements Specification - URS)

A követelmény specifikáció (URS) egy olyan dokumentum, amely részletesen leírja a felhasználó vagy az üzleti igényeket egy adott rendszerrel, berendezéssel, szoftverrel vagy folyamattal kapcsolatban. Ez a dokumentum a megrendelő vagy a felhasználó szemszögéből fogalmazza meg, hogy mit vár el a validálandó entitástól.

A URS fő célja, hogy egyértelmű és érthető módon rögzítse a felhasználói elvárásokat, ezáltal alapot teremtve a tervezéshez, fejlesztéshez, beszerzéshez és végső soron a validáláshoz. Segít elkerülni a félreértéseket és biztosítja, hogy a megvalósított rendszer vagy folyamat megfeleljen a felhasználói igényeknek.

Az URS a validálási folyamat alapja. Meghatározza, hogy mit kell validálni, és milyen kritériumok alapján fogjuk megállapítani, hogy a validálás sikeres volt-e. A validálási tesztek és protokollok a URS-ben rögzített követelményekre épülnek [6] [13] [14].

5.2 Validációs Tervezés (Validation Plan – VP)

A validációs tervezés (VP) egy átfogó dokumentum, amely leírja a teljes validálási megközelítést és a végrehajtandó validálási tevékenységeket egy adott rendszerre, berendezésre, szoftverre vagy folyamatra vonatkozóan. Ez a dokumentum a validálási folyamat "útitervének" tekinthető [6] [13] [14].

A VP fő célja, hogy strukturált és dokumentált módon megtervezze és irányítsa a validálási folyamatot. Biztosítja, hogy a validálás megfelelően legyen megtervezve, végrehajtva, dokumentálva és jóváhagyva. Segít a validálási erőfeszítések hatékony kezelésében és a szabályozási követelményeknek való megfelelésben [6] [8] [13].

A VP szorosan kapcsolódik a URS-hez. A URS határozza meg *mit* kell validálni (a felhasználói igényeket), míg a VP leírja *hogyan* fogjuk validálni (a validálási megközelítést és a végrehajtandó tevékenységeket). A VP-ben meghatározott validálási kritériumoknak közvetlenül a URS-ben rögzített követelményekre kell hivatkozniuk [6] [13].

A VP biztosítja, hogy a validálási folyamat szervezett, átlátható és következetes legyen. Segít elkerülni a validálási tevékenységek véletlenszerűségét és biztosítja, hogy minden kritikus aspektus megfelelően legyen validálva [6] [13] [14].

Összehasonlítás és összegzés

Mind a validációs tervezés (VP), mind a követelmény specifikáció (URS) elengedhetetlen a sikeres validáláshoz. A URS lefekteti a validálás alapját azáltal, hogy egyértelműen meghatározza a felhasználói elvárásokat, míg a VP biztosítja, hogy ezek az elvárások megfelelően legyenek validálva egy strukturált és dokumentált folyamat keretében. A két dokumentum szorosan együttműködik, és egymásra épülve biztosítják a validált rendszer vagy folyamat megfelelőségét [6] [12] [13] [14].

A rendszertervezés és -fejlesztés validálása tipikusan négy fő kvalifikációs lépésen keresztül történik: Tervezési Kvalifikáció (Design Qualification - DQ), Telepítési Kvalifikáció (Installation Qualification - IQ), Működési Kvalifikáció (Operational Qualification - OQ) és Teljesítmény Kvalifikáció (Performance Qualification - PQ). Ezek a lépések biztosítják, hogy a rendszer a tervezett módon működjön és megfeleljen az előre meghatározott követelményeknek [6] [13] [14].

1. táblázat: URS és VP összehasonlítása

Jellemző	Követelmény Specifikáció (URS)	Validációs Tervezés (VP)
Fókusz	A felhasználói és üzleti igények leírása.	A validálási folyamat megtervezése és irányítása.
Tartalom	Funkcionális és nem funkcionális követelmények, adatkövetelmények.	Validálási stratégia, kritériumok, tesztelési stratégia, felelősségek.
Cél	Az elvárások egyértelmű rögzítése.	A validálás szervezett és dokumentált végrehajtásának biztosítása.
Időpont a folyamatban	A validálási folyamat elején készül.	A URS elkészülte után, a validálás megkezdése előtt készül.
Kinek szól?	Elsősorban a fejlesztőknek, beszállítóknak és validálóknak.	Elsősorban a validálási csapatnak és a menedzsmentnek.
Alapja minek?	Felhasználói és üzleti igények, jogszabályok.	URS, kockázatértékelés, szabályozási követelmények.

A DQ, IQ, OQ és PQ egymásra épülő lépések. A DQ biztosítja a megfelelő tervezést, az IQ a helyes telepítést, az OQ a megfelelő működést a kritikus tartományban, míg a PQ a hosszú távú, üzemi körülmények közötti megbízható teljesítményt igazolja. Mindegyik lépés dokumentált bizonyítékot szolgáltat a rendszer alkalmasságára vonatkozóan [6] [13] [14].

A rendszertervezés és -fejlesztés validálásának ezen lépései (DQ, IQ, OQ, PQ) elengedhetetlenek annak biztosításához, hogy a rendszer megfeleljen a felhasználói igényeknek, a specifikációknak és a vonatkozó szabályozásoknak. A lépésenkénti végrehajtás és a részletes dokumentáció garantálja a rendszer minőségét és megbízhatóságát [6] [13] [14].

6. HOGYAN VALÓSÍTHATÓ MEG HATÉKONYAN AZ IQ EGY ICP-OES BERENDEZÉS ESETÉN?

Az alábbi lépések egy Induktívan Csatolt Plazma Optikai Emissziós Spektrométer (ICP-OES) számítógépes rendszerének validálási folyamatából az IQ-t mutatja be egy magyarországi gyógyszeripari minőségellenőrző laboratórium kapcsán. Az ICP-OES egy analitikai műszer, amelyet elemi összetétel meghatározására használnak különböző mintákban. A rendszer magában foglalja magát a spektrométert, a hozzá tartozó számítógépet, az adatgyűjtő és -feldolgozó szoftvert, valamint a jelentéskészítő funkciókat. A gyógyszeriparban a megbízható és pontos analitikai eredmények elengedhetetlenek, ezért a rendszer validálása kritikus fontosságú a termékminőség biztosítása és a hatósági előírásoknak való megfelelés szempontjából.

Az IQ során annak bizonyítására került sor, hogy az ICP-OES rendszer és a hozzá tartozó számítógépes komponensek a jóváhagyott tervek és specifikációk szerint lettek telepítve. A számítógépes rendszerre vonatkozóan az IQ lépései tartalmazták:

- **A számítógép és perifériák ellenőrzése:** Ellenőriztem, hogy a szállított számítógép és annak perifériái megfelelnek-e a specifikációban leírtaknak.

- **A szoftver telepítésének ellenőrzése:** Mind az operációs rendszer mind pedig az ICP-OES-hez tartozó szoftverek esetében végrehajtottam a gyártói leírásoknak megfelelően a telepítési folyamatokat.

- **Hálózati kapcsolat ellenőrzése:** Beállításra került a számítógép és a spektrométer közötti, valamint a laboratóriumi hálózattal való megfelelő hálózati kapcsolat.

- **Hozzáférés-szabályozás konfigurációjának ellenőrzése:** Megoldásra került, hogy a felhasználói fiókok és a hozzáférési jogosultságok a tervek szerint legyenek implementálva.

