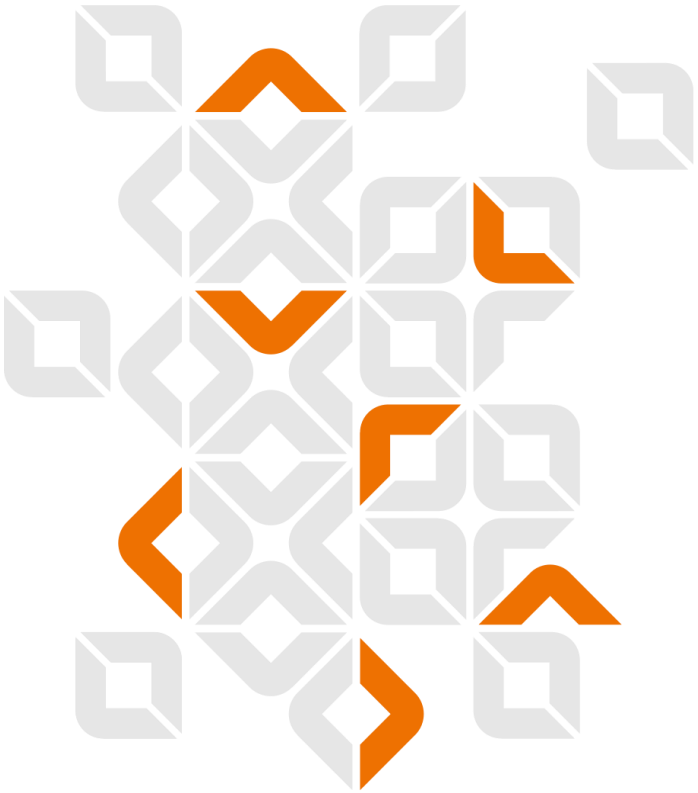
Az IT és az OT viszonyrendszere, a konvergencia humán és adminisztratív aspektusai



Készítette: Kocsis Tamás

Kiadás dátuma: 2022.11.22

Dokumentum verzió: 1.0

SECURITY TESTING LABORATORY
MAKING THE WORLD SAFER

Tartalom

Bevezető

A digitális transzformáció korát éljük. A digitális technológiák fejlődése átalakítja mindennapjainkat, jelentős változásokat előidézve a gazdasági és a magánéletben. Ez az átalakulás azonban nem csak technológiai fejlődést jelent egy vállalat életében, nem csak a lehető legtöbb vállalati tevékenység és folyamat digitális alapokra helyezését jelenti, hanem olyan szervezeti változásokat, amelyek nyitottá, befogadóvá és kezdeményezővé teszik a vállalatot az innovációra. A kialakult innovatív szemlélet legnagyobb jelentősége, hogy a vállalat a régebbi technológiák újra értelmezésével, a modern technológiák alkalmazásával és fejlesztésével folyamatosan képes növelni teljesítőképességét, ezáltal a digitális transzformáció a gazdasági és üzleti élet hajtóerejévé válik.

Az ipari és termelési környezetek digitális transzformációja olyan korszakváltást jelent, amely során a korábbi analóg rendszerek és folyamataik digitalizálásra kerülnek. Mind minden fejlődés, ez a változás sem járhat konfliktusok nélkül, és bár a korábbi paradigmák még jó ideig velünk maradnak, megjelentek az olyan új koncepciók, mint például az Ipar 4.0, adatvezérelt gyártás vagy a virtuális gyárak paradigmái, amelyek kikényszerítik a konfliktusok feloldását és a paradigmaváltást.

Az új koncepciók nagyon jelentősen támaszkodnak az információtechnológiai rendszerekre ezért a legnagyobb konfliktushelyzet az IT és az OT területek integrálódásából, konvergenciájából adódik. Az IT-OT konvergencia számos kihívás elé állítja a vállalatokat, mert a velünk élő régi paradigmák elválasztják és megosztják a szakembereket és szakterületeket. Az informatikai és a termelés- vagy folyamatirányítási szakemberek, illetve az egyes szakterületek eltérő evolúciós folyamatok mentén fejlődtek, más értékrendet és preferenciát hordoznak, ezért az IT/OT konvergencia nem csupán a technológiák, hanem a szakemberek és a szervezeti egységek szükségszerű átalakulását és integrációját is jelenti.

Az IT és OT összekapcsolódását és a területek együttműködését megnehezíti, hogy a területek szakemberei között jelentős feszültség tapasztalható. A digitális transzformáció konfliktushelyzeteket hoz a felszínre, amelyek feloldásához a területeknek jobban meg kellene ismernie egymást, ezért jelen tanulmány az informatikai terület szakemberei számára igyekszik humán és adminisztratív szempontból bemutatni az OT világát, szereplőit és a terület működési szempontjait, technológiai és kiberbiztonsági vonatkozásait.

Az ipari rendszerek legfőbb gyengeségének az elavult, jellemzően biztonsági funkciókat nem megvalósító kommunikációs protokollokat, az elavult és sérülékeny operációs rendszereket, vagy a hagyományos IT-ban már elterjedt biztonsági alrendszerek hiányát tekintik, amelyeket a digitális transzformáció beemel az egyébként már eleve sérülékeny informatikai környezetekbe, azonban a digitális világban nem a technológia, hanem az ember és a felhasználó sebezhetősége jelenti a legmagasabb kockázatot. A digitális transzformáció nem szünteti meg a területek saját sérülékenységeit vagy gyengeségeit, a digitalizációval létrejött konvergens struktúra mindkét terület sérülékenységeit hordozza, és az együttes kitettség súlyosan fenyegeti az összekapcsolt rendszerek és az adatok sértetlenségét, bizalmasságát és rendelkezésre állását. **Az IT és az OT terület saját kockázatai a digitális transzformáció hatására összeadódnak, sőt, a konvergencia kiberbiztonsági szempontból új kockázatokat is létrehoz, az egymásra utaltságban és az együttműködésben rejlő kockázatokat.**

A humán és adminisztratív aspektusok vizsgálatára jó okot adhatnak az orosz-ukrán konfliktus során tapasztalható kibertámadások, láthatóan mindkét fél előszeretettel választ ki célpontnak valamilyen irányitástechnikai vagy vezérlési rendszert, vagy egyéb kritikus infrastruktúraelemet[1]. A korábbi 2015-ös konfliktus során is tapasztalható volt a kritikus infrastruktúrák támadása, a legismertebb incidens az ukrán energiaszolgáltatást érte, az elosztórendszer támadása miatt több mint hatvan alállomás esett ki és 230 ezer lakos maradt áram nélkül.

Jelen tanulmány az IT és az OT területek különbségein és egyezőségein alapulva törekszik a termelési, ipari vagy egyéb üzemi infrastruktúrák jellemzőinek ábrázolására. A digitális transzformáció által felszínre hozott konfliktusok a meg nem értettségen alapulnak, így, ha területek képviselői jobban megismerik egymást és a preferenciákat, az IT/OT konvergencia kialakítása feszültségmentesebb és hatékonyabb folyamattá válik. A tanulmány szeretné bemutatni az OT területet az IT és IT biztonsági szakértők részére és megpróbálja megismertetni a terület jellegzetességeit azokkal, akik esetleg az OT biztonság felé szeretnének specializálódni.

Az IT és OT környezetek legfontosabb különbségei

Jelen tanulmány nem vállalkozhat arra, hogy a területek közötti összes eltérést elemezze, azonban a legfontosabb eltéréseket igyekszik számba venni annak érdekében, hogy a későbbiekben a humán, az adminisztratív és a technológiai, valamint a kiberbiztonsági különbségeket be tudja mutatni.

Szempont	Information Technology (OT)	Operational Technology (OT)
Cél, küldetés	A szervezet technológiai frontend és backend információs rendszerei. Feladatuk az üzleti folyamatok működtetése, az üzleti célok teljesítése.	A szervezet üzemi informatikai háttérrendszerei. Feladatuk a termelés és gyártás informatikai környezetének, valamint a termelési folyamatoknak a működtetése és felügyelete.
Prioritások	Az adatok és rendszerek bizalmassága, sértetlensége és rendelkezésre állása (CIA-modell).	Az üzembiztonság (*safety*), folyamatfolytonosság (rendelkezésre állás), folyamat- és adatintegritás, bizalmasság (SAIC-modell).
Összetevők, komponensek	Szerverek, munkaállomások, adattárak, felhő, biztonsági eszközök, mobileszközök, webalkalmazások, hálózati eszközök.	PLC/DCS, SCADA, adatgyűjtők, szenzorok, motorok és egyéb terepi eszközök, protokollkonverterek, gyártásirányítók (MES).
Életciklus	3-5 éves életciklus, folyamatos törekvés a modernizálásra, fejlesztésre (*„piszkáld, hogy működjön!"*).	10-25 éves életciklus, csak a feltétlen szükséges változások (*„ne piszkáld és akkor működik!"*).
Működés	Eredetileg is együttműködő, összekapcsolt alkalmazások, rendszerek és hálózatok összessége.	Eredetileg szigetrendszerű, önálló működés, nem volt cél a rendszerek és eszközök hálózati összekapcsolása.

[1] *https://securityaffairs.co/wordpress/129009/cyber-warfare-2/russia-ukraine-critical-infrastructure-attacks.html*

Biztonsági koncepció	„*Data first*", adatközpontú szemlélet, a biztonság e köré szerveződik.	„*Process first*", a biztonság a technológiai folyamatok fenntartására és a berendezés, emberélet és környezet megóvására szerveződik.
Személyzet	Rendszergazdák, IT mérnökök, biztonsági mérnökök és felhasználók. „*Fehérgalléros*" munkavállalók.	Operátorok, karbantartók (TMK), terepi mérnökök (*field engineer*), PLC programozók, folyamat- és automatizálási mérnökök. „*Fehér-* és *kékgalléros*" munkavállalók.
Dokumentáció	Üzemviteli, üzemeltetési szempontból jól dokumentált és szabályozott.	Üzemviteli és üzembiztonsági szempontból jól dokumentált és szabályozott
Szabályozás	Információvédelmi szempontból jól szabályozott.	Az információvédelem az egyik legalacsonyabb prioritással jelenik meg, a szabályozás jellemzően nem megvalósított.
Szabályozás	Kiberbiztonsági szempontból jól dokumentált és szabályozott, rendelkezésre állnak a megfelelő biztonsági eszközök, módszerek és jó gyakorlatok	Kiberbiztonsági szempontból fejlődő terület, jellemzően nincs kialakult jó gyakorlat, szabályozás és nem állnak rendelkezésre a szükséges biztonsági eszközök.
Fejlesztési szempont	A fejlesztéskor törekednek a „*security by design*" elv figyelembevételére, a kiberbiztonság beépül a fejlesztési folyamatba.	A fejlesztéskor a funkcionalitás, teljesítmény és a megbízhatóság kap hangsúlyt, a kiberbiztonság megjelenése még várat magára.
Üzemeltetés	Az IT rendszereket a szervezetek maguk üzemeltetik és tartják karban, illetve igénybe vehetnek alvállalkozó (outsource) partnert.	Az OT rendszereket jellemzően a szállítók, integrátorok vagy a gyártók üzemeltetik és tartják karban, akár nagyobb berendezésenként eltérő üzemeltetés és karbantartás is megjelenhet. Szervezet és iparágfüggő.
Elhelyezkedés	Centralizált rendszerek, adatközpontokban, szerverszobákban és irodahelyiségben működnek, könnyű hozzáférés és megközelítés jellemzi.	Iparágtól és alkalmazástól függően szennyezett[2] környezetekben üzemel, terepi körülmények, decentralizált és akár elszigetelt (szigetrendszerű) működés, nagy távolságok áthidalása és a terepi viszonyokat tekintve akár nehéz megközelítés és hozzáférés jellemzi.

Eszközök és technológiák

Az IT (*Information Technology*) mint információtechnológia az adatok (információk) létrehozásáért, mozgásáért, feldolgozásáért, eléréséért és kezeléséért felel. Az eszközöket tekintve az IT területen a kiszolgáló (szerver) hardver és a (felhasználói) munkaállomások

[2] A por vagy a nedvesség csak a kisebbik rossz, de az ipari rendszerek gyakran kémiailag is szennyezett környezetekben üzemelnek, például savnak, lúgnak, olajos szennyezésnek, magas vagy éppen rendkívül alacsony hőmérsékletnek kitéve működnek. Sok esetben pedig a szennyezésmentes környezet jelent nagy kihívást, például a gyógyszergyártás területén belül a tisztaszoba-jellegű terek, ahová a bejutás is meglehetősen nehézkes, akár többszörös fertőtlenítést, csírátlanítást is igényel.

működnek, amelyek kiszolgálói vagy felhasználói szoftverkomponenseket futtatnak. A berendezések közötti kapcsolatokat a hálózati eszközök, switchek, routerek és egyéb kapcsolóberendezések biztosítják. Természetesen az IT-hoz tartozónak lehet tekinteni a különféle egyéb irodatechnikai berendezéseket is mint például a nyomtatók, projektorok és megjelenítők, mobiltelefonok, iratmegsemmisítők, és sok kisebb szervezetek esetben tapasztalható, hogy kis túlzással minden elektromos árammal működő berendezést az IT terület hatáskörébe sorolnak.

Az OT (*Operational Technology*) a fizikai környezet jelenségeinek érzékelésén, a fizikai környezet jeleinek digitálissá alakításáért és a berendezések, eszközök, anyagok mozgásáért és kezeléséért felelős. Míg az IT célja az információ (adat) előállítása, elérhetővé tétele vagy feldolgozása, addig az OT a fizikai környezet változásainak észlelésére, illetve a változások kiváltására és azok felügyeletére szerveződik[3].

Az eszközöket tekintve meglehetősen nehéz egyértelműen meghatározni, hogy mely berendezések és szoftverkörnyezetek sorolhatók az OT területhez, mivel az egyes ágazatok és szektorok más-más eszközöket használhatnak, de szűkebb értelemben ide tartozónak tekintjük az alábbi berendezéseket, eszközöket és szoftverkörnyezeteiket:

- Programozható logikai kontrollerek (PLC)
- Elosztott vezérlési rendszerek (DCS)
- Ember-gép interfészek (HMI)
- (folyamat, eszköz) felügyeleti és adatgyűjtő rendszerek (SCADA)
- Termelésirányító rendszerek (MES)
- Különféle védelmi és automatika rendszerek (villamos védelem, rendszer és készülékautomatika, logikai retesz stb)
- Programozói szoftverkörnyezetek és platformok
- Kezelői és felügyeleti, programozói szoftverek
- Szenzorok, műszerek, érzékelők, motorikus berendezések, környezetszabályozók és más fizikai, terepi berendezések, stb.
- Kamerák, épületautomatika, fizikai biztonsági rendszerek, stb.

Már csak a terminológia miatt is nehéz meghatározni az OT területhez tartozó eszközöket, berendezéseket vagy szoftvereket. A hazai terminológiában elterjedt ipari informatika megnevezés korábban jól alkalmazható volt, hiszen minden olyan informatikai eszközre és berendezésre kiterjedt, amelyet valamely ipari tevékenység során használtak fel, azonban ez mára túlhaladottá vált, nehezen értelmezhető például egy épületautomatizálási környezetben, holott komponenseit tekintve (például PLC vezérlés) akár ugyanazon, vagy nagyon hasonló eszközöket használ fel.

---

[3] A SeConSys ajánlott definíciója szerint az OT „Olyan hardver, szoftver, hálózati eszközök/rendszerek, amelyek az ipari berendezések, eszközök, folyamatok és események közvetlen megfigyelése és/vagy felügyelete révén változást észlelnek vagy okoznak azokban" Forrás: https://seconsys.eu/wp-content/uploads/2022/03/SeConSys_online_kezikonyv_2022_FINAL_22-03-03.pdf (16. melléklet)

Korábban az ipari vezérlési rendszerek (*Industrial Control System*, ICS) megnevezés egyértelműbben lehatárolt jelentést hordozott, például a 2015 májusában kiadott NIST SP 800-82 rev2 „*Guide to Industrial Control Systems (ICS) Security*" jellemzően csak az ipari vezérlési és felügyeleti eszközök kiberbiztonságával foglalkozott és egyéb vezérlési rendszerek esetében (például kamerás megfigyelőrendszerek, épületautomatizálási rendszerek, tűzjelző és egyéb vészeseti rendszerek, stb) annyi kijelentéssel élt, hogy azok az ipari vezérlési rendszerekhez hasonló képességekkel és jellemzőkkel bírnak, így a megfogalmazott javaslatok és kontrollok referenciaként használhatóak ezeknek a rendszereknek a biztonságosabbá tételéhez. A 2022 áprilisában kiadott rev3 változat[4] azonban korábbi határokat jelentősen felpuhította és a dokumentumtervezet már a „*Guide to Operational Technology (OT) Security*" címet kapta, ezzel együtt pedig a hatóköre is sokkal szélesebbé vált. Külön érdekesség, hogy az Internet of Things (IoT) is megjelenik a dokumentumban, amely az OT területhez tartozónak tekinti az ipari IoT (IIoT) eszközöket – ezzel pontot téve a régi vitára, miszerint az IoT tulajdonképpen nem OT, hanem annak csak „*kistestvére*". A megfogalmazás szerint minden olyan berendezést az OT területhez sorol, amely a fizikai környezettel kölcsönhatásban van, vagy ezeket az eszközöket felügyeli, programozza, menedzseli, kapcsolódásukat, adatcseréjüket és együttműködésüket lehetővé teszi. Az OT berendezések tehát az eszközök, folyamatok és események megfigyelésével és/vagy vezérlésével érzékelik a változásokat, közvetlenül vagy közvetetten változást okoznak az eszközökben, folyamatokban és a fizikai környezetben.

Az Information Technology és az Operational Technology területek nevében szerepel a „*technológia*" kifejezés, azaz céljukat technológiai eszközök és berendezések használatával valósítják meg. A közös pont ebben az esetben a technológia, és bár ez nem csak névleges egyezés, de korántsem jelenti azt, hogy ugyanazokat a megoldásokat és ugyanúgy használják.

Az OT berendezései a terület specifikus elvárásainak megfelelő, az IT-ból akár ismerős, de azoktól akár jelentősebben eltérő technológiák felhasználásával működnek. A vezérlők eszközök operációs rendszere lehet valamilyen egyedi operációs rendszer, de akár ismertebb és testreszabott Linux disztribúció, vagy egyéb „*UNIX-szerű*" megoldás, de lehet akár Windows is (például ilyen a Beckhoff legtöbb PLC eszköze). Fontos azonban különbséget tenni a megoldások között. Valóban léteznek olyan eszközök, amelyek az IT-ból ismert valamely Linux disztribúció kisebb-nagyobb átalakításából származó operációs rendszert futtatják, azonban még mindig sokkal jellemzőbbek a különféle valósidejű (*Real-time OS*, RTOS) operációs rendszerek és firmwarek. Ezekre az RTOS rendszerekre ráakasztható a „*UNIX-like*" címke, hiszen valamikor valamilyen UNIX-szerű ősből fejlődtek ki, de semmiképpen nem lehet azt mondani, hogy ugyanaz a Linux vagy UNIX lenne, amely az IT eszközökön működik. Talán a két legismertebb ilyen operációs rendszer a QNX[5] és a VxWorks. A QNX első változata 1982-ben jelent meg, és 1990-ben jelentősen átdolgozva vált az egyik legismertebb mikrokernel-alapú és „*UNIX-szerű*" RTOS szakrendszerré. A VxWorks első változata még 1987-ben jelent meg és rendszer megbízhatóságát talán az jelzi a legjobban, hogy a Curiosity Mars rover landolását a VxWorks vezérelte. A különféle beágyazott rendszerek operációs rendszerei esetében mára már megtalálhatók az IT világból ismert megoldások specializált változatai, például *Windows Embedded* verziók vagy valamely Linux disztribúció beágyazott változata is.

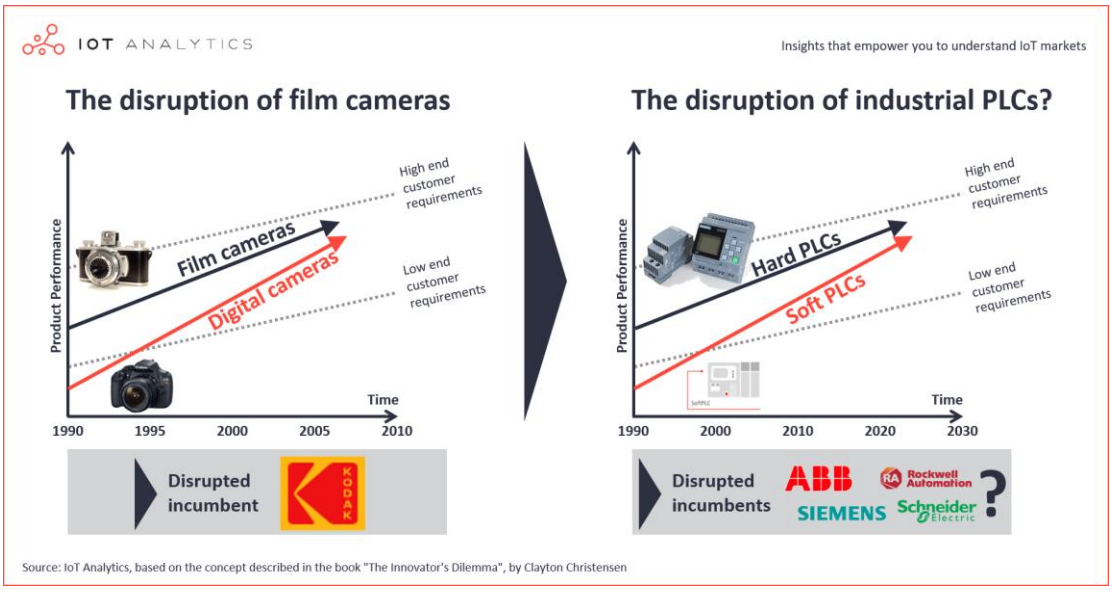
---

[4] *https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft*

[5] *Real Time Operating System, RTOS*

Az alkalmazási rétegben több, az IT területről már jól ismert technológia felhasználása köszönhet vissza. Az ismertebb adatbáziskiszolgálók (például PostgreSQL, MSSQL, MySQL, MongoDB, InfluxDB, Oracle, Elastic vagy egyéb, „*noSQL*" komponensek) ott működnek a különféle adatgyűjtő rendszerekben, a webes felületeket sok esetben az IT világban is előszeretettel használt Apache vagy Nginx webszerverek módosított változatai szolgálják ki. Egy termelésirányítási rendszer (MES) durván leegyszerűsítve a vállalatirányítási rendszer (ERP) „iparosított" változata, amely építőelemei között megtalálhatóak lehetnek a már jól ismert IT technológiák. Azonban nem lehet azt állítani, hogy a MES nem különbözik jelentősen a hagyományos IT alkalmazásoktól. A MES kiegészülve a vezérlési, irányítási vagy szabályzási képességgel, a termelés telemetrikus adataival, batch kontrollal és batch rekordokkal egy új és az OT számára kiemelten fontos konvergens technológiát jelent, amelyet az IT és az OT közösen hoz létre. A modern DCS rendszerek esetében is megjelenhetnek a klasszikus IT technológiák implementációi, például a virtualizáció vagy akár egy Active Directory címtár felhasználásával, amely a DCS-től már elválaszthatatlan, mert a DCS hitelesítési és jogosultságkezelési alrendszerét biztosítja. Azonban a DCS-ben ott vannak a vezérlő kontrollerek, amelyek valamilyen valósídejű operációs rendszert futtatnak, ezért ha az egész ökoszisztémát nézzük, megint csak egy új, konvergens technológia jelenik meg, amelyet az IT és az OT közösen hoz létre.

