# SZAKDOLGOZAT

**Gubis Dávid**

**2025**

**Magyar Agrár- és Élettudományi Egyetem**

**Károly Róbert Campus**

**Vidékfejlesztés és Fenntartható Gazdaság Intézet**

**Gazdaságinformatikus alapképzési szak**

# Vállalati informatikai problémák elemzése és megoldási javaslatok megfogalmazása a Hatvani Bosch vállalat példáján keresztül

**Belső konzulens:** **Dr. Zörög Zoltán**
**egyetemi docens**

**Belső konzulens intézete/tanszéke:** **Vidékfejlesztés és Fenntartható Gazdaság Intézet**

**Készítette:** **Gubis Dávid**

**Károly Róbert Campus**

# 2025Tartalomjegyzék

# Bevezetés

A modern ipar színterén az információtechnológia már nem csak háttérszereplő, hanem a vállalatok működésének egyik alappillére. A gyártó- és szolgáltató cégek mindennapi folyamatai, a termelésirányítástól a logisztikán és adminisztráción át egészen a kutatás-fejlesztésig, szorosan összefonódnak az IT-rendszerek zökkenőmentes működésével. Egy több telephelyen tevékenykedő multinacionális nagyvállalat esetében az IT-infrastruktúra megbízhatósága már nem csupán belső hatékonysági kérdés, hanem kulcsfontosságú versenyképességi tényező is: már a legkisebb fennakadás is jelentős pénzügyi és reputációs kockázatot hordozhat.

Az IT-szolgáltatások menedzselése az elmúlt néhány évben már nem csupán háttérművelet, hanem a vállalati siker leglényegesebb mozgatórugója, különösen az automatizálás és a digitalizáció korában. Az informatikai szolgáltatásmenedzsment (ITSM) és az ITIL-keretrendszer kritikus szerepet tölt be abban, hogy a szervezetek gyorsan reagálni tudjanak a technológiai és üzleti környezet változásaira (Krishnan és Ravindran, 2017; Vicente és Gama, 2013).

Ezzel egy időben a vállalati informatikai környezet egyre összetettebbé szépül. A felhőszolgáltatások rohamos elterjedése, a folyamatosan bővülő és heterogénebb eszközpark, a hibrid munkavégzés mindennapossá válása, valamint az adatvédelem és a kiberbiztonság egyre szigorodó követelményei újabb, friss kihívásokat állítanak az IT-szervezetek elé. Az informatikai részlegeknek egyszerre kell megfelelniük a stratégiai szinten megfogalmazott digitalizációs céloknak, a folyamatos innovációra vonatkozó elvárásoknak, s a napi operatív működés zökkenőmentességének. Mindez tovább növeli a terhet a hálózati infrastruktúra üzemeltetése, az eszközpark kezelése és a felhasználói támogatási folyamatok felett.

Jelen szakdolgozat célkitűzése, hogy a fenti általános kihívásokat egy konkrét vállalati példán keresztül boncolgassa, és olyan gyakorlati megoldási ajánlatokat dolgozzon ki, melyek egyaránt fokozzák a mindennapi működés hatékonyságát és az informatikai szolgáltatások minőségét. A kutatás szíve a *Hatvani Robert Bosch Elektronika Kft.* (röviden Hatvani Bosch), amely a Bosch nemzetközi vállalatcsoport egyik legkiemelkedőbb kelet-közép-európai gyártó- és fejlesztési bázisa. A telephely kulcsszereplőként jelenik meg az autóipari elektronikai komponensek gyártásában és fejlesztésében, miközben több ezer munkavállaló számára korszerű munkakörnyezetet teremt.

A Hatvani Bosch informatikai működésének szívét a *Bosch Digital* részleg adja, amely a vállalat telephelyi IT-szolgáltatásainak minden aspektusáért felel. Ide tartozik a hálózati infrastruktúra gondozása, a munkaállomások és mobileszközök teljes életciklusának kezelése, az IT Space felhasználói támogatási központ üzemeltetése, valamint számos kisebb, ám a mindennapi működés szempontjából létfontosságú kiegészítő szolgáltatás. A telephely mérete, a gyártási folyamatok 24/7-es ütemezése és a globális Bosch hálózathoz való szoros integráció mind olyan tényezők, amelyek különösen érzékennyé teszik a rendszer esetleges hiányosságait.

A dolgozat három meghatározó területre helyezi a hangsúlyt:

- **Hálózati infrastruktúra:** a belső adatforgalom, a kommunikációs csatornák és a gyártási berendezések informatikai összekapcsolása kulcsfontosságú. A tipikus hibaforrások (sávszélesség-problémák, hálózati leállások, illetve kábelezési hiányosságok) feltérképezése után a cél a folyamatok alapos dokumentálása és proaktív, előrelátó hibamegelőző javaslatok kidolgozása.

- **IT-eszközpark (fleet management):** A vállalat laptopjainak, asztali gépeinek, Tiny PC-inek és mobiltelefonjainak nyilvántartási pontossága, a kiadás-visszavétel nyomon követhetősége, valamint az eszközök időben esedékes cseréje egyaránt jelentős kihívást jelentenek. A dolgozat ezen a területen az automatizálás és a digitalizáció által nyújtott lehetőségeket is alaposan elemzi.
- **IT Space (felhasználói támogatás):** a helyszíni ügyfélszolgálat működését, a készletek kezelését és az időmenedzsmentet egyaránt a felhasználói elégedettség befolyásolja. A felmerülő szervezési és kapacitásbeli nehézségek alapos felmérése után olyan ajánlásokat dolgozunk ki, amelyek célja a szolgáltatás színvonalának emelése és a válaszidő lerövidítése.

A kutatás alapját egy kvalitatív megközelítés adja: a Bosch Digital részleg dolgozóival folytatott interjúk, a belső folyamatleírások és a személyes megfigyelések együtt biztosítják az empirikus hátteret. Ez a módszer lehetővé teszi, hogy ne csak a látható tünetekre koncentráljunk, hanem feltárjuk a problémák mögött rejlő szervezeti és technológiai okokat is. A vizsgálat nem csupán a jelenlegi hiányosságok felmérésére irányul, hanem arra is, hogy olyan fejlesztési irányokat azonosítsunk, amelyek zökkenőmentesen beépíthetők a vállalat mindennapi gyakorlatába, és hosszú távon növelik az informatikai szolgáltatások megbízhatóságát és költséghatékonyságát.

A dolgozat felépítése ennek megfelelően alakul. A bevezetést követő szakirodalmi áttekintés a vállalati informatikai rendszerek üzemeltetéséről szóló nemzetközi irodalmat, a hálózati infrastruktúra és az eszközpark-kezelés legfontosabb kihívásait, valamint az IT-támogatási szolgáltatások bevált gyakorlatait veszi górcső alá. Ezt követik az esettanulmány-fejezetek, amelyek részletesen bemutatják a Hatvani Bosch telephely informatikai problémáit három fő területen. A dolgozat zárófejezete összefoglalja az eredményeket, és konkrét megoldási javaslatokkal él a feltárt problémák orvoslására.

# 1. Szakirodalmi áttekintés

A szakirodalmi áttekintés feladata, hogy szilárd alapot biztosítson a dolgozat gyakorlati részéhez: részletesen bemutatom az informatikai infrastruktúra elméleti fogalmait, legfontosabb komponenseit, valamint a hálózati rendszerek tervezésének alapelveit. Ezt követően rátérek az IT-szolgáltatás-kezelés (ITSM) és az infrastruktúra-menedzsment kulcsfontosságú keretrendszereire, külön hangsúlyt fektetve az ITIL koncepciójára. Ezek az elméleti keretek lehetővé teszik, hogy a Hatvani Bosch hálózati rendszerével kapcsolatos tapasztalatokat megfelelően értelmezzük és a megfelelő kontextusba helyezzük.

## 1.1. Informatikai infrastruktúra fogalmi keret

Az informatikai infrastruktúra (IT infrastructure) a hardver- és szoftveres elemek szövevényes hálózata, amely az adatok, rendszerek és felhasználók közti kommunikációt és működést biztosítja a szervezeten belül. Ebbe a rendszerbe beletartoznak a fizikai eszközök (routerek, switchek, kábelek, szerverek, tűzfalak), a logikai rétegek (virtuális hálózatok, VLAN-ok, routing protokollok), valamint a különféle szoftveres alkalmazások és szolgáltatások. Így tehát a hálózati infrastruktúra nem csupán egy sor fizikai kötés, hanem egy szervesen összefonódó egység, ahol az egyes komponensek összehangoltan működnek.

## 1.2. Hálózati infrastruktúra tervezési elvek és kihívások

A gondosan megtervezett hálózati infrastruktúra nem csupán működőképes, hanem könnyen skálázható, megbízhatóan biztonságos, redundánsan felépített és egyszerűen menedzselhető is. Ennek megvalósításához alapvető elveket kell követni: a hálózat szegmentálása és zónái közötti elkülönítés, a redundancia beépítése, a terhelés elosztására szolgáló megoldások alkalmazása, a hierarchikus topológia használata, több rétegű biztonsági védelmek integrálása, a központi felügyelet és automatizálás kiépítése, valamint a folyamatos megfigyelés és monitorozás. A tervezési folyamatban azonban számos nehézség adódik, például a költségnyomás, a heterogén eszközpark kezelése, az örökölt rendszerek integrációjának kihívásai, illetve a biztonsági kockázatok hatékony kezelése.

## 1.3. Infrastruktúra-menedzsment és IT-szolgáltatás-kezelés (ITSM / ITIL)

A modern vállalatok egyre inkább az IT-infrastruktúra stabilitására és alkalmazkodóképességére támaszkodnak. Az IT-szolgáltatások menedzselése az elmúlt években az üzleti siker egyik leglényegesebb tényezőjévé vált, különösen az automatizálás és a digitalizáció korában. Az informatikai szolgáltatásmenedzsment (ITSM) és az ITIL keretrendszer kulcsfontosságú szerepet játszanak abban, hogy a cégek gyorsan reagálni tudjanak a technológiai és üzleti környezet változásaira (Krishnan és Ravindran, 2017; Vicente és Gama, 2013).

Az informatikai szolgáltatásmenedzsment (ITSM) fő feladata, hogy a számítástechnikai folyamatokat egységes keretbe szervezze, majd azokat a lehető legoptimálisabb módon finomhangolja. Ebben a célban az ITIL-keretrendszer egy olyan struktúrát biztosít, amely megkönnyíti a szolgáltatások átlátható és hatékony irányítását (Bichler és Bhattacharya, 2011). Számos kutatás (például Shastri és Thampi, 2021; Krishnan és Ravindran, 2017) rámutat arra, hogy az ITIL bevezetése, különösen az automatizált folyamatokkal kombinálva, drámai módon növeli a vállalati hatékonyságot, miközben lényegesen csökkenti az üzemeltetési költségeket. Az Ipar 4.0 technológiák bevezetésével a hálózati infrastruktúra és az IT-biztonság is új kihívásokkal szembesül, ahol az automatizált konfigurációkezelés és a kiber-fizikai rendszerek szoros integrációja kulcsfontosságú szerepet kap (Panetto és munkatársai, 2019; Zhao és Rao, 2017).

