Engineering Sciences
ISSN: 1308 7231
Article ID: 1A0492

Status : Research Article
Received: 05.05.2024
Accepted: 25.10.2024

Esra Söğüt
Gazi University, esrasogut@gazi.edu.tr, Ankara-Türkiye
O. Ayhan Erdem
Gazi University, ayerdem@gazi.edu.tr, Ankara-Türkiye

DOI	http://dx.doi.org/10.12739/NWSA.2024.19.4.1A0492	
ORCID ID	0000-0002-0051-2271	0000-0001-7761-1078
Corresponding Author	Esra Söğüt	

SCADA SİSTEMLERİ İLE SİBER GÜVENLİK İLİŞKİSİNİN İNCELENMESİ: MİNİ SİSTEMATİK TARAMA

ÖZ

Gelişen teknolojiyle birlikte, scada sistemlerini hedef alan siber saldırılar da karmaşıklaşmakta ve sürekli olarak yenilenmektedir. Scada sistemleri enerji, ulaşım, su yönetimi ve üretim gibi kritik altyapılarda hayati rol oynadığı için bu sistemlerin güvenliği büyük bir önem taşımaktadır. Sistemlerin sürekliliğinin sağlanması ve kullanılan verinin korunması gereklidir. Bu yüzden siber güvenlik konusu scada temelinde de incelenmelidir. Scada sistemlerine yönelik siber saldırılar, öngörülerin ötesinde yıkıcı etkiler yapabilmekte ve bu saldırıların tespit edilip önlenmesi için önem arz etmektedir. Bu çalışmada, scada sistemleri ile siber güvenlik ilişkisine dair akademik literatür incelenmektedir. Kitap, makale ve konferans yayın türleri mini sistematik tarama yöntemiyle analiz edilmektedir. Bu alanda dünyadaki mevcut durumlar değerlendirilmekte ve yapılan çalışmaların yönelimleri hakkında bilgiler sunulmaktadır. Elde edilen verilerden faydalanılarak gelecekte yapılacak çalışmalar hakkında yol gösterici olmak hedeflenmektedir.

Anahtar Kelimeler: Scada, Siber Güvenlik, Sistematik Tarama, Saldırılar, Modbus

RELATIONSHIP BETWEEN SCADA SYSTEMS AND CYBER SECURITY: MINI SYSTEMATIC REVIEW

ABSTRACT

With the advancement of technology, cyber attacks targeting scada (supervisory control and data acquisition) systems have become increasingly complex and are continuously evolving. Scada systems play a vital role in critical infrastructures such as energy, transportation, water management, and manufacturing, making their security a matter of utmost importance. Ensuring the continuity of these systems and the protection of the data they utilize is essential. Therefore, cybersecurity must also be examined within the context of scada systems. cyber attacks targeting scada systems can have devastating effects beyond expectations, and it is important to detect and prevent these attacks. This study examines the relationship between scada systems and cyber security through a review of the academic literature. Book, article and conference publication types are analyzed using a mini systematic review method. Current situations in the world in this field are evaluated and information is provided about the trends of the studies conducted. Utilizing the findings, the study aims to serve as a guide for future research and developments in the cybersecurity of scada systems.

Keywords: Scada, Cyber Security, Systematic Review, Attacks, Modbus

How to Cite:
Söğüt, E. ve Erdem, O.A., (2024). Scada sistemleri ile siber güvenlik ilişkisinin incelenmesi: Mini sistematik tarama, 19(4):56-66, DOI: 10.12739/NWSA.2024.19.4.1A0492.

1. GİRİŞ (INTRODUCTION)

Teknolojik gelişmeler yaşanmasının etkileri siber güvenlik dünyasına da yansımaktadır. Farklı ve gelişmiş sistemlerin çeşitli alanlarda kullanılmaya başlanması, gerçekleştirilen süreçlerin işleyişini de hızlandırmaktadır. Buna ek olarak veri ile ilgili sürdürülen işlemlerin kapasitesi ve kapsama alanları da genişlemektedir. Bu durum siber güvenlik dünyasında hem avantajlı hem de dezavantajlı şekilde değerlendirilmektedir. Siber güvenlik dünyasında güvenliğin sağlanması gizlilik, bütünlük, erişebilirlik, süreklilik, yetkinlik ve test edilebilirlik gibi birçok unsura bağlıdır [1]. Bu nedenle sadece bireysel olarak ürettiğimiz ve kullandığımız veri için değil büyük ölçekli işletmelerde veya kurumlarda ele alınan veri için de siber güvenlik konusu değerlendirilmektedir. Kullanılan cihazların sayısındaki artış, internet kullanımının yaygınlaşması, kapsamlı ve performansı yüksek yazılım veya donanım kullanılması yapılmak istenen işleri hızlandırmakta ve çalışanların yükünü hafifletmektedir. Bu durum verinin saklanmasını, düzgün şekilde kullanılmasını ve işletilen diğer süreçlerin devamlılığının sağlanmasını ve gerekli birçok işlemi zorunlu kılmaktadır [2]. Örneğin, kişisel olarak kullanılan bir akıllı saatin çalışmasında yaşanan problem çok ciddi sorunlara yol açmayabilir fakat mobil cihazlardaki popüler olarak kullanılan işletim sistemlerinde yaşanacak yazılımsal bir sorun olumsuz sonuçlara sebep olabilir [3].