Az utóbbi években a hardverfüggetlenség és a virtualizációs törekvések elérték a vezérlés- és irányítástechnikai rendszereket is és egyre nagyobb teret kapnak a különféle szoftver-alapú (*software defined*) megoldások. A szoftveres PLC vagy DCS vezérlők elterjedése hardverfüggetlenné teheti a korábban szinte csak speciális és dedikált hardverrel működő megoldásokat, költséghatékonyabb, skálázhatóbb és gyorsabban kiépülő infrastruktúrákat létrehozva. A szoftver-alapú vezérlés- és irányítástechnika együtt jár a virtualizáció térnyerésével, hiszen a szoftveres vezérlési rendszerek akár virtualizált eszközökön is üzemelhetnek, még inkább elszakadva a korábban bebetonozott és megkerülhetetlen hardveres környezetektől. Ezek a változások nagymértékben szektorfüggőek, egy termelési rendszerekben sokkal inkább megvalósíthatóak, mint például egy nukleáris, vagy egyéb erőművi infrastruktúrában.



Forrás: https://iot-analytics.com/soft-plc-industrial-innovators-dilemma/

Ezt az óriási technológiai változást hasonlítani lehet ahhoz, amikor a hagyományos (analóg) fényképezőket felváltotta a digitális kamera, így a jelenséget (a fejlődést) a nagy gyártók oldaláról akár már diszruptívnak is lehet tekinteni.

Ezek a példák talán rámutatnak arra, hogy az IT és az OT terület az eltérések ellenére bizonyos tekintetben egyre közelebb kerül egymáshoz, így az igazi különbséget nem a felhasznált technológia, hanem a technológia felhasználásának célja, módja, illetve az azt meghatározó elvárások, megfelelőségek és preferenciák jelentik.

Szemlélet, kiberbiztonság és preferenciák

Bármennyire is közeledjen egymáshoz az IT és az OT terület hardver vagy szoftverkörnyezete, a szemléletbéli különbségek sokkal nehezebben tudnak feloldódni. Az informatika a „*data first*" elven működik, azaz elsődleges értéknek az adatot tekinti. Az IT kiberbiztonsága is ennek megfelelően szerveződik, az OT esetében azonban nem az adat, hanem maga a (gyártási vagy irányítási) folyamat *egésze* képviseli az értéket („*process first*"). E szemlélet olyan preferencia különbségeket határoz meg, amelyeket részletesebben szükséges bemutatni.

A nemzetközi biztonsági ajánlások és szabványok a területek összehasonlításán és az eltérések kezelésén alapulnak, például az ipari vezérlőrendszerek (ICS[6]) biztonságossá tételével foglalkozó NIST SP-800-82 ajánlás[7] az IT berendezések és rendszerek biztonságával foglalkozó NIST SP 800-53 ajánláson alapul, annak kiegészítő értelmezéseként és kontrollgyűjteményeként jelenik meg, amely az ipari vezérlőrendszerek és az IT rendszerek közötti eltéréseket és az eltérések kezeléséhez szükséges kiberbiztonsági kontrollokat veszi figyelembe. A kifejezetten ipari automatizálási és vezérlési környezetek kiberbiztonsági kihívásainak kezelésére létrehozott IEC 62443 szabvány[8] elvárásai és kontrolljai is az IT terület kiberbiztonsági elvárásainak és funkcionalitásának területre és igényekre szabott változatai, amelyek a területek közötti eltérések kezelése mellett támogatják a kiberbiztonság megvalósításának, fenntartásának és ellenőrzésének tevékenységét. De említhető akár a szektoriális TISAX szabvány[9] is, amely az autóipari szervezetek információbiztonságával foglalkozik, és amely az általános információbiztonsági irányítási rendszer, az ISO/IEC 27001 kontrolljain alapul.

Az IT biztonsági eszközök, tevékenységek és kontrollok értékével kapcsolatban a kibertámadások növekvő mennyiségét és kárértékét tekintve meglehetősen sok kérdés merülhet fel az utóbbi években.

A CheckPoint Research szerint 2021-ben az előző évhez képest 50%-al növekedett a kibertámadások száma, a negyedik negyedévet tekintve heti 900 támadás érte átlagosan a szervezeteket[10]. A Ponemon Institute és az IBM „*Cost of a Data Breach Report*" jelentése szerint a

---

[6] *Industrial Control System (ICS). Az ajánlás 3. kiadása (rev 3) már kitágítja a hatókört és nem csak ICS, hanem az OT rendszerekre vonatkozik.*

[7] *https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final - valamint az OT kiberbiztonságára fókuszáló, jelenleg tervezetként elérhető rev3 verzió*

[8] *https://verveindustrial.com/resources/blog/the-ultimate-guide-to-protecting-ot-systems-with-iec-62443/*

[9] *https://www.quality.org/knowledge/securing-the-tisax-label*

[10] *https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/*

sikeres támadások és incidensek miatt bekövetkezett adatszivárgási események átlagos költsége/kárértéke 3,86 millió dollárról 4,24 millió dollárra nőtt 2021-ben, amely az előző évet tekintve 10%-os növekedést, és egyben a valaha mért legmagasabb kárértéket jelenti[11].

Ha az IT biztonsági incidensek és sikeres kibertámadások száma és kárértéke egyre növekszik, akkor miért kellene az OT világában azokat az elveket és módszereket alkalmazni, amelyek láthatóan az IT kiberbiztonságával kapcsolatosan sem vezetnek sikerre?

Jellemzően azonban a sajtó és a statisztikák nem foglalkoznak azokkal a hárított kibertámadásokkal (vagy kibertámadási kísérletekkel), amelyeket a különféle védelmi technológiák, vagy éppen a felkészült biztonsági személyzet együttesen és sikeresen kivédtek. Ezek számosságát legfeljebb becsülni lehet, de aki már látott például tűzfal vagy behatolásvédelmi biztonsági naplót közelebbről, a sok tíz- vagy akár százezres nagyságrendű heti eseményblokkolási bejegyzés alapján könnyen megértheti, hogy milliárdos hárított eseményszámokról beszélhetünk akár csak napi szinten is, és ezekre jut a statisztikákban kiemelt és elemzett sikeres kibertámadások mennyisége. Ez persze nem csökkenti a bekövetkezett események súlyát és kárértékét, azonban árnyalhatja azt a vélekedést, hogy az IT biztonság gyakorlati értéke drasztikusan csökken. Ellenkezőleg, az IT és kiberbiztonság egyre nagyobb hangsúlyt kap nemcsak nemzetközi szinten, de hazánkban is, akár még a középiskolai tananyag részévé is válhat hamarosan[12].

Nem szabad elfelejteni, hogy egy IT védelmi technológia csak annyira tud hatékony lenni, amennyire az adott szervezet (és az üzemeltető humán erőforrás) képes felhasználni a védelmi technológiát. Erre jó példa az amerikai Target Corporation üzletlánc esete[13], akik a legmodernebb (FireEye és Symantec) védelmi technológiákba ruháztak be, ennek ellenére negyvenmillió bankkártya rekordot lopott el tőlük a támadó, mert a védelmi rendszer automatikus blokkolási funkciója nem volt bekapcsolva, az eszközök által jelzett kártékony eseményeket az üzemeltetők figyelmen kívül hagyták, azt feltételezve, hogy téves riasztásokat küld a rendszer. **Hiába van tehát fejlett védelmi technológia bevezetve, ha azt nem hatékonyan használják fel a szervezetek.**

Nem kétséges, hogy az IT biztonság óriási kihívásokkal néz szembe, és az sem tagadható, hogy a támadó és a védekező oldal között egyre szélesebbre nyílik az ollószár, azonban nem szabad elfelejteni, hogy az IT biztonságnak van múltja, kultúrája, technológiája, szabályozási törekvése – és (többnyire) rendelkezésre áll az IT biztonságra szakosodott, speciális kompetenciákkal dolgozó humán erőforrás. Van tehát motiváció, szándék, képesség és erőforrás, ezek azonban legfeljebb csak nyomokban lelhetők fel jelenleg az OT biztonság területén belül.

Ezek alapján talán nem légből kapott azt állítani, hogy ha az OT egyre több, az IT területén már bevált megoldás testreszabott változatát használja fel, akkor az IT biztonság módszerei a terület

---

[11] *https://www.ibm.com/security/data-breach*

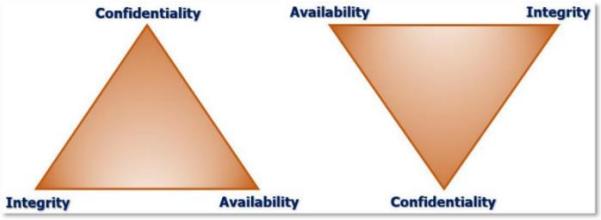
[12] *„Pintér Sándor belügyminiszter már pedzegette, hogy az iskolai tananyagba is bele kellene kerülnie a kiberbiztonság oktatásának" (Források: https://24.hu/tech/2022/06/12/magyar-kiberbiztonsag-kiberhadsereg-kibervedelem, illetve https://telex.hu/belfold/2022/05/18/pinter-sandor-miniszterjelolt-kulturalis-bizottsagi-meghallgatas)*

[13] *https://www.crn.com/news/security/300072031/missed-fireeye-alerts-reportedly-warned-of-security-lapse-at-target.htm*

egyedi sajátosságainak figyelembevételével, az eltérések kezelésével, az eljárások és kontrollok területre szabásával alkalmasak lehetnek az OT biztonság megteremtésére és fenntartására.

Az IT és OT rendszerekkel kapcsolatos biztonsági elvárások azonban jelentősen különböznek, ezért az eltérésekre is figyelemmel kell lenni. A klasszikus értelmezésben az IT biztonság a CIA modellben, a bizalmasság, sértetlenség és rendelkezésre állás teljesülése mentén tud megvalósulni[14], a rendszer vagy az adat állapota akkor tekinthető biztonságosnak, ha az adathoz vagy a rendszerhez csak az arra jogosult fér hozzá, az adatintegritás szavatolt, illetve az adat a kellő pillanatban a rendelkezésre áll. Az OT rendszerek esetében azonban nem csak rendszerről (berendezésről) és adatról van szó, hanem arról a folyamatról is, amelyben az OT berendezés vagy rendszer a fizikai környezet állapotát, változásait vagy jeleit átalakítja digitális jelekké, illetve a digitális jelek alapján befolyásolhatja a fizikai környezet állapotát.

Az OT rendszerek biztonsága a CIA modell fordítottjával jellemezhető, az AIC[15] tehát a rendelkezésre állás, integritás és bizalmasság hármasát jelenti. Az AIC modell teljesülését a berendezésre, rendszerre, adatra és folyamatra is vizsgálni kell ahhoz, hogy megállapítható legyen a kiberbiztonság állapota. Egy berendezés kiberbiztonsági állapota megfelelő lehet, azonban az eszköz működése nem feltétlenül szavatolja, hogy a folyamatbiztonság is megfelelő. Elképzelhető, hogy a telemetrikus adatok bizalmasságát a védelmi intézkedések szavatolják, azonban az adatintegritás sérthető, vagy éppen a berendezés rendelkezésre állása degradálható.



CIA modell vs. AIC modell[16]

CIAS modell (Gartner)[17]

A Gartner (és más szereplők) rámutattak arra, hogy további preferencia is létezik a digitális biztonságban, mégpedig a *Safety*, amely talán leginkább az üzembiztonság kifejezést takarja. A CIAS modellben az üzembiztonság (*Safety*) a preferenciasor végére került, ez azonban határozottan nem illeszthető az OT berendezésekkel és rendszerekkel kapcsolatos elvárásokhoz.

Az OT területen az üzembiztonság (*Safety*) valójában a preferenciasor elejére kerül, így alakul ki a SAIC modell[18]. Az OT rendszerek és berendezések működésével szemben támasztott egyik legfontosabb elvárás, hogy a berendezés vagy rendszer működése ne jelentsen kockázatot a berendezés vagy rendszer épségére és ne jelentsen kockázatot az emberi életre, egészségre és a (szűkebb vagy tágabb) fizikai környezetre. Az üzembiztonság elvárása független az adott

---

[14] *CIA modell: Confidentiality, Integrity, Availability, itthon elterjedt a „BSR" rövidítés, a Bizalmasság, Sértetlenség és Rendelkezésre állás hármasa*

[15] *Availability, Integrity, Confidentiality (AIC) (Forrás: https://www.fireeye.com/blog/executive-perspective/2016/08/developing_a_securit.html)*

[16] *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve, 16.2 ábra (Forrás: https://seconsys.eu/wp-content/uploads/2022/03/SeConSys_online_kezikonyv_2022_FINAL_22-03-03.pdf)*

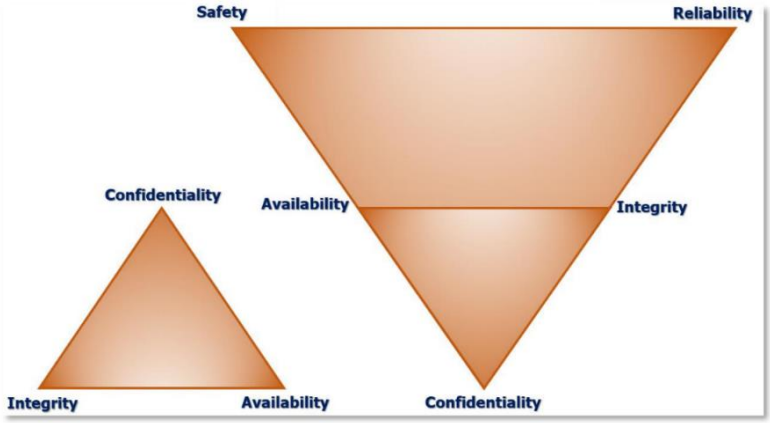
[17] *https://twitter.com/gartner_it/status/1166236190657392640*

[18] *Safety, Availability, Integrity, Confidentiality (SAIC)*

szektortól, éppen úgy igaz egy nukleáris berendezésre, mint egy biomassza erőműre vagy egy sörgyár termelési berendezéseire, legfeljebb abban lehetnek különbségek, hogy az üzembiztonságot milyen szinten várja el megvalósítani az ágazati szabályozás és a törvényi kötelezettség.

Bár az üzembiztonság teljesülése magában foglalja a megbízható és folyamatos működést, azaz a rendszer vagy berendezés (és folyamat) működése az elvárásoknak megfelelően és biztonságosan valósul meg, a megbízhatóság kritériuma néhány szektorban (például energetika) sokkal nagyobb hangsúlyt is kaphat.

A SeConSys, mint a magyar tulajdonú kiberbiztonsági, valamint villamosenergetikai védelmi és irányítástechnika cégek, villamosenergetikai társaságok, továbbá az illetékes állami szervezetek szakembereinek önkéntes, szakmai együttműködésén alapuló szervezet kiadta a kritikus (jellemzően villamosenergetikai) infrastruktúrák ipari felügyeleti rendszereinek kiberbiztonsági képességét fejlesztő „*Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve*" című anyagát, amelyben egy saját megközelítéssel kiemeli a megbízhatóságot az üzembiztonság alól és önálló preferenciaként jeleníti meg.



CIA vs. SR+AIC (SeConSys megközelítés)[19]

A SeConSys megközelítése nem csak a villamosenergetikai rendszerekkel kapcsolatban lehet helytálló (különös tekintettel a villamos védelmi berendezésekre). A gyártói és termelői szektor (*manufacturing*) esetén a termelésfolytonosság igényét maximálisan kiszolgálja a megbízhatóság, így ez a preferencia, illetve az *SR+AIC* preferenciasor a legtöbb szektor esetében megállja a helyét, bár nemzetközi szinten ez a megnevezés még nem terjedt el, illetve a megbízhatóságot sok esetben az üzembiztonság tényezői közé sorolják.

Az IT-OT viszonyrendszerben kiberbiztonsági szempontból tehát a preferencák közti különbség jelenti az egyik nagyobb problémát, mert amíg az IT a rendszerek és adatok bizalmasságának, sértetlenségének és rendelkezésre állására fókuszál, addig OT oldalon a szakemberek az eszközök és rendszerek üzembiztonságának, megbízhatóságának és rendelkezésre állásának fenntartásában érdekeltek, és például a bizalmasság fenntartására már nem jut elegendő humán, anyagi és technikai erőforrás.

---

[19] *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve, 16.3 ábra (Forrás: https://seconsys.eu/wp-content/uploads/2022/03/SeConSys_online_kezikonyv_2022_FINAL_22-03-03.pdf)*

A preferenciák közötti különbségek és az azokból adódó problémák tetten érhetők a különféle berendezések és eszközök fejlesztésével kapcsolatban is.

Egy IT berendezés vagy szoftver fejlesztésekor a gyártó törekedik a biztonságos fejlesztési módszertanok alkalmazására, a biztonsági funkciók kialakítására, illetve a fejlesztésbiztonság megvalósítására. A termék kiberbiztonsága fontos értéktöbbletet jelent, sok esetben az értékesítés nem csak a modern funkcionalitást, hanem a termék kiberbiztonsági képességeit is kiemeli, két azonos képességű termék között akár döntési tényezőt is jelenthet a biztonság. Az IT területen egyre gyakrabban előfordul, hogy egy terméket vagy berendezést annak ellenére sem vásárolnak meg, hogy jóval olcsóbb, mint a versenytársak, a korábbi sérülékenységek, incidensek (és azok lekezelésével kapcsolatos pozitív vagy negatív információk) és általánosságban a megoldás vélt vagy valós biztonsági hiányosságai egyre többször szerepet játszhatnak a döntésben.

Az OT területen lényegesen több egyedi fejlesztéssel lehet találkozni, a házon belüli fejlesztés, illetve a beszállítók, partnerek, integrátorok által különféle komponensekből épített rendszerek sokkal gyakoribbak, mint az IT területen, ezért a biztonságos fejlesztési módszertanok alkalmazása, a fejlesztésbiztonság megvalósítása és általánosságban a termék kiberbiztonsági funkcióinak kialakítása jelentős lemaradással küzdhet. A megrendelői oldalról gyakran hiányoznak azok az elvárások, amelyek teljesítésével a lemaradás behozható lenne, a megrendelők sok esetben nem is várják el a szállítóktól a kiberbiztonság szem előtt tartását. Értékesítési és marketing szempontból a funkcionalitáson, a megbízhatóságon és üzembiztonságon, illetve az alacsonyabb bekerülési költségen van a hangsúly.

OT marketing értékek[20]

Életciklus, üzemi környezet és megbízhatóság

Az eszközök és berendezések életciklusát tekintve megállapítható, hogy míg az IT esetében rövidebb, addig az OT berendezésekkel kapcsolatban jóval hosszabb életciklussal lehet számolni. Az életciklus elemzések és kutatások különbözőképpen definiálják az életciklus fogalmát.

[20] *https://info.comforth.hu/hu/uc-2100 - Itt marketing bár nem fogalmazza meg értéktöbbletként a kiberbiztonságot, a gyártó (Moxa) azonban jelentős erőfeszítéseket tesz a berendezések kiberbiztonságának fejlesztésére.*

Talán a legfrappánsabb megfogalmazás szerint az életciklus folyamat „*az ötlet kipattanásától a termék kihalásáig tart*”[21], így míg egy 5-6 éves IT berendezés elavultnak tekinthető és törekednek az eszköz cseréjére, addig egy 10-25 éves OT eszköz esetén sem feltétlenül merül fel, hogy az eszközt ki kell vonni az üzem alól és gondoskodni kell a cseréjéről.

Az IT a „*működik mert piszkálom*”, az OT pedig a „*működik, mert nem piszkálom*” elvet követi. Az OT rendszerek esetében üzembiztonsági okokból a működtetők törekednek a változások elkerülésére (mind a kiberbiztonsági folyamatokban, mind pedig az eszközcserék területén), ennek a legfőbb oka, hogy a gyártási, termelési vagy egyéb OT folyamatok nagyon szorosan egymásra épülnek és minden változás (beleértve a modernizációt is) fenyegethetik a folyamat épségét, üzembiztonságát és a szervezet üzleti céljainak elérését. Ugyancsak a változtatások elkerülésére sarkalhatja a szakembereket, hogy bizonyos környezetekben (például gyógyszergyártás, nukleáris technológiák, stb.) csak átfogóan tesztelt és/vagy minősített (validált) rendszerek működhetnek. Egy kisebb változás után a teljes rendszert újra kell(ene) tesztelni és/vagy validálni, amely rendkívül idő-, erőforrás- és költségigényes folyamat.

Az IT-ban a változás és a technológia fejlődése kevesebb kockázattal jár, nehezen elképzelhető olyan változás, amely miatt úgy sérülnének az üzleti folyamatok, hogy az az emberi életre és egészségre, vagy a környezet épségére kockázatot jelentene. Az OT esetében akár egy PLC eszköz cseréje is nagyon komoly problémákat vethet fel, például előfordulhat, hogy a PLC-ben futó logika (program) nem fog megfelelően működni, amely hatással lehet a teljes vezérlési vagy egyéb folyamatra is.

Az OT eszközök hosszabb életciklusára az üzleti megtérülésnek is jelentős hatása van. Egy üzem vagy akárcsak egyetlen gépsor létesítése, bevezetése óriási költségekkel jár, több tíz- vagy százmillió forintnyi beruházásnak kell megtérülnie, ez pedig nem tud megvalósulni az IT-ban megszokott és általánosan számolt 3-5 év alatt. A rendszernek „ki kell termelnie” a bekerülési költségét és az üzleti hasznot, tehát a szervezetek abban érdekeltek, hogy a megbízható és folyamatosan termelő berendezés minél tovább működésben maradjon.

