# Kritik İnfrastruktur Obyektlərində SCADA Sistemlərinin Kibertəhlükəsizliyi və Kiberkriminalistik Təhlili Metodları

Mehdi Əhmədov[1], Təbriz Cəfərov[2]
[1]Sumqayıt Dövlət Universiteti, Sumqayıt, Azərbaycan
[2]ADA Universiteti , Bakı Azərbaycan
[1]*mehdi.ehemdov077@gmail.com*, [2]*tjafarov@ada.edu.az*

***Xülasə*— Bu məqalədə kritik infrastruktur obyektlərində istifadə olunan SCADA (Supervisory Control and Data Acquisition) sistemlərinin kibertəhlükəsizlik problemləri təhlil edilir. SCADA sistemlərinin enerji və sənaye sahələrində rolu nəzərə alınaraq əsas risklər müəyyən olunur. Eyni zamanda jurnal qeydlərinin analizi (log analysis), şəbəkə trafikinin analizi (traffic analysis) və hadisə xronologiyasının qurulması kimi kiberkriminalistik metodlar araşdırılır. Məqalədə SCADA sistemləri üçün paylanmış və hibrid arxitektura modeli təklif edilir.**

***Açar sözlər*— *SCADA sistemi; kibertəhlükəsizlik; kritik infrastruktur; SIEM; kiberkriminalistika.***

## I. GİRİŞ

Müasir dövrdə sənaye və energetika sistemlərinin rəqəmsallaşdırılması idarəetmə proseslərinin avtomatlaşdırılmasına və səmərəliliyinin yüksəlməsinə səbəb olmuşdur. SCADA (Supervisory Control and Data Acquisition) sistemləri bu prosesdə əsas idarəetmə vasitəsi kimi çıxış edir və kritik infrastruktur obyektlərinin idarə olunmasını təmin edir. Lakin SCADA sistemlərinin şəbəkə mühitinə inteqrasiyası onların kiberhücumlara qarşı həssaslığını artırır. Bu səbəbdən SCADA sistemlərində kiber təhlükəsizlik məsələlərinin araşdırılması aktual elmi-praktiki problem kimi çıxış edir.

## II. SCADA SİSTEMLƏRİNİN MAHİYYƏTİ VƏ İŞLƏMƏ PRİNSİPİ

SCADA (Supervisory Control and Data Acquisition) sistemləri sənaye və enerji infrastrukturunda texnoloji proseslərin uzaqdan idarə olunması və monitorinqi üçün istifadə olunan kompleks avtomatlaşdırma sistemləridir [1, 2]. Bu sistemlər real-vaxt rejimində məlumatların toplanmasını, emalını və operatora təqdim olunmasını təmin edir. SCADA sistemlərinin əsas məqsədi istehsal və ötürmə proseslərinin təhlükəsiz, fasiləsiz və səmərəli şəkildə idarə edilməsidir. SCADA sistemlərinin əsas funksiyalarına məlumatların toplanması, proseslərin monitorinqi, uzaqdan idarəetmə, siqnalizasiya sistemi və məlumatların arxivləşdirilməsi daxildir [1]. Bu funksiyalar vasitəsilə operatorlar sistemin cari vəziyyətini izləyə və zəruri hallarda idarəetmə prosesinə müdaxilə edə bilirlər.

SCADA sistemləri bir neçə əsas komponentdən ibarətdir. Bunlara proqramlaşdırıla bilən loji kontrollerlər (Programmable Logic Controller – PLC), uzaq terminal qurğuları (Remote Terminal Unit – RTU), insan-maşın interfeysi (Human-Machine Interface – HMI) və mərkəzi serverlər daxildir [1, 2]. PLC və RTU-lar sahə səviyyəsində yerləşərək sensor və icraedici qurğulardan məlumat toplayır, həmçinin idarəetmə əmrlərinin icrasını təmin edir. HMI sistemi operatora vizual interfeys təqdim edir, serverlər isə məlumatların emalını və saxlanılmasını təmin edir.

SCADA sistemlərinin arxitekturası adətən çoxsəviyyəli struktur üzrə qurulur. Bu struktur sahə səviyyəsi, idarəetmə səviyyəsi və nəzarət səviyyəsindən ibarətdir [1]. Sahə səviyyəsində sensorlar və icraedici qurğular, idarəetmə səviyyəsində PLC və RTU-lar, nəzarət səviyyəsində isə SCADA serverləri və HMI sistemləri yerləşir. Müasir SCADA sistemləri şəbəkə texnologiyalarından istifadə etməklə müxtəlif obyektlər arasında məlumat mübadiləsini təmin edir.

SCADA sistemlərinin fəaliyyətində informasiya texnologiyaları (Information Technology – IT) və əməliyyat texnologiyaları (Operational Technology – OT) mühitləri arasında fərqlər mühüm rol oynayır [3, 4]. IT sistemləri əsasən məlumatların saxlanması və emalına yönəldiyi halda, OT sistemləri fiziki proseslərin idarə olunmasına xidmət edir. OT mühitində real-vaxt rejimi, aşağı gecikmə və sistemin fasiləsiz fəaliyyəti əsas prioritetlərdir. Bu səbəbdən IT sistemlərində tətbiq olunan bəzi təhlükəsizlik və idarəetmə yanaşmaları OT mühitində birbaşa tətbiq oluna bilmir.

Beləliklə, SCADA sistemləri müasir sənaye və enerji infrastrukturlarının əsas idarəetmə vasitəsi kimi çıxış edir. Bu sistemlərin düzgün qurulması texnoloji proseslərin fasiləsizliyi, operativ idarəetmə və kiber təhlükəsizlik baxımından mühüm əhəmiyyət daşıyır.

