İsgəndərzadə Hüseyn Qasım oğlu

E-mail: h.isgenderzade@mail.ru

Səfərəliyeva Sənubər Salam qızı

E-mail:MestehzadeS@mail.ru

Tağıyev Samir Elçin oğlu

E-mail: Tagiyevsamir1997@outlook.com

Azərbaycan Texniki Universiteti, Bakı

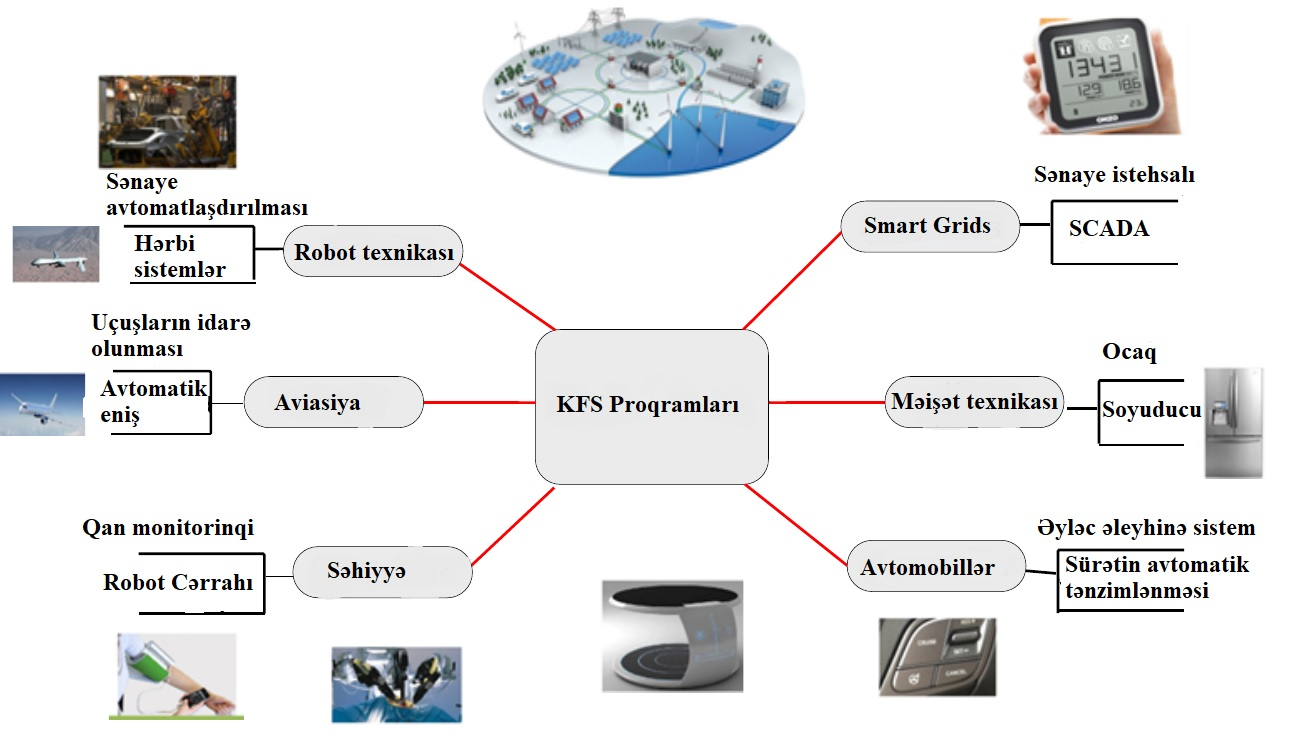
**KIBER-FIZIKI SISTEMLƏRIN**

**FƏALIYYƏTININ TƏHLÜKƏSIZLIK PROBLEMLƏRI**

**Annotasiya.** Proseslərin monitorinqi, şəbəkə hesablamaları və onların fəaliyyətinin effektiv idarə edilməsilə bu proseslərdə sistemin təhlükəsizliyinin təmin edilməsi, təhlükəsiz və etibarlı idarəetmə mühitinin təmin edilməsində hücumların əvvəlcədən təsbit edilməsi və lokallaşdırılması üçün lazımi tədbirlərin görülməsi çox vacib tətqiqat məsələsidir. Bu baxımdan məqalədə şəbəkə hesablamalarında və onların fəaliyyətinin effektiv idarə edilməsində kiber-fiziki sistemin fəaliyyətini pozmağa yönəlmiş müxtəlif təhdid və hücumlar təhlil və tətqiq edilmişdir.

