



Ipari kibervédelem a gyakorlatban

Kocsis Tamás

Kiber-fizikai környezetek - OT

- Programozható rendszerek, észlelik a fizikai környezet változásait és/vagy kiváltják a változást a fizikai környezetben,
 - Irányítástechnika, automatizáció, folyamatvezérlés
 - PLC, DCS, PCS, HMI, RTU, SCADA – vezérlőeszközök
 - Szenzorok, motorok, aktuátorok, műszerek, jelzők, stb – terepi eszközök
- A kiber-fizikai vagy OT környezetek a kritikus infrastruktúrák technológiai rétege
- OT nélkül nincs gyártás, egészségügy, energiatermelés, víz, közlekedés, stb.
 - OT nélkül nincs fejlett civilizáció,
 - OT nélkül nincs fogyasztói társadalom



Kiber-fizikai környezetek - OT

- A kiber-fizikai jellemző, hogy egyszerre hatnak rá a digitális és a fizikai világ veszélyei
 - Digitális veszélyek: kiberkockázatok és kiberfenyegetések
 - Fizikai veszélyek: mechanikai, elektromos, biológiai, környezeti, tárolt energiák, sugárzás, stb.
- A fizikai oldalról az OT felkészült, az üzembiztonság az első!
- A digitális/kiber oldalon **20 év elmaradás** az IT-hoz képest!
- 1973: Modicon 084 – az első programozható logikai kontroller
- Szó nem volt arról, hogy az eszközöket össze kell kapcsolni, pláne hálózatokba kötni

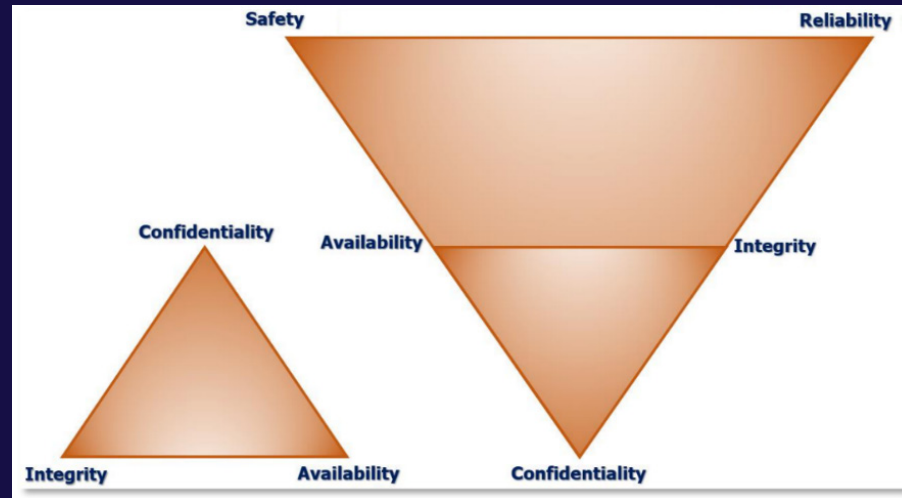


Kiber-fizikai környezetek - OT

- **Az IT ~~≠~~ OT!**

- A fizikai világ és a fizikai folyamatok, a környezet befolyásolása,
- Közvetlen hatások a fizikai környezetre,
- Nem adat-, hanem folyamatközpontú,
- Más életciklus (15-25 év),
- Más a kiberbiztonság célja és funkciója,
- Más preferenciák és sorrend!

