

Research article

Journal of Smart Systems Research (JOINSSR) 7(1), 79-93, 2026
Received: 8-Mar-2026 Accepted: 9-Jun-2026
https://doi.org/10.58769/joinssr.1905520

Siber Fiziksel Sistemlerin İncelenmesi ve Değerlendirilmesi

Tutku COŞKUN [1], Esra YOLCU [2], Sıla KUDU [3], Yusuf Bera SANLI [4], Beyza Nisa ÖZTÜRK [5], Tamer EREN [6*]

[1] Endüstri Mühendisliği Bölümü, Mühendislik ve Doğa Bilimleri Fakültesi, Kırıkkale Üniversitesi, Türkiye.
tutkuucskn@gmail.com
[2] Endüstri Mühendisliği Bölümü, Mühendislik ve Doğa Bilimleri Fakültesi, Kırıkkale Üniversitesi, Türkiye.
esrayolcu1102@gmail.com
[3] Endüstri Mühendisliği Bölümü, Mühendislik ve Doğa Bilimleri Fakültesi, Kırıkkale Üniversitesi, Türkiye.
silakudu89@gmail.com
[4] Endüstri Mühendisliği Anabilim Dalı, Fen Bilimleri Enstitüsü, Kırıkkale Üniversitesi, Türkiye.
beraasanli@gmail.com
[5] Endüstri Mühendisliği Anabilim Dalı, Fen Bilimleri Enstitüsü, Kırıkkale Üniversitesi, Türkiye.
beyzanisaozturk@gmail.com
[6] Endüstri Mühendisliği Bölümü, Mühendislik ve Doğa Bilimleri Fakültesi, Kırıkkale Üniversitesi, Türkiye.
tamereren@gmail.com

ÖZ

Günümüzde Endüstri 4.0'ın temel taşı olan Siber Fiziksel Sistemler (SFS); hesaplama, ağ ve fiziksel süreçlerin entegrasyonuyla üretimden kritik altyapılara kadar geniş bir sahada dönüşümün öncüsüdür. Ancak literatür incelendiğinde, bu sistemlerin tasarım süreçlerinde karşılaşılan siber güvenlik, sistem dayanıklılığı ve maliyet gibi birbiriyle çelişen kriterlerin eş zamanlı optimizasyonu noktasında metodolojik bir darboğaz olduğu görülmektedir. Mevcut çalışmaların çoğunlukla kavramsal çerçevede kalması ve teknik parametreleri bütüncül bir sayısal modelle önceliklendirememesi, uygulamaya yönelik karar süreçlerinde nesnellik kaybına yol açmaktadır. Bu çalışmanın temel amacı, SFS ekosistemindeki karmaşık teknik gereksinimleri analiz ederek, belirsizlik altında en uygun sistem mimarisini belirleyen bütüncül bir değerlendirme çerçevesi sunmaktır. Bu kapsamda, karar vericilerin sübjektif yargılarını ve teknik belirsizlikleri modele dahil edebilen Pisagor Bulanık AHP yöntemiyle kriter ağırlıkları hesaplanmış; alternatif tasarımlar ise TOPSIS yöntemiyle sıralanmıştır. Analiz neticesinde; Veri Güvenilirliği (0,277) ve Siber Güvenlik (0,162) en kritik öncelikler olarak saptanırken, Maliyet (0,161) faktörünün teknik yeterlilikle başa baş bir öneme sahip olduğu matematiksel olarak kanıtlanmıştır. Nihai değerlendirmede; uç bilişim ile merkezi analitik gücü birleştiren Hibrit Kontrol Mimarisi (A3), 0,604 ideal çözüm değeriyle en dirençli ve verimli mimari olarak belirlenmiş; onu sırasıyla Bulut Tabanlı Merkezi Sistem (A1) ve

* Sorumlu yazarın e-posta adresi: tamereren@gmail.com

Cite as: Coşkun, T. & Yolcu, E. & Kudu, S. & Sanlı, Y.B. & Öztürk, B. N. & Eren, T. (2026). Siber Fiziksel Sistemlerin İncelenmesi ve Değerlendirilmesi, *Journal of Smart Systems Research, 7*(1), 79-93. https://doi.org/10.58769/joinssr.1905520

Creative Commons Attribution 4.0 International (CC BY 4.0) license (https://creativecommons.org/licenses/by/4.0/)

Kenar Bilişim Destekli Sistem (A2) takip etmiştir. Bu araştırma, SFS literatüründeki "tek boyutlu değerlendirme" eksikliğini gidererek, uygulayıcılar için matematiksel doğruluğu yüksek, stratejik bir karar destek mekanizması sunması bakımından özgün bir değer taşımaktadır.

Anahtar Kelimeler: Siber fiziksel sistemler, Endüstri 4.0, Siber güvenlik, Dijital dönüşüm, Yapay zeka

Examination and Evaluation of Cyber-Physical Systems

ABSTRACT

Cyber-Physical Systems (CPS), which serve as the cornerstone of Industry 4.0 today, are driving transformation across a wide range of fields from manufacturing to critical infrastructure through the integration of computing, networking, and physical processes. However, a review of the literature reveals a methodological bottleneck in the simultaneous optimization of conflicting criteria such as cybersecurity, system resilience, and cost encountered during the design processes of these systems. Since most existing studies remain within a conceptual framework and fail to prioritize technical parameters through a comprehensive numerical model, this leads to a loss of objectivity in application-oriented decision-making processes. The primary objective of this study is to analyze the complex technical requirements within the SFS ecosystem and present a comprehensive evaluation framework that identifies the most suitable system architecture under uncertainty. In this context, criterion weights were calculated using the Pythagorean Fuzzy AHP method, which incorporates decision-makers' subjective judgments and technical uncertainties into the model; alternative designs were then ranked using the TOPSIS method. As a result of the analysis, Data Reliability (0.277) and Cybersecurity (0.162) were identified as the most critical priorities, while it was mathematically proven that the Cost (0.161) factor holds equal importance to technical adequacy. In the final evaluation, the Hybrid Control Architecture (A3), which combines edge computing with centralized analytical power, was identified as the most resilient and efficient architecture with an ideal solution value of 0.604; it was followed by the Cloud-Based Centralized System (A1) and the Edge Computing-Supported System (A2). This research addresses the "one-dimensional evaluation" gap in the SFS literature and holds unique value in providing practitioners with a strategic decision-support mechanism backed by high mathematical accuracy.

Keywords: Cyber-physical systems, Industry 4.0, Cyber security, Digital transformation, Artificial intelligence.

1 Giriş

Siber Fiziksel Sistemler (SFS); hesaplama birimleri, iletişim ağları ve fiziksel süreçlerin kusursuz bir entegrasyonuyla fiziksel dünyayı sanal dünya ile birleştiren stratejik yapılardır. Sensörler ve aktüatörler aracılığıyla fiziksel ortamdan veri toplayan bu sistemler, veriyi dijital düzlemde işleyerek fiziksel dünyaya kritik geri beslemeler sağlamaktadır (Öztürk, 2020). Günümüzde Endüstri 4.0 paradigmasının temel taşı haline gelen SFS teknolojileri; akıllı üretim, otonom lojistik ve dinamik tedarik zinciri süreçlerinde köklü dönüşümler yaratarak endüstriyel verimliliği yeni bir boyuta taşımıştır (Gedik, 2021; Özdemir ve Özgüner, 2018).

Dijitalleşme dalgasının yaygınlaşması, SFS uygulamalarının sanayi sınırlarını aşarak çok geniş bir sektörel yelpazeye nüfuz etmesine yol açmıştır. Bu bağlamda, lojistik sektöründe operasyonel hızı artıran akıllı depo sistemleri ve otomasyon çözümleri Genç ve Tunalı (2022), SFS'nin sahadaki somut gücünü temsil etmektedir. Benzer şekilde, yeni ürün geliştirme süreçlerinde bu bileşenlerin kullanımı literatürde stratejik bir rekabet unsuru olarak vurgulanmaktadır (Göksu ve Atay, 2018). Ancak bu teknolojik yayılım, sistem karmaşıklığını artırırken kritik altyapılara yönelik siber güvenlik risklerini de beraberinde getirmiştir (Acarer, 2020). Bilgisayar ağları üzerinden gerçekleştirilen saldırı analizleri

Dicle (2022) ve elektronik sınav sistemleri gibi dijital platformların hedef alınması Akaslan (2021), SFS mimarilerinin sadece "akıllı" değil, aynı zamanda "dirençli" tasarlanması gerektiğini kanıtlamıştır.