## III. SCADA SİSTEMLƏRİNİN DÖVLƏT VƏ KRİTİK İNFRASTRUKTUR ÜÇÜN MAHİYYƏTİ

SCADA sistemləri müasir dövlətlərin idarəetmə və təhlükəsizlik mexanizmlərində mühüm rol oynayan texnoloji platformalardan biridir. Xüsusilə kritik infrastruktur obyektlərində – enerji, su təchizatı, nəqliyyat və sənaye sahələrində – bu sistemlər texnoloji proseslərin fasiləsiz və təhlükəsiz şəkildə idarə olunmasını təmin edir [5, 6]. Dövlət səviyyəsində SCADA sistemlərinin tətbiqi yalnız texniki

7DOI: 10.25045/forensic.gov.2026.57

idarəetmə vasitəsi kimi deyil, həm də strateji nəzarət və qərar qəbuletmə aləti kimi qiymətləndirilir [3, 4].

Azərbaycan Respublikasında kritik infrastrukturun qorunması və idarə olunması hüquqi baxımdan da tənzimlənir. "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının müvafiq qanunun 1-ci maddəsinə görə, Azərbaycan Respublikasının milli təhlükəsizliyi dövlətin müstəqilliyinin, suverenliyinin, ərazi bütövlüyünün, konstitusiya quruluşunun, xalqın və ölkənin milli maraqlarının, insanın, cəmiyyətin və dövlətin hüquq və mənafelərinin daxili və xarici təhdidlərdən qorunmasının təmin edilməsidir [7].

Azərbaycan Respublikasının "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunu ilə kritik informasiya infrastrukturu dövlət idarəçiliyi, müdafiə, səhiyyə, maliyyə bazarları, energetika, nəqliyyat, informasiya texnologiyaları, telekommunikasiya, su təchizatı və ekologiya sahələrində fəaliyyəti təmin edən, funksionallığının pozulması dövlətin, cəmiyyətin və vətəndaşların maraqlarına mühüm zərər vura bilən informasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və informasiya-kommunikasiya şəbəkələrinin məcmusu kimi müəyyən edilir [8].

Azərbaycan Respublikası Prezidentinin 28 avqust 2023-cü il tarixli sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası" dövlətin, cəmiyyətin və insanların informasiya-kommunikasiya texnologiyalarından (İKT) təhlükəsiz istifadəsinin təmin edilməsinə, milli informasiya təhlükəsizliyi səviyyəsinin yüksəldilməsinə, dövlət və özəl şəbəkələrin, həmçinin kritik informasiya infrastrukturlarının təhlükəsizliyinin gücləndirilməsinə xidmət edir [9].

"Azərbaycan Respublikasının Milli Təhlükəsizlik Konsepsiyası"nda informasiya təhlükəsizliyi siyasətinə xüsusi bölmə ayrılmışdır [10]. Konsepsiyaya görə, ölkədə informasiyanın, dövlət informasiya ehtiyatlarının və informasiya infrastrukturunun müdafiəsi üzrə milli sistem inkişaf etdirilir və möhkəmləndirilir. Bu istiqamətdə 17 iyul 2023-cü ildə "Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları"nın təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı qəbul edilmişdir [11].

Bu çərçivədə enerji infrastrukturu və ona xidmət edən SCADA sistemləri dövlətin təhlükəsizlik siyasətinin mühüm elementi hesab olunur [3]. Bundan əlavə, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu informasiya sistemlərinin, o cümlədən SCADA kimi idarəetmə sistemlərinin təhlükəsizliyinin təmin edilməsini hüquqi müstəvidə tənzimləyir [8]. Qanunda informasiya resurslarının qorunması, icazəsiz müdaxilələrin qarşısının alınması və məlumatların təhlükəsizliyinin təmin olunması əsas prinsip kimi müəyyən edilmişdir.

Kritik informasiya infrastrukturu sahəsində Azərbaycan Respublikası Prezidentinin 17 aprel 2021-ci il tarixli fərmanı ilə hüquqi və institusional əsaslar formalaşdırılmış, 27 may 2022-ci il tarixli qanun dəyişiklikləri ilə isə kritik informasiya infrastrukturu anlayışı daha da dəqiqləşdirilmiş və təhlükəsizlik tələbləri gücləndirilmişdir. Bu normativ sənədlər SCADA sistemlərinin də daxil olduğu enerji və sənaye obyektlərinin xüsusi qorunan obyektlər kimi qiymətləndirilməsini təmin edir [8, 11].

Enerji təhlükəsizliyi dövlət təhlükəsizliyinin ayrılmaz tərkib hissəsidir və bu sahədə SCADA sistemlərinin rolu əvəzolunmazdır. Elektrik şəbəkələrinin idarə olunması, qəza hallarının vaxtında aşkarlanması və enerji balansının qorunması məhz bu sistemlər vasitəsilə həyata keçirilir [12, 13]. SCADA sistemləri enerji axınlarının monitorinqinə və operativ idarəetməyə imkan verərək enerji sisteminin dayanıqlılığını artırır.

Milli təhlükəsizlik baxımından SCADA sistemləri strateji əhəmiyyət daşıyan obyektlərdə geniş tətbiq olunur. Elektrik stansiyaları, yarımstansiyalar, neft-qaz emalı müəssisələri kimi obyektlərdə bu sistemlərin işləməsi iqtisadi və sosial sabitlik üçün kritik əhəmiyyətə malikdir [5, 14]. Bu səbəbdən SCADA sistemlərinin təhlükəsizliyi dövlət səviyyəsində nəzarətdə saxlanılır və onların qorunması üçün xüsusi hüquqi və texniki tədbirlər həyata keçirilir [3, 6].