Arról azonban szó sincs, hogy az OT terület nem innovatív. A folyamat- és gyártásautomatizáció óriási fejlődésen ment keresztül az elmúlt néhány évben. Az Ipar 4.0 (és már 5.0) ha nem is alapjaiban változtatta meg az OT területet, de olyan változásokat indikált, amelyek a termelési hatékonyság növelésével és az adatvezérelt gyártással kapcsolatban felér egy közepesebb méretű ipari forradalommal, az *Internet of Things* (IoT) megjelenése pedig a korábbiakhoz képest is hihetetlen mértékben tágította ki az OT terület határait.

Az innováció mindig is az ipar egyik legfontosabb mozgatórugója volt, talán nem véletlen, hogy a legelső életciklus-jellegű kutatás is az autóiparhoz köthető. 1922-ben Raymond B. Prescott az 1900 és 1920 közötti időszak autógyártási adatait vizsgálva állapította meg a termékek piaci viselkedésével kapcsolatban, hogy a termékek az idő előrehaladtával különféle fázisokon mennek keresztül. A fázisokat és a fejlődést grafikonon ábrázolta, amely “S” alakja nagyban hasonlít a későbbi életgörbe ábrákhoz. Az OT tehát nagyon is innovatív, azonban sokkal óvatosabb, mint az IT terület, mert az üzembiztonsági és termelésfolytonossági elvárásokat

[21] *(Forrás: Életciklus-elemzés, életciklus hatásértékelés, Tóthné dr. Szita Klára, Miskolci Egyetem Gazdaságtudományi kar, 2008)*

tekintve minden fejlesztés és eszközcsere az IT-ban megszokottnál magasabb kockázatokat hordoz.

Az OT területen tapasztalható óvatosság másik oka, hogy míg az IT-ban egy-egy változtatás viszonylag jól modellezhető és tesztelhető, addig az OT esetében erre sokkal kevesebb lehetőség van. Egy már működő, termelő gyártósor vagy egyéb, összetett gépi berendezés esetén a komponensek modernizációjához és cseréjéhez jellemzően nem áll rendelkezésre tesztkörnyezet, **a változtatás hatásai az egész berendezésre (és a támogatott folyamat egészére) nehezen vagy egyáltalán nem modellezhetők**.

Az IT már sikeresen megküzdött ezzel a problémával. A virtualizáció megjelenése a vállalati rendszerekben nagymértékben csökkentette az informatika hardverekkel szembeni kitettségét, lehetőséget biztosít a szoftver előtérbe helyezésének, illetve a virtualizációs környezetekben a tesztelés is egyszerűbben megvalósítható.

A hardverhez kötöttség (mint blokkoló jelenség) feloldásával az OT már régóta próbálkozik. A legkorábbi példaként a különféle PLC emulátorokat lehet említeni, ahol a programozó emulált környezetben tesztelhette a programját. A fejlődés mára már eljutott arra a szintre, hogy megjelentek a különféle virtualizált és szoftveres technológiák, például szoftveres PLC eszközök vagy a virtualizált DCS kontrollerek, de ezek alkalmazhatóságát erősen meghatározza az adott ágazat vagy terület, és sok esetben nem jelentenek valós alternatívát. A virtualizált gyártás vagy virtuális gyárak (mint „*Digital Twin*") koncepciója feltételezhetően megoldást fog jelenteni a problémára (néhány ágazatban és területen), azonban az ehhez szükséges technológia még gyermekcipőben jár – legalábbis az IT-ban már évek óta alapfunkcióként tekintett virtualizációhoz képest[22].

Az IT berendezések általában irodai, illetve szerverszobai vagy adatközponti környezetekben működnek, ahol a környezet jellemzően tiszta (nem túl szennyezett), felügyelt és monitorozott, például hőmérséklet vagy páratartalom szenzorok és egyéb környezeti érzékelők segítségével. Az infrastruktúra jól megközelíthető és fizikailag elérhető, a fizikai hozzáférésvédelem ellenőrzött és felügyelt. Az eszközök általános, irodai kialakításúak vagy kifejezetten a szerverszobai vagy adatközponti felhasználásokra tervezettek, a berendezések megbízhatósága átlagosnak mondható. Az elhelyezés és az infrastruktúra szervezés centralizációra törekszik, az adatátvitelt nagysebességű, 100 és 10Gbit/sec közötti hálózati kapcsolatok teszik lehetővé.

Az OT esetében gyakran terepi viszonyok között kell a megbízható és folyamatos működést fenntartani. A terepi környezet sok esetben erősen szennyezett, elektromos zajoktól, elektromágneses zavaroktól, kémiai behatásoktól, erős vibrációtól vagy akár extrém hőmérséklettől terhelt. Az OT berendezések fizikai kialakításának igazodnia kell a felhasználási környezethez, ezeket a megfelelőségeket pedig ágazati, területi előírások, élet- és környezetvédelmi rendeletek és szabványok rögzítik. Egy tűz- és robbanásveszélyes térben más kialakítású és védelmű berendezést szabad csak működtetni, mint egy kémiai szennyezéstől terhelt környezetben, vagy éppen ellenkezőleg, egy szabályozott atmoszférájú, szennyezésmentes tisztatérben, ahol a légköri nyomás, páratartalom és megengedett részecskeszennyezés is nagyon erősen kontrollált.

---

[22] Az is nehezítő tényező, hogy a különféle terepi, fizikai eszközök virtualizációja (például szenzor, motor, szervo, stb) ma még nehezen elképzelhető.

OT terepi viszonyok vs IT adatközponti, szerverszobai környezet[23]

Az OT rendszerek gyakran decentralizáltan működnek, akár sokszáz vagy ezer kilométer távolságban is üzemelhetnek olyan berendezések, bázisállomások, terminálok, amelyek megközelítése a terepi viszonyokat tekintve meglehetősen nehézkes, az eszközök hozzáférhetősége gyakran korlátozott. Ennek megfelelően az adatátviteli kapcsolatok a néhány tíz-száz kbit/sec sebességtől (például URH vagy akár műholdas adatátvitel) kezdve bármilyen lehet, a GPRS vagy LTE kapcsolatoktól a gigabites optikai hálózatig bezárólag[24]. Míg az IT-ra a folyamatos, megbízható és alacsony késleltetésű hálózati kapcsolat jellemző, az OT esetében az adatátvitel késleltetése akár igen magas is lehet, az adatátviteli technológiától, a távolságtól és az adatátvitelt befolyásoló környezeti viszonyoktól függően.

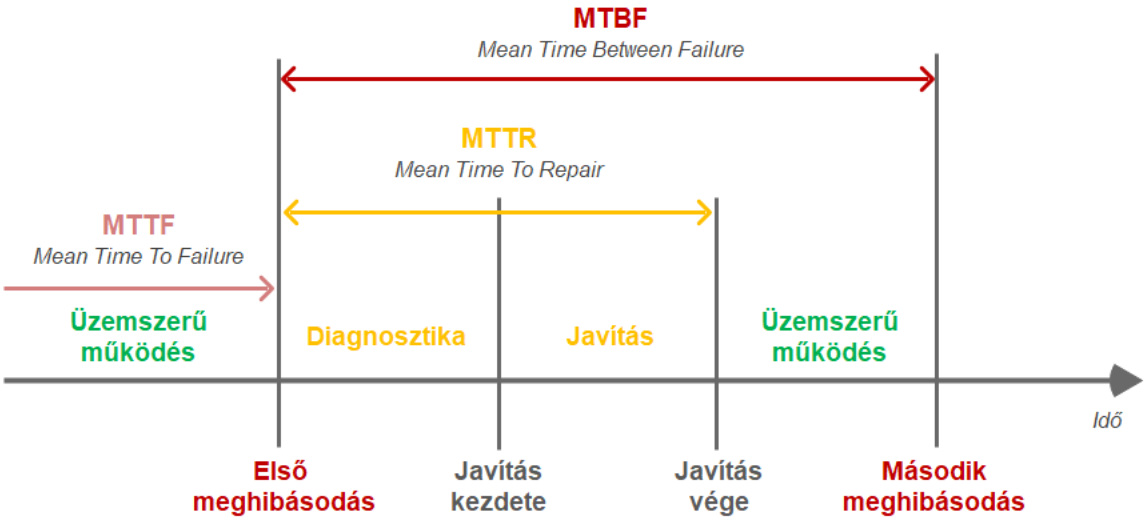
A felhasznált komponensek megbízhatóságának és rendelkezésre állásának szempontjából is jelentős eltérés tapasztalható. A megbízhatóság azt jelenti, hogy az eszköz vagy berendezés az elvárt funkciókat a meghatározott körülmények között a meghatározott ideig képes nyújtani. A rendelkezésre állás ezzel szemben azt jelenti, hogy az eszköz a szükséges időben rendelkezésre áll, azaz amikor szükséges, az eszköz képes a tőle elvárt funkcionalitást biztosítani. A rendelkezésre állás és a megbízhatóság ebből a szempontból kiegészítik egymást és üzembiztonsági szempontból egy működő, üzemi környezetben általában együtt értelmezhetők.

Az eszközök életciklusa és megbízhatósága között szoros kapcsolat van, azonban az életciklus és élettartam meghatározására legalább húszféle számítási módszertant dolgoztak ki az utóbbi évtizedekben, így egy-egy beszerzés előtt meglehetősen nehéz előre tájékozódni. A műszaki eszközök megbízhatóságának és rendelkezésre állásának értékelésére több, általában statisztikai becslésen (és a még kevésbé egzakt jóslaton) alapuló mértéket is meghatározhatnak, ilyenek lehetnek például az MTFF, MTTF, MTBF vagy MTTR értékek.

---

[23] Forrás: https://www.reddit.com/r/PLC/comments/orzc1g/modern_pc_oh_speck_of_dust_got_inside_im_broken/ és https://www.akcp.com/blog/environmental-monitoring-for-data-centers-and-server-rooms/

[24] Érdemes megemlíteni az IoT világ egyre népszerűbb és terjedőben lévő átviteli technológiáit is, mint például a LoRa, Sigfox vagy NB-IoT adatkapcsolatokat.



Megbízhatósági és rendelkezésre állási mértékek, értékek

A *Mean Time to First Failure* (MTFF) vagy *Main Time To Failure* (MTTF) értékekkel ábrázolják a berendezés első meghibásodásáig tartó időszakot. Ezt az értéket a gyártók egyik terület esetében sem szívesen határozzák meg.

A *Mean Time Between Failure* (MTFB) általában két meghibásodási esemény közötti időablakot jelenti, bár értelmezhetik a legelső és a második hibaesemény közötti időtartamnak is. Általában az MTBF értéket határozzák meg a gyártók gyakrabban, azonban mint minden ilyen megbízhatósági mérték, az MTBF is feltételezéseken alapul és gyakran tévesen azonosítják az eszköz élettartamával, holott például egy 2 701 531 órás MTBF értékkel rendelkező eszköz esetén nehezen feltételezhető, hogy az adott készülék 308 évig képes üzemelni.

Az MTBF értéket a gyártók arányként, az adott berendezés egész élettartamára vonatkoztatva határozzák meg, azonban itt már a feltételezés is szerepet játszik, mivel feltételezik, hogy a meghibásodási arány az élettartamon belül közel állandó marad. Ez azonban természetesen nem így van, az eszközök a normál élettartamon belül mutatják a legkisebb és közel állandó meghibásodási arányt, azonban az elhasználódás miatt az eszköz hamarabb is működésképtelenné válhat, mint azt az MTBF érték alapján várnák. Az MBTF tehát a teljes élettartamra vonatkoztatott meghibásodási aránynak tekinthető.

A *Main Time To Repair* (MTTR) érték a karbantartás számára az egyik legfontosabb KPI. A meghibásodott eszköz vagy rendszer javításáig vagy helyreállításig eltelt időt jelenti, amely alatt a hibás vagy nem működő állapotból az eszköz vagy rendszer működő és üzemszerű állapotba kerül. Az MTTR nem a megbízhatósággal, hanem a rendelkezésre állással van szoros kapcsolatban. Minél magasabb az MTTR érték, annál gyengébb a rendelkezésreállás, hiszen az adott eszköz vagy rendszer annál tovább marad a hibás vagy nem üzemszerű állapotban. Ha azonban az MTBF értéke növekszik, akkor azzal a rendelkezésre állás értéke is növekedni fog.

A nagyobb igénybevételhez és a magasabb elvárásokhoz igazodva az OT eszközök és berendezések a terepi környezetekben megbízhatóbban és nagyobb rendelkezésre állás mellett üzemelnek, mert a kialakításukkor maximálisan figyelembe veszik a környezetből és a felhasználás módjából adódó extra terhelést.

	IT switch	OT switch
Eszköz	**Cisco SG300-28 switch[25]**	**EDS-208A-M-ST-T switch[26]**
Üzemi hőmérséklet	0 - 40 °C	-40- 75°C
Üzemi páratartalom	10 - 90 %	5 - 95%
MTBF	179 141 óra (20,4 év)	2 701 531 óra (308,3 év)
Shock	-	IEC 60068-2-27
Vibration	-	IEC 60068-2-6
Freefall	-	IEC 60068-2-31
Hazardous Locations	-	ATEX, Class I Division 2[27]

Példa egy hasonló funkciójú IT és OT eszköz terepi képességeire

Reference number	Continuous hours @ 30 degrees C	Continuous years @ 30 degrees C
BMXP341000	413347	47
BMXP342010	389418	44
BMXP342020	391864	45
BMXP342030	384868	44

Legacy KB System (APS) Data: RESL186926 V1.0, Originally authored by DaSo on 07/11/2007 07/11/2007
Related ranges: Modicon M340

Published on: 7/11/2007 **Last Modified on:** 9/29/2021

MODICON M340 PLC (CPU) MTBF értéke

[25] *https://www.cisco.com/c/en/us/products/collateral/switches/small-business-smart-switches/data_sheet_c78-610061.html*

[26] *https://www.moxa.com/en/products/industrial-network-infrastructure/ethernet-switches/unmanaged-switches/eds-208a-series/eds-208a-m-st-t*

[27] *Olyan környezet, ahol gáz, gőz vagy köd állapotú veszélyes anyagok és a levegő keverékéből álló robbanásveszélyes légkör normál üzem során valószínűleg nem alakul ki (csak egyéb hiba bekövetkezte miatt, például perforálódik egy tartály), de ha mégis előfordul, akkor a robbanásveszély csak rövid ideig áll fenn.*

Storage Temperature (package included)	-40 to 75°C (-40 to 167°F)
Shock	IEC 60068-2-27
Vibration	IEC 60068-2-64
Standards and Certifications	
Safety	EN 62368-1, UL 60950-1
EMC	EN 55032/35, EN 61000-6-2/-6-4
EMI	CISPR 32, FCC Part 15B Class A
EMS	IEC 61000-4-2 ESD: Contact: 4 kV; Air: 8 kV IEC 61000-4-3 RS: 80 MHz to 1 GHz: 10 V/m IEC 61000-4-4 EFT: Power: 2 kV; Signal: 1 kV IEC 61000-4-5 Surge: Power: 1 kV; Signal: 1 kV IEC 61000-4-6 CS: 10 V IEC 61000-4-8 PFMF
RED	EN 300 328 EN 301 893 EN 301 489-1/17/19/52 EN 301 511 EN 301 908-1 EN 303 413 EN 62311
Green Product	RoHS, CRoHS, WEEE
Hazardous Locations	Class I Division 2, ATEX
MTBF	
Time	441,032 hrs (AIG-501-T-US-AZU-LX, AIG-501-T-EU-AZU-LX, AIG-501-T-AP-AZU-LX) 453,637 hrs (AIG-501-T-AZU-LX)

Moxa AIG-500 ipari PC – 50 év MTBF[28]

MTBF Estimates for R1304RPMSHOR

Subassembly (Server in 40C ambient air)	Server Model R1304RPMSHOR MTBF (hours)	FIT (flrs/10^9 hrs)
S1200V3RPM board	371,523	2,692
Power Supply - 450W MiniERPS	967,300	1,034
Cooling Fan (1-fixed fans)	490,000	2,041
Cooling Fan (2-fixed fans)	77,680	12,873
Front Panel board	8,272,282	121
HS Backplane(4x3.5")	935,180	1,069
Totals without motherboard =	**58,300**	**17,138**
Totals with motherboard =	**50,400**	**19,830**

Intel szerver (R1304RPMSHOR) – 5,7 év MTBF[29]

Az OT terület eszközei jellemzően tehát megbízhatóbban és magasabb rendelkezésre állás mellett üzemelnek[30] – olyan környezetekben és terepi viszonyok között, ahol a hagyományos IT eszközök alkalmazása nem javasolt, illetve akár súlyos üzembiztonsági kockázatot jelentene. Természetesen ez azzal is jár, hogy az OT eszközök ára jellemzően jóval magasabb, mint a hagyományos IT berendezéseké, ezzel jelentősen megnövelve a beruházások költségét, amelyet sokkal hosszabb idő alatt tudnak a rendszerek csak „kitermelni", így míg az IT-ban egy 5 éves eszköz esetében már erősen megfontolják az eszköz cseréjét, addig az OT területen egy tizenöt,

---

[28] *https://cdn-cms.azureedge.net/getmedia/1ec7dd5b-86d6-47ef-8f3f-d4a84fd20a84/moxa-aig-500-series-datasheet-v1.0.pdf*

[29] *https://www.intel.com/content/dam/support/us/en/documents/motherboards/server/sb/s1200rpcalculatedmtbfestimatesrev1_0.pdf*

[30] *Persze az IT világában is vannak példák a nagyon régóta működő berendezésekkel kapcsolatban. Például az egyetemi világban néhol még működő DEC Microvax II-höz hasonlóan régi kiszolgálók, vagy akár lehet említeni azokat a városi legendákat, amelyek hőse egy szerverterem sarkában üzemelő ősöreg toronyszerver, amely megsárgult, korszakos portól borított burkolata alatt minden kétséget kizárólag egy Novell NetWare 3.11 halhatatlan szíve dobog. Az ilyen berendezések azonban éles környezetben inkább csak a kivételt erősítik.*

vagy akár húsz éve folyamatosan működő berendezéssel kapcsolatban sem merül fel feltétlenül a csere igénye[31].

A hosszú életciklusok ezzel együtt azt eredményezik, hogy egy idő után az évtizedes vagy akár évtizedek óta üzemelő eszközöknek együtt kellene működnie az újabb beruházásokból származó modern(ebb) berendezésekkel és megjelennek a különféle interoperabilitási, a régi rendszerek és az új rendszerek összekapcsolásából és együttműködéséből származó problémák. Ezeknek a problémáknak a többsége hatással van az egész rendszer egészének kiberbiztonságára, mert egy lánc csak annyira erős, mint annak leggyengébb láncszeme: ha nem vezetnek be védelmi intézkedéseket és kompenzációs kontrollokat, **a rendszer egészének eredő kiberbiztonsága a legalacsonyabb kiberbiztonsági érettséggel rendelkező eszköz kiberbiztonságával lesz egyenlő**.

Szerepkörök, tevékenységek, privilégiumok

Az IT terület esetében alapvetően három jól körül határolható szerepkör létezik, a fejlesztő, a felhasználó és a kiemelt privilégiumú felhasználó. A kiemelt privilégium valamilyen többletjogosultságot jelent, ez takarhat egy „*power user*" szereplőt, aki például a felhasználóhoz képest rendelkezik valamilyen plusz jogosultsággal (például képes a felhasználónál mélyebb szintű beavatkozásra), de általában inkább olyan személyt jelent, aki az adott rendszerben valamilyen adminisztrátori vagy rendszergazdai jogosultsággal rendelkezik. Természetesen a folyamatoktól függően ennél jóval szélesebb körű is lehet egy IT rendszer működtetésében és felhasználásában résztvevő szereplők listája, de jellemzően mindegyik szereplő visszavezethető a három alapvető szerepköri csoportra. A szereplők mindegyike „*fehérgalléros*" munkatársnak tekinthető, akik általánosan irodai környezetben végzik tevékenységeiket.

Az IT esetében általában élesebben elhatárolódik egymástól a fejlesztői, üzemeltetői, támogatói és biztonsági tevékenység. A szerepkörök és tevékenységek szétválasztása az IT biztonság egyik fontos elvárása, ezért a különféle szabályzatok és eljárásrendek (több-kevesebb sikerrel) igyekeznek feloldani az összeférhetetlenségi helyzeteket. Például egy átadott, produktív rendszer időszakos biztonsági felülvizsgálata viszonylag ritkán a fejlesztő vagy az üzemeltető tevékenysége, ahogyan egy rendszerszállító esetében sem javasolt, hogy a bevezetett megoldás biztonsági ellenőrzését a rendszerszállító valósítsa meg. A független ellenőrzés ilyen esetekben képes az összeférhetetlenségi helyzeteket feloldani és hiteles információkkal szolgálhat a rendszer biztonságával kapcsolatban. A nagyobb végfelhasználói szervezetek esetében a fejlesztés és az üzemeltetés is két külön területnek számít[32], a kisebb hazai szervezeteknél azonban az IT oldalon is tapasztalható a két szerepkör keveredése, sok esetben a fejlesztők igyekeznek az általuk fejlesztett rendszereket üzemben és működésben tartani.

Az OT esetben a szerepkörök kevésbé megfoghatók, jóval több esetben lehet találkozni a szerepkörhalmozás jelenségével, és az IT alapvető hármas szerepköre is nehezen értelmezhető a területre.

---

[31] Szektoriális szinten ez eltérő lehet, van ahol akár harminc éve hibamentesen működő berendezésekkel is találkozni lehet. Erre jó példa lehet a mai napig is előszeretettel használt Siemens SIMATIC S5 PLC család, amely 1979-ben jelent meg és a gyártói támogatás csak 2020-ban szűnt meg. (Forrás: Siemens, WayBackMachine)

[32] Az üzemeltetés és a fejlesztés szoros együttműködéséből létrejövő DevOps inkább a szolgáltatásfejlesztés és a különféle felhős és egyéb szoftverszolgáltatások területeire jellemző.

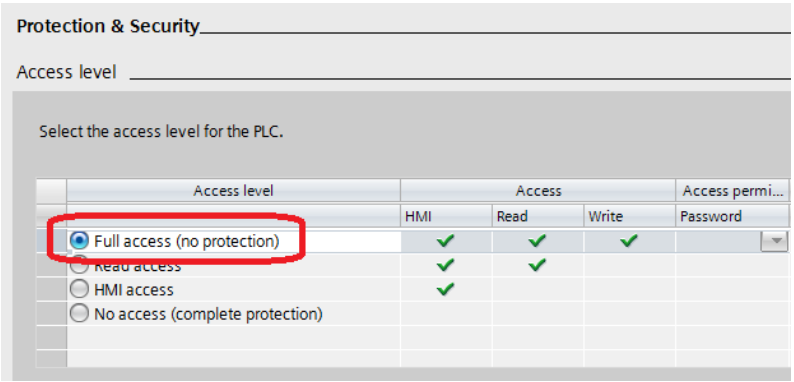
A felhasználói szerepkör az OT esetében gyakorlatilag bármilyen munkakört takarhat, ide tartoznak például a gépekkel és berendezésekkel dolgozó kezelők, a felügyeletet biztosító operátorok vagy akár egy elektrikus is, aki (megfelelő engedélyezési és jóváhagyási eljárások után) a felhasználói felületen keresztül béníthat egy villamos védelmi eszközt, vagy a műszakos szakszemélyzet, akik a visszakapcsolás előtt tesztelik a villamos védelmi funkciókat.