Benzer şekilde, kritik altyapı sistemlerinin saldırıya uğraması da ciddi sonuçlar doğurmaktadır. Örneğin, Florida şehrinde şehir su sağlayıcısı sistemlerine yönelik bir saldırı gerçekleştirilmiş. Su tesisi uzaktan erişim yöntemleri ile saldırganlar tarafından ele geçirilmiş ve şehre dağıtılan suyun kimyasal bileşenlerinin oranları değiştirilmeye çalışılmış. Operatörler erken fark ettiği için halk zarar görmeden soruna müdahale edilmiş, saldırı engellenmiş ve su kullanılabilir hele getirilmiş [4]. Su, elektrik, gaz, güneş gibi kaynaklar kritik altyapılar sayesinde işlenmekte, yapılar arasında iletilmekte ve halkın kullanımına ulaşacak şekilde dağıtılmaktadır. Bunlara ek olarak hava, tren, deniz ve uzay yolculuklarında da bu yapılar kullanılmaktadır. Hem kurumlar, belediyeler, küçük şirketler gibi yerel bölgelerde hem de devletlerarası alanlarda bu kritik yapılar önemli roller üstlenmektedir. Bu yapıların işleyişlerinde olabilecek herhangi bir aksaklık maddi kayıplara, itibar kayıplarına ve hatta vatandaşların can kaybına bile sebebiyet verebilir. Bu sebeplerden dolayı kritik altyapıların hem fiziksel hem de siber güvenliğinin korunması ve sürekliliğin sağlanması zorunlu hale gelmiştir [5].

Özelleştirilmiş bazı sistemler kritik altyapılardaki süreçleri, olayları ve alarmları merkezi bir noktadan izlemek, kontrol etmek ve müdahale etmek için kullanılmaktadır. Bu sistemlerden en sık kullanılanı denetleyici kontrol ve veri toplama (supervisory control and data acquisition-scada) sistemidir. Scada sistemlerinin kullanıldığı en bilinen örnek ise belediyelerin temiz ve kirli su operasyonlarıdır. Belediyeler su seviyelerini, boru basıncını ve kamu suyu dağıtım tesislerinde bulunan tanklardaki sıcaklığı izlemek için altyapı tesislerinde scada sistemlerini kullanır [6]. Scada sistemlerinde yaşanabilecek fiziksel veya siber aksaklıklar halkın ve bölgede yaşayan diğer canlıların yaşamını tehlikeye sokabilir. Halkın yaşamını kolaylıkla idame edebilmesini zorlaştırabilir. Maddi ve manevi kayıplar yaşanmasına sebep olabilir. Scada sistemlerinin uluslararası kritik altyapılarda kullanılan bir sistem olduğu düşünüldüğünde güvenliğin sağlanmasının ne kadar gerekli olduğu anlaşılmaktadır. Ayrıca, siber saldırılar sonucunda bu sistemlerin fiziksel olarak güvenliği de tehlikeye girmektedir. Kritik altyapıların dolayısıyla scada sistemlerinin siber güvenliğinin sağlanması için birçok çalışma yapılmaktadır. Scada sistemleri, kendine has yapısı nedeniyle yeni

sistemlerle bütünleşme noktasında geride kalmıştır. Dış ağa açılma, internet kullanımının yaygınlaşması, uzaktan kontrol gibi yeni durumlar da ortaya çıkması güvenlik risklerini de beraberinde getirmiştir. Bu yenilikler işlevselliği ve performansı arttırabilir fakat yeni güvenlik açıklıklarını ve sorunlarını da hazırlayabilir. Tüm bu sebepler göz önünde bulundurulduğunda, scada sistemlerinin siber güvenlik alanında değerlendirilmesi önem arz etmektedir.

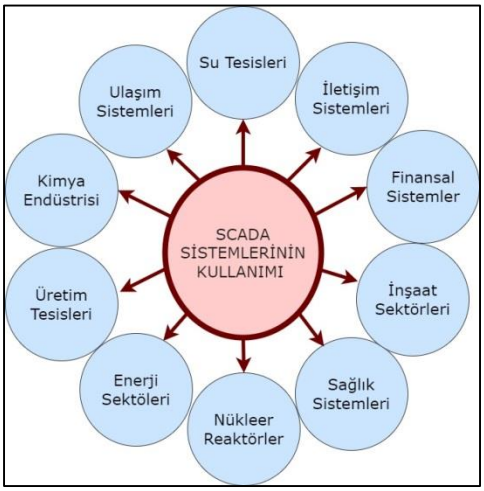
Bu çalışmada mini sistematik tarama yöntemi kullanılarak scada sistemleri ve siber güvenlik yayınlarının durumu analiz edilmiştir. Bilimsel yayınlar içerisinde kitap, kitap bölümü, makale, inceleme yazısı, konferans bildirisi ve konferans inceleme yazısı olarak yapılanlar son 10 yıl için taranmıştır. Farklı tarama özellikleri olan scopus ortamında hedeflenen tüm işlemler gerçekleştirilmiştir. Bu işlemler ile ilgili bilgilere ilerleyen bölümlerde yer verilmektedir. Bu çalışma sonucunda siber güvenlik alanında scada sistemlerinin değerlendirilmesi, evrensel gelişmelerin durumu ve gelecekte olabilecek gelişmeler konusunda tahminlerde bulunulması amaçlanmaktadır.

1.1. Arka Plan (Background)

Çalışmada scada sistemleri ve siber güvenlik konuları temel olarak değerlendirilmiştir. Tarama yapılırken farklı anahtar ifadeler kullanılarak çalışma alanı zenginleştirilmiştir. Çalışmada ele alınan konular ve amaçlar bu bölümde açıklanmakladır.

1.2. Scada Sistemleri (Scada Systems)

Doğal gaz, petrol, su ve elektrik gibi kaynakların işlenmesinde, iletiminde ve dağıtımında genel olarak scada sistemleri kullanılmaktadır. Buna ek olarak, süreçlerin ve farklı noktalardan alınan verilerin kontrol edilmesinde ve izlenmesinde de bu sistemler kullanılmaktadır. Scada sistemleri temel olarak ana kontrol birimi, uzak terminal birimi, insan makine ara yüzü ve haberleşme ağı bileşenlerine sahiptir. Scada sistemleri farklı alanlarda, sektörlerde ve kapsamda kullanılmaktadır. Şekil 1'e göre scada sistemleri enerji, finans, sağlık, ulaşım veya üretim gibi birçok sektörde yer almaktadır [6].