Nəticə etibarilə, SCADA sistemləri Azərbaycan Respublikasında kritik infrastrukturun idarə olunması, enerji təhlükəsizliyinin təmin edilməsi və milli təhlükəsizliyin qorunması baxımından strateji əhəmiyyətə malikdir. Bu sistemlərin hüquqi əsaslarla qorunması və inkişaf etdirilməsi dövlətin prioritet istiqamətlərindən biri hesab olunur.

## IV. SCADA SİSTEMLƏRİNİN KRİTİK İNFRASTRUKTUR SAHƏLƏRİNDƏ TƏTBİQİ

SCADA sistemləri kritik infrastruktur sahələrində texnoloji proseslərin avtomatlaşdırılması, monitorinqi və operativ idarə olunması üçün geniş tətbiq olunur [1, 2]. Bu sistemlər real-vaxt rejimində məlumatların toplanmasını, emalını və vizuallaşdırılmasını təmin edərək obyektlərin təhlükəsiz və fasiləsiz fəaliyyətinə şərait yaradır. Müxtəlif sahələrdə SCADA sistemlərinin tətbiqi həmin sektorların texnoloji və idarəetmə xüsusiyyətlərinə uyğun şəkildə formalaşır.

Enerji sektorunda, yəni istehsal, ötürmə və paylanma mərhələlərində SCADA sistemləri elektrik enerjisinin idarə olunmasında əsas texnoloji vasitələrdən biri kimi çıxış edir [12, 13]. Elektrik stansiyalarında istehsal proseslərinə nəzarət, generatorların işləmə parametrlərinin izlənilməsi və enerji istehsalının optimallaşdırılması bu sistemlər vasitəsilə həyata keçirilir. Yarımstansiyalarda gərginlik səviyyəsinin tənzimlənməsi, kommutasiya qurğularının (switchgear) idarə olunması və qəza hallarında operativ müdaxilə SCADA sistemlərinin əsas funksiyalarına daxildir.

Neft-qaz sənayesində SCADA sistemləri hasilat, emal və nəql proseslərinin kompleks şəkildə idarə olunmasında mühüm rol oynayır [1, 5]. Neft və qaz quyularında hasilat proseslərinin monitorinqi, boru kəmərlərində təzyiq və axın səviyyələrinin nəzarətdə saxlanılması, nasos və kompressor stansiyalarının idarə olunması bu sistemlər vasitəsilə təmin edilir. Potensial sızmaların və texniki nasazlıqların vaxtında aşkarlanması isə ekoloji və iqtisadi risklərin azalmasına kömək edir.

Su və kanalizasiya sistemlərində SCADA texnologiyaları

suyun təmizlənməsi, saxlanması və paylanması proseslərinin avtomatlaşdırılmasını təmin edir [1, 6]. Su anbarlarında səviyyə nəzarəti, nasos stansiyalarının idarə olunması, suyun keyfiyyət göstəricilərinin monitorinqi və təmizləyici qurğuların fəaliyyəti SCADA sistemləri vasitəsilə izlənilir. Kanalizasiya sistemlərində isə tullantı sularının toplanması, daşınması və təmizlənməsi prosesləri nəzarətdə saxlanılır ki, bu da sanitariya təhlükəsizliyi və ətraf mühitin qorunması baxımından mühüm əhəmiyyət daşıyır.

Nəqliyyat və logistika sistemlərində SCADA sistemləri müxtəlif nəqliyyat infrastrukturlarının idarə olunmasında istifadə olunur [1, 2]. Dəmir yolu sistemlərində siqnalizasiya və hərəkətə nəzarət, avtomobil yollarında trafik idarəetmə sistemləri, hava limanlarında və limanlarda logistika əməliyyatlarının koordinasiyası SCADA texnologiyalarının tətbiqi ilə həyata keçirilir. Bu sistemlər nəqliyyat axınının optimallaşdırılmasına, təhlükəsizliyin artırılmasına və gecikmələrin minimuma endirilməsinə imkan verir.

Sənaye və istehsalat müəssisələrində SCADA sistemləri istehsal proseslərinin avtomatlaşdırılması və optimallaşdırılması üçün geniş istifadə olunur [1, 2]. Metallurgiya, kimya, qida sənayesi və digər istehsalat sahələrində texnoloji proseslər SCADA vasitəsilə nəzarətdə saxlanılır. Avadanlıqların işləmə vəziyyətinin izlənilməsi, istehsal parametrlərinin tənzimlənməsi və məhsuldarlığın artırılması bu sistemlərin əsas üstünlüklərindəndir.

Beləliklə, SCADA sistemləri müxtəlif kritik infrastruktur sahələrində proseslərin avtomatlaşdırılmasını, təhlükəsizliyini və səmərəliliyini təmin edən əsas texnoloji platforma kimi çıxış edir [5, 6]. Bu sistemlərin geniş tətbiqi müasir sənaye və dövlət infrastrukturlarının dayanıqlı inkişafı üçün mühüm şərtdir.

## V. SCADA SİSTEMLƏRİNDƏ KİBERTƏHLÜKƏSİZLİK PROBLEMLƏRİ

SCADA sistemləri kritik infrastrukturun əsas idarəetmə komponentlərindən biri olduğuna görə onların kiber təhlükəsizliyi xüsusi əhəmiyyət kəsb edir [15, 2]. Bu sistemlər əvvəllər əsasən qapalı və izolyasiya olunmuş mühitdə fəaliyyət göstərsə də, müasir dövrdə şəbəkə texnologiyalarının və uzaqdan idarəetmənin tətbiqi nəticəsində xarici şəbəkələrlə inteqrasiya olunmuşdur. Bu isə SCADA sistemlərini müxtəlif kibertəhlükələrə daha həssas vəziyyətə gətirmişdir.

