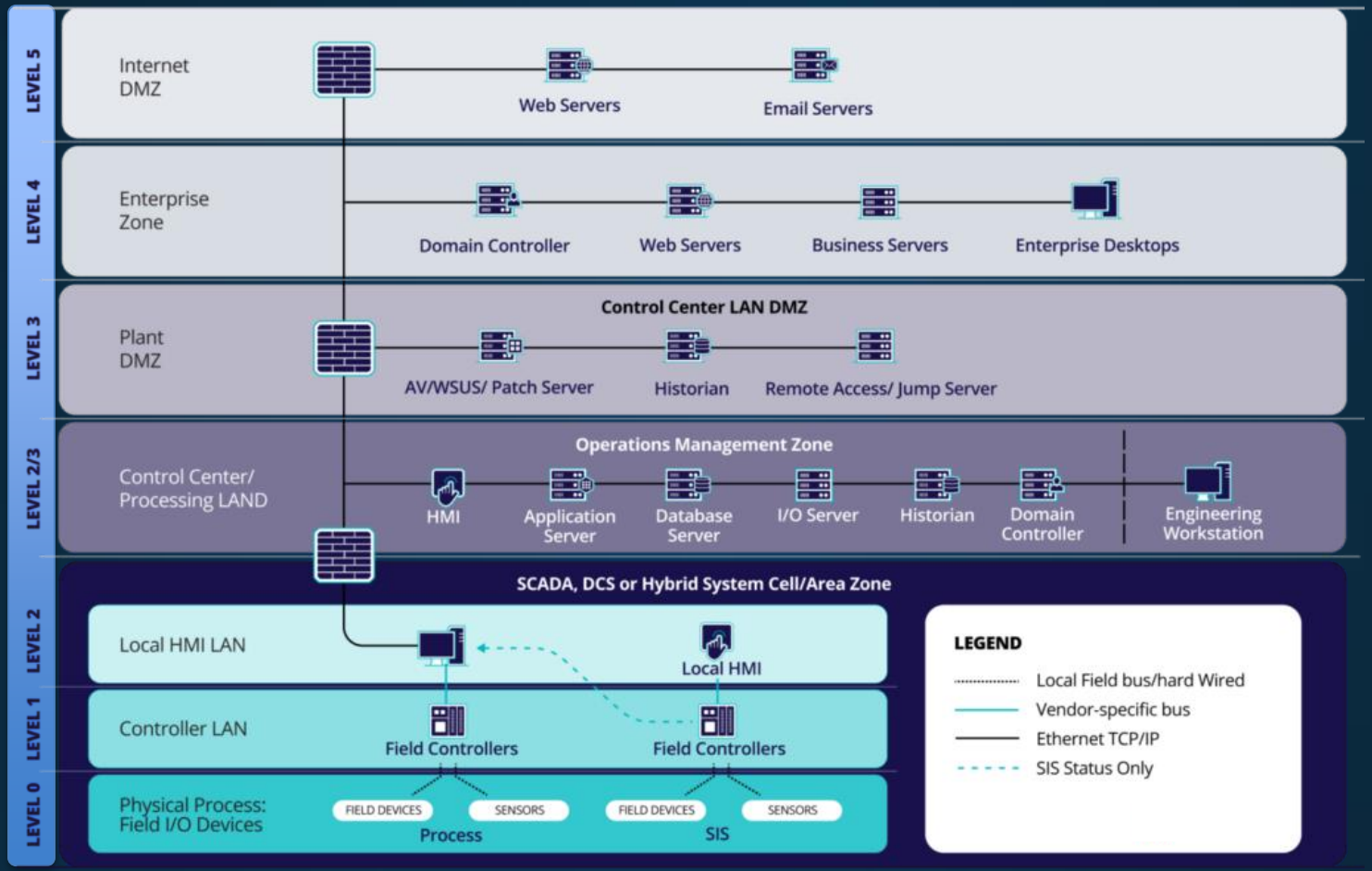
ALVERAD
TECHNOLOGY FOCUS

NIS2

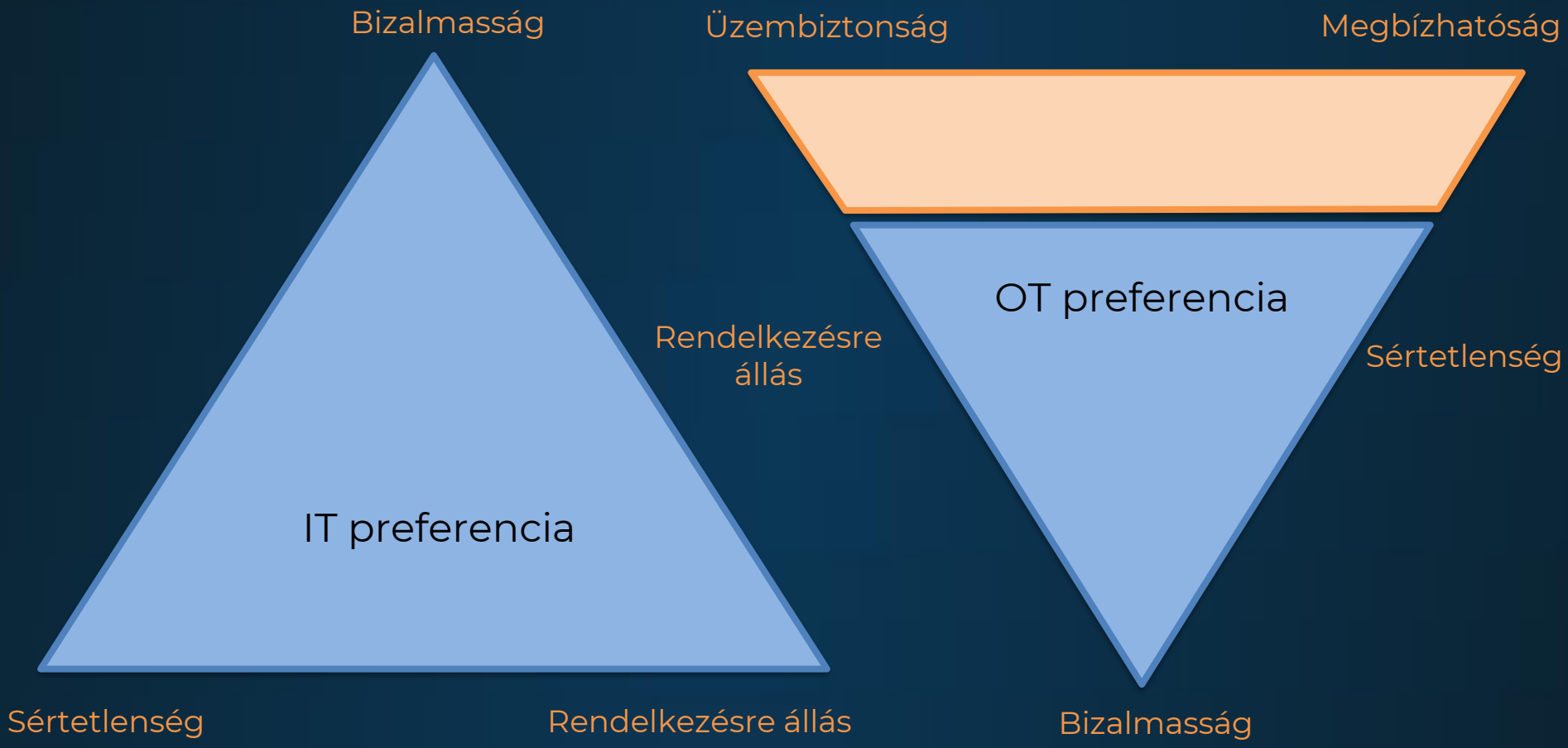
az ipari rendszerek szemszögéből

2024. 12. 06.

Elektronikus Információs Rendszer – OT rendszer (is)