Söz konusu güvenlik ve performans risklerinin yönetilmesinde; yapay zekâ ve makine öğrenmesi tabanlı yaklaşımlar, tehditlerin tespiti ve proaktif savunma mekanizmalarının geliştirilmesinde hayati bir rol oynamaktadır (Efe 2021; Özdemir ve Özgüner, 2018). Özellikle Endüstri 5.0 ve Toplum 5.0 kavramlarının yükselişiyle, SFS' lerin teknik başarısı kadar toplumsal ve insani etkileri de akademik tartışmaların odağına yerleşmiştir (Büyükgöze, 2020). Yeni sanayileşen ülkeler için bu geçiş süreci, siber risklerin yönetimi noktasında dikkatli bir strateji gerektirmektedir (Duran, 2024). Türkiye'de de SFS, yapay zekâ ve dijital dönüşüm üzerine yapılan akademik çalışmalar son yıllarda ivme kazanmış olsa da Akgül vd. (2018); Kaygın vd. (2019) literatürdeki bu çalışmaların büyük oranda belirli alt alanlara odaklandığı ve bütüncül bir performans değerlendirme çerçevesinden yoksun olduğu gözlemlenmektedir (Öztürk, 2020).

Bu çalışmanın temel hareket noktası, literatürdeki söz konusu parçalı yapıyı ve bütüncül analiz eksikliğini gidermektir. Klasik değerlendirme yaklaşımlarının SFS ekosistemindeki belirsiz uzman görüşlerini ve teknik karmaşıklığı modellemekte yetersiz kalması, daha esnek bir metodoloji kullanımını zorunlu kılmıştır. Bu bağlamda çalışmada; kriter ağırlıklarının belirlenmesinde karar verici öznelliğini ve belirsizliğini yüksek doğrulukla yansıtabilen Pisagor Bulanık AHP yöntemi tercih edilmiştir. Elde edilen ağırlıklar ışığında, alternatif sistem mimarilerinin performansını matematiksel olarak sıralayan TOPSIS yöntemi kullanılarak en uygun mimari tespit edilmiştir. 29 farklı akademik çalışma üzerinden kurgulanan bu karar destek modeli, siber güvenlik kısıtları ile operasyonel verimliliği aynı potada eriterek Türkiye'deki Endüstri 4.0 dönüşümü için teorik değil, uygulanabilir ve sayısal verilerle doğrulanmış bir yol haritası sunmaktadır.

2 Literatür Taraması

Akademik yazın incelendiğinde, dijital dönüşüm ve güvenlik odaklı çalışmaların temel olarak Endüstri 4.0'ın sektörel izdüşümleri, teknik siber güvenlik uygulamaları ve sosyoteknik dönüşümün etkileri olmak üzere üç ana temada toplandığı görülmektedir. İlk grupta yer alan çalışmalar; Endüstri 4.0'ın lojistik süreçlerindeki rolünü Genç ve Tunalı (2022), Özdemir ve Özgüner (2018), yeni ürün geliştirme stratejilerini Göksu ve Atay (2018) ve tedarik zinciri yönetimini Gedik (2021) analiz etmektedir. Bu teknolojik dönüşümün beşerî sermaye ve personel yetkinliği üzerindeki kritik etkileri ise Akgül vd. (2018) ve Şentürk ve Büber (2023) tarafından ele alınmıştır. Ancak, literatürdeki bu çalışmaların önemli bir kısmının Sağbaş ve Gülseren (2019), Kaygın vd. (2019) ve Efe (2021) yöntem olarak betimsel literatür taramasına dayanması, alandaki ampirik ve teknik derinliğe sahip veri analizi ihtiyacını açıkça ortaya koymaktadır.

Siber güvenlik eksenindeki tartışmalar incelendiğinde; çalışmaların bir bölümü makro ölçekli devlet politikaları ve siber risk yönetimine odaklanırken Acarer (2020) ve Kiraz (2021), diğer bir bölümü IoT Avcı (2022), akıllı depo sistemleri ve raylı sistemler Özarpa vd. (2021) gibi spesifik altyapıların güvenliğini irdelemektedir. Teknik derinlik açısından; MITM saldırılarına karşı savunma yöntemleri Dicle (2022), siber saldırı analiz modelleri Söğüt ve Erdem (2020), Akaslan (2021) ve yapay zekâ tabanlı güvenlik sistemleri Gençoğlu (2022) literatürde önemli bir yer tutmaktadır. Buna karşın, Toplum 5.0 ve Metaverse gibi güncel kavramlara odaklanan çalışmalar Mandal vd. (2022) ve Kürkcü (2024) büyük ölçüde kavramsal çerçeve sunmakla sınırlı kaldığı ve teknik açıdan önemli boşluklar barındırdığı görülmektedir.

Literatürde siber güvenlik farklı boyutlarıyla ele alınmıştır. Altınkış ve Barkuş (2023), dijital ortamlarda kişisel veri güvenliğini inceleyerek bireysel veri mahremiyetine yönelik tehditleri derleme yöntemiyle değerlendirmiştir. Erkul (2024), siber güvenlik politikalarını güç ve caydırıcılık perspektifinden ele alarak konuyu literatür taraması kapsamında analiz etmiştir. Gürdal Limon (2023) ise siber güvenliği savaş yönetim sistemleri bağlamında inceleyerek özellikle savunma ve güvenlik alanındaki etkilerini analiz etmiştir. Ancak mevcut çalışmaların büyük ölçüde derleme, literatür taraması veya kavramsal

analiz düzeyinde kaldığı; nicel modelleme ve karar destek mekanizmaları içeren uygulamalı çalışmaların sınırlı olduğu görülmektedir.

Bu çalışmanın literatüre sağladığı temel katkı ve metodolojik farklılık, mevcut çalışmaların büyük ölçüde derleme veya durum tespiti düzeyinde kalmasından kaynaklanmaktadır. Literatürdeki bu kuramsal yoğunluğun aksine, siber tehdit istihbaratında makine öğrenmesi Özdemir (2024) ve karma yöntemli denetim mekanizmaları Özkan ve Dinç (2025) gibi çalışmaların sayısı oldukça kısıtlıdır. Dolayısıyla bu çalışma, literatürdeki yöntemsel tekdüzeliği aşarak, siber güvenlik stratejilerini sadece teorik bir düzlemde değil, ampirik bir çerçevede sentezleyerek mevcut teknik boşluğu doldurmayı hedeflemektedir.