**Açar sözləri:** KFS, aktuator, monitorinq,vandalizasiya, İoT .

Kiber-fiziki sistemlər (KFS) kiber və fiziki sfera (dünya) arasında şəbəkə vasitəsilə əlaqələndirilən rabitə, nəzarət və hesablama komponentlərinin birləşməsidir. Bu sistemlər fiziki hadisələri sensorların və aktuatorların tətbiqi ilə onların mövcud olduğu mühitdən izləməyə və qərar qəbul etmək üçün mərkəzləşdirilmiş sistemlə əlaqə yaratmağa imkan verir [1]. KFS-in müxtəlif kritik infrastruktur sahələrində məsələn, tibbdə, intellektual nəqliyyat sistemində (İTS), təhlükəsizlik və nəzarət sistemləri kimi sahələrdə tətbiq olunması ilə təhlükəsizliyə məhəl qoyulmadığı təqdirdə yarana biləcək təhlükələrin qabaqcadan proqnozlaşdırılmasına imkan yaranır. KFS-in səviyyəsi onun potensial istifadəçiləri olan ABŞ və Avropa İttifaqı kimi inkişaf etmiş ölkələrin enerji sektorunda, səhiyyədə, məişət texnikasında, istehsalda, ağıllı nəqliyyat və ətraf mühitin monitorinqi kimi bir çox sahələrdə bu sistemin tədqiqi və inkişafı üçün böyük sərmayələrin qoyulması ilə sübut edilir və hal-hazırda KFS sisteminin dizaynı, modelləşdirilməsi və tətbiqi ilə bağlı müxtəlif tədqiqat təşəbbüsləri davam etdirilir. Şəkil 1-də kiber-fiziki sistemlərin müxtəlif tətbiqlərinin ümumiləşdirilmiş sxemi təsvir olunmuşdur.

