BULANIK FMEA YÖNTEMİNİ KULLANARAK BİLGİ GÜVENLİĞİNDE RİSK ANALİZİ

RISK ANALYSIS IN INFORMATION SECURITY USING FUZZY FMEA METHOD

YILDIZ MERVE YEŞİLÇİMEN

PROF. DR. ÖZLEM MÜGE TESTİK

Tez Danışmanı

Hacettepe Üniversitesi

Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin

Endüstri Mühendisliği Anabilim Dalı için Öngördüğü

YÜKSEK LİSANS TEZİ olarak hazırlanmıştır.

2024

Tezimi, hayatım boyunca hep destekçim olan sevgili anneciğime, babacığıma ve her daim yolumu aydınlatan ağabeyime ve hep kalbimde olacak olan çok sevdiğim dedeciğime ithaf ediyorum.

ÖZET

BULANIK FMEA YÖNTEMİNİ KULLANARAK BİLGİ GÜVENLİĞİNDE RİSK ANALİZİ

Yıldız Merve YEŞİLÇİMEN

Yüksek Lisans, Endüstri Mühendisliği Bölümü

Tez Danışmanı: Prof. Dr. Özlem Müge TESTİK

Ocak 2024, 70 sayfa

İnternet ve bilişim teknolojilerinin hızlı evrimi ve yaygın kullanımı, kurumların iş süreçlerini desteklemek amacıyla bilişim sistemlerine olan bağımlılıklarını artırmıştır. Bu bağımlılık, çeşitli sektörlerde faaliyet gösteren kurumların günlük operasyonlarını sürdürebilme ve rekabet avantajı elde etme noktasında kritik bir unsurdur. Ancak, aynı zamanda da kurumları, bilgi teknolojisi sistemlerine yönelik potansiyel tehditlere karşı daha savunmasız hale getirmektedir. Bu tehditler, veri kaybına neden olarak iş sürekliliğini olumsuz etkileyebilmektedir. Kurumların, bilgi varlıklarını etkili bir şekilde korumak için güvenlik önlemleri ve risk yönetimi stratejileri geliştirmeleri gerekmektedir. Alınan önlemler, bilgi güvenliği açıklıklarından kaynaklanan potansiyel kayıpları minimize ederek kurumların maliyetlerine olumlu bir etki sağlamakta, böylece şeffaf ve güvenilir kurum imajı desteklenmiş olmaktadır.

Bilgi güvenliği risk yönetiminde, potansiyel başarısızlıkları en aza indirmek için bu tez çalışması Hata Modu ve Etkileri Analizi (Failure Mode and Effect Analysis-FMEA) yöntemini bulanık yaklaşımla birlikte sunmaktadır. Bulanık FMEA yöntemi, klasik

FMEA'nın kapsam ve esnekliğini artırdığından riskleri değerlendirmede daha pratik, etkili ve kullanışlı olması nedeniyle tercih edilmiştir.

Çalışma kapsamında, bir kurumda taşınabilir ortam ve cihazlara ait bilgi güvenliğinin; gizlilik, bütünlük ve erişilebilirlik olarak tanımlanan üç temel unsurundan herhangi birinde veya birkaçında oluşabilecek risklerin belirlenmesi ve bu risklerin önlenmesi için öneriler getirilmesi amaçlanmaktadır. Risklerinin mümkünse ortadan kaldırılması, değilse etkisinin düşürülmesini hedeflenmektedir.

Bulanık FMEA yöntemi için yedi kişilik bilgi güvenliği alanında uzman bir ekiple çalışılmıştır. Uzmanlar, ISO/IEC 27001 BGYS ekibinde de aktif görev almaktadır. Çalışmada belirlenen hata modları için Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanmış olan Bilgi ve İletişim Güvenliği Rehberi'nde 6 ana varlık grubundan biri olarak yer alan 'Taşınabilir Cihaz ve Ortam Güvenliği' başlığındaki tedbir maddelerinden yararlanılmıştır. Çalışma yapılan kurumda yer alan taşınabilir cihaz ve ortamlara ilişkin 21 adet hata modu belirlenmiş ve uzmanlardan bu hata modlarının; olasılık, şiddet ve tespit edilebilirliklerinin 10 farklı dilsel değişken yardımıyla değerlendirilmeleri istenmiştir. Aykırı değerlerin değerlendirmeye alınmaması için her bir parametre için medyan üzerinden hesaplamalar yapılmıştır. Elde edilen verilerle klasik ve bulanık FMEA karşılaştırılması yapılmış, iki yöntem arasında güçlü bir ilişki olduğu sonucuna varılmıştır.