Tablo 1: *Literatür Taraması*

Yazar	Konu	Yöntem
Göksu vd. (2018)	Yeni ürün geliştirmede Endüstri 4.0 rolü	Literatür Taraması
Özdemir ve Özgüner (2018)	Endüstri 4.0 ve lojistik sektörüne etkileri: Lojistik 4.0	Literatür Taraması/ derleme
Akgül vd. (2018)	Sanayi 4.0 Sürecinde Gazetecilik Sektöründe Çalışacak Personelin Mesleki Yetenek ve Yeterliliğine Yönelik Değerlendirme ve Öngörüler	Literatür Taraması/ Kurgulama
Karasulu (2019)	Derin öğrenme kullanarak çoklu ortam sisteminde sahne ve olayların tespiti	Literatür Taraması
Sağbaş ve Gülseren (2019)	Endüstri 4.0 açısından sanayide dijital dönüşüm ve olgunluk seviyesinin ölçümü	Değerlendirme/Literatür taraması
Kaygın vd. (2019)	Endüstri 4.0'a akademik bakış	Literatür Taraması
Söğüt ve Erdem (2020)	SCADA / Endüstriyel Kontrol Sistemlerinde siber terör saldırılarının veri madenciliği ve makine öğrenmesi algoritmaları ile tespit edilmesi	Veri/Model/Analiz
Acarer (2020)	Ülke güvenliğimizde alınabilecek makro siber güvenlik önlemleri	Ampirik Veri Toplama
Büyükgöze (2020)	Toplum 5.0 ve dijital sağlık	Literatür Taraması
Efe (2021)	Yapay zekâ odaklı siber risk ve güvenlik yönetimi	Literatür Taraması
Büyükbingöl (2021)	Sosyal bilimlerde deney ve gözlem imkânı sunan yöntem önerisi	Artifical SocietyComputational Experiment-Parallel Execution (ACP)
Akaslan (2021)	Elektronik sınav sistemlerine yönelik siber saldırılar ve caydırıcı yöntemler	Değerlendirme Analizi
Özarpa vd. (2021)	Akıllı raylı sistemlerde kullanılan alt sistemlerin kritik seviye analizi	AHP
Kiraz (2021)	Türkiye'de siber güvenlik politikalarının güvenlikleştirme ve risk algısı üzerinde etkisi	Literatür Taraması
Gedik (2021)	Endüstri 4.0 teknolojilerinin üretim ve tedarik zinciri üzerindeki etkilerinin incelenmesi	Literatür Taraması
Genç ve Tunalı (2022)	Akıllı depo sistemleri	Derleme Çalışması
Avcı (2022)	Akıllı evlerde IoT teknolojileri ve siber güvenlik	Literatür Taraması
Dicle (2022)	Bilgisayar ağlarında gerçekleşen MITM saldırılarına karşı savunma yöntemleri	Araştırma/Uygulama
Mandal vd. (2022)	Sanal dünyada gizlilik ve güvenlik problemleri	Literatür Taraması
Gençoğlu (2022)	IPS sistemlerinde yapay zekanın son beş yıldaki değişimi	Kurumsal İnceleme/ Literatür Taraması
Gürdal Limon (2023)	Siber güvenlik açısından savaş yönetim sistemleri	Analiz Tekniği
Altınkış ve Barkuş (2023)	Dijital ortamlarda kişisel veri güvenliği	Derleme Çalışması

Varol (2023)	Dijital dönüşüm ve yapak zeka teknolojilerinin muhasebe ve denetim meslekleri üzerine etkisi	İnceleme
Şentürk ve Büber (2023)	Endüstriyel değişim sürecinin insan kaynakları yönetimi uygulamalarına etkisi	Nitel Araştırma
Özdemir (2024)	Siber tehdit istihbaratında yapay zeka ve makine öğrenmesi	Tehdit Analizi
Erkul (2024)	Siber güvenlik politikasını güç ve caydırıcılık üzerinden anlamlandırma	Literatür Taraması
Kürkcü (2024)	Özgürlük ve güvenlik ilişkisi açısından metaverse	Literatür Taraması
Özkan ve Dinç (2025)	Rusya'daki güvenlik anlayışı ve toplumsal denetim mekanizması analizi	Çoklu Yöntem Araştırması

3 Metodoloji

Bu çalışmada, Siber Fiziksel Sistemlerin (SFS) teknik ve operasyonel performans özellikleri, karmaşık karar süreçlerindeki belirsizlikleri minimize edebilen bütünleşik bir Çok Kriterli Karar Verme yaklaşımıyla sistematik olarak analiz edilmiştir. Araştırma süreci; kapsamlı bir literatür taraması ve uzman görüşleri aracılığıyla veri güvenilirliği, siber güvenlik, maliyet, sistem dayanıklılığı ve enerji verimliliği gibi temel performans kriterlerinin belirlenmesiyle başlamış; tüm metodolojik akış literatürdeki standart çözüm adımları Öztürk (2020); Yüksel vd. (2024) dikkate alınarak kurgulanmıştır. Kriterlerin göreli önem derecelerinin hesaplanmasında, geleneksel bulanık kümelere oranla uzman yargılarındaki tereddütleri ve üyelik dışı durumları daha esnek bir şekilde modelleyebilen Pisagor Bulanık Analitik Hiyerarşi Süreci (AHP) yöntemi kullanılmıştır Tuğrul (2022); Büyükbingöl (2021). Bu yöntemde, karar vericilerin değerlendirmeleri üyelik ve üyelik dışı dereceleri arasındaki kareli toplam ilişkisi üzerinden ele alınarak, SFS gibi yüksek belirsizlik içeren teknolojik altyapılarda matematiksel olarak daha tutarlı sonuçlar elde edilmiştir. Hesaplanan kriter ağırlıkları, alternatif sistem mimarilerinin başarı sıralamasının oluşturulması amacıyla TOPSIS yöntemine entegre edilmiştir Tuğrul (2022). Bu aşamada, her bir mimari tasarımın pozitif ideal çözüme olan yakınlığı ve negatif ideal çözümden uzaklığı analiz edilerek nihai performans skorları hesaplanmıştır. İncelenen akademik çalışmalar ve bibliyometrik veriler üzerinden kurgulanan bu bütünleşik karar destek modeli Öztürk (2020); Yüksel vd. (2024), siber güvenlik kısıtları ile operasyonel verimliliği aynı potada eriterek, "Hibrit Kontrol Mimarisinin diğer tasarımlara göre daha dirençli bir çözüm sunacağı" yönündeki temel araştırma hipotezini doğrulamayı ve Türkiye'deki Endüstri 4.0 dönüşümü için uygulanabilir bir değerlendirme çerçevesi sunmayı amaçlamaktadır.

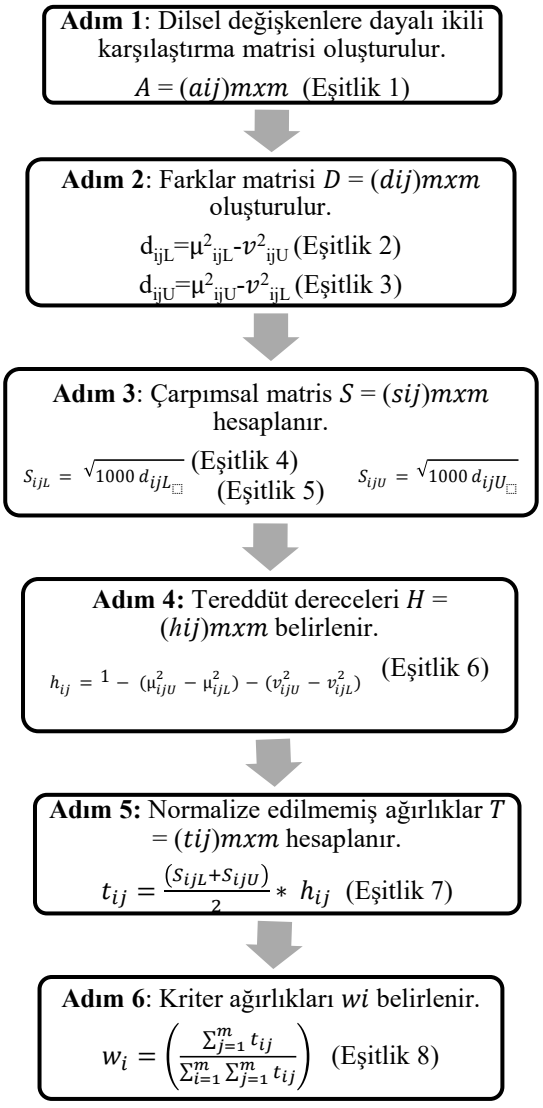
3.1 Pisagor Bulanık AHP Yöntemi

Analitik Hiyerarşi Prosesi (AHP), karar vericilerin çok kriterli problemleri sistematik olarak analiz etmelerini sağlayan ikili karşılaştırmalara dayalı bir ÇKKV yöntemidir. Kriter ve alternatiflerin göreli önemlerini belirlerken, klasik AHP net sayılarla çalıştığı için insan yargılarındaki belirsizlikleri tam yansıtamaz. Bu nedenle AHP, bulanık mantıkla bütünleştirilmiş ve Bulanık AHP geliştirilmiştir; burada değerlendirmeler dilsel ifadelerle modellenip bulanık sayılarla temsil edilir. Geleneksel bulanık kümelerin yetersiz kaldığı durumlarda ise Pisagor Bulanık AHP devreye girer; üyelik ve üyelik olmama derecelerinin kareleri toplamı 1'e eşit veya daha küçük olacak şekilde karar vericilerin tereddütleri daha esnek ve güçlü ifade edilir, böylece belirsizlik içeren problemler için daha tutarlı sonuçlar elde edilir. Pisagor Bulanık AHP'de ikili karşılaştırmalar dilsel değişkenler aracılığıyla yapılmakta ve bu ifadeler Pisagor bulanık sayılarla modellenmektedir. Analizde kullanılan dilsel değişkenler ve bunlara karşılık gelen Pisagor bulanık sayılar Tablo 2'de sunulmuştur.

