Szakdolgozat

Poncski Viktor

2025

Magyar Agrár- és Élettudományi Egyetem
Károly Róbert Campus
Vidékfejlesztés és Fenntartható Gazdaság Intézet
Gazdaságinformatikus alapképzési szak

Vállalati informatikai problémák és kihívások a Bosch környezetében

Belső konzulens: Dr. Zörög Zoltán
egyetemi docens

Belső konzulens intézete/tanszéke: Vidékfejlesztési és Fenntartható Gazdaság Intézet

Készítette: Poncski Viktor

Károly Róbert Campus
2025

Tartalomjegyzék

1. Bevezetés

Az informatika napjainkban a vállalatok működésének egyik legmeghatározóbb pillére. A digitalizáció, az automatizálás és az automata döntéshozatal olyan tényezők, amelyek nélkül egy modern nagyvállalat nem lehet versenyképes sokáig. A vállalati informatikai rendszerek megbízható működése, a biztonságos adatkezelés, valamint a folyamatos fejlesztés és karbantartás alapvető fontosságú a mindennapi operatív és stratégiai folyamatok szempontjából.

A hatvani Bosch gyáregységben 2021-ben csatlakoztam az IT-csapathoz, mint informatikus gyakornok. Számomra ez nagy lehetőség volt, ugyanis egy multinacionális cégnél rengeteg olyan informatikai központú feladat van, melyből sokat lehet tanulni. Gyakornokként megtanulhattam többek között a hálózati csatlakozó aljzatok (patchpanel) Switchel való összekötését, amit végpont aktiválásnak hívtunk. Ez egy nagyon nagy figyelmességet és pontosságot igénylő feladat volt, mivel a Switchen a patchkábel kötése közben aktív végberendezések működtek, melyek feladata mai napig is vevői partnereink kiszolgálása, a termékek gyártása. Ezen végberendezések általában beültetőgépek, csavarozók, kemencék, illetve egyéb automatizált gyártástámogató végeszközök voltak. A feladataim során sok tapasztalatot szereztem kommunikáció, hibaelhárítás, valamint olyan megoldások bemutatásával, amellyel az osztályunkon bizonyos folyamatokat rugalmasabban tudtunk kezelni.

2023-ban azt a lehetőséget kaptam, hogy informatikai karrieremet főállású pozícióban folytassam osztályunkon, amivel elindultam egy, akkor számomra ismertnek hitt úton. Mint kiderült, ahogy az élet is tartalmaz nekünk meglepetéseket, úgy sok olyan dologról hittem az IT világában, hogy már volt vele tapasztalatom, de az igazi munka és tanulás csak ezután következett. Felvilágosultam, hogy az IT mellett az ipari környezetben az OT (Gyártási Informatika) is szerepet tölt be, viszont ebbe még akkoriban nem volt tudomásom. Ekkor kezdtem el igazán megérteni, hogy feladatim és felelősségi köreim fokozatos bővülésével már nem csupán technikai támogatást nyújtok, hanem stratégiai szerepet is támogatok munkáimmal a gyártási, logisztikai, létesítménygazdálkodási, és egyéb folyamatokban.

Az egyre több felelősségi kör egyre több kihívásokat is jelent. Szükséges munkáim során is priorizálnom azokat a dolgokat, amikkel elsődlegesen szükséges foglalkoznom. A napi szinten előforduló IT problémák, legyen szó a 2004-ben megírt szoftverről, amit Windows 11-en akarnak futtatni, a hálózati hibákon át, a kiberbiztonsági incidensekig. A skála, mint láthatjuk igen széles, és ezen az osztályon monoton munkavégzésről szó sincs, hiszen törekednünk kell nem csak magunkat fejleszteni eközben, hanem figyelmet fordítani arra is, hogy környezetünk, ipari számítógépinket is korszerűsítsük, biztonságossá tegyük. Nincs idő lemaradásra, főleg egy olyan iparágban, ahol a verseny mellett fontos kihívás a pontosság, precizitása, és megfelelés a vevői követelmények számára, a cég portfóliójának növelése érdekében.

A vállalatban lévő informatika rendszerek tehát nem maradhat le a napjainkban szükséges elvárásoktól. Ezen rendszerek fejlesztése nem csupán technológiai kérdés, hanem a folyamatos alkalmazkodás is a piaci igényekhez. Dolgozatomban saját szakmai tapasztalataimra és példákra támaszkodva mutatom be, miként lehet a mindennapi általános működés során felmerülő problémákat hatékonyan kezelni, és miként tudunk hozzájárulni, hogy kialakuljon lépésről lépésre egy stabil, biztonságos és jövőálló IT-s háttér egy vállalatnál.

1.1 A témaválasztás indoklása

Az informatika még a 2000-es évek elején gyerekcipőben járt, s a robbanásszintű térhódításával nagyon nehéz lépést tartani. Egyik pillanatról a másikra alakultak át rendszerek, fejlődtek alkalmazások és adatbázisok, és mindezekkel együtt létrejöttek az automata rendszereken alapuló, mesterséges intelligenciát használó robotok, biztonsági mechanizmusok, valamint újabb és modernebb eszközök és komponensek. Ahogyan a postai levelezést lassan leváltotta a levelezőkliensek használata, úgy a hálózati technológián működő már mondhatni modernebb technológiát, a VoIP telefonokat is felváltotta a kommunikációs platformok sokasága.

Ipari környezetben az informatika szélessávon hozzájárul a vállalat stabil működéséhez, hatékonyságához, versenyképességéhez. Napjainkban létfontosságú rendszerelem a termeléskiesés mentes gyártás bevezetése, a redundáns hálózat kialakítása. Mindezek csak akkor lehetségesek, ha elhivatottak vagyunk elavult berendezéseinken, vagy akár folyamatainkon változtatni annak érdekében, hogy minél kevesebb legyen a hibafaktor.

A vállalati IT-s problémák és azok bekövetkezései azonnali megoldási javaslatokat igényelnek. Napjainkban a vállalatok rendkívül sok olyan negatív tényezőnek vannak kitéve, ami meggátolhatja a fejlődést, mivel az elavult rendszerek, programok, nem naprakész adatbázisok, redundancia és helyreállíthatóság hiánya olyan károkat képesek okozni, amelyek megakadályozhatják egy vállalat stabil működésit, veszélyeztetve ezzel rangsorát és hírnevét.

A vállalati informatikai problémák és megoldási javaslatuk című témát azért választottam, mivel elmúlt éveim során rendkívül sok munkatapasztalattal gazdagítottam tudásom. Ezek általában olyan egyéni, ritka előfordulású hibák, amelyekre még nem csak megoldási javaslat, best-practice (legjobban bevált gyakorlat) nem született, magával a hibával még a szakirodalmakban sem találkoztunk. Ekkor fel kell mérnünk azon lehetőségeket, bizonyos hibák, problémák milyen úton-módon történtek meg. Milyen kommunikációs csatornát használtak a probléma bejelentésére, jól megfogalmazott-e maga a hiba a felhasználó által, továbbá, egy bizonyos incidens esetén a megfelelő személy van-e a vonal végén, aki a megoldási útban tudja el kalauzolni a végfelhasználót a megoldás irányába.

Dolgozatom írása során olyan esettanulmányt is bemutatok, mely hasznos lehet arra a célra, hogy a mai rohanó IT világunkban bizonyos folyamatokból időnként ki kell tekinteni. Ne csak a fát lássuk, hanem az erdőt is, azaz, minél szélesebb szögben tároljon felénk a hiba, minél több ember vonjunk bele, akik más perspektívából is elemezni tudják a felmerülő problémákat kiváltó okokat.

1.2 A téma szakmai és személyes aktualitása

Talán az informatikai rendszerek nem is függtek még annyira a gyártáson, mint napjainkban. Biztonságos, rendszeresen karbantartott és menedzselt eszközeikkel olyan környezetet tudunk biztosítani, mely nemcsak javíthat a gyártási gépek állomásainak hatékonyságán, de biztosítja a hiba esetén az azonnali reagálást, mellyel csökkenteni tudjuk az álláidőt, termeléskiesés idejét.

A vállalati informatika szakmai aktualitását tovább növeli, hogy a kiberbiztonsági kockázatok az utóbbi években egyre nagyobb hangsúlyt kaptak. Egy gyártóvállalatnál, ahol a gépek hálózati kapcsolatban állnak, egy esetleges támadás nemcsak adatvesztést, hanem akár termelésleállást is okozhat. Emellett az ipar 4.0 és az IoT (Internet of Things) eszközök elterjedésével a vállalatok informatikai rendszerei még összetettebbé váltak, ami tovább növeli a hibalehetőségek számát. (Gergő Benedek, 2020)

Az én szemszögemből ez a téma azért is fontos, mivel a Bosch-nál töltött éveim alatt megtapasztaltam, milyen felelősségteljes és sokrétű munka egy nagyvállalati IT-környezet üzemeltetése. Érdekes volt látnom, hogyan hatnak bizonyos informatikai döntések a termelési folyamatokra vagy akár több száz felhasználó munkájára. A gyakorlati munka során nemcsak technikai ismereteimet bővítettem, hanem megtanultam, hogy mennyire fontos a precizitás, a gyors problémamegoldás és a csapatmunka az informatikában.

Egy másik személyes aktualitás, hogy az elmúlt években a vállalatnál több modernizációs projekt is zajlott, amelyek célja az informatikai infrastruktúra fejlesztése, a biztonság növelése és a rendszerek integrációjának javítása volt. Ezekben a projektekben való részvételem segített jobban megérteni, milyen összefüggések vannak a technológia, a hatékonyság és a költségek között.

Összességében a téma nemcsak szakmai szempontból releváns, hanem személyes fejlődésemhez is szorosan kapcsolódik. Úgy érzem, hogy a dolgozat lehetőséget ad arra, hogy átfogóan bemutassam azokat a kihívásokat és tanulságokat, amelyekkel az elmúlt években a vállalati informatikai munkám során találkoztam.

1.3 A dolgozat célja, hipotézisek

A dolgozatom fő célja, hogy feltárja és rendszerezze a vállalati informatikai környezetben előforduló problémákat, valamint bemutassa az ezekre adható lehetséges megoldásokat és fejlesztési irányokat. A cél nem pusztán a problémák technikai elemzése, hanem annak bemutatása is, hogy az informatikai döntések milyen hatással vannak a vállalati működés egészére különösen a gyártási, logisztikai és adminisztratív folyamatokra.

A dolgozatban szeretném megvizsgálni, milyen típusú informatikai hibák fordulnak elő leggyakrabban egy ipari környezetben, mi okozza ezeket, és milyen módszerekkel lehet megelőzni vagy gyorsabban kezelni őket. Emellett célom, hogy bemutassam, hogyan épül fel egy jól szervezett IT-támogatási rendszer, milyen szerepe van a hibajegykezelő rendszereknek, a dokumentációnak és a felhasználói kommunikációnak a hatékony működés fenntartásában.

Külön figyelmet fordítok a gyakorlati példákra és saját tapasztalataimra a Bosch hatvani gyárából. Ezek a példák rávilágítanak arra, hogyan lehet a valós problémákat strukturáltan elemezni, és milyen fejlesztési javaslatok segíthetik a vállalat informatikai rendszerének fejlődését.

A dolgozat további célja, hogy egyfajta útmutatót is nyújtson a vállalati IT-problémák kezeléséhez, amely a jövőben más vállalatok vagy informatikai szakemberek számára is hasznos lehet. Végső soron az elemzés hozzájárulhat ahhoz, hogy az informatikai részlegek hatékonyabban működjenek együtt a termelési és adminisztratív területekkel, ezáltal növelve a vállalat egészének hatékonyságát és biztonságát.

A dolgozat tehát nemcsak a technológiai kihívásokat kívánja bemutatni, hanem azt is, hogyan lehet az IT-t stratégiai eszközként használni a vállalati célok eléréséhez.

Dolgozatom során 4 hipotézist állítottam fel, melyre dolgozatom összefoglaló részében válaszolom meg a kidolgozott esettanulmányom és tapasztalataim szerint:

1. A digitalizáció és automatizáció ajtót nyithat a modern kibertéri sebezhetőségeknek?
2. Az automatizált védelmi rendszerek megnehezíthetik a problémaelhárítást?
3. Fejlődő infrastruktúra mellett biztosítható az elavult gyártóberendezések támogatása?
4. IT biztonsági tudatosságunk naprakészen megállja a helyét az Ipar 4.0 világában?

2. A vállalati informatika szerepe ipari környezetben

Az ipari környezetben működő vállalatok számára az informatikai rendszerek jelentősége folyamatosan növekszik. A modern gyártás, a logisztikai folyamatok, a minőségellenőrzés és a vállalati adminisztráció ma már elképzelhetetlen stabil és biztonságos IT-infrastruktúra nélkül. A vállalatoknak nem csupán a termelési adatok és üzleti információk kezelését kell biztosítaniuk, hanem a felhasználói, személyi adatok védelmét és a rendszerek megbízható működését is garantálniuk kell.

Az ipari vállalatok folyamatosan támaszkodnak hálózati kapcsolatokra, amelyek lehetővé teszik az adatok valós idejű továbbítását a gyártósorok, a raktárak, a tervezési osztályok és az adminisztráció között. A digitális eszközök, szenzorok és automatizált rendszerek integrációja révén a gyártás optimalizálható, a hibák gyorsan azonosíthatók, és a döntéshozatal megalapozottabbá válik. Az adatok valós idejű elérhetősége azonban csak akkor biztosítható, ha a vállalat stabil és biztonságos IT-infrastruktúrát működtet.

Ugyanakkor az informatikai fejlődés üteme az ipari környezetben gyakran meghaladja azon vállalatok képességeit, amelyek még csak a hagyományos gyártási rendszerekkel dolgoznak. Ez különösen érvényes a kiberbiztonság, a rendszerfrissítések és az adatvédelem területén. A vállalatoknak folyamatosan azon kell dolgozniuk, hogy az IT-rendszereik megfeleljenek a mai világ biztonsági követelményeinek, és képesek legyenek megvédeni magukat a potenciális támadásoktól, adatvesztéstől vagy termeléslеállástól. (Microsoft, 2025)

1. ábra: Az iparágat fenyegető gyakori fenyegetések

Forrás: https://hungarian.opswat.com/blog/5-strategies-for-securing-critical-manufacturing-environments

A cégek számára tehát elengedhetetlen, hogy folyamatosan fejlesszék és karbantartsák IT-rendszereiket, és olyan biztonsági, adatkezelési és monitoring megoldásokat alkalmazzanak, amelyek lehetővé teszik számukra, hogy a versenyképes és megbízható működés a mai technológiai környezetben is fenntartható legyen.

2.1 Az informatikai rendszerek jelentőségé a vállalatoknál

A Robert Bosch Elektronika Kft. hatvani gyára egy modern, nagy volumenű elektronikai gyártó üzem, ahol a termelési folyamatok, az anyagáramlás, a minőségellenőrzés és az adminisztráció szoros összefüggésben áll az informatikai rendszerekkel. Az IT-infrastruktúra nem csupán háttérszolgáltatás, hanem a gyártás és az üzleti folyamatok alapvető gerincét képezi. A gyár napi működése nagymértékben függ a szerverek, hálózatok, automatizált rendszerek és felhasználói alkalmazások stabilitásától, teljesítményétől és biztonságától.

A vállalat informatikai rendszerei számos kritikus feladatot látnak el. Elsődlegesen támogatják a termelési folyamatok automatizálását, beleértve az assembly-line vezérlést, a robotizált gépek működését és a gyártósori adatgyűjtést. A valós idejű adatgyűjtés lehetővé teszi a termelés hatékonyságának folyamatos monitorozását, a hibák gyors azonosítását és a beavatkozások ütemezését. A rendszerek ezen túlmenően biztosítják az anyagáramlás és készletkezelés optimalizálását, amely elengedhetetlen a gyártási folyamatok zavartalanságához és a költséghatékonyság fenntartásához. (Demeter Krisztina, 2016)

Egy másik kiemelt terület a minőségbiztosítás és adatkezelés, amelyhez szintén elengedhetetlen az informatika szerepe. A gyártott alkatrészek és termékek minden fontos paramétere elektronikus nyilvántartásba kerül, amely nemcsak a termékfelelősség és nyomon követhetőség szempontjából fontos, hanem a folyamatos fejlesztés és a hibamegelőzés szempontjából is. A hatékony adatkezelés lehetővé teszi a statisztikai elemzéseket, a trendek és anomáliák gyors azonosítását, valamint a döntéshozatal támogatását a menedzsment szintjén.