IT ≠ OT

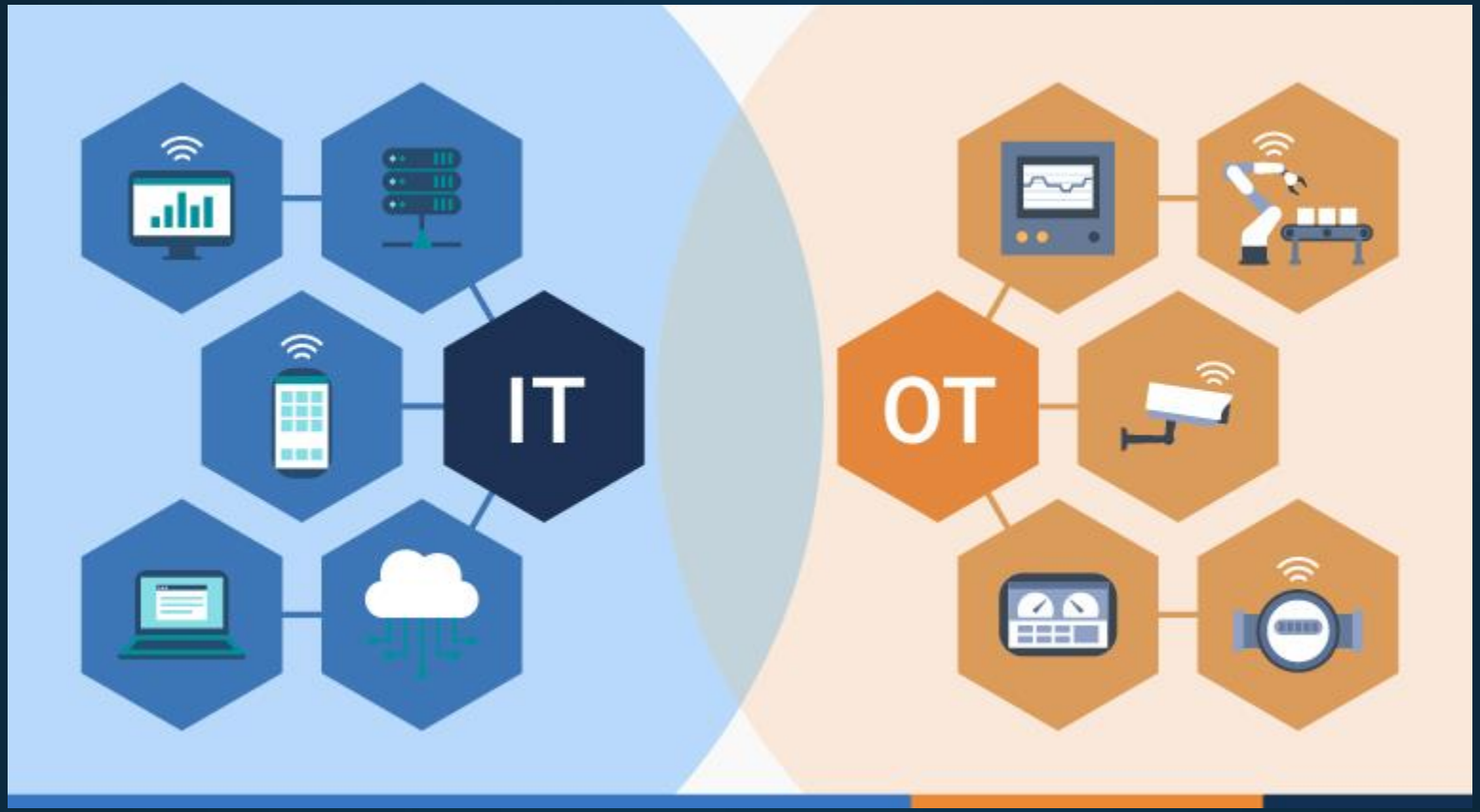

Bizalmasság
IT preferencia
Sértetlenség
Rendelkezésre állás
Üzembiztonság
Megbízhatóság
OT preferencia
Rendelkezésre állás
Sértetlenség
Bizalmasság

IT ≠ OT

	Information Technology (IT)	Operational Technology (OT)
Összetevők, komponensek	Szerverek, munkaállomások, adattárak, felhő, biztonsági eszközök, mobileszközök, webalkalmazások, hálózati eszközök.	PLC/DCS, SCADA, adatgyűjtők, szenzorok, motorok és egyéb terepi eszközök, protokollkonverterek, gyártásirányítók.
Életciklus	3-5 éves életciklus	10-25-50 éves életciklus
Működés	Együttműködő, összekapcsolt alkalmazások, rendszerek és hálózatok összessége.	Szigetrendszerű, önálló működés.
Biztonsági koncepció	„Data first”, adatközpontú szemlélet.	„Process first”, folyamat központú szemlélet.
Személyzet	Rendszergazdák, IT mérnökök, biztonsági mérnökök és felhasználók. „Fehérgalléros” munkavállalók.	Operátorok, karbantartók, terepi mérnökök és automatizálási mérnökök. „Fehér- és kékgalléros” munkavállalók.
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.
Elhelyezkedés	Centralizált rendszerek, adatközpontokban, szerverszobákban.	Decentralizált és akár elszigetelt működés, nagy távolságok, és terepi viszonyok.