- **Adatállományok mentésének ellenőrzése:** Az adatmentést az előírásoknak megfelelően automatizáltam a szabályozói előírásoknak megfelelően.

7. SZÁMÍTÓGÉPES BEÁLLÍTÁSOK, RENDSZERKÖVETELMÉNYEK ÉS TECHNIKAI KONFIGURÁCIÓK

7.1 A számítógép és perifériák ellenőrzése

Az ICP-OES műszer számítógépes rendszerének validálása során első lépésként az URS-ben (User Requirements Specification) rögzített elvárások alapján ellenőriztem, hogy a készülékhez mellékelt számítógép megfelel-e a gyártó által előírt követelményeknek. Ennek részeként meg kellett vizsgálnom, hogy a számítógép rendelkezik-e minden olyan hardveres elemmel és interfésszel, amelyek elengedhetetlenek a spektrométer és a számítógépes vezérlőszoftver közötti stabil kommunikáció biztosításához.

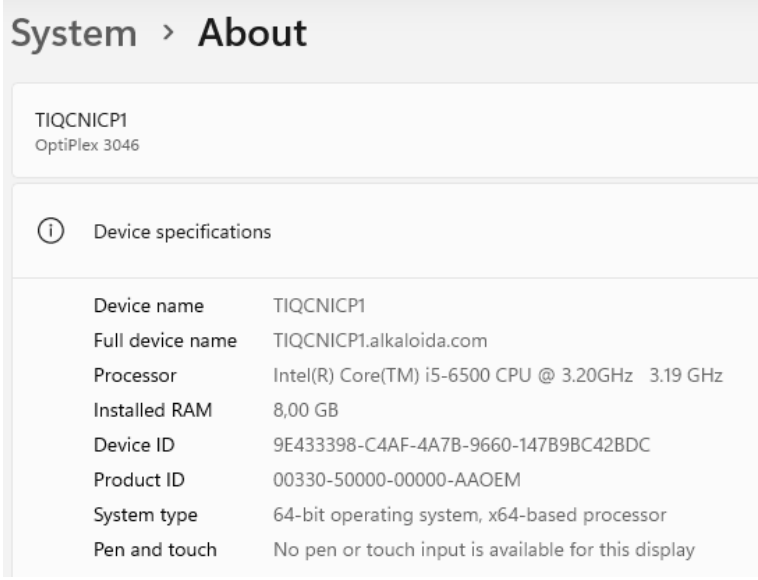
Ezenfelül részletesen átvizsgáltam a számítógép hardveres felszereltségét annak érdekében, hogy megfelel-e a gyártó által előírt minimális rendszerkövetelményeknek. A vizsgálat kiterjedt a központi egység (CPU), a memória (RAM), a háttértár (HDD/SSD), a grafikus és kommunikációs interfészek meglétére, valamint a hálózati illeszkedésre.

2. táblázat: ICP-OES-hez kapcsolt számítógép minimum rendszerkövetelményei

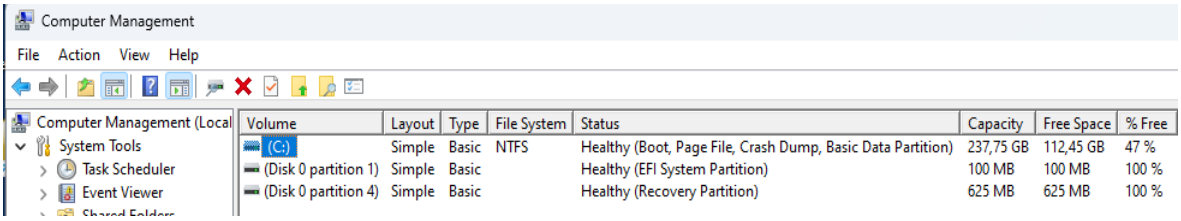
Processzor	Intel Core i5-6500 3.20 GHz
Memória	8 GB
Szabad lemezterület	100 GB
Képernyő felbontás	Minimum 1024 x 768 32bit colour screen resolution, or higher
Hálózat	10/100Mbps Ethernet
Bővíthetőség	2 PCI slots
Csatlakozási lehetőségek	2 x USB 2.0 port 2 x RJ-45 LAN port

A hardveres megfelelőség mellett elengedhetetlen volt annak is a felmérése, hogy a számítógép képes-e illeszkedni a laboratórium informatikai infrastruktúrájába. Ez magában foglalta a helyi hálózati követelményeknek való megfelelést, illetve a rendszerbiztonsági előírások – például a domain-integráció, tűzfal- és GPO-beállítások – teljesülésének vizsgálatát is.

A gyártó által meghatározott minimális hardverkövetelményeket az 1. táblázat tartalmazza.



3. ábra: ICP-OES-hez kapcsolt számítógép hardverkövetelménye



4. ábra: ICP-OES-hez kapcsolt számítógép HDD kapacitása

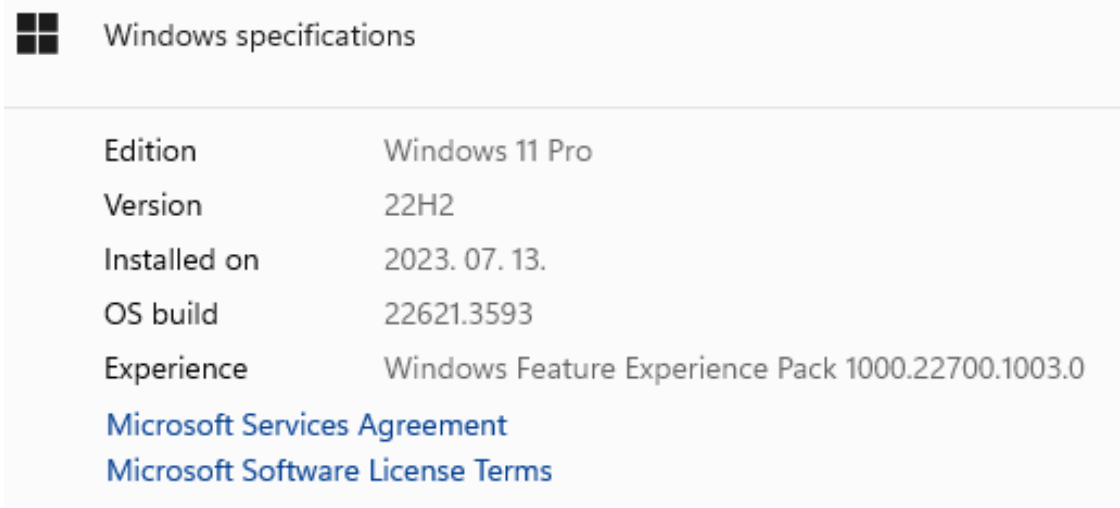
Az ICP-OES laborberendezéshez kapott számítógép hardver specifikációjának ellenőrzését követően (3.ábra) (4.ábra) a következő megállapítást tettem. a rendszerhez tartozó fizikai komponensek megfelelnek a gyártói specifikációknak és az URS-ben rögzített követelményeknek. Ennek megfelelően a validálási folyamat a következő szakaszba léphet, amely az operációs környezet és a szoftverkomponensek telepítésére és konfigurációjára fókuszál.

7.2 A szoftver telepítésének ellenőrzése

A fizikai komponensek megfelelőségének igazolását követően sor került az operációs rendszer és az alkalmazott szoftverek telepítésére. Ez a lépés az Installation Qualification (IQ) egyik kulcsfontosságú része, mivel ezen környezeti tényezők stabil és validált működése biztosítja a laboratóriumi rendszer teljes funkcionalitását.
Az operációs rendszer tekintetében a gyártó az alábbi minimális követelményként határozta meg a támogatott környezetet:

Microsoft Windows 10 Pro (Service Pack 1), 64 bites verzió.