CIA/BSR



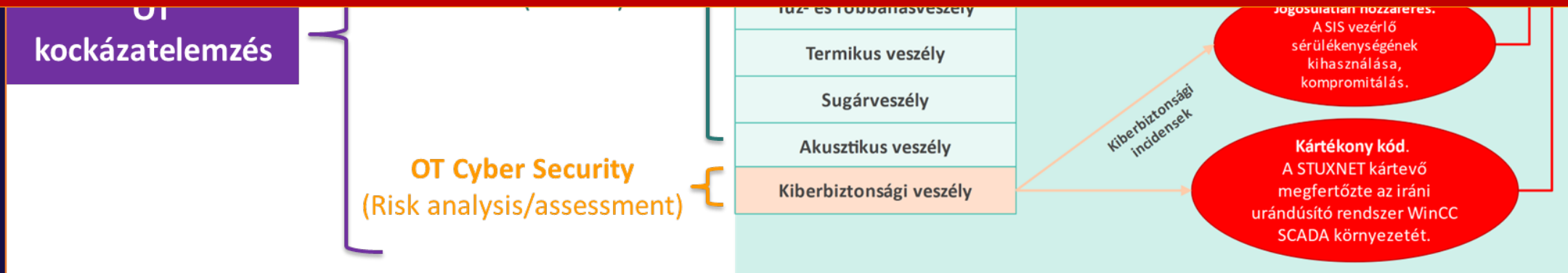
SAIC/SRAIC



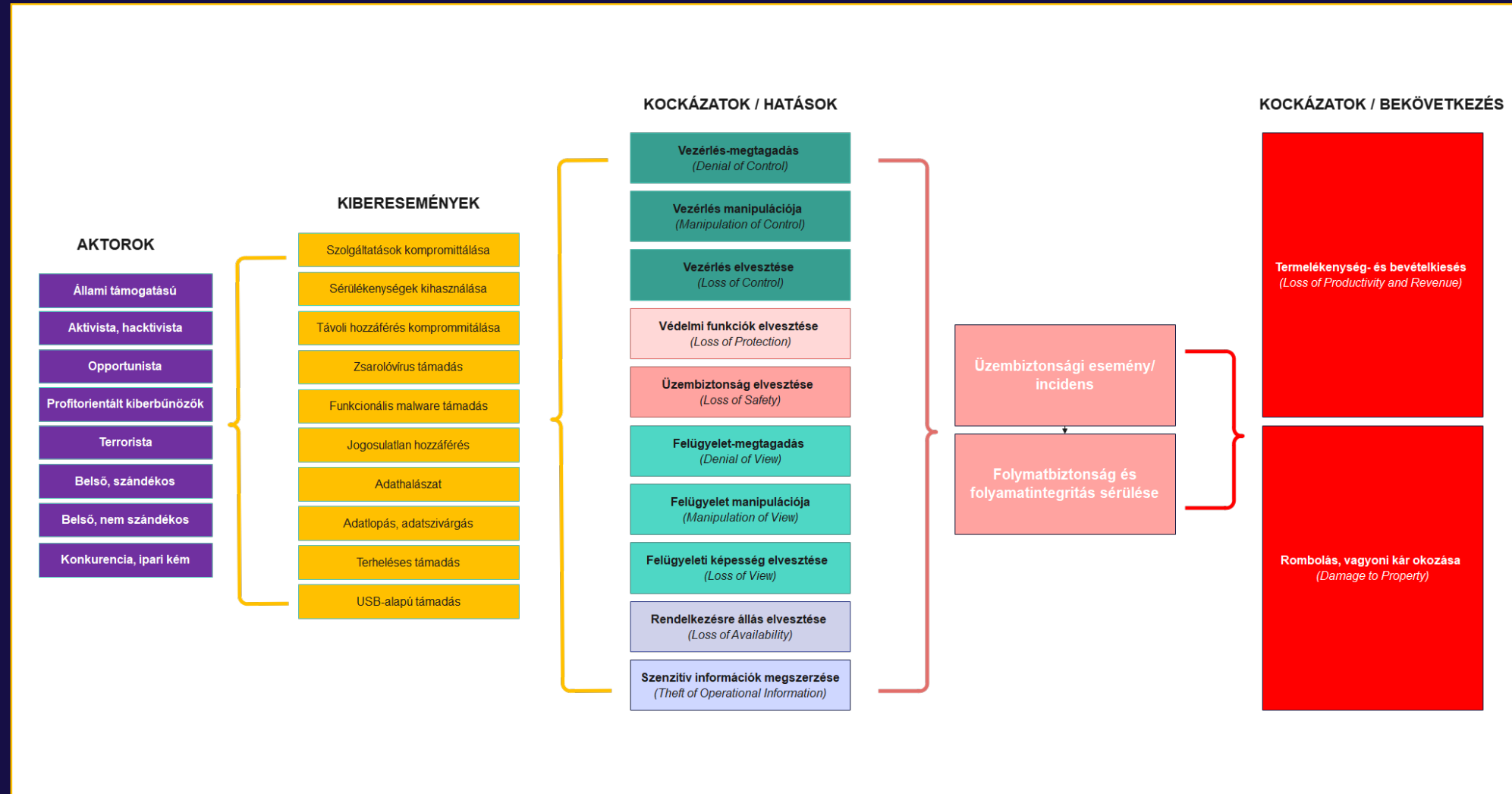
Kockázatok és fenyegetések

- Az OT nem foglalkozik kiberkockázatokkal
- Az OT veszélyekkel és üzembiztonsági kockázatokkal foglalkozik!
 - Veszélyek: mechanikai, elektromos, biológiai, sugár, tűz, robbanás, stb,
 - Kockázat: deviancia által kiváltott/realizálódott veszély, veszélyes állapot kialakulása

A kiber események vagy incidensek ugyanazokat a veszélyes állapotokat és káreseményeket idézhetik elő!



Kiber-> fizikai hatások



Az OT kiberbiztonság célja

IT biztonság, kiberbiztonság

- Szolgáltatások kompromittálása
- Sérülékenységek kihasználása
- Távoli hozzáférés kompromittálása
- Zsarolóvírus támadás
- Funkcionális malware támadás
- Jogosulatlan hozzáférés
- Adathalászat
- Adatlopás, adatszivárgás
- Terheléssel támadás
- USB-alapú támadás



OT kiberbiztonság

- Vezérlés-megtagadás
(Denial of Control)
- Vezérlés manipulációja
(Manipulation of Control)
- Vezérlés elvesztése
(Loss of Control)
- Védelmi funkciók elvesztése
(Loss of Protection)
- Üzembiztonság elvesztése
(Loss of Safety)
- Felügyelet-megtagadás
(Denial of View)
- Felügyelet manipulációja
(Manipulation of View)
- Felügyeleti képesség elvesztése
(Loss of View)
- Rendelkezésre állás elvesztése
(Loss of Availability)
- Szenzitív információk megszerzése
(Theft of Operational Information)