Şekil 1. Scada sistemlerinin kullanıldığı sektörlerden bazıları [6]
(Figure 1. Some of the industries where scada systems are used [6])

Scada sistemlerinde iletişimi sağlayan ağ yapısı, sistemin bütününü etkileyebilecek özelliktedir. Haberleşme için kablolu, kablosuz bağlantıların yanı sıra Modbus, Profibus, Conitel veya Dnp3 gibi özel protokoller de kullanılmaktadır. Özellikle Modbus protokolü geleneksel scada sistemlerinde sıklıkla tercih edilmektedir [7].

1.3. Siber Güvenlik (Cyber Security)

Geleneksel scada sistemleri yapısı gereği internet bağlantısı olmadan kapalı alanlarda faaliyet göstermektedir. Bu sistemlerin dış ağdan bağımsız şekilde tasarlanmasından dolayı, gelişen teknolojiye entegre olunmasında sorunlar meydana gelmektedir. İnternet kullanımının kısıtlı olması, farklı teknolojilerle bütünleşememe ve uzaktan erişim yöntemlerinin kullanılmaya başlanması gibi durumlar yeni siber güvenlik sorunlarını ortaya çıkarmaktadır. Gelişen ve değişen teknolojik olaylara ayak uydurmakta zorlanan scada sistemleri birçok farklı güvenlik açıklıkları barındırmaktadır. Örneğin, scada sistemlerinde haberleşme ağında sıklıkla kullanılan modbus protokolü birçok güvenlik açıklığına sahiptir. Bu durum farklı siber saldırılarının uygulanmasına ve sistemlerin olumsuz şekilde etkilenmesine zemin hazırlamaktadır. Açıklıklar hakkında bilgi sahibi olan, uygulamalar geliştiren, çıkarı olan, ulusal ya da uluslararası düzeyde faaliyet gösteren saldırganlar scada sistemlerini potansiyel hedefler haline getirmektedir [6].

1.4. Motivasyon (Motivation)

Dünyada yaşanan gelişmelerin ve yeniliklerin fark edilmesi ve takip edilmesi amaçlarıyla scada sistemleri ve siber güvenlik ile ilgili konular dikkate alınmıştır. Çalışma kapsamında belirlenen amaçlar ve kullanılan metodoloji doğrultusunda cevap arayan sorular şu şekildedir:

- Yayınların anahtar ifadelere göre tarama sonucundaki sayıları nedir?
- Yayınların yıllara göre dağılımları nasıldır?
- Yayınların ülkelere göre dağılımları nasıldır?
- Yayınların dillere göre dağılımları nasıldır?
- Yayınların türlerine göre dağılımları nasıldır?
- Yayınların çalışma alanlarına göre dağılımları nasıldır?
- Yayın taranırken kullanılan anahtar kelimelerin etkisi nedir?

2. ÇALIŞMANIN ÖNEMİ (RESEARCH SIGNIFICANCE)

Bu çalışmada scada sistemleri ile siber güvenlik ilişkisinin incelenmesi mini sistematik tarama şeklinde yapılmıştır. Çalışma siber güvenlik konusu scada temelinde de incelenmesinin gerekliliğini ortaya koymaktadır. Bu alanda dünyadaki mevcut durumlar değerlendirilmekte ve yapılan çalışmaların yönelimleri hakkında bilgiler sunulmaktadır. Elde edilen verilerden faydalanılarak gelecekte yapılacak çalışmalar hakkında yol gösterici olmak hedeflenmektedir.

Önemli Noktalar (Highlights):

- Scada sistemlerinin önemi ortaya konulmuştur.
- Scada sistemleri yapısı gereği internet bağlantısı olmadan kapalı alanlarda faaliyet gösterebilir.
- Scada sistemleri doğal gaz, petrol, su ve elektrik gibi kaynakların iletiminde ve dağıtımında kullanılabilir.

3. YÖNTEM (METHOD)

Bu çalışmada scada ve scada güvenliği ile ilgili kitap, kitap bölümü, makale türleri ve konferans bildiri türleri olarak yapılan yayınlar taranmaktadır. Bu işlemde sistematik tarama yönteminden faydalanılmaktadır. Sistematik tarama, benzer konuları ve yöntemleri içeren çalışmaların belirli bir metodolojik yaklaşıma göre kapsamlı şekilde değerlendirilmesidir. Benzer çalışmaların seçilmesi, araştırılması, çalışmalarla ilgili veri toplanması, veri analizi ve sentez yapılması aşamaları bulunmaktadır [8 ve 9]. Çalışmada yer alan aşamalara bu bölümde yer verilmektedir.