## 1.4. Hálózatelméleti modellek és komplex rendszerek

Az infrastruktúra működésének alaposabb megértését a hálózatelmélet különféle eszközei teszik lehetővé. A perkolációs elmélet, a többrétegű hálózatok és a robusztussági modellek révén feltérképezhető a rendszer sebezhetősége és a kritikus csomópontok. Ezek az elméletek szilárd alapot nyújtanak a Hatvani Bosch hálózatának vizsgálatához, különösen a reziliencia és az automatizáció szempontjából.

## 1.5. Összefüggések és alkalmazás a dolgozat témájához

Az előző alfejezetek együttesen teremtik meg azt az elméleti alapot, amelyre a dolgozat gyakorlati része épül. Az infrastruktúra fogalmi és menedzsment-kereteinek mélyreható megismerése lehetővé teszi a Hatvani Bosch hálózatának rendszerszintű feltérképezését, feltárva ezzel a legfontosabb kihívásokat és a potenciális fejlesztési irányokat. A következő fejezetben a vállalat hálózati infrastruktúrájának konkrét felépítését, működését és felmerülő problémáit részletesen ismertetem.

# 2. Hálózati infrastruktúrában felmerülő problémák és megoldásaik

Az Hatvani Robert Bosch Elektronika Kft. informatikai hálózata a vállalat teljes működésének egyik legkritikusabb alappillére. Itt kapcsolódik össze az ipari termelés, a logisztikai folyamatok, a minőségellenőrzés, sőt az irodai rendszerek is, így mindegyik egymással adatcserén keresztül kommunikál. Egy gyártóüzem esetében a stabil és gyors hálózati kapcsolat már nem csupán kényelmi szempont, hanem az üzemfolytonosság alapvető feltétele: ha a hálózat akár néhány percre leáll, az azonnali termelésmegállást, anyagi károkat és adatvesztést is eredményezhet.

A vállalati hálózati infrastruktúra egyik legkritikusabb eleme a TCP/IP alapú kommunikáció. Bár a TCP/IP protokoll rendkívül robusztus és széles körben elterjedt, kutatások rámutatnak arra, hogy számos biztonsági rést rejt magában, például IP-spoofingot, DNS-hamisítást és szolgáltatásmegtagadásos (DoS) támadásokat. Ennek ellensúlyozásához elengedhetetlen a tűzfalak, a titkosítási technológiák és a behatolásészlelő rendszerek szakszerű beállítása (Gangane és Kakade, 2015). Az Ethernet/IP-alapú rendszerek lehetővé teszik a gyártási és vállalati hálózatok zökkenőmentes összekapcsolását, ugyanakkor ez a kapcsolódás növeli a támadási felületet is. Ezen környezetek biztonságát speciális IDS-szabályokkal és kifinomult forgalomszűrési technikákkal lehet erősíteni (Laughter és Williams, 2006). Az IPv6 és a VLAN technológiák további biztonsági lehetőségeket kínálnak: az ACL, az RA-Guard és a SEND protokollok alkalmazásával a hálózati hozzáférések szigorúbb kontrollja valósítható meg (Shabalin és Kaliberda, 2017). A DNS protokoll esetében a több szintű védelmet nyújtó MLS DNS-architektúrák segítik a biztonságos névfeloldás megvalósítását és a hálózati támadások minimalizálását (Clark és munkatársai, 2009).

A Hatvani Bosch gyárban működő hálózat mérete és komplexitása a számszerű adatokban is szavakkal nehezen kifejezhető: több mint *944* aktív hálózati eszköz, közel *15 900* port, s egyben *100* rack szekrény alkotja a technikai infrastruktúrát. A kábelezés teljes hossza meghaladja az ezer kilométert, és a rendszer egyszerre több mint *135* logikai alhálózatot (VLAN-t) képes kezelni.Az elérhető adatok alapján egyértelműen látszik, hogy a gyár informatikai rendszere már nem egy egyszerű lokális hálózat (LAN), hanem egy vállalati szintű, redundanciával felszerelt, kiemelkedő rendelkezésre állással bíró hálózati architektúra, amely megfelel a globális Bosch-szabványok előírásainak.

Kiss Dániel, a Bosch Digital hatvani csapatának hálózati technikusa, alapos bepillantást engedett a hálózat struktúrájába és működésébe. Az interjúban kifejtve a napi üzemeltetés gyakorlati dimenzióit, a hibakezelés mechanizmusait, valamint a fejlesztések várható hatásait.

„A hálózat stabilitása a gyártásban mindent visz. Egyetlen hibás port vagy egy rosszul konfigurált switch már elegendő ahhoz, hogy egy teljes gépsor leálljon. Éppen ezért a mi feladatunk az, hogy minden pillanatban biztosítsuk az adatkapcsolat megszakítás nélküli fennmaradását.”

*(Saját interjú - Kiss Dániel, hálózati technikus, Bosch Digital Hatvan, 2025)*

## 2.1. A hálózat szerepe és jelentősége a gyártási folyamatban

A Hatvani Bosch gyár fő profilja az autóipari elektronikai alkatrészek fejlesztése és gyártása, amely nagymértékben támaszkodik az automatizált termelésre. A gyártóberendezések (PLC-k, robotkarok, kamerák, szenzorok) folyamatos adatcseréje teszi lehetővé a precíz,

hibátlan működést. Mindez csak akkor valósulhat meg, ha a hálózati infrastruktúra alacsony késleltetéssel (low latency) és magas sávszélességgel (high bandwidth) működik.

A hálózaton keresztül zajló kommunikáció messze nem homogén: a termelési adatgyűjtő rendszerek, az adminisztrációs alkalmazások, a biztonsági megoldások és a szerverkapcsolatok mind eltérő hálózati igényeket támasztanak. Ennek fényében a Bosch egy háromrétegből álló, többrétegű (multi-layered) architektúrát választott, amely a *core, a distribution és az access rétegeket* foglalja magába, és így képes a változatos követelményeknek megfelelni.

Egy háromszintes architektúra nemcsak a teljesítmény növelésében, hanem a biztonság és a hibaizoláció javításában is kulcsfontosságú szerepet tölt be.

Kiss Dániel így fogalmazott:

„Amint egy disztribúciós switch hibásodik, a forgalom magától a redundáns vonalra átirányul. Ez a gyakorlatban azt jelenti, hogy a gyártásban észre sem veszik, hogy bármilyen hiba történt."

Bosch hálózata úgy lett megtervezve, hogy éjjel-nappal, 24/7 üzemidőt biztosítson. Ennek érdekében a legkritikusabb hálózati elemek (a core switchek, tűzfalak és routerek) redundáns, azaz high-availability módon működnek. Így, ha egy eszköz meghibásodik, a tartalék azonnal átveszi a feladatot, a szolgáltatás pedig megszakítás nélkül folytatódik.

## 2.2. Fizikai hálózati felépítés

A Hatvani Bosch hálózat fizikai infrastruktúrája több mint húsz év során lassan, de határozottan átalakult: a korábban egyszerű, lapos struktúrából egy átgondolt, hierarchikusan felépített rendszer lett.

### 2.2.1. Core layer (gerinchálózat)

A hálózat szívét a *core layer* alkotja, amely a különböző épületek és csarnokok közötti adatforgalmat biztosítja. Ebben a szintben *Cisco Catalyst 9500-32QC* típusú switchek működnek, *40 Gbps*-es és *100 Gbps*-es optikai portokkal felszerelve. A berendezéseket két redundáns rackben helyezik el a központi adatközpontban, és etherchannel kapcsolaton keresztül kommunikálnak a disztribúciós rétegekkel.

A core réteg a hálózat „autópályájaként" szolgál: innen indul minden adatforgalom, és ide gyűlik össze minden csomag. A villámgyors sebesség és a redundancia mellett a biztonság is kiemelten fontos. Ennek biztosítása érdekében a Bosch duál tűzfal megoldást (HA firewall pair) használja, amely hiba esetén automatikusan átveszi a forgalmat.

### 2.2.2. Distribution layer (elosztó réteg)

A distribution réteg fő feladata, hogy a forgalmat a különféle hálózati szegmensek között szétosztja. Hatvanban, a Bosch telephelyén ez jellemzően *Cisco 9500-as és 9300-as* eszközök stackelt konfigurációjával valósul meg, amely lehetővé teszi, hogy több switch logikailag egyetlen egységként viselkedjen. Ennek következtében az adminisztráció egyszerűbbé válik, és a rendszer redundanciája is növekszik.

A disztribúciós réteg kulcsfontosságú szerepet játszik a biztonsági zónák elkülönítésében. Itt alkalmazzák a VLAN-szegmentálást (Virtual Local Area Network segmentation): az irodai, gyártási, szerver- és biztonságtechnikai hálózatok mind fizikai, mind logikai szinten szigorúan elkülönülve működnek.

### 2.2.3. Access layer (hozzáférési réteg)

Az access réteg felelőssége, hogy a különféle eszközök és végpontok (legyenek azok munkaállomások, PLC-k, kamerák vagy nyomtatók) zökkenőmentesen csatlakozhassanak. Hatvani Bosch telephelyén a hálózati infrastruktúrát főként Cisco Catalyst 9200CX és az Industrial Ethernet (IE) 3400/4000 szériájú switchek biztosítják. Ezeket az ipari switcheket úgy tervezték, hogy a gyártósori környezethez tökéletesen illeszkedjenek: por- és hőálló burkolat, redundáns tápellátás, valamint beépített automatikus visszaállítási (auto-recovery) funkció.

Az access rétegen helyezkednek el az RJ45 rézkábelek és az optikai uplinkek, illetve innen indul a Wi-Fi 6-os hálózat a Cisco 9800-as Wireless Controller (WLC) segítségével. Dániel elmondása szerint:

„A gyártási zónákban az access switchek a legterheltebbek, hiszen minden PLC és kamera innen kommunikál. Ha egy ilyen switch hibázik, az egész gépsor megállhat.”