SCADA sistemlərində əsas problemlərdən biri onların ilkin dizayn mərhələsində kiber təhlükəsizlik amillərinin tam nəzərə alınmamasıdır [3, 2]. Bu sistemlər daha çox funksionallıq və operativlik prinsipi əsasında qurulduğuna görə təhlükəsizlik mexanizmləri bir çox hallarda sonradan əlavə olunmuşdur. Nəticədə bəzi SCADA sistemlərində autentifikasiya və şifrələmə mexanizmləri zəif və ya qeyri-kafi səviyyədə qalır.

Şəbəkə səviyyəsində SCADA sistemləri müxtəlif kiber hücumlara məruz qala bilər. Bu hücumlara icazəsiz giriş, şəbəkə trafikinin dinlənilməsi (sniffing), məlumatların dəyişdirilməsi və manipulyasiyası (tampering), həmçinin araya girmə hücumu (man-in-the-middle) daxildir [15, 2]. Xüsusilə bəzi sənaye protokollarının, məsələn, Modbus və ya bəzi hallarda Beynəlxalq Elektrotexnika Komissiyasının 61850 standartı (IEC 61850) tətbiqlərinin təhlükəsizlik baxımından zəif konfiqurasiya olunması hücum ehtimalını artırır [12, 13].

SCADA sistemlərində geniş yayılmış təhlükələrdən biri də xidmətdən imtina və paylanmış xidmətdən imtina (DDoS) hücumlarıdır (DoS/DDoS) [2, 6]. Bu tip hücumlar nəticəsində idarəetmə sistemlərinin fəaliyyəti müvəqqəti və ya tam dayana bilər. Bu isə enerji sistemlərində, istehsalat müəssisələrində və digər kritik obyektlərdə ciddi nəticələrə səbəb olur, operativ idarəetməni çətinləşdirir və qəza risklərini artırır.

Digər mühüm problem insan faktoru ilə bağlıdır. SCADA sistemlərində çalışan operatorların və texniki heyətin təhlükəsizlik qaydalarına tam riayət etməməsi, zəif parollardan istifadə etməsi və ya sosial mühəndislik hücumlarına qarşı hazırlıqsız olması sistem üçün əlavə risk yaradır [1, 15]. Xüsusilə daxili təhlükə (insider threat) faktorları bu sahədə ciddi problemlərdən biri hesab olunur.

SCADA sistemlərində proqram təminatı və avadanlıqların yenilənməsi də çətinlik yaradır [1, 2]. Əməliyyat texnologiyaları (OT) mühitində sistemlərin fasiləsiz işləməsi tələb olunduğuna görə yenilənmələrin idarə edilməsi (patch management) hər zaman vaxtında həyata keçirilmir. Bu isə köhnə və zəifliklər məlum olan sistemlərin istifadədə qalmasına səbəb olur və hücumçular üçün əlavə imkanlar yaradır.

Bundan əlavə, SCADA sistemlərinin informasiya texnologiyaları (IT) şəbəkələri ilə inteqrasiyası da təhlükəsizlik risklərini artırır [1, 3]. IT mühitində baş verən kiber insidentlər OT sistemlərinə keçərək daha ciddi nəticələrə səbəb ola bilər. Bu səbəbdən IT və OT sistemləri arasında düzgün təhlükəsizlik sərhədlərinin qurulmaması ciddi boşluq kimi qiymətləndirilir [4, 16].

Nəticə olaraq, SCADA sistemlərində kibertəhlükəsizlik problemləri çoxşaxəli olub texniki, təşkilati və insan faktorları ilə bağlıdır. Bu problemlərin mövcudluğu kritik infrastrukturun təhlükəsizliyinə birbaşa təsir göstərdiyindən onların aradan qaldırılması kompleks və sistemli yanaşma tələb edir.

## VI. SCADA SİSTEMLƏRİ ÜÇÜN OPTİMAL KİBERTƏHLÜKƏSİZLİK HƏLLƏRİ

SCADA sistemlərinin təhlükəsizliyinin təmin edilməsi üçün yalnız bir müdafiə mexanizmi kifayət etmir. Bu sahədə texniki, təşkilati və arxitektura səviyyəsində kompleks yanaşma tətbiq olunmalıdır [1, 4, 16]. Xüsusilə kritik infrastruktur obyektlərində SCADA sistemləri real-vaxt rejimində işlədiyi üçün təhlükəsizlik tədbirləri həm sistemi qorumalı, həm də onun fasiləsiz fəaliyyətinə mane olmamalıdır [1, 3].

### *A. Texniki həllər*

SCADA sistemlərində əsas təhlükəsizlik tədbirlərindən biri şəbəkə segmentasiyasıdır [1, 16]. Bu yanaşmada informasiya texnologiyaları (IT) və OT şəbəkələri bir-birindən ayrılır, idarəetmə sistemlərinə birbaşa giriş məhdudlaşdırılır. Şəbəkənin ayrı-ayrı zonalara bölünməsi hücumun bir sahədən digər sahəyə yayılmasının qarşısını alır.

Bundan əlavə, sənaye idarəetmə sistemləri üçün şəbəkə təhlükəsizlik divarı (Industrial Control Systems firewall – ICS firewall) və sənaye mühitinə uyğun təhlükəsizlik

mexanizmlərinin tətbiqi vacibdir [1, 16]. Bu təhlükəsizlik divarları adi IT təhlükəsizlik divarlarından fərqli olaraq SCADA protokollarını və sənaye trafikini nəzərə almalıdır. Onlar yalnız icazə verilmiş bağlantılara və əmrlərə icazə verməli, şübhəli fəaliyyətləri bloklamalıdır.