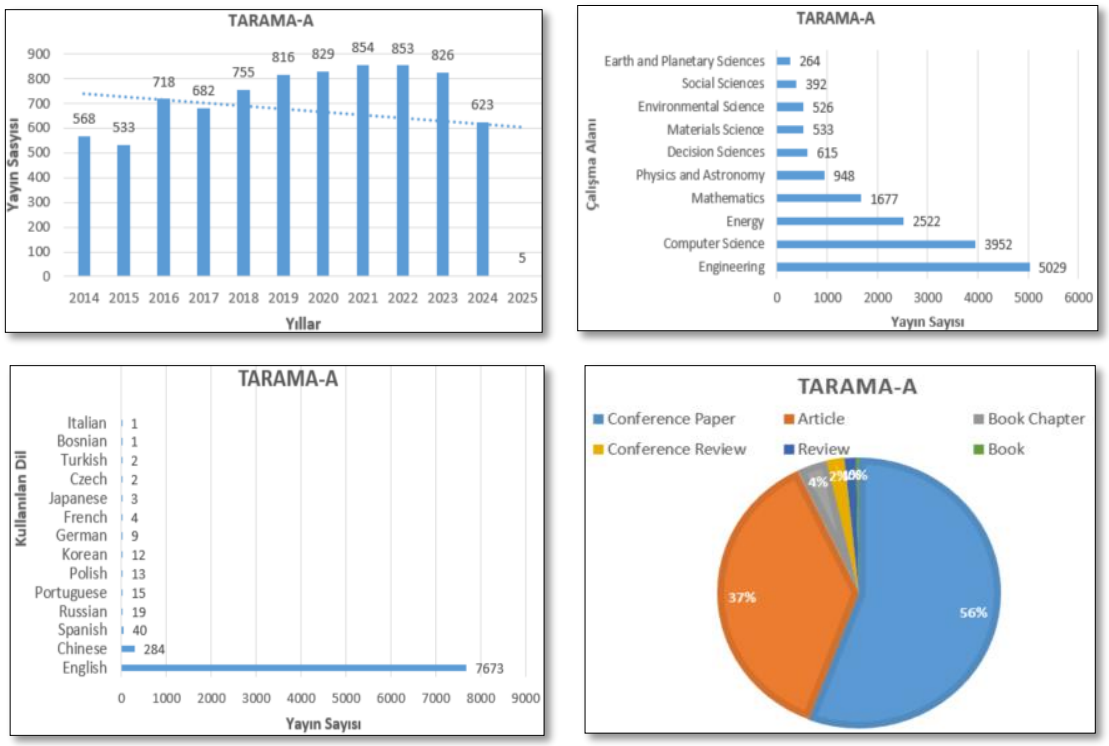
- **Benzer Çalışmaların Seçilmesi ve Araştırılması:** Bu aşamada scada, scada güvenliği, scada güvenliğinde atak/saldırı/tespit/engelleme ve scada güvenliğinde Protokol/Modbus gibi anahtar ifadelere sahip olma özellikleri belirlenmiştir. Bu ifadeler veya kelimeler; çalışmaların başlığında, özetinde veya anahtar kelimeleri içerisinde yer alacak şekilde tarama alanında kullanılmıştır. Bu özellikleri içeren yayınlardan kitap, kitap bölümü, makale, inceleme yazısı, konferans inceleme yazısı ve konferans bildirisi türleri olanlar seçilmiş ve araştırılmıştır.
- **Veri Elde Edilmesi:** Günümüzde sıklıkla kullanılan bilimsel yayın indeksleme veri tabanı olan Scopus ortamı tercih edilmiştir. Scopus veri tabanında farklı filtreleme, sorgulama veya sınıflandırma seçenekleri bulunmaktadır. Ayrıca elde edilen veriye ait görsel bilgiler de kullanıcıya sunulmaktadır [10]. Sahip olduğu kapsamlı veri tabanı, sunduğu filtreleme ve görselleştirme özelliklerinden dolayı çalışmada Scopus kullanılmıştır.
- **Veri Analizi ve Sentez:** Scopus veri tabanı üzerinde belirli anahtar kelimelere göre tarama yapılarak ilgili yayınlara ulaşılmıştır. Bu yayınlar için yayınlanma yılı aralığı olarak son on yıl belirlenmiştir. Yeni başlayacak yıla ait çalışmalar da yapılmış ve yayınlamış olduğu için tarih aralığı 2014-2025 yılının ilk yarısı olarak ayarlanmıştır. Çalışmada Scopus ortamından elde edilen veriler grafikler ve tablolar halinde gösterilmiştir. Ayrıca Bunlar üzerinde ayrıntılı analizler gerçekleştirilmiştir.
- **Tarama Yapılırken Kullanılan Anahtar İfadeler:**
  Tarama-A
  Scada Anahtar İfadesine Göre Yapılan Tarama: (“Scada”)
  Tarama-B
  “Scada” Ve “Security” Anahtar İfadelerine Göre Yapılan Tarama: (“Scada” Or “Security”)
  Tarama-C
  “Scada” Ve “Security” Ve (“Attack” Veya “Intrusion” Veya “Detection” Veya “Prevention”) Anahtar İfadelerine Göre Yapılan Tarama: (“Scada” And “Security” And (“Attack” Or “Intrusion” Or “Detection” Or “Prevention”))
  Tarama-D
  “Scada” Ve “Security” Ve (“Attack” Veya “Intrusion” Veya “Detection” Veya “Prevention”) Ve (“Protocol” Veya “Modbus”) Anahtar İfadelerine Göre Yapılan Tarama: (“Scada” And “Security” And (“Attack” Or “Intrusion” Or “Detection” Or “Prevention”) And (“Protocol” Or “Modbus”)

4. BULGULAR (FINDINGS)

Çalışmanın amacında belirlenen maddelere yönelik elde edilen bulgular alt başlıklar halinde bu bölümde sunulmaktadır.

4.1. Tarama-A (Scan-A)

İlk madde olan scada alanında yapılan tüm çalışmaların son on yıllık taraması yapılmıştır. Buna göre 17.044 adet yayın bulunmuştur. Bu yayınlardan kitap, kitap bölümü, makale türleri ve bildiri türleri olanlar seçildiğinde ise 16.724 yayın geriye kalmıştır. Yayınların yayınlanma tarihleri olarak son on yıl seçildiğinde de 8.062 adet yayın bulunmuştur. Bu yayınların son on yıl içindeki yayınlanma dağılımlarına, yayınların farklı konu alanlarına göre dağılımlarına, yayınlar hazırlanırken kullanılan dillere göre elde edilen dağılımlara ve yayın türlerinin dağılımlarına Şekil 2’de yer verilmiştir. Diğer 4 tarama için de bu kriterler kullanılmıştır.