## 2.3. Logikai felépítés és hálózati szegmentálás

A Bosch hálózata logikailag szigorú, szegmensenként elkülönített felépítéssel rendelkezik, ami garantálja, hogy a forgalom mindig kontrollált és biztonságos maradjon. A VLAN-szegmentálás ebben a környezetben a legfontosabb védelmi és szervezési eszköz: minden funkcionális terület saját VLAN-ba kerül, így a forgalom csak szabályozott, előre meghatározott módon áramolhat a különböző zónák között. Az 1. táblázat a logikai zónákat mutatja be.

1. **táblázat:** Az elsődleges logikai zónák:
(Forrás: saját szerkesztés)

| **Zóna neve** | **Funkció** | **Biztonsági szint** | **Jellemző eszközök** |
|---|---|---|---|
| **Office Network** | Adminisztrációs és irodai eszközök | Közepes | Laptopok, nyomtatók |
| **Production Network** | Gyártásvezérlő rendszerek | Nagyon magas | PLC, ipari PC-k, robotvezérlők |
| **Server Network** | Kiszolgálók és adatmentés | Magas | VMware szerverek, storage |
| **Wireless Network** | Mobil és laptop eszközök | Közepes | Access pointok |
| **CCTV Network** | Biztonsági kamerák és rögzítők | Magas | IP kamerák, NVR-ek |

A VLAN-határok között áramló forgalmat tűzfalak irányítják. Ezek a védelmi rendszerek nem csupán egyszerű engedélyezési listákkal operálnak, hanem Deep Packet Inspection (DPI) és Intrusion Prevention System (IPS) képességekkel is fel vannak szerelve. Ennek köszönhetően a hálózat már a célrendszerhez való eljutás előtt képes azonosítani és leállítani a gyanús adatcsomagokat.

Kiss Dániel úgy véli, hogy a logikai elválasztás a gyakorlati életben is számtalan problémát tud elhárítani:

„Korábban, amikor még kevesebb VLAN volt, előfordult, hogy egy gép véletlenül más zónába került. Ezért most minden új eszköz már előre regisztrált IP-címet és zónát kap, így kizárt, hogy rossz helyre kapcsolódjon.”

## 2.4. A hálózat kiterjedtsége és fizikai elhelyezkedése

A Hatvani Bosch üzem hálózata nem egy központi csomópont köré épül, hanem elosztott topológiát alkalmaz; minden csarnok és a nagyobb épületrész saját disztribúciós és access réteggel rendelkezik, amely optikai uplinkeken keresztül csatlakozik a központi core szinthez. Ennek a kialakításnak köszönhetően a forgalmi torlódások előfordulásának valószínűsége jelentősen csökken, miközben az egyes zónák önálló működésüket is megtartják.

A LAN Physics 2023 dokumentációja szerint a hálózati berendezések száma épületenként eltérő, de átlagosan egy csarnokban 10-15 rack szekrény található, amelyekben egyenként 2-4 switch helyezkedik el.

A gyártási területeken a kábezelés átgondoltan felépített: a gerincet CAT6 UTP és multimódusú optikai szálak képezik, míg a redundáns vonalakat elkülönített kábelcsatornákban vezetik.A redundancia megvalósulása és a jelölési rendszer egyaránt hozzájárul a hibakezelés gördülékenységéhez, minden egyes kábel és port egy egyedülálló azonosítót visel, amelyet a LAN Physics adatbázis tárol.

## 2.5. A hálózatot működtető technológiák és protokollok

A Hatvani Bosch informatikai hálózatát több, egymással szorosan összehangolt protokoll és technológiai megoldás alkotja, amelyek közös célja a kimagasló rendelkezésre állás, a biztonság és a forgalom hatékony optimalizálása. Ipari környezetben ezek a megoldások különösen lényegesek, mivel már egy apró konfigurációs hiba vagy hardver meghibásodása is súlyos termelésleállást eredményezhet.

### 2.5.1. Dinamikus útválasztás (OSPF - Open Shortest Path First)

Az OSPF egy dinamikus routing protokoll, amely automatikusan meghatározza a hálózati útvonalakat, és hiba esetén alternatív irányba tereli a forgalmat. A Bosch hálózatában az OSPF biztosítja, hogy a különböző disztribúciós switchek közötti adatforgalom mindig a legoptimálisabb úton haladjon.

A protokoll egy belső topológiai térképet kezel, amelyet állandóan frissít, így a hálózat mindig képes a változásokhoz alkalmazkodni.

Kiss Dániel a következőképpen magyarázta:

„Régebben, amikor még statikus route-okkal dolgoztunk, egy hiba után kézzel kellett átírni a konfigurációkat. Most az OSPF automatikusan átszámolja az útvonalakat, így a forgalom átirányítása gyakorlatilag észrevétlen.”

*(Saját interjú - Kiss Dániel, a Bosch Digital Hatvan hálózati technikusa, 2025)*

### 2.5.2. Redundancia és aggregáció (LACP - Link Aggregation Control Protocol)

Az üzem optikai uplinkjei gyakran párban, LACP aggregációval működnek. Ennek következtében több fizikai kábel egy logikai linkként egyesül, és ha az egyik szál megszakad, a másik azonnal átveszi a forgalmat.Ezzel egy időben a sávszélesség is növekszik, mivel a több link egymásra épülve összeadódik.

„Az LACP-nek köszönhetően nem kell tartalék portokat kézzel konfigurálni. Ha az egyik kábel megszakad, a másik azonnal átveszi a szerepét, mindezt a felhasználók észre sem veszik.” - tette hozzá Dániel.

### 2.5.3. Hurokmentesítés (STP/RSTP)

Az STP, vagyis a *Spanning Tree Protocol*, arra hivatott, hogy megakadályozza a hálózati hurkok (network loops) megjelenését. Ezek a ciklusok könnyen túlterhelhetik, vagy akár bénuláshoz is szoríthatják a hálózatot. A Hatvani Bosch telephelyén már az RSTP (Rapid Spanning Tree Protocol) gyors változata működik, amely lényegesen felgyorsítja a konvergenciát, így hiba esetén pár másodperc alatt új, stabil útvonalat teremt.

Dániel rámutatott, hogy ipari környezetben az STP hibák különösen komoly veszélyt jelentenek:

„Volt rá példa, hogy egy ipari switch rosszul viselkedett, és hurok keletkezett. Az egész csarnok hálózata belassult. Most már az RSTP és a broadcast storm control megakadályozza, hogy ez újra megtörténjen.”

### 2.5.4. Portbiztonság és végpont-ellenőrzés (Port Security, 802.1X)

A Hatvani Bosch hálózat védelmének sarokköve a port security és az 802.1X-alapú hitelesítés, amelyek révén kizárólag engedélyezett eszközök léphetnek be a hálózatba.A rendszer állandóan ellenőrzi a portokra csatlakozó eszközök MAC-címeit; amikor egy eddig nem látott, ismeretlen készülékre bukkant, automatikusan lekapcsolja a portot, vagy értesíti az üzemeltetést.

„Ha valaki ismeretlen laptopot dug be egy gyártósori portra, a rendszer azonnal észreveszi, és lezárja a kapcsolatot. Ezzel rengeteg biztonsági incidens előzhető meg.” - mondta Dániel.

## 2.6. A „Secure BCN” projekt: a hálózati modernizáció új korszaka

A Bosch-csoport már a 2020-as évek elején ráébredt, hogy a kézzel irányított, hagyományos hálózati rendszerek már nem képesek lépést tartani a digitális ipar (az Industry 4.0) által támasztott követelményekkel. Ennek a felismerésnek a hatására indult el a Secure BCN (Bosch Corporate Network) projekt, amelynek célja egy teljesen automatizált, központilag menedzselt hálózati architektúra kiépítése.

A Hatvani Bosch az egyik első pilot telephely. A projekt fő komponense a Cisco DNA Center. Ez a rendszer egy grafikus felületen keresztül teszi lehetővé a hálózat központi felügyeletét, konfigurálását és hibakezelését, mindezt emberi beavatkozás nélkül.

Kiss Dániel a változás lényegét a következő szavakkal fogta össze:

„Régebben minden konfigurációt PuTTY-ban, konzolon kellett megcsinálni. Most a DNA Center felületén látjuk az egész hálózatot, és akár egy gombnyomással lehet firmware-t frissíteni vagy portot beállítani. Ez hatalmas előrelépés.”

### 2.6.1. Automatizálás és intelligens portkezelés

A Secure BCN legnagyobb innovációja az, hogy a portok konfigurálása teljesen automatizált. Amikor egy eszközt (például laptopot, PLC-t vagy IP-kamerát) csatlakoztatnak a hálózathoz, a rendszer azonnal felismeri a típusát és a jogosultsági szintjét, majd automatikusan hozzárendeli a megfelelő VLAN-t és a kapcsolódó hozzáférési szabályokat.

„Most már mindegy, melyik portba dugjuk az eszközt. A DNA Center felismeri a MAC-címet, és tudja, hova tartozik. Nincs többé manuális VLAN-beállítás.”

*(Saját interjú - Kiss Dániel, Bosch Digital Hatvan, 2025)*

Az alkalmazott megoldás erőteljesen mérsékli az emberi hibák gyakoriságát, mivel a múltban egy rosszul beállított VLAN vagy IP-cím akár a teljes hálózat leállását is okozhatta. Emellett

az automatizálás időmegtakarítást biztosít, és egységes, szabványos konfigurációt garantál a teljes hálózati környezetben.

### 2.6.2. A „greenfield” és „brownfield” megközelítés

A Hatvani Bosch jelenleg a *greenfield* fázisban tevékenykedik, ami azt jelenti, hogy az új infrastruktúra teljesen elkülönül a meglévő hálózattól, párhuzamosan épül. Az új rackekben már a Secure BCN által felügyelt eszközök sorakoznak, melyek fokozatosan integrálódnak a gyári hálózatba.

„Most greenfield módon, rackenként építjük be az új switcheket. Először külön teszteljük őket, hogy minden funkció működjön, aztán majd jön a brownfield, amikor a meglévő switcheket is migráljuk.” - mondta Dániel.

A későbbi *brownfield migration* szakaszban a régi, működő hálózati elemek is átkerülnek a DNA Center felügyelete alá, ez azonban jóval bonyolultabb folyamat, mivel az élő termelés közben kell végrehajtani.

## 2.7. Az adatgyűjtés és láthatóság szerepe (Basic Visibility projekt)

Mielőtt a Secure BCN bevezetésére sor került volna, a három évig tartó Basic Visibility program már adatokat gyűjtött a hálózat működéséről:

- melyik eszköz melyik switchporthoz kapcsolódott,
- milyen gyakorisággal,
- milyen VLAN-ban működött,
- és milyen IP-címet használt.

Az adatok révén egy hatalmas hálózati adatbázist hoztunk létre, amely ma már a DNA Center automatizmusainak alapját képezi.