A Bosch hatvani gyárában az IT-rendszerek biztonsága és megbízhatósága kiemelten fontos. A gyártósorok és a hálózatok bármilyen fennakadás esetén azonnal termelésleálláshoz vezethetnek, ami jelentős költségekkel jár. Ezért a vállalat folyamatosan törekszik a hálózati infrastruktúra redundanciájára, a rendszerfelügyelet automatizálására, valamint a kiberbiztonsági protokollok és szabályzatok szigorú betartatására. Az IT nemcsak a problémák gyors azonosításában játszik szerepet, hanem megelőző eszközként is, például az automatizált riasztások, hozzáférés-ellenőrzések és rendszerfrissítések révén. Emellett az informatikai rendszerek elengedhetetlenek a felhasználói támogatás és belső kommunikáció szempontjából. A gyári dolgozók, mérnökök és technikusok mindennapi munkáját segítik a különböző intranet rendszerek, belső alkalmazások és kommunikációs platformok. A hibajegyek kezelése, a hozzáférések adminisztrálása és az IT-támogatás hatékony működése közvetlenül hozzájárul a gyártás folyamatos üteméhez és a munkavállalók elégedettségéhez. (Kovács László, 2018)

Összességében elmondható, hogy a Robert Bosch Elektronika Kft. hatvani gyárában az informatikai rendszerek jelentősége stratégiai szinten jelenik meg, mivel nélkülük a gyártási folyamatok nem lennének hatékonyak, a termelékenység csökkenne, és a minőségbiztosítási elvárások sem teljesíthetők. Az IT tehát nem csupán technikai háttér, hanem a vállalat működésének alapvető meghatározó tényezője, amely egyben lehetőséget kínál a folyamatok optimalizálására, a költségek csökkentésére és a versenyképesség növelésére.

2.2 Gyártási és informatikai rendszerek integrációja, automatizációja

Az elmúlt években nemcsak a hatvani gyárban, hanem számos más Bosch telephelyen is kiemelt figyelmet kapott a gyártási folyamatok automatizálása és digitalizálása. A cél minden esetben az volt, hogy a gyártás hatékonyságát növeljük, a hibalehetőségeket csökkentsük, és a fizikai munkaerőt részben tehermentesítsük, miközben új, technológiailag fejlettebb szerepköröket biztosítunk számukra.

A hatvani gyár egyik legjelentősebb fejlesztése az automata raktározási rendszer bevezetése volt, amely biztosítja, hogy a gyártósorokhoz szükséges alapanyagok a lehető leggyorsabban és legpontosabban jussanak el. Ezt a rendszert szorosan kiegészíti az úgynevezett AGV (Automated Guided Vehicle) rendszer, amely automatikusan közlekedik a gyártócsarnok területén, és az anyagmozgatási folyamatokat emberi beavatkozás nélkül képes elvégezni. Természetesen a mai napig működnek úgynevezett “Milkrun” manuális szállítóeszközök is, amelyeket a dolgozók vezérelnek. Azonban az AGV-k bevezetésével ezek használata fokozatosan csökken, mivel az automata járművek megbízhatóbban, gyorsabban és biztonságosabban végzik el a szállítási feladatokat. Az új rendszer bevezetése miatt elengedhetetlen volt a vezeték nélküli infrastruktúra megfelelő kiépítése, valamint a dolgozók oktatása az új technológiák kezelésére.

Az automatizáció kulcsfontosságú szerepet tölt be az Ipar 4.0 megvalósításában. A cél, hogy minden gyártóállomás olyan fejlettségi szintet érjen el, ahol minimális emberi beavatkozással - vagy akár teljesen önállóan - képes a termelési folyamat végrehajtására. Ez nemcsak a gyártási sebességet növeli, hanem csökkenti az emberi hibákból eredő selejtek számát is. Ugyanakkor az automatizált rendszerek működése komoly informatikai támogatást igényel. Ha egy állomás valamilyen okból nem tudja biztosítani a megszokott termelési volument, az IT szakembereknek, karbantartóknak vagy technikusoknak gyorsan be kell avatkozniuk. Az ilyen beavatkozások során különösen fontos, hogy a hálózati kommunikáció stabil legyen, és az állomás biztonságosan tudjon kapcsolódni a központi szerverekhez. (Ászity Sándor, 2019)

A gyártósori rendszerek védelme érdekében minden olyan alkalmazást, amely távoli elérést biztosított (például TeamViewer, Remote Desktop), fokozatosan eltávolítottak az üzemi gépekről. Helyette bevezetésre került egy biztonságos RSA alapú megoldás, amely kizárólag az arra jogosult technikusok számára teszi lehetővé a távoli hozzáférést, meghatározott időkorláton belül. A hozzáférések minden esetben IT Service Portal jegy alapján történnek, amelyben rögzítik a beavatkozás célját, idejét és felelősét.

A hozzáférést fizikailag is védeni kell: az RSA-boxokon található kulcs elfordításával aktiválható az engedélyezett módosítási funkció, ezzel is biztosítva, hogy a változtatások kizárólag karbantartási vagy fejlesztési célból történjenek.

Korábban, amikor még VNC-alapú megoldásokat használtunk, gyakran előfordult, hogy nem volt egyértelmű, ki dolgozik éppen a gépen. Ennek következtében voltak olyan esetek, amikor egy helyi operátor elindította a gyártósort, miközben egy távoli kolléga paraméterezést végzett ugyanazon az eszközön. Ez hibás termékekhez, sőt kisebb balesetekhez is vezettethetett volna.

Az új rendszerrel ezek a problémák teljes mértékben kiküszöbölhetők, hiszen minden távoli hozzáférés ellenőrzött, naplózott és időben korlátozott. Ezzel a Bosch a lehető legmagasabb üzemi biztonságot és adatvédelmet biztosítja a gyártási folyamatokban, miközben megőrzi az informatikai rendszerek stabilitását és az üzletmenet-folytonosságot.

3. Jellemző vállalati informatikai problémák

A modern vállalati informatika rendkívül összetett rendszerekből áll, amelyek magukban foglalják a vállalati szoftvereket, adatbázisokat, hálózatokat, felhasználói eszközöket, valamint az OT (Operational Technology) rendszereket, amelyek közvetlenül a gyártási folyamatokat irányítják. Az IT és OT világának integrációja számos előnyt kínál, de egyben új típusú problémákat is generál. Az alábbiakban a leggyakrabban előforduló problémaköröket mutatjuk be. (OPSWAT, 2025)

Az ipari vállalatok nagy része ERP rendszerekre, például SAP S/4HANA-ra támaszkodik a pénzügyi, logisztikai, gyártási és készletkezelési folyamatok támogatására. A rendszer elérhetetlensége vagy lassú működése súlyos hatással van a termelésre és a vállalati döntéshozatalra. Gyakori problémák közé tartozik: a rendszer túlterheltsége, nem megfelelő kapacitástervezés, verziófrissítések késedelmes alkalmazása vagy inkompatibilitás a meglévő üzleti folyamatokkal. Az ERP rendszerek hibái közvetlen anyagi veszteséget okozhatnak, és gyakran dominó hatást indítanak el a beszállítói láncban. (Káplár Judit, 2023)

Az OT rendszerek esetében, például gyártósori vezérlők, SCADA rendszerek, PLC-k integrációja az IT hálózattal új kihívásokat jelent. A különböző protokollok, az elavult OT eszközök és az IT biztonsági szabályok közötti eltérések gyakran vezetnek kommunikációs problémákhoz, hálózati késleltetésekhez és hibás adatgyűjtéshez. Az OT rendszerek leállása közvetlenül befolyásolja a gyártást, ezért az IT/OT integrációban kiemelt fontosságú a megbízható adatátvitel és a redundancia kialakítása.

A beszállítói ERP vagy logisztikai rendszerek elérhetetlensége komoly problémát jelent, különösen az ipari láncokban, ahol az anyagáramlás és a gyártás szorosan összekapcsolódik. Egyetlen partner rendszerének kiesése is késleltetheti a termelést, és jelentős költségtöbbletet okozhat. Ezért a vállalatoknak nemcsak saját rendszereiket, hanem a beszállítói lánc IT infrastruktúráját is folyamatosan figyelemmel kell kísérni.

A vállalati informatikai rendszerek egyre inkább ki vannak téve a kiberbűnözésnek, beleértve a zsarolóvírusokat, adatlopásokat, valamint a sötés weben (darkneten) történő információárulást. Egy zsarolóvírus támadás vagy adatlopás nemcsak a pénzügyi veszteséget növeli, hanem a vállalat hírnevét és a partnerkapcsolatokat is veszélyezteti. Az IT-részlegeknek folyamatosan figyelniük kell a biztonsági frissítéseket, a hozzáférés-kezelést, az alkalmazottak tudatosságát, és hatékony incidenskezelési tervet kell kidolgozniuk.

A lassú hálózat, a nem megfelelő sávszélesség, a redundancia hiánya vagy az elavult hálózati eszközök mind komoly akadályt jelenthetnek a termelési és üzleti folyamatok számára. Az IT-rendszerek teljesítménye és a felhasználói élmény szoros összefüggésben áll a hálózat stabilitásával, így ezeknek a problémáknak a kezelése kulcsfontosságú a folyamatos működés biztosításához.

A régi laptopok, munkaállomások és szerverek lassítják a napi munkát, és biztonsági kockázatot jelentenek, ha nem támogatják az aktuális szoftvereket vagy biztonsági protokollokat. Hasonlóan kritikus a szoftverlicenszek kezelése: a jogtalan vagy lejárt licenszek nemcsak jogi problémákat okoznak, hanem a munkafolyamatok megszakadásához is vezethetnek. (Szilágyi Gábor, 2025)

3.1 Kommunikációs nehézségek a felhasználókkal

Az informatikai támogatás egyik legnagyobb kihívása nem feltétlenül technikai jellegű, hanem inkább a kommunikációs problémákhoz köthető. Bár a legtöbb esetben a felhasználó és az IT-szakember közös célja a probléma gyors és hatékony megoldása, a gyakorlatban gyakran előfordulnak félreértések, pontatlan információk vagy akár nyelvi akadályok, amelyek lassítják a folyamatot és növelik a hibalehetőséget. Saját munkatapasztalataim alapján a Bosch környezetében ezek a nehézségek mindennaposok, különösen a nagyvállalati méret és a nemzetközi munkakörnyezet miatt.

Az egyik leggyakoribb jelenség, hogy a felhasználó nem tudja pontosan leírni a problémát, amellyel szembesül. Ez nem feltétlenül az ő hibája, hiszen általában nem rendelkezik mélyebb technikai tudással, és a jelenségeket saját szemszögéből (sokszor laikus nyelven) próbálja megmagyarázni. Például gyakran hallani olyan bejelentéseket, mint „nem működik az internet”, ami valójában lehet egy hálózati hiba, egy VPN-kapcsolati probléma, vagy akár egy alkalmazás időszakos leállása.

A pontatlan megfogalmazás következménye, hogy a feladott ticketek nem mindig a megfelelő megoldócsoporthoz kerülnek. Ennek oka sokszor az, hogy a felhasználó maga sem tudja a probléma eredeti forrását, vagy hiányosan adja meg a szükséges információkat. Ez felesleges köröket eredményez, hiszen a hibajegy előbb egy nem releváns csoporthoz kerül, majd onnan átirányításra kerül a megfelelő szakértőkhöz, ami természetesen megnöveli az átfutási időt, és rontja a jegy KPI megoldási idejét.

A Bosch környezetében szerencsére rendelkezésre áll egy időpontfoglaló rendszer, amely lehetőséget biztosít 15 vagy 30 perces személyes megbeszélésekre. Ezek során az IT-szakember közvetlenül a felhasználóval együtt tudja tisztázni a problémát, ami sokkal hatékonyabb, mint a hosszadalmas e-mailváltás. Tapasztalatom szerint sokszor egy rövid személyes beszélgetés során olyan információk is kiderülnek, amelyeket a felhasználó írásban nem említett meg.

Egy másik bevált gyakorlat, hogy ha a felhasználó hibajegye nem tartozik az adott IT-s hatáskörébe, az IT-s új ticketet hozhat létre a felhasználó nevében. Ez azért előnyös, mert az informatikus sokkal pontosabban, technikai részletekbe menően tudja leírni a problémát, így az incidens sokkal gördülékenyebben kerül a megfelelő megoldócsoport elé. Ezzel a módszerrel a félreértések száma jelentősen csökkenthető.

Egy jól és pontosan megfogalmazott hibajegy valóban fél siker, hiszen a helyes diagnózis felállítása alapvetően meghatározza a megoldás gyorsaságát és minőségét.

A nyelvi akadályok áthidalására több módszer is bevált:

- Vizualizáció használata: képernyőfotók, rövid videók segítenek abban, hogy pontosabb képet kapjunk a hibáról.
- Egyszerűsített kommunikáció: kerülni kell a túlzott szakzsargont, és a megoldást lépésről lépésre, érthetően kell átadni.
- Többcsatornás kommunikáció: ha élő szóban nem világos a helyzet, e-mailben vagy chatben gyakran pontosabban leírható a probléma.

(Purdue Global, 2025)

3.2 Hálózati problémák

Egy modern gyártóüzem működésének legfontosabb alappillére a stabil, megbízható és korszerűen karbantartott hálózati infrastruktúra. A hálózat tekinthető a gyártósorok és vezérlőegységek „ütőerének”, hiszen ez biztosítja a különböző végpontok közötti zavartalan kommunikációt, valamint a gyártási folyamatok folyamatos adatáramlását.

A technológiai fejlődés és az ipari digitalizáció rohamos üteme egyre nagyobb kihívásokat támaszt a hálózati rendszerekkel szemben. A stabil működés érdekében kiemelten fontos a rendszeres karbantartás és az időszakos tesztelések végrehajtása, amelyek biztosítják a gyártási infrastruktúra megbízhatóságát, rendelkezésre állását és redundanciáját.

A hatvani Robert Bosch Elektronika Kft. esetében is alapvető elvárás a modern, stabil és megfelelően karbantartott hálózati infrastruktúra működtetése. Az üzem informatikai részlegének feladata, hogy a gyártási folyamatok zavartalansága érdekében a hálózat minden eleme folyamatos felügyelet alatt álljon. A Bosch szabályozásai szerint évente kötelező elvégezni egy teljes redundanciatesztet, amely során ellenőrzik, hogy a hálózat kritikus komponensei - mint például a disztribútorok, core switchek és routerek képesek-e önállóan és hibamentesen átváltani tartalék ágra egy esetleges meghibásodás vagy áramkimaradás esetén.

A teszt egyik legfontosabb szempontja a helyes sorrend betartása az eszközök leállításakor és újraindításakor. Egy hibás sorrend vagy elhamarkodott beavatkozás ugyanis felboríthatja a hálózati logikát, ami elnyújtott helyreállításhoz és akár termelésleálláshoz is vezethet. A teszt célja, hogy a hálózat a teljes leállítást követően legfeljebb 30 percen belül az eredeti állapotába visszaálljon, emberi beavatkozás nélkül.

Az áramellátási tesztet automatikusan, az UPS tápegységek kikapcsolásával és a betáp megszakításával hajtják végre. A folyamat során keletkező minden logot és rendszeradatot továbbítani kell a központi szakosztály felé, amely elemzi és validálja a teszt eredményét, értékelve a redundancia hatékonyságát.

A Hatvani Bosch gyár, a Connected Hub-bal együtt, kritikus létesítménynek számít, ezért a hálózati hibák esetén az állásidő minimalizálása kiemelt fontosságú. A gyártási állomások számára jelenleg nem áll rendelkezésre teljes redundáns hálózat, így például egy Layer 2-es szinten működő access switch meghibásodása közvetlenül megakaszthatja a termelést. Ilyen esetekben elengedhetetlen a gyors reagálás és a helyreállítás azonnali megkezdése.

Minden hálózati eszközből modelltől, firmware és verziószámtól függően legalább egy azonos paraméterű tartalék (spare) eszközt tart készenlétben. Ez lehetővé teszi, hogy hiba esetén az eszközt teljes egészében kicseréljék, ahelyett, hogy moduláris javítással próbálkoznának, ami időigényes és kockázatos lenne. A hibás eszközöket később bevizsgálják vagy garanciális úton javíttatják, de a gyártás folyamatos működése mindig elsődleges szempont.

