

MODERN IPARI KÖRNYEZET INFORMATIKAI HÁLÓZATI LEHETŐSÉGEI A RENDELKEZÉSRE ÁLLÁS BIZTOSÍTÁSA ÉRDEKÉBEN

IT NETWORK OPPORTUNITIES OF MODERN INDUSTRIAL ENVIRONMENT TO ENSURE AVAILABILITY

Göcs László^{1*}, Pásztor Attila¹, Johanyák Zsolt Csaba¹,

¹ Informatika Tanszék, GAMF Műszaki és Informatikai Kar, Neumann János Egyetem, Magyarország
<https://doi.org/10.47833/2021.3.CSC.003>

Kulcsszavak:

Ipar 4.0
megbízható hálózat
IT biztonság
Turbo Ring
Turbo Chain

Keywords:

Industry 4.0
reliable network
IT security
Turbo Ring
Turbo Chain

Cikk történet:

Beérkezett 2021. szept. 8.
Átdolgozva 2021. szept. 15.
Elfogadva 2021. szept. 20.

Összefoglalás

Az ipari informatikai rendszerek működése megköveteli a magas szintű megbízhatóságot, redundanciát, karbantarthatóságot és biztonságot, ezért törekedni kell olyan technológiák alkalmazására, melyek biztosítják ezeket. A cikk bemutat olyan hálózati megvalósításokat, melyek egy Ipar 4.0-s rendszer kialakításához szükségesek lehetnek.

Abstract

The operation of industrial IT systems requires high level reliability, redundancy, maintainability and security, so efforts must be made to use technologies that ensure these. This article presents network implementations that may be required to build an Industry 4.0 system.

1. Bevezetés

Az informatikai rendszerek, beleértve az ipari informatikai rendszereket, megbízható működését úgy értelmezzük, hogy az alkalmazói rendszernek (felhasználói programok és adatok) a tervezés és megvalósítás során kialakított funkcionalitását egy megbízható informatikai alaprendszer (hardver és alapszoftver) az adott biztonsági osztálynak megfelelő követelményeknek megfelelő szintű rendelkezésre állással biztosítja a felhasználó részére. Rendelkezésre álláson azt a valószínűséget értjük, amellyel egy definiált időintervallumon belül a rendszer a tervezéskor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható. Rendelkezésre áll egy alkalmazás vagy erőforrás, mikor a működésének képes eleget tenni, képes feladatokat fogadni, működni. Értékét százalékban adják meg. Szerverek esetén ez az az idő, amikor képesek kiszolgálni a klienseket.

$$\text{Rendelkezésre állás (R)} = \frac{T_{\text{üz}} - \sum_{\text{üz}} T_{ki}}{T_{\text{üz}}} \times 100\%$$

* Kapcsolattartó szerző. Tel.: +36 76 516-417
E-mail cím: gocs.laszlo@gamf.uni-neumann.hu

ahol $T_{üz}$ az üzemidő periódus, amelyre a rendelkezésre állást értelmezzük és T_{ki} a kiesési idő egy alkalomra. Egy ipari környezetben nem megengedhető a kiesés, ezért a kiesési időt befolyásoló tényezőket kell komolyan venni, melyek az alábbiak:

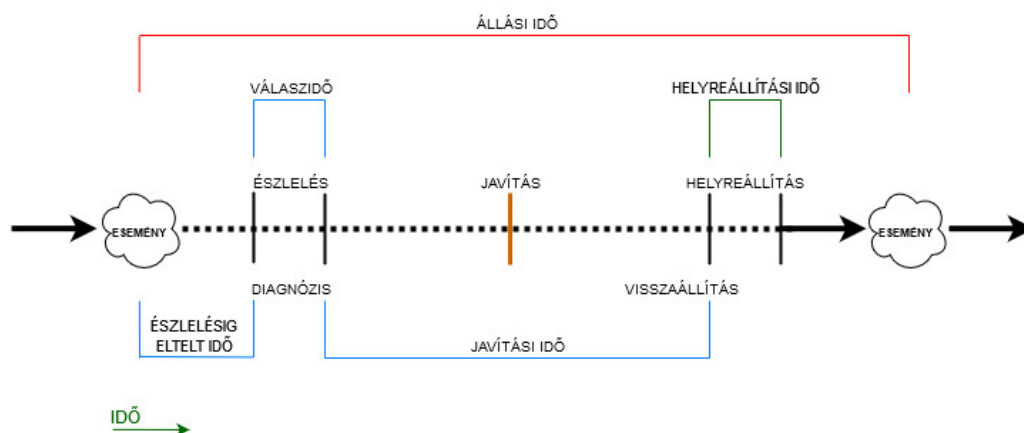
- az újraindítási képesség megvalósítása,
- a hibaáthidalás folyamatának kialakítása,
- a rendszerkonfiguráció hatékony menedzselése

A rendelkezésre állás menedzsment

- Megbízhatóság (reliability): egy információtechnológiai összetevő azon képessége, hogy ellásson egy megkívánt funkciót meghatározott körülmények között, egy meghatározott időtartamra.
- Karbantarthatóság (maintainability): egy számítógépes komponens vagy szolgáltatás azon képessége, hogy meg lehet tartani egy olyan állapotban, vagy vissza lehet állítani egy olyan állapotba, amelyben képes ellátni a megkívánt funkciót.
- Szolgáltatási képesség (serviceability): szerződéses kikötés, amely meghatározza az informatikai komponens rendelkezésre-állását az adott összetevőket szolgáltató és karbantartó külső szervezettel való megegyezés szerint.
- Biztonság (security): lehetővé teszi a számítógépes komponensek vagy informatikai szolgáltatások elérését biztonságos körülmények között.

Az informatikai rendszereket és szolgáltatásokat úgy kell tervezni, hogy megbízhatóak, hibátűrők és karbantarthatók legyenek teljes életciklusuk során, a tervezéstől, a megszüntetésükig. A hatékony és eredményes rendelkezésre-állás menedzsment a következő hasznokat eredményezi: az informatikai szolgáltatások javuló minőségét, az új és meglévő informatikai szolgáltatások költség-hatékony nyújtását, az informatikai infrastruktúra javuló menedzselhetőségét, jobb tervezési képességét, az informatikai szolgáltatások biztonságosabb nyújtását.

Az alábbi ábra egy bekövetkezett esemény és a hozzá kapcsolódó helyreállítás közti kapcsolatot mutatja be:



1. ábra Események közti idők meghatározása

Ez a tanulmány megpróbálja összefoglalni azokat a területeket, melyeket fontos szem előtt tartani annak érdekében, hogy egy megbízható és jól működő ipari rendszert alakítsunk ki. A cikk a hálózati rétegek több területét érintik. A fizikai kiépítésnél a kábelezési előírások, lehetőségek fogalmazódnak meg. A kommunikációs eszközöknél az ipari környezetben előnyös szabványok kerülnek bemutatásra. A végpontokon lévő berendezések megfelelő kiválasztása mellett a biztonságos adatátvitel, adattárolás lehetősége, a felhasználói hitelesítés fontossága szintén szerepet kap a cikkben.

2. Strukturált hálózat

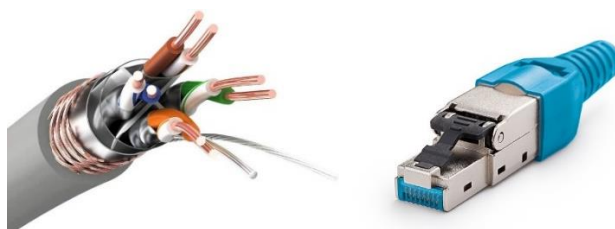
A hálózati kommunikáció alappillére a fizikai réteg. Ez adja meg a teljes informatikai infrastruktúra alapját, ezért ezt nagy körültekintéssel kell kiépíteni. Nagyon fontos, hogy az ipari rendszerek közti kommunikáció folytonossága és stabilitása a lehető legmegbízhatóbb legyen [14]. Egy kommunikációs hiba akár végzetes is lehet egy ipari folyamatban, komoly kiesést vagy hibás termék gyártását eredményezheti a termelésben. A strukturált hálózat tervezéskor figyelembe kell venni a gyártó rendszer környezetét, a lehetséges zavaró tényezőket. A „MICE” besorolás egy jó kiinduló pont lehet tervezéskor. A mozaikszót alkotó négy környezeti elem a következő:

- M: mechanikus (ütés, vibráció, törés, húzóerő, hajlítás stb.)
- I: behatolás (például víz, por folyadék és részecskék formájában)
- C: éghajlati/kémiai (hőmérséklet, UV-sugárzás, páratartalom, szennyeződéseknek való kitettség, például olaj vagy gáz stb.)
- E: elektromágneses (túlfeszültségek, EMI/RFI interferencia, mágneses mezők, tranziensek stb.)

A MICE-besorolásban mind a négy betű után egy szám jelenik meg. A szám a környezeti tényezőnek való kitettség „súlyosságát” jelzi:

- 1: alacsony súlyosság (általában kereskedelmi irodai környezetben található)
- 2: közepes súlyosság (általában könnyűipari környezetben található)
- 3: nagy súlyosság (általában nehézipari környezetben található)

Fontos, hogy a megfelelő, jól átlátható és karbantartható topológiát építsünk ki, ami megkönnyíti a karbantarthatóságot. Egy ipari környezetben a fizikai réteg kiépítése elsősorban vezetékes technológián alapul. A kábelezés kialakításánál elsődleges szempont a megbízható és minőségi alapanyagok használata. A kettős árnyékolás biztosítja az átviteli megbízhatóságot az elektromágneses interferenciával rendelkező területekre, márpedig egy ipari környezetben jobban előfordul az ilyen jellegű zavaró tényező, mint egy irodai hálózatnál. Továbbá fontos szempont, hogy a működési hőmérsékletük $-30...80^{\circ}\text{C}$ között is lehet, adatátviteli sebességük pedig 2,5 vagy 5Gbit/sec.



2. ábra Speciális Ethernet kábel és csatlakozási lehetőség

A speciális külső burkolat ellenáll az ásványi olajoknak és a kopásnak, de ami még fontosabb, hogy halogénezett adalékokat tartalmazó vegyületek ne legyenek benne, tűzvédelmi okokból, így halogénmentes (kapcsolódó szabvány: MSZ EN 60754-1/2 [3]) kábeleket szükséges használni. Az ISO/IEC 11801:2017 [2] – Strukturált kábelezés szabvány betartása az információs technológiák összes átviteli protokoll működőképességének feltételét és egyúttal garanciáját jelenti. A szabvány 3. része az ipari környezetről szól, ahol meghatározzák az egyes részek (szabványok) címében megadott környezetben használható kábelezés teljesítménykategóriáit, a hálózatok szerkezetét és hierarchiáját [1].

A hálózati összeköttetés másik lehetséges módja az SPE (Single Pair Ethernet), mely az Ethernet továbbítását csak egy pár rézvezetéken keresztül végzi el és lehetővé teszi mind az

adatátvitelt Ethernet-en keresztül, és egyidejűleg a tápellátást (PoDL) is. Ez a technológia a kábel átmérő 25%-os csökkenését eredményezheti a hagyományos Ethernet kábelhez képest. A szabványosított SPE interfészek ideálisan alkalmasak a hatékony adatátvitelre a gyár- és folyamatautomatizálásban IEC 63171-2 (IP20) és IEC 63171-5 (IP67) szabványoknak megfelelően.



3. ábra Single Pair Ethernet csatlakozások

Bizonyos ipari környezetben már előtérbe helyeződik az optikai kábelek használata, melyeknek nagy az átviteli sebességük, nagy távolságok áthidalására szolgálnak (pl külön gyártósori épületek közötti összeköttetés), kis csillapítást biztosítanak, és érzéketlenek az elektromágneses zavarokkal szemben.