„Három éve folyamatosan gyűjtjük a switchek forgalmi adatait. Ez nemcsak hibakeresésnél segít, hanem a jövőbeli automatizált portbeállításokhoz is alapot ad.” - magyarázta Kiss Dániel.

A Bosch Digital központi hálózati osztálya, amelybe a Hatvani telephely is beletartozik, alaposan feldolgozza a begyűjtött adatokat, és az AI technológiára épülő, testre szabott javaslatokat készít a jövőbeni hálózati konfigurációk tervezéséhez.

Ennek hatására a rendszer már előzetesen jelezni képes, ha egy adott eszköz hibásan működik, vagy ha egy port szokatlan forgalmat generál.

## 2.8. Kiberbiztonsági fejlesztések és tűzfalarchitektúra

A Hatvani Bosch hálózati fejlesztései között a kiberbiztonság egy további kiemelt területként jelenik meg. Mivel az ipari hálózatok egyre gyakrabban kerülnek a zsarolóvírusok és a célzott kibertámadások célpontjába, a Bosch az elmúlt néhány évben az ACL (Access Control List) szabályozás helyett a tűzfal-központú védelmet részesítette előnyben.

A jelenlegi rendszer felépítése több egymásra épülő biztonsági réteget vonultat fel:

- **Perimeter firewall**: gondoskodik arról, hogy a telephely külső hálózati kapcsolatai védve legyenek a kívülről érkező támadásokkal szemben.
- **Internal Firewall**: gondoskodik arról, hogy az irodai és a gyártási zónák közti forgalom szigorú szabályok szerint zajljon.

- **IDS/IPS (Intrusion Detection/Prevention System**): a forgalmat mélyrehatóan átvizsgálja, s önállóan szűri ki, blokkolja a gyanús mintákat.
- **Logolás és SIEM**: minden hálózati eseményt gondosan rögzít, így a későbbi elemzések során bőven nyomot találunk.

Dániel szerint ez a váltás az egyik legfontosabb lépés volt:

„Régen ACL-listákat kellett kézzel szerkeszteni, és ha valami kimaradt, az gondot okozott. Most a tűzfal szabályai központilag vannak kezelve, és a rendszer sokkal gyorsabban reagál."

Bosch Digital kiberbiztonsági stratégiája a „Zero Trust" elv mentén épül: minden hálózati kapcsolatot addig tekintünk potenciálisan gyanúsnak, amíg nem tudja bizonyítani, hogy ellenkezőleg megbízható. Ez a megközelítés különösen lényeges a gyártósori berendezéseknél, ahol a fizikai hozzáférés is szigorú korlátozások alá esik.

## 2.9. Üzemeltetés és hibakezelés a gyakorlatban

A hálózati infrastruktúra gördülékeny működését nem csak a technológia, hanem az üzemeltetési folyamatok és a mögöttes szervezeti struktúra is meghatározza. Hatvani Boschnál a mindennapi hálózati feladatok ellátásáért a Bosch Digital (BD) helyi IT-csapata felel, míg a hálózat stratégiai irányítását és fejlesztését a Bosch globális, dedikált hálózati osztálya koordinálja.

A helyi informatikai csapat az úgynevezett elsőszintű (first-line) támogatás szerepét tölti be, azaz a hibák elsődleges felismerését és helyszíni megoldását végzi. Amennyiben a felmerülő gond hálózati vagy konfigurációs eredetű, a feladat a második szintű (second-line) támogatásra átkerül, amelyet a hálózati osztály lát el; itt egy több, tapasztalt mérnökből álló csapat biztosítja a megfelelő beavatkozást.

Kiss Dániel e módon írta le:

„Mi vagyunk az első szint, akik a terepen dolgoznak. Ha valami nem működik, először mi vizsgáljuk meg. Ha kiderül, hogy a hiba mélyebben van, például VLAN-szinten vagy a core switchen, akkor bevonjuk a hálózati osztályt."

*(Saját interjú - Kiss Dániel, hálózati technikus, Bosch Digital Hatvan, 2025)*

A hibabejelentések és azok nyomon követése a Bosch belső IT Service Desk és az FCM Helpdesk platformjain keresztül valósul meg. Itt a felhasználók jelezhetik, ha hálózati gondokba ütköznek, legyen szó lassú kapcsolatról, a szerverhez való hozzáférés hiányáról vagy a Wi-Fi szakadásáról. A rendszer automatikusan rögzíti a bejelentéseket, majd hatásuk mértéke szerint priorizálja őket.

### 2.9.1. A leggyakoribb hibák és okai

A hálózati hibák lényegét tekintve két meghatározó csoport különíthető el: hardveres hibák és **szoftveres / konfigurációs hibák**.

**A hardverrel összefüggő hibák:**

- **RJ45 csatlakozók sérülése vagy oxidációja:** gyakran felmerülő probléma a gyártósori környezetben, ahol a kábelek állandó fizikai igénybevétellel szembesülnek.
- **Kábelhibák:** megtört vagy túlságosan hosszú kábelek, helytelen krimpelés, jelvesztés.
- **Switch vagy port meghibásodása:** leggyakrabban az access rétegben jelenik meg, mivel ott a legmagasabb a terhelés.

- **Hőmérsékleti problémák**: ipari környezetben egyes rackek túlmelegedhetnek, ha a hűtés nem megfelelő.

**Szoftver- és konfigurációs hibák:**

- **VLAN-kiosztási tévedés**, ha egy berendezés egy nem számára rendelt VLAN-ba kerül, már nem képes hozzájutni a létfontosságú erőforrásokhoz.
- **IP-címütközés**, a manuális beállításokból eredő.
- **Loop és broadcast storm**: egy olyan hálózati zavar, amely rendszerint a nem megfelelően beállított switch vagy ipari eszköz hibájából ered.
- **Port security események**: amikor egy engedély nélküli eszköz próbál kapcsolódni, a rendszer letiltja az érintett portokat.

Kiss Dániel szerint a hibák több mint felét még mindig emberi tényezők okozzák:

„A legtöbb problémát az okozza, ha valaki rossz helyre dug be egy kábelt, vagy egy gépet átrak másik portra, de nem szól. Ilyenkor a port security azonnal letiltja a kapcsolatot, és nekünk kell újra engedélyezni.”

### 2.9.2. Hibaelhárítási folyamat és diagnosztikai eszközök

A hibakezelés folyamatát a Boschnál szabványosították;

1. **A bejelentést felvesszük** az ITSD rendszerbe
2. **Az elsődleges diagnózist** a helyi IT-csapat állította fel, tapasztalatukra támaszkodva.
3. **Hálózati elemzés** a switch naplókból, a portstatisztikákból és az SNMP-adatokból származó információk alapján
4. Amikor a hiba súlyosabb kategóriába sorolható, a felmerült **problémát** a hálózati osztály felé kell **továbbküldeni.**

A diagnosztikai folyamat során a LAN Physics adatbázis kulcsfontosságú szerepet játszik: minden switchportot, eszközkapcsolatot és VLAN-összerendelést gondosan nyilvántart.

„A LAN Physicsben azonnal látjuk, hogy egy eszköz melyik switchhez és porthoz tartozik. Ha valaki bejelenti, hogy nincs hálózat, elég a hostname-et beírni, és máris tudjuk, hol kell keresni.” - mondta Dániel.

Továbbá a *SolarWinds* és a *Cisco DNA Center* műszerfalai élő forgalmi és hibaadatokat jelenítenek meg, ami lehetővé teszi, hogy a hibák nagyrésze már a felhasználók tapasztalása előtt felfedezhető legyen.

## 2.10. Fejlesztési irányok és szervezeti hatások

A Secure BCN projekt bevezetése nem csupán technológiai változást hoz, hanem egyúttal szervezeti struktúra- és kompetenciafejlesztési átalakulást is indít el a Bosch Digital csapatai körében.

### 2.10.1. Az automatizálás hatása az üzemeltetésre

A DNS-szerű, automatizált konfigurációkezelés már most azt sugallja, hogy a közeljövőben a manuális beavatkozások száma fokozatosan csökkenni fog.

„Régebben napi szinten kellett belépnünk konzolról, portokat engedélyezni vagy VLAN-t állítani. Most inkább az a feladat, hogy figyeljük a rendszert, értelmezzük a logokat, és előre lássuk a problémákat.” - mondta Kiss Dániel.

Az algoritmusok egyre nagyobb mértékben átvehetik a döntéshozatalt, de a szakértelem jelentősége még inkább előtérbe kerül, hiszen a rendszerek értelmezését és felügyeletét továbbra is emberi kompetenciákra kell alapozni.

### 2.10.2. Tudásátadás és képzés

A Hatvani Bosch IT-csapata rendszeresen részt vesz a *Cisco Networking Academy* és a Bosch belső IT-képzésein, ahol a cél, hogy a kollégák magabiztosan kezeljék az SDA (Software Defined Access) és a DNA Center rendszereit.

„Mi is tanuljuk a rendszert. Az új eszközök teljesen más szemléletet kívánnak. Sok idő, mire az ember megszokja, hogy a konfigurációk már nem kézzel készülnek, hanem sablonból."

A Bosch Digital jövőbeli működésének alappillérét a képzések adják: arra törekszünk, hogy minden telephely önállóan, a központi irányelveket betartva képes legyen saját hálózatát kezelni.

## 2.11. Összegzés és fejlesztési hatások

Az elmúlt két évtizedben a Hatvani Bosch hálózati infrastruktúrája jelentős átalakuláson ment keresztül. A kezdeti egyszerű IP-szegmentációs felépítés ma már egy korszerű, redundáns és automatizált hálózatként működik, amely teljes mértékben megfelel a gyártás digitalizációjának követelményeinek.

A *Secure BCN* és a *Cisco DNA Center* bevezetésével a hálózati üzemeltetés egy új korszak küszöbén áll:

- A portok automatikus konfigurálásának köszönhetően a kézi beavatkozás feleslegessé válik.
- A hibakeresés lényegesen gyorsabb, s a pontossága is nő
- A biztonsági szintek felügyelete központilag is megoldható.
- A hálózati adatok átláthatósága új, eddig nem látott szintre emelkedik.

Kiss Dániel szavait idézve:

„A cél, hogy minden eszköz automatikusan felismerhető legyen, és a rendszer maga döntse el, milyen jogosultságot kap. Ez biztonságosabb és gyorsabb, mint bármi, amit eddig használtunk."

## 2.12. Záró megállapítások

A Hatvani Bosch hálózati infrastruktúrája élénk példát ad arra, hogyan képes egy ipari környezet a digitalizáció által támasztott kihívásokra reagálni. Az üzemeltetés frontvonalában Kiss Dániel és csapata mindennap küzd a bonyolult hálózati környezet fenntartásának nehézségeivel, miközben a fejlesztések hosszú távon pont az ő feladataikat könnyítik meg, s egyúttal növelik hatékonyságukat.