A számítógépre Microsoft Windows 11 Pro, 64 bites verziójú operációs rendszert telepítettem (5.ábra), amely igazodik a gyógyszergyár vállalati informatikai környezetének elvárásaihoz.



5. ábra: Az ICP-OES számítógépen futó operációs rendszer típusa

A kiválasztás és telepítés során vizsgált szempontok:

- A Windows 11 Pro verzió illeszkedik a vállalat központi hálózati struktúrájába, támogatja a domain tagságot és a cég által alkalmazott GPO-házirendek végrehajtását.
- A rendszer jogtiszta, megfelelően aktivált és frissített állapotban került beüzemelésre.

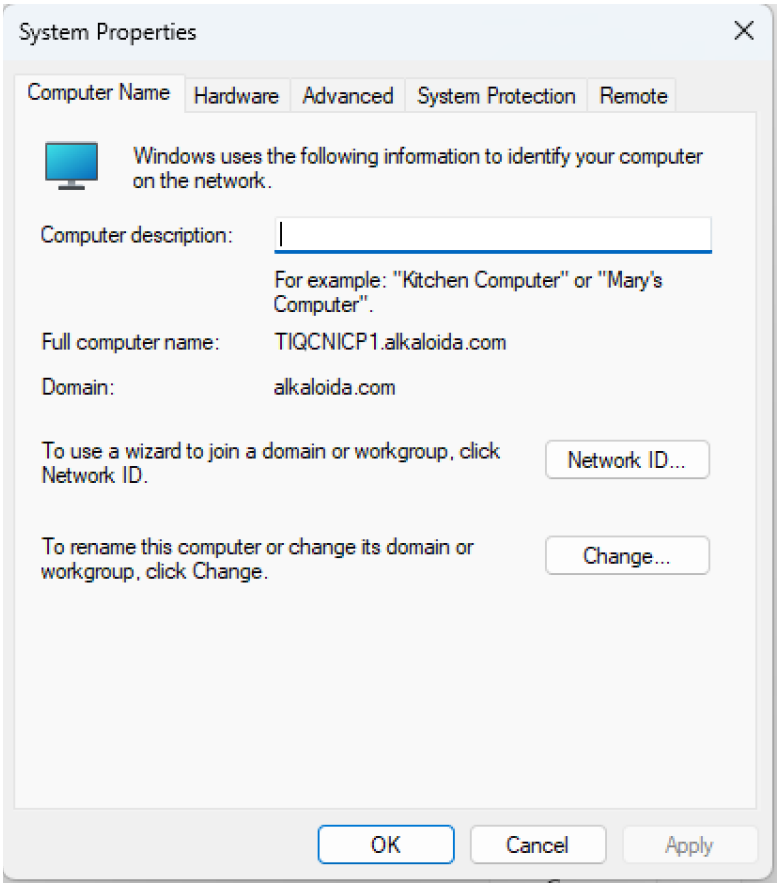
- A szükséges biztonsági frissítések telepítve lettek, a Windows Update szolgáltatás aktív.
- A hálózati szolgáltatások, tűzfalbeállítások, valamint az audit naplózási lehetőségek a GMP-előírások szerint lettek konfigurálva.
- A Microsoft Windows 11 Pro rendszer kompatibilis volt az Agilent ICP Expert CFR szoftverrel, nem jelentkezett inkompatibilitás vagy stabilitási probléma a telepítés során (6. ábra).

6. ábra: ICP Expert CFR szoftver működése

7.3 Hálózati beállítások

Az URS-ben rögzített követelmények alapján a rendszer hálózati beállításainak kialakításakor két kiemelt szempontot kellett figyelembe vennem: egyrészt a hálózati nyomtatási funkciók biztosítását, másrészt a felhasználók egyedi azonosításon alapuló hitelesítését a számítógépre történő bejelentkezés során.

Ezen követelmények teljesítéséhez különböző megoldási lehetőségeket mérlegeltem. A legbiztonságosabb és hosszú távon leginkább fenntartható megoldásként azt választottam, hogy a számítógépet beléptetem a vállalat központi tartománykezelő rendszerébe (7. ábra).



7. ábra: A számítógép domain-be történő beléptetésének igazolása

A tartományhoz való csatlakozás számos előnyt biztosított:

- Lehetővé tette a központi felhasználókezelést, ahol minden felhasználó egyedi azonosítóval és jogosultsági szinttel fér hozzá a rendszerhez,
- Hozzáférhetővé váltak a hálózati nyomtatók, így az URS-ben szereplő nyomtatási követelmény is teljesült,
- Elérhetővé váltak a megosztott vállalati erőforrások, fájlszerverek, mentési helyek, és központilag szabályozott GPO-házirendek,
- Biztosított lett az adatintegritás és nyomon követhetőség, mivel minden bejelentkezés naplózásra került.

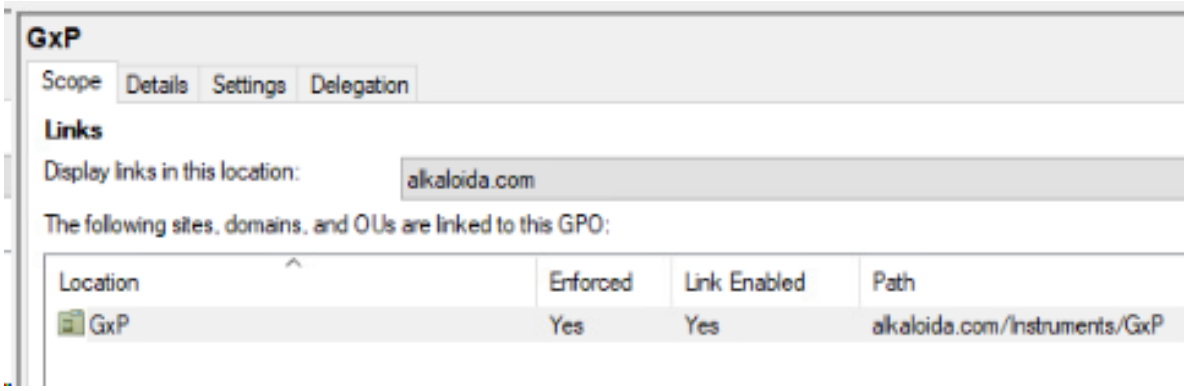
A domainbe történő integráció egyúttal alapot adott a validálási folyamat további lépéseihez is, különös tekintettel a GxP-követelmények szerinti audit trail, hozzáférés-ellenőrzés és adatbiztonság kialakítására.

7.4 Hozzáférés-szabályozás konfigurációjának ellenőrzése

A számítógép megfelelő tartományba történő integrálását követően egyértelművé vált számomra, hogy az URS-ben rögzített hozzáférés-szabályozási elvárások leghatékonyabban a tartománykezelő (Domain Controller) által biztosított Group Policy Object (GPO) alapú szabályzással valósíthatók meg.

Ez a megközelítés lehetővé teszi a felhasználói jogosultságok, biztonsági beállítások, naplózás és adatvédelem központi és egységes kezelését, valamint biztosítja a rendszer auditálhatóságát és megfelelőségét a GMP-környezetben elvárt adatintegritási elveknek.