Anahtar Kelimeler: Bilgi Güvenliği, Risk Analizi, FMEA, Bulanık FMEA

ABSTRACT

RISK ANALYSIS IN INFORMATION SECURITY USING FUZZY FMEA METHOD

Yıldız Merve YEŞİLÇİMEN

Master of Science, Department of Industrial Engineering

Supervisor: Prof. Dr. Özlem Müge TESTİK

January 2024, 70 pages

The rapid development and widespread use of the Internet and information technologies have increased the dependence of organizations on information systems to support their business processes. This dependency is a critical element for organizations in various industries to sustain their daily operations and gain competitive advantage. However, it also makes organizations more vulnerable to potential threats to their information technology systems. These threats can cause data loss and negatively impact business continuity. Organizations must develop security measures and risk management strategies to effectively protect their information assets. The measures taken will have a positive impact on the cost of the organization by minimizing potential losses due to information security vulnerabilities, thus supporting the image of a transparent and reliable organization.

In order to minimize potential failures in information security risk management, this thesis presents the Failure Mode and Effect Analysis (FMEA) method with a fuzzy approach. The fuzzy FMEA method is preferred because it is more practical, effective

and useful in assessing risks, as it increases the scope and flexibility of the classical FMEA.

This study analyzes the information security of portable media and devices in an organization in terms of one or more of the three basic elements defined as confidentiality, integrity and availability with the goal of eliminating the risks if possible and reducing their impact if not.

The Fuzzy FMEA method was developed with a team of seven information security experts. The experts are also actively involved in the ISO/IEC 27001 ISMS team. For the failure modes identified in the study, the precautionary items under the title of Mobile Device and Environment Security, which is one of the 6 main asset groups in the Digital Transformation Office of the Presidency of the Republic of Turkey Information and Communication Security Guide, were used. The experts were asked to rate the occurence, severity and detectability of these failure modes using 10 different linguistic variables. The median was calculated for each parameter to exclude outliers from the evaluation. A comparison of traditional and fuzzy FMEA was made with the resulting data and it was concluded that there was a strong relationship between the two methods.

Keywords: Information Security, Risk Analyses, FMEA, Fuzzy FMEA

TEŞEKKÜR

Değerli tez danışmanım Sayın Prof. Dr. Özlem Müge Testik'e; sürecin en başından itibaren motive edici geri bildirimleri sayesinde çalışmama olan inancımı her daim canlı tutmamı sağladığı için ve verdiği değer, gösterdiği sonsuz anlayış ve sunduğu teşvik için minnettarım. Rehberliği ve desteği için teşekkürlerimi sunuyorum.

Çalışmamda yer alan bilgi güvenliği uzmanlarının her birine ve değerli bilgilerini benimle paylaşan, sorularımı hiçbir zaman yanıtsız bırakmayan tüm çalışma arkadaşlarıma, uzmanlarımıza, koordinatörümüze ve daire başkanımıza destekleri ve içten yardımları için en içten teşekkürlerimi sunuyorum.

Ve son olarak çok değerli anneciğim, babacığım, ağabeyim her zaman yanımda olduğunuz, beni cesaretlendirdiğiniz ve sonsuz sevginiz için teşekkürlerin en büyüğünü sizlere ediyorum, iyi ki varsınız.