A modernizáció hatására a Hatvani Bosch nemcsak a technológiai színvonalon, hanem szervezeti felkészültségében is jelentős előrelépést ért el. A hálózati automatizálás, a biztonság megerősítése és a tudásmegosztás együttesen teszik lehetővé, hogy a gyár a Bosch-csoport egyik legkorszerűbb informatikai központjává váljon.

A Secure BCN projekt, amely a Hatvani Boschnál valósult meg, a hálózati automatizálás és biztonság erősítésének egyik legkiemelkedőbb példája. A projekt célkitűzése, hogy az IT-biztonsági konfigurációkat automatizált módon kezelje, így mérsékelve az emberi beavatkozás szükségességét és minimalizálva a hibák előfordulási esélyét (Chauhan, 2025). Az automatizált megoldások a hálózatbiztonság terén szervesen illeszkednek az ITIL- és

ITSM-elvű keretekhez, melyek a stabil és proaktív működés biztosítását helyezik előtérbe (Zhao és Rao, 2017).

# 3. Az IT-eszközpark fejlesztése és menedzsmentje

A Hatvani Robert Bosch Elektronika Kft. informatikai infrastruktúrájának egyik sarokköve az IT-eszközpark, amely közvetlenül elősegíti a gyártási, logisztikai és irodai folyamatok zökkenőmentes működését. Ennek a parknak a karbantartása, rendszeres frissítése és korszerűsítése nem csupán technikai feladat, hanem egyben kritikus üzemfolytonossági és biztonsági kérdés is.

A flottakezelő rendszer bevezetésekor az informatikai biztonság kiemelkedő jelentőséggel bír. Mivel a járművek és az eszközök közti kommunikáció általában TCP/IP protokollra épül, ezáltal fokozottan érzékeny a hálózati támadásokra. A gondosan beállított tűzfalak, a szegmentált VLAN-hálózatok, valamint a VPN- és TLS-alapú titkosítási megoldások jelentősen növelik a rendszer megbízhatóságát és adatvédelmi szintjét. Az ipari automatizálási hálózatok biztonságát vizsgáló kutatások szerint az ilyen típusú megközelítések csökkentik az adatvesztés és a hálózati incidensek kockázatát (DePriest, 1997).

A cég közel ezernyi számítógépet üzemeltet, melyek közül több száz a gyártási területen végez kritikus feladatokat. Ezek az eszközök nem csupán az irodai munkát támogatják, hanem az automatizált termelési rendszerek irányításában is kulcsfontosságú szerepet játszanak. Egy meghibásodott vagy elavult gép ezért közvetlenül ronthatja a gyártás hatékonyságát, s akár leállást is okozhat.

Bosch Digital hatvani csapatának tagjaként személyesen is bekapcsolódtam az IT-eszközpark korszerűsítését célzó Windows 11 migrációs programba. A projekt 2025-ben vált kiemelt feladattá, miután a Microsoft 2025. október 14-én hivatalosan megszüntette a Windows 10 támogatását. Ez a határidő a gyárra komoly próbatételt jelentett, mivel a meglévő gépek túlnyomó része még mindig Windows 10-et futtatott.

## 3.1. Az IT-eszközpark jelentősége és összetétele

A hatvani gyár eszközparkja számos változatos kategóriát ölel fel, a felhasználás konkrét szakterületétől függően. Az irodai terekben elsősorban laptopok, kompakt SFF (Small Form Factor) PC-k, valamint asztali towerek találhatók; ezzel szemben a gyártási szektorban a kisméretű Tiny PC-k veszik át a vezető szerepet, mivel szerény méretük és ipari szintű strapabírásuk lehetővé teszi, hogy szervesen illeszkedjenek a gépsorok mellé.

Az eszközök a vállalati hálózat szövetébe szövedve, a Bosch Configuration Management Interface (CMI) és az End Device Management Tool (EDMT) rendszerek szinergiájával működnek. A CMI gondoskodik a szoftveres felügyeletről, a frissítések dinamikus bevezetéséről, valamint a biztonsági konfigurációk precíz beállításáról; az EDMT pedig a készülékek egész életciklusát követte nyomon a telepítés kezdetétől a selejtezés végéig.

Az IT-eszközpark üzemeltetésének talán legnagyobb kihívása, hogy egyszerre kell kielégíteni a gyártási stabilitás és a folyamatos innováció követelményeit. Mivel a termelésben használt PC-ket csak a tervezett leállások idején lehet frissíteni, minden egyes változtatást gondosan elő kell készíteni, hogy elkerüljük a váratlan meghibásodásokat.

## 3.2. A Windows 11-re való átállás szükségessége

2025 elején a vállalat központi IT-irányelvei meghatározták, hogy az év végéig minden telephelyen meg kell történnie a Windows 11-re való teljes átállásnak. A döntés mögött nem csupán a Windows 10 támogatásának megszűnése húzódott meg, hanem az is, hogy az új rendszer sokkal fejlettebb biztonsági lehetőségeket nyújt, többek között a TPM 2.0 modul támogatását, korszerűbb eszköz-titkosítást és hardveres védelmet.

A Windows 11-re való átállás projektjénél talán a leglényegesebb szempont az informatikai biztonság szilárd biztosítása. Az automatizált rendszerfelügyeleti megoldások, köztük a központosított frissítés- és jogosultságkezelés, jelentősen mérséklik az emberi tévedésekből adódó kockázatokat, egyúttal erősítik a hálózat védelmét. A kutatások szerint, ha Windows és Linux rendszereket egyszerre kezelünk, az AES-256 titkosítás és a biztonságos virtuális kommunikációs csatornák (VPN) használata elengedhetetlen az adatbiztonság szempontjából (Basinya, 2018). Az új generációs IT-környezetekben is gyakran háttérbe szorulnak a kulcsfontosságú hálózati protokollok (például a DNS, a DHCP vagy a TCP/I), és ha ezeket figyelmen kívül hagyják, komoly biztonsági rések nyílnak meg. A protokollok alapos kezelése ezzel egyidőben a vállalati informatikai biztonság szilárd alapja (Guluzade, 2024).

A probléma abból adódott, hogy a gyárban körülbelül ezer Windows-operációs rendszerrel rendelkező számítógép működött, de ezek mintegy kétszázanál több nem felelt meg a Windows 11 által előírt minimális hardverkövetelményeknek. Mindez csak fokozta a problémát, mivel ezeket az eszközöket tipikusan a gyártósorokban üzemeltették, ahol egy rendszerleállás azonnal termelési kiesést idézett volna elő.

Miután a Windows 10 támogatása megszűnt, a gépek biztonsági frissítései leálltak, és a vállalat kockázatelemzése szerint ez komoly sebezhetőségi és adatvédelmi kockázatot jelentett. Ez a projekt nem csupán egy technológiai frissítést jelentett, hanem egy üzletmenet-folytonossági feladatot is, amelynek célja az volt, hogy egyetlen eszköz se legyen működésképtelen támogatás hiányában.

## 3.3. A projekt előkészítése

Az első projektfázis a felmérés és az adatgyűjtés köré épült, ahol a Bosch Digital csapata az SCCM (System Center Configuration Manager) rendszeréből kinyert riportok alapos elemzésével foglalkozott. Az összegyűjtött adatokból kiderül, melyik eszköz milyen Windows-verziót, melyik buildet és milyen firmware-t futtat, s egyben látható, hogy telepítve van-e a TPM 2.0 modul, illetve, hogy támogatja-e a Secure Boot funkciót.

Az érintett eszközök felsorolását átböngészve három különálló kategóriát fogalmaztunk meg:

1. **Frissíthető gépek**, melyek hardveres feltételei megfelelnek a Windows 11 telepítéséhez.
2. **Korlátozottan frissíthető gépek**, melyek néhány beállítás finomhangolása és egy BIOS-frissítés után már megfelelően használhatóvá válnak.
3. **Nem frissíthető gépek,** amiket ki kellett cserélni.

Az utolsó kategóriába sorolt, mintegy 200 gép cseréje önmagában már egy külön projektfeladatot jelentett.

## 3.4. A frissítések végrehajtása a CMI-n keresztül

A projekt egyik kulcsfontosságú technikai eleme a Configuration Manager Interface (CMI) volt; ezen keresztül a Windows 11 frissítéseket push-módszerrel szállítottuk a gépekre. A folyamat azonban nem volt teljesen automatizált: minden gépnél manuálisan kellett beindítani a frissítést, majd alaposan ellenőrizni, hogy a telepítés valóban lefutott-e.

A frissítés előtt minden gépet a webes riporton keresztül átnéztek, hogy a kötelező Windows 10 frissítések, például a 22H2 build, már telepítve vannak-e. Ha valamelyik frissítés hiányzott, az adott gép tulajdonosával közvetlenül kellett egyeztetni.

„A projekt során kulcsfontosságú volt a felhasználókkal való kommunikáció. Hiába ment rá a push, ha a gép tulajdonosa nem frissítette időben, az egész folyamat elakadt.”

*(forrás: Saját interjú, Bosch Digital Hatvan,2025)*

Ez a szakasz egyszerre jelentett technikai és kommunikációs kihívást; a felhasználók aktív bevonása és lelkesítése hiányában a projekt tempója valószínűleg jelentősen elcsúszott volna. A tapasztalat egyértelműen rámutat, hogy a dinamikus, kétirányú kommunikáció legalább olyan fontos, mint magának a technikai megvalósításnak az elvégzése.

## 3.5. Az eszközcserék lebonyolítása

A projekt második, már igazán jelentős szakaszában a nem kompatibilis eszközök fizikai cseréje zajlott le. A központi beszerzés keretében 400 friss Dell Optiplex Tiny PC érkezett, amelyek már leváltották a korábban használt, elavult gépeket.

Az újdonsült gépek előre telepített Windows 11-gyel érkeznek, ám a vállalati környezethez szükséges beállításokat, például a domain-csatlakozást, a szoftverkészletet és a biztonsági szabályzatokat, kézzel kellett konfigurálni. A telepítést az *EDMT (End Device Management Tool)* ticket-rendszerrel valósítottuk meg, ahol minden cseréhez egyedi ticketet kellett felvenni.

Mivel a felhasználók nem saját maguk indították a folyamatot, minden egyes eszközcserét kézi értesítés és előzetes időpont-egyeztetés előzte meg. Három hét folyamán mintegy háromszáz bejelentést dolgoztunk fel, ami átlagosan naponta húsz-két-öt számítógép telepítésével egyenlő.