4. ábra Optikai csatlakozás és SFP modul

3. Hálózati eszközök

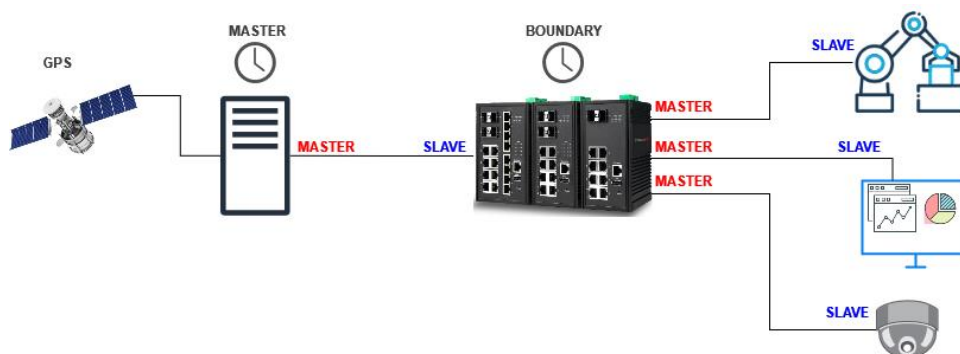
Egy ipari környezetben kizárólag az erre a célra gyártott hálózati berendezéseket célszerű használni. Az otthoni és irodai felhasználási területre gyártott eszközök nem alkalmasak erre a feladatra. Az ilyen ipari switch-ek kiépítés szempontjából DIN-sínre is szerelhetők, mely segítségével könnyen beépíthetők az ipari környezetbe moduláris felépítésüknek köszönhetően.



5. ábra ipari menedzselhető Ethernet switchek

3.1. Időzítés

Nagyon fontos hogy egy kiépített rendszerben a berendezéseknek összhangban kell lenni, ezért nagy pontosságú időzítésre, és időmérésre van szükség. Ennek érdekében az NTP-t (Network Time Protocol) már felváltotta a Nagy pontosságú IEEE 1588 PTP (Precision Time Protocol) óra szinkronizációs protokoll. Ezt a protokollt támogató eszközök használata szükséges az ipari környezetben.



6. ábra Időprotokoll működése [10]

A PTP-nek két féle óratípusa van, a master és a slave. A végponti eszközben lévő óra a slave. A mestert ideális esetben egy külső rádió óra irányítja, vagy egy GPS vevő szinkronizálja a megfelelő hozzá csatlakoztatott slave órákat. A hálózatban lesznek átviteli csomópontok is, pl Ethernet switch egy szabályozó órával. Ez a szabályozó óra slave óráként viselkedik a master órához viszonyítva, aztán vált, hogy master óráként működjön a végponti slave eszközökhöz képest. Minden egyes slave óra szinkronizálva van a master órához időben, frekvenciában és fázisban, és szinkronizálva van az összes többi slave csomópontokhoz is.

Ennek a hálózati protokollnak a használata már régebben elterjedt pl. blue tooth-on kommunikáló eszközök esetén is.[9] Itt a master-slave típusú hálózatokat piconet hálózatnak és az ezek halmazaként alkalmazott hálózatokat scatternetnek nevezik. Ezt a modellt használják többek között robot-swarmok kommunikációs protokolljaként is.[7][8]

3.2. Csatlakozási biztonság

A hálózatban használt Ethernet switchek egyik fő kategóriája a menedzselhető switchek. Ezek lényege, hogy nem csak az alapvető switch működésre képesek (csomagok továbbítása), hanem több biztonsági beállítási lehetőségük van a teljes eszközön, vagy akár külön-külön a csatlakozási portokon is.