İÇİNDEKİLER

ŞEKİLLER

ÇİZELGELER

SİMGELER VE KISALTMALAR

Simgeler

a	Bulanık sayı alt sınır değeri
b	Bulanık sayı orta değeri
c	Bulanık sayı üst sınır değeri
D	Tespit Edilebilirlik
O	Olasılık
S	Şiddet
μ	Üyelik fonksiyonu

Kısaltmalar

AHP	Analitik Hiyerarşik Proses
BÇS	Bulanık Çıkarım Sistemi
BG	Bilgi Güvenliği (IS)
BGYS	Bilgi Güvenliği Yönetim Sistemi (ISMS)
BS	Bilgi Sistemleri
BT	Bilgi Teknolojileri (IT)
CBDDO	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
CIA	Gizlilik, Bütünlük, Erişilebilirlik
DoS	Hizmet Reddi
ERP	Kurumsal Kaynak Planlaması
ETA	Olay Ağacı Analizi
FE	Hata Etkisi
FM	Hata Modu
FMEA	Hata Modu ve Etkileri Analizi
FMECA	Hata Modu Etkileri ve Kritiklik Analizi
FTA	Hata Ağacı Analizi
IEC	Uluslararası Elektroteknik Komisyonu
ISO	Uluslararası Standardizasyon Kuruluşu

ISRA	Bilgi Güvenliği Risk Analizi
ISRAM	Bilgi Güvenliği Risk Analizi Yöntemi
MCDM	Çok Kriterli Karar Verme
PC	Kişisel Bilgisayar
RPN	Risk Öncelik Sayısı (RÖS)
TOPSIS	İdeal Çözüme Benzerliğe Göre Sıralama Tercihi Tekniği

1. GİRİŞ

Bilgi sistemlerine yönelik saldırılar artık yeni dijital çağda iş yapmanın bir parçası olarak kabul edilmektedir (Bidgoli, 2006). Kurumlar genellikle müşteri bilgileri, finansal bilgiler, ticari sırlar ve diğer hassas verileri barındırmaktadır. Taşınabilir cihazlar, bu tür bilgileri içerdiği için, bu verilerin yetkisiz erişimden, kaybolmaktan veya çalınmaktan korunması kritik öneme sahip olmaktadır. Taşınabilir cihazların bilgi güvenliği, kurumların sürdürülebilirliği, rekabet avantajlarını koruma, yasal uyumluluk ve itibarlarını korumaları açısından oldukça önemlidir. Özellikle devlet düzeyinde, stratejik bilgilerin korunması ulusal güvenlik açısından da kritik olmaktadır. Bilginin korunması sadece bireylerin ve kurumların çıkarları için değil, aynı zamanda toplumun genel güvenliği ve istikrarı için de belirleyicidir. Bilgi güvenliği önlemleri, her düzeyde bilgiye erişimi kontrol etmeyi, veri bütünlüğünü korumayı ve bilginin yetkisiz kişilerin eline geçmesini önlemeyi amaçlamaktadır.

Risk, her zaman işletmelerin doğasında bulunmaktadır. Bilgi güvenliği riskleri de bu genel risk kategorisine dâhildir. Riskler, kabul edilmeli ve yönetilmeli, güvenlik kontrolleri etkin bir şekilde uygulanmalıdır. Riskleri kabul edilebilir bir seviyeye indirgemek için çok sayıda strateji ve güvenlik kontrolü bulunmaktadır (Bidgoli, 2006). Sonuç olarak bilgi güvenliği risklerinin varlığı kabul edilmelidir ve bu riskleri etkili bir şekilde yönetmek ve sürekli olarak güvenlik önlemlerini güncellemek için aktif bir yaklaşım benimsenmelidir.

Bilgi güvenliğinde risk analizinin amacı; bilgi teknolojileri kaynaklarını, potansiyel ihlallerin zarar derecelerine göre önceliklendirilmesi yoluyla optimize etmektir (Shaikh ve Siponen 2023).

Geçmişte yüksek güvenilirlik sağlamak için test ve analize odaklanmak yeterli olsa da bu, günümüzde yeterli olmamaktadır. Çünkü test ve analiz süre ve maliyetleri oldukça yüksektir. Süre ve maliyetlerin kısıtlı olduğu durumlarda geliştirmenin erken safhalarında yüksek kalite ve güvenilirlik sağlanmalıdır. Tam da bu aşamada hataların öngörülebilmesi ve önlenebilmesi için FMEA (Failure Mode and Effect Analysis /Hata Modu ve Etkileri Analizi) oldukça işlevsel ve günümüzde süreçler ve ürünler için en bilinen analiz araçlarından biri olmaktadır (Yang ve ark., 2008; Carlson, 2012).