Tablo 2: *Pisagor Bulanık Sayı Ölçeği ve Dilsel Değişkenler (Öztürk vd., 2020)*

Dilsel Değişkenler	Pisagor Bulanık Sayılar			
	En Düşük Üye Olma Derecesi (μL)	En Yüksek Üye Olma Derecesi (μU)	En Düşük Üye Olmama Derecesi (vL)	En Yüksek Üye Olmama Derecesi (vU)
Kesinlikle Düşük (KD)	0,000	0,000	0,900	1,000
Çok Düşük (ÇD)	0,100	0,200	0,800	0,900
Düşük (D)	0,200	0,350	0,650	0,800
Ortalamanın Altı (OA)	0,350	0,450	0,550	0,650
Eşit (E)	0,197	0,197	0,197	0,197
Ortalama (O)	0,450	0,550	0,450	0,550
Ortalamanın Üstü (OÜ)	0,550	0,650	0,350	0,450
Yüksek (Y)	0,650	0,800	0,200	0,350
Çok Yüksek (ÇY)	0,800	0,900	0,100	0,200
Kesinlikle Yüksek (KY)	0,900	1,000	0,000	0,000

Pisagor Bulanık AHP yöntem adımları Şekil 1'de gösterilmiştir.

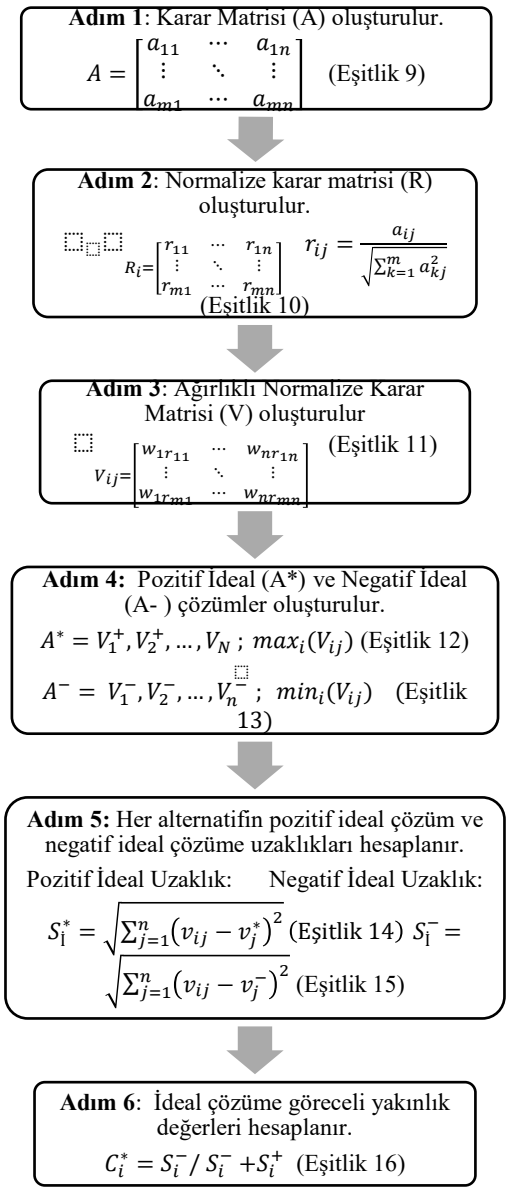


Şekil 1. Pisagor Bulanık AHP Yöntem Adımları

İlk adımında karar problemi için kriterler belirlenir ve uzman görüşleri doğrultusunda dilsel değişkenler kullanılarak Eşitlik 1' de gösterilen ikili karşılaştırma matrisi daha sonra Pisagor bulanık sayılar kullanılarak ikili karşılaştırma matrisi elde edilir. Eşitlik 2 ve 3 ile fark matrisi hesaplanır. Oluşturulan bu değerler kullanılarak bulanık öncelik değerleri elde edilir ve kriterlerin göreli önem derecelerini belirleyen ağırlık vektörü Eşitlik 3 ve Eşitlik 4 kullanılarak hesaplanır. Ardından Pisagor bulanık sayılar üzerinde normalizasyon işlemi Eşitlik 5 uygulanarak kriter ağırlıkları düzenlenir. Eşitlik 6 ile tereddüt dereceleri elde edilir. Normalize edilmemiş ağırlıklar Eşitlik 7 yardımıyla hesaplanır. Sonrasında kriterlerin nihai ağırlıkları Eşitlik 8 ile hesaplanır.

3.2 TOPSIS Yöntemi

TOPSIS yöntemi, Yoon ve Hwang tarafından geliştirilmiş olup, alternatifleri ideal çözüme en yakın ve negatif ideal çözüme en uzak olacak şekilde sıralar. Çözüm süreci, ölçütlerin satırlarda, alternatiflerin sütunlarda yer aldığı bir matrisin oluşturulmasıyla başlar. TOPSIS yöntemi 6 aşamadan oluşmaktadır ve bu adımlar Şekil 2'de verilmiştir.



Şekil 2. TOPSIS Yöntemi Adımları

TOPSIS yöntemi, çok kriterli karar verme problemlerinde alternatiflerin ideal çözüme yakınlıklarına göre sıralanmasını sağlayan bir yöntemdir. Yöntemin uygulanmasında öncelikle Eşitlik 9 kullanılarak karar matrisi oluşturulur. Daha sonra karar matrisi Eşitlik 10 ile normalize edilerek farklı ölçeklerdeki veriler karşılaştırılabilir hale getirilir. Normalize edilen değerler kriter ağırlıkları ile çarpılarak Eşitlik 11' deki ağırlıklı normalize karar matrisi elde edilir. Bu aşamadan sonra Eşitlik 12 ile pozitif ideal çözüm (en iyi değerler) ve Eşitlik 13 ile negatif ideal çözüm (en kötü değerler) belirlenir. Alternatiflerin hem pozitif ideal çözüme hem de negatif ideal çözüme olan uzaklıkları Eşitlik 14 ve 15 kullanılarak hesaplanır. Son aşamada ise her alternatif için ideal çözüme göreli yakınlık katsayısı Eşitlik 16 ile hesaplanarak alternatifler bu değerlere göre sıralanır ve en yüksek değere sahip alternatif en uygun seçenek olarak belirlenir.

4 Teori ve Hesaplama

Bu bölüm, SFS mimarilerinin değerlendirilmesinde karşılaşılan karmaşıklığın modellenmesine yönelik teorik altyapıyı ve bu altyapının hesaplama sürecine entegrasyonunu içermektedir.

4.1 Teori

SFS mimarilerinin performans analizi, doğası gereği yüksek düzeyde belirsizlik ve çok boyutlu karar parametreleri içermektedir. Mevcut literatürde geleneksel karar verme yöntemleri, karar vericilerin "kararsızlık" durumlarını ve bilginin eksik ifade edildiği bulanık alanları modellemede yetersiz kalabilmektedir. Bu çalışmada tercih edilen Pisagor Bulanık AHP yöntemi, geleneksel sezgisel bulanık kümelere kıyasla daha geniş bir üyelik derecesi alanı sunarak, SFS güvenliği ve maliyet dengesi gibi çelişkili kriterlerin yarattığı belirsizliği daha esnek bir matematiksel düzlemde ifade etme imkanı sağlar.