3.2.1. Port-zárolás

Egy rendszerbe integrált switch esetében nem biztos, hogy a beüzemelés során minden csatlakozási port aktívan rész vesz az üzemeltetésben. Ezért egy egyszerű, de hatásos biztonsági beállítást kell elvégeznünk, melynek lényege, hogy a nem használt csatlakozási portokat letiltjuk. Ezáltal ha bármilyen eszköz csatlakoztatásra kerül, nem tud semmilyen kommunikációt létesíteni az éles hálózattal, mindaddig, amíg a rendszeradminisztrátor nem aktiválja a portot (miután meggyőződött az eszköz biztonságáról). Példa egy 24 portos switch 10-24 csatlakozási pontjainak tiltására:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface range f0/10-24
Switch(config-if-range)#shutdown
```

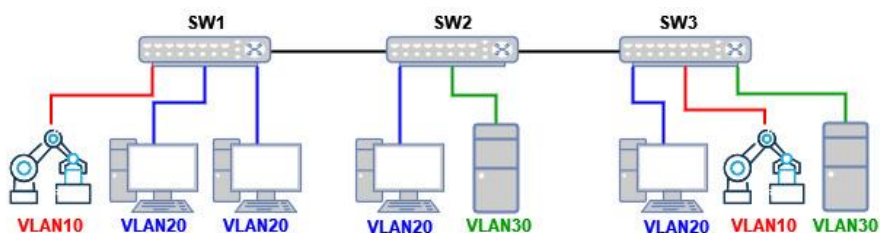

3.2.2. Port biztonság

A switchek minden egyes portjára megadható az arra csatlakoztatott eszköz azonosítója (MAC address), ennek értelmében semmilyen más berendezés nem tud aktív lenni a rendszerben, ezáltal a nem kívánatos csatlakozás elkerülhető. Ha nem az a készülék került csatlakoztatásra, amelynek az azonosítója regisztrálva lett, a port tiltva lesz.

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 1234.5678.9ABC
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security
```

3.3. Virtuális LAN-ok

Nagy kiterjedésű vállalati hálózatonál elengedhetetlen a szeparáció. Ez azt jelenti, hogy bizonyos területek külön álló IP hálózaton vannak (VLAN-ok). A gyakorlatban ez azt jelenti, hogy egy közös fizikai hálózaton más-más logikai hálózatok vannak kialakítva. Előnye, hogy azon végpontok, berendezések, melyek távol esnek egymástól, összehangolhatóak egy hálózatba. Általában a termelési részt szokták a irodai hálózattól elszeparálni. Ennek a megoldásnak biztonsági oka is van, hiszen egy esetleges rosszindulatú szoftver, mely hálózati támadást okozna, nem tud kárt okozni a teljes rendszerben.

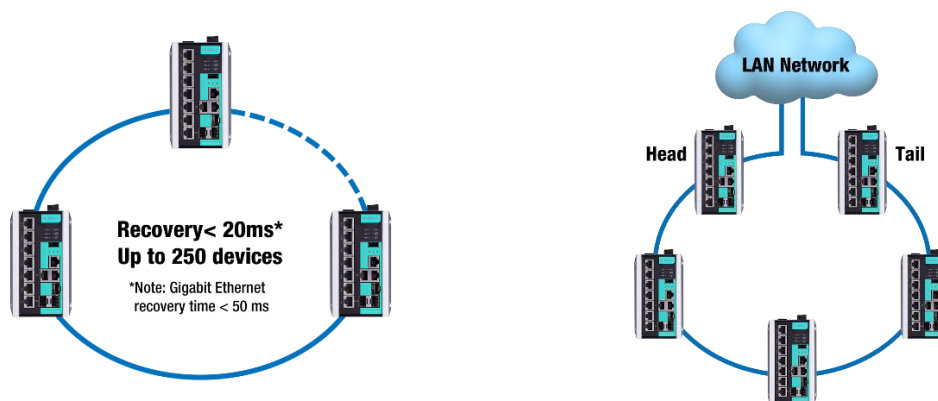


7. ábra Virtuális alhálózatok

3.4. Redundáns kommunikáció

A gyűrűs topológia nagyon népszerű és költséghatékony módszer a hálózat kiépítésére, és az iparágban az egyik leghatékonyabb megoldásnak számít a hálózati leállások elkerülésére [12].