Bilgi teknolojilerinin çeşitlenmesiyle birlikte potansiyel riskler de sürekli artmaktadır. Kurumlar, potansiyel risklerin belirlenerek önlenebilmesi ya da etkisinin minimize

edilebilmesi için risk analiz çalışmalarına ağırlık vermektedir. Bilgi güvenliğinde yapılan risk analiz çalışmalarında FMEA yöntemi kullanılması ile etkili bir sonuç alınacağı düşünülmektedir.

Bilgi güvenliği alanında, riskler genellikle belirsizlik içermektedir. Bu riskleri, uzmanların bilgi, deneyimi ve yorumlamaları sayesinde daha iyi anlamak ve değerlendirmek için çalışmada, belirsiz durumlarda kullanıldığında anlamlı sonuçlar verebilen bulanık FMEA yönteminden yararlanılmıştır. Bulanık FMEA, klasik FMEA yöntemini bulanık mantık ile birleştirerek, bilgi güvenliği risklerini daha etkili bir şekilde değerlendirmek için kullanılan bir yöntem olarak karşımıza çıkmaktadır.

2. LİTERATÜR ÖZETİ

2.1. FMEA

Chiozza ve Ponzetti (2009), tıbbi hataları azaltmaya ve hasta güvenliğini artırmaya yönelik bir FMEA modeli önermektedirler. Çalışmada, laboratuar ortamlarında, yüksek risk içeren durumlarda risklerin ortadan kaldırılması ya da etkisinin azaltılması amacıyla ISO tarafından da önerilen FMEA risk analizi yapılmıştır. Laboratuar ortamlarında, hasta bakımının tüm sürecinde ölçüm ve karşılaştırmalar yapılırken, hasta güvenliğinin artırılması ve maliyet tasarrufunun sağlanması istenilmektedir. Küçük bir hastanede yapılan uygulama sonucunda bu amaca ulaşıldığı gözlenmiştir.

Kim ve ark. (2013), akıllı telefonlarda yazılım güvenliği analizi için FMEA ve Hata Ağacı Analizini birlikte kullanmışlardır. Akıllı telefonlardaki hata modlarının, güvenlik sistemi yazılımıyla ilgili olduğu öne sürülerek, bu bütünleşik yaklaşım ile hataların azaltılması ve kategorize edilmesinin sağlanması ve zayıf güvenlik ağların azaltılması amaçlanmıştır. Çalışmada, akıllı telefon kullanıcılarının kamuya açık web sitelerinde iki yıl boyunca kaydedilen verileri kullanılmıştır. Sonuçta, bu iki metodun entegre kullanımının, güvenlik sistemleri tekniğiyle aralarında güçlü bir ilişki olduğu iddia edilmektedir.

Schmittner ve ark. (2014), çalışmalarında yeni yaklaşım olarak temel FMEA'dan bilinen hata nedeni, hata modu ve hata etkisi modelini kullanarak birleşik bir neden-sonuç modeli kullanmışlardır. Klasik FMEA kapsamı, güvenlik açıklarını ve güvenliğe yönelik saldırıları kapsayacak şekilde genişletilmiştir. Model, daha sonra bir endüstriyel ölçüm sistemine uygulanmıştır. Yöntemin, sistemin erken tasarım aşamalarında analizi için en uygun yöntemlerden biri olduğu sonucuna varılmıştır.

Silva ve ark. (2016), çalışmalarında büyük veri sürecinin önemli aşamalarında risk değerlendirmesine izin veren FMEA ve Gri Teoriyi kullanmayı önermişlerdir. Makale, FMEA ve Gri Teoriyi kullanarak güvenlik açıklarının yaygın hale gelmesi ile ilişkili belirsizlik ve riskleri tanımlayarak büyük verinin farklı özelliklerinin bilgi güvenliği riskleri ile bağlantısına ait çeşitli görüşler sunmaktadır. Önerinin pratikte uygulanabilirliğini göstermek için uzman bilgisine dayalı gerçekçi veriler içeren sayısal bir örnekte uygulama yapılmıştır. Bu örnekte; tanımlama ve erişimi yönetme, cihazı ve uygulamayı kaydetme, altyapıyı yönetme ve veri yönetimini ve büyük verilerin güvenlik açıklarıyla ilgili 20 hata modu analiz edilmiştir. Sonuçta; veri yönetiminin büyük veri riskinin en önemli yönü olduğu gösterilmiştir.