IT ≠ OT - egységes értékelés ?

IT: NIST 800-53



OT: NIST 800-82

IT ≠ OT - egységes értékelés !

IT: NIST 800-53

OT: NIST 800-82

Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

IT: NIST 800-53

- Az érintett szervezet automatikus mechanizmusokat használ a naplóbejegyzések felülvizsgálatának, elemzésének és jelentési folyamatainak integrálására.

OT: NIST 800-82

- Amennyiben az EIR nem támogatja a naplóbejegyzések gyűjtését, a naplóbejegyzések felülvizsgálatát az EIR rendszerbiztonsági tervében meghatározott rendszerességgel manuális ellenőrzéssel kell végezni.

- **Magyarázat:** A helyettesítő védelmi intézkedések magukba foglalhatják például a kézi mechanizmusokat vagy eljárásokat. Olyan eszközök esetében, ahol a naplóbejegyzések gyűjtését nem tudják megvalósítani, időszakos manuális felülvizsgálatra lehet szükség.

Eszköz zárolása

IT: NIST 800-53

- Meghatározott időtartamú inaktivitás után vagy a felhasználó erre irányuló lépése esetén, az eszköz zárolásával megakadályozza az EIR-hez való további hozzáférést.

OT: NIST 800-82

- Abban az esetben, ha az EIR nem rendelkezik automatikus zárolási képességgel, vagy vészhelyzetben azonnali kezelői reakcióra van szükség, ezért zárolással nem lehet megakadályozni az EIR-hez való hozzáférést, a szervezet kockázatértékelés alapján helyettesítő intézkedést vezet be, amelyet dokumentál az EIR rendszerbiztonsági tervében.

Az elektronikus információs rendszer helyreállítása és újraindítása

IT: NIST 800-53

- Az érintett szervezet a meghatározott helyreállítási idővel és helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő időtartam alatt gondoskodik az EIR utolsó ismert, üzembiztos állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

OT: NIST 800-82

- Az érintett szervezet a meghatározott helyreállítási idővel és helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő időtartam alatt gondoskodik az EIR utolsó ismert, üzembiztos állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.
- **Magyarázat:** Az érintett szervezet megvizsgálja, hogy az EIR utolsó ismert, üzembiztos állapotba történő helyreállításakor a felmerülő kockázatok figyelembevételével a rendszer állapotváltozóit vissza kell-e állítani a kezdeti értékekre vagy az üzemszünet előtti értékekre.

Behatolásvizsgálat (penetration testing)

IT: NIST 800-53

- Az érintett szervezet behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal a meghatározott EIR-eken vagy rendszerelemeken

OT: NIST 800-82

- Az érintett szervezet az OT funkciók zavartalanságának biztosításával behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal a meghatározott EIR-eken vagy rendszerelemeken.
- **Magyarázat:** A behatolásvizsgálatokat megfontoltan alkalmazzák az OT-hálózatokon, hogy az ellenőrzési folyamat ne befolyásolja hátrányosan az OT-funkciókat. Az OT-rendszerek általában nagyon érzékenyek az időzítési korlátokra, és korlátozott erőforrásokkal rendelkeznek. A helyettesítő ellenőrzések közé tartozik például a replikált, virtualizált vagy szimulált rendszer alkalmazása a behatolásvizsgálat elvégzéséhez. Előfordulhat, hogy a tesztelés elvégzése előtt le kell állítani a gyártás alatt álló OT rendszert. Ha az OT-rendszereket tesztelés céljából lekapcsolják, a teszteket lehetőség szerint a tervezett OT leállások idejére kell ütemezni. Ha a behatolásvizsgálatot nem OT-hálózatokon végzik, fokozottan ügyelni kell, hogy a tesztek ne terjedjenek át az OT-hálózatra.

10 – 25 év

Kerülő megoldások

- Architektúrák
- Komponensek képességei
- Szemléletmód
- Fehér és kék galléros párbeszéd

Beépített biztoság

Köszönöm a figyelmet!

- Hinkel Attila
- +36.20.928.9449
- hinkel.attila@alverad.hu