A **Turbo Ring** a Moxa által 2007 -ben kifejlesztett technológia, amely hálózati redundanciát biztosít a rendszerek redundanciájához. Lényegében a Turbo Ring minden switchet gyűrűs topológiában köt össze. Általában, ha ezt nem felügyelt switchekkel végzik, végtelen ciklus jön létre, ami hálózati hibát okoz. A Moxa által felügyelt kapcsolók használatával azonban kiküszöbölhető a végtelen hurok, ha beállítunk egy Ethernet portot a felügyelt switchen, hogy letiltsa, és csak akkor engedélyezze, ha hibát észlel [5]. A Moxa Turbo Ring technológiája lehetővé teszi a hálózatok helyreállítását 20 ms-on belül (10G/1G Ethernet helyreállítási idő <50 ms) akár 250 csomóponttal rendelkező hálózaton. A **Turbo Chain** egy nagyon rugalmas redundancia technológia, amely korlátlan redundáns hálózatbővítést kínál, és széles körben elterjedt hálózatokon való használatra készült. A Turbo Chain felülmúlja a hagyományos gyűrűs topológiákat, mivel kiváló rugalmasságot, korlátlan bővítést és egyszerűsített konfigurációt biztosít, amely lehetővé teszi a hálózati üzemeltetők számára, hogy csökkentsék a telepítési költségeket, amikor külön redundáns gyűrűket csatlakoztatnak egymáshoz [6].



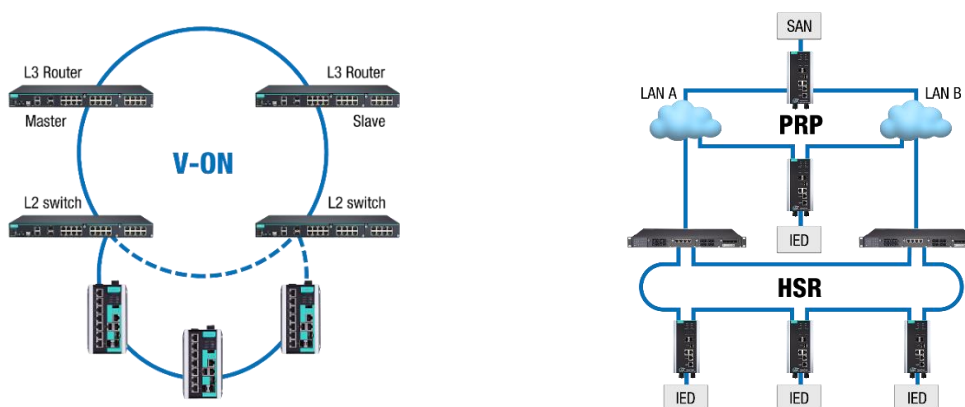
8. ábra Moxa Turbo Ring és Turbo Chain technológia [11]

A **V-ON** biztosítja, hogy az egyszerű és összetett hálózatok ezredmásodpercen belül helyreálljanak a kapcsolat meghibásodása esetén. A V-ON-t multicast hálózati alkalmazásokhoz tervezték, például ipari automatizálási PLC-khez és videó megfigyelő rendszerekhez. Ha ezt a technológiát Turbo Ring vagy Turbo Chain láncokkal kombinálják, akkor redundanciát tud biztosítani az egész hálózat számára.

Jellemzők:

- A 2. réteg átvitelének helyreállítása <50 ms az unicast és multicast hálózatok esetén
- A 3. réteg átvitelének helyreállítása <300 ms az unicast és multicast útválasztó hálózatokhoz
- Milliszekundum szintű router redundancia

A párhuzamos redundancia protokoll (**PRP**) és a nagy rendelkezésre állású zökkenőmentes redundancia (**HSR**) két olyan technológia, amelyek zökkenőmentes átvitelt biztosítanak akkor is, ha a hálózat egy része meghibásodik. A PRP két független, párhuzamosan működő hálózaton keresztül, csomagok duplikálásával éri el az aktív hálózati redundanciát, míg a HSR elsősorban gyűrűs topológiákhoz készült [6].