Míg az IT terület arra törekszik, *hogy csak a munkavégzéshez szükséges* és a *lehető legszűkebb* jogosultsággal rendelkezzen a felhasználó, addig az OT esetében erre sokkal kisebb hangsúlyt fektetnek és azt tartják szem előtt, hogy az adott felhasználó *minden olyan* jogosultsággal rendelkezzen, amely *szükséges lehet* a munkája elvégzéséhez. Míg az irodai tevékenységek általában átláthatók és tervezhetők, a terepi körülmények között végzett munka gyakran igényelhet előre nem tervezhető megoldásokat, amelyekhez viszont szükségesek lehetnek többletprivilégiumok. Az OT ezért nem törekszik erős korlátok közé szorítani a jogosultságokat, mivel a folyamatos üzem alatt bármikor bekövetkezhetnek előre nem látható események, amelyek igénylik az azonnali beavatkozásokat. Ha egy operátor hajnali kettőkor nem tud leszabályozni egy folyamatot, csak mert „*elméletileg*" a jelenségnek nem lenne szabad bekövetkeznie és ezért az operátor nem rendelkezik jogosultsággal a folyamat megszakítására, az esemény bekövetkeztekor már nem lesz lehetőség kitölteni a jogosultságigénylő formanyomtatványokat és megigényelni a szükséges privilégiumokat. Ide tartozik az IT biztonság egyik jól ismert kontrollja is, a sikertelen bejelentkezési kísérletek észlelésekor a hozzáférés automatikus letiltása, amelyet az OT berendezések esetében csak nagyon óvatosan szabad csak alkalmazni, mert ugyan a védelem sikeresen hárítana egy nyers erővel történő támadást, azonban a támadás indulhat azzal a céllal is, hogy a kezelőket a támadó a védelem segítségével kizárja a rendszerből, ezáltal ellehetetlenítve a későbbi kezelői beavatkozásokat.

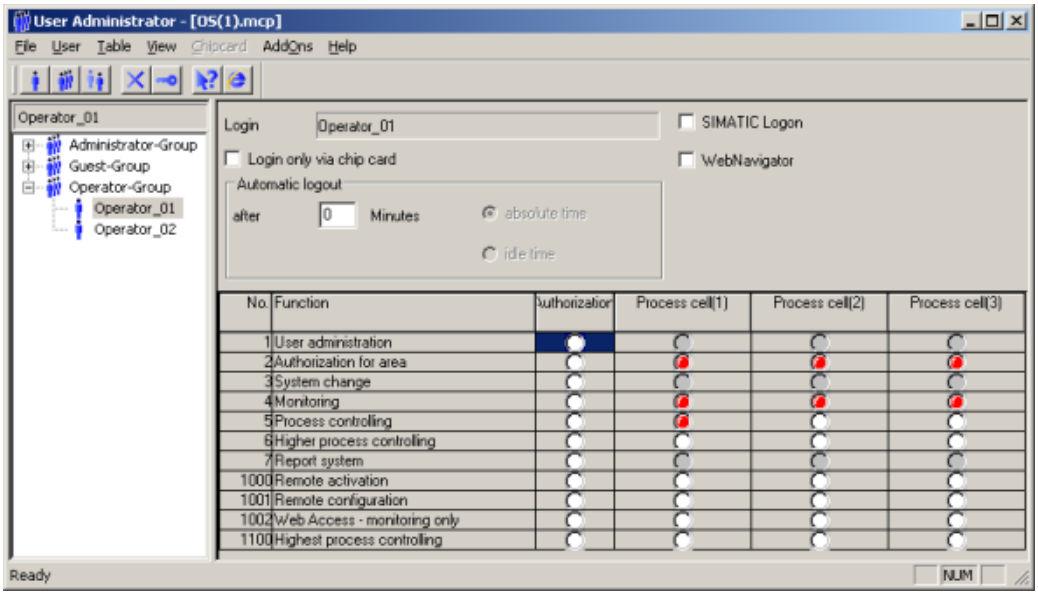
Az irodai munkákkal kapcsolatos álláshirdetésben gyakran találkozhatunk különféle elvárásokkal, amelyek a leendő munkavállaló számítógépfelhasználói képzettségével kapcsolatosak, például elvárás a Windows vagy az Office „felhasználói szintű ismerete" – ugyanakkor egy OT pozíció esetében sokkal nehezebb megfogalmazni, mit is értünk felhasználói ismereten, holott sok esetben a „*kékgalléros*" munkatevékenységekhez is hozzátartozik például a számítógép és a Windows használat. Az OT területen a felhasználói kör alapképzettsége rendkívül széles skálán mozoghat, a „felhasználó" – *mint szerepkör* – kevésbé, vagy nem tipizálható és a képességbéli hiányosságok kezelésére is sokkal nehezebb valamilyen megoldást találni.

Az OT terület felhasználói szerepköre abból a szempontból is eltér az IT-ban megszokottól, hogy az OT felhasználói adott esetben nagyon komolyan bele tudnak avatkozni egy berendezés, rendszer vagy folyamat működésébe. Az IT törekszik arra, hogy a felhasználói és privilégizált felhasználói szerepkörök el legyenek választva egymástól, például egy felhasználó nem kap lokális adminisztrátori jogosultságot a számítógépére (vagy egy kiszolgálóra), azonban az OT esetében ez a szétválasztás nem tud az IT-hoz hasonlóan megvalósulni. Míg az IT-ban nehezen elképzelhető, hogy egy felhasználó leállít és lekapcsol egy kiszolgálót, addig az OT esetében nem ritka, hogy egy kezelő akár egy teljes technológiai sort lekapcsol. Ugyanígy, az IT rendszer esetében egy villanyszerelő nem feltétlenül tud akkora ráhatással lenni egy rendszerre, mint az OT esetében, ahol az ipari villanyszerelők folyamatosan a vezérlőszekrényekben dolgoznak. Az OT szerepköri viszonyrendszere képlékeny és rendkívül nehéz az IT-ban megszokott granuláris jogosultságkezelést megvalósítani.

A kiemelt privilégiumok esetén még nehezebb az összehasonlítás, mert az OT területen a kiemelt privilégium fogalma nehezen értelmezhető. A régebbi berendezések nem is teszik lehetővé kiemelt privilégiumú felhasználók létrehozását, gyakorlatilag egyetlen jogosultsági szint létezik, amely minden funkció elérését lehetővé teszi. A modernebb eszközök már általában tartalmaznak valamilyen felhasználói megkülönböztetést, például csak olvasási, vagy írási és olvasási jogosultsággal rendelkező felhasználói szerepkörök is létrehozhatók. Ebből a szempontból már egy írási-olvasási jogokkal rendelkező hozzáférés is privilégizáltnak számít, hiszen lehetőséget biztosít az eszköz összes funkciójának elérésére és az eszköz konfigurációjának módosítására. A legújabb eszközök már igyekeznek az IT-ban megszokott jogosultságkezelési séma átvételére, és a felhasználói szerepkörök csak bizonyos funkciókhoz férhetnek hozzá, azonban sajnos ezeket a képességeket gyakran nem használják, ha van is felhasználói hitelesítés elvárva, általában ott igyekeznek a legtöbb jogosultságot biztosítani annak érdekében, hogy a lehető legalacsonyabb adminisztrációval a lehető legüzembiztosabb működés legyen megvalósítható.



Egyszerű jogosultságkiosztás



Funkció alapú jogosultságkiosztás

Egy másik megközelítésben a kiemelt privilégium nem feltétlenül jelenti a beavatkozási képesség mélységét. Egy gépkezelő is képes lehet egy berendezés vagy akár egy technológiai sor leállítására, ehhez akár még csak felhasználói jogosultság sem szükséges: elegendő hozzá (például) a berendezés oldalán elhelyezett vészleállító gomb megnyomása. 2021 augusztus 29-én

váratlanul leállt a New York-i metróhálózat egy szakasza és nyolcvan szerelvény rekedt az alagutakban, mert a központi vezérlőben található vészleállítóról hiányzott a biztonsági fedél és véletlenül valaki megnyomta a gombot. Látható tehát, hogy akár privilégizált hozzáférésnek tekinthető maga a fizikai hozzáférés lehetősége is, mert aki képes hozzáférni a vészleállítóhoz (vagy egy PLC szekrényhez, de akár csak egy szabadon hozzáférhető kábelhez vagy csatlakozóhoz), az már bele tud avatkozni a berendezés vagy akár egy teljes technológiai sor működésébe. Mivel a fizikai hozzáférés gyakorlatilag bármilyen beavatkozásra lehetőséget adhat, ezért az ipari vagy üzemi környezetekben igyekeznek a fizikai biztonságra nagyobb hangsúlyt fektetni és például erősebben kontrollálni a fizikai hozzáférés lehetőségeit[33].

Néhány szektorban vagy specifikusabb környezetben a privilégizált hozzáférés nem is a rendszerbe vagy a működésbe való beavatkozási képességhez kapcsolódik. Például egy erőművi rendszerben az operátor vagy kezelő ugyan nem rendelkezik bizonyos jogosultságokkal (például nem tud egy erőművi blokkot lekapcsolni vagy szimulációt futtatni), de a blokk működéséért felelős személy (például blokkmester) már képes ilyen funkciókat is elérni, tehát valamilyen engedélyezési eljárás és folyamat alapján egy szereplő felruházható speciális többletjogosultsággal. Privilégizált hozzáférőnek azonban nem a többletjogosultsággal rendelkező vagy azt időszakosan birtokló felhasználót tekintik, hanem azt a szereplőt, aki ezekkel a jogosultságokkal felruházhat egy másik felhasználót. Például privilégizált felhasználónak tekinthető egy főmérnök, akinek a döntése alapján az irányítástechnika jogosultságkezelési tevékenységével megbízott szereplője hozzárendeli a többletjogosultságot a felhasználóhoz. Ebben a megközelítésben tehát nem a kiemelt (megkülönböztetett) jogosultságot birtokló, vagy a jogosultsági szintet beállító, hanem a jogosultságot odaítélő személyt kell privilégizált felhasználónak tekinteni.

Egy másik példában a karbantartási vagy szerelési tevékenység során szükség lehet a villamos védelmi berendezések kiiktatására (bénítására). A folyamatban az ipari villanyszerelő (például a fizikai hozzáférés birtokában) – *mint végrehajtó* – képes lehet a villamos védelem bénítására, azonban ettől akkor sem válik privilégizált felhasználóvá, ha a bénítás nem fizikailag, hanem esetleg egy IP-képes és menedzselhető eszköz felhasználói felületén bejelentkezve valósul meg[34]. A folyamatban az a személy tekinthető privilégizált felhasználónak, aki engedélyezi és/vagy ellenőrzi a villamos védelem kiiktatását, vagy újra aktiválását. Ezek a példák talán jól szemléltetik, hogy az OT privilégizált felhasználói szerepköre gyakran nem is a végrehajtói oldalon, hanem az adminisztratív, szabályozói vagy éppen az ellenőrzési oldalon jelent (a kiberbiztonság szempontjából is) kiemelt- vagy többletjogosultságot.

Míg az IT-ban élesebben elhatárolódnak egymástól az eszközök vagy rendszerek gyártói, integrátori és üzemeltetési tevékenységei és szerepkörei, addig az OT területen ezek a határok gyakran elmosódnak.

---

[33] *Több-kevesebb sikerrel. Sajnos tudomásul kell venni, hogy bármilyen hatékony és jó egy OT rendszer logikai védelme, a fizikai biztonsági hiányosságok miatt sokkal egyszerűbb és könyebb a logikai védelmet kijátszani. Ez egy olyan alapvető különbség, amely az OT területen sokkal jobban szükségessé teszi a fizikai és logikai védelem egymáshoz igazítását, mint az IT környezetekben.*

[34] *Nagyfeszültség esetén jellemzően kerülik a távoli beavatkozási lehetőséget biztosító védelmi megoldások használatát. A villamos védelem kiiktatása olyan tevékenység, amely nagyon szigorú kontroll alatt áll, hiszen nemcsak a berendezés károsodhat, de az emberi élet és egészség is veszélybe kerülhet.*

Egy gépgyártó az általa tervezett és fejlesztett berendezést leszállítja, üzembe helyezi és a működést folyamatosan támogatja, azaz a fejlesztő, integrátor, üzemeltető és támogató is ugyanazt a partner és gyakran ugyanazokat a személyeket jelenti. Ez akár még a kvázi „*dobozos*" termékek gyártókra is igaz, például az Emerson, Yokogawa, Siemens, Schneider és a piac többi nagy szereplője is megjelenhet egy ügyfélprojektben szállítóként, integrátorként, üzemeltetőként vagy támogatóként. Így előfordulhat olyan folyamat, ahol egy személy négy szerepkörben végez munkát, ezért minden létező jogosultsággal rendelkezik.

Az OT gyakran kényszerül kiegészítő megoldásokkal élni a kiberbiztonsági megfelelőség tekintetében. Sok esetben a terület jellegzetes működése miatt nem lehet az IT biztonságban megszokott és bevett eljárásokat követni, hanem valamiféle kerülőmegoldás alkalmazására, professzionális kifejezéssel elve „*kompenzációs kontroll*" bevezetésére van szükség.

A kompenzációs kontroll lényege, hogy ha nem lehet egy védelmi intézkedést alkalmazni, akkor akár több, különálló intézkedéssel próbálja meg a szervezet a kockázatot csillapítani. A kompenzációs kontrollok közös jellemzője, hogy szinte soha nem annyira hatékonyak (még együttesen sem), mint az az intézkedés, amely kiváltására vagy helyettesítésére születtek, azonban mégis valamilyen választ és csillapítást jelentenek az adott problémára. Például a szerepkörök szétválasztása sok esetben nem megoldható, ha a gyártó, szállító és integrátor, működtető és támogató is ugyanaz a külsős partner. Ebben az esetben a szerepkörhalmozás kockázatára nem lehet egyszerűen jó választ adni, ezért kompenzációs kontrollként erős személybiztonsági eljárásrendet vezet be a szervezet annak érdekében, hogy a szerepkörhalmozás kockázatait csillapítani tudja, illetve műszaki kontrollként bevezeti, hogy a logikai beavatkozások (frissítés, javítás, programletöltés, paraméter vagy konfigurációmódosítás, stb) csak megadott mérnöki állomásokról legyenek megvalósíthatók, ahol viszont minden tevékenységet videószerűen rögzít. A szerepkörök közötti átjárásokat, összeférhetetlenséget és es ezekből adódó visszaélési lehetőségeket a szervezet nem tudja teljesen megszüntetni, azonban kompenzációs kontrollal gondoskodhat arról, hogy humán és műszaki oldalról követhetővé és elszámoltathatóvá tegye a beavatkozásokat.

A kompenzációs kontrollok példája alapján ismét érdemes megerősíteni, hogy az IT biztonság módszerei jól alkalmazhatóak az OT világában, azonban azokat a terület jellegzetességeire kell szabni. A példát tovább elemezve felismerhető, hogy a személybiztonsági eljárásrend működtetése alapvető elvárás bármely érettebb IT biztonsági szabályozási környezetben, míg a logikai tevékenység rögzítése az IT biztonság *Privileged Access Management* (PAM), azaz a kiemelt felhasználók tevékenységének kontrolljának és felügyeletének területéről lehet ismerős, ahol elvárt, hogy a rendszergazdai és adminisztratív jogosultsággal rendelkező felhasználók tevékenysége részletesen rögzítésre kerüljön. A két bevett, IT biztonsági kontroll együttes alkalmazása tehát nem szünteti meg, de elfogadható szintig képes kompenzálni az OT terület szerepköri anomáliáiból fakadó kockázatokat.

Szabályozási környezetek, kompetenciák

Az IT terület kiberbiztonsági szabályozása általában már kialakított és működtetett keretrendszereken alapul. Egyre jellemzőbb, hogy még a kisebb szervezetek is létrehozzák a maguk IT (vagy Informatikai) Biztonsági Szabályzatát, illetve a szükséges eljárásrendeket, noha még most is sok esetben tapasztalható, hogy a szabályzatok inkább csak a „fióknak készülnek", azaz valamilyen megfelelőségi kényszer hatására jöttek létre és nem a valós működésre és

működtetésre vonatkoznak. Ez a jelenség az IT területen is óriási kockázatot hordoz, az elvárt folyamatokat leíró szabályzatok és a valós működés (gyakorlat) közötti különbség jelenti a legtöbb kiberbiztonsági hiányosság, gyengeség és sérülékenység forrását.

Üzemeltetési területen kedvezőbb a helyzet, az üzemeltetést végző szervezeti egység és az üzemeltető munkatársak alapvető érdeke, hogy az üzemeltetési folyamatok megfelelően dokumentáltak legyenek, mert ez az a know-how, amely alapján az üzemeltető személyzet tevékenykedik, ennek hiányában tulajdonképpen nem is lehet tervszerű üzemeltetési folyamatokról beszélni. Kisebb szervezeteknél természetesen előfordul, hogy üzemeltetési kézikönyv vagy egyéb üzemeltetési dokumentáció sem áll rendelkezésre, ezért auditori szempontból a dokumentációk megléte és azok minősége az érettségi szint egyik fontos fokmérőjének számít.

Az OT területen a működtetéshez szükséges dokumentációk általában rendelkezésre állnak és talán még jobb minőségű anyagokkal is lehet találkozni, mint az IT üzemeltetési dokumentációk. A megfelelő gépkönyvek, vagy akár a tevékenységeket leíró munkautasítások nélkül nem lehet a berendezéseket üzembiztosan működtetni, munkavédelmi vagy élet- és balesetvédelmi szempontokból is kötelezőnek lehet tekinteni ezeket a dokumentumokat. Sok esetben a tulajdonos vagy megbízó nem is veszi át a rendszert vagy a berendezést a dokumentáció nélkül, az IT-ban ez a kisebb szervezetek esetében sajnos gyakrabban előfordulhat. Mindkét területen problémás lehet azonban az üzemeltetési dokumentumok naprakészen tartása, de amíg az IT-ban gyakoribbak az olyan fejlesztések és változtatások, amelyek miatt frissíteni kellene a dokumentációt, az OT-ban ez sokkal ritkábban fordul elő és a már említett munkavédelmi vagy élet- és balesetvédelmi okokból jobban dokumentáltak a változások.

A kiberbiztonsági szabályozást tekintve az OT azonban óriási hátrányban van.

Míg az IT területen az IBSZ vagy akár egy szabványon alapuló információbiztonsági irányítási rendszer (IBIR, ISO 27001, stb.) képes kontrollokat megfogalmazni és az IT- vagy információbiztonsági folyamatokat működtetni, addig az OT területen ez jelenleg hiányzik. A legtöbb esetben az IBSZ hatóköre csak az informatikai területre terjed ki, az ipari és üzemi rendszerek ki vannak zárva a szabályzat hatóköréből és az OT mindennemű kiber- és információbiztonsági szabályozási környezet nélkül üzemel.

Ennek oka, hogy a terület jellegzetességei és az IT-tól való eltérései miatt az IT biztonsági szabályok jelentős része közvetlenül nem alkalmazható az OT területre, az adaptálásra pedig a szervezet nem tud vagy nem akar erőforrást fordítani. Főleg az OT terület képviselői igyekeznek elkerülni az IBSZ-be foglalt szabályok alkalmazását, mivel az adaptálás nélkül kikényszerített szabályok és eljárások súlyosan fenyegethetik az üzembiztonságot, termelés- vagy folyamatfolytonosságot. Ha esetleg vezetői szintre eszkalálódik a kérdés, a menedzsment nem fogja az IT vagy az IT biztonság képviselőjét támogatni egy olyan érvrendszerrel szemben, amelyben nullánál többször előfordul az a kijelentés, hogy *„akkor nem fog működni és leáll a termelés, szóval részemről oké, de a felelősséget Te vállalod!"*

Mindkét félnek igaza van, tehát egyik félnek sincsen igaza.

Közvetlenül nem lehet és nem is szabad az IBSZ kontrolljait kikényszeríteni az OT területen, azonban szabályozás nélkül nincsen lehetőség az OT kiberbiztonsági funkcióit kialakítani, mivel akkor nincsen olyan elvárásrendszer, amelyre felépíthetőek a humán, adminisztratív és technikai védelmi funkciók.

Erre a (sajnos meglehetősen általános) helyzetre jelentene megoldást az OT Biztonsági Szabályzat (OTBSZ) elkészítése.

Az OT szabályozási környezete sokféleképpen kialakítható, létrehozható az IBSZ-tól teljesen független szabályzatként is, azonban jobb megoldásnak tűnik egy olyan szabályzat kidolgozása, amely az IBSZ alá van rendelve, és azokra a kontrollokra terjed ki, amelyek csak adaptálva és átalakítva alkalmazhatók az OT terület folyamataira és eljárásaira. Minden olyan vonatkozásban, amelyek egyébként az IBSZ-ben megtalálhatók és közvetlenül is alkalmazhatók, elegendő csak az adott IBSZ kontrollt behivatkozni. Az OTBSZ tartalmazhat továbbá olyan kontrollokat is, amelyek ugyan szerepelnek az IBSZ-ben, azokra azonban nem csak hivatkozik, hanem azokat módosítva és testre szabva átemeli át és adaptálja a saját környezetébe.

Az ilyen átvételek számos „kikönnyítést" tartalmazhatnak, talán a legjobb példa erre egy klasszikus jelszóhigiéniás kontroll bemutatása és elemzése.