A beállítások megvalósításának első lépése a célzott házirendobjektum (Group Policy Object – GPO) létrehozása volt (8.ábra) a vállalat tartományvezérlő rendszerében. Az új GPO a számítógép biztonsági és hozzáférés-kezelési beállításainak központosított szabályozására szolgált, összhangban az URS-ben rögzített validálási követelményekkel.

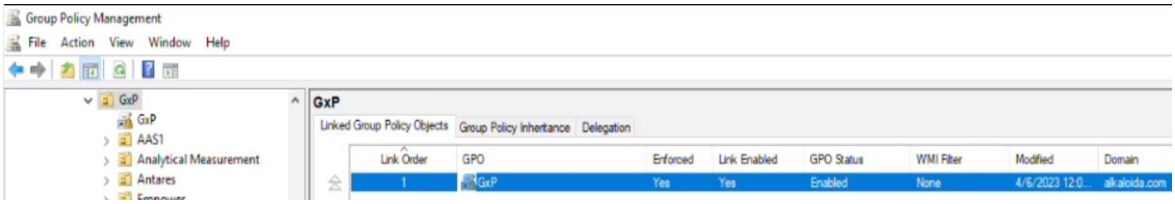


8. ábra: Új GPO létrehozása

A létrehozott GPO-t ezt követően hozzárendeltem ahhoz a számítógépcsoporthoz, amely az ICP-OES rendszerhez kapcsolódó eszközt és annak vezérlésére használt számítógépet tartalmazta (9.ábra). A csoportos hozzárendelés lehetővé tette, hogy a házirend csak az érintett eszközökre érvényesüljön, elkerülve ezzel a vállalati tartomány többi gépére gyakorolt nem kívánt hatásokat.

A létrehozott házirendben számos paraméter került meghatározásra, amelyek a felhasználói munkakörnyezet megjelenését és működését szabályozzák. Ezek közé tartozott többek

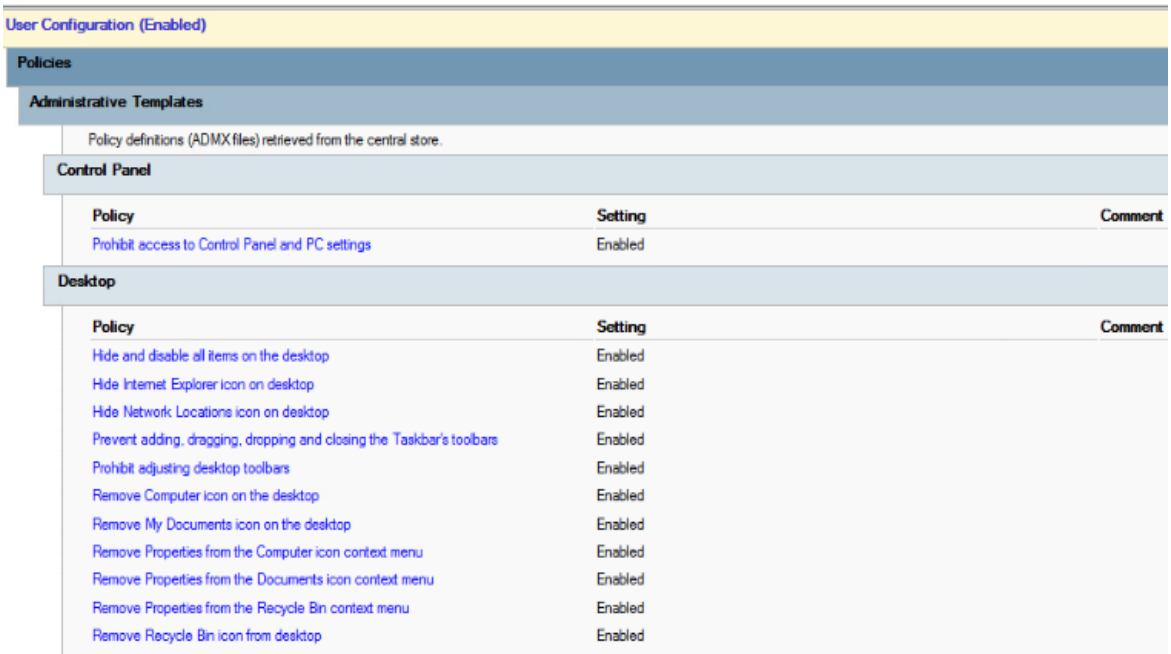
között a felhasználói bejelentkezést követően elérhető Vezérlőpult- és asztalfunkciók korlátozása (10. ábra), valamint a Start menü viselkedésére és tartalmára vonatkozó szabályozások beállítása (11. ábra).



9. ábra: GPO hozzárendelése a számítógépcsoporthoz

A beállítások megalkotásakor kiemelt szempont volt, hogy a felhasználók kizárólag azokhoz az alkalmazásokhoz és rendszerfunkciókhoz férjenek hozzá, amelyek elengedhetetlenek az általuk végzett validált tevékenységhez.

Ennek érdekében a házirend segítségével biztosítottam, hogy minden egyes szerepkörhöz (pl. operátor, megfigyelő) csak az URS-ben előírt jogosultságokkal és hozzáférési lehetőségekkel rendelkező munkakörnyezet jelenjen meg (12. ábra).



10. ábra: Vezérlőpulti és asztali szabályozások

Desktop/Desktop		
Policy	**Setting**	**Comment**
Prohibit adding items	Enabled	
Prohibit changes	Enabled	
Prohibit closing items	Enabled	
Prohibit deleting items	Enabled	
Prohibit editing items	Enabled	
Start Menu and Taskbar		
Policy	**Setting**	**Comment**
Add Logoff to the Start Menu	Enabled	
Force classic Start Menu	Enabled	
Prevent changes to Taskbar and Start Menu Settings	Enabled	
Prevent users from adding or removing toolbars	Enabled	
Prevent users from customizing their Start Screen	Enabled	
Prevent users from resizing the taskbar	Enabled	
Remove access to the context menus for the taskbar	Enabled	
Remove All Programs list from the Start menu	Enabled	
Choose one of the following actions	Remove and disable setting	