A szűkös időkeret miatt a Hatvani Bosch Informatikai Osztály a hálózati problémák elhárítása érdekében 0-24 órás ügyeleti rendszert tart fenn. Minden hónapban két kijelölt kolléga látja el az ügyeletet: az egyik a hotline (forródrót) készüléket kezeli, amelyen az esti és éjszakai órákban (18:00-06:00) hívhatók, míg a másik kolléga a bejárós, helyszíni szerepkört tölti be. Ez a rendszer biztosítja, hogy bármilyen hálózati hiba esetén azonnal megkezdődhessen a hiba diagnosztizálása és elhárítása, minimalizálva ezzel a termeléskiesés idejét.

Informatikai osztályunkon évente kötelezően végrehajtásra kerül egy teljes körű redundanciateszt, amely a hálózati infrastruktúra stabilitását és helyreállítási képességét vizsgálja. A teszt célja annak ellenőrzése, hogy bármilyen áramkimaradás vagy rendszerhiba esetén a hálózati eszközök különösen a magas prioritású berendezések, mint a disztribútorok, core switchek és routerek képesek legyenek automatikusan és emberi beavatkozás nélkül visszaállni az eredeti működési állapotukba.

A redundanciateszt során meghatározott sorrendben történik az eszközök fokozatos leállítása. Ennek betartása kulcsfontosságú, mivel egy rossz sorrendben végrehajtott leállítás könnyen felboríthatja a hálózati topológiát, ami késleltetheti a helyreállítást, és hibás hálózati viselkedést eredményezhet. A tesztet követően minden logfájlt és eseményadatot továbbítani kell a központi Bosch szakosztály felé, ahol megtörténik a validálás és az eredmények részletes elemzése.

A teszt folyamata automatizált: az áramellátás megszakítása UPS (Uninterruptible Power Supply) egységek segítségével történik, melyek szimulálják az áramszünetet. A folyamat gyorsítása nem megengedett, hiszen minden eszköz működését valós körülmények között kell vizsgálni.

Mivel a hatvani gyár a Connected Hub raktárával együtt kritikus infrastruktúrának minősül, kiemelt szempont, hogy egy esetleges hálózati meghibásodás esetén a gyártási állásidőt a lehető legkisebbre csökkentsük. A gyártóállomások számára jelenleg nincs teljes körű redundáns hálózati kiépítés, ezért különösen fontos a gyors reagálás és a készenléti (spare) eszközök rendelkezésre állása. Egy Layer 2-es szinten üzemelő access switch meghibásodása esetén például nincs lehetőség az eszköz hosszadalmas javítására vagy modulcserére. Ilyenkor azonnali eszközcserére van szükség, a hibás berendezést pedig bevizsgálásra vagy garanciális javításra küldjük vissza. Ezzel biztosítható, hogy a gyártási folyamat a lehető legrövidebb időn belül folytatódhasson. A gyors hibaelhárítás érdekében a hatvani Bosch Informatika részleg 0-24 órás ügyeleti rendszert működtet. Minden hónapban két kolléga felel az ügyeleti feladatokért: az egyikük a hotline (forró drót) telefonszámot kezeli, amelyet az esti és éjszakai órákban hívhatnak, míg a másik kolléga bejárós szerepet tölt be, és szükség esetén a helyszíni beavatkozást végzi.

Ez a rendszer nemcsak a gyors hibakezelést teszi lehetővé, hanem hozzájárul a vállalat megbízhatóságához és gyártási hatékonyságához is. Tapasztalataim alapján a jól szervezett karbantartási folyamatok és az előre megtervezett hálózati struktúra kulcsfontosságú a gyártási leállások minimalizálása és a magas rendelkezésre állás fenntartása szempontjából.

Korábban a hálózati infrastruktúra gerincét HPE Aruba eszközök alkották, amelyek megbízhatóan működtek, azonban a gyártás növekvő adatforgalma és a modern biztonsági követelmények miatt elengedhetetlenné vált a Cisco infrastruktúrára való átállás. Ennek fő oka a Cisco fejlettebb menedzsment- és redundanciakezelési képessége, valamint a gyári sztenderdekhez való jobb illeszkedése volt.

A hálózati architektúra háromrétegű topológiára épül:

Core réteg: két, egymással redundáns kapcsolatban álló Cisco Catalyst 9500 sorozatú eszköz biztosítja a hálózati gerincet. Ezek látják el a Layer 3 routing funkciókat és a különböző VLAN-ok közötti forgalmat.

Distribution réteg: a fő disztribútorok (Cisco Catalyst 9300-as sorozat) a gyár különböző zónáiban helyezkednek el, és gyűjtik az access switchek forgalmát. Itt történik a forgalomirányítás, szűrés, valamint a hálózati biztonsági házirendek kezelése.

Access réteg: a gyártósorokhoz, terminálokhoz és vezérlőgépekhez csatlakozó Cisco Catalyst 9200 switchek alkotják. Ezek biztosítják az eszközök Layer 2 szintű elérését, valamint VLAN-szegmentációval támogatják a logikai elkülönítést.

A gyár teljes hálózata redundáns optikai összeköttetésekkel működik, amely két különböző szolgáltatói irányból érkezik. A legtöbb fő hálózati kapcsolat 10 Gbps sebességű optikai uplinkeken keresztül zajlik, míg a gyártási zónákban 1 Gbps-os csatlakozások dominálnak.

Az egész hálózat menedzselése központilag, Cisco DNA Center és Cisco Prime Infrastructure segítségével történik, ami lehetővé teszi az automatikus konfigurációt, hibafelügyeletet és topológiai átláthatóságot. (Cisco, Understanding Cisco DNA and Catalyst Software eBook, 2024)

Egyik műszak során több PLC-vezérlő kommunikációja megszakadt, a rendszer pedig „Device unreachable” hibát jelzett. A vizsgálat során kiderült, hogy az egyik újonnan telepített munkaállomás manuálisan beállított, statikus IP-címet kapott, amely ütközött egy gyártási eszköz IP-címével.
A probléma megoldásaként bevezetésre került egy DHCP-foglalási rendszer, amely automatikusan kiosztja a fix IP-címeket MAC-cím alapján, kizárva a manuális hibázás lehetőségét. Ezen felül minden új eszköz csatlakoztatása előtt előzetes IP-audit történik az adott VLAN-ban.

Egy külső vállalkozó által végzett építési munka során Horton városrészben véletlenül elvágták a fő disztribútor optikai összeköttetését. A hiba azonnal érzékelhető volt, mivel több alhálózat forgalma megszűnt. A gyár azonban felkészült ilyen eshetőségekre: a hálózat rendelkezik redundáns optikai útvonallal és másodlagos internetszolgáltatóval, amely bérelt vonalon keresztül biztosítja az alternatív kapcsolatot.

A failover mechanizmus automatikusan aktiválódott, és a forgalom kevesebb mint 40 másodperc alatt helyreállt. Az esetről részletes log- és syslog-adatok kerültek továbbításra a központi hálózatüzemeltetési részleg felé, akik elemezték az átállási időt és megerősítették a redundanciahatékonyságot.

Egy másik esetben a gyártósor egyik switchez csatlakoztatott állomás véletlenül loopback hibát generált, amely rövid idő alatt szórási vihart idézett elő. Ez akkor fordul elő, amikor hálózaton belül az forgalomirányító bekötési hiba miatt saját magába végződik.

Ennek következtében a forgalomirányító automatikusan port security és storm control mechanizmus alapján letiltotta az érintett portot, hogy megakadályozza a hálózat további terhelését, viszont ezáltal a forgalomirántyó már nem tudta kiszolgálni a többi, ugyan arra a switchre bekötött gyártógépet, ami kiesést okozott. A hibát kiváltó állomás firmware-hibás hálózati kártyával rendelkezett, amit cserét követően a port visszaengedése után a kommunikáció helyreállt. Az eset után minden gyártási VLAN-ban aktiválásra került a BPDU Guard és loop detection funkció, megelőzve a hasonló problémákat a jövőben, és csak a hibásan bekötött állomás esetében legyen port letiltás. (Cisco, Understand the Spanning Tree PortFast BPDU Guard Enhancement, 2025)

Ezek a hálózati hibák jól mutatják, hogy akár a legmodernebb rendszerekben is előfordulhatnak váratlan helyzetek, viszont megfelelő karbantartási- és felügyeleti folyamatokkal ezek gyorsan és hatékonyan kezelhetők.

3.3 Hardverproblémák

Egy vállalati informatikai rendszer megbízhatóságának kulcsa a hardware. A processzorok, alaplapok, memóriák, tárolók, és hálózati eszközök szervizelhetősége vagy elavultsága, hibás működése vagy inkompatibilitása közvetlen módon befolyásolja a gyártórendszer hatékonyságát, stabilitását és elérhetőségét. (Szilágyi Gábor, 2025)

A memóriahibák (bit-flip, hibás programkód, ECC-hibák zárlat vagy kisülés miatt) adatvesztést vagy rendszerösszeomlást okozhatnak.

Alaplaphibák (hő által meghajolt, hibás áramkör, hibás chipset, feszültségingadozás) legtöbbször instabil működést vagy perifériahibákat okoznak. Ugyanilyen fontos a tápellátás: ha az alulméretezett vagy öregedett táp nem tudja stabilan ellátni árammal a gépet, az túlterhelés alatt leállhat vagy kiszámíthatatlanul viselkedhet.

A tároló HDD, SSD meghibásodása adatvesztéssel és szektorhibákkal járhat, az nem elegendő hűtés pedig túlmelegedést eredményez, ami gyorsítja az alkatrészek élettartamát és idővel az adattártolón lévő adatok korruptságához vezet.

A hardver vagy szoftver inkompatibilitás például elavult driverek, firmware-problémák vagy nem támogatott buszrendszerek szintén instabilitást, hibás működést és biztonsági kockázatokat okozhat. Az ilyen hibák gyakran csak akkor derülnek ki, amikor már több komponens együttműködése sérült, ami az egész rendszer integritását veszélyezteti.

A hardverhibák nem csupán technikai problémát jelentenek közvetlenül érintik a rendszerintegritást, az adatok megbízhatóságát és a szolgáltatások elérhetőségét. Egyetlen hibás memóriachip is okozhat adatvesztést, míg egy tápellátási probléma vagy meghibásodott tároló a teljes rendszerösszeomlást, majd leállását idézheti elő.

Ipari környezetben, ahol a folyamatos működés kritikus, a hardverhibák termeléskiesést, anyagi veszteséget és akár biztonsági kockázatot is jelenthetnek. Emiatt kiemelten fontos a komponensek állapotának folyamatos monitorozása, a redundancia alkalmazása, valamint az olyan diagnosztikai eszközök használata, mint a SMART-adatok vagy az ECC-hibaszámlálók.

Amikor a hardver még működőképes, de az operációs rendszer vagy az alkalmazások elavultak, a rendszer biztonsági szempontból sebezhetővé válik. Olyan ipari környezetben, ahol gyakran régi rendszerek működnek kritikus folyamatokban - ez különösen érzékeny kérdés, hiszen a modern biztonsági előírásokkal való összehangolás sokszor kompromisszumokat igényel. (Heténi Petra, 2023)

Az elavult rendszerek nem mindig kompatibilisek az újabb operációs rendszerekkel, driverekkel, protokollokkal vagy hardverekkel. Ilyenkor egy modern szoftver nem képes kommunikálni a régi interfészekkel, vagy a régi hardverhez nem található támogatott driver. Ennek következtében gyakori a rendszerinstabilitás vagy az adatvesztés. A Hardware Compatibility List (HCL) segíthet annak meghatározásában, mely hardver- és szoftverkombinációk működnek megbízhatóan együtt. Bár a lista hiánya nem feltétlenül zárja ki a működést, a tapasztalat azt mutatja, hogy az ellenőrzött és dokumentált konfigurációk hosszú távon stabilabbak.

Az elavult rendszerek gyakran tartalmaznak ismert, javítatlan biztonsági hibákat, amelyek kihasználhatók.

Minden olyan hardver, amely például Windows 10, vagy annál régebbi operációs rendszert tartalmaz, szükséges úgynevezett hardeningeket bevezetni. Hardeningnek olyan szigorításokat

nevezünk, melyek egy adott rendszeren, a rendszerbizotonság és kibervédelem tekintetében szigorító intézkedésként vezetünk be. Ilyen lehet például a nem használt programok és szolgáltatások eltávolítása, a az USB jogosultság letiltása, valamint ellátni az adott állomás vezérlő számítógépjét vírusírtó alkalmazással. fontos, hogy biztosítanunk kell minden régi operációs rendszere a legutolsó biztonsági frissítések telepítését. (Kenfack, 2023)

A patch management ezért kulcsfontosságú: magában foglalja a sérülékenységek azonosítását, a frissítések tesztelését, ütemezését és telepítését. Ipari (OT/ICS) környezetben azonban a folyamatos patch-elés nem mindig kivitelezhető, mivel a rendszerek nem állíthatók le bármikor. Ilyenkor alternatív megoldások - például hálózati szeparáció, tűzfalas védelem vagy virtual patching - jelenthetnek reális kompromisszumot. (Tamás K. , 2022)

Az elavult rendszerek esetében a konfigurációs és adat-integritás is fokozottan veszélyeztetett. Egy nem naprakész rendszer könnyebben manipulálható - akár támadók, akár belső hibák révén. A rendszeres integritásellenőrzések, checksummák és digitális aláírások segítenek a változások nyomon követésében.

A rendelkezésre állás növelésére a redundancia, a virtualizáció, valamint a karbantartási ablakok optimalizálása jelenti a legésszerűbb irányt. Egy jól tervezett backup- és restore-folyamat csökkenti az újraindítás idejét és a termeléskiesés mértékét.

Az alábbi 4 megoldással tudjuk az esetleges hibák elkerüli elavult gyártási gépek esetében:

Hálózati esetben: szeparáció és zónázás: Az elavult rendszerek legyenek elkülönített hálózati szegmensekben, minimális kommunikációval más hálózatok felé.

Virtualizáció nézetében: Az eredeti rendszerek futtathatók konténerben vagy virtuális gépben, így csökkenthető a fizikai hardverfüggés, és az üzemeltetési költségek.

Jogosultságkezelés: Törekendünk kell a minimum jogosultság elvére, azaz csak a felhatalmazott, személyek, vagy állomás felelősök és szervizesek férhessenek hozzá adminisztratív funkciókhoz.

Hitelesítés és naplózás: Minden rendszeres változást hitelesítenünk kell, hogy megfelelnek-e az It-biztonsági előírásoknak, valamint dokumententálni kell

3.4 Gyártási-IT integrációs kihívások

A modern ipari környezetekben az informatikai (IT) és az operatív technológiai (OT) rendszerek közötti integráció az egyik legnagyobb kihívás. Míg az IT-rendszerek főként az adatok kezelésére, feldolgozására és biztonságára fókuszálnak, addig az OT-rendszerek célja a gyártási folyamatok folyamatos, valós idejű vezérlése és felügyelete.

A két terület közötti összhang megteremtése elengedhetetlen a hatékony és biztonságos működéshez - ugyanakkor ez számos technikai, biztonsági és szervezeti nehézséget is magával hoz.

A Robert Bosch Elektronika Kft. hatvani telephelyén ez a kihívás különösen jól megfigyelhető, mivel a gyárban több ezer különböző gyártóeszköz, szenzor, PLC és ipari számítógép működik, amelyek mind folyamatos hálózati kommunikációt igényelnek. A termelési adatok valós időben áramlanak az IT-rendszerekbe, például a MES (Manufacturing Execution System) és az ERP (Enterprise Resource Planning) rendszerek felé.

Hálózati szeparáció és biztonsági zónák kialakítása közben az egyik legnagyobb kihívás az IT és OT hálózatok közötti biztonságos kommunikáció megteremtése.

A hatvani Bosch gyárban a hálózat zónákra van osztva:

- a gyártási (OT) hálózat,
- az irodai (IT) hálózat,
- valamint az adminisztratív és külső hozzáférési zóna.

Ezek között tűzfalak, VLAN-szegmentációk és ACL-szabályok biztosítják a forgalom kontrollálását.
A probléma ott jelentkezik, amikor egyes gyártóberendezések (pl. régebbi PLC-k vagy ipari számítógépek) nem képesek a modern hálózati protokollokat kezelni, vagy nem támogatják az IPv6-ot és a biztonságos autentikációs mechanizmusokat.