Az IBSZ számos helyen fogalmazza meg a különféle rendszerekben és alkalmazásokban használható jelszavakkal kapcsolatos elvárásait, például definiálja, hogy minden rendszerben és alkalmazásban kötelező a legalább 8 karakteres jelszó, a kis- és nagybetűk, illetve speciális karakterek használata, valamint a 60 naponkénti kötelező és kikényszerítendő a jelszócsere. Ezt a kontrollt sok esetben nem lehet az OT területen alkalmazni (hiába kötelező az IBSZ szerint), mert vagy az adott eszköz nem képes megvalósítani, vagy egyszerűen üzembiztonsági okokból nem lehet jelszóhasználathoz kötni egy adott funkciót. Például egy HMI felületen és képernyőn nem várhat el a szervezet jelszóhitelesítést, hiszen akár egy vészeseti leállítást nem lehet jelszóhoz kötni. El lehet képzelni, ahogy a berendezés éppen széthajtja magát és a robbanáshatáron pörög, miközben az eseményt észlelő és a beavatkozást megkezdeni kész gépkezelő megpróbál visszaemlékezni az éppen aktuális jelszavára, majd háromszor még el is rontja a beíráskor a jelszót, ezzel esetleg kizárva magát. Sok esetben a vezérlőeszközök szigetrendszerben üzemelnek, azaz nem rendelkeznek olyan hálózati kapcsolattal, amely lehetővé tenné a központi jelszókezelési folyamatokat, a jelszócseréket így eszközönként és manuálisan kellene megvalósítani akár többszáz eszközön, amelyre egyetlen szervezetnek sincsen erőforrása. Látható tehát, hogy a legáltalánosabb jelszóhigiéniás IT kontroll kikényszerítése is akár olyan üzembiztonsági kockázatot jelenthet, amelyet egyetlen felelős személy sem akar – *és nem is fog* – felvállalni, illetve sok esetben erőforrás sem áll rendelkezésre a kontroll működtetésére.

Az OTBSZ azonban a közvetlenül nem alkalmazható kontrollokat is képes „kikönnyíteni", például részletesen definiálja, hol *nem szükséges alkalmazni*, vagy olyan megfogalmazással él, amely kockázathoz köti vagy kockázattal arányos módon várja el a kontrollokat, például a vészleállításra lehetőséget biztosító HMI felületek esetében nem vár el hitelesítést és jelszóhigéniát. Itt lehet visszautalni a kompenzációs kontrollok alkalmazására. A példát tovább elemezve az említett HMI esetében az OTBSZ tehát nem fogja elvárni az egyedi, névhez kötött, azonosítást és számonkérhetőséget biztosító felhasználói hitelesítést, valamint a hozzá tartozó jelszóhigéniát, azonban ha a számonkérhetőség és azonosíthatóság az OT esetében is fontos (azaz kockázat, ha nem tudjuk ki állította le a berendezést), kompenzációs kontrollként (például) kamerás megfigyelést vezet be az adott területre és rögzíti, hogy mely kezelő használta a HMI felületet és állította le a berendezést. Látható tehát, hogy az OTBSZ rendkívül flexibilis – *és az OT számára élhető!* - szabályzati környezet kialakítását is lehetővé teszi azáltal, hogy felhasználja a már kialakított IT- és információbiztonsági kontrollokat, vagy azokat kockázatarányosan testre

szabja, a kikönnyítésekből fakadó esetleges hiányosságok kezelésére pedig kompenzációs kontrollokat vezet be.

Felmerülhet a kérdés, hogy ha lehetséges megfelelő OT biztonsági szabályozási környezetet kialakítani, akkor a szervezetek miért nem élnek ezzel a lehetőséggel?

Korábban is felvetésre került, hogy a szervezetek esetleg nem tudnak vagy nem akarnak erre erőforrást fordítani. Ennek oka, hogy az IBSZ sem csak úgy előkerült a semmiből. Az informatikai biztonsági szabályzati környezet kialakítását megelőzte[35] egy kockázatelemzési folyamat, amely során a szervezet (önállóan vagy külső szakértőket bevonva) feltárta majd elemezte a lehetséges tényezőket, amelyek a rendszerek és adatok bizalmasságát, sértetlenségét és rendelkezésre állását fenyegethetik, megállapította és értékelte a kockázatokat, majd azok kezelésére (megszüntetésére vagy csillapítására) a kockázatokkal arányos védelmi intézkedéseket hozott, amelyek végül az informatikai biztonsági szabályzatban öltöttek testet. Ugyanezen tevékenységeket szükséges az OT esetében is elvégezni, azonban már nem csak a bizalmasságot, sértetlenséget és rendelkezésre állást, hanem az üzembiztonságot és a megbízhatóságot is vizsgálva. Ez nem csak nagyon jelentős humán és anyagi erőforrást igényel, hanem olyan kompetenciákat is, amelyek legfeljebb részlegesen álnak csak a szervezetek rendelkezésére.

Míg IT oldalon ott vannak az egyes üzleti területek alkalmazásgazdái, IT üzemeltetési és architektúra mérnökök, IT biztonsági szakemberek, információbiztonsági szakértők, illetve a kockázatelemzésben és kockázatkezelésben jártas (akár külsős) kollégák, addig az OT esetében a terület megfelelő szakértői támogatása meglehetősen hiányos.

A legalapvetőbb probléma, hogy míg IT oldalon (belső, vagy külső forrásból) rendelkezésre állnak IT biztonsági és információbiztonsági szakemberek, addig az OT biztonsági szakértők meglehetősen ritkák. Az OT bár innovatív terület, a kiberbiztonságot tekintve jelentős elmaradásokkal küzd mind a technológiai és a humán területen, és még nem tudta kitermelni az IT-hoz hasonlóan évek, évtizedek óta tevékenykedő biztonsági szakértői rétegét. Ennek oka, hogy míg a különféle IT biztonsági munkakörök a piaci igény hatására az informatikai munkaerőpiac talán legkeresettebb és legjobban fizetett pozícióivá váltak, addig a piaci igény hiányában nem volt érdemes a szakembereknek az OT kiberbiztonságára specializálódni. Csak mostanában kezdett el jelentősebben felfutni az OT biztonsági terület, és jelentek meg azok az igények, amelyekre reagálva talán megindul a szükséges humán erőforrás képzése és remélhetőleg nagy számosságban megjelennek majd az OT biztonsági szakemberek.

OT biztonsági szakembert képezni azonban nem egyszerű. Jó ötletnek tűnne az IT biztonsági szakértőket bevetni az OT területén is, azonban ez az út általában[36] nem járható. Az IT biztonsági szakértők gondolkodásmódja a legtöbb esetben túl merev az OT meglehetősen változó és képlékeny struktúrájához. Még ha el is tudjuk fogadni a terület eltéréseit és másságát, az IT

---

[35] Jó esetben megelőzte. Sajnos tapasztalható olyan eljárás is, amely során egy teljesen idegen szervezet szabályzati környezetét igyekeznek átalakítani anélkül, hogy elvégezték volna a kockázatelemzés folyamatát. Ez az eljárás nem vezet használható és valós értékeket képviselő szabályzati környezetekhez, az így készült szabályzatok általában a „fióknak" készülnek, esetleg valamilyen megfelelőséget akarnak a meglétével kipipálni. Az így készült szabályzatok nem állják ki sem az idő próbáját, sem pedig a valós ellenőrzési vagy audit tevékenységet.

[36] Jelen tanulmány szerzője közel húsz év IT biztonsági tevékenység után öt éve foglalkozik az OT biztonsággal, a következőekben megfogalmazott vélemény a saját, hazai tapasztalatain alapul.

biztonság túl steril és dogmatikus, nagyon nehezen tud alkalmazkodni az OT terepi viszonyaihoz és világához.

Bár az IT biztonság előszeretettel hangoztatja, hogy „*nincs százszázalékos biztonság!*" – mégis annak megvalósítására, vagy elérésére törekszik. Általában kemény kontrollokban gondolkodik, amelyek képesek az irodai felhasználók („*OSI Layer 8*") „kilengéseinek" kockázatait redukálni, azonban ez alkalmazhatatlan az OT világában, mivel az OT felhasználói kör a korábbiakban bemutatottak alapján jelentősen eltér az IT-ban megszokottól. Az OT kiberbiztonsági szempontból puha és flexibilis kontrollokat igényel, a kiberbiztonság csak sokadlagos tényező, nem pedig irányadó és erőltethető szemlélet. Tapasztalat szerint az OT világában az IT biztonsági kollégákat olyan megmondóembereknek tartják, akik kívülállóként akarnak megoldani helyzeteket úgy, hogy sem a területet, sem pedig a terület problémáit nem ismerik.

A másik probléma, hogy a legtöbb IT biztonsági szakértő egyéb informatikai területről specializálódott a kiberbiztonság felé. Korábbi informatikai szakterületeiken jelentős tapasztalatokat gyűjtöttek, majd a tapasztalataikat felhasználva váltak etikus hackerekké, biztonsági mérnökökké, információbiztonsági szakértőkké, stb. A korábbi, nagytudású infrastruktúra- és üzemeltetési mérnökök, kódokba veszve éveket töltő fejlesztő- és szoftvermérnökök, adatbázis specialisták, vagy a veterán és sokat látott rendszergazdák mind-mind hozták magukkal a hosszú évek, évtizedek alatt gyűjtött tudásukat és váltak az IT biztonság jeles szakértőivé, képviselőivé. Azonban esetükben hiányoznak azok a terepi tapasztalatok, amelyek nélkül nem lehet az OT folyamatait megérteni és nem lehet a folyamatok, eszközök és rendszerek kockázatait meghatározni.

Egy korábbi IT infrastruktúra- vagy architektúra mérnök azért képes megérteni és értékelni egy informatikai rendszer kockázatait, mert éveken keresztül maga is informatikai rendszereket épített fel. Egy hálózatbiztonsági szakértő éveket töltött különféle hálózatok megtervezésével, kiépítésével és működtetésével, azaz minden kapcsolódó kockázatot képes felismerni és értékelni. Egy fejlesztőből vagy szoftvermérnökből etikus hackerré vált szakértő a korábbi munkájából adódóan ismeri a szoftvertervezés és a kódolás világát, pontosan tudja, hogy hol válhat egy szoftver sérülékennyé, azokat hogyan és milyen módszerekkel tudja egy támadó kihasználni és a rendszert kompromittálni.

De ha a leendő OT biztonsági szakértő nem dolgozott OT területen, nem épített berendezést, nem programozott ipari vezérlést, nem hozott létre folyamat- vagy gyártásautomatizálási eljárásokat, nem dolgozott villamos- vagy egyéb védelmi berendezésekkel, irányítástechnikával, nem piszkolta be a kezét PLC vagy egyéb kapcsolószekrényekben, hogyan érthetné meg a terület problémáit, hogyan ismerhetné fel és értékelhetné a terület kockázatait? Legfeljebb az IT biztonsági tapasztalatait próbálhatja meg átültetni, ezért is nevezhető ez módszer sterilnek és dogmatikusnak.

A leghatékonyabb módszer, ha a terepi tapasztalatokkal már rendelkező, folyamattervezésben, automatizációban, irányítástechnikában jártas, esetleg gépépítésben, PLC programozásban és integrációban is tapasztalt munkatárs kerül átképzésre. A szükséges IT és IT biztonsági szakismereteket sokkal könnyebb megtanulni, mint az OT kompetenciákat és a sokéves terepi tapasztalatokat megszerezni.

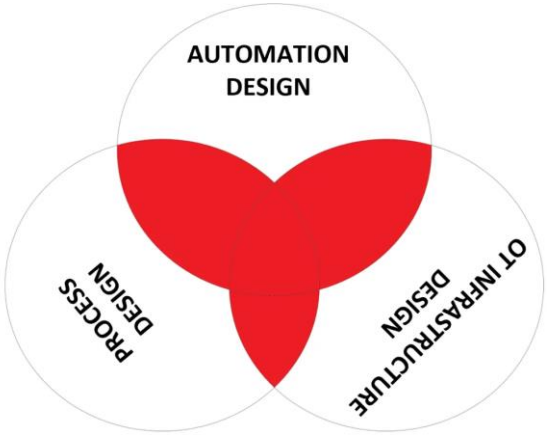
Az OT terület kockázatainak megértéséhez és főleg a kockázatok értékeléséhez több területi kompetenciára is szükség van. Sinclair Koelemij, a Honeywell szakértője három kompetenciaterület uniójában látja megvalósíthatónak az OT környezetek kockázatelemzését:

- Folyamatmérnöki terület,
- Automatizációs mérnöki terület
- OT infrastruktúra mérnöki terület

A folyamatmérnök és folyamattervezési terület mély szinten és részleteiben ismeri az adott üzemi folyamatokat, pontosan tisztában van azok lehetséges eseményeivel, kimeneteleivel, az egymásra épülő folyamatok esetleges akadályoztatásából adódó problémákkal, lehetséges reakciókkal, hibakezelési lehetőségekkel, a folyamatbiztonság követelményeivel és azok megvalósításával. Általában (és szükségszerűen) magasszintű ismeretekkel rendelkezik az automatizáció területén is, de jellemzően nem konfigurálja a rendszereket, azaz a folyamatok precíz megtervezését követően nem ő fordítja le a folyamatot az automatizáció nyelvére.

Az automatizációs mérnök és az automatizációs tervezési terület alakítja át a megtervezett folyamatokat az automatizáció nyelvére, azaz ők azok, akik rendelkeznek a különféle automatizálási funkciók magasszintű ismereteivel, az eszközök és berendezések konfigurációjához, a vezérlési rendszerek programozásához és működtetéséhez szükséges kompetenciákkal, tudják, hogy milyen forrásból milyen adatok érkeznek és távoznak, azok hogyan befolyásolhatják a folyamat működését, biztonságát és folytonosságát.

Az OT infrastruktúra mérnök az IT üzemeltetői kompetenciákat hasznosítja az OT területen. Ismeri a speciális berendezések működését, képes a különféle ipari hálózati eszközök és a rendszerek kapcsolatainak biztosítására. Képes a folyamatok működéséhez szükséges adatcsere eljárások megvalósítására és a különféle terminálok, felhasználói felületek, illetve az IT-ban is alkalmazott kiszolgálók hardveres és szoftveres üzemeltetésére. Az üzemi folyamatok részleteivel, illetve az automatizációs berendezésekkel kapcsolatban általában erősen korlátozott ismeretekkel rendelkezik, azokat csak a szükséges mértékig látja át.



OT kockázatelemzéshez szükséges kompetenciaprofil[37]

Sinclair Koelemij részletesen elemzi a szükséges kompetenciaprofil összetevőit és rámutat arra a hazai tapasztalatok alapján is észlelhető jelenségre, hogy sok esetben a kiberbiztonság az OT infrastruktúra üzemeltető személy vagy szervezeti egység feladatává vált, holott pont ez az a terület, ahol a folyamatokkal és az automatizációs funkciókkal a legkevésbé vannak tisztában. Ettől függetlenül, ha megfelelő a szakterületek közötti együttműködés, véleményem szerint az OT infrastruktúramérnök képes lehet az OT kiberbiztonsági szakértői tevékenység ellátására,

[37] *https://industrialcyber.co/expert/the-ot-security-skills-gap/*

azonban munkája során sokkal jobban támaszkodnia kell a folyamattervezési és az automatizációs szakemberekre.

A három szükséges kompetenciaterület a hazai szervezetek esetében ráadásul nem is különül el egymástól, ez legfeljebb a nagy szervezetek esetében valósul meg, a kisebb üzemekben vagy egyéb OT környezetekben ezek a szerepkörök akár teljesen átfedhetik egymást és sok esetben olyan kulcsember-helyzetek alakulnak ki, ahol csak egy-két munkatárs rendelkezik az összes kompetenciával. Ugyanaz a személy tervezi meg részletesen a folyamatokat, aki azokat automatizációs szinten is megvalósítja, mellette pedig még konfigurálja és működteti is az OT kiszolgáló- vagy hálózati eszközöket. Ilyen felállásban természetesen a kiberbiztonsággal is ennek a személynek kell(ene) foglalkoznia.

A hazai tapasztalat, hogy az OT infrastruktúramérnöki szerepkör egyáltalán nem létezik. Sok esetben lehet találkozni azzal a megvalósítással, hogy az IT felelősségi- és tevékenységi köre csak egy bizonyos pontig (általában a falialjzatig vagy portig, jobb esetben az arra csatlakoztatott, már OT fennhatóságú hálózati eszközig) terjed ki, utána már az IT nem illetékes és nem foglalkozik az OT rendszerekkel („*Onnantól oldjátok meg magatok*!). Az OT persze megoldja, de mivel az infrastruktúramérnöki, hálózatbiztonsági és IT biztonsági kompetencia hiányzik a területről, a megoldások sok sebből véreznek és a rendszer infrastruktúra szinten is sebezhetővé válik.

Nem feltétlenül jobb a helyzet akkor sem, ha egy külsős szállító vagy integrátor építi fel és működteti az OT rendszert. A folyamattervezési kompetencia ilyenkor a rendszertulajdonos szervezet oldalán található, míg az automatizációs és OT infrastruktúra kompetencia a külsős partner birtokában van. Ebben az esetben az OT kiberbiztonsági feladatköre a külsős szállítóra hárulhat, akik viszont a folyamattervezés és folyamatbiztonság elvárásait (és a folyamatfunkciókat) esetleg nem ismerve kellene, hogy kialakítsa a kiberbiztonsági képességeket úgy, hogy maga sem infrastruktúra- és hálózatbiztonsági, vagy kiberbiztonsági szakértő.

A különféle szektoriális sztenderdeknek és törvényi előírásoknak való megfelelés egyre nagyobb hangsúlyt kap nem csak nemzetközi, de hazai szervezetek életében. A sztenderdek és a törvényi elvárások is kitérnek a biztonsági és kiberbiztonsági képességekre. Természetesen a törvényi előírásoknak való megfelelés a leghangsúlyosabb, hazai vonatkozásban ilyen például a „*2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*[38]" szóló rendelkezés. Egy szervezetnek tehát akár a saját szektorára jellemző sztenderdnek (például élelmiszeripari vagy autóipari megfelelőség) és kijelölés esetén a nemzeti létfontosságú rendszerelemekkel kapcsolatos elvárásoknak (törvényi megfelelőség) is meg kell felelnie, ez pedig a külsős szállító és üzemeltető esetén különösen problémás lehet. Annak megfogalmazása, hogy a szükséges (például kiberbiztonsági) tevékenységek elvégzése pontosan kinek a feladata, és kinek milyen felelőssége van a törvényi megfelelőség szempontjából, egyáltalán nem egyszerű. Például erőművi rendszer esetében (energia ágazat, távhő alágazat[39]) sok esetben a gyártó szállítói, integrátori, üzemeltetői és támogatói szerepkörben is megjelenhet. Az OT kiberbiztonsági tevékenységekhez, kockázatelemzéshez szükséges kompetencia elemek nagyobb részben ilyenkor jellemzően a gyártó vagy külsős partner oldalán találhatók meg,

[38] *https://net.jogtar.hu/jogszabaly?docid=a1200166.tv*

[39] *1. melléklet a 2012. évi CLXVI. törvényhez, https://net.jogtar.hu/jogszabaly?docid=a1200166.tv*

azonban hogyan lehet egy nagy nemzetközi gyártóra hárítani a hazai törvényi megfelelőség teljesítését? Egy ágazati sztenderd (például autóipari vagy élelmiszeripari megfelelőség) esetén sokkal egyszerűbb a helyzet, a szállított rendszerek többnyire ilyen sztenderdek alapján kerülnek kiépítésre, az egyes komponensek sok esetben már rendelkeznek a megfelelő tanúsítványokkal ahhoz, hogy az adott ágazati környezetben alkalmazhatók legyenek. De egy magyar törvényi megfelelőség nem sokat mond egy amerikai vagy német gyártónak.

Látható, hogy az OT terület kockázatelemzése multidiszciplináris tevékenység, és sok esetben a szükséges kompetenciák sem állnak hozzá rendelkezésre, azokat összeszervezni és a kockázatelemzés rendelkezésére bocsátani nem egyszerű feladat. Az OT biztonsági szakember az egyes szakterületi kompetenciák birtoklásával és a szakterületek támogatásával képes lehet (kisebb rendszerek esetén) akár önállóan is elvégezni a kockázatelemzést (majd az intézkedéseket végre is hajtja), azonban egy komplex és nagy infrastruktúra esetén erre a legjobb megoldás egy olyan kompetenciaközpont létrehozása, ahol az összes szakterület képviselteti magát és akiknek tudását az OT biztonsági szakértő fogja össze és szintetizálja.

Az IT és információvédelem vagy IT biztonság világában erre is van jógyakorlat, a nagyobb szervezetekben működő infrastruktúra és/vagy biztonsági bizottság (*infrastructure & security committee*) tevékenysége az OT világába is beemelhető és megvalósítható. A bizottságban képviseltetheti magát az IT, a folyamattervezés és automatizálás és az üzleti terület is, közös erőfeszítéssel és minden terület számára elfogadhatóan megvalósítható a kockázatelemzés, létrehozhatók a különféle védelempolitikai és biztonsági stratégiai elvárások, szabályzatok, tervek és egyéb magasszintű anyagok, amelyeknek végrehajtásáról az egyes területek képviselői gondoskodnak, a bizottság pedig képes a végrehajtás értékelésére és ellenőrzésére.

Személyiségi jellemzők, készségek

A személyiségtípusokkal kapcsolatosan rengeteg kutatás és modell létezik, de közös pontjuk, hogy valamilyen pszichológiai kategorizálási módszeren keresztül próbálják meg csoportokba sorolni a személyeket annak érdekében, hogy jobban megérthetőbbé váljon az emberek közötti interakció, az egymás közötti kommunikáció és az emberi viselkedés.

Carl Gustav Jung szerint két alapvető csoportra oszthatók személyiségük alapján az emberek, az extrovertált és introvertált típusokra. A két csoport között természetesen vannak átmenetek, sok egyéb jellemző és preferencia határozza meg, hogy mely nagyobb halmazhoz közelít a vizsgált alany személyisége, de valamely nagyobb csoportba minden ember besorolható.

A kifelé forduló (extrovertált) személyiség típusba tartozó emberek aktivitása főleg a külvilág felé irányul, szeretnek a középpontban lenni, kapcsolatteremtő képességük jó. Nyitott szemléletűek, törekednek arra, hogy bemutassák magukat, képességeiket és értékeiket a világnak. Intuitívak, döntéseikben gyorsak és magabiztosak, nem idegenkednek felületes információk alapján cselekedni. A csapatmunka, a másokkal való együttműködés nem jelent számukra problémát, gyakran törekednek a vezetői szerep elnyerésére.

A befelé forduló (introvertált) személyiség típusba tartozó emberek aktivitása jellemzően befelé irányul. Ez nem jelenti azt, hogy minden introvertált félénk és elzárkózó lenne, csupán azt, hogy igyekeznek kerülni a külvilág felé való nyitást, ezért az extrovertált személyiség ellenpólusának tekinthetők. Elemző gondolkodás és higgadtság jellemzi őket, az intuitív és gyors döntések

helyett az értelmezésre, elemzésre és átgondolásra törekednek. Kerülik a kezdeményezést és a konfrontációt, sokkal inkább a saját, mintsem a külvilág elvárásainak akarnak megfelelni.

Kevés szakirodalom foglalkozik specifikusan az informatikai területeken dolgozó munkavállalók személyiségjegyeivel, az OT területeken belül tevékenykedőkkel kapcsolatban pedig végképp nem áll rendelkezésre specifikus elemzés.