11. ábra: Asztali és Start menüre vonatkozó szabályozások

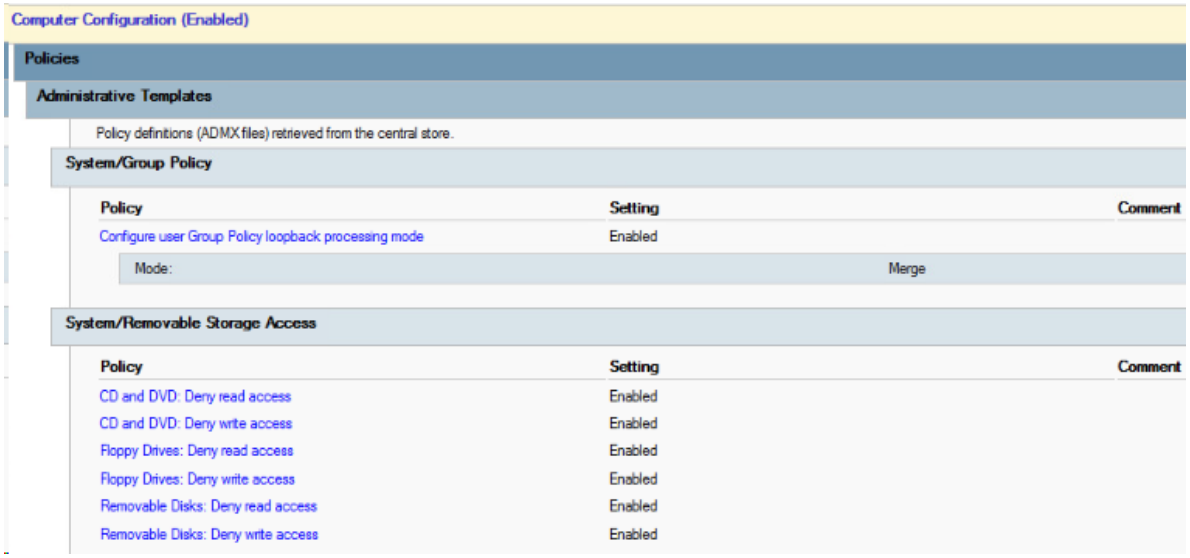
Policy	Setting	Comment
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Enabled	
Remove Balloon Tips on Start Menu items	Enabled	
Remove common program groups from Start Menu	Enabled	
Remove Default Programs link from the Start menu.	Enabled	
Remove Documents icon from Start Menu	Enabled	
Remove Favorites menu from Start Menu	Enabled	
Remove frequent programs list from the Start Menu	Enabled	
Remove Games link from Start Menu	Enabled	
Remove Help menu from Start Menu	Enabled	
Remove links and access to Windows Update	Enabled	
Remove Music icon from Start Menu	Enabled	
Remove Network Connections from Start Menu	Enabled	
Remove Network icon from Start Menu	Enabled	
Remove Pictures icon from Start Menu	Enabled	
Remove pinned programs from the Taskbar	Enabled	
Remove Recent Items menu from Start Menu	Enabled	
Remove Run menu from Start Menu	Enabled	
Remove Search Computer link	Enabled	
Remove Search link from Start Menu	Enabled	
Turn off all balloon notifications	Enabled	
Turn off personalized menus	Enabled	

12. ábra: Alkalmazásokra, ikonokra és figyelmeztetésekre vonatkozó szabályok

Kiemelt figyelmet fordítottam a házirenden belül az USB-eszközök használatának korlátozására (13.ábra), mivel az adatintegritás fenntartása és a rendszer potenciális sebezhetőségének csökkentése szempontjából ez kritikus jelentőségű. Az eltávolítható

adathordozók engedély nélküli használata súlyos kockázatot jelenthet a GMP-környezetben, hiszen nem dokumentált adatmozgatás, külső vírusforrások, vagy a mérésekhez tartozó fájlok nem megfelelő kezelése is előfordulhat.

A konfigurált szabályozás segítségével a felhasználók számára alapértelmezetten tiltottá vált az USB-portokon keresztüli adathozzáférés, kivéve azokat az eszközöket, amelyeket a rendszeradminisztrátor vagy a minőségbiztosítás külön engedélyezett. Ez a beállítás jelentősen hozzájárult a laboratóriumi számítógépes rendszer informatikai integritásának és validált működésének biztosításához, megfelelve a GMP-előírásokban és az EU GMP Annex 11-ben megfogalmazott szigorú adatintegritási követelményeknek.



13. ábra: Külső adathordozó használatának tiltására vonatkozó szabályzás

Az utolsó, kiemelésre érdemes szabályozás a programfuttatási jogosultságok korlátozására vonatkozik. Ennek célja, hogy a bejelentkezett felhasználók kizárólag a validált rendszer működéséhez szükséges, előzetesen engedélyezett alkalmazásokat használhassák.

A kialakított beállítások értelmében a rendszerre bejelentkező felhasználóknak nincsen jogosultságuk tetszőleges program vagy adatállomány végrehajtására, sem lokális, sem hálózati forrásból. Ez különösen fontos a GMP-szabályozás alatt működő informatikai környezetekben, ahol minden nem kontrollált futtatás adatintegritási, biztonsági vagy funkcionális kockázatot jelenthet (14.ábra).

System		
Policy	**Setting**	**Comment**
Prevent access to registry editing tools	Enabled	
Disable regedit from running silently?	Yes	
Policy	**Setting**	**Comment**
Prevent access to the command prompt	Enabled	
Disable the command prompt script processing also?	No	
System/Ctrl+Alt+Del Options		
Policy	**Setting**	**Comment**
Remove Task Manager	Enabled	
Windows Components/File Explorer		
Policy	**Setting**	**Comment**
Display the menu bar in File Explorer	Enabled	
Do not allow Folder Options to be opened from the Options button on the View tab of the ribbon	Enabled	
Do not move deleted files to the Recycle Bin	Enabled	
Hide these specified drives in My Computer	Enabled	
Pick one of the following combinations	Restrict all drives	