Eszközazonosítás és hálózati láthatóság tekintetében A gyártási hálózatban folyamatosan változik a csatlakoztatott eszközök száma - új gépek, tesztberendezések, diagnosztikai eszközök kerülnek beüzemelésre. Ez komoly kihívást jelent az eszközazonosítás és a forgalom-ellenőrzés területén.

Korábban előfordult, hogy egy újonnan telepített gyártóegység ismeretlen MAC-címmel jelent meg a hálózatban, ami biztonsági riasztást váltott ki.

Mivel az ipari eszközök gyakran nem támogatják a modern hitelesítési eljárásokat (pl. 802.1X), alternatív megoldásokat kellett alkalmazni.

A Cisco hálózati átállás során bevezetésre került az Identity Services Engine (ISE), amely MAC-cím alapú hitelesítést biztosít, így az ismeretlen eszközök automatikusan karantén VLAN-ba kerülnek. A gyártási switchportokon bevezetésre került a port security limitálás (max. 1 MAC / port), ami megakadályozza a jogosulatlan eszközök csatlakoztatását. A hálózati láthatóság növelése érdekében az SNMP és NetFlow alapú forgalommonitorozás került bevezetésre, amely valós idejű képet ad az OT hálózat működéséről. (Tamás M. , 2021)

A gyártási és informatikai rendszerek közötti együttműködés gyakran akad el a verziókülönbségek miatt. Egyes gyártóberendezések firmware-je nem kompatibilis az újabb hálózati szoftverekkel, ami kommunikációs hibákhoz vezethet.

A hatvani Bosch gyárban több alkalommal előfordult, hogy egy új hálózati frissítés után a gyártóvezérlő eszközök egy része elvesztette a kapcsolatot a szerverrel.

Megoldási lépéseknek lehetnek: Az informatikai osztály és a gyártási mérnökség közösen létrehozott egy tesztkörnyezetet, ahol a frissítéseket éles bevezetés előtt validálják. Minden firmware- és hálózati frissítéshez Change Request kerül kiadásra, amelyet csak jóváhagyás után lehet telepíteni. Az inkompatibilis eszközökhöz átmeneti firmware bridge megoldás készült, ami lehetővé tette a fokozatos átállást az új verziókra.

Az IT és OT csapatok közötti együttműködés néha nem technikai, hanem szervezeti kihívás.

A gyártási rendszerekért felelős mérnökök és az informatikai szakemberek eltérő prioritások mentén dolgoznak: míg az IT az adatbiztonságot és megfelelőséget tartja szem előtt, addig a gyártás a folyamatos működést helyezi előtérbe.

Megoldási lépések:

- Közös IT-OT koordinációs meetingek bevezetése, ahol minden változtatást előre egyeztetnek.
- Egy „Change Freeze Window” bevezetése a gyártási időszakokra, amikor semmilyen hálózati vagy szoftverfrissítés nem végezhető.
- Dokumentált incidenskezelési folyamat készült, amely pontosan rögzíti, hogy egy hiba esetén melyik csapat meddig jogosult beavatkozni.

A gyártási és IT rendszerek integrációja nélkülözhetetlen a modern, adatvezérelt termeléshez, azonban komoly technikai és szervezeti kihívásokat is rejt. A hatvani Bosch gyár példája jól mutatja, hogy a sikeres integrációhoz nem elég a fejlett technológia - szükség van a folyamatos kommunikációra, közös szabványokra és egységes változáskezelésre.

A tapasztalatok alapján az IT és OT rendszerek közötti határvonal fokozatosan elmosódik, és a jövő gyáraiban ezek a rendszerek egy egységes, biztonságos és automatizált ökoszisztémában fognak együttműködni.

3.5 Adatbiztonsági problémák

Bár az elmúlt idők során, miközben az informatikai világa fejlődött, megtanulhattuk, hogyan kell mindennapjaink online terében óvnunk személyes adatainkat, kijelenthetjük, hogy az odafigyelés és szakmai önismeret mellett már-már kevésbé tudunk megfelelni a biztonságos internetezésnek. Sokszor szembe jöhetett már velünk olyan „direkt célzott" E-mail vagy SMS, ami olyan szövegezési formátumot tartalmaz, amely megfelel a standard változatnak. Figyelemmel kell lenni továbbá, ha például internetbankot használunk, valóban azon az oldalon-e adjuk meg bizalmas banki adatainkat, amelyet már szinte mindennap használtunk reflexszerűen. Itt a hangsúly a reflexszerűségen van. A mai rohanó időnkben sokszor átsiklunk bizonyos kritikus fontosságú kulcsszócskákon, amik felkiáltójelként tudnak hatni ránk, egy adott nyugodtabb, szabadidős tevékenységeink között.

Nem mindegy ugyanis, hogy az enbankom.hu helyett az enbaknom.hu oldalra navigálunk. Adataink megadása rosszindulatú weboldalon nem csak személyes adatainkat kompromittálhatja, de akár, például céges számítógépen tárolt adatainkat, mentett jelszavainkat céges központi weblapokhoz, egyéb adatokat is meg tudnak tőlünk szerezni, amit később vagy adathalászat céljára, vagy célzott egy, cég ellen irányuló információszerzés okozatából húznak ki belőlünk. Szinte minden nap hallani a hírekben, hogy a kétfaktoros hitelesítés biztonságot adhat az ügyfeleknek, hiszen ez megakadályozza a hamis weboldalakat. IT-s szempontból azonban, ez egy picit megmosolyogtató. Ha egy hamis weboldal a bejelentkezési adataink után kéri a hitelesítési kódot, amit a banknál megadott telefonszámunkra kapunk meg, egyszerű módon csak begépeljük az ugyan azon bankfiók által használt telefonszámról küldött kódot az adatmezőbe, majd enter gomb megnyomása után 503 Server Error üzenet kapunk, vagy egy tájékoztatót, miszerint a belépés karbantartási munkálatok miatt a bejelentkezési művelet nem lehetséges.

Mi történt? A hamis weboldalra begépelt adatainkat a rendszer egy szerverre elküldi, ahol bizonyos rosszindulatú emberek ezeket az adatokat egy automata program segítségével a valós bank weboldalára pötyögik be. Ekkor a gonosz embernél kér egy hitelesítő kódot a valós bankoldal, ami hamis formában megjelenik az áldozat számítógépének képernyőjén, bizonyítva a rutin kód beírási műveletet. Azonban a célszemély nem tudja, hogy tulajdonképpen Ő lesz az, aki megadja a támadó számára a hamis weboldalon keresztül a saját, a támadó által indított valós bejelentkezés hitelesítő kódját. Íme, a támadó már bent is van az áldozat valós bankfiókjában, míg a célszemély csodálkozik a karbantartási képernyőn, ami egy hamisított tükör másolata a valós internetbank oldalnak.

Ezen példát 'Man it the Middle' támadásnak nevezzük. Ennyit a kétfaktoros hitelesítés hitelességéről. Nem hiába törvényi előírás az IT biztonsági tudatossági képzések tartása a vállalat dolgozói számára, hogy milyen olyan apró jelekre tudnak figyelni, amivel megakadályozható az információ sérülékenység és adattal való visszaélés.

Továbbá fontos, hogy a kiberbiztonságot szorgalmazó szabályozások követelhetik már a vállalatoktól a NIS2 megfelelés érdekében, hogy vezessék be a szigorított hitelesítést, vagy akár a többfaktoros hitelesítési módszer alkalmazását. Erre többféle alkalmazás létezik, például cég által fejlesztett saját fejlesztésű (token alapú), biometrikai, fizikai eszköz (USB Pendrive, SmartCard) de használhatunk Google, vagy Microsoft Authenticatort is.

Az adathalászatra való figyelemfelhívás fontos szereppel bír a vállalatok biztonsága érdekében. Fontos a megelőzés, mivel, ha már kikerülhettek adatok a nyílt hálózatra, már lehet késő cselekednünk. A Bosch vállalatában véletlenszerű időnként (általában negyedévente) a Bosch

központi adtavédelmi osztálya (DSO - Data Security Office) által küldött direkt adathalász E-mailt kiküldeni a kollégák számára, tudván, hányan írják be céges E-mail címkét és jelszavukat az adott „hamis, de a céges környezeti elemeket felhasználó” valósnak is tűnhető oldalra. Ha kiszúrjuk, hogy ez egy célzott adathalász üzenet, az Outlook központi levelező programban ezt tudjuk jelenteni, melyre, ha rákattintunk „Report as Spam” egy gratuláló E-mail küld a központi adatvédelmi osztály, miszerint a felhasználó helyesen járt el. Ha azonban a kolléga megadja az adatait, az adatvédelmi osztály felhívja a figyelmét, hogy bár ez egy Bosch által szimulált adathalász levél, ami nem tárolja a jelszavát, jobban figyeljen oda.

Ezen figyelmeztető email különféle belsős oktatásokat biztosít a felhasználó számára úgynevezett tudatosságnövelő tréningek keretében, melyek bárki számára ingyenesen elvégezhetőek, törekedve ezzel a kollégák IT tudatosságainak védelmére.

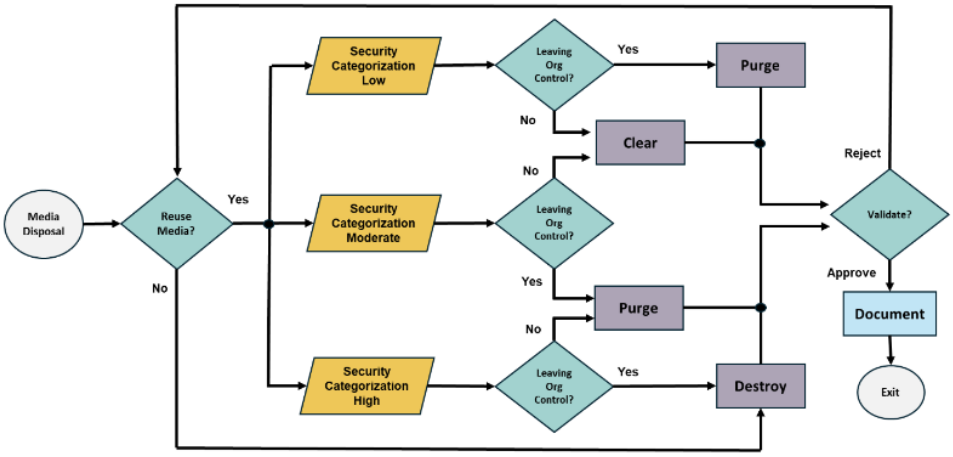
Nem minden az, aminek látszik. Találkozhattunk már E-mail-ben lévő webcím-hivatkozással. Ez egy ártalmatlan, általában kék színnel jelölt hiperhivatkozás. Tehetünk egy próbát, mennyire tudunk biztonságtudatosan olvasni E-mailt mindennapjainkban. Ezen az URL bár úgy látszik, google.com oldalra irányít, a link mögött más oldal található (uni-mate.hu). Ezért nem mindegy, hogy egy hiperhivatkozásnál a megjelenített szöveget vesszük alapul, vagy a linket, ami mögött van.

Nem csak az oldalt tudják hamisítani ily módon, hanem manipulálni tudják az egyes cégek valósnak tűnő bejelentkezési ablakát. Egy, a Bleeping Computer 2022-es cikke alapján a Chrome web böngészőben egy ideig lehetőség volt arra, hogy külön felugró ablakban a célzott személyeket megtévesztve, más cég logóit használva átverjék a felhasználókat a bejelentkezési ablakkal (Single-Sign-On bejelentkezési metódus). Bár ezt a sérülékenységet javították, a rosszindulatú támadók és adathalászok mindig keresnek újabb és újabb módszert arra, hogyan fürkésszék ki a gyanút nem sejtő célszemélyektől az adatokat. Ezt a módszert Böngésző a böngészőben (BitB) támadásnak nevezik, amit a régebbi, elavult böngészőkben még mindig kihasználhatnak. (Lawrence Abrams, 2022)

Egy vállalat során a leselejtezett, eladásra kívánt eszközök sanitizálása rendkívül szigorú protokoll betartásával jár, hogy megelőzzük az esetleges céges vagy személyes adatok kiszivárgásának lehetőségét 3. fél számára. Minden eszköz, mely a gyár területét elhagyja, szükséges az adatok visszaállíthatatlan törlése. Ehhez a NIST által szabványosított 800-88 adatmegsemmisítési megoldást alkalmazzuk alkalmazással, vagy fizikai adatmegsemmisítéssel egyetemben. (Ramaswamy Chandramouli, 2025)

2. ábra: Adattörlés és adatmegsemmisítési folyamat

Forrás: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf



4. Problémaelemzési módszerek

A hibaelhárítás az első és egyik legfontosabb alapelv a hozzáértésnek. Minden problémamegoldó készség, amit el kell sajátítanunk a fizikai rétegnél kezdődik Másszóval, minden hibaelhárítást a legalapvetőbb szinten kell kezdeni Minden be van dugva? minden megfelelően van bekötve? Az ilyen típusú problémákat általában a legkönnyebb elhárítani, és őszintén szólva gyakran ezek a problémát kiváltó fő források. Hálózati kimaradások, a szoftverhibák, és még a végfelhasználói hibák is próbára teszik a problémamegoldó képességeinket bár vannak olyan esetek, amikor a kreatív gondolkozás megoldja a problémát a legfontosabb, hogy az IT-s tapasztalat miatt rendelkezem olyan képességekkel, amilyen a legtöbb probléma megoldásához vezethet.

Mindig el kell kerülni az olyan felesleges lépéseket, amelyek késleltethetik a probléma megoldását, vagy a hibát, amelyek nagyobb problémát okoznak.

Mindig a probléma felmérése az elsődleges pontunk, Adatokat gyűjtünk az ügyfelektől vagy kollegáktól, de közben már használjuk az IT-s megfigyelőképességeinket is. Egy felhasználó például azt hiheti, hogy a probléma egy dologok, ami valójában másról van szó.

Esetleg azt gondolhatja, hogy a számítógépe azért lassú mert vírussal fertőzött, holott valójában csak midig alvó módba tette a laptopját, és csak újra kellett indítania a normális működéshez.

Ezután a fizikai szemrevételezést vesszük alapul. Netán azért nincs hálózat az egyik gépen, mert kábelszakadás van az egyik érpárban? Vagy nem jó alhálózatba került a switchport konfigurálása? Ezek után még koránt sem végeztünk, a 3. lépés a változások keresése. Fel kell derítenünk milyen változások mentek végbe egy adott rendszeren, amitől kezdődően a hibák felmerültek. Egy frissítés? Egy program telepítése? egy hardvereszköz cseréje? Végső lépés, az ötletelés. Fel kell állítanunk elméleteket, ha a hiba továbbra is fennáll. Ez lehet egy vagy több szcenáriók is, mely nyomvonalán elindulva megoldási utat kaphatunk a hiba elhárításában.

Ezen szcenáriókat érdemes rangsoroljuk, hogy melyiknek van a legtöbb valószínűsége, illetve értelme a javítás céljából.

A hibaelhárítás gyakran követlei a kommunikáció hatékonyságát. Mindig fel kell készülnünk, hogy lehet maga a hiba bekövetkezés és az ehhez tartozó elhárítási folyamata olyan időpontban jelentkezik nálunk, ami számunkra kellemetlen idegtépő lehet például egy gyárvezetés előtti laptop lefagyás. Ilyen fontosabb eseteken is mindig készüljünk B-tervel.

A Boschban a problémák gyors és hatékony kezelése érdekében a dolgozók rendelkezésére áll a Hotline, ahol azonnali segítséget kaphatnak kisebb, azonnali megoldást igénylő problémák esetén, valamint az IT Service Desk, amely komplexebb, hosszabb távú megoldásokat koordinál, nyomon követi a hibákat és biztosítja, hogy minden felmerülő probléma dokumentált módon kerüljön kezelésre. A folyamat során érdemes minden eredményt írásban vagy vizuális eszközökkel rögzíteni, hogy a tudás megmaradjon és később is visszakereshető legyen.

A módszerek alkalmazása során figyelembe kell venni a szervezet sajátosságait és a projekt nagyságát, mert kisebb feladatoknál egyszerűbb megközelítés is elegendő, míg nagyobb, összetettebb projektekhez részletesebb és alaposabb elemzés szükséges. Az elemzés sikerességét a követelmények utólagos módosításainak ritkasága, az érintettek elégedettsége és a projekt időben és költségkereten belüli megvalósítása mutatja, és a Boschnál szerzett tapasztalatok egyértelműen alátámasztják, hogy a problémák alapos és rendszeres elemzése elengedhetetlen ahhoz, hogy a projekt kockázatai csökkenjenek, a fejlesztett rendszer a felhasználók igényeit teljes mértékben kielégítse, és a csapat hatékonyan és célzottan tudja végezni a munkáját.