Teorik çerçevede, SFS bileşenlerinin heterojen yapısı; kriterlerin sadece sayısal değerlerle değil, uzman görüşlerine dayalı dilsel değişkenlerle de ağırlıklandırılmasını zorunlu kılmaktadır. Pisagor Bulanık AHP, bu dilsel yargıları matematiksel bir tutarlılıkla işleyerek kriterler arasındaki hiyerarşik bağımlılığı ortaya koymaktadır. Karar modelinin ikinci aşamasında kullanılan TOPSIS yöntemi ise, belirlenen bu ağırlıkları kullanarak alternatif mimarilerin "ideal çözüme olan geometrik uzaklığını" hesaplar. Bu bütünleşik metodoloji, SFS gibi kritik sistemlerin mimari seçiminde sadece en iyi performansı değil, aynı zamanda en az riskli (negatif ideale en uzak) çözümü de belirlemeye yönelik teorik bir temel oluşturmaktadır.

4.2 Hesaplama

Analiz sürecinde, SFS mimarilerinin performansını belirleyen sekiz ana kriter (K1-K8), uzman görüşleri ve sektörel teknik gereksinimler doğrultusunda Pisagor bulanık sayılarla normalize edilerek ikili karşılaştırma matrislerine dönüştürülmüştür. Hesaplama aşamasında öncelikle Pisagor bulanık skor fonksiyonları yardımıyla kriterlerin nihai ağırlıkları (K7: 0,277, K1: 0,162 vb.) elde edilmiştir. Bu ağırlıklandırma, matematiksel olarak veri güvenilirliği ve siber güvenliğin, operasyonel süreklilik üzerindeki belirleyici etkisini sayısal olarak doğrulamaktadır.

Elde edilen ağırlık vektörleri, TOPSIS çözüm matrisine entegre edilerek üç farklı alternatif mimari (A1, A2, A3) için "Pozitif İdeal Çözüme Yakınlık Dereceleri" hesaplanmıştır. Hesaplama sonuçları, Hibrit Kontrol Mimarisinin (A3) ideal çözüme en yakın (0,604) performans skoruna ulaştığını göstermektedir. Bu sayısal çıktı, uç bilişim ile merkezi bulut sistemlerinin entegrasyonunun, teorik olarak öngörülen "düşük gecikme-yüksek güvenlik" optimizasyonunu pratik bir çözüm kümesine dönüştürdüğünü kanıtlamaktadır.

5 Bulgular ve Tartışma

Bu bölümde, Türkiye ölçeğinde SFS mimarilerinin değerlendirilmesine yönelik uygulanan hibrit karar modelinin çıktıları; teknik gereksinimler, operasyonel darboğazlar ve literatürdeki tartışmalar ekseninde derinlemesine analiz edilmektedir. Uygulama süreci, yalnızca sayısal bir sıralama sunmakla kalmayıp, SFS ekosistemindeki stratejik önceliklerin rasyonel bir dökümünü ortaya koymaktadır.

Pisagor Bulanık AHP analizi sonucunda elde edilen ağırlıklar (Tablo 7), SFS tasarımında güvenlik ve veri bütünlüğünün operasyonel parametrelerin önüne geçtiğini matematiksel olarak kanıtlamaktadır. Veri Güvenilirliği (K7: 0,277) ve Siber Güvenlik (K1: 0,162) kriterlerinin toplamda kararın yaklaşık %44'ünü domine etmesi, endüstriyel sistemlerin dijitalleşme sürecinde "verinin doğruluğu" ve "dış müdahalelere karşı direnç" olgularının en kritik öncelikler olarak kabul edildiğini göstermektedir.

Gerçek Zamanlılık (K4: 0,020) ve Sistem Dayanıklılığı (K2: 0,012) kriterlerinin nispeten düşük ağırlık alması, bu parametrelerin sistemsel değerinden ziyade karar verme sürecindeki "ayırt edici" rolleriyle ilgilidir. Literatürde Göksu vd; Karasulu [5, 31] vurgulandığı üzere, güncel SFS altyapılarında gerçek zamanlı tepki verme kabiliyeti artık standart bir teknik gereksinim kabul edilmektedir. Karar vericiler, modern sistemlerin bu hızı zaten karşılayacağını varsaydığı için, tercihlerini hızın ötesindeki "risk yönetimi" ve "ekonomik sürdürülebilirlik" (K8: 0,161) eksenine kaydırmışlardır. K2'nin (Sistem Dayanıklılığı) payı ise, fiziksel dayanıklılığın artık siber güvenlik (K1) şemsiyesi altında "dijital direnç" olarak tanımlanması ile açıklanabilir; yani sistemin ayakta kalması artık mekanik bir sorundan ziyade siber bir savunma meselesi olarak algılanmaktadır.

Alternatiflerin ideal çözüme yakınlık derecelerine göre sıralandığı TOPSIS analizinde (Tablo 8), Hibrit Kontrol Mimarisi (A3) 0,604 başarı skoru ile en optimize çözüm olarak öne çıkmaktadır. A3'ün başarısı, siber güvenlik (K1) ile maliyet (K8) arasındaki çelişkili ilişkiyi en dengeli şekilde yönetilmesinden kaynaklanmaktadır.

Bu sonuç, Acarer [6] ve Özdemir B. [26] tarafından savunulan, merkezi denetim ile yerel işleme gücünün entegrasyonu gerekliliğiyle tam bir uyum içerisindedir. Çalışma, literatürdeki genel geçer "hibrit modeller verimlidir" savını, Pisagor Bulanık AHP ve TOPSIS metodolojisiyle sayısal bir düzleme taşıyarak ampirik bir kanıt sunmuştur. Ek olarak Literatürdeki bazı çalışmalarda Genç vd. [4] kenar bilişimin (A2) düşük gecikme avantajı nedeniyle ön planda olması beklenirken; çalışmamızda A2'nin 0,408 skorla son sırada kalması dikkat çekicidir. Bu durum, Türkiye özelindeki SFS uygulamalarında karar vericilerin "maliyet-etkin güvenlik" beklentisinin, saf teknik performans ve hızın önüne geçtiğini göstermektedir.

5.1 Problem Tanımı

SFS, fiziksel süreçlerin bilgisayar tabanlı algoritmalarla entegre edildiği karmaşık yapılar olarak Endüstri 4.0'ın temelini oluşturmaktadır. Ancak, bu sistemlerin tasarım ve değerlendirme süreçlerinde karşılaşılan en büyük problem, siber güvenlik, sistem dayanıklılığı ve maliyet gibi birbiriyle çelişen çok sayıda kriterin aynı anda optimize edilmesindeki güçlüklerdir. Literatürde bu sistemlerin teknik gereksinimleri genellikle tek boyutlu olarak ele alınmakta, belirsizlik içeren karar verme süreçlerinde bütüncül ve sayısal bir metodolojinin eksikliği hissedilmektedir. Özellikle Türkiye ölçeğindeki akademik çalışmaların çoğunlukla kavramsal çerçevede kalması, teknik parametreleri önceliklendiren ve en uygun sistem mimarisini bilimsel yöntemlerle belirleyen uygulama temelli modellerin yetersizliğini ortaya koymaktadır. Bu çalışma, söz konusu çok kriterli karmaşıklığı çözmek ve karar vericiler için objektif bir değerlendirme çerçevesi sunmak amacıyla kurgulanmıştır.

5.2 Kriterlerin Belirlenmesi

Uygulama sürecinde kullanılan değerlendirme kriterleri, incelenen akademik çalışmalar ve SFS alanındaki teknik gereksinimler temel alınarak belirlenmiştir. Kriterler; sistemin yapısal sağlamlığı, operasyonel verimliliği ve güvenlik standartları dikkate alınarak oluşturulmuştur. Belirlenen kriterler; Siber Güvenlik (K1), Sistem Dayanıklılığı (K2), Enerji Verimliliği (K3), Gerçek Zamanlılık (K4), Birlikte Çalışabilirlik (K5), Ölçeklenebilirlik (K6), Veri Güvenilirliği (K7) ve Maliyet (K8) olmak üzere sekiz ana başlık altında toplanmıştır. Bu kriterler, SFS alanında tasarlanan sistemlerin hem operasyonel performansını hem de güvenlik açıklarını bütüncül bir şekilde değerlendirebilecek şekilde tasarlanmıştır. Tablo 4'te her bir kriterin kapsamı ve değerlendirme boyutları ayrıntılı biçimde açıklanmıştır.