14. ábra: Programfuttatási jogosultságokra vonatkozó szabályzás

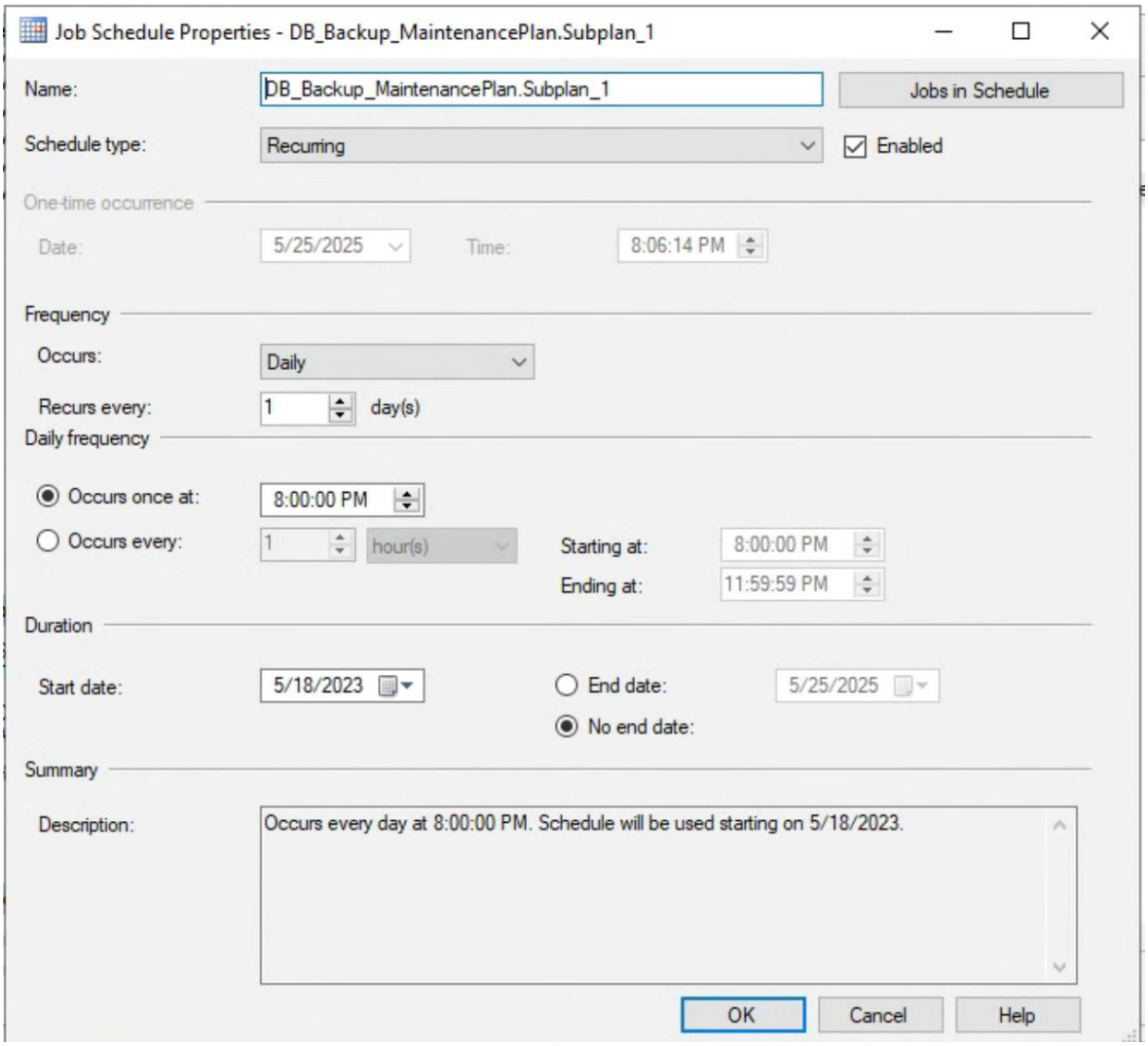
7.5 Adatmentés és archiválás

A mentési stratégia meghatározásakor elsődleges szempontként azt vizsgáltam meg, hogy az ICP-OES műszerhez tartozó Agilent ICP Expert szoftver milyen módon kezeli és tárolja az adatokat. A rendszer működéséből adódóan a szoftver minden felhasználói adatot, mérési eredményt, beállítási konfigurációt és log fájlt egy SQL adatbázisban tárol, amely a számítógépen lokálisan futó Microsoft SQL Server példányon keresztül működik.
A szoftver architektúrájának és az adatkezelési elveinek áttekintése alapján megállapítottam, hogy a telepített SQL Server példány támogatja az időzített automatikus adatbázismentést, mely során a teljes adatbázis-tartalom egy előre definiált struktúrában és formátumban (.bak fájlban) kerül lementésre egy előre kijelölt könyvtárba.

A lokálisan futó SQL Server Express által naponta generált .bak kiterjesztésű adatbázismentési állományokat automatizáltan kellett átmozgatni a központi szerverre, ahonnan – a vállalati szabályozás szerint – az adatok további redundáns archiválása történik mágnesszalagos tárolóra (tape backup). Ez a gyakorlat kiemelten fontos a gyógyszeripari környezetben, ahol a mérési és rendszeradatok megőrzése hosszú távra kötelező.

Ezen lehetőséget kiaknázva olyan megoldást választottam, amelyben az SQL Server natív mentési mechanizmusát használom a napi szintű adatmentés biztosítására. A konfiguráció során:

- létrehoztam egy automatizált feladatot az SQL Server Agent segítségével, amely naponta mentést készít az ICP-OES által használt adatbázisról (14.ábra)
- a mentések célhelyét egy védett, lokális mappára állítottam be (D:\ICP_Database_Backups\),
- az adatbázis kezelő által mentett fájlokat egy batch szkript segítségével másoltam fel a vállalati előírásoknak megfelelően egy központi szerverre,
- a teljes folyamatot automatizáltam a Windows Task Scheduler segítségével



15. ábra: SQL adatbázis automatikus napi mentés létrehozása

Az SQL Server által generált .bak kiterjesztésű mentési fájlok napi archiválása és központi szerverre való biztonságos átmásolása érdekében az alábbi batch szkriptet készítettem:

```
„echo on
For /f "tokens=1,2,3,4,5 delims=/. " %%a in ('date/T') do set
CDate=%%a_%%b_%%c%%d
echo Date: %CDate%
mkdir
"\\tisfsbck4\d$\DATABACKUP\MEFO\second_floor\tiqcnicp1\Backup
\%CDate%"
echo Folder created!
echo SET logfile:
SET
LOGFILE="\\tisfsbck4\d$\DATABACKUP\MEFO\second_floor\tiqcnicp
1\Backup\%CDate%\log_%CDate%.txt"
call :Logit >> %LOGFILE%
exit /b 0
:Logit
echo zipping Database_backup...
"\\tisfsbck4\d$\scripts\7-Zip\7z.exe" a -tzip
"\\tisfsbck4\d$\DATABACKUP\MEFO\second_floor\tiqcnicp1\Backup
\%CDate%\icp1_database.zip"
"\\tiqcnicp1\d$\Database_backup\ICP1"
echo Done!”
```

A mentési folyamat automatizálására írt batch szkript célja, hogy biztosítsa a rendszeres, dokumentált és biztonságos adatmentést a validált rendszerhez kapcsolódó SQL adatbázisról. A szkript működése egyszerű, de megbízható logikai lépések mentén épül fel, és teljes egészében a Windows operációs rendszer beépített parancssori eszközeire, valamint PowerShell-funkcionalitására épül.

Az általam elkészített szkript működése az alábbi elven alapul:

1. Dátumbélyeg képzése

   A szkript első lépésként az aktuális dátum alapján előállít egy formázott YYYYMMDD típusú dátumbélyeget, amelyet a tömörített fájl nevében fog használni. Ez biztosítja, hogy minden mentési fájl egyértelműen azonosítható legyen a létrehozás dátuma alapján:

   ```
   For /f "tokens=1,2,3,4,5 delims=/. " %%a in ('date/T')
   do set CDate=%%a_%%b_%%c%%d
   ```

2. Létrehoz egy új mappát az adott napi mentéshez

   A hálózati meghajtón (\\tisfsbck4\d$...) készít egy új mappát a CDate (aznapi dátum) alapján:

   ```
   mkdir
   \\tisfsbck4\d$\DATABACKUP\MEFO\second_floor\tiqcnicp1\Ba
   ckup\%CDate%
   ```

3. Előkészíti a naplófájlt

   Létrehoz egy naplófájlt az újonnan létrehozott mappába:

   ```
   SET
   LOGFILE=\\tisfsbck4\d$\DATABACKUP\MEFO\second_floor\tiqc
   nicp1\Backup\%CDate%\log_%CDate%.txt
   ```

4. Hívja a Logit szubrutin-t, és a naplófájlba irányítja a kimenetet

   Lefuttatja a Logit nevű rész-szkriptet, és annak minden kimenetét (üzenetét) a naplófájlba írja.

   ```
   call :Logit >> %LOGFILE%
   ```

5. Szkript vége

   A fő szkript itt befejeződik.

   ```
   exit /b 0
   ```

6. Logit szubrutin – a tényleges mentés

   Felírja a naplóba, hogy elkezdi a Database_backup mappát tömöríteni.

Elindítja a 7-Zip programot (a hálózati helyen lévő 7z.exe futtatásával), ami a „Database_backup\ICP1” mappát egy zip-fájlba tömöríti (icp1_database.zip néven) az aznapi mappába.
Ha kész, „Done!” üzenetet ír.