4.1 A gyökérok-elemzés jelentősége

A gyökérok elemzés (Root Cause Analysis) egy rendszerezett, adatokra épülő megközelítés, amelynek célja, hogy feltárja egy probléma valódi, alapvető okait egy szervezeten belüli folyamatban vagy rendszerben. Ennek segítségével nemcsak a tüneteket kezeljük, hanem olyan tartós megoldásokat tudunk bevezetni, amelyek hosszú távon megelőzik a hasonló hibák újbóli előfordulását. (Chrissy Kidd, 2024)

Főállásom mellett vállalnom kell bizonyos időnként (amikor az adott probléma fennáll) az ügyeleti szerepkör betöltését. Egyik napon egy kollegáka felhívott, miszerint két gyártósori állomás nem működik, mert nem tudja elérni a gyártási szervert, ahonnan az előre definiált adatokkal tudna a vezérlőegység a gyártáshoz szükséges adatokat bekérni. Amikor beértem a helyszínre, akkor szembesültem a következő hibaüzenettel, miszerint duplikált IP-címet kapott mindkét állomás vezérlőegysége. Mint kiderült, tesztelés céljából egy olyan IP-címet állítottak be az újonnan beüzemelő állomáson, amely már egy régóta üzemelő állomásra beállításra került valamikor.

Az eset IP-cím ütközést okozott, mivel a kollégák kihagyták azont, a BD informatika osztály által javasolt lépéseket, miszerint minden Bosch hálózatra aktiválandó eszközt jelezni kell a gyártási IT csapat felé, akik biztosítják az új állomásra az IP-címet, elkerülve ezzel a véletlenül egy alhálózatban lévő gépek címütközését. Ez a folyamat elmaradt, mivel a szervizes és beüzemelő kollégáknak magas prioritásban kellett az állomást beüzemelni. A nem felelő folyamat követés miatt olyan állomást is megállítottak, amely szakszerűen átesett ezen a folyamaton. A gyors megállásra felvettem a gyártási IT támogató csapattal a kapcsolatot és biztosítottak olyan IP-címet az alhálózatban, amely szabad, és nincs használatban. Később, miután a hiba elhárult és az állomások újraindítása után mindkét berendezés elindult, E-mail formájában értesítettem az új állomást beállító kollégát a szükséges folyamatokról, hogy a jövőben ilyen ne fordulhasson elő.

A következő 5 miért elemzés (1. Táblázat) segít rendszerezetten feltárni egy probléma valódi, gyökérokát, ezért reprezentatív folyamatként bemutatom, miért következett be az IP-cím ütközés, és hogyan előzhető meg hasonló eset a jövőben.

1. Táblázat: Az 5-miért módszer alkalmazása címütközési problémára
Forrás: saját szerkesztés

Miért kérdés	Válasz / Ok	Megjegyzés / Következtetés
1. Miért nem működnek a gyártósori állomások?	Mert a vezérlőegységek nem tudják elérni a gyártási szervert.	A hálózati kommunikáció megszakadt.
2. Miért nem tudják elérni a szervert?	Mert mindkét állomás duplikált IP-címet kapott.	IP-cím ütközés történt az alhálózatban (VLAN-ban).
3. Miért kapott mindkét állomás azonos IP-címet?	Mert az újonnan beüzemelt állomásra manuálisan egy már használatban lévő IP-címet állíthattak be.	Tesztelés közben nem követték a hivatalos IP-kiosztási eljárást.
4. Miért nem követhették a hivatalos IP-kiosztási folyamatot?	Mert a beüzemelő és szervizes kollégák siettek a gyártósor mielőbbi elindításával, és kihagyták a BD informatika osztály által javasolt állomásbeüzemelési lépéseket.	Az időnyomás és a prioritás miatt a folyamat nem lett betartva, vagy nem volt ismert.
5. Miért nem volt betartva megfelelően a folyamat?	Mert a folyamat követésének fontossága nem volt eléggé tudatosítva, illetve nem volt megfelelő kontroll vagy ellenőrzési pont a hálózati aktiválás előtt.	Képzési és folyamatkövetési hiányosság áll fenn.

Ahogyan a táblázatból kivehető, az 5 Miért módszer (5 Whys) egy egyszerű, mégis hatékony problémamegoldó eljárás, melynek feladata és célja, hogy a felszíni tünetek helyett a probléma valódi, gyökérokát tárja fel. A módszer lényege, hogy egy adott problémára öt egymást követő Miért? kérdést teszünk fel, minden alkalommal a kapott válasz okát vizsgálva.

Ezzel a lépésről lépésre, tégláról téglára történő kérdések feltevésével lehet eljutni a valódi kiváltó okig, amelyet, ha megszüntetünk, a probléma tartósan megoldódik, nem csak átmeneti megoldást ad. Az 5 Miért elemzés különösen hasznos gyártási, informatikai és szolgáltatási folyamatokban, mert átláthatóvá teszi az összefüggéseket, és segíti a folyamatfejlesztést. Bár a probléma felderítése olykor hosszas folyamatnak tűnik, a hiba ignorálás, a nem megfelelő kezelése súlyosabb problémát idézhet elő későbbiekben (például gyakoribb előfordulásokat, termeléskiesési idő megnövekedését)

Fontos kiemelni, hogy mi, mint Informatikán dolgozók mit tehetünk a felvilágosítás mellett, ugyanis ebben mi is hibásak vagyunk egy részben. Mindezen hibasorozat nem eszkalálódott volna abban az esetben, ha csak olyan eszközt, állomást, komponenst engedélyezünk a Bosch hálózatára, amely átment a regisztrálási procedúrán. Jelenleg erre folyamatban van egy rendkívül nagy erőforrást és kapacitást igénylő rendszer bevezetése, a Cisco-SDA bevezetése, mely lehetővé teszi, hogy adott eszköz csak akkor kommunikálhasson a hálózaton, ha annak MAC-címe regisztrálva lett az adatbázisban. Ezáltal, a regisztrációs folyamat közé iktatva egy falat, mellyel megakadályozhatjuk, hogy idegen (vagyis nem regisztrált eszköz) hálózati elérést kapjon a hálózat, ezzel kivédve az esetleges hibásan konfigurált, vagy nem engedélyezett eszközök hálózatra kötését. A Cisco-SDA továbbá egy olyan biztonsági modell, ami segíti a felhasználói és eszközhozzáférés automatizálását és biztonságossá tételét.

Az alábbi 5 lépésből álló pont segítségül szolgálhat bármilyen olyan problémára alkalmazhatóak, melyek még lehetnek számunkra is ismeretlenek, és mi is csak a felderítés közben ismerünk fel:

1. Tárjuk fel a problémát okát: A kommunikáció rendkívül fontos tényezőt játszik mind a hibát észlelő felhasználó, mind az IT-s számára. Egy jól megfogalmazott probléma fél megoldás tud lenni.

2. Gyűjtsünk minél több rendelkezésre álló adatot: Az 5 miért kéredzés kulcsszerepet tud játszani.

3. Azonosítsuk a hibát kiváltó okot, okokat: Meg kell győződnünk arról, hogy a problémát valós megoldással tudjuk elhárítani, amivel nem csinálunk nagyobb kért, és nem jár nagy időveszteséggel.

4. Valósítsuk meg a hibát kiváltó ok megszüntetését: Alkalmazzuk a hibaelhárítást, amely folyamatát a megfelelően kommunikált úton fogunk megoldani,

5. Dokumentáljuk tevékenységeinek: Talán az egyik legfontosabb lépés annak érdekében, hogy milyen megelőző intézkedések, illetve folyamatok során lehet a jövőben elkerülni a felmerülő hibát. Adjunk tanácsot, illetve osszuk meg kollegainkkal is az esetet, ha hasonló hibával szembesülnek, gyorsan tudjanak reagálni egy ezáltal már nem ismeretlen problémára.

4.2 Eszkalációs létrák, incidens kezelési alapok

Az IT-biztonság és a zavartalan működés biztosítása érdekében a Boschnál jól meghatározott eszkalációs létrák és incidenskezelési szabályok működnek, amelyek lehetővé teszik, hogy a felmerülő problémákat gyorsan és hatékonyan kezeljük.

Ha az incidens bonyolultabb vagy magasabb kockázatot jelent, például kritikus gyártási gép kiesése, szerverleállás vagy adatvesztés veszélye áll fenn, az eset az IT Service Desk-hez kerül, ahol a probléma részletes dokumentálása, kategorizálása és a megfelelő szakértőkhöz történő továbbítása történik, és itt érvényesül az eszkalációs létra, amely meghatározza, hogy az adott probléma milyen szintű kezelést igényel, milyen határidőn belül kell reagálni, és melyik csapat felelős a megoldásért.

Az incidenskezelési folyamat során minden lépést rögzítenek a rendszerben, beleértve a probléma leírását, a megtett intézkedéseket és a végső megoldást, így a csapat tanul a korábbi esetekből és a jövőben gyorsabban tud reagálni hasonló helyzetekben. Például, ha egy gyártási folyamatot támogató belső alkalmazás rendszeresen összeomlik, az IT Service Desk a megfelelő fejlesztői és programteszteléssel foglalkozó csapat bevonásával elemzi az okokat, frissítéseket vagy konfigurációs módosításokat javasol, és a megoldás után dokumentálja az intézkedéseket a ServiceNow ticketkezelő rendszerben, hogy a hasonló incidensek kezelését standard, dokuemntált módon lehessen végrehajtani. Az eszkalációs létra és az incidenskezelési alapok tehát biztosítják, hogy a hibák gyorsan, rendszerszerűen és átláthatóan kerüljenek kezelésre, és minimalizálják a rendszerleállásból adódó kockázatokat a Bosch IT-rendszereiben.

2. táblázat: Lokális és központi IT Incidensek bekategorizálása

Forrás: Saját szerkesztés

Kategória	IT szolgáltatáskiesés (O1 – Eseménykezelés)	Magasszintű IT szolgáltatáskiesés (O7light)	IT Krízis (O7 – IT Szolgáltatás Folytonosság Menedzsment)
Leírás	Egy vagy több, a BD által kínált IT-megoldás nem érhető el, vagy csak korlátozottan működik.	Egy vagy több, a BD által kínált IT-megoldás teljesen leállt, és ez jelentős hatással van az üzletileg kritikus folyamatokra.	Egy vagy több, a BD által kínált IT-megoldás teljesen leállt, és az üzletileg kritikus folyamatok leállnak.
Meghatározás	IT szolgáltatáskiesésnek minősül az, amikor az egyik vagy több IT-megoldás rendellenességet mutat a megszokott működéshez képest.	Magasszintű IT szolgáltatáskiesésnek számít, ha jelentős mértékben romlik az üzletileg kritikus folyamatok működése.	IT krízis akkor áll fenn, ha az üzletileg kritikus folyamatok súlyosan érintettek és teljesen leállnak.
Fő jellemzők	- Üzleti folyamat (pl. gyártás, szállítás, értékesítés) megszakadása.	- A leállás időtartama **valószínűleg 4 óránál hosszabb**.	- A leállás időtartama **nem kiszámítható**.
	- Magas rendelkezésre állású IT-szolgáltatás vagy termék kiesése.	- Az ok részben ismert, de az elhárítás ideje nem biztos.	- Az ok **ismert és az egész BD Crisis Team tud róla**.
	- Szállítási határidők vagy ügyfélhez kapcsolódó kötelezettségek nem tarthatók.	- Több üzleti terület érintett.	- A helyzet **nem kezelhető szokásos eljárásokkal**.
	- Jelentős minőségromlás (pl. szoftverhiba, vírus, biztonsági probléma).	- Üzletileg kritikus folyamat sérül egy meglévő SLA megszegésével.	- Üzletileg kritikus folyamat sérül egy meglévő SLA megszegésével.
Felelős személy / döntéshozó	A **Critical Ticket Lifecycle Management csapata** elindítja a kritikus jegy folyamatot és bevonja a **Validation Manager-t (VaM)**, ha szükséges.	A magasszintű IT kiesést a BD informatikai osztály krízis-vezetője hirdeti ki.	Az **IT krízist** a BD informatikai osztály krízis-vezetője hirdeti ki.
Lezárási feltétel	Az IT szolgáltatáskiesés / Magasszintű IT szolgáltatáskiesés / IT Krízis véget ér, ha az IT-megoldás vagy a kerülő megoldás (workaround) újra elérhető és működőképes.		

Az IoT rendkívüli előretörésével, valamint a vállalati informatikai környezetben robbanásszerűen terjedő automatizáció következtében a vállalatok komoly kihívásokkal néznek szembe. Napi szinten hallhatunk híreket arról, hogy különböző cégek zsarolóvírus-támadás áldozatává váltak, vagy adathalászati kísérletek célpontjai lettek, amelyek következtében bizalmas, illetve szigorúan bizalmas adatok kerültek nyilvánosságra. (Csanád, 2025)

A huszonegyedik században a kiberbiztonság fenntartása, bevezetése és rendszeres felülvizsgálata már stratégiai fontosságú kérdéssé vált. Az üzletmenet-folytonosság szempontjából elengedhetetlen olyan megelőző intézkedések kidolgozása, amelyek biztosítják, hogy a gyártási folyamatban részt vevő állomások, valamint a munkavállalók céges laptopjai és az azokon tárolt adatok a megfelelő titoktartási követelményeknek megfelelően, illetéktelenek számára hozzáférhetetlen módon legyenek kezelve. Ebben segít az Európai Unió új kiberbiztonsági szabályozása, a NIS2 irányelv.

A NIS2 a tagállamok számára egységes elvárásokat fogalmaz meg az incidensek kezelésére, valamint a bekövetkezett eseményeket követő válságkommunikáció folyamatára. A dokumentum részletesen ismerteti azokat a pontokat, amelyek betartása segíti a vállalatokat a kiberbiztonsági incidensek megelőzésében. (Dr. Váczi Dániel, 2025)

Kiberbiztonsági incidensnek nevezünk minden olyan eseményt, amely megsérti vagy veszélyezteti az informatikai rendszerek bizalmasságát, sértetlenségét vagy rendelkezésre állását például egy rosszindulatú program terjedését, adatlopási kísérletet, jogosulatlan hozzáférést vagy hibás konfigurációt. Az incidensek súlyosságától függő bekategorizálása nem csak technikai kérdés, hanem stratégiai is: fel kell mérnünk, hogy a Bosch hatvani telephelye mennyire felkészülten, határozottan és gyorsan tud reagálni egy esetleges kibertámadásra.

Az ebből következő incidenskezelés lépéseit a NIS2 dokumentum részletesen meghatározza. Minden szervezetnek rendelkeznie kell egy írásban rögzített incidenskezelési tervvel. A Robert Bosch-nál ezt Emergency Concept néven ismerjük. A dokumentum olyan irányelveket tartalmaz, amelyek segítségével az IT-csapatok felismerhetik, elemezhetik és dokumentálhatják az informatikai incidenseket.

Ha rendellenes vagy gyanús tevékenységet észlelünk, azt elemzés követi, amely során a szakemberek megállapítják, hogy valóban támadásról van-e szó, és mekkora a kockázat mértéke. Amennyiben valós vészhelyzettel állunk szemben, azonnal meg kell tenni az Emergency Concept-ben rögzített intézkedéseket. Ilyenkor a kijelölt kríziscsapat és a központi krízis csapat bevonásával gyors reagálást kell biztosítani a károk minimalizálása, valamint a vírusok vagy férgek további terjedésének megakadályozása érdekében. A fertőzött gépeket izoláljuk, a kompromittált hozzáféréseket letiltjuk, és a biztonsági csapat megkezdi a rendszer helyreállítását.

A vállalat minden gyártással foglalkozó telephelyén kötelező egy helyszíni koncepció (Location Concept) megléte, amelyet központi direktíva ír elő. Ezt a dokumentumot jómagam és kollégám készítettük a logisztikai és létesítménygazdálkodási területekre. Az anyag 57 oldalas, magyar és angol nyelven is elérhető, és bárki számára megtekinthető. Legfontosabb alapelve, hogy minden logisztikai és létesítménygazdálkodási rendszerhez tartozzon mentés és visszaállítási dokumentáció.