Digər mühüm istiqamət girişə nəzarət (access control) və identifikasiya mexanizmləridir [1, 4]. SCADA sistemlərinə giriş yalnız səlahiyyətli şəxslərə verilməli, istifadəçilər rol əsaslı idarə olunmalıdır. Güclü parol siyasəti, çoxfaktorlu identifikasiya və operator fəaliyyətlərinin qeydiyyatı icazəsiz giriş risklərini azaldır.

### *B. Arxitektura yanaşması*

SCADA sistemləri üçün optimal yanaşmalardan biri hibrid SCADA modeli hesab oluna bilər [1, 3]. Bu modeldə idarəetmə yalnız bir mərkəzdən asılı olmur. Hər bir stansiyada lokal SCADA sistemi saxlanılır, regional səviyyədə Sub-SCADA mərkəzləri yaradılır, mərkəzi səviyyədə isə ümumi nəzarət və koordinasiya təmin edilir.

Bu yanaşmada lokal, regional və mərkəzi idarəetmə prinsipi tətbiq olunur. Lokal SCADA sistemi obyektin gündəlik idarə olunmasını təmin edir. Regional Sub-SCADA mərkəzləri bir neçə stansiyanın fəaliyyətinə nəzarət edir və ehtiyat idarəetmə funksiyasını yerinə yetirir. Mərkəzi SCADA isə ümumi monitorinq, koordinasiya və kiber nəzarət funksiyasını daşıyır.

Bu modelin əsas üstünlüyü ondan ibarətdir ki, mərkəzlə əlaqə kəsildikdə belə lokal və regional sistemlər öz fəaliyyətini davam etdirə bilir [3, 4]. Bu, SCADA sistemlərinin dayanıqlılığını artırır və tək nöqtədən asılılıq riskini azaldır.

Bundan əlavə, paylanmış məlumat modeli (distributed data) və replikasiya (replication) yanaşması tətbiq oluna bilər. Bu zaman məlumatlar yalnız mərkəzi bazada saxlanılmır, həm də lokal və regional səviyyələrdə qorunur. Məlumatların sinxronlaşdırılması nəticəsində həm ümumi nəzarət təmin olunur, həm də qəza və ya hücum zamanı məlumat itkisi riski azalır [1, 3].

### *C. Monitorinq və nəzarət*

SCADA sistemlərinin təhlükəsizliyində davamlı monitorinq xüsusi əhəmiyyət daşıyır. Bu məqsədlə təhlükəsizlik məlumatları və hadisələrinin idarə edilməsi sistemi (Security Information and Event Management – SIEM) tətbiq olunmalıdır [4, 6]. SIEM müxtəlif mənbələrdən gələn jurnal qeydlərini (logs) və təhlükəsizlik hadisələrini toplayaraq analiz edir, şübhəli fəaliyyətləri müəyyənləşdirir və təhlükəsizlik komandalarına xəbərdarlıq edir.

Jurnal qeydlərinin analizi (log analysis) kiber hadisələrin araşdırılması üçün əsas vasitələrdən biridir [1, 2]. SCADA serverləri, insan-maşın interfeysi (HMI) sistemləri, təhlükəsizlik divarları, operator girişləri və şəbəkə avadanlıqlarından toplanan jurnal qeydləri hücumun mənbəyini, vaxtını və təsirini müəyyən etməyə imkan verir. Bu yanaşma həm təhlükənin aşkarlanması, həm də sonrakı kiberkriminalistik təhlil üçün vacibdir.

Bundan əlavə, anomaliyaların aşkarlanması (anomaly detection) texnologiyalarının tətbiqi SCADA sistemlərində qeyri-adi davranışların aşkarlanmasına kömək edir [2, 15]. Normal trafik və sistem davranışı müəyyən edildikdən sonra ondan kənara çıxan fəaliyyətlər avtomatik olaraq şübhəli hadisə kimi qiymətləndirilir. Bu üsul xüsusilə gizli və yavaş inkişaf edən hücumların erkən mərhələdə aşkarlanması üçün effektivdir.

Nəticə etibarilə, SCADA sistemlərinin kiber təhlükəsizliyi üçün ən optimal yanaşma texniki müdafiə, hibrid arxitektura və mərkəzləşdirilmiş monitorinq mexanizmlərinin birlikdə tətbiqidir [1, 4, 16]. Bu model həm sistemin dayanıqlılığını artırır, həm də kiber insidentlərin vaxtında aşkar olunmasına və araşdırılmasına imkan yaradır.

## VII. SCADA SİSTEMLƏRİNDƏ KİBERKRİMİNALİSTİKA VƏ HADİSƏ ANALİZİ

SCADA sistemlərində rəqəmsal kriminalistika (digital forensics) kritik infrastrukturda baş verən kiber hadisələrin aşkar edilməsi, araşdırılması və sübutların toplanması prosesini əhatə edir [1, 6]. Bu prosesin əsas məqsədi hücumun mənbəyini, istifadə olunan metodları və sistemə təsirini müəyyən etməkdir. SCADA mühitində kriminalistika klassik IT sistemlərindən fərqlənir, çünki burada yalnız informasiya deyil, həm də enerji axını, təzyiq və temperatur kimi fiziki proseslər idarə olunur [1, 3]. Buna görə də hər hansı kiber insident real texniki və iqtisadi nəticələrə səbəb ola bilər.