9. ábra Moxa V-ON és PRP HSR technológia [11]

4. Ipari számítógépek

A megszokott munkaállomások melyeket az irodai alkalmazásoknál használnak, nem megfelelőek az ipari környezetben (olaj, gáz, hőmérséklet). Ahogy a hálózati eszközök, úgy a számítógépek is ki vannak téve különböző zavaró jeleknek, valamint a könnyebb kiépítés miatt a DIN-sínre való

szerelhetőségük nagy előny. Így az ipari környezete is speciális munkaállomásokat preferálnak, amik lehetnek kijelzővel egybe épített panel PC-k is.



10. ábra Ipari munkaállomások

5. Felhasználók kezelése

Olyan környezetben, ahol a felhasználók száma meghaladja a 20-25 főt, valamint a berendezések használata nem helyhez kötött, vagyis egy felhasználónak több helyen is kell belépnie munkavégzés miatt, a központi hitelesítés a legjobb megoldás. A nagyszámú hálózati eszközök menedzselésére szintén nélkülözhetetlen egy hitelesítő szerver használata. Ennek a megvalósítására az **AAA protokoll** a megfelelő megoldás. A protokoll részei:

- Authentication (hitelesítés)
- Authorization (jogosultság kezelés)
- Accounting (naplózás)

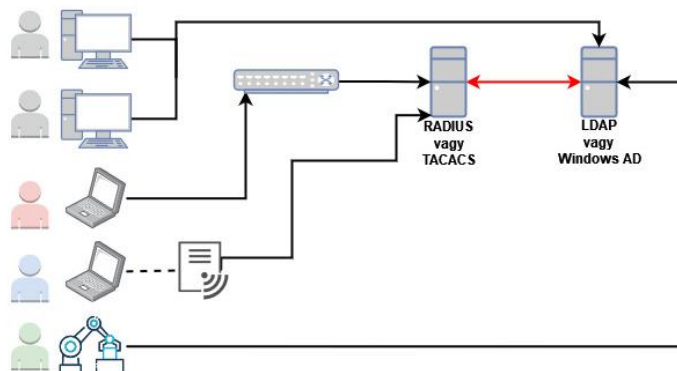
A szerver alapú megoldás lényege, hogy a belépésnél a bekért adatokat továbbküldjük egy szerverre, melyek típusai lehetnek:

- RADIUS: Remote Authentication Dial-In User Service
- TACSACS: Terminal Access Controller Access Control System

Egy router AAA konfigurációja:

```
R1(config)#aaa new-model
R1(config)#radius-server host 192.168.1.3
R1(config)#radius-server key Radius12345
R1(config)#aaa authentication login default group radius
```

A felhasználói adatbázis lehet a hitelesítő szerveren is, vagy akár a szerver összeköttetésben van egy LDAP vagy Windows Active Directory-val. Így egy adatbázis segítségével tudunk hitelesítést biztosítani a hálózati eszközöknek, irodai munkaállomásoknak, ipari berendezéseknek.



11. ábra Központi felhasználói kezelés

6. Összefoglalás

A cikk átfogó képet ad arról, hogy egy mai ipari környezet kialakítására milyen lehetőségek vannak. Fontos az informatikai rendszerek kialakításánál figyelembe venni minden területet. A különböző technológiáknak egy közös egységet kell alkotni, mert csak úgy lehet biztosítani a megfelelő és biztonságos működést. Az ipari rendszerekbe integrált informatikai elemek, eszközök nem a hagyományos piaci szegmensek építőelemeiből tevődnek össze, így a költségük is magasabb lehet, de egy termelési rendszerrel kifizetődőbb egy jól és megbízhatóan, biztonságosan működő informatika kiépítése [13].