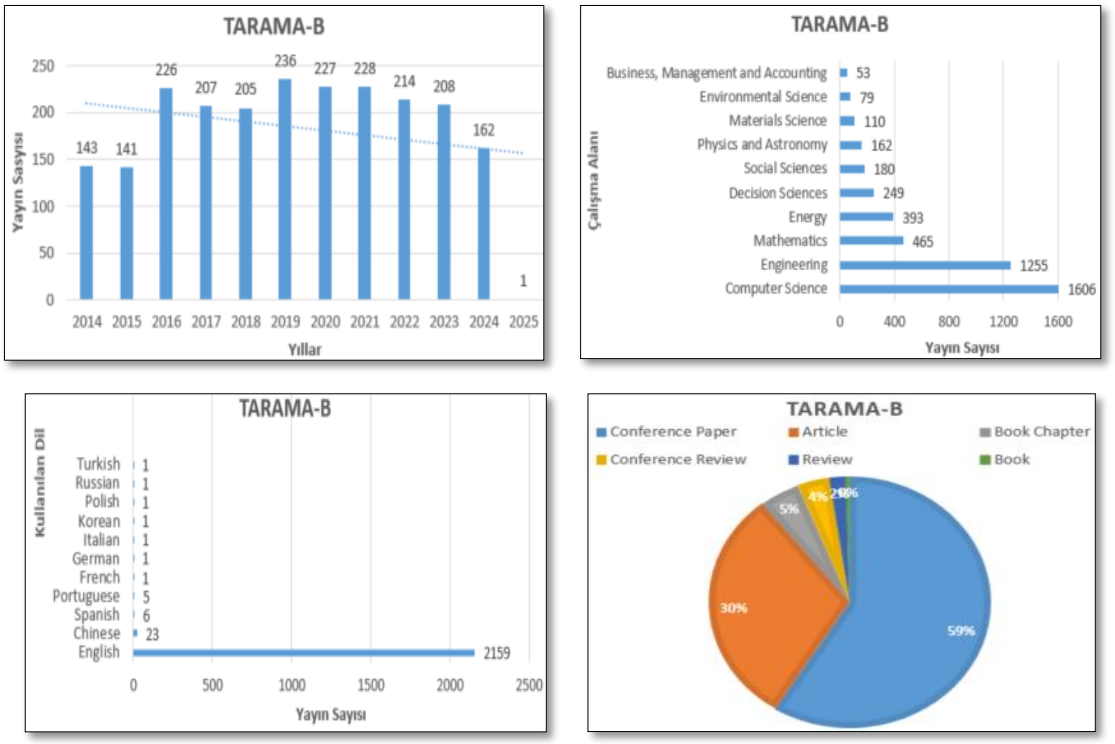


Şekil 2. Tarama-A yayınlarının dağılımları (son on yıla göre, çalışma alanlarına göre, kullanılan dillere göre, yayınların türlerine göre dağılımlar)
(Figure 2. Distributions of Scan-A publications (distributions according to the last ten years, subject areas of study, languages used, and types of document))

Tarama-A ile elde edilen yayınların, yayınlandıkları yıllara bakıldığında 2016 yılında yükselişe geçildiği görülmüştür. 2019-2023 yılları arasındaki yayın sayıları birbirine yakın olmuştur fakat 2024 yılında yayın sayısı fark edilir şekilde düşüşe geçmiştir. 2025 yılına henüz girilmemesine rağmen yeni çalışmalar yayınlanmaya başlanmıştır. Yayınların hangi alanlarda veya konularda yer aldığının belirlenmesinde ilk on alan dikkate alınmıştır. En çok yayın ile ilk sırada %31 oranıyla mühendislik, %24 ile bilgisayar bilimleri ve %15 ile enerji alanları yer almaktadır. Kullanılan diller incelendiğinde ise yayınların neredeyse tamamı İngilizce olarak yazılmıştır. Türkçe olarak yazılan 2 tane yayın bulunmaktadır. Tarama-A İçin En Fazla Yayın Konferans Bildirisi Olarak Üretilmiştir. Yayınların yarısından daha fazlası bu türde yayınlanmıştır. İkinci sırada makale türündeki yayınlar gelmiştir.

4.2. Tarama-B (Scan-B)

İkinci madde olan scada ve güvenlik alanında yapılan tüm çalışmalar taranmıştır. ("Scada" Or "Security") anahtar ifadeleri için yapılan taramaya göre 3.421 tane yayın bulunmuştur. Yayınlar içerinde kitap, kitap bölümü, makale türleri, bildiri türleri olanlar ve son on yıllık zaman diliminde yapılanlar filtrelendiğinde ise geriye 2.198 yayın kalmıştır. Bulunan yayınların son on yıllık yayınlanma dağılımlarına, çalışma alanlarına, dillerine ve yayın türlerine göre dağılımlarına Şekil 3'te yer verilmiştir.