Rəqəmsal kriminalistika kompüter sistemlərində və şəbəkələrdə baş verən hadisələrin elmi əsaslarla araşdırılmasıdır [1]. SCADA mühitində bu anlayış daha geniş məna daşıyır və həm proqram təminatının, həm də fiziki proseslərin analizini əhatə edir. Bu sahədə əsas məqsəd hücumun mərhələlərini müəyyən etmək, istifadə olunan zəiflikləri aşkar etmək və sübutları hüquqi baxımdan etibarlı formada təqdim etməkdir. SCADA sistemlərində kriminalistik proses adətən hadisənin aşkarlanması, sübutların toplanması, analiz və hesabat mərhələlərindən ibarət olur.

SCADA sistemlərində sübutların toplanması çoxmənbəli və həssas prosesdir [1, 6]. Sübutlar əsasən SCADA serverlərindən, tarixi məlumat bazalarından (historian databases), insan-maşın interfeysi (HMI) qeydlərindən, operator fəaliyyətlərindən, PLC və RTU cihazlarının yaddaşından, şəbəkə avadanlıqları və təhlükəsizlik divarı (firewall) qeydlərindən əldə olunur. Bu prosesdə əsas prinsip sübutların dəyişdirilmədən qorunmasıdır. Bunun üçün məlumatlar yalnız oxuma rejimində (read-only mode) çıxarılır, ehtiyat nüsxələr yaradılır və məlumatların bütövlüyü heş qiymətləri (hash values) vasitəsilə yoxlanılır. SCADA sistemlərində əlavə çətinlik ondan ibarətdir ki, analiz çox vaxt sistem dayandırılmadan aparılmalıdır. Bu səbəbdən canlı kriminalistik analiz (live forensics) yanaşmasından istifadə olunur [1].

SCADA sistemlərində jurnal qeydlərinin analizi (log analysis) kiber hadisələrin araşdırılmasının əsasını təşkil edir [1,2]. Jurnal qeydlərində operator girişləri, sistem dəyişiklikləri, siqnalizasiya hadisələri və texniki nasazlıqlar əks olunur. Bu məlumatların təhlili vasitəsilə icazəsiz giriş cəhdləri, sistemdə qeyri-adi dəyişikliklər və istifadəçi fəaliyyətində anomaliyalar müəyyən edilə bilər. Şəbəkə trafikinin analizi (traffic analysis) isə SCADA sistemlərində baş verən məlumat mübadiləsini araşdırmağa imkan verir [1], [2]. Bu zaman IEC 61850, Modbus və digər sənaye protokolları üzərindən ötürülən paketlər təhlil

olunur. Trafik analizi vasitəsilə araya girmə hücumu (man-in-the-middle), paket manipulyasiyası və qeyri-adi trafik davranışları aşkarlana bilər. Bu yanaşma xüsusilə gizli və uzunmüddətli hücumların müəyyən edilməsində effektivdir.

Kiberkriminalistik analizdə ən vacib mərhələlərdən biri hadisələrin xronologiyasının qurulmasıdır [1]. Bu mərhələdə müxtəlif mənbələrdən toplanan məlumatlar, yəni jurnal qeydləri, sistem qeydləri və şəbəkə trafiki birləşdirilərək hadisələrin ardıcıllığı müəyyən edilir. Xronologiya qurulduqdan sonra hücumun nə vaxt başladığı, hansı mərhələlərdən keçdiyi, sistemə hansı təsirləri göstərdiyi və hansı zəiflikdən istifadə etdiyi müəyyən oluna bilər. Bu analiz həm hadisənin tam başa düşülməsinə, həm də gələcəkdə oxşar hücumların qarşısının alınmasına kömək edir [2, 15].

SCADA sistemlərində kiberkriminalistika yalnız texniki analiz prosesi deyil, həm də təhlükəsizlik strategiyasının mühüm hissəsidir [1, 6]. Sübutların düzgün toplanması, jurnal qeydləri və şəbəkə trafikinin analizi, həmçinin hadisə xronologiyasının qurulması kiber insidentlərin effektiv araşdırılmasına imkan yaradır. Bu yanaşma həm mövcud təhlükələrin aradan qaldırılmasına, həm də gələcək risklərin minimuma endirilməsinə xidmət edir.

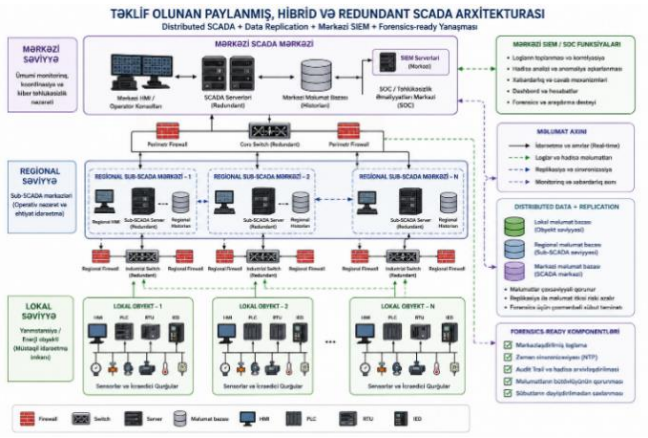
## VIII. Təklif Olunan Model Və Praktiki Yanaşma

Bu tədqiqatda kritik infrastruktur obyektlərində SCADA sistemlərinin kiber təhlükəsizliyinin gücləndirilməsi, idarəetmənin fasiləsizliyinin təmin olunması və kiber insidentlərin kriminalistik baxımdan daha operativ araşdırılması üçün paylanmış, hibrid və ehtiyatlı arxitektura (redundant architecture) modeli təklif olunur. Bu yanaşmanın əsas məqsədi SCADA sistemlərinin yalnız mərkəzi idarəetmədən asılı qalmadan lokal və regional səviyyələrdə də dayanıqlı fəaliyyət göstərməsini təmin etməkdir.