Az empirikus vélemények (és persze sztereotípiák) alapján az IT területen dolgozók esetében a más munkakörökhöz képest nagyobb valószínűséggel találhatók meg az introvertált személyek. Nincsen ez másképpen az OT világán belül sem. Az OT berendezések - *mint kiberfizikai rendszerek* - a való világ jeleit alakítják digitális jelekké, illetve a digitális jelekből fizikai változásokat hoznak létre. A folyamattervezés és az automatizálás mindenekelőtt tehát racionális, módszeres és aprólékos gondolkodást, tervezői és mérnöki szemléletet igényel. A tévedések kárt okozhatnak a berendezésekben és a környezetben, illetve súlyosan fenyegethetik az emberi életet és testi egészséget, ezért az intuitív és gyors döntések nem jellemzőek az OT világán belül. Ellenkezőleg, a megfontoltság, körültekintő és aprólékos tervezés és végrehajtás a sokkal jellemzőbb, a berendezések és a környezet, valamint az emberi élet épségének, védelmének elvárása még megfontoltabb, analitikusabb és kritikusabb szemléletű személyiséget kíván.

Mind az IT, mind az OT területén belül rengeteg munkakör és pozíció létezik. Korábban már szó esett arról, hogy az irodai tevékenységű IT-val szemben az OT területen jóval vegyesebb a felhasználói kör, a felhasználók között a terepi környezetekben dolgozó „*kékgalléros*" munkatársak is képviseltetik magukat, sőt akár nagyobb számban is megjelenhetnek, mint a „*fehérgalléros*" munkavállalók. Ez még jobban árnyalhatja a személyiségtípusok megjelenését, ezért személyiségtípusok helyett sokkal inkább a készségeken van a hangsúly mindkét területen, de az OT világában különösen.

Az informatikai szakemberek jellegzetes személyiségjegyeivel és készségeivel kapcsolatban egy 2014-ben megjelent publikáció[40] megpróbálta összehasonlítani az informatikai és nem informatikai területen dolgozók személyiségi jellemzőit és készségeit. A kutatás célja annak megállapítása volt, hogy különböznek-e és ha igen, milyen mértékben különböznek az informatikai területen dolgozók a más foglalkoztatottságú személyektől. Ennek a kutatásnak az alapját egy 2004 és 2012 között gyűjtött, közel 86 ezer munkavállalót szerepeltető adattömb szolgáltatta, amelyben csaknem 13 ezer személy jelölte meg, hogy jelenleg vagy korábban valamilyen informatikai technológiával kapcsolatos területen dolgozott.

A kutatás eredményei véleményem szerint akkor is relevanciával bírnak, ha figyelembe vesszük a technológia és a digitalizáció robbanásszerű fejlődését és feltételezzük, hogy az eltelt nyolc év alatt a piaci igényekben végbement változások (beleértve a technológiai területeket jelentősen érintő gazdasági válságokat, illetve a pandémiás szituációkat) alkalmazkodásra kényszerítik a munkavállalókat. Tudományosan többféle megközelítés létezik azzal kapcsolatban, hogy változhat-e és ha igen, mennyire változhat az ember személyisége az idő, a társas kapcsolatok, a környezet és egyéb behatások függvényében, tehát az alkalmazkodás kifejezés jobban igazodik a szervezetszociológiai megközelítéshez, és igaz lesz abban az esetben is, ha a munkavállaló

[40] *„Distinctive Personality Traits of Information Technology Professionals" - https://ccsenet.org/journal/index.php/cis/article/download/36413/21414*

személyisége nem megváltozik, hanem „csak” tudatosan kontrollálva adaptálódik a szervezet és a munkakör igényeihez[41].

A kutatás során tíz jellemzőt és készséget vizsgáltak meg és hasonítottak össze az informatikai és egyéb területeken dolgozó munkavállalókkal kapcsolatban.

Jellemző, készség	IT területi átlag	Egyéb területi átlag
Nyitottság	3.73	3.74
Lelkiismeretesség	3.29	3.36
Érzelmi stabilitás	3.37	3.43
Együttműködés	3.53	3.49
Extrovertáltság	3.59	3.80
Asszertivitás	3.40	3.55
Optimizmus	3.70	3.82
Gyakorlatiasság	2.98	2.63
Motiváltság	3.21	3.34
Ügyfélközpontúság	4.21	4.19

A személyiségjellemzők átlagos pontszámai informatikai és az egyéb foglalkozások esetében[42]

Látható, hogy a vizsgált mintában hét területen mértek rosszabb pontszámokat az IT munkavállalók esetében és csak három esetben fordult elő, hogy az IT munkavállalók adott jellemzőjét vagy készségét pozitívabban értékelték, az együttműködés, a gyakorlatiasság és az ügyfélközpontúság esetében.

Az együttműködés értékelése mindenképpen szembe megy a sztereotípiával, de valójában mára már egyáltalán nem jellemző, hogy az IT munkavállaló magányos gerillaharcosként, szinte számkivetetten küzd. Még a nagyobb önállóságot igénylő fejlesztési feladatok esetén is kiemelten fontos az együttműködés, nem csak a munkatársakkal, hanem az egyes fejlesztői csapatok között is.

A gyakorlatiasság területén nem meglepő az eredmény, a publikáció részletesen kitér arra, hogy a legtöbb IT tevékenység racionális és logikus hozzáállást igényel, a problémamegoldás és hibaelhárítás a mindennapok része. A kutatás bizonyította azt a vélekedést, hogy az informatikai területen alacsonyabb a kifelé forduló, extrovertált és magasabb a befelé forduló, introvertált személyiségű munkavállalók száma, mivel sok olyan tevékenység létezik a szakmán belül, ahol

---

[41] Véleményem szerint a személyiség és a készségek is fejleszthetők. A kiberbiztonsági képességfejlesztés mára az egyik legfontosabb védelmi területté vált a növekvő fenyegetettség kockázatainak csillapítására. Sokféle megközelítés létezik ezen a területen is, például abban sincsen konszenzus, hogy a személyiségfejlesztés hozza magával a készségek fejlődését, vagy pedig a készségek fejlesztése hat ki majd a személyiségre. A személyiségfejlesztés véleményem szerint inkább a szervezetfejlesztési tevékenységekben kerül jobban fókuszba, a kiberbiztonság általában megelégszik a készségek fejlesztésével.

[42] Distinctive Personality Traits of Information Technology Professionals” – Table1 - https://www.ccsenet.org/journal/index.php/cis/article/view/36413

alacsony az interperszonális interakciók száma, és ezek a pozíciókban jobban tudnak alkalmazkodni az introvertált személyek. Ezt azonban érdemes az együttműködési jellemzőnél mért magasabb pontszámmal együtt értelmezni: lehet, hogy több introvertált személyt vonz az informatika, viszont ezzel együtt is jobban együttműködő a terület, mint más foglalkoztatottság esetén.

Az ügyfélközpontú gondolkodás és cselekvés abban gyökerezik, hogy a szervezeteken belül az informatika kiszolgáló szerepkörben működik, a célja az üzleti területek (vagy a felhasználók) adat- és információtechnológiás kiszolgálása. A szervezetfejlesztési tevékenységeken belül az informatikai szervezetfejlesztés nagyon erős fókuszt helyez az ügyfélközpontúságra és igyekszik az IT tevékenységeket határozottan szolgáltatáscentrikussá alakítani.

Ahogy korábban említésre került, az OT terület munkavállalóival kapcsolatban még nem készült ehhez hasonló kutatás, így legfeljebb empirikus és szubjektív módon lehet összehasonlítani a két terület munkavállalóinak személyiségjegyeit és készségeit. Mégis érdemes ezzel a kérdéssel foglalkozni, mivel az OT és az IT területek között sok esetben tapasztalható együttműködési problémákat nem csak a preferenciák közötti különbségek, hanem például a személyiségjegyek és készségek közötti eltérések is okozhatják. A 2014-es kutatás mért értékeit referenciaként felhasználva véleményem szerint empirikus úton az alábbi eltérések azonosíthatók és értelmezhetők:

Jellemző, készség	IT terület	OT terület	Empirikus és szubjektív értelmezés
Nyitottság	3.73	**IT > OT**	*Az OT kevésbé nyitott a változásokra. Ami működik, az működik, ne javítsuk meg. A változás kockázattal jár.*
Lelkiismeretesség	3.29	**IT < OT**	*A kiberfizikai tevékenységek negatív hatással lehetnek a berendezések, az emberi élet és egészség, illetve a környezet épségére. A precizitáshoz való ragaszkodás érték, a kis eltérés is nagy hiba.*
Érzelmi stabilitás	3.37	**IT < OT**	*Az irányítás és a kontroll nem csak a berendezésekre és a fizikai világ változásaira terjed ki, a belső törekvés az egyensúly és az optimális működés fenntartása ösztönös stresszoldóként működhet. Kevesebb az interakció az emberekkel, így a stresszforrás jelentős része kezelhetőbb.*
Együttműködés	3.53	**IT > OT**	*Kevesebb az interakció az emberekkel, az együttműködési készség fejlettsége alacsonyabb szintű. Ez a más területekkel való együttműködésre jellemzőbb, általában az OT-n belül jobban egymásra vannak a személyek utalva, a területen belüli együttműködés ezért hatékonyabb. A változásokkal szembeni tartózkodás az együttműködésre is kihathat.*
Extrovertáltság	3.59	**IT > OT**	*A kevesebb emberi és több gépi interakció jobban vonzza az introvertáltabb személyiségeket. Ez akár a gépkezelők vagy operátorok esetében is megfigyelhető, akiket bár munkatársak vesznek körül, a tevékenységük azonban jobban fókuszál magára a működtetett berendezésre.*
Asszertivitás	3.40	**IT > OT**	*Az önérvényesítés területén az IT is elmarad más területektől, az OT viszont az IT-nál is alacsonyabb asszertivitással működik. Ennek lehetséges oka, hogy a kontroll és irányítás motivációja teljesül a berendezések és gépek feletti irányítás elérésével, nincs erős késztetés a humán szereplőkkel szembeni asszertivitásra.*
Optimizmus	3.70	**IT > OT**	*Az OT terület jóval érzékenyebb a hibákra és eltérésekre, a folyamatos éberség fenntartása, az analitikus és kritikus gondolkodás is magával vonzhatja a pesszimistább szemléletet. A pesszimistább szemléletnek jóval kisebb hatása van a motiváltságra, ez feltételezi, hogy a pesszimizmust a terület jobb realitásérzékelésként értelmezi.*
Gyakorlatiasság	2.98	**IT < OT**	*A találékonyság és a terepi viszonyokhoz való alkalmazkodás még az informatika átlagfeletti problémamegoldó képességénél is jobb eredményt hoz. Működnie kell, ezért működni is fog.*

Motiváltság	3.21	**IT < OT**	*Lehetséges, hogy a viselt felelősség (élet- és környezetvédelem, berendezések védelme, stb) a lelkiismeretesség és az érzelmi stabilitás együttesen erősebb motivációt jelentenek.*
Ügyfélközpontúság	4.21	**IT > OT**	*Az alacsonyabb önérvényesítő és a más területekkel való együttműködési képesség együttesen gátolhatja az ügyfélközpontú szemlélet megerősödését. Lehetséges, hogy a folyamatos működés a területen nem értelmezhető szolgáltatásnak, hanem egy alapvető és minden körülmények között teljesítendő elvárásként jelenik meg.*

A személyiségjellemzők összehasonlítása, saját és empirikus értelmezés

Több tényező is szerepet játszhat a sok esetben tapasztalható alacsonyabb együttműködési készség rögzülésében. A területen nagyobb gyakorisággal megjelenő introvertált személyiségek - a személyiségtípusnak megfelelően - nehezebben képesek az interakciók kezelésére, ráadásul a kevésbé asszertív magatartás miatt nehezebben tudnak érvényesülni az OT terület igényei és elvárásai. Ha a vitás helyzetekben több alkalommal sem tudja valaki a saját érdekét érvényesíteni, kialakulhat és rögzülhet egy védelmi szerepet betöltő elutasító séma, amely megnehezíti vagy gátolja az együttműködési készség kialakulását és fejlődését.

Az együttműködés hajtóereje a kompromisszum, azonban az OT terület több szituációban sem kész kompromisszumot kötni. Ezek zömmel olyan esetek, amelyek az OT véleménye szerint negatív hatással vannak vagy *lehetnek* a folyamatbiztonságra, a folyamatos működésre, vagy az üzembiztonságra, azaz ebből a szempontból a magasabb szintű lelkiismereti készség is szerepet játszhat abban, hogy más szervezeti egységek esetleg nem tartják kellő mértékben együttműködőnek az OT területet. Itt fontos kiemelni, hogy egy adott eseménynek, felvetésnek vagy elvárásnak nem kell feltétlenül negatív hatással lennie az OT rendszerek és folyamatok működésére. Az elutasító és nem együttműködő magatartás akkor is megjelenhet, ha az OT csak *feltételezi*, hogy esetleg a számára fontos preferenciák sérülhetnek.

A szervezetfejlesztési folyamatokban nagy hangsúlyt kaphatnak az úgynevezett *win-win* szituációk elérésére való törekvések. A *win-win* köznyelvi értelemben azt jelenti, hogy egy konfliktus vagy probléma kezelése olyan módon zárul, amelyet mindkét fél nyereségnek tud elkönyvelni. Valójában azonban ez a legtöbb esetben nem tud megvalósulni, mert mindkét félnek fel kell adnia valamit az elvárásaiból ahhoz, hogy létrejöjjön egy mindenki számára elfogadható kompromisszum. Valójában tehát önállóan egyik fél sem nyer, **a két fél csak *együtt, mint szervezet* nyer**, és megoldanak egy olyan problémát, amely korábban mindkét félre, azaz a szervezetre negatív vagy rosszabb esetben romboló hatást gyakorolt. Az OT azonban nem tud feladni olyan álláspontot, amely az üzembiztonságot és a folyamatbiztonságot érinti. Nem teheti meg, mert a rendszerekért, emberéletért és egészségért érzett felelősség ezt nem teszi lehetővé. Ilyen esetekben az OT merevnek és elutasítónak tűnhet, olyan területnek, amely nem kész még csak kompromisszumot sem kötni.

Az OT esetében tapasztalható lehet, hogy a konfliktushelyzetek kialakulását elkerülő stratégiával igyekszik megelőzni. Ez a viselkedés az alacsonyabb önérvényesítő és együttműködési készségből következhet, sok esetben a konfliktushelyzet nem kezelhető az OT számára, mert nem rendelkezik a megoldáshoz szükséges képességgel, erőforrással és asszertivitással, illetve a konfliktusból adódó esetleges (szervezeti, személyi) károk meghaladhatják a megoldásból származó (szervezeti, személyi) nyereséget. Az elkerülésre törekvő konfliktuskezelési stratégia sokáig sikeres lehet, azonban a megoldatlan (elkerült vagy halogatott) konfliktusok a háttérben felgyűlnek és súlyosan rombolhatják a munkavállalói önbecsülést, a terület motivációját és az együttműködési készséget.

Az IT területet célzó kutatásból látható volt, hogy az informatikai terület kevésbé asszertív, mint az egyéb foglalkoztatottságúak. Az IT területen magasabb számban mértek befelé forduló személyiségű munkavállalókat, az önérvényesítő magatartás pedig sokkal nehezebben tud kialakulni, ha a személyiség introvertált. Mivel az OT esetében magasabbnak tűnik az introvertált személyiségű munkavállalók száma, ezért érthető, ha az asszertivitás készsége alacsonyabb szinten jelenik meg a területen.

Vélhető, hogy az asszertivitás hiányosságai interperszonális és szervezeti szinten is problémát jelenthetnek, azonban a lelkiismereti készség fejlettsége megakadályozza, hogy ez közvetlenül visszahasson a működtetett rendszerekre. Interperszonális szinten tapasztalható, hogy a terület munkavállalói akár HR szempontból sem képesek az IT területen dolgozó kollégáikhoz hasonló önérvényesítésre, például sokkal nehezebben mondanak nemet egy-egy olyan plusz feladatra, amely már meghaladja a rendelkezésre álló erőforrásokat. Ennek tünetei lehetnek a túlmunkák, túlvállalások, felgyűlő feladatok, fokozódó stresszérzet, vagy az elégedetlenség és motivációvesztés, amely a fejlettebb lelkiismereti készséggel párosulva további frusztrációt okozhat és előbb-utóbb az érzelmi stabilitás megbomlásához vezethet.

Amikor azonban arról van szó, hogy egy olyan változással szemben kell képviselni az OT érdekeit, amelyek vélten vagy valósan fenyegethetik a rendszerek üzembiztonságát és megbízhatóságát, az OT nagyon is képes asszertív lenni, sőt, ebben az esetben más területek részéről merülhet fel, hogy az OT túlságosan is asszertív kommunikációt folytat és nincs tekintettel mások felelősségére vagy kötelezettségére. Az asszertivitás és az asszertív kommunikáció ugyanis arany középutat jelent, ahol a két véglet, a passzivitás és a mindent elsöprő érdekérvényesítés között kell megtalálni a megfelelő egyensúlyt a sikeres és pozitív önérvényesítés érdekében. Amikor az OT esetleg kapásból azzal söpör el egy érvet, hogy „*akkor nem fog működni a rendszer és az a te felelősséged lesz!*" az az asszertív kommunikáció szempontjából olyan véglet, amellyel a másik fél nem tud mit kezdeni. Kiberbiztonsági szempontból ez - ha nem is közvetlenül - de közvetetten visszahathat a működtetett rendszerekre, azok kiberbiztonsági állapotára.

Az ügyfélközpontúság szempontjából az IT jó ideje egyértelműen kiszolgálói és szolgáltatói szerepkörben működik. Az IT tulajdonképpen informatikai szolgáltatások összességeként is tekinthető, ahol a felhasználói kör és az üzleti területek a biztosított szolgáltatásokon keresztül érzékelik a terület jelenlétét és működését, illetve ahol a szolgáltatások minősége határozza meg a terület sikerességét vagy sikertelenségét. Az IT tehát a felhasználókat, mint ügyfeleket kezeli, a terület tevékenységének értékét pedig az ügyfelek elégedettségéből lehet kikövetkeztetni. Rossz felsővezetői vélekedésként tekinthetők azonban az olyan kijelentések, miszerint az IT közvetlenül nem termel értéket, mert az ügyfélelégedettség és a hatékony működés az a közvetlen érték, amelyet egy jól működő IT az üzemeltetési és fejlesztési szolgáltatásokon keresztül megteremt. Ha a szervezet lehetőségeihez képest az ügyfélelégedettség alacsony, a szolgáltatások színvonala is feltételezhetően gyenge, ez pedig megakadályozhatja a szervezetet az üzleti céljainak elérésében, sőt, súlyos vagyoni és nem vagyoni károk okozója is lehet.

Az OT terület nem kiszolgálóként vagy szolgáltatóként, hanem termelőként tekint magára. Előfordulhatnak olyan kommunikációs végletek, ahol az OT érvrendszeréven megjelenik például az az ismerős kijelentés, hogy „*az IT nem termel, mi termelünk!*", amely persze ugyanúgy rossz és szűklátókörű álláspont, mint korábban a felsővezető esetében, valamint alapjaiban akadályozhatja a területek közötti együttműködést. Az OT esetében az ügyfélközpontúság készségének hiányossága abból fakadhat, hogy a terület úgy véli, nem szolgáltatást nyújt, hanem

a termelés fizikai megvalósulását teszi közvetlenül lehetővé. Ez csak régen volt igaz, mára azonban egy modern és fejlett OT terület a digitális transzformáció felgyorsulása és az Ipar 4.0 igényrendszere (például adatvezérelt gyártás) miatt már szolgáltatásokat is meg kell(ene), hogy valósítson, legalább a folyamatos és pontos információszolgáltatást, amely nélkülözhetetlen a különféle termelésirányítási és termelésoptimalizációs rendszerek számára. Sok esetben sajnos már az információszolgáltatás, illetve a más területeken feldolgozott információk alapján indikált változások is nehezen találnak befogadásra a területen, az ügyfélközpontúság készségének esetleges hiányosságai pedig az Ipar 4.0 és a digitális transzformáció hátráltatójaként jelenhetnek meg a szervezet életében. **Az üzleti terület már elvárja, hogy az OT kezdeményező legyen és előálljon olyan fejlesztési javaslatokkal és szolgáltatásokkal, amelyek hatékonyabbá, átláthatóbbá, tervezhetőbbé teszi a gyártást és termelést, ezért az ügyfélközpontúság és szolgáltatáscentrikusság készségeinek fejlesztése kiemelt fontossággal bír.**

Motiváció, elismertség, hivatástudat

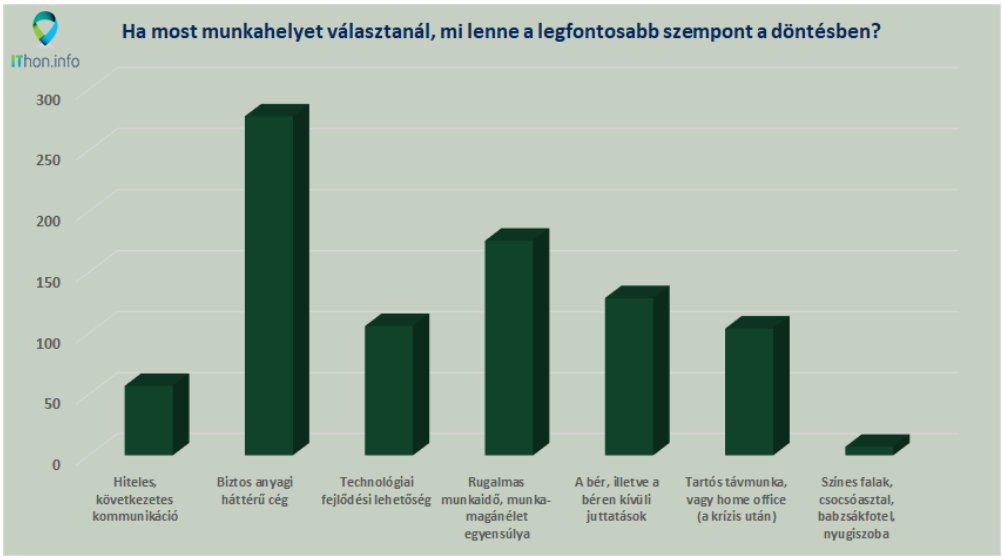
A munkáltatók gyakran tekintenek a munkabérre a legfőbb motivációs eszközként, azonban az informatikai szektort célzó kutatások több alkalommal is megerősítették, hogy az IT esetében már nem a munkabér számít a leginkább motiválónak. Fontos tényező, de sokkal kevésbé kap már szerepet a munkavállalói elégedettségben, mint korábban.