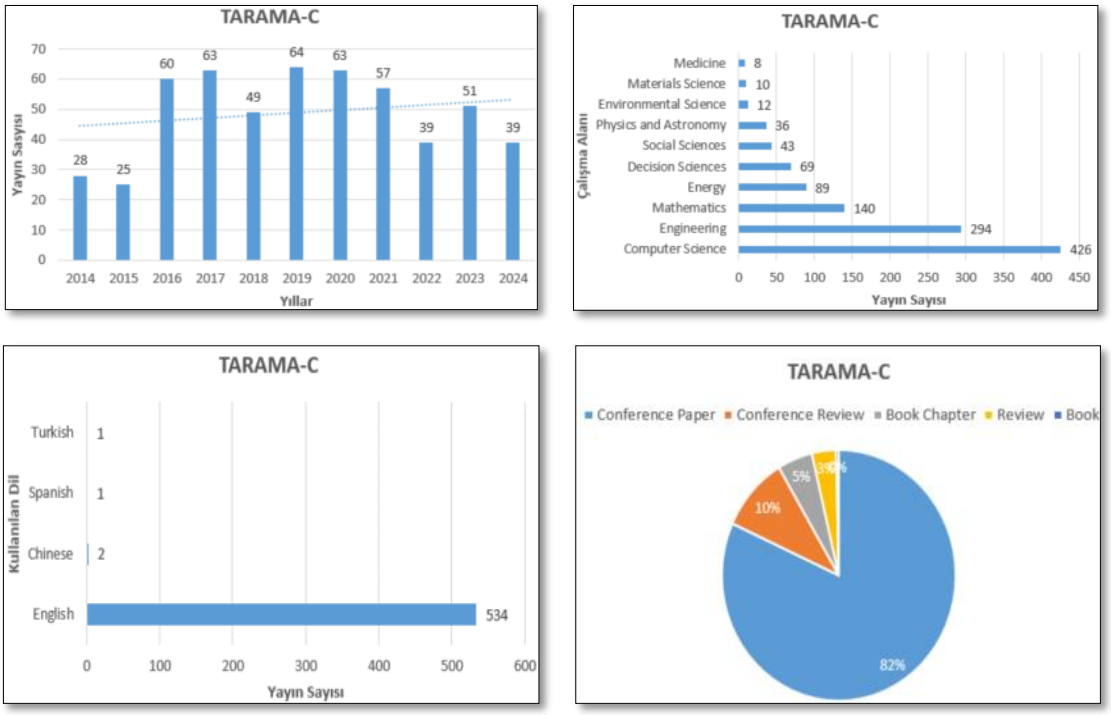


Şekil 3. Tarama-B yayınlarının dağılımları
(Figure 3. Distributions of Scan-B publications)

Tarama-B ile elde edilen yayınlar incelendiğinde 2016 yılında sayıda artış olduğu fakat bu artışın istikrarlı şekilde devam etmediği görülmüştür. En fazla yayın 2019 yılında yapılmış ve her sene yapılan yayın sayısı giderek düşmüştür. Hatta en az yayın 2024 yılında yapılmıştır. Alan temelli inceleme yapıldığında bu sefer bilgisayar bilimlerindeki yayın sayısı sayıca üstün gelmiştir (%35). Bu alana en yakın olarak %26 oranıyla mühendislik gelmiştir. Yayınların dilleri ele alındığında ingilizce dilinin hâkimiyeti göze çarpmaktadır. Sadece 1 tane yayının türkçe olarak yazıldığı belirlenmiştir. Yayın türlerine bakıldığında en fazla yayının (yaklaşık %60) yine konferans bildiri olduğu görülmüştür. %30 oranıyla ikinci sırada ise makale çalışmaları yer almıştır.

4.3. Tarama-C (Scan-C)

Üçüncü maddede scada ve güvenlik kelimelerine ek olarak birkaç anahtar ifade daha kullanılmıştır. Saldırı, Girişim, Tespit Veya Engelleme Kelimeleri De Eklenerek ("scada" and "security" and ("atttack" or "intrusion" or "detection" or "prevention")) taraması yapılmıştır. İlgili alanlarda yapılan tarama sonucunda 1.057 adet yayın olduğu görülmüştür. On yıllık zaman aralığındaki yayın türleri filtrelemesi yapıldığında ise 538 yayın kalmıştır. Bunların son on yıllık yayınlanmaya göre, çalışma alanlarına göre, kullanılan dillere göre ve yayın türlerine göre Şekil 4'te yer verilmiştir.

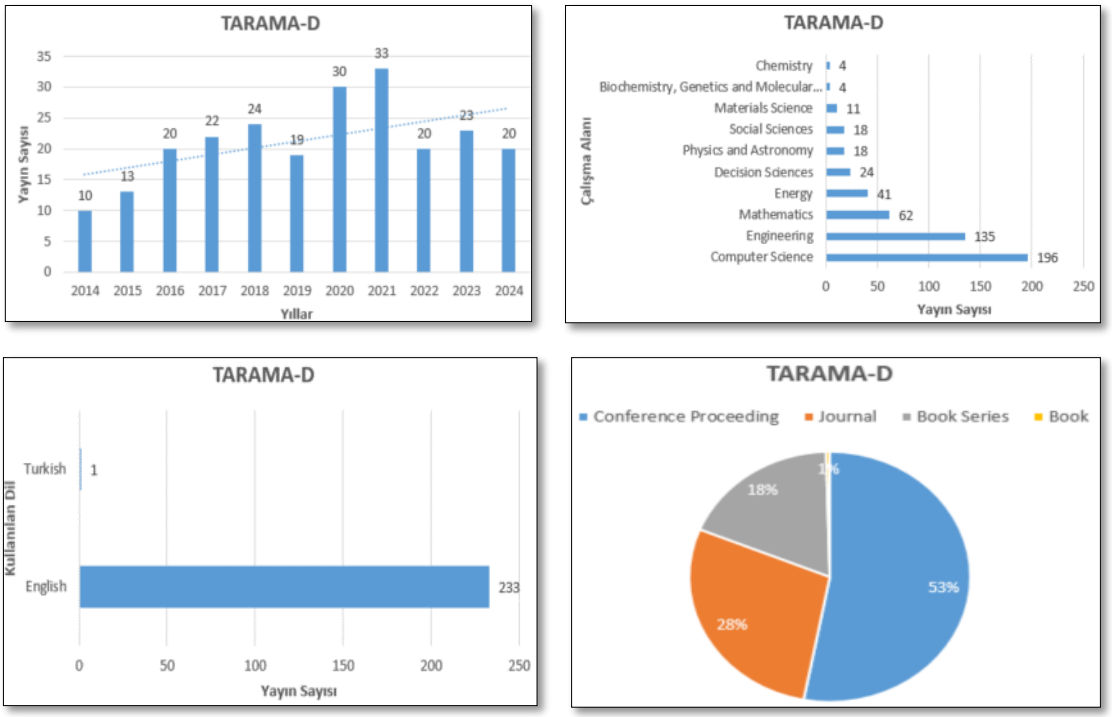


Şekil 4. Tarama-C yayınlarının dağılımları
(Figure 4. Distributions of Scan-C publications)