Təklif olunan modeldə SCADA idarəetməsi üç əsas səviyyə üzrə təşkil edilir: lokal, regional və mərkəzi səviyyə. Lokal səviyyədə hər bir yarımstansiya və ya enerji obyekti müstəqil SCADA idarəetmə imkanına malik olur. Bu səviyyədə HMI, PLC, RTU, ağıllı elektron qurğu (Intelligent Electronic Device – IED) və digər texnoloji avadanlıqlar vasitəsilə obyektin real-vaxt rejimində monitorinqi və idarə olunması həyata keçirilir. Beləliklə, mərkəzi sistemlə əlaqə kəsildiyi halda belə obyekt öz texnoloji funksiyalarını davam etdirə bilir. Təklif olunan modelin ümumi quruluşu, səviyyələrarası əlaqə, məlumat axını və mərkəzi SIEM/SOC inteqrasiyası Şəkil 1-də göstərilmişdir.

Regional səviyyədə bir neçə lokal obyektin fəaliyyətini əlaqələndirən Sub-SCADA mərkəzləri yaradılır. Bu mərkəzlər həm operativ nəzarət, həm də ehtiyat idarəetmə funksiyasını yerinə yetirir. Regional səviyyənin mövcudluğu mərkəzi sistemdə texniki nasazlıq, rabitə problemi və ya kiber insident baş verdiyi hallarda sistemin tam dayanmasının qarşısını alır və ümumi dayanıqlılığı artırır.

Mərkəzi səviyyədə ümumi monitorinq, koordinasiya və kiber təhlükəsizlik nəzarəti həyata keçirilir. Burada mərkəzi SCADA nəzarət sistemi ilə yanaşı, təhlükəsizlik məlumatları və hadisələrinin idarə edilməsi sistemi (Security Information and Event Management – SIEM) və təhlükəsizlik əməliyyatları mərkəzi (Security Operations Center – SOC) infrastrukturu yerləşdirilir. Mərkəzi SIEM sistemi lokal və regional səviyyələrdən daxil olan jurnal qeydlərini (logs), hadisə qeydlərini və təhlükəsizlik siqnallarını toplayaraq analiz edir. Bu yanaşma ayrı-ayrı obyektlərdə baş verən hadisələrin vahid mərkəzdən izlənilməsinə və əlaqəli hücumların daha tez aşkarlanmasına imkan yaradır.




Şəkil 1. Təklif olunan paylanmış, hibrid və redundant SCADA arxitektura modeli.

Modelin mühüm komponentlərindən biri paylanmış məlumat modeli (distributed data) və replikasiya (replication) yanaşmasıdır. Bu yanaşmaya əsasən, məlumatlar yalnız mərkəzi bazada saxlanılmır, həm də lokal və regional səviyyələrdə qorunur. Lokal səviyyədə yaranan texnoloji məlumatlar, operator əməliyyatları, siqnalizasiya qeydləri və sistem jurnal qeydləri əvvəlcə obyektin özündə saxlanılır, daha sonra regional və mərkəzi sistemlərlə sinxronlaşdırılır. Bu isə həm məlumat itkisi riskini azaldır, həm də kiber insident zamanı müxtəlif səviyyələrdən sübutların əldə olunmasına şərait yaradır.

Replikasiya prosesi SCADA sistemlərinin iş prinsipinə uyğun təşkil edilməlidir. OT mühitində real-vaxt rejimi və fasiləsizlik əsas tələb olduğundan məlumat ötürülməsi sistemin işinə əlavə yük yaratmamalıdır. Buna görə də kritik idarəetmə komandaları ilə təhlükəsizlik və analiz məqsədli məlumatlar ayrılmalı, mərkəzi sistemə əsasən filtr olunmuş jurnal qeydləri, hadisə qeydləri və analitik məlumatlar ötürülməlidir. Bu yanaşma həm trafikin optimallaşdırılmasına, həm də sistemin təhlükəsizliyinə xidmət edir.

Təklif olunan modeldə kriminalistik araşdırmaya hazır sistem yanaşması (forensics-ready approach) xüsusi əhəmiyyət daşıyır. Bu prinsipə əsasən SCADA sistemi yalnız idarəetmə və monitorinq üçün deyil, həm də gələcəkdə baş verə biləcək kiber hadisələrin araşdırılması üçün əvvəlcədən hazır vəziyyətdə layihələndirilir. Bunun üçün sistemdə mərkəzləşdirilmiş jurnal qeydləri, zaman sinxronizasiyası, audit izi (audit trail), hadisələrin arxivləşdirilməsi və məlumatların bütövlüyünün qorunması mexanizmləri tətbiq olunmalıdır. Kriminalistik araşdırmaya hazır yanaşmanın tətbiqi kiber insident zamanı araşdırma prosesini əhəmiyyətli dərəcədə asanlaşdırır. Hadisə baş verdikdə hansı istifadəçinin sistemə nə zaman daxil olduğu, hansı əmrlərin icra edildiyi, hansı cihazlarda dəyişiklik baş verdiyi və şəbəkədə hansı qeyri-adi fəaliyyətin müşahidə olunduğu daha dəqiq müəyyən edilə bilir. Bu isə hadisə xronologiyasının qurulmasını, hücumun mənbəyinin müəyyən edilməsini və zəifliklərin aşkarlanmasını sürətləndirir.