A *Jobsgarden* infokommunikációs szektort célzó 2017-es felmérésében[43] a megkérdezettek 78 százaléka a kihívást jelentő feladatokat, 59 százalékuk pedig a kiemelkedő jövedelmi lehetőségeket jelölte meg fontos motivációként. A home office, a kiegyenlített munka-magánélet viszony és a legújabb technológiákhoz való hozzáférés a felmérés szerint közepes motivációs erővel bír, ezeket a lehetőségeket a válaszadók nagyjából fele jelölte meg. A válaszadók 79 százaléka szerint a munkaadónak biztosítania kell a folyamatos szakmai fejlődés lehetőségét, 71 százalékuk elvárja a rugalmas munkavégzés támogatását, 70 százalékuk pedig az izgalmas és kihívást jelentő projekteket. Az eredmények alapján a szektor dolgozóit – nemtől függetlenül – legkevésbé a béren kívüli juttatásokkal tudják megfogni a vállalatok, ezt elvárásként csak a kitöltők 9 százaléka jelölte meg.

Az *IThon.info* által 2020-ban, a pandémiás időszak első évében készített felmérés[44] hasonló eredményt mutat, bár ezen kutatás inkább arra fókuszált, hogy az ágazat szereplői hogyan reagálnak a pandémiás helyzetre és hogyan tudják megőrizni munkavállalóik biztonságérzetét. A felmérésben a munkahelyváltoztatással kapcsolatban állítottak fel egy olyan preferenciasort, amely aktív munkaviszonyban motivációs preferenciaként, vagy munkavállalói elvárásként is értelmezhető.

[43] *https://happyhunter.blog.hu/2017/10/09/lanyok_irany_az_ict_szektor*

[44] *https://www.digitalhungary.hu/e-volution/Az-informatikusok-30-a-egyaltalan-nem-fel-attol-hogy-elvesziti-munkajat/9340/*



Munkavállalói elvárások munkahelyváltáskor

A munkabér és a juttatások szempontjából a legtöbb hazai vállalat nehézségekkel küzd, ez a jelenség az IT szektorban még inkább tapasztalható.

Az Informatikai Vállalkozások Szövetsége (IVSZ) által készített szakpolitikai ajánlás[45] részletesen ismerteti a jelenséget és annak negatív következményeit és külön kiemeli a KKV és nagyobb vagy multinacionális vállalatok között kialakuló bérfeszültségi helyzetet. A kisebb vállalatok csak nehezen, vagy egyáltalán nem tudnak a nagyobb cégek juttatási csomagjaihoz hasonló kereteket biztosítani, ez jelentős versenyhátrányba hozhatja a kisebb szervezeteket. Azonban a nagyobb vállalatok számára is egyre növekedő terhet jelent, hogy kielégítsék a munkavállalók juttatási elvárásait. Ez különösen igaz a fiatal pályakezdők esetében, de a későbbiekben is problémát jelent az egyre magasabbra kúszó bérigény. A munkavállalók megszerzéséért folyó kiélezett verseny az informatikai szektorban odáig „hajtotta fel" a munkabéreket, amelyek kitermelése lassan már lehetetlenné, vagy legalábbis rendkívül nehézzé válik.

Az OT terület több szempontból is hátrányos helyzetbe kerül, ha a juttatásokat és a kiegészítő motivációs eszközöket hasonlítjuk össze. Egyrészt az OT munkavállalói vagy felhasználói rétege a korábbiakban ismertetettek szerint nem csak közepesen- vagy magasan képzett munkavállalókból áll, hanem nagy számban megjelennek az alacsonyabb képzettségű munkatársak is, akik valamilyen szakmunkás, segédmunkás vagy betanított szerepkörökben tevékenykednek. Ennek a „*kékgalléros*" felhasználói rétegnek a motiválása és motiváltsága (ezen belül természetesen a juttatási csomag) jelentősen eltérhet a magasabb képzettségű, „*fehérgalléros*" munkavállalókétól.

Az IT szektor munkavállalói esetében motivációt jelentő elvárások egy része az OT területen nem, vagy csak erős korlátozással teljesíthető.

A rugalmas és flexibilis munkaidő, valamint a magánélettel egyensúlyban lévő munkavégzés nehezen megvalósítható egy, az év 365 napján működő, termelő és emiatt többműszakos

[45] *https://ivsz.hu/wp-content/uploads/2021/06/ginop-5-3-5-kutatasi-zarojelentes-szakpolitikai-ajanlas-informatika-agazati-munkaeropiaci-tunetterkep-ivsz-enrawell.pdf*

munkarendet követő munkahelyen, ahol a műszakok beosztása szigorú(bb) rendet követ és nehezen megváltoztatható. A beosztás és a műszakszervezés flexibilitása nagyrészben függhet a rendelkezésre álló erőforrásoktól, sok esetben tapasztalható, hogy a „*kékgalléros*" személyzet esetében is küzdenek a munkáltatók a szükséges erőforrás és kapacitás biztosításával.

Az OT esetében ugyancsak sok esetben nem megvalósítható a távmunka vagy a home office, hiszen a vezénylő- és kezelői helységben, vagy a terepen dolgozók (karbantartók, gépkezelők, elektrikusok, stb) tevékenysége megköveteli a fizikai jelenlétet. Vannak olyan szerepkörök, amelyekben megvalósítható a távmunka és a home office, azonban ez már súlyosan hatással lehet a kiberbiztonságra, mert az OT környezetek távoli elérését kiemelt biztonsággal kell(ene) megvalósítani annak érdekében, hogy megakadályozzák a jogosulatlan hozzáférést és az ebből adódó kiberbiztonsági és üzembiztonsági kockázatok kialakulását. Sok esetben a munkavállalók részére ezért (illetve a folyamatos és többműszakos jelenlét miatt) nincsen távmunka és távelérés kialakítva, az ilyen távoli bejelentkezések (a szükséges biztonsági kontrollok mellett) jellemzően a különféle támogatók és supportosok részére használhatók.

A fejlődési és tanulási lehetőség nehezebben teljesíthető egy olyan környezetben, amely legfőbb célja az állandóság, azaz a folyamatos és csaknem kőbe vésett paraméterek alapján történő működés fenntartása. Kísérletezni, kutatni, újabb és újabb technológiákat kipróbálni egy folyamatosan működő, termelő környezetben nem, vagy csak nagyon elvétve lehet. Ugyancsak ide tartozik az is, hogy a rendszerek életciklusa sem teszi szükségessé a folyamatos tanulást, egy felépített rendszert 10-20 évig kell működésben tartani és üzemeltetni. Ritkán van lehetőség új rendszerek létesítésével foglalkozni, ilyen esetekben viszont természetes, hogy az új rendszerhez szükséges kompetenciákat meg kell szerezni, majd azokat az életciklusnak megfelelően hosszú ideig és azonos szinten kell tudni alkalmazni.

Az érdekes és változatos munka elvárása is ugyanezen okokból nehezen teljesíthető bizonyos szerepkörökben, bár személyes tapasztalat, hogy a terepen dolgozó munkavállalók kifejezetten érdekesnek és változatosnak találják a különféle hibaelhárítási vagy javítási feladatokat, ahogyan egy TMK-s kolléga fogalmazott: „*Változatos, mert minden nap más valami romlik el".*

Az informatikusok motiválásáról szóló cikkében[46] Südi Miklós felvet egy nagyon plasztikus képet, amely szerint az informatikusokat motiválja az összetett, bonyolult és kihívásokkal teli feladat, és a cél elérése érdekében akár hegyeket is meg tudnak mozgatni, ha úgy érzik, azért lettek kiválasztva a feladat teljesítésére, mert éppen ők az egyedüliek, akik az adott problémát képesek megoldani. Véleményem szerint ez nem csak az IT munkatársakra jellemző, és általános motivációs eszköznek tekinthető a személy fontosságának és különleges kompetenciájának kiemelése és elismerése. Südi hozzáteszi, hogy „A sikeres megoldást követően azonban az elismerés mellett meg kell adni számára "*a gép forog az alkotó pihen* jóleső, teremtő érzését is". Az OT területen azonban a gép mindig forog és az alkotó soha nem pihenhet, a folyamatos készenlét és rendelkezésre állás mellett a teremtő érzés erodálódik és egyre kevésbé tud jóleső, ezáltal motivációs tényező lenni.

Ha nem a rendszertulajdonos és termelőszervezetek munkavállalóit, hanem az OT terület szolgáltatói szféráját vizsgáljuk, sokkal több a közös vonás az IT és OT szolgáltatásokat,

[46] *https://bitport.hu/motivacio-3-0-v00000011-informatikusra-szabva.html*

tanácsadást, tervezést, rendszerintegrációt nyújtó szervezetek között mind munkavállalói, mind pedig motivációs viszonyokban.

Ha a munkabért, mint motivációs eszközt tekintjük, hazai viszonyokban az OT terület egyértelműen hátrányba kerül az IT-val való összehasonlításban. Egy *„városi legendát"* is szeretnék itt szerepeltetni, mert nem csak a bérezéssel kapcsolatban tapasztalható hátrányokat, de a bérezés és a viselt felelősség viszonyát is jól ábrázolja.

„Egy vidéki és veszélyes vegyianyagokat felhasználó nagy termelőszervezetnél az egyik mérnök béremelési kérésének elutasítása során elhangzott, hogy az illető mérnök már így is annyit keres, mint egy sebészprofesszor, irreális tehát a bérigénye. A mérnök ezt úgy kommentálta, hogy ha egy sebészprofesszor hanyagul végzi a munkáját, egyszerre legfeljebb egy emberben tud kárt tenni, ő viszont akár ezerben is."

Talán ez a „városi legenda" jól ábrázolja, hogy az OT bizonyos területein a bérezés és a viselt felelősség nem feltétlenül arányos, így a jövedelem, mint motivációs tényező nem tud kellően hatékony lenni.

A fizetesek.hu oldal segítségével összehasonlíthatók a két terület fizetései. Az oldal adatai alapján összegyűjtésre kerültek jellemző IT és OT pozíciók, illetve a bérezések tól-ig határai.

OT pozíció	Br. bér (tól)	Br. Bér (ig)
Szervizmérnök	460 178 Ft	966 867 Ft
PLC-programozó	390 079 Ft	882 565 Ft
Villamosmérnök	425 045 Ft	872 349 Ft
Karbantartási mérnök	337 774 Ft	852 767 Ft
Energetikai mérnök	365 132 Ft	803 299 Ft
Folyamatmérnök	437 214 Ft	795 051 Ft
Energetikai berendezéskezelő	255 823 Ft	659 523 Ft
Technológus	350 321 Ft	653 281 Ft
Elektrotechnikus	271 638 Ft	624 838 Ft
Technikus	284 266 Ft	621 087 Ft
Szerviztechnikus	279 966 Ft	601 017 Ft
Villanyszerelő	281 306 Ft	596 117 Ft
Felülvizsgáló technikus	207 772 Ft	572 076 Ft
Elektroműszerész	314 640 Ft	566 304 Ft
Elektronikai műszerész	264 889 Ft	553 818 Ft
Villamossági szerelő	242 824 Ft	539 184 Ft
Javító, szerelő alkalmazott	193 460 Ft	526 841 Ft

IT pozíció	Br. bér (tól)	Br. Bér (ig)
IT-tervező	612 121 Ft	1 612 239 Ft
Vezető fejlesztő	691 024 Ft	1 552 780 Ft
IT Termékmenedzser	464 149 Ft	1 425 951 Ft
ABAP programozó	467 484 Ft	1 341 401 Ft
Oracle programozó	358 157 Ft	1 271 929 Ft
Szoftvermérnök	498 545 Ft	1 249 880 Ft
Python programozó	428 776 Ft	1 248 776 Ft
Informatikai biztonsági szakértő	424 633 Ft	1 207 160 Ft
DevOps mérnök	536 495 Ft	1 195 509 Ft
IT-tanácsadó	446 495 Ft	1 174 508 Ft
Business Intelligence Specialist	489 068 Ft	1 137 231 Ft
IT-projektmenedzser	477 344 Ft	1 137 060 Ft
Game developer	284 133 Ft	1 132 724 Ft
Data scientist	455 882 Ft	1 129 098 Ft
Javascript programozó	392 640 Ft	1 124 763 Ft
Scrum Master	541 912 Ft	1 109 936 Ft
iOS fejlesztő	359 103 Ft	1 106 242 Ft
Objective-C programozó	264 711 Ft	1 074 998 Ft
Java programozó	479 875 Ft	1 073 275 Ft
Backend developer	325 938 Ft	1 040 678 Ft
Rendszermérnök	458 612 Ft	1 027 389 Ft
SAP szakember	408 119 Ft	988 747 Ft
C programozó	339 038 Ft	972 945 Ft
ASP.NET programozó	401 967 Ft	962 176 Ft

Frontend developer	424 915 Ft	940 172 Ft
Android fejlesztő	424 413 Ft	913 996 Ft
PHP programozó	374 982 Ft	897 512 Ft
Hálózati adminisztrátor	363 959 Ft	895 249 Ft
Adatbázis adminisztrátor	352 873 Ft	882 766 Ft
Szervizmérnök	292 904 Ft	852 554 Ft
Honlaptervező	343 020 Ft	779 764 Ft
Rendszeradminisztrátor	325 367 Ft	772 735 Ft
IT/Műszaki támogató	320 577 Ft	745 746 Ft
IT auditor	276 727 Ft	731 098 Ft
Szerviztechnikus	285 625 Ft	667 091 Ft

OT és IT fizetési sávok összehasonlítása[47]

Egy régebbi háttérbeszélgetés során hangzott el a fizetési helyzetnek egy sommás összefoglalója: *„Az OT fizetések ott végződnek, ahol az IT fizetések kezdődnek*[48]**"**. Ez a kijelentés a korábbi években közelebb állt a valósághoz, mára az OT terület esetében is észlelhető, hogy emelkedtek a bérek, azonban az IT területen sokkal dinamikusabb a növekedés, és látható, hogy óriási különbségek tapasztalhatók a területek között.

Az OT terület szolgáltatói környezetében, a különféle ipari rendszerintegrátorok, tanácsadók, gépépítők, berendezésgyártók esetében a bérezés jobban hasonlítható az IT szektorban tapasztaltakhoz. Egy háttérbeszélgetés során elhangzott azonban, hogy az alapvetően óra- vagy napidíjas szolgáltatói (például fejlesztői) árak területén is észlelhető eltérés, például egy fejlesztő cég akár másfélszeres óra- vagy napidíjjal számolhat az IT-jellegű fejlesztések során, holott ugyanazon fejlesztői dolgoznak az OT vagy az IT célú fejlesztéseken. Egy másik háttérbeszélgetés alatt egy korábban vezetői pozíciót betöltő, magasan kvalifikált automatizációs mérnök számolt be arról, hogy amikor ügyféloldalról átváltott a szolgáltatói oldalra, a korábbi fizetéséhez képest csaknem másfélszeres szorzóval számolható munkabérrel kezdett az új munkahelyén.

A bérezéssel és egyéb motivációs tényezővel kapcsolatos problémák az utánpótlás szempontjából súlyos gondot okozhatnak.

Az Informatikai Vállalkozások Szövetsége (IVSZ) által készített szakpolitikai anyag[49] az informatikai szektorra vonatkozólag megemlíti, hogy a felmérésben válaszoló munkáltatók szerint a pályakezdők irreális bérelvárásokat támasztanak a munkaadókkal szemben. Háttérbeszélgetéseken keresztül gyűjtött információk alapján ez az OT területre is igaz, a kialakult bérversenyben egyre nehezebb a hazai vállalkozásoknak a munkaerő felvétele és megtartása. Előfordul, hogy a munkáltató alacsonyabb képzettségű és olcsóbb munkaerő alkalmazásával igyekszik az erőforrásproblémákat kezelni, azonban a rendszerek komplexitása miatt ez a stratégia hordozhat üzembiztonsági kockázatokat, a rendszert felépítő és a legapróbb rendellenesség jeleit is felismerő munkatársak minőségi pótlása egyáltalán nem megoldható

[47] *Az adatok a fizetesek.hu oldalról származnak és a 2022 augusztusi időszakot tükrözik*

[48] *Kőszegi László, OT szakértő*

[49] *https://ivsz.hu/wp-content/uploads/2021/06/ginop-5-3-5-kutatasi-zarojelentes-szakpolitikai-ajanlas-informatika-agazati-munkaeropiaci-tunetterkep-ivsz-enrawell.pdf*

ezzel a módszerrel és jelentős képességvesztés következhet be. Ha jelentőssé válik az erőforráshiány, az további pluszmunkát és terhelést jelent a területre. A termelésnek, gyártásnak és a folyamatoknak működnie kell, ez pedig csak többletterhelés mellett tud megvalósulni, ezáltal tovább csökkenhet a munkatársak motivációja és tovább nőhet a fluktuáció.

Az OT viszonylagos állandósága mellett nem csak a rendszerek, hanem a kezelőszemélyzet esetében is számolni kell az elöregedés jelenségével, amely szoros kapcsolatban áll az utánpótlás kérdésével. A hosszú évek alatt megszerzett és az adott rendszerre vonatkozó mélyszintű kompetencia és tapasztalat a szervezet számára elveszhet, ha a tudást birtokló kezelőszemélyzet például nyugdíjba megy, vagy akár egészségügyi okokból kényszerül távozásra. Sok esetben a működtetéshez és karbantartáshoz szükséges tudás csak a fejekben található meg, akár egy-egy idősebb kolléga távozása közép- és hosszútávon hatással lehet a rendszerek üzembiztos működésére.

A nagyvállalati informatika erősen törekedik a standardizálásra és a munkafolyamatok lebontására, ezért viszonylag jól képes kezelni a fluktuációt, azonban az OT esetében az egyedi, vagy akár több beszállítótól és közreműködőtől származó rendszerek miatt a standardizálásra nagyon kevés lehetőség van, a komplex, egymásra épülő munkafolyamatok pedig a lebontást teszik meglehetősen problémássá, így a fluktuáció is sokkal fájdalmasabban érintheti az OT területet.

A már 15-20 éve ugyanazon munkáltatónál dolgozó, közepesen és magasan kvalifikált, 50-60 év közötti korosztály esetében érdekes - és véleményem szerint az OT világra nagyon is jellemző-, a motivációval összefüggő jelenség is tapasztalható. Néhány háttérbeszélgetésben elhangzott, hogy ezen munkavállalók a rendszerhez és munkaáltatóhoz rögzültnek vélik magukat, amely egészen különös, kettős állapotot eredményez: ugyan nem érzik jól magukat a jelenlegi pozíciójukban az adott munkáltatónál, azonban a felépített, hosszú évek vagy évtizedek óta működtetett és a *sajátjának tekintett* rendszerek iránt érzett felelősség miatt nem törekednek munkáltatót váltani. Ezekben az esetekben a munkáltatóval szembeni lojalitás háttérbe szorult, a személy, valamint az általa működtetett technológiák és folyamatok között kialakult kötődés szolgál hajtóerőként és egyfajta hivatástudat alakulhat ki. *Brandeis* szerint a hivatás olyan foglalkozás, amelyet a személyes igények háttérbeszorításával és főként mások szolgálata érdekében űznek és ahol nem a pénzbeli megtérülése jelenti a siker mértékét. Ez véleményem szerint illeszkedik az ilyen esetekre, azonban az ilyen a hivatástudattal rendelkező személy nem közvetlenül a szervezetet, hanem inkább a működtetett rendszereket és folyamatokat szolgálja. *Flexner*[60] megközelítésében a hivatást űzők a „társadalmi jó" elősegítésén munkálkodnak, és ha az üzembiztonságot nem csupán az üzleti elvárások oldaláról tekintjük, hanem figyelembe vesszük a környezet és az emberi élet és egészség megóvásának szándékait, ezen munkavállalók esetében nem csupán pozícióról vagy állásról, hanem hivatásról és hivatástudatról beszélhetünk. A rendszerhez és a munkáltatóhoz való rögzültség egy másik, talán kevésbé szerencsés példája, ha a már 15-20 éve ugyanazon munkáltatónál dolgozó munkavállaló a tudását és tapasztalatát annyira lokalizáltnak és specializáltnak érzi, hogy úgy véli, ha akarna

[50] *Flexner hat olyan kritériumot sorol fel, amelyek alapján egy foglalkozás hivatásnak tekinthető. A hivatás intellektuális és nagy felelősséggel járó; tanult szakma, amely széleskörű ismereteken és nem rutinon alapul; inkább gyakorlati mintsem akadémikus; technikái megtaníthatók és ez jelenti a szakmai képzés alapját, belsőleg jól szervezett; és az altruizmus motiválja. (Forrás: http://real.mtak.hu/93616/1/ht201834_129-136.pdf)*

sem tudna munkáltatót és munkát váltani. Ilyen esetekben súlyos belső frusztráció alakulhat ki, amely a motiváció, illetve az érzelmi stabilitás megingásához és erodálódásához vezethet.

Képezhetőség, tudatosság, fejleszthetőség

Az információtechnológia robbanásszerű fejlődése és a digitalizáció felgyorsulása a szemünk előtt változtatja meg az IT világát. Az újabb és újabb technológiák megjelenése és azok rendkívül gyors alkalmazása miatt az IT területeken dolgozók folyamatos tanulási kényszerben vannak, akár csak 1-2 év kihagyás is komoly versenyhátrányt jelenthet a számukra.

Az OT esetében is jelen van az innováció, azonban a fejlesztések üteme és az új technológiák alkalmazása sokkal lassabb. Talán a legjobb példa erre, hogy az informatika világában ma majdnem elképzelhetetlen, hogy negyven éves kommunikációs protokollt alkalmazzon valamely technológia, míg az OT esetében a jelenleg is leggyakrabban használt MODBUS kommunikációs protokoll 1979-ben jelent meg[51] és nehéz találni olyan nagyobb OT környezet, amelyben ne működnének MODBUS kapcsolaton keresztül kommunikáló berendezések. Az új technológiák adaptálása sokkal lassabb az OT világban, így a rendszertulajdonosok OT területein dolgozók esetében a folyamatos tanulási kényszer első sorban nem az új technológiák és kompetenciák elsajátítására, hanem a működtetett rendszerek, a rendszerek, az összefüggések és egymásra hatások egyre mélyebb megismerésére koncentrálódik. Nincs szükség és lehetőség arra, hogy újabb és újabb technológiákat ismerjenek meg, a fejlődés és tanulás a hosszú életciklusú rendszerek minél mélyebb szintű megismerésére és a komplex folyamatok és függőségek megértésére korlátozódik. Ez egyébként akár a szervezeten belüli pozícióváltásra is igaz, míg az IT-ban könnyebben mozognak a munkavállalók az egyes részterületek között, és válik egy fejlesztőből esetleg üzemeltető, biztonsági szakember vagy projektvezető, alkalmazásüzemeltetőből hálózati üzemeltető, infrastruktúra szakértőből csapatvezető, addig az OT világában az adott részterületen belül maradva a kompetencia növelése mellett is a részterület marad a tevékenység fókusza.