Yayın sayısındaki ilk artış 2016 yılında görülmüştür. Daha sonraki yıllarda ciddi artışlar görülmemiş aksine 2021 yılından sonra sayılarda düşüş görülmüştür. Diğer grafik incelendiğinde, en çok yayın ile ilk sırada %38 oranıyla bilgisayar bilimleri, daha sonra %26 ile mühendislik ve üçüncü sırada %12 ile matematik alanları yer almıştır. Yayın diline bakıldığında İngilizce dili çalışmaların tamamına yakınında kullanılmıştır. Türkçe yayınlara bakıldığında ise sadece 1 adet yayın yapıldığı görülmüştür. Yayın türleri grafiğine göre, çalışmaların tamamına yakınının konferans türündeki çalışımlar olduğu belirlenmiştir. Konferans türündeki çalışmaların büyük çoğunluğunu (%82) konferans bildirisi ve geri kalanını konferans inceleme yazısı (%10) oluşturmuştur.

4.4. Tarama-D (Scan-D)

Bu maddede scada, güvenlik, saldırı, girişim, tespit veya engelleme kelimelerine protokol veya modbus anahtar ifadeleri de eklenmiştir. İlgili alanlarda yapılan yayınlar taranmıştır (“scada” and “security” and (“atttack” or “intrusion” or “detection” or “prevention”) and (“protocol” or “modbus”)). Bu filtrelemeye göre toplam 289 adet yayın bulunmuştur. Kitap, kitap bölümü, makale türleri ve bildiri türleri on yıllık zaman aralığında taratıldığında ise 234 yayın elde edilmiştir. Bu yayınlara ait ilgili grafiklere Şekil 5 olarak yer verilmiştir.



Şekil 5. Tarama-D yayınlarının dağılımları
(Figure 5. Distributions of Scan-D publications)

Tarama-D için yapılan analizlerde, çalışma sayılarının yıllar geçtikçe arttığı fakat 2021 yılından sonra bir kırılma yaşandığı görülmüştür. 2022, 2023 ve 2024 yıllarında birbirine yakın sayılarda çalışma yapıldığı ve 2025 yılına ait henüz bir çalışma olmadığı dikkat çekmiştir. Bir sonraki grafiğe göre, çalışma alanı olarak bilgisayar bilimleri %38 ile ilk sırada ve mühendislik %26 ile ikinci sırada yer almıştır. Bu iki alandan sonra diğer alanlarda, çalışma sayıları önemli derecede düşmüş ve giderek daha az yayın elde edilmiştir. Tüm çalışmaların 1 tanesi dışında olanların dili İngilizcedir. Sadece 1 tane olan bu yayın ise Türkçe diliyle yazılmıştır. Son grafik ele alındığında ise kitap yayın türünün de (%19) çalışmalarda yer aldığı görülmüştür. En fazla yapılan çalışma türü konferans yayınları ve daha sonra makale yayınları olarak literatürde yer almıştır.

5. SONUÇLAR (CONCLUSIONS)

Scada sistemlerinin siber güvenlik ile ilişkisini ve dünyadaki genel durumu göstermek için belirlenen anahtar ifadelere göre sistematik tarama yöntemi kullanılmıştır. Buna göre elde edilen bulgular 5 başlık altında değerlendirilmiştir. Tüm bulgular sonucunda bazı sonuçlara varılmıştır. Tarama-A, Tarama-B, Tarama-C ve Tarama-D Verileri, akademik yayınların yıllar içindeki dağılımı, çalışma alanları, kullanılan dil ve yayın türleri açısından önemli bulgular sunmaktadır. Tarama-A ve Tarama-B için yayın sayılarında 2016 yılında bir artış gözlenmiş, ancak Tarama-B'de bu artışın sürdürülebilir olmadığı ve 2024 yılına kadar yayın sayılarında azalma olduğu belirtilmiştir. Tarama-C ve Tarama-D'de de benzer şekilde 2021 yılından sonra yayın sayılarında düşüş olduğu görülmüştür. Bununla birlikte, Tarama-D'de 2022-2024 yılları arasında istikrarlı bir yayın sayısı elde edilmiştir.

Çalışma alanlarına göre, bilgisayar bilimleri tüm taramalarda en yüksek oranı elde etmiş ve lider alan olmuştur. Mühendislik alanı ise bilgisayar bilimleri'ni takip eden ikinci sıradaki alan olarak dikkat

çekmiştir. Tarama-A'da mühendislik birinci sıradayken (%31), Tarama-b, Tarama-c ve Tarama-d'de bilgisayar bilimleri sırasıyla %35, %38 ve %38 oranlarıyla lider konumdadır. Scada ve siber güvenlik alanı enerji, matematik, karar bilimleri ve farklı disiplinlerde daha düşük oranlarla temsil edilmiştir.