Kihívások

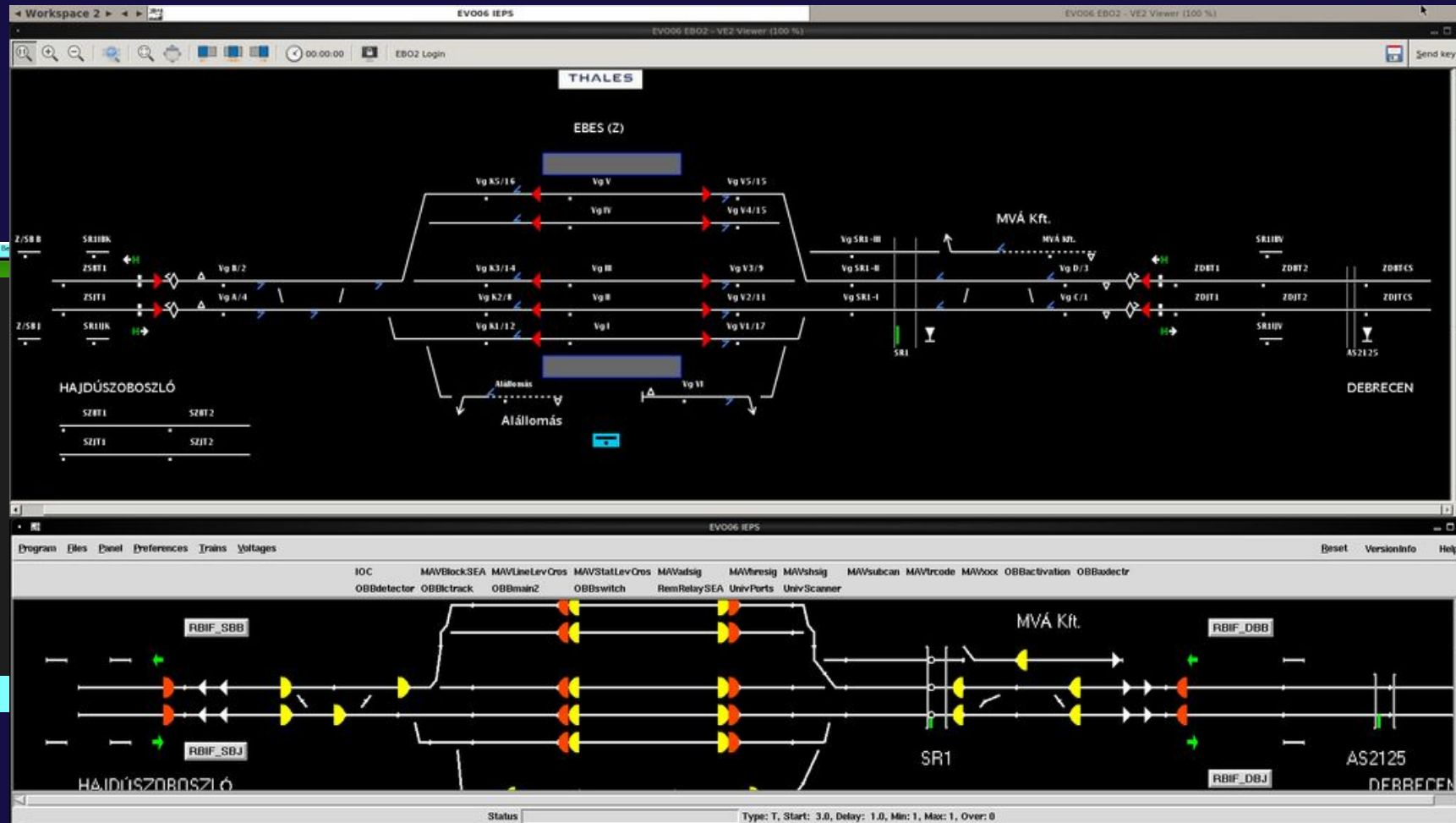
- **Az IT ~~NOT~~!**

- Az IT-ban 10 éve is „ciki”, 5 éve már „elképzелhetetlen” állapotok
 - Minden egyben hálózatok, jelszavak hiánya, 1 karakteres jelszavak,
 - Frissítések és javítások nincsenek,
 - Nem tudják milyen eszközök üzemelnek (inventory hírből sincsen),
 - Nem tudják ki, mikor és honnan fér hozzá a berendezésekhez,
 - Nem ipari eszközök ipari környezetekben,
 - Titkosítatlan, hitelesítés nélküli protokollok, stb



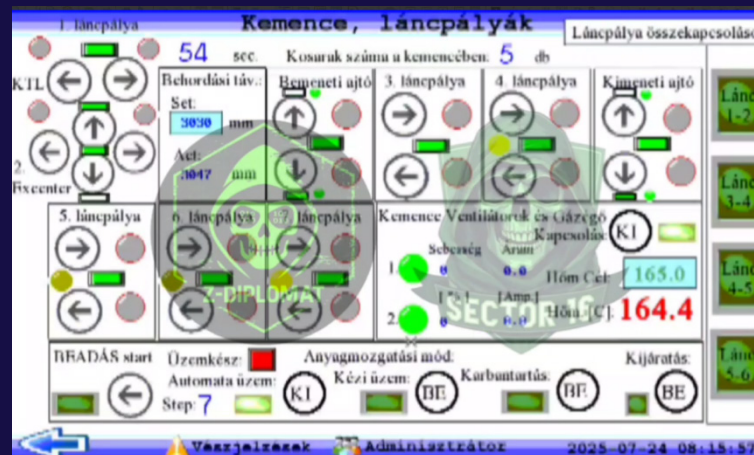
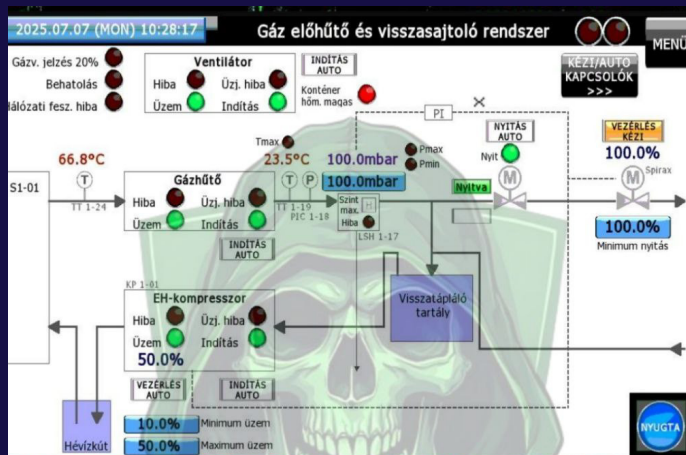
Kihívások

- Az IT ~~NOT~~!
 - Nagyon távoli hozzáférések



Az OT kiváló célpont!