2.2. Bulanık Risk Analizi ve Bulanık FMEA

Bowles ve Pelaez, (1995), Hata Modu Etkileri Kritiklik Analizinde (FMECA) bulanık mantık temelli yeni bir teknik sunmaktadır. Düzeltici faaliyetler için hataların önceliklendirilmesinde; klasik kritiklik analizindeki gibi hata modunun olasılığı, şiddeti ve tespit edilebilirliği kullanılmaktadır. Ancak, bu parametreler çalışmada bir bulanık kümenin üyeleri olarak temsil edilmekte, kural tabanlı bir sistem ile birleştirilmekte, min-max çıkarımı ile değerlendirilmekte ve ardından hatanın riskliliğini değerlendirmek için bulanıklaştırılmaktadır.

Bu yaklaşım sayesinde geleneksel yöntemlere göre çeşitli avantajlar sağlanmaktadır:

1. Kritiklik değerlendirilmesinde kullanılan dilsel terimlerle doğrudan hata modları ile ilişkili riskin tanımlanması olanağı bulunmaktadır.
2. Nicel veriler ile değerlendirme yapılmasının yanı sıra belirsizlik içeren bilgiler de tutarlı bir şekilde ele alınmaktadır.
3. Olasılık, şiddet ve tespit edilebilirlik parametrelerinin birleştirilmesi için daha esnek bir yapı sağlanmaktadır.

Kritikliğin değerlendirilmesi aşamasında bulanık mantık temelli iki yaklaşım sunulmaktadır: İlki, kullanıcıdan alınan veya güvenilirlik analizinden elde edilen net girdileri kullanan klasik Risk Öncelik Sayısı (Risk Priority Number-RPN) hesaplamasıdır. İkinci yöntem ise daha az bilginin olması durumunda bulanık girdiler kullanmaktadır. Bu, tasarım süreçlerinde ilk aşamalarda kullanılabilen bir yöntemdir. İkinci yöntemde, RPN hesabında tanımlanan dilsel değişkenler doğrudan kullanılmaktadır. Bulanık mantık, FMECA'da tanımlı arızaları önceliklendirmek için tasarım süreci boyunca kullanılabilecek bir araçtır. Sonuç olarak, mevcut bilgiler belirsiz, muğlak, nitel veya kesin olmasa bile, tasarım aşamasında bir arızanın etkilerini düzeltmek veya hafifletmek için uygun eylemlerin önceliklendirilmesine olanak tanımaktadır.

Xu ve ark. (2002), FMEA'nın bulanık değerlendirmesini motor turboşarj sistemleri için yapmışlardır. Prototip değerlendirme uzman sistemi ve bulanık mantık tabanlı bir FMEA tekniği geliştirmişlerdir. Klasik FMEA metodolojisi ile karşılaştırıldığında, çalışmada özetlenen bulanık çıkarım tekniği sayesinde çeşitli avantajlar sağlanmıştır. Örneğin; FMEA ile ilgili tüm bilgiler net girdiler yerine, insan iletişimine ve uzman deneyimine dayalı doğal dilsel değişkenlerle tanımlandığından gerçek durum daha esnek bir şekilde yansıtılmaktadır. Bulanık mantık net olmayan verilerin kullanılmasına olanak tanıdığından bileşenlerin ve sistemin çeşitli durumlarını kolayca işleyebilmektedir. Ayrıca, bir arada kullanılacak fikirlerin tamamen bağımsızlığı gibi bir varsayım bulunmamaktadır. Arıza modlarıyla etkileri arasında karşılıklı

bağımlılıklar mümkün olabilir. FMEA için de bu önemli olmaktadır. Çalışma sonucunda, hata modlarının en şiddetli etkisine karşı cevap verebilecek iki aşamalı çıkarım modülü geliştirmişlerdir. Geliştirilen uzman değerlendirme sistemi sayesinde mühendisleri bilgi birikimi ve uzmanlığı FMEA sürecine tam olarak dâhil edilmektedir. Bu da ciddi oranda maliyet tasarrufu sağlamaktadır.