Tablo 4: *Kriterler ve Açıklamaları*

Kriter Adı	Açıklama
Siber Güvenlik (K1) Öztürk (2020)	Veri bütünlüğü, yetkisiz erişime karşı direnç ve şifreleme mekanizmalarının gücü.
Sistem Dayanıklılığı (K2) Gedik (2021)	Arıza veya siber saldırı durumunda sistemin kritik fonksiyonlarını sürdürebilme kapasitesi.
Enerji Verimliliği (K3) Avcı (2022)	Sensör ve aktüatörlerin minimum enerji tüketimiyle maksimum verimlilik sunması.
Gerçek Zamanlılık (K4) Dicle (2022)	Sistemin fiziksel dünyadan gelen veriye tepki verme hızı ve gecikme süresi.
Birlikte Çalışabilirlik (K5) Gençoğlu (2022)	Farklı donanım ve yazılım protokollerinin birbirleriyle sorunsuz veri değişimi yapabilmesi.
Ölçeklenebilirlik (K6) Varol (2023)	Sistemin artan veri trafiği veya eklenen yeni cihazlara karşı performansını koruması.
Veri Güvenilirliği (K7) Altıntaş ve Barkuş (2023)	Sensörlerden alınan verilerin doğruluğu ve dış gürültüden etkilenme düzeyi.
Maliyet (K8) Özdemir ve Özgüner (2018)	Kurulum, bakım ve operasyonel süreçlerin toplam maliyet etkinliği.

5.3 Alternatiflerin Belirlenmesi

Çalışma kapsamında değerlendirilecek olan alternatif sistem mimarileri; SFS Endüstri 4.0 sürecindeki teknik gereksinimler ve literatürdeki yaygın uygulama modelleri referans alınarak üç ana başlıkta belirlenmiştir. İlk alternatif olan Bulut Tabanlı Merkezi Sistem (A1); verilerin tek bir merkezden yönetildiği ve geniş depolama kapasitesi sunduğu için modele dahil edilmiştir. Bu mimari, Öztürk (2020) ile Özdemir ve Özgüner (2018) tarafından vurgulanan merkezi lojistik ve veri yönetimi yapıları temel alınarak kurgulanmıştır. İkinci alternatif olan Kenar Bilişim Destekli Sistem (A2); düşük gecikme süresi ve yerinde veri işleme avantajı nedeniyle seçilmiştir. Bu seçimde Gedik (2021) ile Genç ve Tunalı (2022) tarafından önerilen akıllı üretim ve depo otomasyon sistemlerindeki dağıtık mimariler referans alınmıştır. Son olarak, yerel hızı merkezi analitik güçle birleştiren Hibrit Kontrol Mimarisi (A3); Acarer [6] tarafından siber güvenlik ve operasyonel süreklilik üzerine sunulan karma çözüm önerileri doğrultusunda modele eklenmiştir. Açıklamalı alternatifler tablosu Tablo 5'te verilmiştir.

Tablo 5: *Alternatifler ve Açıklamaları*

Alternatif Adı	Açıklama
Bulut Tabanlı Merkezi Sistem (A1)	Verilerin tek merkezden yönetilmesi ve geniş depolama kapasitesi.
Kenar Bilişim Destekli Sistem (A2)	Düşük gecikme süresi ve yerinde veri işleme.
Hibrit Kontrol Mimarisi (A3)	Yerel hız ile merkezi analitik gücün birleşimi ile operasyonel süreklilik.

5.4 Uygulama Sonucunun Değerlendirilmesi

Kriterler Pisagor Bulanık AHP yöntemi kullanılarak ağırlıklandırılmış, alternatiflerin sıralanması ise TOPSIS yöntemiyle gerçekleştirilmiştir.

5.4.1 Pisagor Bulanık AHP ile Kriterleri Ağırlıklandırılması

Pisagor Bulanık AHP yöntemi kapsamında uzman görüşleri doğrultusunda oluşturulan kriterlerin ikili karşılaştırma matrisi Tablo 6'da sunulmuştur.

Tablo 6: *Kriterlerin İkili Karşılaştırması*

Kriterler	K1	K2	K3	K4	K5	K6	K7	K8
K1	E	Y	OÜ	ÇY	OA	KY	ÇD	O
K2	D	E	ÇD	OA	ÇD	ÇD	KD	D
K3	OA	ÇY	E	O	O	D	OA	ÇY
K4	ÇD	OÜ	O	E	KD	OA	ÇD	ÇD
K5	OÜ	ÇY	O	KY	E	D	KD	OA
K6	KD	ÇY	Y	OÜ	Y	E	Y	Y
K7	ÇY	KY	OÜ	ÇY	KY	D	E	KD
K8	O	Y	ÇD	ÇY	OÜ	D	KY	E

Pisagor Bulanık Sayı Ölçeği ve Dilsel Değişkenler kullanılarak, literatür taraması ve uzman görüşleri sonucuna dayanarak seçilen kriterlerin eşitlik (1) yardımıyla ikili karşılaştırmaları oluşturulmuştur. Köşegen elemanlarda kriterlerin kendileriyle eşit kabul edilmesi sağlanmış ve karşılaştırmalar dilsel ifadeler aracılığıyla Pisagor bulanık sayılara dönüştürülmüştür. Pisagor Bulanık AHP yöntemi kapsamında ikili karşılaştırma matrisi normalize edilmiştir. Pisagor Bulanık AHP yöntemi uygulanarak yapılan hesaplamalar sonucunda kriterlerin nihai ağırlık değerleri elde edilmiştir. Belirlenen bu ağırlıklar ve kriterlerin önem sıralaması Tablo 7'de gösterilmiştir.

Tablo 7: *Pisagor Bulanık AHP ile Ağırlıklandırılmış Kriterler*

Kriter Kodu	**Ağırlık**
K7	0,277
K1	0,162
K8	0,161
K6	0,130
K5	0,128
K3	0,110
K4	0,020
K2	0,012

Pisagor Bulanık AHP yöntemi kullanılarak elde edilen kriter ağırlıkları incelendiğinde, en yüksek önceliğe sahip kriterin Veri Güvenilirliği (K7) olduğu görülmektedir (0,277). Bu sonuç, değerlendirme kapsamında veri doğruluğu ve güvenilirliğinin karar sürecinde belirleyici bir unsur olarak öne çıktığını göstermektedir. Veri Güvenilirliğini sırasıyla Siber Güvenlik (K1) (0,162), Maliyet (K8) (0,161), Ölçeklenebilirlik (K6) (0,130) ve Birlikte Çalışabilirlik (K5) (0,128) kriterleri izlemektedir. Bu bulgu, sistemin güvenlik altyapısının güçlendirilmesi, ekonomik sürdürülebilirliğin sağlanması ve büyüme kapasitesinin desteklenmesi gibi unsurların da karar vericiler açısından önemli olduğunu ortaya koymaktadır. Diğer taraftan, Enerji Verimliliği (K3) kriterinin ağırlığı 0,110 olup orta düzeyde bir öneme sahiptir. Buna karşılık Gerçek Zamanlılık (K4) (0,020) ve Sistem Dayanıklılığı (K2) (0,012)

kriterlerinin en düşük ağırlık değerlerine sahip olduğu belirlenmiştir. Bu durum, ilgili karar problemi kapsamında dayanıklılık ve gerçek zamanlılık unsurlarının diğer kriterlere kıyasla daha düşük öncelikte değerlendirildiğini göstermektedir. Sonuç olarak, Pisagor Bulanık AHP yöntemi ile elde edilen ağırlık dağılımı, karar sürecinde özellikle veri güvenilirliği ve güvenlik temelli kriterlerin ön planda tutulduğunu; ekonomik ve yapısal kriterlerin ise bunu tamamlayıcı bir rol üstlendiğini ortaya koymaktadır.