„A telepítő helyiségben egyszerre akár tíz Tiny PC-t is előkészítettünk. Azonban hamar kiderült, hogy a rendelkezésre álló nyolc LAN-port kevés, ezért beépítettünk egy 48 portos switch-et, hogy párhuzamosan több gépet tudjunk telepíteni.”

*(forrás: Saját interjú, Bosch Digital Hatvan,2025)*

Ez a feladat igazi intenzív kihívásként jelentkezett: a fleet management team három hétig tartó erőfeszítéssel bíbelte a fizikai előkészítést, a csomagok kibontását, a rendszer konfigurálását, s végül a regisztrációt. A csere során visszavettük a régi berendezéseket, a felhasználók pedig új, Windows 11-es számítógépekkel gazdagodtak.

## 3.6. Kihívások és problémák

A projekt folyamán számos technikai és szervezeti kihívás is felbukkant:

- **Felhasználói együttműködés hiánya**: több esetben úgy tapasztaltuk, hogy a gép tulajdonosait meggyőzni arról, hogy időben visszajuttassák az eszközöket, vagy elindítsák a frissítések újraindítását, nem volt egyszerű.
- **Időnyomás:** a 2025. október 14-i határidő szorította a projektet, csupán néhány hét állt a rendelkezésre, hogy a gyártásban lévő több száz gépet átalakítsuk.
- **Erőforrás-korlátok**: szűkös LAN-portok, korlátozott hely és emberi kapacitás.
- **Adatmentési és kompatibilitási kérdések**: egyes gyártási szoftverek kizárólag a Windows 10 környezetben biztosítottak stabil működést, így ezekhez a programokhoz külön tesztelési lépéseket kellett beiktatni.

Az egyik legkritikusabb fenyegetés a körülbelül kétszáz darab, a gyártósoron használt Tiny PC elavult állapota volt, hiszen október elején még egyetlen frissítést sem kaptak. Egy esetleges egyidejű támogatásvesztés nem csak komoly fennakadásokat idézett volna elő, de akár a teljes gyártási folyamat leállását is eredményezhette volna.

Három hét intenzív munka után ez a szám 34-re csökkent, ami már egy kezelhető kockázati szintet jelentett.

## 3.7. Tanulságok és javaslatok

A projekt során kiderült, hogy az eszközpark-menedzsment feladatai túlmutatnak a technológiai szférán, hiszen kommunikációs és szervezési vonalat is érintenek. A legfontosabb tanulságok a következők:

- A **tervezés időben történő megvalósítása** kulcsfontfontosságú, egy ilyen mértékű átállást érdemes legalább hat hónappal előbb megkezdni.
- A **felhasználók bevonása** kulcsfontosságú; az IT-projektek sikerét gyakran a végfelhasználók együttműködési hajlandósága határozza meg.
- Hasznos lenne, ha hosszú távra egy **automata frissítési mechanizmust** hoznánk létre, amely a CMI-n keresztül önműködően szervezi meg a jelentős operációs rendszer-frissítéseket.

A projekt következtében a Hatvani Bosch üzem informatikai rendszerét 2025. októberig úgy hangolták, hogy az mindenben megfeleljen a Bosch-csoport által szigorúan megkövetelt biztonsági és kompatibilitási előírásoknak, ennek eredményeként a gyártás zökkenőmentesen zajlik a Windows 11 operációs rendszerben.

## 3.8. Összegzés

A Windows 11-re való átállás projektje egy hihetetlenül összetett feladatként jelent meg, amely a technikai szakértelem mellett szervezési, kommunikációs és időmenedzsment készségeket is elvárt. A projektben való személyes részvételem lehetőséget adott arra, hogy közvetlenül tapasztaljam meg, milyen kihívásokkal jár egy vállalati szintű informatikai változás kezelése.

Az átállás során szerzett tapasztalatok a jövőbeni fejlesztések és frissítések szempontjából is iránymutatóak lehetnek, hiszen egyértelművé vált, hogy a siker kulcsa az előkészítés, az átlátható folyamatmenedzsment és a hatékony kommunikáció az érintett felhasználókkal.

# 4. Az IT Space problémái és fejlesztési irányai

Az IT Space, amely a Hatvani Robert Bosch Elektronika Kft. informatikai struktúrájának része, kiemelt szerepet tölt be: ez az egység az egyik legfontosabb, és közvetlen felhasználói kapcsolatokkal rendelkező szekció. Feladata, hogy naponta a gyárban dolgozó több ezer munkatárs számára zökkenőmentes informatikai támogatást, az eszközök gördülékeny kezelését és a felmerülő hibák gyors megoldását biztosítsa. Az IT Space feladata a vállalat helyi IT Helpdesk biztosítása, mintegy első védelmi vonalként közvetítve a felhasználók és a központi Bosch Digital infrastruktúra között.

Mivel a Bosch csoport a világ minden táján több százezer informatikai berendezést kezel, a helyi IT-csapatok (a hatvani Bosch IT Space egységét is beleértve) szigorú protokollok és kidolgozott folyamatok mentén dolgoznak. Az informatikai folyamatok központosított, ITIL-alapú működése egyfelől egységesítést és biztonságot biztosít, másfelől a helyi igények és a napi operatív feladatok kezelése során több gyakorlati akadályba ütközik, főleg a ticketkezelés, a kommunikáció és a rendszerintegráció terén.

A következő fejezetben részletezzük az IT Space működésének legfontosabb vonásait, feltárjuk a már azonosított problémákat, valamint bemutatjuk a már megkezdett és a tervezett fejlesztési irányokat, melyek a hatékonyság, az átláthatóság és a digitalizáció erősítését tűzték ki célul.

## 4.1. Az IT Space szerepe és folyamatai

Az IT Space feladata, hogy a felhasználók számára zökkenőmentes támogatást nyújtson, a helyszíni eszközök állapotát folyamatosan karbantartsa, a felmerülő hibákat hatékonyan orvosolja, s a teljes IT-eszközparkot mindennap gondosan üzemeltethesse. Az alkalmazottak a vállalati IT Service Portalon keresztül adhatnak le bejelentést, ez a felület egyúttal a hibabejelentések (incidensek), a szolgáltatásra vonatkozó kérvények (service requestek) és az új eszközök rendelésének indítására szolgáló platform.

Az érkezett igények automatikusan ticketekké alakulnak; ezeket az IT Space csapat a SMT (Service Management Toolkit) rendszerben dolgozza fel.A flotta menedzsmenthez kapcsolódó eszközadatok és státuszok az EDMT (End Device Management Tool) adatbázisában találnak otthonra, ahol biztonságosan őket tárolja.

Az IT Service Portal, az SMT és az EDMT három rendszere együttesen gondoskodik arról, hogy az IT-folyamatok minden szakaszát lefedjék, a kezdeti lépésektől a végső lezárásig. A rendszer ma több párhuzamos platformon működik, ám az adatáramlás és a státusz-szinkronizáció ezek között nem mindig valós időben valósul meg. Az IT Space mindennapi működésében a rendszerkomplexitás kétségtelenül az egyik legnagyobb kihívás.

## 4.2. Az IT Space jelenlegi működési kihívásai

Az IT Space részleg feladata, hogy a vállalat belső informatikai szolgáltatásai magas rendelkezésre állással és zavartalan működéssel rendelkezzenek. Az ITIL alapelveinek érvényesítése ezen a téren különösen fontos, hiszen felgyorsítja az incidensek megoldását és erősíti a felhasználói elégedettséget. Az automatizált jegykezelő rendszerek és folyamatok bevezetése csökkenti az emberi hibákat, miközben javítja a válaszidők hatékonyságát (Elhefnawi, 2013; Gray, 2006).

Az IT Space nem csak egy egyszerű technikai támogató központ, hanem a vállalati informatikai szolgáltatásmenedzsment (ITSM) konkrét helyi megtestesülése, pont azon a színtéren, ahol a digitális infrastruktúra működését emberi közelségben érzékeljük.

Az IT Space feladatai rendkívül sokszínűek:

- felhasználói eszközök (laptopok, Tiny PC-k, monitorok, perifériák) kiadása és kezelése,
- szoftveres segítségnyújtás, a hibabejelentések körültekintő feldolgozása
- hálózati incidensek átküldése, majd alapos felderítése
- a hozzáférések és jogosultságok hatékony menedzselése
- Az informatikai eszközpark nyilvántartásának naprakészen tartása és az EDMT-rendszer frissítése

Az IT Space a napi feladatok során szoros együttműködésben dolgozik a fleet managementtel, mert minden egyes eszköz áthelyezése, cseréje vagy javítása közvetlenül befolyásolja az eszköznyilvántartási folyamatokat. Az IT Space-ben szerzett gyakorlati tapasztalataimra építve több, a hatékony működést gátló tényező is feltűnik: egyesek a folyamatok szervetlen voltaiból, mások az infrastruktúra hiányosságaiból, sőt a kommunikációs szakadékokból táplálkoznak.

### 4.2.1. Magas ügyfélforgalom és kapacitásproblémák

A legszembetűnőbb nehézség az IT Space-ben a fizikai terület túlzsúfoltsága. Sok munkatárs még mindig személyesen befordul az irodába olyan ügyekkel, amelyek online is intézhetők, például jelszócserét, kisebb szoftverhibákat vagy eszközhozzáférési kérdéseket. A személyes forgalom időnként olyannyira nő, hogy az IT Space munkatársai adminisztráció helyett ügyfélszolgálati feladatokat végeznek, miközben háttérfeladataik (eszközkiadás, riportolás, EDMT-frissítés) késnek.

**Fejlesztéshez kapcsolódó javaslat:** Az IT Service Portal használatára való felhasználói oktatás, valamint egy önkiszolgáló terminál (vagy egyszerűen kioszk) bevezetése az IT Space bejáratánál. Ez lehetőséget adna arra, hogy a legegyszerűbb, de mégis kritikus kéréseket (fiókzárolás, jelszóreset vagy USB-hozzáférés) a dolgozók online benyújthassák, ezáltal a személyes megjelenések mennyisége csökken.

### 4.2.2. A többplatformos működés és az integráció szükségessége

A jelenlegi működés három önálló, ugyanakkor egymáshoz szorosan kapcsolódó rendszerre épül:

1. **IT Service Portal**: egy webes felület, amely a felhasználók számára látható, a ServiceNow-ra építve. Ezen a felületen hozhatók létre ticketek, adhatók le eszközrendelések, kérhetők jelszóújítások, vagy indíthatók szoftverkérések.
2. **SMT (Service Management Toolkit)**: a Bosch által kifejlesztett belső rendszer, amely az IT Space-nek nyújtja a ticketek kezelését, rangsorolását és végleges lezárását.
3. **EDMT (End Device Management Tool)**: egy átfogó eszköznyilvántartási és -kezelési platform, amely a kliens- és hálózati eszközök minden adatát tárolja, beleértve a státuszjelzéseket, a ticket-azonosítókat és az életciklus-információkat.