3. ábra: A hatvani telephelyre készített helyszíni koncepció tartalomjegyzéke
Forrás: Saját szerkesztés

	Helyszíni koncepció Logisztika (OTL) és Létesítménygazdálkozás (OTR) területeire	Verziószám: 1.0	Oldal 1/57	BOSCH
Kiadó: BD/SLE-EET3	Htv Location Concept for OTL, OTR – [HU]	Szerző BD/SLE-EET3	Dátum 2025 október 17.	

Bizalmassági	Elérhetőség	Változásvédelem
1	1	1

Tartalomjegyzék – I.

Amikor főállásban csatlakoztam a Robert Bosch csapatához, első feladataim közé tartozott a meglévő biztonsági mentési dokumentumok felülvizsgálata. Sajnos azt tapasztaltam, hogy több dokumentáció hiányos volt - például nem tartalmazta a mentés és visszaállítás időtartamát. A központi direktíva áttanulmányozása után kiegészítettük ezeket az anyagokat olyan alappillérekkel, amelyek biztosítják, hogy egy esetleges NIS2-audit során a cég megfeleljen az előírt követelményeknek.

Az új dokumentum már tartalmazza a gépeken található szoftverek és felhasználók listáját, a jogosultsági csoportokat, a telepített frissítéseket, valamint az esetleges sérülékenységeket is,

nyitott pontként kezelve. A backup-restore folyamatot évente legalább egyszer el kell végezni, hogy mindig a legfrissebb mentéssel rendelkezzünk. A dolgozókat is oktatjuk, hogy hiba esetén - akár a helyszínen kívül is képesek legyenek a helyreállítás végrehajtására.

4.3 8D riport és annak alkalmazása

Az elmúlt négy évem során a Bosch hatvani gyárában szerzett tapasztalataim során világossá vált számomra, mennyire kritikus a minőségbiztosítás az autóipari gyártásban. A hibamentes gyártás nem csupán a végtermék minőségét biztosítja, hanem a teljes beszállítói lánc átláthatóságát is, ami elengedhetetlen a hatékony termeléshez.

A 8D egy olyan problémamegoldó módszer, mely segítségével a hibák gyorsan azonosíthatók, a gyökérokok feltárhatók, ezáltal hosszútávú megoldások születhetnek. Célom, hogy bemutassam a 8D eljárás működését. Mivel a 8D igen átlátható és egyszerű, lehet kombinálni más megoldómódszerekkel is, mint például az öt miért-el. A 8D eljárás nyolc lépésből álló, szisztematikus problémamegoldó módszer, amely elsősorban sorozatgyártásban, főként az autóiparban alkalmazott. A célja nem csupán a hiba kiküszöbölése, hanem annak gyökérokának azonosítása és hosszú távú megszüntetése.

A 8D problémaelemző módszer általában közép és nagyvállalatok minőségbiztosítási alappillére. Párhuzam vonható az ipar fejlettsége, és a benne közreműködő vállalatok nagysága között, valamint elmondható, hogy minél bonyolultabb az előállított végtermék, annál több az előállításában közreműködők száma. A gépjárműgyártó nagyvállalatok számos beszállító nagy-vállalatot foglalkoztatnak, ezért jellemzően ebben az iparágban magas a 8D eljárást használók száma (53%). Azonban más iparágakban is találkozhatunk a metódust felhasználó vállalatokkal. A felhasználók körében a gépipar (24%), az elektronikai ipar (18%), a kémiai ipar (3%) is képviselteti magát. (Koncz Annamária, 2015)

A gyakorlatban azt tapasztaltam, hogy a 8D módszer elsősorban a nagyobb és közepes vállalatoknál működik jól, mivel ezeknél a beszállítói lánc bonyolult, és több folyamatot külső cégek végeznek. A módszer alkalmazása egyenes arányban áll a vállalat méretével és a termék komplexitásával. Kisvállalkozásoknál ritkábban alkalmazzák, mivel a folyamatok kevésbé komplexek, és a hibák gyorsabban lokalizálhatók.

A 8D eljárás nyolc lépésből áll, amelyek a PDCA-ciklusnak megfelelően csoportosíthatók:

D1 - A 8D csoport létrehozása

A probléma kezelésére különböző részleghez tartozó kollégákat hívunk össze, amely az IT, termelés és szervizes kollégákból áll. A csapat feladata, hogy a problémát átfogóan vizsgálja, és a lehető leggyorsabban javasoljon megoldásokat.

D2 - A probléma leírása

Például ügyeleti esetben egy előre elkészített form segítségével megyünk végig a gyors kérdéseken: mikor jelentkezett a hiba, melyik állomás érintett, ki a másodlagos kontaktszemély.

D3 - A hiba elszigetelése

A problémát a lehető legszűkebb körre korlátozzuk, például egy adott gépsorra. Itt az IT rendszerek nagy segítséget nyújtanak, mert a gyártási folyamatok valós idejű adatainak elemzése gyorsítja a hibák azonosítását.

D4 - A gyökérok feltárása

Ebben a lépésben alkalmazzuk az 5 Miért? módszert a hiba kiváltó okainak feltárására. Gyakorlati példaként már bemutatott IP-cím ütközési probléma diagramábrájával felérkezhetjük azon gyökérokokat, melynek segítségével a hiba elkerülhető lesz a közeljövőben.

D5 - Végleges javító intézkedések kiválasztása

A lehetséges megoldások közül kiválasztjuk azokat, amelyek hosszú távon is megakadályozzák a hiba ismétlődését. Ezen pontál a gyártási informatikai rendszerek segítségével megfigyelhetjük a javulást, és előre láthatjuk, mely intézkedések a legmegfelelőbbek.

D6 - A javító intézkedések megvalósítása

A kiválasztott intézkedéseket ismertetjük és alkalmazzuk. Informatikai szempontból ez gyakran magában foglalja a szoftverek konfigurálását, adatbázisok frissítését, és a hibák automatikus monitorozását.

D7 - Visszacsatolás

A bevezetett intézkedések eredményét dokumentáljuk, és visszajelzést adunk a csapatnak és az érintett értékáramnak. Ez biztosítja, hogy minden érintett tisztában legyen a gyártási állomáson történt változtatásokkal és az elért eredményekkel.

D8 - A csapatmunka elismerése

Nincs is annál jobb érzés, mint tagja lenni egy olyan problémamegoldásnak, melybe mindannyian valami formában közös munkát tettünk. A Bosch környezetben gyakori, hogy a sikeres 8D riportot a vállalati portálon is közzéteszik, mint jó gyakorlatot (best-practice).

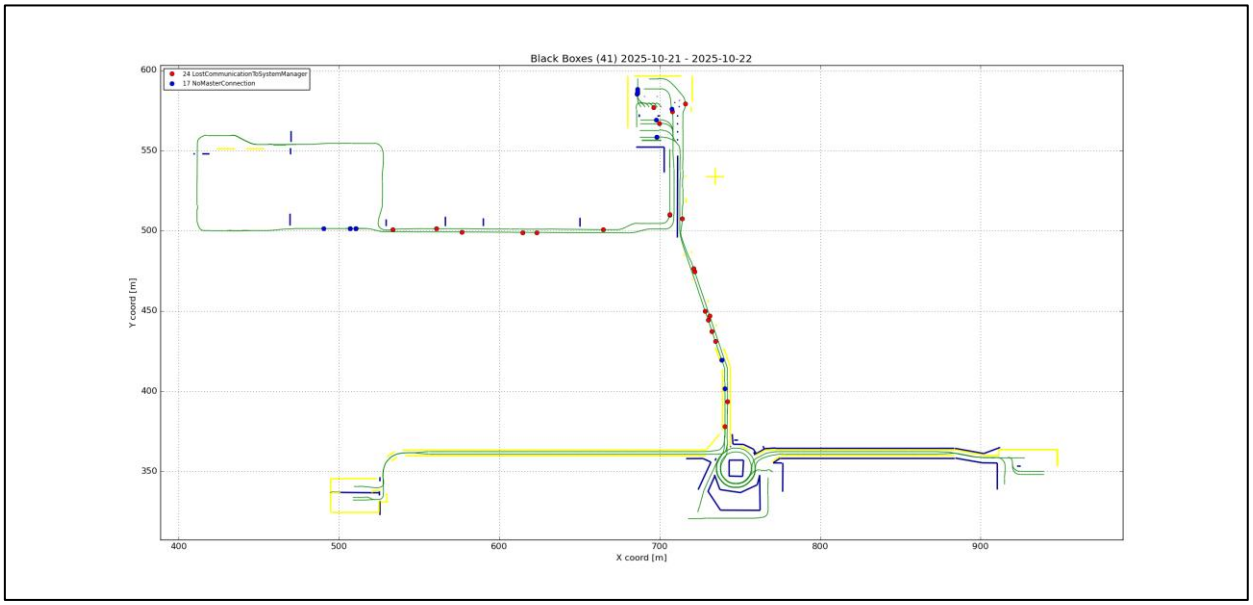
A Bosch gyárában a szoftveres nyomon követés, a riportálás és a folyamatok monitorozása szoros összekapcsolásban van a 8D folyamattal, így az informatikai rendszerek kulcsszerepet kapnak a problémamegoldásban.

5. Esettanulmány (Valós incidens problémamegoldása)

A szakdolgozat gyakorlati részében egy, a Bosch Hatvani Gyárában bekövetkezett valós informatikai incidens kerül bemutatásra és elemzésre. Az esettanulmány célja, hogy szemléltesse, milyen komplex problémák merülhetnek fel egy ipari környezetben működő vezeték nélküli hálózat és automatizált anyagmozgató rendszer (AGV - Automated Guided Vehicle) együttműködése során, illetve milyen lépések vezethetnek a hiba pontos azonosításához és hosszú távú megoldásához.

A gyárban 2025 elején jelentkeztek először a Toyota által üzemeltetett AGV-flotta kommunikációs problémái. A 25 darab, WiFi-hálózatra csatlakozó jármű időszakosan megszakította a kapcsolatot a központi szerverrel, ami az automata szállítási folyamatokat lelassította, illetve bizonyos esetekben le is állította. A hibajelenségek elsősorban az AGV-k mozgásának megtorpanásában, illetve az útvonal-információk elvesztésében mutatkoztak meg.

4. ábra: A Toyota forgalom megjelenítőjén pirossal ábrázolt AGV-k megállásai
Forrás: Saját szerkesztés



A probléma különösen kritikus, mivel az AGV-k valós idejű, megszakításmentes adatkapcsolatra támaszkodnak. Már néhány másodperces kommunikációs kiesés is az útvonal újrakalkulálását, vagy a jármű teljes leállását eredményezheti. Az eset rámutat arra, hogy az ipari WiFi-hálózatok tervezése és üzemeltetése során nemcsak a lefedettség, hanem a stabil roaming és az interferenciamentes kommunikáció is kulcsfontosságú.

A vizsgálat során mind a Toyota, mind a Bosch több szakmai csapata - helyi IT, hálózati szakértők, valamint a Cisco TAC - bevonásával elemezte a hibát. A feltárt adatok és tesztek alapján számos lehetséges ok merült fel, a hardveres cseréktől kezdve a firmware- és hálózati konfigurációs problémákig.

A következő alfejezetek részletesen ismertetik az esettanulmány célját, a vizsgálat módszertanát, a hibaazonosítás folyamatát, valamint azokat az intézkedéseket, amelyek a probléma megoldását szolgálták.

5.1 Az esettanulmány célja és kérdései

Az esettanulmányom célja az volt, hogy bemutassam, hogyan azonosítható és kezelhető egy vállalati szintű, ipari WiFi hálózaton jelentkező kommunikációs hiba, amely automatizált gyártási folyamatokat érint. A Bosch Hatvani Gyárában működő Toyota AGV-rendszer egy komplex, több komponensből álló infrastruktúrára épül, amelynek megbízhatósága közvetlen hatással van a termelési folyamatok folytonosságára és hatékonyságára.

A célom, hogy a konkrét incidensen keresztül bemutassam:

hogyan történik a hiba detektálása, naplózása és visszakövetése egy több alrendszert érintő hálózati környezetben,

milyen módszerekkel lehet elkülöníteni a hálózati, hardveres és szoftveres hibákat,

hogyan zajlik a kommunikáció a vállalati IT különböző szintjei között (L1-L3 támogatás, gyártó bevonása, Cisco TAC),

és milyen intézkedések szükségesek egy ipari WiFi infrastruktúra optimalizálásához, hogy az megfeleljen a valós idejű adatátvitelt igénylő rendszerek követelményeinek.

Az AGV WiFi-probléma vizsgálata kiváló példa arra, hogyan találkozik a vállalati informatikai háttér és az ipari automatizálás. A hálózat stabilitása itt nem csupán „felhasználói kényelem” kérdése, hanem közvetlenül befolyásolja a gyártás termelékenységét. Egy rövid ideig fennálló kommunikációs megszakadás is az automata jármű leállását, a folyamatlánc megszakadását, vagy akár anyagmozgatási torlódásokat okozhat.

A vizsgálat során ezért a cél az volt, hogy a kommunikációs láncot - az AGV komponenseitől a Cisco hozzáférési pontokon (Access Point) át egészen a központi WiFi vezérlőig - minden rétegében elemezzük. A fő kérdések, amelyekre választ keresett a csapat:

- Mi okozza az AGV-k időszakos hálózati megszakadását, és ezek milyen mintázatot követnek?
- A probléma forrása hardveres, szoftveres, vagy konfigurációs jellegű?
- Hogyan hat a WiFi-hálózat sűrűsége, az access pointok elhelyezkedése és az interferencia az AGV-k roaming viselkedésére?
- Milyen optimalizálási lehetőségek vannak a hálózati infrastruktúra és a kliensek oldalán a stabilabb adatkapcsolat érdekében?
- Milyen módszerekkel lehet hosszú távon biztosítani a rendszer megbízható működését, elkerülve a hasonló incidenseket?

Az esettanulmány során tehát nem csupán a konkrét hibajelenségre kerestem választ, hanem a mögötte húzódó hálózati működési elvek megértésére is törekedtem. Informatikusként különösen érdekes volt látni, hogyan reagál a hálózat valós időben egy mozgó, folyamatosan roamingoló eszközflottára, és milyen finomhangolások szükségesek ahhoz, hogy az ipari WiFi valóban stabil, késleltetésmentes adatátvitelt biztosítson.

5.2 A vizsgálat módszertana

A vizsgálatom célja az volt, hogy az AGV-k és a gyári WiFi-infrastruktúra közötti kommunikációs hibákat szakszerű módon azonosítsuk. A probléma összetettsége miatt a vizsgálatot több szinten, szakaszosan végeztük, a hardveres, szoftveres és hálózati komponenseket egyaránt bevonva.

Minden beavatkozást mérések, loggyűjtések és visszacsatolások követtek, amelyek alapján a következő lépés meghatározhatóvá vált. A vizsgálat során a cél a hibaforrás pontos lokalizálása, a lehetséges befolyásoló tényezők kizárása, valamint a hálózati konfiguráció optimalizálása volt.

A hiba felismerése a Toyota által üzemeltetett AGV-flottát monitorozó rendszerből indult ki. Az AGV-k központi PLC-je (CVC600) folyamatosan naplózta a kommunikációs megszakadásokat, amelyeket a Toyota virtuális szervere vizualizált térképes hibajelöléssel, pontos időbélyegekkel és pozícióadatokkal.

A Bosch IT csapata ezen adatok alapján kezdte meg a hibák elemzését. Az adatokat kiegészítettük:

- WiFi Controller naplózásokkal (eseménybejegyzés, időtúllépés roaming események),
- Cisco Access Point naplókkal (RSSI, SNR, roaming előzmények),
- AGV-kliensek hálózati diagnosztikai adataival, valamint helyszíni megfigyelésekkel és videófelvételekkel az AGV mozgásáról.

A mérések célja az volt, hogy azonosítsuk a kapcsolatmegszakadások időbeli és térbeli mintázatát, valamint elkülönítsük, hogy a hiba melyik rétegben (fizikai, hálózati, vagy alkalmazási) jelentkezik.

A hibakeresés során szisztematikusan vizsgáltuk az AGV három fő komponensét:

- Zebra ET40 tablet - központi kommunikációs felület, amely az útvonal adatokat kapja és továbbítja.
- LSR2000 lézerszenzor - akadály- és pozícióérzékelésért felelős eszköz.
- CVC600 PLC - a mozgásvezérlés központi egysége.