A belső, szervezeten belüli karrierív sokkal kötöttebb, például egy erőművi rendszeren belül a gépész szakterület munkavállalója előbb kazángépész, majd erőművi gépész majd blokkgépész lesz, egyre több területi rendszert és azok összefüggéseit átlátva és egyre több felelősséget felhalmozva. Ez a karrierív akár 15-20 évet is felölelhet és látható, hogy a tanulási folyamat jellemzően a részterületen belül, a hosszú életciklusú rendszerekre korlátozódik.

Az IT esetében rengeteg lehetőség adódik a tanulásra és más, újabb kompetenciák elsajátítására. A hivatalosan, például gyártói szaktanfolyamok és tréningek mellett bármely munkavállaló akár a szabadidejét felhasználva is könnyen hozzáférhet újabb és újabb tudásanyagokhoz, például az online oktatásokon keresztül.

A legnépszerűbb online oktatási platform, az Udemy jelenleg 185 ezer képzést kínál, ezek jórésze valamely IT területre célzott oktatás. A képzések gyakorlatilag a kezdőtől a haladó tudásszintig tartanak, megfizethető és elérhető árakon van lehetősége az érdeklődőnek fejlesztenie magát.

---

[51] *A MODBUS TCP/IP változata 23 éve, 1999-ben jelent meg.*

Példa az Udemy népszerű IT-jellegű kurzusaira	
Képzés	**Hallgatószám**
Python programozás	35 712 243
Web fejlesztés	11 142 118
Machine learning	6 972 151
SQL	5 777 328
AWS certification	5 833 549
Ethical Hacking	10 719 512
Cyber Security	3 903 114
Photoshop	10 730 388
Grafikai tervezés	3 317 239

Udemy online oktatási portál, népszerű IT kurzusok

Az IT területen sokkal egyszerűbb olyan újabb tudásanyag vagy kompetencia összegyűjtése és megszerzése, amellyel szervezeten belül vagy a szervezeten kívül területet, specializációt vagy pozíciót tud váltani a munkavállaló. Az OT esetében ez az út sokkal rögösebb és jobban az adott szervezethez kötött lehet.

Szaktanfolyamok, gyártói képzések az OT területen belül is léteznek. Egy szervezet működtethet olyan berendezéseket, amelyek gyártója és/vagy szállítója elvárja, hogy csak olyan kezelő- és karbantartó személyzet üzemeltesse a rendszereket, amely részt vett a hivatalos gyártói oktatáson, és képzésen, valamint megszerezte a kompetenciát igazoló szükséges minősítéseket. Jellemzően az ilyen képzések főleg az új belépők esetén elvártak, de előfordulhat, hogy a gyártó vagy szállító periodikusan megismételteti a tréninget a személyzettel, azonban az ilyen ismétlő oktatások a meglévő technológia optimálisabb és üzembiztosabb kihasználására fókuszálnak.

A nagy rendszertulajdonosok, gyártó- és termelő szervezetek sok esetben belső képzési rendszert működtetnek. Egy új belépőnek meg kell szereznie a helyi rendszerekre vonatkozó tudást, hiába rendelkezik valaki például elektrikus szakvégzettséggel, attól még nem nyúlhat hozzá a szervezet rendszereihez, nagyon komoly, többlépcsős és általában vizsgákkal szakaszolt képzési programot kell végig csinálnia ahhoz, hogy önállóan munkát végezhessen. Nem ritka, hogy egy-másfél évig csak felügyelet alatt végezhet valaki munkát, a betanulási időszak tehát sok esetben jóval hosszabb, mint az IT esetén.

A nagy szervezetek működtethetnek átképző programokat, amelyek az utánpótláshiány megoldására fókuszálnak. Az ilyen programok előképzettség nélkül is nyitva állnak az érdeklődők előtt és az érdeklődő már a képzés időszakában is munkaviszonyba kerül a szervezetnél. Ilyen program például a Veolia Akadémia[52], ahol egy kb. egy hónapos felkészítő szakasz után 6-9 hónapos, gyakorlatorientált képzés következik, ahol a résztvevőt a Veolia saját szakemberei a különféle erőművi környezetekben oktatják és a hallgatók elsajátíthatják a konkrét munkafolyamatokat, megtanulhatják a különféle rendszerek és berendezések kezelését. A belső képzések nagyon nagy jelentőséggel bírnak az OT területen belül, a munkavédelmi és

[52] *https://www.veolia.hu/hu/hirek/elindult-veolia-akademia-szakmai-kepzest-es-stabil-munkahelyet-kinal-veolia-csoport*

üzembiztonsági okok miatt sok esetben évenként meg kell ismételniük a munkavállalóknak a különféle képzéseket, illetve a szervezeten belüli mozgásokhoz is általában szükség van valamilyen belső képzésre, de látható, hogy a képzések jellemzően a szervezet rendszereire és azok mélyebb megismerésére fókuszálnak, erősen lokalizáltak és specifikusak.

A kisebb szervezetek jellemzően nem tudnak belső programokat működtetni, esetükben az OT munkavállalók szakmai fejlődése még inkább elmaradhat egy IT területen foglalkoztatottétól, aki akár önerőből és a szabadidejét felhasználva maga gondoskodhat a képzéséről és akár teljesen új szakterületi kompetenciákat is elsajátíthat.

Egy kisebb termelőszervezet technológiai vezetője a háttérbeszélgetésen úgy fogalmazott, hogy minden megüresedett pozícióval kapcsolatban meghirdetik a pályázatot, de jellemzően nem tudnak új embert felvenni a pozícióra, hanem megpróbálják azt a szervezeten belülről betölteni, mert a már ott dolgozók legalább valamennyire ismerik a folyamatokat és a rendszereket, ezzel azonban más-más területeken válik gazdátlanná egy-egy munkafolyamat és ezt az erőforráshiányt tologatják akár évekig. „*Végül az egész begyűrűzik és lesz néhány terület, ahol hiányos tudással és csak félig-meddig dolgoznak, aztán jönnek a hibák és a minőségromlás*". Nem csak az OT-ra jellemző az a jelenség, hogy „ideiglenesen" vagy tűzoltás jelleggel igyekeznek az erőforráshiányt azzal megoldani, hogy valamely másik területről toboroznak „önkéntest" a tevékenység ellátására, azonban az OT területen az ilyen megoldások akár az üzembiztonságot is fenyegethetik. Az OT munkavállalók ezért általában nem jól tolerálják az ilyen erőforrásáthelyezéseket és motivációt romboló kényszerként élik meg a hasonló szituációkat. Az „önkéntes" toborzással kapcsolatban egy beszélgetőpartner filmes hasonlattal élt: „*Úgy vagyunk vele, mint Rasczak hadnagy a Csillagközi Invázió című filmben, amikor pótolnia kell az egyik szakaszparancsnokot: - Rico! Kell nekem egy tizedes! Maga lesz az haláláig, vagy amíg jobbat nem találok!*"

Képzés és fejlesztés szempontjából az OT területen figyelembe kell venni a felhasználók differenciálódását. Ahogy korábban már megfogalmazásra került, az OT felhasználók és munkavállalók között fehér- és kékgalléros személyzet is megtalálható. Véleményem szerint a két terület sokkal jobban képes együttműködni a másikkal, mint más foglalkozások esetében. A mérnök is gyakran munkaruhában és védőfelszerelésben dolgozik a terepen, az egymásra utaltság és a terepi viszonyok miatt a munkaruhák színe „*kifakulhat*", ha a fizikai és szellemi munkakörök dolgozói szorosabb együttműködésben tevékenykednek. Az oktatás és képzés szempontjából azonban mindenképpen figyelembe kell venni a munkavállalói rétegek közötti különbségeket. Egy vegyianyagokkal dolgozó termelőszervezetnél a korábban csak a szellemi munkakörökre célzott felhasználói biztonságtudatossági programot kiterjesztették a fizikai dolgozókra is, azonban hiába szabták testre az oktatási anyagot, a program nem volt sikeres, nem tudta elérni a munkavállalókat. A vállalat ekkor taktikát változtatott, a vállalati biztonságtudatossági képzést elbújtatta egy céges családi napi rendezvénye mögé és beágyazta a család és a gyermekek digitális biztonságával, internet használatával kapcsolatos előadásokba. A korábban elutasító munkavállalók is érdeklődővé váltak, hiszen mindenkinek fontos a gyermekek és a család védelme, a program így képes volt felkelteni az érdeklődést és képes volt alapvető kiberbiztonsági tudatossággal kapcsolatos elemeket átadni a munkavállalóknak. A későbbiekben már családi nap nélkül is jobb hatékonysággal lehetett a szükséges tudást és információkat átadni a munkavállalóknak, egyszerűen csak a kontextusokat kellett úgy alakítani, hogy a felhasználó kötni tudja az ismereteket a saját magánéletének digitális biztonságához. A példából talán látható, hogy a két réteg különbsége

ellenére is lehetőség van képzéseket megvalósítani, ha figyelembe veszik a munkavállalói rétegek közti eltéréseket.

Kiberbiztonsági szempontból az IT terület képzése sokkal egyszerűbb, bár a program sikere nagyban függ a képzési anyag minőségétől és az általános szervezeti kultúrától. Alapvetően egy IT munkakör esetén már elvárássá vált valamilyen kiberbiztonsági jártasság, a biztonsági szabályzatok a nagyobb szervezetek esetében rendelkeznek a szerepkörökhöz kötött kiberbiztonsági oktatásokkal és képzésekkel kapcsolatban. Mivel a kiberbiztonság jelenleg sokkal erősebben kötődik az informatikai területekhez, ezért a kiberbiztonsági képzések már beépülhettek a folyamatokba, míg az OT területen még az is magyarázatra szorul, hogy egyáltalán miért van szükség ilyen képzésekre. Az IT esetében a főbb szakterületeknek megvan a maga kiberbiztonsági tevékenységi köre, például a fejlesztők esetében a biztonságos kódolás (*secure coding*), vagy az üzemeltetők esetében a biztonságos üzemeltetés és *hardening*, de az OT esetében a szerepkörökhöz és tevékenységekhez kötött kiberbiztonsági funkciók még nem tudtak kialakulni. Az OT esetében a kiberbiztonsági alapok is hiányoznak és nem állnak rendelkezésre olyan szabályzatok sem, amelyek elvárnák az ilyen jellegű képzéseket és oktatásokat.

Az OT területen már az oktatásszervezés is nagy nehézségekkel küzd, a szigorúbb és több műszakos munkarend miatt az élőszereplős oktatások megszervezése is nehézkes, mivel úgy kell az oktatások időpontjait megszervezni, hogy azok igazodjanak a munkabeosztásokhoz és műszakokhoz. Ezért sok esetben a szervezetek törekednek az élőszereplős oktatások minimalizálására és igyekeznek az elektronikus/online képzési forma preferálására, azonban előfordul, hogy az ilyen képzések eredményessége és hatékonysága elmarad a hagyományos, fizikai jelenlétet követelő oktatásokétól.

Az IT mára jellemzően nagy hangsúlyt helyez a biztonsági tudatosításra és a biztonságtudatossági tevékenységekre, azaz olyan oktatási és képzési tevékenységekre, amelyek célja az informatikai környezetek, a digitalizációs technológiák és a munkafolyamatok biztonsági kihívásait jól ismerő, a fenyegetéseket felismerő, a megelőzéshez és elhárításhoz tevékenyen hozzájáruló magatartási forma és felhasználói attitűd megteremtése, illetve hosszú távú fenntartása. Az OT területen ilyen jellegű oktatási és képzési tevékenység jellemzően nincsen és ez a hiányosság súlyosan akadályozza a terület kiberbiztonsági érettségének növelését.

Míg az informatikában mára vezetői szinten is elfogadottá vált az a vélekedés, hogy a képzés és oktatás az egyik legfontosabb és legköltséghatékonyabb védelmi intézkedés, addig az OT területen a vezetői szinteken sem jelent meg a biztonságtudatossági képzések igénye. Sok esetben ennek maga a terminológia is az oka lehet, a biztonság az OT területen az üzembiztonságot (*safety*) jelenti, amelynek minden körülmények között meg kell felelnie a szervezetnek, azaz amikor egy vezető biztonságtudatosságról hall, számára ez egy mindig is teljesített követelmény volt, hiszen a rendszerek és folyamatok biztonságos működtetése elvárt és garantált. Feltehetően érdemesebb lenne kiberbiztonsági tudatosításról, vagy a terület kiberbiztonsági érzékenyítéséről beszélni, amely kifejezések sokkal értelmezhetőbbek lehetnek az OT világában.

Ha a terminológiai akadály sikeresen leküzdésre került, a kiberbiztonsági tudatosítás vagy érzékenyítés tevékenység kialakításának másik nagy hátráltatója a hamis biztonságérzet vagy hamis biztonságtudat, amely az egyik legsúlyosabb és szervezeti-szintű kiberbiztonsági kockázat. Ez olyan „testképzavar”, amelyben a szervezet jellemzően hiányos információk és régi

berögződések alapján nem ismeri fel a saját kitettségét, nem észleli a fenyegetettséget, vagy úgy vélekedik, hogy az egyáltalán nem érinti, esetleg úgy gondolja, hogy a megfelelő intézkedésekkel már elviselhető szintig csillapította a kockázatokat. Röviden tehát a szervezet vagy terület azt érzi, hogy a működése biztonságos, de valójában nem az.

A szervezeti kultúra szempontjából az OT esetében még a magasabban kvalifikált, „*fehérgalléros*" munkakörökben is berögzült az a nézet, hogy az ipari, irányítástechnikai, vezérléstechnikai vagy egyéb automatizációs rendszerek védett és zárt környezetben üzemelnek, azokhoz legfeljebb csak fizikailag lehet jogosulatlanul hozzáférni, ezért a kiberbiztonságra és a kiberbiztonsági érzékenyítésre nincsen szükség. Sok esetben találkozhatunk azzal a hárítással, hogy az OT rendszereknek nincsen internet kapcsolata, ezért a kiberfenyegetettségek nem jelentenek kockázatot, tehát a logikai védelemre sincsen szükség. Ez az álláspont egyértelműen helytelen, számtalan incidens bizonyította, hogy ma már az OT rendszerek sem zártak, nem szigetüzemben működő infrastruktúraelemekből felépülő architektúrák. A jogosulatlan hozzáférés nem csak fizikailag, de logikailag is megvalósítható ezért a logikai védelemre és a kiberbiztonságra egyértelműen szükség van az OT területen is. A modern OT infrastruktúrák és az Ipar 4.0 elvárják, hogy az OT rendszerek együttműködjenek az IT terület alkalmazásaival, rendszerek és a rendszerek közötti kapcsolatok pedig kihasználható sérülékenységeket hordozhatnak. Ugyancsak el szokott hangzani, hogy mivel internet kapcsolat nincsen, legfeljebb az IT/irodai hálózatból lehet hozzáférni az OT rendszerekhez, az irodai hálózatot pedig az IT biztonsági tevékenységek miatt megbízhatónak lehet tekinteni. Ez az álláspont is helytelen, **az OT szempontjából *minden hozzáférést biztosító hálózatot* idegen és megbízhatatlan hálózatnak kell tekinteni**, még akkor is, ha az a szervezet saját irodai vagy IT hálózata. Még az egyes OT hálózati szegmensek és zónák közötti kapcsolat esetében is kontrollálni kell a hálózati forgalmakat és az adott zóna szempontjából minden egyéb OT zónát is javasolt idegennek tekinteni.

A hamis biztonságérzet feloldása az OT területen kiemelt fontossággal bír, mert blokkolja a szükséges humán, adminisztratív és technikai védelmi intézkedések megvalósítását. A hamis biztonságérzet feloldását a vezetői szinten kell megkezdeni. Erre a kiberbiztonsági érzékenyítés a *második* legjobb (és javasolt) módszer, a vezetőket célzó kiberbiztonsági tudatosítás képes lehet megismertetni a vezetőkkel a vonatkozó fenyegetéseket és kockázatokat és képes lehet a vezetői elkötelezettség létrehozására, amely az alapját képezi az OT kiberbiztonsági képességfejlesztésének. Sajnos az *első* és leghatékonyabb (de nem javasolt) módszer egy incidens elszenvedése, amely azonnal és végérvényesen megszünteti a hamis biztonságérzetet.

Látható tehát, hogy a kiberbiztonsági érzékenyítés kiemelt fontossággal bír az OT világában. Egyrészt az érzékenyítés nélkül a vezetői réteg kiberbiztonság iránti elkötelezettsége nem alakítható ki, másrészt az elkötelezett vezetők által létrehozott humán, adminisztratív és technikai védelmi intézkedések sem fenntarthatóak, ha az OT felhasználói rétege ebben nem válik együttműködő partnerré, és nem alakul ki az OT környezetek, a kiberfizikai technológiák és a munkafolyamatok biztonsági kihívásait jól ismerő, a fenyegetéseket felismerő, a megelőzéshez és elhárításhoz tevékenyen hozzájáruló magatartási forma és felhasználói attitűd.

Záró gondolatok

Az IT/OT konvergencia jelenti a kulcsot az ipar digitális transzformációjához. A legtöbb esetben azonban csak technológiai és üzleti fókusszal kutatják a területet, holott a hatékony

együttműködés nem elképzelhető a területek szabályozási környezeteinek és munkavállalóinak szervezeti szintű integrációja nélkül.

Egy konferencia háttérbeszélgetésen elhangzott vélemény szerint az informatikus kollégák számára az OT terület munkavállalói a *szentineléz* törzshöz hasonlíthatnak, akik az utolsó, izolációban élő „érintetlen", vadászó-gyűjtögető életmódot folytató, kőkorszaki társadalmak közé tartoznak, és akik érintetlenségüket meglehetősen harciasan védelmezik. Az analógia sértő lehet ugyan, de mint minden analógia, ez is hordoz valós tartalmat.

A tanulmányban több esetben is előfordul, hogy az IT és OT közötti különbségek elmaradásként, hátrányként vagy hiányosságként kerülnek értékelésre. Ez az IT oldaláról megáll(hat)ja a helyét, azonban, ha az OT területet a korábbi izoláción belül vizsgáljuk, az OT „társadalma" ezeddig harmóniában élt a saját világával, amit tehát egy informatikus esetleg elmaradásként érzékelhet, az az OT számára a megszokott, bevett és üzembiztos. Az OT a *szentineléz* törzshöz hasonlóan tud ugyan egy furcsa és idegen külvilág létezéséről, azonban azzal korábban egyáltalán nem foglalkozott és a külvilág is igyekezett nem megzavarni az életüket. A *szentineléz* törzshöz hasonlóan az OT is korszakokat élt túl azzal, hogy megvédte életmódját és életterét, azonban az analógia itt véget ér, a külvilág és a digitális transzformáció betört az OT világába, és a változás már nem elkerülhető.

A *szentinelézek* gyakorlatilag mindenkit lenyilaznak, akik megzavarják életüket, mondhatni mereven elutasítók a külvilággal szemben, de az OT ezt már tovább nem tudja megtenni, azonban a digitális transzformáció sem járhat azzal a kockázattal, hogy a külvilág olyan betegségeket hurcoljon az OT közösségébe, amely ellen a törzs immunrendszere nem tud védekezni. Pedig a digitális transzformáció legnagyobb kiberbiztonsági kockázata pont ebből áll, ahogyan a *szentinelézek* immunrendszere sem tudna védekezni egy modern ember számára legfeljebb kellemetlenséget okozó influenzával szemben, úgy az OT terület sem képes az információtechnológiai rendszerek kiberbiztonsági kockázataival kibővült saját kockázatait kezelni. Az IT/OT konvergencia tehát azzal jár, hogy az IT-nak az OT kockázataival, az OT-nak pedig az IT kockázataival együtt kellene tudnia létezni. Ez óriási kihívás elé állítja mindkét terület képviselőit, ezek a kihívások pedig első sorban nem technológiai védelmi eszközökkel, hanem sokkal inkább a humán és az adminisztratív védelem megerősítésével kezelhetők. A technológiai sérülékenységek legtöbbje szabályzati vagy humán okokra vezethető vissza, például azért nem biztonságos egy OT protokoll (vagy rendszer), mert nincsen olyan szabályozás és elvárásrendszer a szervezeten belül, amely elvárná, hogy az legyen, illetve meghatározná, hogyan legyen az.

A legtöbb OT környezetben egyáltalán nem foglalkoznak a kiberbiztonsági kockázatokkal, hiszen a békés izloáció évtizedei alatt ez az igény soha nem merült fel, azonban a digitalizáció és a konvergencia igénye ezt a hiányosságot felszínre hozta és elvárja, hogy pótlásra kerüljön. Humán oldalról ezeket az igényeket meglehetősen nehéz kielégíteni, az OT terület még nem termelte ki a saját kiberbiztonsági szakértői rétegét, ezt az űrt jelenleg még az IT biztonsági szakembereknek kell betöltenie.

Az IT/OT konvergencia létrejöhet papíron, összekapcsolhatóak a rendszerek, létrejöhet adatvezérelt gyártás vagy akár virtuális gyárak is elkezdhetnek üzemelni, de valójában a konvergencia nem tud addig élhetően megvalósulni, amíg a területek nem hajlandóak egymástól tanulni. Az OT-nak el kell fogadnia, hogy az izolációs korszaknak vége és nyitnia kell a külvilág felé. Le kell tenni az íjat és el kell sajátítania az életben maradás új eszköztárát, amelyre a „modern" világban szüksége van, az IT-nak pedig úgy kell tudnia a tudástranszfert

megvalósítani, hogy az OT érintetlensége csak a szükséges mértékben sérüljön és megőrizhesse önazonosságát és integritását. A felelősség közös, az IT/OT konvergencia csak a területek közötti magasfokú együttműködéssel valósítható meg.

Köszönetnyilvánítás

A tanulmány nem jöhetett volna létre azon kiváló szakemberek segítsége nélkül, akik évek óta igyekeznek hidat verni az IT és az OT területek közötti szakadék felett.

Kiemelt köszönet illeti azon kollégákat, akik értékes tanácsaikkal segítették a tanulmány elkészítését:

- *Görgey Péter, SeConSys*
- *Bóna Péter, Com-Forth Kft.*
- *Papik Gábor, ProcessControlConsulting kft.*
- *Kőszegi Rexia László, industrial hacker*

Szeretnénk köszönetet mondani a SeConSys szakmai együttműködés munkatársainak is, akik példaértékű tevékenységükkel utat mutatnak a szakmának. A villamosenergia szektor és a kritikus infrastruktúrák védelmével kapcsolatos szakértői munkájuk bebizonyítja, hogy az IT/OT konvergencia nem csak egy szervezeten belül, de szektoriális szinten is megvalósítható.