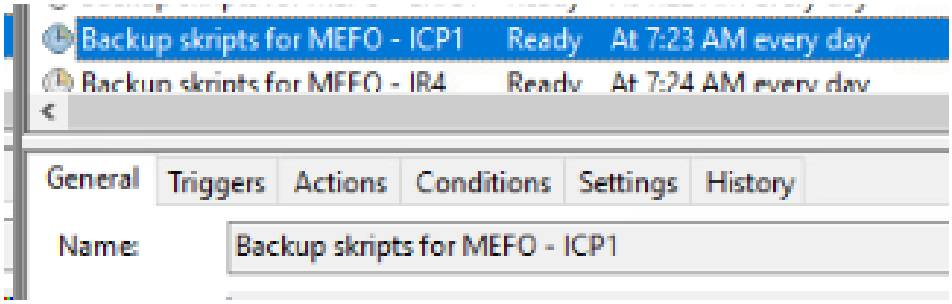
```
:Logit
echo zipping Database_backup...
"\\tisfsbck4\d$\scripts\7-Zip\7z.exe" a -tzip
"\\tisfsbck4\d$\DATABACKUP\MEFO\second_floor\eric1\Backu
p\%CDate%\thermo.zip" "\\tiqcneric1\c$\Program Files
(x86)\Thermo"
echo Done!
```

A batch szkript napi szintű, felhasználói beavatkozástól mentes futtatásának érdekében a Windows Task Scheduler (Feladatütemező) eszközt használtam. A cél az volt, hogy a mentési folyamat minden nap ugyanabban az időpontban automatikusan lefusson, biztosítva ezzel a konzisztens adatmentést és az adatintegritási elvárások teljesülését.

A feladat beállítása a következő lépések alapján történt.

1. Feladat létrehozása

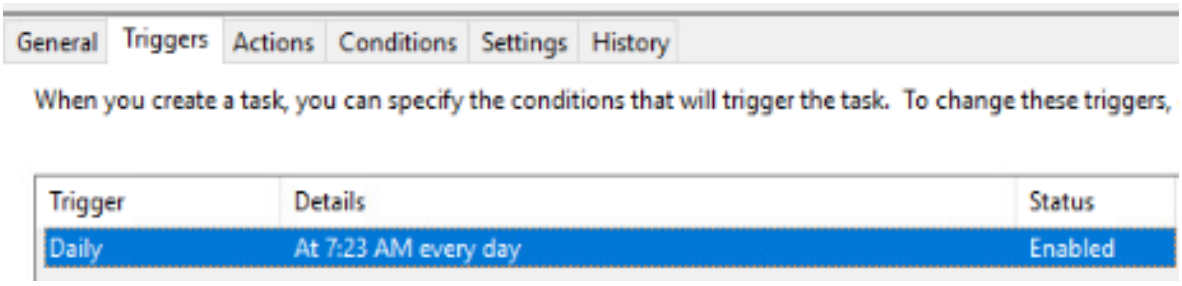
- A „Feladatütemező” (Task Scheduler) konzolban új feladatot hoztam létre (15.ábra)
- Beállítottam, hogy a feladat legmagasabb jogosultsággal fusson, hogy a rendszerfájlokhoz és hálózati erőforrásokhoz is hozzáférhessen.



16. ábra: Windows Task létrehozása a Schedulerben

2. Trigger (időzítés) beállítása

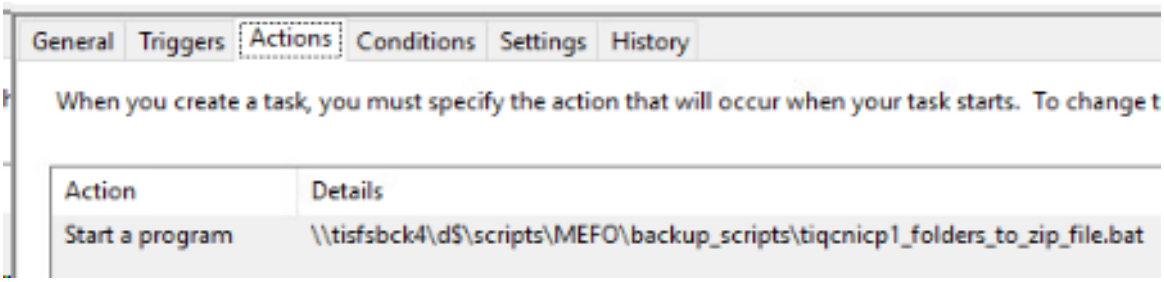
- A „Trigger” fülön napi futtatási ciklust állítottam be.
- Időpontként 07:23 lett meghatározva, amikor még nem folyik munkavégzés.
- A futtatás ismétlése naponta történik, határozatlan ideig.



17. ábra: A batch szkript napi szintű futtatásának beállítása

3. Action (művelet) beállítása

- A „Művelet” típusnál „Program indítása” lett kiválasztva.
- A Program/script mezőbe a .bat fájl pontos elérési útját adtam meg (\\tisfsbck4\d$\scripts\MEFO\backup_scripts\tiqcnicp1_folders_to_zip_file.bat).



18. ábra: A bacth szkript file futtatásának beállítása

4. Beállítások és viselkedés

- Engedélyeztem, hogy a feladat akkor is fusson, ha a felhasználó nincs bejelentkezve.
- A hiba esetén történő újra próbálkozás lehetőségét is aktiváltam.
- A futás naplózása a backup_log.txt fájlban történik, ami a későbbi audit során visszakereshető.

Ez a megoldás biztosítja, hogy a mentési folyamat teljesen automatizált, emberi

beavatkozástól mentes és dokumentált legyen – megfelelve a GMP környezetben elvárt folyamatbiztonságnak és átláthatóságnak. Ez a megközelítés lehetővé teszi az adatok visszakereshetőségét és helyreállíthatóságát, valamint megfelel az adatintegritásra vonatkozó GMP és GAMP® 5 elvárásoknak. A beállítás dokumentáltan, képernyőképekkel és mentési naplókkal együtt került archiválásra az IQ protokoll részeként.

A fenti folyamat bemutatja, hogy egy komplex analitikai műszer, mint az ICP-OES számítógépes rendszerének validálásának létfontosságú része az IQ. A gondosan megtervezett és végrehajtott beállítások biztosítják, hogy a rendszer megfelel a felhasználói igényeknek, a specifikációknak és a vonatkozó szabályozásoknak. Ezáltal a laboratórium megbízható és pontos analitikai eredményeket tud szolgáltatni, hozzájárulva a gyógyszeripari termékek minőségének biztosításához és a hatósági követelményeknek való megfeleléshez. A részletes dokumentáció pedig bizonyítja a validált állapotot és lehetővé teszi a rendszer későbbi karbantartását és a változások kezelését.

8. ELÉRT EREDMÉNYEK ÉS A TANULSÁGOK

A bemutatott folyamatban a gyógyszeripari minőségellenőrző laboratóriumban végrehajtott ICP-OES számítógépes rendszer validálása sikeresen lezárult, és számos fontos eredményt és tanulságot hozott.

8.1 Elért eredmények

- **A rendszer validált állapotának elérése:** Az IQ, OQ és PQ lépések sikeres végrehajtásával bizonyításra került, hogy az ICP-OES rendszer tervezése, telepítése, működése és teljesítménye megfelel az előre meghatározott felhasználói követelményeknek és a specifikációknak.
- **Megfelelőség a szabályozási követelményeknek:** A validálási folyamat során különös figyelmet fordítottam a gyógyszeriparban érvényes szabályozásoknak (pl. 21 CFR Part 11) való megfelelésre, így biztosítva a hatósági auditok sikeres teljesítését.
- **Jobb adatminőség és integritás:** A validálás során bevezetett kontrollok és eljárások hozzájárulnak az adatok minőségének és integritásának javulásához, csökkentve a hibák és a manipuláció kockázatát.
- **Hatékonyabb működés:** A validált rendszerrel a laboratóriumi munkafolyamatok hatékonyabbá válnak, mivel a rendszer megbízhatóan és következetesen működik.