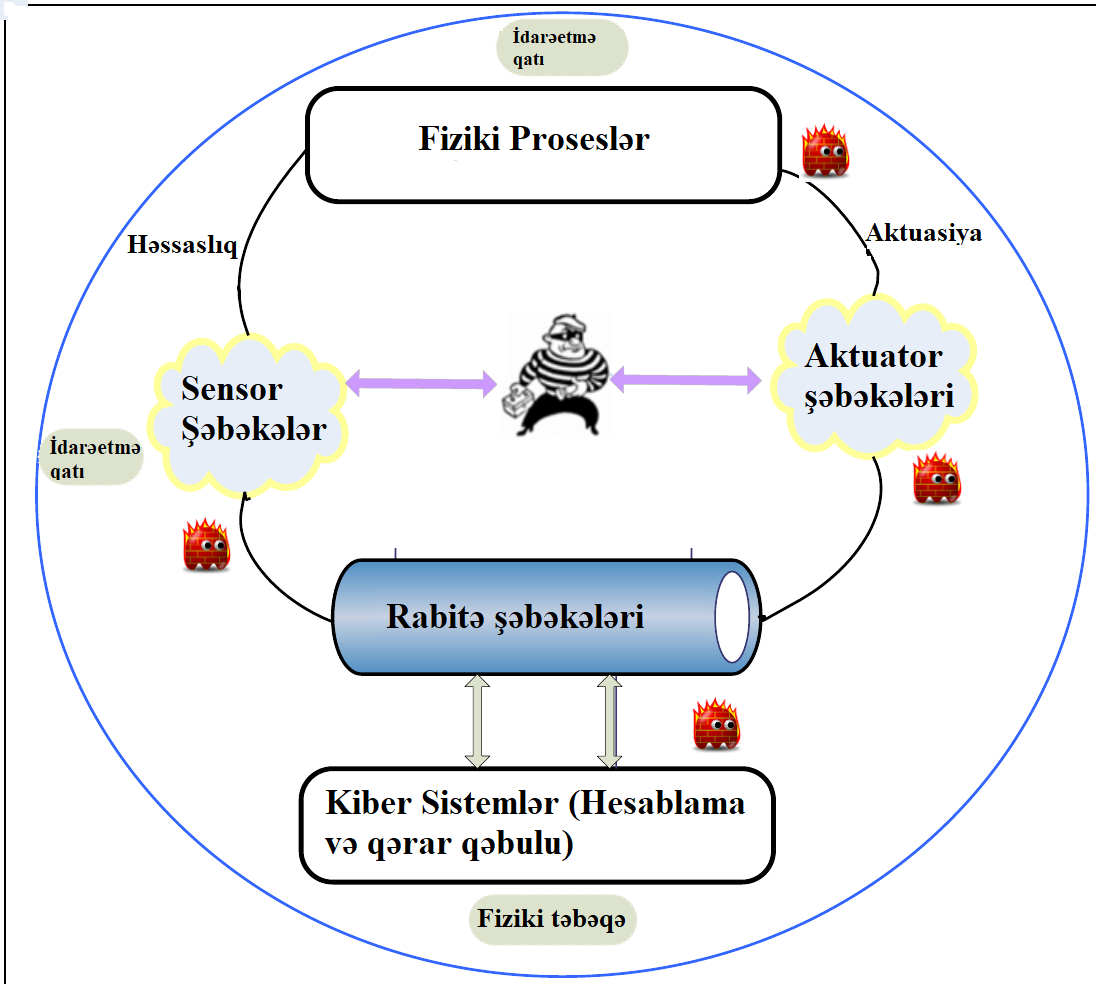


Şəkil 1. Kiber- fiziki sistemlərin tətbiqi

Dünya populyasiyasının sürətlə böyüməsi səbəbindən kiber-fiziki sistemdəki təhlükəsizlik imkanları bu dünyada olan insanların fəaliyyətinə nəzarət və onların effekli idarə edilməsi üçün böyük imkanlar yaradır. Ümumiyyətlə, kiber-fiziki sistemlər birləşdirilmiş hesablama şəbəkələri, çox kanallı əlaqə sahələri və multipleks metodologiyasıdır. Kiber-fiziki sistem real vaxt şəraitində ünsiyyət, məlumatların emalı, hesablama xətti ilə çox inteqrasiya olunmuş şəbəkə sahələrində maddi varlıq kimi bir çox cəhətdən sistemin imkanlarını artırsa da kiber-fiziki infrastrukturun tətbiqində bir sıra texnoloji rejimlərdə hələ də böyük problem sistem təhlükəsizliyidir.

KFS-də təhlükəsizlik aspektləri- KFS-in əsas funksiyası proseslərin monitorinqi, şəbəkə hesablamaları və onların fəaliyyətinin effektiv idarə edilməsilə bu proseslərdə sistemin təhlükəsizliyinin təmin edilməsinə yönəlir. Monitorinq prosesi zamanı səhv məlumatlar sistemə daxil ola bilər, şəbəkə səviyyəsində məlumatlar korlanmış və ya tıxanmış ola bilər, zərərli yoxlamalar və hesablamalar aparmaq üçün xarici təsirli hesablama prosesi həyata keçirilə bilər və fiziki komponentlər vandalizasiyanın qarşısını alına bilər və ya şəkil 2-də göstərildiyi kimi aktuatorların özləri fiziki hücumlara məruz qala bilər. Son dövrlərdə kiber-fiziki sistemə qarşı hücumlarda ciddi artım müşahidə olunur və bu hücumların səbəbləri fərqli olsa da hökumətə, biznesə, digər ictimai və özəl qurumlara kütləvi şəkildə təsir göstərə bilər. Bu qəbildən olan təhdidlər:

1.Etibarsız işçilər: Müasir dövrün ən ciddi təhlükəsizlik məsələlərindən birisi təşkilat daxilində şəbəkənin həssas hissələrinə daxil olan və onlara verilən etimaddan sui-istifadə edərək prosesləri idarə etmə imkanı olan insan faktorudur.



Şəkil 2: Müxtəlif təbəqələrə təhlükəsizlik hücumları

2.Hakerlər / Kibercinayətkarlar: Bu təcavüzkarlar sistemdə istənilən təhlükəli fəsadların törədilməsinə səbəb olurlar.

3.Rəqib hökumətlər : Hökümətlər kəşfiyat məlumatlarını əldə etmək, iqtisadi inkişafı ləngitmək və ya infrastruktura zərər vermək üçün dövlət təşkilatlarına haker hücumlarını

təşkil edirlər.

4. Rəqib təşkilatlar: Müxtəlif terrorçu qruplar kimi təşkilatlar da özlərinin rəqib münasibətləri səbəbindən digər təşkilatlara qarşı kiberhücum təşkil edə bilərlər.