A három rendszer közti adatáramlás egy egymásra épülő, láncszerű struktúrában valósul meg: A felhasználó a Service Portalon keresztül indít egy igényt → az adat az SMT-hez kerül feldolgozásra → végül az EDMT-ben frissül az érintett eszköz státusza. Az egész folyamat általában jól működik, de a különböző backendek és adatmodellek közti eltérések miatt a kommunikáció nem mindig marad szinkronban, és gyakran többszörösen redundáns.

Egy gyakorlati példában, ha egy felhasználó gépet szeretne megrendelni, a folyamat a következő sorrendben valósul meg:

1. Az IT Service Portal felületén a „Request a Computer” feliratú csempére rákattint, és kitölti az ott található form-ot

2. A beérkező kérelmet a ServiceNow rendszerében rögzítik,

3. Az adat az SMT felé kerül átküldésre,

4. Ezt követően a rendelést az EDMT-hez küldik, ahol a feldolgozási folyamat elindul.

Minden rendszer önálló adatbázist tart fenn, így a státuszfrissítéseket és a lezárásokat gyakran manuális visszajelzést igényelnek az IT-csapat részéről.

#### 4.2.3. Egymással párhuzamos rendszerarchitektúrák és redundánsan felépített folyamatok

A többplatformos működés komplex problémákat vet fel, amelyek a következők:

- A három különböző rendszerben a ticketek állapota nem mindig egyezik.
- A felhasználó számára nem teljesen átlátható, hol tart a benyújtott kérése.
- Az IT Space munkatársainak duplikált adminisztratív feladatokat kell ellátniuk.
- A hibakeresés üteme lecsökken, mivel az információk több, egymástól távol eső forrásban vannak eloszlatva.

Az összetett rendszer leépíti a napi munka hatékonyságát és az átláthatóságot is, különösen akkor, amikor egyszerre rengeteg ticketet kell kezelni.

### 4.3. A ServiceNow-integrációs fejlesztés

A Bosch Digital a közeljövőben megkezdi az SMT és az EDMT rendszerek ServiceNow környezetbe való integrálását. Az új architektúra ambíciója, hogy a három szétválasztott platform helyett egy összefűzött, központi keretrendszert hozzon létre, amely a ticketek minden szakaszát (a felhasználók első bejelentésétől a végső lezárásig) lefedi.

A fejlesztés vezérelő koncepciója, hogy egyetlen adatforrásra és egyetlen backendre építsünk.A jövőben minden bejelentés, frissítés és eszközinformáció a ServiceNow háttérrendszerében kerül tárolásra, ezáltal az IT Space és a flottakezelő csapat egy egységes felületen fog együtt dolgozni.

A változás meghatározó összetevői:

- Az SMT funkciók beillesztése a ServiceNow platformba
- Az EDMT adatbázis szinkronizálása a ServiceNow háttérrendszerrel,
- Közös riportálási és dashboard rendszer bevezetése
- Központosított, egységes jogosultságkezelés.

Az integráció drámai módon lecsökkenti a kézi adminisztrációt, s egyben mérsékelni fogja az adatátvitel során bekövetkező hibák számát. A felhasználók egyetlen felületen tekinthetik meg a ticketek állapotát, míg az IT Space valós időben kap friss információkat az eszközpark helyzetéről.

Az új rendszer bevezetését várhatóan 2026 elején hajtják végre, a pilot telephelyek listáján a Hatvani Bosch is megjelenik. A fejlesztés hosszú távon arra ad esélyt, hogy a digitális papírhasználat teljesen háttérbe szoruljon, miközben a folyamatok automatikusan a központi ITIL műszerfalak felé irányulnak.

### 4.3.1 Az integráció előtti állapot kihívásai

Az összetett, több rendszert egyesítő felépítés következtében a belső folyamatok egyre időrablóbbak, és a csapaton belüli kommunikációra is nagyobb nyomás nehezedik.

**Az új rendszer bevezetésétől várható hatások:**

- **Egységes adatmodell**: minden eszközt és ticketet egy helyen lehet nyomon követni és kezelni.
- **Központi dashboard**: valós időben érkező riportok az IT-vezetés és a Bosch Digital felé.
- **Felgyorsult felhasználói** visszajelzés: a jegyek státusza azonnal frissül.
- **Csökkentett manuális munka:** automatizált státuszfrissítések és ticket-átirányítás.
- **Átláthatóbb folyamatirányítás**: így az IT Space csapat könnyebben tudja rangsorolni az eseteket.

## 4.4. Operatív problémák az IT Space működésében

Az IT Space működését több, napi szinten felmerülő nehézség is érinti:

- **Túlterheltség**: A csapat csupán néhány tagból áll, ám naponta több tucat új ticket érkezik, ami könnyen meghaladja a rendelkezésre álló kapacitásukat.
- **Felhasználói kommunikáció**: több felhasználó még mindig személyesen lép be az irodába, ahelyett, hogy a Service Portalon keresztül jelentenék a hibákat.
- **Ticketprioritás**: A rendszer automatikusan meghatározott prioritásai gyakran nem tükrözik pontosan a tényleges üzleti sürgősséget.
- **Dokumentációs nyomás**: a jegyek lezárása során gyakran egy egész sor adminisztratív lépésbe ütközünk.

E problémák egy részének forrása az, hogy a folyamatokat egy szigorúan centralizált, ITIL-elveire épülő szabályrendszerhez kötik; ez a struktúra azonban nem mindig képes a helyi specifikus igényekhez való tökéletes illeszkedésre.

## 4.5. Fejlesztési javaslatok és megoldási irányok

A felhalmozott tapasztalatokra támaszkodva már egyértelműen körvonalazódnak a következő fejlesztési irányok:

1. **Automatizált ticket routing**: a ServiceNow integráció lehetővé teszi, hogy a beérkező kéréseket automatikusan kategorizálják és a megfelelő csoportokhoz rendeljék, ezáltal a manuális ticket-elosztás mértéke jelentősen csökken.

2. **Önkiszolgáló tudásbázis**: a felhasználók kényelmesen hozzáférhetnek, kereshetnek benne, ami nagymértékben mérsékli a helpdesk-re nehezedő nyomást.

3. **KPI-monitoring és dashboard**: amikor a valós időben frissülő kulcsfontosságú mutatók (például az átlagos válaszidő, a lezárási idő és a ticket backlog) megjelennek a felületen, az nagyban könnyíti a kapacitástervezést.

4. **Az IT Service Portal használatát támogató kommunikációs kampány**: a felhasználók tájékoztatása, mely problémákat kezelhetnek önállóan.

5. **Közös IT- és flottakezelési riport**: az EDMT és a ServiceNow integrációjával az eszközök állapota, a frissítések és a ticket-adatok egy helyen áttekinthetők.

## 4.6. Összegzés

Az IT Space gördülékeny működése nélkülözhetetlen ahhoz, hogy a Hatvani Bosch informatikai rendszere megbízhatóan stabil maradjon. A mindennapi működés közben azonban a többplatformos ticketkezelés, a manuális folyamatok és a kommunikációs korlátok jelentős kihívásként bukkanak fel.

A ServiceNow bevezetése, amely már a közeljövőben várható, a vállalat informatikai digitalizációjának egyik legkritikusabb és legjelentősebb lépést jelenti. Az SMT és az EDMT rendszerek összeolvadása nem csupán az IT Space-ot, hanem a teljes helyi IT-üzemi folyamatot egyetlen egységes struktúrába fonja. Az átalakítás révén a működés gördülékenyebbé válik, az adminisztrációs terhek csökkennek, és a teljes IT-infrastruktúra most már valós időben nyomon követhető és átlátható.

A projekt hosszú távon biztosítja, hogy a Hatvani Bosch informatikai szervezete hatékonyabb, gyorsabb és egységesebb módon reagáljon a felhasználói igényekre, miközben szervesen beilleszkedik a Bosch Digital nemzetközi IT-transzformációs stratégiájába.

# 5. Összegzés és értékelés

Az elmúlt évek során a Hatvani Robert Bosch Elektronika Kft. informatikai rendszere jelentős fejlődési hullámot élvezett, miközben technológiai és szervezeti dimenzióiban egyaránt új szintekre emelkedett. A vállalat működésének szívében áll az informatikai infrastruktúra, az eszközpark és a hálózati háttér, amelyek összhangja garantálja, hogy a gyártási és adminisztratív folyamatok akadálytalanul folyjanak.

A szakdolgozat fejezetei alaposan feltérképezték a vállalat informatikai rendszerének főbb területeit, a hálózati infrastruktúrát, az IT-eszközpark működését, s az IT Space egység mindennapi kihívásait és a fejlesztés lehetséges irányait. A vizsgálatok fényében egyértelműen megállapítható, hogy a Hatvani Bosch informatikai működése kiemelkedően magas színvonalat képvisel; ugyanakkor számos szegmensben elengedhetetlen a célzott, jól felépített fejlesztések bevezetése, hogy a globális Bosch Digital stratégia által támasztott elvárásoknak továbbra is megfelelően megfeleljen.

## 5.1. Az informatikai infrastruktúra értékelése

Az infrastruktúra fejezetben bemutatott alapos elemzések világosan kimutatták, hogy a Hatvani Bosch informatikai hálózata egyszerre stabil és korszerű, de mögötte egy hihetetlenül összetett felépítés áll. A gyártási és irodai részlegek közti fizikai, valamint logikai szegmentálás erős biztonsági védelmet nyújt, ám a hálózat folyamatos karbantartása és fejlesztése állandó figyelmet követel.

A hálózatfejlesztésre irányuló projektek (köztük a LAN Physics felújítása) nyilvánvalóan erősítették a rendszer megbízhatóságát és jelentősen bővítették a skálázhatóságát. Az interjúkból származó tapasztalatok fényében megfogalmazható, hogy a hálózatfejlesztési folyamatokban a vállalat fokozatosan a szerkezetileg átgondolt, alaposan dokumentált és szabványosított megoldások felé hajlik.

A legfőbb eredmény, hogy a hálózati rendszer már moduláris szerkezetben bővíthető, ami megalapozza a közeljövő digitális átalakulására és IoT-re épülő gyártási projektjeit.