Az ICP-OES rendszer sikeres validálása jelentős előnyökkel járt a gyógyszeripari minőségellenőrző laboratórium számára, biztosítva a megbízható analitikai eredményeket és a szabályozási megfelelőséget. A validálási folyamat során szerzett tapasztalatok és tanulságok értékesek lehetnek a jövőbeni validálási projektek tervezése és végrehajtása során is. A gondos tervezés, a szoros együttműködés, a részletes dokumentáció és a folyamatos karbantartás kulcsfontosságú a validált rendszerek hosszú távú működésének biztosításához.

ÖSSZEFOGLALÁS

A szakdolgozat a kockázatalapú validálás (RBV) elveit és alkalmazását vizsgálta, különös tekintettel egy konkrét számítógépes rendszer, az ICP-OES validálásának folyamatán keresztül fókuszálva az IQ-ra. A munka során bebizonyosodott, hogy a kockázatalapú validálás hatékony megközelítés a validálási folyamatok optimalizálására, amely lehetővé teszi az erőforrások célzott felhasználását a kritikus kockázatú területeken.

A szakdolgozat részletesen bemutatta a kockázatalapú validálás alapelveit, hangsúlyozva a kockázat azonosításának és értékelésének, a validálási erőfeszítések priorizálásának, a tudományos és adatvezérelt megközelítésnek, a teljes életciklus figyelembevételének, a dokumentáció fontosságának és a folyamatos fejlesztés elvének jelentőségét.

Az ICP-OES rendszer validálásán keresztül a szakdolgozat gyakorlati példával illusztrálta a validálási folyamat lépéseit egy komplex analitikai műszer esetében. Az elemzés rávilágított a felhasználói követelmények specifikációjának (URS) alapvető szerepére, valamint a tervezési, telepítési, működési és teljesítmény kvalifikációk egymásra épülő jellegére.

A szakdolgozat feltárta a validálási folyamat során felmerülő potenciális kihívásokat, mint például a nem egyértelmű követelmények, a tervezési hiányosságok, a telepítési problémák, a működési eltérések, a teljesítménybeli elégtelenségek, a dokumentációs hiányosságok, az erőforrás-szűkösség és a szabályozási megfelelés biztosításának nehézségei. Emellett a munka megoldási javaslatokat is kínált ezekre a kihívásokra, hangsúlyozva a proaktív tervezés, a kockázatértékelés, a szoros együttműködés és a részletes dokumentáció fontosságát.

Összességében a szakdolgozat megállapította, hogy a kockázatalapú validálás egy értékes és hatékony megközelítés a számítógépes rendszerek validálására a szabályozott iparágakban. Az ICP-OES rendszer esete jól illusztrálja a módszer gyakorlati alkalmazását és a belőle származó előnyöket, hangsúlyozva a gondos tervezés, a kockázatok figyelembevétele és a részletes dokumentáció nélkülözhetetlenségét a sikeres validálási projektekhez.

SUMMARY

This thesis examined the principles and application of risk-based validation (RBV), with a particular focus on a case study involving the validation of a specific computerized system, the ICP-OES, emphasizing the IQ (Installation Qualification) phase. The work demonstrated that risk-based validation is an effective approach for optimizing validation processes, enabling targeted use of resources in areas of critical risk.

The thesis presented the fundamental principles of risk-based validation in detail, highlighting the importance of risk identification and assessment, prioritization of validation efforts, scientific and data-driven approaches, consideration of the entire system lifecycle, the significance of documentation, and the principle of continuous improvement.

Through the case study of the ICP-OES system validation, the thesis provided a practical example of the validation process steps for a complex analytical instrument. The analysis emphasized the essential role of User Requirement Specifications (URS), as well as the interdependent nature of design, installation, operational, and performance qualifications.

The thesis identified potential challenges encountered during the validation process, such as unclear requirements, design deficiencies, installation issues, operational deviations, performance shortcomings, documentation gaps, limited resources, and difficulties in ensuring regulatory compliance. Furthermore, the thesis offered solutions to these challenges, emphasizing the importance of proactive planning, risk assessment, close collaboration, and thorough documentation.

In conclusion, the thesis found that risk-based validation is a valuable and efficient approach for validating computerized systems in regulated industries. The ICP-OES case study effectively illustrates the practical application and benefits of the methodology, underlining the necessity of careful planning, risk consideration, and comprehensive documentation for successful validation projects.

IRODALOMJEGYZÉK

[1] Kerekes Éva, Bánhegyi Gábor (2019): Gyógyszeripari minőségbiztosítás. Medicina Könyvkiadó Zrt., Budapest. ISBN: 9789632267306.

[2] Török Krisztina (2015): GMP kézikönyv. SpringMed Kiadó, Budapest. ISBN: 9789639929887.

[3] Jakabné dr. Bajzáth Ágnes (szerk.) (2012): Gyógyszeripari informatika és automatizálás. Debreceni Egyetem, Gyógyszerésztudományi Kar. https://dea.lib.unideb.hu/dea/bitstream/handle/2437/164096/gyogyszeripari_informatika_es_automatizalas.pdf

[4] Sinkó Zoltán (2012): A számítógépes rendszer validálása a gyógyszeriparban. Gyógyszerészet, 56. évf. 5. szám, 313-320. o. https://www.gyogyszeresztudomany.hu/cikkek/a-szamitogepes-rendszer-validalasa-a-gyogyszeriparban/

[5] OGYÉI: Gyógyszeripari informatikai rendszerek validálása – iránymutatás (2020) Országos Gyógyszerészeti és Élelmezés-egészségügyi Intézet (OGYÉI). https://www.ogyei.gov.hu/gyogyszeripari_informatikai_rendszerek_validalasa_iranymutatas

[6] ISPE (2022): GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems. 2nd Edition. International Society for Pharmaceutical Engineering, Tampa, FL. ISBN: 9781945584302. https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition

[7] U.S. Food and Drug Administration (FDA): 21 CFR Part 11 – Electronic Records; Electronic Signatures. (Title 21, Code of Federal Regulations, Part 11.) https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11

[8] European Commission: EudraLex – Volume 4 – Good Manufacturing Practice (GMP) Guidelines, Annex 11: Computerised Systems.
https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf

[9] World Health Organization (WHO): WHO Technical Report Series, No. 996, Annex 5: Guidance on Good Data and Record Management Practices (2016).
https://www.who.int/publications/m/item/trs996-annex5

[10] MHRA (2018): GxP Data Integrity Guidance and Definitions.
Medicines and Healthcare products Regulatory Agency, United Kingdom.
https://www.gov.uk/government/publications/gxp-data-integrity-guidance-and-definitions

[11] PIC/S PI 011-3: Good Practices for Computerised Systems in Regulated "GxP" Environments (2021).
Pharmaceutical Inspection Co-operation Scheme.
https://picscheme.org/en/publications?tri=publication_desc

[12] ICH Q9: Quality Risk Management (2005).
International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use.
https://database.ich.org/sites/default/files/Q9_Guideline.pdf

[13] Nash, R.A., & Wachter, A.H. (eds.) (2003): Pharmaceutical Process Validation: An International, 3rd Edition.
Marcel Dekker, New York. ISBN: 9780824740365.

[14] Zou, M.H., & King, K.A. (2017): Validation of Computerized Systems in Pharmaceutical Production.
Pharmaceutical Technology Europe, 29(8), 20-23.
https://www.pharmtech.com/view/validation-computerized-systems-pharmaceutical-production

[15] FDA (2007): Guidance for Industry: Computerized Systems Used in Clinical Investigations.
U.S. Food and Drug Administration.
https://www.fda.gov/media/85183/download

ÁBRAJEGYZÉK

TÁBLAJEGYZÉK