Dil kullanımı açısından, dört tarama da İngilizcenin baskınlığını göstermektedir. Yayınların büyük çoğunluğu İngilizce yazılmış olup, tarama-a'da 2, diğer taramalarda yalnızca 1 Türkçe yayın bulunmaktadır. Bu durum, akademik çalışmaların uluslararası geçerlilik açısından İngilizce'ye olan bağımlılığını açıkça ortaya koymaktadır. Scada ve siber güvenlik çalışmalarında Türkçe yayın olması gelecekte daha fazla Türkçe yayın yapılabilmesi konusunda motive edici bir durumdur.

Yayın türleri değerlendirildiğinde, konferans bildirileri tüm taramalarda en yaygın yayın türü olmuştur. Özellikle Tarama-C'de konferans türündeki yayınların %82 gibi yüksek bir orana ulaştığı görülmüştür. Makale yayınları, genellikle ikinci sırada yer alırken, Tarama-D'de ek olarak kitap yayınlarının da %19 oranında yer aldığı dikkat çekmektedir. Bu bulgular, akademik çalışmaların büyük ölçüde konferans ve makale formatlarında üretildiğini göstermektedir. Konferanslarda uzmanların bir araya gelip fikir alışverişinde bulunabilmesi ve ilgili konularda daha hızlı eyleme geçilmesi makale ve kitap türü yayın olanaklarına göre daha kolay ve hızlı olabilmektedir. Bu durumdan dolayı scada ve siber güvenlik ile ilgili problemler veya çözümler daha çok ulusal veya uluslararası konferanslarda ele alınmış olabilir.

Tarama sonuçlarına göre genel olarak siber güvenlik anahtar ifadesi ile 8.062 yayın bulunurken alt alanlara göre tarama yapıldığında bu sayılar ciddi oranda düşmüştür. Scada, siber güvenlik ve saldırılarla ilgili taramada 538 adet yayın ve bu taramaya protokol veya modbus eklenmesi ile 234 adet yayın elde edilmiştir. Scada ve siber güvenliğin alt dallarıyla ilgili yapılan çalışma sayısı oldukça az ve yetersiz durumdadır. Disiplinler arası çalışma sayıları da yeterli durumda değildir. İngilizce dili dışında hazırlanan çalışma sayısı neredeyse yok denilecek kadar azdır.

Gelişen ve karmaşıklaşan teknolojinin kullanılmaya başlandığı kritik altyapılar, siber saldırılar için potansiyel hedefler olmaya devam edecektir. Bu yüzden, scada ve siber güvenliğin alt dallarıyla ilgili çalışmalar yapılması, uygulamalar geliştirilmesi ve ülkelerin de bu alanlarda hâkimiyet kurması önem arz etmektedir. Akademik yayınların devlet destekleriyle zenginleştirilmesi ve gelecek yıllar için bu alanlarda yatırım yapılması gereklidir. Böylece siber dünyada akademik gelişmenin önü daha da açılmış olacaktır.

ÇIKAR ÇATIŞMASI (CONFLICT OF INTEREST)

Yazarlar çıkar çatışması bildirmemiştir.

FİNANSAL AÇIKLAMA (FINANCIAL DISCLOSURE)

Yazarlar bu çalışma için herhangi bir mali destek almadığını beyan etmiştir.

ETİK STANDARTLAR BEYANI (DECLARATION OF ETHICAL STANDARDS)

Makalenin yazarları bu çalışmada kullanılan materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel izin gerektirmediğini beyan eder.

KAYNAKLAR (REFERENCES)

[1] Erol, S.E., Aksoy, Ç., and Sağıroğlu, Ş., (2023). Social big data applications and challenges. concurrency and Computation:

Practice and Experience, 35(5):E7567. Https://Doi.Org/10.1002/Cpe.7567
[2] Koçak, A., Söğüt, E., Alkan, M., and Erdem, O.A., (2023). Detection of different windows pe malware using machine learning methods. Journal of Polytechnic, 26(3): 1185-1197. Https://Doi.Org/10.2339/Politeknik.1207704.
[3] Kiraz, Ö. and Doğru, İ.A., (2024). Visualising static features and classifying android malware using a convolutional neural network approach. Applied Sciences, 14(11):4772. Https://Doi.Org/10.3390/App14114772.
[4] Naraine, R. Https://Www.Securityweek.Com/Remote-Hacker-Caught-Poisoning-Florida-City-Water-Supply/. Securityweek Network.
[5] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A., (2015). Guide to ındustrial control systems (Ics) security. Nıst Special Publication. 800(82):16. Https://Nvlpubs.Nist.Gov/Nistpubs/Specialpublications/Nıst.Sp.800-82r2.Pdf.
[6] Söğüt, E. and Erdem, O.A., (2023). A multi-model proposal for classification and detection of ddos attacks on scada systems. Applied Sciences, 13(10):5993. Https://Doi.Org/10.3390/App13105993.
[7] Polat, H., Türkoğlu, M., Polat, O., and Şengür, A., (2022). A novel approach for accurate detection of the ddos attacks in sdn-based scada systems based on deep recurrent neural networks. Expert Systems With Applications, 197:116748. Https://Doi.Org/10.1016/J.Eswa.2022.116748.
[8] Şencan, Ö.A., Atacak, İ. ve Doğru, İ.A., (2022). Sosyal Ağlarda topluluk ve konu tespiti: bir sistematik literatür taraması. International Journal of Informatics Technologies, 15(3). Https://Doi.Org/10.17671/Gazibtd.1061332.
[9] Kılınç, H., (2022). Nesnelerin interneti konusunda gerçekleştirilen akademik çalışmaların eğilimleri: Bir sistematik tarama. Dijital Teknolojiler ve Eğitim Dergisi, 1(1):57-67. Https://Doi.Org/10.5281/Zenodo.6647667.
[10] Elsevier, https://Www.Scopus.Com/. Scopus Website.