Birmənalı olaraq şəbəkə sistemi tamamilə etibarlı olmadığından kiber-fiziki sistemə hücum edilmə şansı həmişə mövcuddur. Ona görə də kiber-fiziki sistemdə hansısa hücum aşkar edildikdə sistemin etibarlı təhlükəsizliyini və çevikliyini təmin etmək üçün müvafiq tədbirlər görülməlidir.

1. Proqnozlaşdırma mexanizmləri: Sistemin uğursuz, zərərli fəaliyyətini proqnozlaşdırmaq

üçün müəyyən alqoritm tətbiq edilir.

2. Kiber-fiziki sistem (KFS) üçün hazırlanmış xüsusi proqram təminatı tətbiq edilir.

Bu mexanizmlərin reallaşdırılması üçün məlumatları birbaşa əldə etməyə imkan verən, hissetmə və rabitə imkanları olan Things of Internet (IoT) fiziki obyektlər şəbəkəsi istifadə edilmişdir.

IoT, fərdlərə və ya obyektlərə fərqli identifikatorları təqdim edən və İnternetdən istifadə edərək onları birləşdirən və məlumatları insan qarşılıqlılığı olmadan ötürən bir çərçivədir. Hər bir şəbəkədə kiber-fiziki sistemlər kimi, təhlükəsizliyə nail olmaq üçün qulaq asma əleyhinə, məxfilik, şifrələmə, girişə nəzarətin identifikasiyası tələbi ilə etibarlı əlaqə nöqtəsi və təhlükəsizlik və məxfilik məsələlərini dəstəkləyən yanaşmalar tələb olunur. Təhlükəsiz bir saxlama üçün şifrələmə alqoritmlərinə əsaslanan və məlumatın qorunmasını təmin edən bir cihaz lazımdır. Doğrulama, məlumat inteqrasiyası, cihazın mövcudluğu, məlumatların məxfiliyi və məxfilik IoT cihazları arasında effektiv və etibarlı əlaqə üçün diqqətəlayiq xüsusiyyətlərdən biridir.

**Nəticə**

Kiber-fiziki sistemlər kiber və fiziki komponentlərin tərkib hissəsi olmaqla, çoxlu sayda məlumatların emal edilməsi və saxlanması imkanı olan bütün tətbiqlərə birmənalı inteqrasiya olunur. Bu sistemlərin üstün cəhəti ixtiyari məlumatın bir şəbəkədə birləşməsi və böyük həcmdə məlumatların etibarlı ötürülməsini və saxlanmasını tələb edən komponentlərdən istifadə edilməsinin mümkünlüyüdür. IoT-nin fiziki komponentləri böyük məlumatların bir-birinə bağlantısını və girişini tələb etdiyindən, şəbəkəyə girişi təmin edən bulud hesablama texnologiyası tətbiq olunur. Bundan əlavə, kiber-fiziki sistemlərin qurğuları və tətbiqi proqramları müxtəlif hücum və təhdidlərə qarşı çox həssas olmalıdır.

İstifadə olunan ədəbiyyat

1. Tang, Lu-An, et al. “Trustworthiness analysis of sensor data in cyber-physical systems”. Journal of Computer and System Sciences, vol. 79, no. 3, pp.383–401, 2013.
2. Wang, Eric Ke, Yunming Ye, Xiaofei Xu, Siu-Ming Yiu. “Security issues and challenges for cyber physical system”. IEEE Green Computing and Communications (GreenCom), ACM Int’lst International Conference on Cyber, Physical and Social Computing (KFSCom), pp.733–738, 2010.
3. Gunes, Volkan, Steffen Peter, Tony Givargis, and Frank Vahid. “A survey on concepts, applications, and challenges in cyber-physical systems”. KSII Transactions on Internet & Information Systems, vol. 8, no. 12, 2014.
4. Govindarasu, Manimaran, Adam Hann, and Peter Sauer. “Cyber-physical systems security for smart grid”. Future Grid Initiative White Paper, PSERC, Feb, 2012.
5. Sridhar, Siddharth, et al. “Cyber-Physical System Security for the Electric Power Grid”. Proceedings of the IEEE 100, no. 1, pp.210–224, 2012.
6. Bertino, Elisa. ‘data-opportunities and challenges”. In Proceedings of the IEEE 37th Annual Computer Software and Applications Conference, pp.479–480, 2013.
7. Zhang, Lichen. “An approach to model complex big data driven cyber physical systems”. In International Conference on Algorithms and Architectures for Parallel Processing, Springer, Cham, pp.740–754, 2014.