5.4.2 Şekilleri Biçimlendirme TOPSIS ile Alternatiflerin Sıralanması

TOPSIS yöntemi çerçevesinde uzman görüşleri doğrultusunda oluşturulan karar matrisi Tablo 8'de verilmiştir.

Tablo 8: *Nihai Sıralama Sonuçları*

Alternatifler	İdeal Çözüm Değerleri	Sıralama
Hibrit Kontrol Mimarisi (A3)	0,604	1.Sırada
Bulut Tabanlı Merkezi Sistem (A1)	0,475	2.Sırada
Kenar Bilişim Destekli Sistem (A2)	0,408	3.Sırada

Çalışma kapsamında ele alınan üç farklı alternatifin TOPSIS yöntem adımları izlenerek gerçekleştirilen nihai analiz sonuçları Tablo 8'de sunulmuştur. Elde edilen bulgulara göre Hibrit Kontrol Mimarisi (A3), 0,604 başarı skoru ile tüm alternatifler arasında ilk sırada yer alarak en ideal çözüm olarak belirlenmiştir. A3 alternatifinin pozitif ideal çözüme en yakın, negatif ideal çözümden ise en uzak performansı sergilemesi, sektördeki "uç bilişim" hızı ile "merkezi analitik güç" birleştirme ihtiyacının bir yansımasıdır. İkinci sırada 0,475 başarı skoru ile Bulut Tabanlı Merkezi Sistem (A1) yer almaktadır. A1 alternatifi istatistiksel olarak dengeli bir performans ortaya koymakla birlikte, özellikle gecikme süresi ve veri güvenliği hassasiyeti yüksek olan endüstriyel süreçlerde Hibrit Mimariye (A3) kıyasla daha zayıf kalmıştır. Kenar Bilişim Destekli Sistem (A2) ise 0,408 başarı skoru ile son sırada yer almıştır.

Bu sonuçlar, literatürdeki benzer çalışmalarla karşılaştırıldığında önemli çıkarımlar sunmaktadır. Örneğin, Acarer [6] ve Özdemir [26] tarafından savunulan siber güvenlik ve operasyonel süreklilik odaklı hibrit yaklaşımlar, bu çalışmada uygulanan TOPSIS analizi ile matematiksel olarak doğrulanmıştır. Literatürde genellikle sadece teknik parametreler üzerinden değerlendirilen SFS mimarileri, bu çalışmada Pisagor Bulanık AHP ile karar vericilerin sübjektif belirsizliklerini de kapsayacak şekilde genişletilmiştir. Sektörel açıdan bakıldığında; K7 (Veri Güvenilirliği) ve K1 (Siber Güvenlik) kriterlerinin en yüksek ağırlığa sahip olması, sanayide dijitalleşme süreçlerinde güvenlik kaygılarının hala birincil öncelik olduğunu kanıtlamaktadır. Sonuç olarak, ÇKKV süreci neticesinde sistem gereksinimlerini en yüksek düzeyde karşılayan hem maliyet etkinliği hem de teknik yeterlilik açısından en dengeli performansı gösteren yapının Hibrit Kontrol Mimarisi (A3) olduğu kanıtlanmış ve uygulama için en uygun model olarak önerilmiştir.

6 Sonuçlar

Bu çalışmada, karar verme sürecinin temelini oluşturan kriter ağırlıklarının belirlenmesinde Pisagor Bulanık AHP yöntemi; alternatiflerin bu kriterlere göre sıralanmasında ise TOPSIS yöntemi kullanılmıştır. Analiz sonuçları, Veri Güvenilirliği (0,277) ve Siber Güvenlik (0,162) kriterlerinin toplam ağırlığın büyük bir kısmını oluşturduğunu göstermektedir. Bu hiyerarşi, incelenen sistem yapısı için veri bütünlüğü ve güvenlik unsurlarının; maliyet (0,161) veya operasyonel esneklik gibi faktörlerden daha öncelikli birer stratejik belirleyici olduğunu akademik olarak kanıtlamaktadır. Kriter ağırlıkları temel alınarak gerçekleştirilen TOPSIS analizi sonucunda, Hibrit Kontrol Mimarisi (A3) 0,604 başarı skoruyla en uygun alternatif olarak belirlenmiştir. A3 alternatifi, özellikle veri doğruluğu gereksinimlerinde sergilediği yüksek performans sayesinde; Bulut Tabanlı Merkezi Sistem (0,475) ve

Kenar Bilişim Destekli Sistem (0,408) modellerine kıyasla daha dirençli ve dengeli bir çözüm sunduğunu matematiksel olarak doğrulamaktadır.

Bu çalışma, Siber Fiziksel Sistemlerin (SFS) performans değerlendirmesinde çok kriterli karar verme yöntemlerini entegre ederek uygulayan özgün bir yaklaşım sunmaktadır. Literatürde SFS tasarımları genellikle sınırlı sayıda ölçüt üzerinden değerlendirilirken, bu araştırma veri güvenilirliği ve siber güvenlik gibi kritik unsurları Pisagor Bulanık AHP yöntemiyle nicel bir temele oturtmuştur. Bu yaklaşım, uzman görüşlerindeki belirsizlikleri minimize ederek, literatürdeki kavramsal tartışmaları matematiksel bir karar destek mekanizmasına dönüştürmektedir. Özellikle Hibrit Kontrol Mimarisinin (A3) başarısı, merkezi sistemlerin işlem kapasitesi ile yerel birimlerin çevikliğini sentezlemesinden kaynaklanmaktadır. Bu durum, Türkiye'deki dijital dönüşüm süreçlerinde "tek tip" mimari yerine, güvenlik ve hız dengesini optimize eden hibrit modellerin akademik ve pratik bir gereklilik olduğunu ortaya koymaktadır.

Gelecek çalışmalar için önerilen yapay zekâ entegrasyonu, sadece genel bir iyileştirme aracı olarak değil, önerilen Hibrit Mimari (A3) içerisinde yerel düğümlere yerleştirilecek bir "Anomali Tespit Katmanı" olarak kurgulanmalıdır. Bu teknik yol haritası dahilinde; uç birimlerde çalışan makine öğrenmesi algoritmaları siber tehditleri ilk aşamada sönümlerken, merkezi sistem tarafında yürütülecek sürdürülebilir enerji yönetimi protokolleri sistemin operasyonel ömrünü optimize edecektir. Böylece, önerilen modelin dinamik senaryolarda test edilmesiyle, SFS ekosistemlerinin hem siber güvenliğe hem de enerji verimliliğine aynı anda yanıt veren otonom ve dirençli yapılara dönüştürülmesi hedeflenmektedir.

7 Beyanname

7.1 Rakip Çıkarlar

Bu çalışmada herhangi bir çıkar çatışması yoktur.

7.2 Yazarların Katkıları

Sorumlu Yazar Tamer EREN: Bu çalışmada araştırma konusunun ve yönteminin belirlenmesi, akademik yönlendirmelerin yapılması, son kontrollerin gerçekleştirilmesi ve makalenin nihai hâline getirilmesi süreçlerinde katkıda bulunmuştur.

1. Tutku ÇOŞKUN: Bu araştırmada çalışmanın literatür taramasının gerçekleştirilmesi, makalenin yazımı, verilerin analiz edilmesi ve içerik oluşturulması süreçlerinde aktif rol almışlardır.

2. Esra YOLCU: Bu araştırmada çalışmanın literatür taramasının gerçekleştirilmesi, makalenin yazımı, verilerin analiz edilmesi ve içerik oluşturulması süreçlerinde aktif rol almışlardır.

3. Sıla KUDU: Bu araştırmada çalışmanın literatür taramasının gerçekleştirilmesi, makalenin yazımı, verilerin analiz edilmesi ve içerik oluşturulması süreçlerinde aktif rol almışlardır.

4. Yusuf Bera SANLI: Bu araştırmada çalışmanın yöntemlerinin uygulanmasinda, geliştirilmesi sürecinde kontrol, yönlendirme, düzeltme ve içerik değerlendirme aşamalarında katkı sağlamışlardır.