- Az első, hazai, kiber-fizikai környezeteket célzó kampány
- **SECTOR 16**
 - Rosszul konfigurált távoli elérések kompromittálása
 - Orosz hacktivisták elkövető csoport
 - 4 hazai áldozat, geotermikus rendszer, HVAC, gyártórendszer, hőközpont,
 - Kompromittált távelérés, VNC
 - Sokkal nagyobb baj lehetett volna



Az OT kiváló célpont!

- Az első, hazai, kiber-fizikai környezeteket célzó kampány
- **SECTOR 16**
 - Sokkal nagyobb baj lehetett volna!!!!
 - 109 hazai, többségében kiber-fizikai rendszer (vízmű, kohó, gyártósor, stb)



The screenshot displays a VNC remote session. On the left, a control interface titled "Állapotok jelzése" (Status Indication) shows various water levels and flow rates for different wells (Kút 1. to Kút 8.) and a vent (Vent 1.). Each well has a status indicator (Üzemen or Szállít) and a power button. The right side of the screenshot shows a terminal window with a list of IP addresses. The IP address 94586277 is highlighted in blue in the terminal output.

Auto. szint figyelés

Állapotok jelzése

About this VNC:

ID: 94586277

← → ↺ 🌐 ?country=HU

Olvashatóra formázás ☒

```
{
  "results": [479020, 1545679, 1556507, 3046520, 6771138, 6829499, 8171029, 8752368, 8752699, 10017917, 1018073
13118654, 16299717, 17570346, 18498499, 20163418, 22585763, 23541258, 23805196, 24867199, 24948006, 25739721, 2
29421732, 29785061, 29809331, 30912200, 32261953, 32962212, 33284464, 33426496, 35090342, 36157625, 37238673, 3
37592840, 38289867, 39045556, 39782168, 40040105, 40996967, 43141564, 43702158, 45584228, 45832141, 46111468, 4
50161101, 51394501, 51621582, 52821119, 52892108, 55672879, 55767105, 59609261, 61530196, 62138374, 62313724, 6
567405773, 68356186, 68761105, 69594504, 70041418, 70769551, 70946148, 72711624, 73235412, 73598831, 77928127, 7
82293093, 82584204, 82757457, 83646434, 85994057, 87361288, 89259874, 89494988, 90283726, 91154183, 91731324, 9
93525021, 94108257, 94239211, 94523113, 94586277, 95340224, 97020999, 97341262, 97537450, 98081494, 98156206, 9
```

Az OT kiváló célpont

- **Növekszik a hazai kiber-fizikai környezetek kitettsége!**
- A kitettséggel együtt a fenyegetés is növekszik
- A kiberkockázatok a termelésfolytonosságot és az üzembiztonságot fenyegetik
- A 20 éves lemaradás „ledolgozása” már nem várható!
- ...és nyakunkon a NIS2 (talán lesz kiber-fizikai követelménykatalógus 😊)



A legnagyobb probléma

- **Nem első sorban műszaki, hanem humán!**
- Ki fog OT kiberbiztonsággal foglalkozni?
 - Az IT nem ért a kiber-fizikai sajátosságokhoz és a kultúrát sem érti (még),
 - Az OT mérnökök nem kiberbiztonsági szakemberek...
 - Nincs, vagy alig van OT kiberbiztonsági szakember itthon (még)

Legyél Te is OT kiberbiztonsági szakember, mert ember kell a gátba! 😊



OT kiberbiztonsági szakemberképzés

<https://kiberakademia.uni-obuda.hu/ot/>



**SZÉCHENYI
EGYETEM**
UNIVERSITY OF GYŐR

Kiber-fizikai rendszerbiztonsági szakemberképzés

<https://felveteli.sze.hu/kiber-fizikai-rendszerbiztonsagi-referens-szakember>



Köszönöm a figyelmet!

tamas.kocsis@alverad.hu