## NƏTİCƏ

Aparılan təhlil göstərir ki, SCADA sistemləri kritik infrastruktur obyektlərinin fasiləsiz və səmərəli idarə olunmasında mühüm rol oynayır. Lakin bu sistemlərin şəbəkə mühitinə inteqrasiyası, IT və OT sahələrinin yaxınlaşması, köhnə avadanlıqların istifadəsi və insan faktoru yeni kiber təhlükəsizlik risklərinin yaranmasına səbəb olur.

SCADA sistemlərinin qorunması üçün yalnız texniki vasitələr kifayət etmir. Şəbəkə segmentasiyası, ICS firewall, giriş nəzarəti, SIEM əsaslı monitorinq, loq və trafik analizi kimi tədbirlər kompleks şəkildə tətbiq edilməlidir. Eyni zamanda kiberkriminalistik təhlil metodlarının əvvəlcədən nəzərə alınması insident zamanı sübutların qorunmasına, hadisə xronologiyasının qurulmasına və hücumun mənbəyinin daha tez müəyyən edilməsinə imkan yaradır.

Təklif olunan paylanmış və hibrid SCADA modeli lokal, regional və mərkəzi idarəetmə səviyyələrinin birgə fəaliyyətini təmin etməklə sistemin dayanıqlılığını artırır. məlumatların replikasiyası (Data Replication) mərkəzi, SIEM inteqrasiyası və forensics-ready yanaşma kritik infrastruktur obyektlərində həm kiber təhlükəsizliyin, həm də insidentlərin araşdırılması imkanlarının gücləndirilməsi baxımından praktiki əhəmiyyət kəsb edir

Ümumilikdə təklif olunan model mərkəzləşdirilmiş kiber nəzarət ilə lokal idarəetmə avtonomluğunu birləşdirir. Yəni sistem mərkəzdən izlənilir və analiz olunur, lakin lokal obyektlər tam şəkildə mərkəzdən asılı vəziyyətə salınmır. Nəticə etibarilə, paylanmış SCADA arxitekturası (Distributed SCADA), məlumatların replikasiyası (Data Replication), mərkəzi SIEM inteqrasiyası və kriminalistik araşdırmaya hazır sistem yanaşması kritik infrastruktur obyektləri üçün daha təhlükəsiz, dayanıqlı və araşdırmaya uyğun idarəetmə modeli kimi qiymətləndirilə bilər.

## ƏDƏBİYYAT


[1] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82 Rev. 2, 2015. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[2] D. Upadhyay and S. Sampalli, "SCADA systems: Vulnerability assessment and security recommendations," Computers & Security, vol. 89, 101666, 2020. doi: 10.1016/j.cose.2019.101666.

[3] IEC Systems Committee on Smart Energy, Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment, IEC, 2018.

[4] NIST, Framework for Improving Critical Infrastructure Cybersecurity, 2018. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[5] ENISA, Cybersecurity in the Energy Sector, European Union Agency for Cybersecurity, 2021. https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy

[6] CISA, Industrial Control Systems Cybersecurity, 2022. https://www.cisa.gov/topics/industrial-control-systems

[7] Azərbaycan Respublikasının "Milli təhlükəsizlik haqqında" Qanunu, 29 iyun 2004-cü il, № 712-IIQ. https://e-qanun.az/framework/5455

[8] Azərbaycan Respublikasının "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunu, 3 aprel 1998-ci il, № 460-IQ. https://e-qanun.az/framework/3525

[9] "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası"nın təsdiq edilməsi haqqında Azərbaycan Respublikası Prezidentinin Sərəncamı, 28 avqust 2023-cü il. https://e-qanun.az/framework/55045

[10] "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyasının təsdiq edilməsi haqqında" Azərbaycan Respublikası Prezidentinin Sərəncamı, 23 may 2007-ci il, № 2198. [Online]. Available: https://e-qanun.az/framework/13373

[11] "Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları"nın təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı, 17 iyul 2023-cü il, № 229. https://e-qanun.az/framework/54651

[12] IEC, IEC 61850: Communication Networks and Systems for Power Utility Automation, 2013. https://cdn.standards.iteh.ai/samples/19181/a0b511d2f63c4f3cbfc66fa2530ce482/IEC-61850-5-2013.pdf

[13] Stormshield, "How the IEC 61850 standard structures the electrical industry," 2020. https://www.stormshield.com/news/how-the-iec-61850-standard-structures-the-electrical-industry/

[14] M. Khalil, "Cybersecurity in the Power Sector 2025: How Utilities Defend Against Cyber Threats," 2025. https://deepstrike.io/blog/cybersecurity-in-the-power-sector-2025

[15] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," Computers & Security, vol. 70, pp. 436–454, 2017. doi: 10.1016/j.cose.2017.06.010.

[16] ISA, ISA/IEC 62443 Industrial Automation and Control Systems Security, International Society of Automation, 2018. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards


## Cybersecurity of SCADA Systems in Critical Infrastructure Facilities and Cyber Forensic Analysis Methods


**Mehdi Ahmadov[1], Tabriz Jafarov[2]**

[1]Sumgayit State University, Sumgayit, Azerbaijan

[2]ADA University, Baku, Azerbaijan

*[1]mehdi.ehemdov077@gmail.com, [2]tjafarov@ada.edu.az*



**Abstract-** This paper analyzes the cybersecurity problems of SCADA (Supervisory Control and Data Acquisition) systems used in critical infrastructure facilities. Considering the role of SCADA systems in the energy and industrial sectors, the main risks are identified. Furthermore, cyber forensic methods such as log analysis, network traffic analysis, and incident timeline reconstruction are examined. The paper proposes a distributed and hybrid architecture model for SCADA systems.



**Keywords-** SCADA system; cybersecurity; critical infrastructure; SIEM; cyber forensics.