5. Beyza Nisa ÖZTÜRK: Bu araştırmada çalışmanın yöntemlerinin uygulanmasinda, geliştirilmesi sürecinde kontrol, yönlendirme, düzeltme ve içerik değerlendirme aşamalarında katkı sağlamışlardır.

Kaynakça

Acarer, T. (2020). Ülke güvenliğimizde alınabilecek makro siber güvenlik önlemleri. *Ubgmd*, *6*(2), 61–71. https://doi.org/10.18640/ubgmd.796168

Akaslan, D. (2021). Elektronik sınav sistemlerine yönelik siber saldırılara karşı önleyici yöntemler: LEUKOLION örneği. *İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *3*(2), 178-183. https://doi.org/10.47769/izufbed.858512

Akgül, H., Akgül, B., & Ayer, Z. (2018). Sanayi 4.0 sürecinde gazetecilik sektöründe çalışacak personelin mesleki yetenek ve yeterliliğine yönelik değerlendirme ve öngörüler. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, *5*(8), 198-205.

Altıntaş, S., & Barkuş, F. (2023). Dijital ortamlarda kişisel veri güvenliği kavramı üzerine bir derleme çalışması. *Ejovoc (Electronic Journal of Vocational Colleges)*, *13*(1), 46-69. https://doi.org/10.17339/ejovoc.1311027

Avcı, İ. (2022). Akıllı evlerde IoT teknolojileri ve siber güvenlik. *Avrupa Bilim ve Teknoloji Dergisi*, (34), 226-233. https://doi.org/10.31590/ejosat.1080228

Büyükbingöl, A. (2021). Sosyal Bilimlere Deney Ve Gözlem İmkâni Sunan Bir Yöntem Önerisi: ACP. Uluslararası Sosyal Bilimler Akademi Dergisi, 7, 1500-1539. https://doi.org/10.47994/usbad.1004236

Büyükgöze, H. (2020). Toplum 5.0 ve dijital sağlık. *SDÜ Sağlık Yönetimi Dergisi*, *2*(2), 143-157.

Dicle, A. (2022). Bilgisayar ağlarında gerçekleşen MITM saldırılarına karşı savunma yöntemleri. *Bilişim Teknolojileri Dergisi*, *15*(2), 205-215.

Duran, Z. (2024). Endüstri 5.0'a geçişte siber güvenlik: Yeni sanayileşen ülkeler üzerine bir inceleme. *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, *25*(3), 745-760.

Efe, A. (2021). Yapay zeka odaklı siber risk ve güvenlik yönetimi. *International Journal of Management Information Systems and Computer Science*, *5*(2), 144-165. https://doi.org/10.33461/uybisbbd.972206

Erkul, İ. Ç. (2024). Birleşik Krallık'ın siber güvenlik politikasını güç ve caydırıcılık üzerinden anlamlandırmak. *Journal of Information Systems and Management Research*, *6*(1), 26-39. https://doi.org/10.59940/jismar.1477284

Gedik, Y. (2021). Endüstri 4.0 teknolojilerinin ve endüstri 4.0'ın üretim ve tedarik zinciri kapsamındaki etkileri: Teorik bir çerçeve. *JOEEP: Journal of Emerging Economies and Policy*, *6*(1), 248-264.

Genç, E., & Tunalı, İ. (2022). Endüstri 4.0 ve Lojistik 4.0 kapsamında akıllı depo sistemleri. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, *9*(4), 194-215.

Gençoğlu, M. T. (2022). IPS Sistemlerde Yapay Zekânın Son Beş Yıldaki Gelişimi. *Computer Science*, 211-218.

Göksu, A., & Atay, M. (2018). Yeni ürün geliştirmede Endüstri 4.0 rolü. *2. Uluslararası Multidisipliner Çalışmaları Kongresi Bildiriler Kitabı* içinde

Gürdal Limon, E. (2023). Siber güvenlik açısından savaş yönetim sistemleri ve Türkiye. *Gaziantep Üniversitesi Sosyal Bilimler Dergisi*, *22*(4), 1466-1481. https://doi.org/10.21547/jss.1341594

Karasulu, B. (2019). Çoklu ortam sistemleri için siber güvenlik kapsamında derin öğrenme kullanarak ses sahne ve olaylarının tespiti. *Acta Infologica*, *3*(2), 60-82.

Kaygın, E., Zengin, Y., & Topçuoğlu, E. (2019). Endüstri 4.0'a akademik bakış. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, *33*(4), 1065-1081.

Kiraz, O. Z. (2021). Siber güvenlik bağlamında yeni tehdit algılamalarının Türkiye'nin güvenlik politikalarına etkileri. *Journal of Management Theory and Practices Research*, *2*(2), 69-88.

Kürkcü, S. (2024). Özgürlük ve güvenlik ilişkisi açısından Metaverse: Dijital yaşamın yenilik perspektifi üzerine bir inceleme. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *33*(1), 15-30. https://doi.org/10.35379/cusosbil.1388145

Mandal, T., Sağır, A. B., Öztürk, M. N. A., & Uysal, M. Y. (2022). Metaverse: Sanal dünyadan gerçek gizlilik ve güvenlik problemlerine. *İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *4*(2), 100-106. https://doi.org/10.47769/izufbed.1130284

Özarpa, C., Avcı, İ., & Kınacı, B. F. (2021). Akıllı raylı sistemlerde kullanılan alt sistemlerin kritik seviye analizi. *Demiryolu Mühendisliği*, (14), 143–153. https://doi.org/10.47072/demiryolu.937278

Özdemir, A., & Özgüner, M. (2018). Endüstri 4.0 ve lojistik sektörüne etkileri: Lojistik 4.0. *İşletme ve İktisat Çalışmaları Dergisi*, *6*(4), 39-47. https://doi.org/10.32479/iicd.147

Özdemir, B. (2024). Siber tehdit istihbaratında yapay zeka ve makine öğrenmesi. *Savunma ve Güvenlik Araştırmaları Dergisi*, *1*(1), 75-96.

Özkan, V., & Dinç, A. (2025). Rosgvardiya'nın güvenlik anlayışı ve dijital gözetim: Rusya'da yeni bir toplumsal denetim mekanizması. *Güvenlik Bilimleri Dergisi* (Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı), 310-339. https://doi.org/10.28956/gbd.1674793

Öztürk, H. (2020). *Türkiye'de siber fiziksel sistemler üzerine yapılan akademik çalışmalar: Bibliyometrik bir değerlendirme* [Yüksek lisans tezi]. Yüksek Öğretim Kurulu Ulusal Tez Merkezi.

Sağbaş, M., & Gülseren, A. (2019). Endüstri 4.0 açısından sanayide dijital dönüşüm ve olgunluk seviyesinin ölçümü. *Journal of Life Economics*, *6*(4), 415-430.

Şentürk, G., & Büber, H. (2023). Endüstriyel değişim sürecinin insan kaynakları yönetimi uygulamalarına etkisi üzerine nitel bir çalışma. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, (66), 65-74. https://doi.org/10.18070/erciyesiibd.1297142

Söğüt, E., & Erdem, O. A. (2020). Endüstriyel kontrol sistemlerine (scada) yönelik siber terör saldırı analizi. *Politeknik Dergisi*, *23*(2),557-566

Tuğrul, F. (2022). Personnel Selection Utilizing The Decision Making Mechanism Created With The Intuitionistic Fuzzy Topsis Method. Mugla Journal of Science and Technology, 8(2), 16-21. https://doi.org/10.22531/muglajsci.1158599

Varol, N. (2023). Dijital dönüşüm ve yapay zekâ: Muhasebenin ve denetimin geleceği. *Denetim ve Güvence Hizmetleri Dergisi*, *3*(2), 162-184.

Yüksel, A., Eren, T., & Güven, E. (2024). Siber fiziksel sistemler: Bibliyometrik analiz. *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, *5*(2), 24-35. https://doi.org/10.54047/bibted.1530609

© This study is submitted for submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY 4.0) license (https://creativecommons.org/licenses/by/4.0/)