## 5.2. Az IT-eszközpark fejlesztéseinek értékelése

A Windows 11 átállását célzó projekt remekül feltárta a Hatvani Bosch informatikai eszközpark komplexitását, és egyúttal rámutatott az IT-csapat magas fokú felkészültségére.A projekt alatt több mint ezer eszközt frissítettünk vagy cseréltünk, miközben a termelés folyamatosan működött, és mindezt három héten belül sikerült elvégezni.Az eddigi projektélmények fényében három alapvető tényező kerül előtérbe:

1. A **felhasználókkal folytatott kommunikáció** kulcsfontosságú szerepet játszik.
2. A **rendszerszintű riportolás** és az állapotellenőrzés elengedhetősége.
3. A **manuális folyamatok korlátai**, amelyek a közeljövőben automatizálás révén enyhíthetők.

Az IT-eszközparkot a Bosch Digital előírásai szerint kezeljük, de a jelenlegi állapota még mindig jelentős humán erőforrást igényel. A fejlesztési javaslatok (automatizált ticketkezelés, MDM-integráció, zero-touch deployment) bevezetése hosszú távon drámaian csökkentheti a karbantartási kiadásokat, s egyben mérsékelheti a rendszerhibák előfordulását.

Végül a projekt egyértelműen azt mutatta, hogy a Hatvani Bosch IT-csapata már képes komplex, szoros határidős informatikai átállásokat megvalósítani anélkül, hogy a gyártási folyamatok egyetlen percig sem leállnának.

## 5.3. Az IT Space működésének értékelése

Az IT Space az informatikai támogatás frontvonalán tevékenykedik, ahol naponta több tucat felhasználói megkeresést kezel. A fejezetben bemutatott tapasztalatok szerint a szervezet erőssége az operatív rugalmasság és az egyéni szakmai kompetencia, azonban jelenleg több struktúrális korlát is megnehezíti működését.

A háromrendszeres működés (az IT Service Portal, az SMT és az EDMT) redundáns és időigényes. Az IT-csapatot a folyamatok közötti szinkronizáció hiánya gyakran arra készteti, hogy egyszerre, párhuzamosan adminisztrálja ugyanazokat az adatokat.

Az előttünk álló ServiceNow-integráció stratégiai szempontból kiemelkedő jelentőséggel bír. Ez az egységesítés nem csupán a rendszerarchitektúra leegyszerűsödését hozza magával, hanem a hatékonyság és az átláthatóság egyaránt fokozódását is előidézi majd. A felhasználói élmény szempontjából ez a megoldás biztosítja, hogy az ügyintézés teljesen digitális környezetben, egyetlen közös felületen valósuljon meg.

Az IT Space működésének átfogó értékelése során egyértelműen megfigyelhető, hogy a csapat rendkívül elkötelezett, ám a jelenleg rendelkezésre álló kapacitás gyakran nem elégséges a felgyarapó feladatkörök befogadásához. A közeljövőben a munka mennyiségének kiegyensúlyozása és a jegykezelés automatizálása talán a fejlődés legfontosabb mozgatórugója lesz.

## 5.4. Átfogó értékelés és következtetések

A Hatvani Bosch informatikai tevékenységét alaposan felmérve azt állíthatjuk, hogy a vállalat IT-rendszere stratégiai szinten stabil, a fejlesztési folyamatok pedig dinamikusak, miközben a mindennapi üzemeltetés során még számos, eddig rejtve maradt optimalizálási lehetőség adódik.

A hálózati infrastruktúra és az IT-eszközpark már a Bosch Digital nemzetközi előírásainak megfelelően működik, ám a helyi IT-folyamatok alapos finomhangolása nélkül nem garantálható, hogy a rendszer hosszú távon is fenntartható és skálázható maradjon.

Az elemzések fényében három meghatározó tanulságot lehet kiemelni:

1. **Az informatikai folyamatok egységesítése a szervezet működésének alapvető mozgatórugója.** Az SMT, az EDMT és a Service Portal rendszerek integrációja az elmúlt évek egyik legjelentősebb előrelépése, amely hosszú távon az egész IT-ökoszisztéma egyszerűsítését szolgálja.
2. **Az automatizáció a jövő felé mutató irányt jelöli.** A Windows 11 átállási projekt és az IT Space működésében előforduló kézi beavatkozások egyértelműen rávilágítottak arra, hogy a digitális munkafolyamatok automatizálása nem csupán a hatékonyságot emeli, hanem a biztonságot és a minőségbiztosítást is megerősíti.
3. **Az IT és a felhasználók közti kommunikáció fejlesztése elmaradhatatlan.** Az eddigi projektek rámutattak, hogy a siker három alapvető összetevőből áll: a proaktív tájékoztatásból, a célzott edukációból és a végfelhasználókkal ápolt közvetlen együttműködésből.

## 5.5. Záró gondolatok

A Hatvani Bosch informatikai részlegének működése remek példát szolgáltat arra, hogy egy globális vállalatnál a helyi IT-csapat miként járulhat hozzá a szervezet átfogó fejlődéséhez. A dolgozatban bemutatott projektek, a hálózatfejlesztéstől a Windows 11-re történő átálláson át

a ServiceNow-integrációig, mind azt támasztják alá, hogy a technikai tudás, a folyamatmenedzsment és az emberi együttműködés szorosan összefonódva vezet a sikerhez.

Az informatikai fejlődés a Boschnél nem csak egy technológiai kérdés, hanem egy stratégiai eszköz is, amely a versenyképesség és a megbízhatóság megőrzését szolgálja  A Hatvani telephely példája rávilágít arra, hogy a folyamatos fejlesztés, az innováció és a kooperáció együttesen nem csupán a gyártási és vállalati folyamatok kiszolgálásához járulnak hozzá, hanem aktívan alakítják, formálják azokat.

# 6. Felhasznált szakirodalmak


Bagmet, K., Krykavskyy, Y., & Melnyk, O. (2023). Parametric assessment of the technological and infrastructure state of enterprises according to Industry 4.0. Management Science Letters, 13(4), 1231–1245.

Bichler, M., & Bhattacharya, S. (2011). IT Service Management and IT Automation. Information Systems Management Journal, 28(2), 85–92.

Chauhan, R. (2025). Automated Security Configuration Management for Enterprise Networking Products. International Journal of Network Security, 19(1), 45–58.

Elhefnawi, A. (2013). ITIL Implementation in a Major Arabian Gulf Company: Approach and Challenges. Journal of Information Technology Case and Application Research, 15(3), 1–10.

Gray, P. (2006). The Challenges of ITIL Implementations. Information Systems Management, 23(4), 87–95.

Krishnan, S., & Ravindran, A. (2017). IT Service Management Automation and its Impact on the IT Industry. International Journal of Computer Applications, 165(3), 12–18.

Panetto, H., Iung, B., & Ivanov, D. (2019). Challenges for the cyber-physical manufacturing enterprises of the future. Annual Reviews in Control, 47, 200–213.

Shastri, D., & Thampi, G. (2021). Automation of IT Service Management Processes. International Journal of Advanced Computer Science and Applications, 12(10), 55–63.

Vicente, R., & Gama, N. (2013). The Value of ITIL in Enterprise Architecture. Procedia Computer Science, 19, 402–409.

Zhao, L., & Rao, H. (2017). A CPS-based intelligence-awareness platform for IT service management. Journal of Industrial Information Integration, 8, 45–56.

Basinya, E. (2018). An automated system of network and system administration of Windows and Linux family operating systems. Science Bulletin of the Novosibirsk State Technical University, 4, 47–58.

Clark, P., Lavin, T. E., Irvine, C., & Shifflett, D. (2009). DNS and Multilevel Secure Networks Architectures and Recommendations. Monterey Security Architecture Reports.

DePriest, M. (1997). Network security considerations in TCP/IP-based manufacturing automation. ISA Transactions, 36, 37–48.

Gangane, S., & Kakade, V. (2015). Base of the Networking Protocol – TCP/IP Its Design and Security Aspects. International Journal of Innovative Research in Computer and Communication Engineering, 3(4), 3712–3718.

Guluzade, D. (2024). Neglecting the fundamentals: How focus on web apps and frameworks leaves gaps in network security. International Journal of Innovative Technologies in Economy, 9(30), 102–112.

Laughter, S., & Williams, R. (2006). An ethernet/IP security review with intrusion detection applications. SCADA and Automation Systems Journal, 18(2), 145–156.

Shabalin, A. M., & Kaliberda, E. (2017). The organization of arrangements set to ensure enterprise IPv6 network secure work by modern switching equipment tools. Dynamics of Systems, Mechanisms and Machines, 1–8.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.

Kharlamov, A., & Parry, G. (2021). The impact of AI on IT service management: A process-level perspective. Information Systems Frontiers, 23(6), 1395–1412.

Lee, J., Bagheri, B., & Kao, H. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18–23.

**MATE Szervezeti és Működési Szabályzat**
**III. Hallgatói Követelményrendszer**
**III.1. Tanulmányi és Vizsgaszabályzat**
**6.13. sz. függeléke: A MATE egységes szakdolgozat / diplomadolgozat / záródolgozat / portfólió készítési útmutatója**
**4.2. sz. melléklete: Nyilatkozat a záródolgozat/szakdolgozat/diplomadolgozat/portfólió nyilvános hozzáféréséről és eredetiségéről (módosítva: 2025. október 16.)**

**NYILATKOZAT**

**a záródolgozat/szakdolgozat/diplomadolgozat/portfólió[1] nyilvános hozzáféréséről és eredetiségéről**

| | |
|---|---|
| A hallgató neve: | _Gubis Dávid_____ |
| A Hallgató Neptun kódja: | _M4I786_____ |
| A dolgozat címe: | _ Vállalati informatikai problémák elemzése és megoldási javaslatok megfogalmazása a Hatvani Bosch vállalat példáján keresztül _____ |
| A megjelenés éve: | _2025_____ |
| A konzulens intézetének neve: | _ Vidékfejlesztés és Fenntartható Gazdaság Intézet _____ |
| A konzulens tanszékének a neve: | _ Vidékfejlesztés és Fenntartható Gazdaság Intézet _____ |

Kijelentem, hogy az általam benyújtott záródolgozat/szakdolgozat/diplomadolgozat/portfólió[2] 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__ év _November_ hó _2._ nap

Gubis Dávid
Hallgató aláírása

a

# NYILATKOZAT

Gubis Dávid (M4I786_) konzulenseként nyilatkozom arról, hogy a záródolgozatot/szakdolgozatot/diplomadolgozatot/portfóliót[1] 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**[2].

A dolgozat állam- vagy szolgálati titkot tartalmaz: igen nem*[3]

Kelt: 2025. 11. 05.

belső konzulens

[1] A megfelelő dolgozattípus meghagyása mellett a többi típus törlendő.
[2] A megfelelő aláhúzandó.
[3] A megfelelő aláhúzandó.

*(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. 2.

.....  .....

**Hallgató aláírása**  **Konzulens/Témavezető aláírása**