Köszönetnyilvánítás

A szerzők köszönetet mondanak a projektben résztvevő intézmények - Nádor Rendszerház Kft., Controlsoft Automatika Szolgáltató Kft., Neumann János Egyetem GAMF Műszaki és Informatikai Kar - kollégáinak. Köszönettel tartozunk a kutatás támogatásáért, amely az "Ipar 4.0 moduláris felépítésű ipari csomagológép fejlesztése integrált adatelemzéssel és mesterséges intelligenciára épülő optimalizálással, hibaelemzéssel 2020-1.1.2-PIACI-KFI-2020-00062" pályázat keretében valósult meg. A projekt a Magyar Állam és az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával, a Széchenyi 2020 program keretében valósul meg.

Irodalomjegyzék

- [1] <https://www.keline.eu/a/58/a-strukturalt-kabelezessel-kapcsolatos-koevetelmenyvaltozasok-az-uj-nemzetkoezi-iso-iec-11801-szabvany> 29.március 2018, KRUGEL EXIM társaság műszaki-fejlesztési munkatársai
- [2] ISO/IEC 11801-1:2017, Information technology — Generic cabling for customer premises — Part 1: General requirements
- [3] MSZ EN 60754-1:2014, Kábel- és vezetékanyagok égésekor fejlődő gázok vizsgálata. 1. rész: A halogénsavgáz-tartalom meghatározása (IEC 60754-1:2011 + 2013. novemberi helyesbítés)
- [4] Perle Systems Technical Notes - PTP - Precision Time Protocol IEEE 1588 V1 and V2 PTP Boundary clock capabilities in Industrial Managed Switches <https://www.perle.com/supportfiles/precision-time-protocol.shtml>
- [5] https://www.quantumautomation.com/uploads/7/3/8/8/7388264/techcorner_44_-_turbo_ring_and_turbo_chain.pdf
- [6] <https://www.moxa.com/en/spotlight/industrial-ethernet/redundancy-technology/technologies>
- [7] Pásztor A., Kovács T., Istenes Z. Piconet and Scatternet Communication Networks in Swarm Intelligence Simulation with Mobile Robots, BULETINUL STIINTIFIC AL UNIVERSITATII POLITEHNICA DIN TIMISOARA ROMANIA SERIA AUTOMATICA SI CALCULATORAE / SCIENTIFIC BULLETIN OF POLITEHNICA UNIVERSITY OF TIMISOARA TRANSACTIONS ON AUTOMATIC CONTROL AND COMPUTER SCIENCE 54(68):(3) pp. 131-136. (2009)
- [8] Pasztor A, Kovacs T, Istenes Z., Swarm intelligence simulation with NXT robots using Piconet and Scatternet, 5th International Symposium on Applied Computational Intelligence and Informatics, SACI 2009. Timisoara, Románia, 2009.05.28-2009.05.29. IEEE Hungary Section, pp. 199-204. DOI: **10.1109/SACI.2009.5136241**
- [9] J. C. Haartsen: The Bluetooth radio system, IEEE Personal Communications 7, 2000, pp. 28-36
- [10] <https://www.perle.com/supportfiles/precision-time-protocol.shtml>
- [11] <https://www.moxa.com/en/spotlight/industrial-ethernet/redundancy-technology/technologies>
- [12] Kahiomba Sonia Kiangala, Zenghui Wang: An Effective Communication Prototype for Time-Critical IIoT Manufacturing Factories Using Zero-Loss Redundancy Protocols, Time-Sensitive Networking, and Edge-Computing in an Industry 4.0 Environment, DOI: **https://doi.org/10.3390/pr9112084**

- [13] Sebastian Saniuk, Anna Saniuk, Dagmar Caganova : Cyber Industry Networks as an environment of the Industry 4.0 implementation Big Data Analysis-based Network Behavior Insight of Cellular Networks for Industry 4.0 Applications **DOI: <https://doi.org/10.1007/s11276-019-02079-3>**
- [14] Dingde Jiang, Yuqing Wang, Zhihan Lv, Sheng Qi, Surjit Singh: Big Data Analysis-based Network Behavior Insight of Cellular Networks for Industry 4.0 Applications. **DOI 10.1109/TII.2019.2930226,**