A Toyota több cserét is végrehajtott (tablet, szenzor, PLC), de ezek nem hoztak változást. Az IP-konfiguráció statikusról DHCP-re váltása sem befolyásolta a hibajelenséget, ami megerősítette, hogy a probléma nem eszközoldali vagy protokollszintű, hanem hálózati kommunikációhoz köthető.

A hálózati elemzés során több eszközt és módszert alkalmaztunk:

Cisco WLC konfiguráció- és firmware-elemzés mellett az időtúllépés, roaming paraméterek és rádiós beállítások vizsgálata.

Ekahau Site Survey és Spektrum Analízis, az Access Pointok elhelyezkedésének, lefedettségének, interferenciájának és csatornaelosztásának vizsgálata.

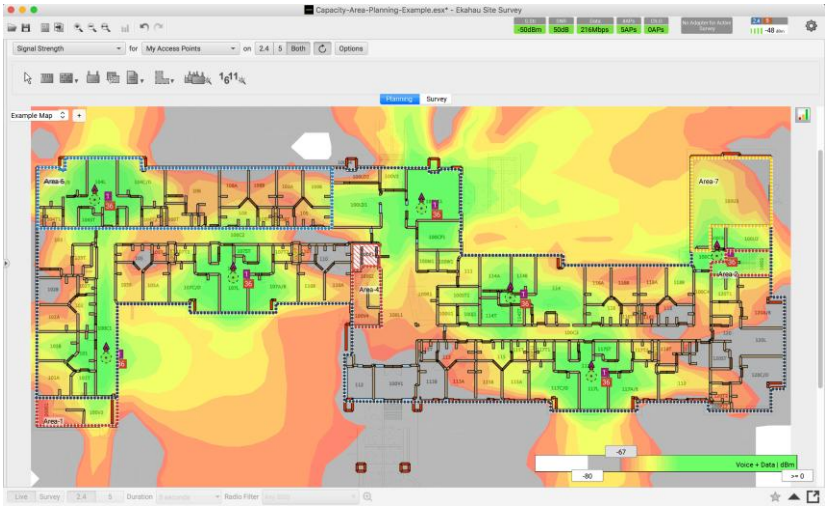
Wireshark és ping trace mérések - az adatfolyam késleltetésének és a kapcsolatmegszakítások idejének rögzítése.

WGB (Workgroup Bridge) loggyűjtés - a Cisco 9120 WGB egységek firmware-szintű hibáinak feltárása.

A vizsgálat során megállapítást nyert, hogy a kommunikációs hibák periodikusan ismétlődnek, és nem helyhez kötöttek, hanem mozgás közben, roaming események során következnek be.

5. ábra: Az Ekahau programmal generált WiFi lefedettségi (heatmap)

Forrás: https://www.ekahau.com/solutions/wi-fi-heatmaps



A Cisco TAC bevonásával végzett elemzés során kiderült, hogy a firmware egy ismert hibát tartalmazott: az M2 csomagban hibás PMKID-t (Pairwise Master Key Identifier) küldött roaming közben, ami hitelesítési hibát eredményezett.

A firmware frissítése részleges javulást hozott, de nem szüntette meg a jelenséget teljesen. Ezt követően a WGB oldali „scanning threshold” és „roaming aggressiveness” paraméterek módosítása történt meg, amely további stabilitásjavulást eredményezett.

A vizsgálat során több szintű eszkalációs folyamatot követtünk:

- L1 (Hotline / helyi IT támogatás) - első szintű diagnosztika, adatgyűjtés.
- L2/L3 (Network LAN & WiFi Team) - konfigurációs és firmware-szintű elemzések, mérési adatok értékelése.
- Cisco TAC (gyártói támogatás) - firmware-hibák vizsgálata, javított verziók biztosítása.
- Ez az együttműködési modell biztosította, hogy a probléma technikai mélységében is feltárható legyen, és a lehetséges megoldások összehangoltan kerüljenek bevezetésre.

A vizsgálat végén az egyik legfontosabb következtetés az volt, hogy az AGV útvonalain túl sok Access Point található, ami felesleges roaming eseményeket és rádiós interferenciát okoz. (M. Mahanta, 2025)

A következő lépésként ezért a teljes gyárterület pontos WiFi layout-felmérése szükséges Ekahau Sidekick eszközzel, amely alapján a csarnokok rádiós újratervezése megvalósítható lesz. Ennek célja, hogy a lefedettség optimalizálásával és a redundáns AP-k kizárásával csökkenjen a roaming események száma, ezáltal az AGV kommunikáció stabilabbá váljon.

5.3 A vizsgálat folyamata és esettanulmányi bemutatása

A vizsgálat 2025 elején kezdődött, amikor a Toyota jelezte, hogy a Bosch hatvani gyárában üzemelő, 25 darabból álló AGV-flotta (Automated Guided Vehicle) időszakosan megszakítja a kapcsolatot a központi virtuális szerverrel. A hiba az automatizált szállítási folyamatokat is érintette, mivel az AGV-k a szervertől kapják az aktuális útvonal és pozíció adatokat, ezért már rövid kommunikációs kiesés is a jármű megállását vagy az útvonal elvesztését eredményezte.

A hibát több forrás is megerősítette. A Toyota által üzemeltetett monitoring rendszer a CVC600 vezérlő PLC adatait gyűjtve hibatérképeket generált, amelyek pontos pozíciók alapján mutatták a kapcsolatmegszakításokat. Emellett videófelvételek és helyszíni megfigyelések is alátámasztották, hogy a járművek időnként megtorpannak, majd újra kapcsolódás után folytatják a mozgást. Ezek az adatok egyértelművé tették, hogy a hiba ismétlődő és hálózati jellegű, nem egyedi eszközhibáról van szó.

A Bosch és a Toyota szakemberei első körben az AGV-komponensek felől közelítették meg a problémát. Lecserélték az ipari Android 6.0 tabletet egy Zebra ET40 modellre, ellenőrizték az LSR2000 lézerszenzor működését, valamint kipróbáltak egy tartalék CVC600 PLC-t is. A módosítások azonban semmilyen változást nem hoztak, és az IP-konfigurációk módosítása (statikusról DHCP-re váltás) sem eredményezett stabilabb kapcsolatot. Mindez arra utalt, hogy a probléma nem az eszközökben, hanem a vezeték nélküli kommunikációs láncban keresendő.

A hálózati oldal vizsgálata során a naplózott eseményekben jól látható periodikusság volt megfigyelhető: a kapcsolatmegszakítások napi rendszerességgel, de különböző időpontokban, mégis hasonló időközönként következtek be. A Cisco Wireless LAN Controller (WLC) naplófájlai, az AP-k RSSI/SNR értékei és a WGB (Workgroup Bridge) naplói alapján feltételezhető volt, hogy a probléma roaming események során lép fel, amikor az AGV mozgás közben egyik AP-ról a másikra vált.

Rövid távú megoldásként először a WLC-n konfigurált SSID session időtúllépési értékét emeltük meg a maximális, 86 400 másodperces határra, ami átmenetileg csökkentette a megszakítások számát. Ezt követte a fast roaming funkció aktiválása mind a WLC, mind az AGV kliensoldalán, amely kis mértékű javulást hozott. Teszteltük továbbá a 2,4 GHz-es sáv használatát is az 5 GHz helyett, bízva abban, hogy a nagyobb lefedettség csökkenti a roaming gyakoriságát, ám a zsúfoltabb rádiós környezet miatt ez sem bizonyult tartós megoldásnak.

A következő lépésben a Bosch hálózati csapata a Cisco TAC (Technical Assistance Center) bevonásával mélyebb firmware- és protokollszintű elemzést indított. A Cisco szakértői a logok alapján azonosították, hogy a Cisco 9120 WGB eszközök firmware-ében egy ismert hiba található: a roaming során az M2 csomagban helytelen PMKID (Pairwise Master Key Identifier) kerül elküldésre, ami hitelesítési hibát eredményez a kliens és az access point között. Ez a firmware-szintű roaminghiba volt az első olyan tényező, amely technikailag magyarázhatta az AGV-k kommunikációs megszakításait.

A javított firmware telepítése után a hiba előfordulása jelentősen redukálódott, a korábbi gyakori megszakítások helyett csak ritka, elszórt hibák maradtak. A WGB oldali konfigurációt ezt követően tovább finomítottuk, módosítva a szkennelési érték és a roaming telejsítményi paramétereket, valamint pontosítottuk a WLC oldali RF-profilokat és hitelesítési időzítéseket. Ezek a beavatkozások további stabilitásjavulást eredményeztek, és az AGV-k kommunikációja érezhetően megbízhatóbbá vált.

A vizsgálat jelenleg is elemzés alatt áll, azonban a rendelkezésre álló adatok alapján nagy valószínűséggel a Cisco vezérlőszoftver roaminghibája okozta a kommunikációs problémákat. A WGB access point firmware frissítése megoldás felé terelte az esetet, és jelenleg is folyamatos megfigyelés zajlik, hogy a változtatások hosszú távon is stabil működést eredményeznek-e.

A hálózati mérések egy másik fontos tanulsága, hogy az AGV-k által bejárt útvonalak mentén túl sok Access Point található, ami felesleges roaming eseményeket generál, és növeli a rádiós interferencia esélyét. Ennek kezelésére a következő lépésként egy részletes, csarnokszintű WiFi-layout felmérés készül az Ekahau Sidekick eszközzel. Az így készült rádiós térkép segítségével a Bosch L2/L3 hálózati csapata optimalizálni tudja majd az AP-k elhelyezkedését, kizárva a feleslegesen átfedő cellákat, és biztosítva az AGV-flotta számára a folyamatos, megszakításmentes kommunikációt.

A vizsgálat során egy összetett, több réteget érintő probléma nyert kilátást, amely egyszerre érintette a hálózati infrastruktúrát, a rádiós környezetet és a firmware-szintű működést. A Cisco roaming firmware hibájának azonosítása és a WGB AP-k frissítése kulcsszerepet játszott abban, hogy a kommunikációs hibák száma drasztikusan csökkenjen. A frissítés után az AGV-k hálózati viselkedése sokkal stabilabbá vált, a roaming események kezelése gyorsabb és hibamentesebb lett, ami a gyártási folyamatok folytonosságában is azonnal érzékelhető javulást eredményezett.

A folyamat jól példázza, hogy az ipari informatikai környezetben a hibák gyakran több tényező együttes hatásából erednek, ezért a diagnosztikát mindig több szinten kell végezni: fizikai, hálózati, szoftveres és konfigurációs rétegekben egyaránt. Az ilyen típusú hibák megoldása nem kizárólag egy adott eszköz újrakonfigurálását jelenti, hanem a teljes kommunikációs lánc viselkedésének átfogó elemzését.

A vizsgálat során az is bebizonyosodott, hogy a firmware-kezelés (lifecycle management) és a verziók nyomon követése kulcsfontosságú tényező az ipari hálózatok stabil működéséhez. A Cisco roamingmodul hibája rávilágított arra, hogy egy apró szoftverkomponens is komoly gyártási fennakadásokat okozhat, ha a rendszer nem megfelelően monitorozott vagy nem frissül időben. Az ilyen környezetekben ezért elengedhetetlen a firmware-verziók központi nyilvántartása, az automatikus értesítések bevezetése, valamint a változások előzetes tesztelése izolált környezetben, mielőtt éles üzemben kerülnek bevezetésre.

A vizsgálat másik tanulsága, hogy a túlzottan sűrű AP-elhelyezés, illetve az egymást átfedő rádiós cellák instabilitást okozhatnak a roaming folyamatban. Az AGV-k mozgása során minden felesleges átváltás növeli a megszakítás kockázatát, ezért a hálózati térkép optimalizálása legalább olyan fontos, mint a kliensoldali beállítások. Az Ekahau-alapú rádiós felmérés segíti majd a Bosch hálózati csapatát abban, hogy a jövőben célzottan, adatvezérelten tudják módosítani az AP-k helyzetét és teljesítményét, csökkentve a zajt és az interferenciát.

A projekt technikai és szervezeti szempontból is értékes tapasztalatokat hozott. Megmutatta, hogy a hálózati stabilitás egy ipari környezetben nem csupán informatikai kérdés, hanem közvetlen termelésbiztonsági tényező is. A sikeres hibaelhárítás mögött több terület szoros együttműködése állt: a Bosch IT hálózati mérnökei, a Toyota fejlesztői és a Cisco TAC szakértői közösen, adat- és logalapú megközelítéssel, egymás kompetenciáira építve jutottak el a megoldáshoz.

6. Összefoglalás

Dolgozatom központi témája a vállalati informatikai problémák és azok megoldási javaslatainak bemutatása volt, különös tekintettel az ipari környezetben jelentkező hálózati és üzemeltetési kihívásokra. A célom az volt, hogy bemutassam, milyen összetett feladatot jelent a gyártást kiszolgáló informatikai rendszerek működtetése, és milyen módszertanokkal, eszközökkel és csapatmunkával lehet a felmerülő hibákat hatékonyan kezelni.

Az elmúlt években az informatika szerepe alapjaiban változott meg a vállalatok működésében. A korábban támogató, háttérfunkcióként kezelt IT mára a termelés, az üzleti döntéshozatal és a vállalati biztonság egyik kulcstényezőjévé vált. A Hatvani Robert Bosch Elektronika Kft.-nél eltöltött négy év szakmai tapasztalat alapján világosan látszik, hogy a gyártóüzemi informatika (Operational Technology - OT) és a klasszikus vállalati IT közötti határvonal fokozatosan elmosódik. Az ipar 4.0 elvárásainak megfelelően a gyártóberendezések, szenzorok és hálózati eszközök már nem önálló egységek, hanem egy egységes, felügyelt informatikai ökoszisztéma részei.

Dolgozatomban bemutattam azokat a tipikus vállalati IT-feladatokat és problémaköröket, amelyekkel a modern gyártási környezetben nap mint nap találkozni lehet: felhasználó- és jogosultságkezelés, biztonsági mentések és hozzáférési szabályozások, a CMDB (Configuration Management Database) karbantartása, a hálózati infrastruktúra felügyelete, valamint az információbiztonsági előírások betartása. Ezek mind olyan tevékenységek, amelyek elsőre adminisztratívnak tűnhetnek, de a gyakorlatban meghatározzák a termelés megbízhatóságát.

Az esettanulmány részben egy valós problémát dolgoztam fel: a Bosch hatvani gyárában üzemelő AGV-rendszer hálózati instabilitását. A konkrét hibaelemzés bemutatta, hogy a vállalati informatikai rendszerekben a hibák sokszor nem egyetlen okra vezethetők vissza, hanem több tényező - hálózati beállítások, firmware-hibák, rádiós interferenciák - együttes hatása idézi elő őket. Az elvégzett vizsgálatok, firmware-frissítések és hálózati finomhangolások nemcsak a konkrét hibát csökkentették, hanem rávilágítottak a strukturált hibakezelési folyamat fontosságára is.

6.1 Dolgozatom összefoglalás

Dolgozatom felépítése három fő részből állt: elméleti háttér, vállalati informatikai működés bemutatása, valamint egy konkrét esettanulmány elemzése. Az elméleti részben áttekintettem a vállalati IT-rendszerek felépítését, fő komponenseit és működési elveit, különös tekintettel a hálózati architektúrákra, az adatbiztonságra, és az üzemeltetés támogatásához kapcsolódó folyamatokra.

Részletesen ismertettem, hogyan működik a vállalati IT a Bosch hatvani gyárában, ahol az informatikai rendszerek szorosan integrálódnak a termelésirányításhoz. A dolgozat kitért a felhasználó- és eszközkezelés, a jogosultságpolitika, a vírusvédelem és a sérülékenységkezelés szervezeti vonatkozásaira is. A különböző feladatok és folyamatok bemutatásán keresztül láthatóvá vált, hogy egy modern gyár informatikai háttere mennyire komplex, és milyen szoros együttműködést igényel az IT és az üzemeltetési területek között.

A dolgozat gyakorlati részében bemutatott AGV WiFi-probléma példája volt annak, hogy az informatikai incidensek elemzése és megoldása miként épül fel egy strukturált, lépésről lépésre felépített folyamatban. A hiba azonosítása, a gyökérok feltárása, a Cisco TAC bevonása, majd a WGB firmware frissítése egyaránt azt mutatta, hogy a hibamegoldás nem kizárólag technikai kérdés, hanem kommunikációs, koordinációs és döntéstámogatási feladat is. Az eset megmutatta, mennyire fontos az adatok gyűjtése és elemzése, a hibaesemények dokumentálása, valamint az, hogy a csapatok közösen értékeljék ki a tapasztalatokat.

A dolgozatban bemutatott módszertanok - mint a probléma szakaszolása, az eszkalációs lánc felépítése, és a hibák visszamérése - mind hozzájárulnak ahhoz, hogy a jövőben hasonló esetek gyorsabban és hatékonyabban kezelhetők legyenek. Az elért eredmények nemcsak a konkrét hiba megszüntetésében mutatkoztak meg, hanem a szervezeti tanulásban is: a dokumentált tapasztalatok beépültek a helyi IT-folyamatokba, és hozzájárultak a hálózat stabilitásának növeléséhez.

Az informatika nem csupán támogató szerepet játszik egy gyártóvállalat életében, hanem stratégiai tényezővé vált. A megbízható, gyors és biztonságos informatikai rendszer ma már elengedhetetlen feltétele annak, hogy a termelés versenyképes és fenntartható legyen.

6.2 Következtetések és jövőbéli irányok

A dolgozatom során megfogalmazott tapasztalataim alapján elmondhatom, hogy a vállalati informatika fejlődése az ipar 4.0 és az automatizálás térnyerésével új szintre lépett. A jövő vállalataiban az IT rendszerek nem csupán az adatforgalom kiszolgálói lesznek, hanem a döntéshozatali folyamatok aktív résztvevői is. Az informatikai infrastruktúra így a vállalati stratégia meghatározó elemévé válik. Bár a technológia fejlődésével újabb és újabb kihívások elé kell nézünk, nekünk IT-soknak, fontos, hogy mindig naprakész információhoz jussunk és betartsuk a szigorításokat.

Hipotéziseimre, feltett kérdéseimre megpróbáltam olyan válaszokat kifejteni, amik akár a későbbi IT-világban is helytállóak lehetnek:

1. A digitalizáció és automatizáció ajtót nyithat a modern kibertéri sebezhetőségeknek?
   „*Minél többet tud egy rendszer, minél több IoT komponensből áll, annál több sebezhetőséget rejt, ezért fontos, hogy olyan IT-infrastrukúra környezetet alakítsunk ki, amely megfelel a Bosch központi direktíva, valamint a mai kibervédelmi előírásoknak”*

2. Az automatizált védelmi rendszerek megnehezíthetik a problémaelhárítást?
   „Hozzá kell szokunk, hogy a rendszerek egyre kevesebb felhasználói beavatkozást igényelnek. Bár ezek a folyamatok lassíthatják a probléma megoldását, megkönnyíthetik a munkánkat a folyamat automata dokumentációjával”

3. Fejlődő infrastruktúra mellett biztosítható az elavult gyártóberendezések támogatása?
   „Az elavult, mai napig produktívan gyártásban működő sebezhető rendszerek elszeparálásával, és hadrendinek biztosításával (például tűzfalkommunikáció szigorítás) biztosítható a régi (legacy) rendszerek üzemeltetése”

4. IT biztonsági tudatosságunk naprakészen megállja a helyét az Ipar 4.0 világában?
   „Nem tudunk minden nap naprakész It-biztosnági információkkal alátámasztani tudásunk, hiszen a folyamatosan megjelenő nulladik-napi sebezhetőségek, és támadók által feltárt kiskapuk a világ fejlődésével egyre több problémát fognak okozni az IT-szakembereknek, ezért szükséges a mesterséges intelligencai automata védelmi mechanizmusok beépítése környezetünkbe”

Ezen túlmenően a hálózati infrastruktúra fejlesztése és újra tervezése is kiemelt szerepet kap. A Zero Trust hálózati modell, a mikroszegmentáció és a biztonsági Fortinet tűzfal zónák bevezetése tovább növeli az üzemek ellenálló képességét mind a technikai hibák, mind a kiberfenyegetések ellen. (pcmegoldasok.hu, 2025)

Személyes tapasztalataim alapján a jövő informatikusa nem csupán technikai szakember, hanem rendszerszemléletű problémamegoldó. Az ipari informatika jövője abba az irányba halad, hogy az IT és az üzemeltetés közötti határ megszűnjen, és létrejöjjön egy közös, integrált digitális rendszer, ahol minden döntés adat vezérelt, és minden rendszer intelligens módon képes reagálni a környezeti változásokra, mint például egy sor átmozgatása, vagy gyártósori beüzemelés. A jövő kihívása az lesz, hogy az informatikai rendszerek ne csak támogassák a termelést, hanem aktívan hozzájáruljanak annak fejlődéséhez biztonságos, gyors és megbízható módon, csökkente ezzel az állásidő megnövekedését, és a selejtes termékek számát.

7. Irodalomjegyzék

Ászity Sándor, D. F. (2019). *Ipar 4.0.* Budapest: Akadémiai Kiadó.

Chrissy Kidd, S. W. (2024. október). *What Is Root Cause Analysis? The Complete RCA Guide*. Forrás: https://www.splunk.com/en_us/blog/learn/root-cause-analysis.html

Cisco. (2024. augusztus). *Understanding Cisco DNA and Catalyst Software eBook*. Forrás: https://www.cisco.com/c/en/us/products/collateral/software/dna-software-ebook-cte.html

Cisco. (2025. május). *Understand the Spanning Tree PortFast BPDU Guard Enhancement*. Forrás: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10586-65.html

Csanád, R. (2025. március). *ADATHALÁSZAT*. Forrás: https://www.jtkpartners.hu/blog/adathalaszat/71822/

Demeter Krisztina. (2016). *Termelés, szolgáltatás, logisztika.* Budapest: Wolters Kluwer Kft.

Dr. Váczi Dániel, O. Á. (2025. szeptember). *WHITEPAPER: NIS 2 MAGYARORSZÁGON Tapasztalatok és javaslatok az elmúlt másfél év gyakorlata alapján*. Forrás: https://www.nis2whitepaper.eu/hu/_files/ugd/3dac62_3efe3e64753d4d0faa561b6cd69cd880.pdf

Gergő Benedek. (2020. február). *Mi is az az IOT? És mi az AIOT? Minden, amit a dolgok internetéről tudni kell*. Forrás: https://lexunit.hu/blog/iot/

Hetényi Petra. (2023. február). *Még mindig hosszú út áll a biztonságos OT-rendszerek előtt*. Forrás: https://www.jovogyara.hu/meg-mindig-hosszu-ut-all-a-biztonsagos-ot-rendszerek-elott.html

Káplár Judit. (2023. október). *Az ERP Rendszerek vezető szerepe a vállalatok irányításában*. Forrás: https://prodosoft.hu/az-erp-rendszerek-vezeto-szerepe-a-vallalatok-iranyitasaban/

Kenfack, P. A. (2023). Strengthening the Security of Supervised Networks by Automating Hardening Mechanisms. In P. A. Kenfack, *Journal of Computer and Communications* (old.: 108-136). Scientific Research Publishing Inc.

Koncz Annamária. (2015. március). *A 8D PROBLÉMAMEGOLDÓ TECHNIKA*. Forrás: https://www.repulestudomany.hu/folyoirat/2015_3/2015-3-01-0227_Koncz_Annamaria.pdf

Kovács László. (2018). *Kiberbiztonság és Stratégia.* Budapest: Dialóg Campus Kiadó.

Lawrence Abrams. (2022. május). *New Phishing toolkit lets anyone create fake Chrome browser windows*. Forrás: https://www.bleepingcomputer.com/news/security/new-phishing-toolkit-lets-anyone-create-fake-chrome-browser-windows/

M. Mahanta, A. T. (2025). Optimizing Access Point Placement in Industrial IoT: A Deep Reinforcement Learning Approach With Q-Learning Verification and Signal Heatmap Visualization. In A. T. M. Mahanta, *IEEE Access, vol. 13* (old.: 121300-121325). IEEE.

Microsoft. (2025. október). *Magyarországon még felfutóban van a kiberbűnözés*. Forrás: https://news.microsoft.com/hu-hu/2025/10/30/nem-vagyunk-kiemelt-celpontjai-a-kibertamadasoknak-megsem-dolhetunk-hatra/

OPSWAT. (2025. február). *Mi az IT/OT konvergencia? Az előnyök, kihívások és jövőbeli innovációk feltárása*. Forrás: https://hungarian.opswat.com/blog/what-is-it-ot-convergence

pcmegoldasok.hu. (2025. november). *Zero Trust hálózati modell: Az új biztonsági paradigma*. Forrás: https://pcmegoldasok.hu/zero-trust-halozati-modell-az-uj-biztonsagi-paradigma/

Purdue Global. (2025. február). *Communication Skills for IT Professionals*. Forrás: https://www.purdueglobal.edu/blog/information-technology/communication-skills-for-it/

Ramaswamy Chandramouli, E. A. (2025. szeptember). *Guidelines for Media Sanitization*. Forrás: https://doi.org/10.6028/NIST.SP.800-88r2f

Szilágyi Gábor. (2025. október 19.). *„Leállt a gép. Megint" – avagy miért lenne jó, ha a rendszer tudna szólni előre?* Forrás: https://gyartastrend.hu/cikk/leallt-a-gep-megint-avagy-miert-lenne-jo-ha-a-rendszer-tudna-szolni-elore

Tamás, K. (2022. november). *Az IT és az OT viszonyrendszere, a konvergencia humán és adminisztratív aspektusai*. Forrás: https://alverad.hu/wp-content/uploads/2024/02/alverad-ot-human-aspektusok-1122-FIN.pdf

Tamás, M. (2021. május 4). *Mi folyik a hálózaton?* Forrás: https://99999.hu/mi-folyik-a-halozaton/

8. Ábrák és táblázatok jegyzéke

Ábrajegyzék

Táblázatjegyzék

NYILATKOZAT

szakdolgozat nyilvános hozzáféréséről és eredetiségéről

A hallgató neve:	Poncski Viktor
A Hallgató Neptun kódja:	E7U5T9
A dolgozat címe:	Vállalati informatikai problémák és kihívások a Bosch környezetében
A megjelenés éve:	2025
A konzulens intézetének neve:	Vidékfejlesztés és Fenntartható Gazdaság Intézet
A konzulens tanszékének a neve:	Agrárdigitalizációs és Szaktanácsadási Tanszék

Kijelentem, hogy az általam benyújtott szakdolgozat egyéni, eredeti jellegű, saját szellemi alkotásom. Azon részeket, melyeket más szerzők munkájából vettem át, egyértelműen megjelöltem, és az irodalomjegyzékben szerepeltettem. Továbbá kijelentem, hogy a dolgozat elkészítése során alkalmazott mesterséges intelligencia-eszközök (pl. szöveggenerálás, nyelvi javítás, fordítás, adatelemzés) használata nem helyettesítette a saját kutatási és alkotói munkámat, azok alkalmazását a források között vagy a módszertani részben feltüntettem, és a szakmai-etikai elvárásoknak megfelelően jártam el.

Ha a fenti nyilatkozattal valótlant állítottam, tudomásul veszem, hogy a záróvizsga-bizottság a záróvizsgából kizár és a záróvizsgát csak új dolgozat készítése után tehetek.

A leadott dolgozat, mely PDF dokumentum, szerkesztését nem, megtekintését és nyomtatását engedélyezem.

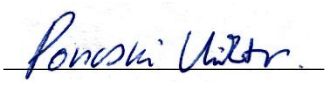
Tudomásul veszem, hogy az általam készített dolgozatra, mint szellemi alkotás felhasználására, hasznosítására a Magyar Agrár- és Élettudományi Egyetem mindenkori szellemitulajdon-kezelési szabályzatában megfogalmazottak érvényesek.

Tudomásul veszem, hogy dolgozatom elektronikus változata feltöltésre kerül a Magyar Agrár- és Élettudományi Egyetem könyvtári repozitori rendszerébe. Tudomásul veszem, hogy a megvédett és

- nem titkosított dolgozat a védést követően
- titkosításra engedélyezett dolgozat a benyújtásától számított 5 év eltelte után

nyilvánosan elérhető és kereshető lesz az Egyetem könyvári repozitori rendszerében.

Kelt: 2025.11.08



Hallgató aláírása

NYILATKOZAT

Poncski Viktor (hallgató Neptun azonosítója: E7U5T9) konzulenseként nyilatkozom arról, hogy a szakdolgozatot áttekintettem, a hallgatót az irodalmi források korrekt kezelésének követelményeiről, jogi és etikai szabályairól tájékoztattam.

A záródolgozatot/szakdolgozatot/diplomadolgozatot/portfóliót a záróvizsgán történő védésre **javaslom / nem javaslom**[1].

A dolgozat állam- vagy szolgálati titkot tartalmaz: igen nem*[2]

Kelt: 2025. 11. 08.

belső konzulens

[1] A megfelelő aláhúzandó.
[2] A megfelelő aláhúzandó.

Hallgatók, doktoranduszok nyilatkozata mesterséges intelligencia (MI) alkalmazásáról

1. Általános adatok

Hallgató neve:	**Poncski Viktor**
Neptun-kódja:	**E7U5T9**
Képzési szint (a megfelelőt jelölje X-szel):	☒ BSc/BA ☐ MSc/MA ☐ Doktori (PhD) ☐ Egyéb: .....
Tantárgy neve/kódja*:	**Szakdolgozati szeminárium 2.**
A munka címe:	**Vállalati informatikai problémák és kihívások a Bosch környezetében**

* doktori értekezés esetén nem kitöltendő

2. Nyilatkozat az MI használatáról

Alulírott, etikai felelősségem teljes tudatában az alábbi nyilatkozatot teszem:

(Kérjük, válasszon egyet az alábbi lehetőségek közül!)

☐ A) Nem alkalmaztam mesterséges intelligencia rendszert vagy szolgáltatást.

(Amennyiben ezt jelölte, a további táblázatok kitöltése nem szükséges.)

☒ B) Alkalmaztam mesterséges intelligencia rendszert vagy szolgáltatást.

(Kérjük, töltse ki a vonatkozó táblázatokat!)

3. A mesterséges intelligencia használatának részletezése

I. TÁBLÁZAT: Asszisztensi vagy kisebb mértékű felhasználás (pl. fordítás, nyelvi korrektúra, ötletelés stb.)

(Ezen felhasználások esetében a konkrét promptok és válaszok csatolása nem szükséges.)

A felhasználás célja	**Alkalmazott MI-eszköz neve és verziója**	**Érintett rész (ha nem a szöveg egészére vonatkozik)**
Angol nyelvű informatikai szavak magyarra fordítása	GPT-5	
Szakirodalmak felkutatása	Consensus 2.0	
Ötletelés	GPT-5	

II. TÁBLÁZAT: Jelentős tartalmi hozzájárulás (pl. egy teljes ábra vagy egy hosszabb szövegrész generálása)

*(Ezekben az esetekben a felhasznált kulcsfontosságú promptok és az MI által adott nyers válaszok dokumentálása és a munka **mellékletében való csatolása szükséges**.)*

A felhasználás célja	Alkalmazott MI-eszköz neve, verziója, elérhetősége	Az érintett fejezet / ábra / táblázat pontos sorszáma	A prompt-naplót tartalmazó melléklet bejegyzésének sorszáma

3/A. Oktató által előírt kiegészítő szabályok (ha vannak)

Amennyiben az adott tantárgy oktatója vagy témavezetője az MI-eszközök használatára vonatkozóan külön szabályokat vagy elvárásokat határozott meg, kérjük, az alábbi mezőben foglalja össze ezeket:

Pl. az MI használatának tilalma bizonyos feladattípusokra; csak konkrét eszköz használata engedélyezett; eltérő hivatkozási elvárások; dokumentációs forma stb.

Oktató vagy témavezető által előírt szabályok:

.....

.....

.....

.....

4. Minden hallgatóra vonatkozó nyilatkozat:

Kijelentem, hogy az MI által esetlegesen generált tartalmakat minden esetben kritikailag felülvizsgáltam, szerkesztettem és a munkába illesztettem. A leadott munka minden eleméért, annak eredetiségéért és tudományos helytállóságáért teljes körű felelősséget vállalok. Tudomásul veszem, hogy a Magyar Agrár- és Élettudományi Egyetem a benyújtott munkát mesterséges intelligencia detektorral ellenőrizheti, és eljárást kezdeményezhet, amennyiben a nyilatkozatom valótlan vagy hiányos.

Kelt: Gyöngyös., 2025.11.08.

Ponesu Viktor .....

Hallgató aláírása

.....

Konzulens/Témavezető aláírása