Alizadeh ve ark. (2022), bir belediye atık su tesisindeki riskleri değerlendirmek ve önceliklendirmek için FMEA ve bulanık FMEA yöntemlerini kullanmışlardır. Önce, 5 uzman ile klasik RPN hesaplaması ile FMEA yapılmış daha sonra olasılık, şiddet ve tespit edilebilirlik değerleri bulanıklaştırılarak, uzman görüşlerinden de yararlanarak bulanık kural tabanı oluşturulmuş ve bulanık FMEA yapılmıştır. 53 hata modu üzerinde çalışılmış ve klasik FMEA ile 53 hata modundan 51'i düşük risk düzeyinde çıkarken 2'si orta risk düzeyinde sonucu çıkmıştır. Ancak buna karşılık uzman görüş ve önerilerinden yararlanılan bulanık FMEA'da 5 hata modu düşük risk düzeyinde, 43 hata modu orta risk düzeyinde ve 5 hata modu da yüksek risk düzeyinde çıkmıştır. Yani bulanık FMEA ile yüksek risk içermediği düşünülen hata modlarının yüksek risk içerdiği anlaşılmıştır. Sonuçta, bulanık FMEA sayesinde risklerin daha iyi önceliklendirildiği ve klasik FMEA'nın dezavantajlarının giderildiği görülmüştür.

2.2.1. Bilgi Teknolojileri ve Bilgi Güvenliğinde Bulanık FMEA

Silva ve ark. (2014), bilgi teknolojisi sistemlerine yönelik saldırılarda oluşabilecek potansiyel veri kayıpları ve veri değişimlerini en aza indirmek için risk analizi yapmışlardır. FMEA ve bulanık teori kullanarak bilgi güvenliği risk yönetimine çok boyutlu bir yaklaşım getirmişlerdir. Bu yaklaşımda; bilgi ve sistemlere erişim, iletişim güvenliği, altyapı, güvenlik yönetimi ve güvenli bilgi sistemleri geliştirme olmak üzere bilgi güvenliği risklerinin beş boyutunu analiz etmişlerdir. Bir kuruluşa ait sistemlerde güvenlik açıklıklarına sebebiyet veren bilgi güvenliği programlarının kritik yönlerinin ve eksikliklerinin anlaşılması için bu çalışma yapılmıştır. Kurulan model bir üniversite araştırma grubu üzerinde değerlendirilmiş ve yapılan bilgi güvenliği risklerinin en önemli boyutunun iletişim güvenliği olduğu sonucuna varılmış ve bunu altyapının izlediği görülmüştür.

Li ve ark. (2018), akıllı şehir sisteminde bilgi güvenliği riskini bulanık ve gri FMEA kullanarak incelemişlerdir. Akıllı şehrin bilgi güvenliğinin beş boyutu analiz edilmiş ve riskleri değerlendirilmiştir. Her boyut için de alt hata türleri bulunmaktadır. Sonuçta, en yüksek risk akıllı altyapı boyutunun doğal, yapay ve fiziksel tehditleri olarak belirlenmiştir. İkinci olarak ise bilgi güvenliğinde eğitim ve bilgi eksikliği gelmektedir. Değerlendirme sonucuna göre akıllı

şehrin bilgi güvenliğini sağlamak için öneriler sunulmuştur. Bu önerilerden bazıları; veri işleme ve filtreleme için bilgi sisteminin iyileştirilmesi, şehirdekilere bilgi güvenliği eğitimi verilmesi, bilgi güvenliği politikalarının uygulanması, akıllı şehirler için bir ulusal bilgi güvenliği sistemi kurulması olarak verilmiştir.

Ershadi (2019), bilgi güvenliği risk yönetiminde karma bir yaklaşım kullanmıştır. Bu karma yaklaşımda; yazılım, iletişim ve insan kaynakları gibi farklı alanlardaki riskler ele alınmıştır. Çalışmanın amacı riskleri belirledikten sonra verimli, etkili ve düzeltici faaliyetlerde bulunmaktır. Bu çalışmada, bilgi güvenliğinin potansiyel riskleri için FMEA kullanılmıştır. Ayrıca ek olarak MCDM yöntemlerinden AHP, TOPSIS ve Shannon Entropi yöntemleriyle karma yaklaşım kullanılmıştır. Öncesinde, bulanık FMEA ile potansiyel hata etkileri tanımlanmış, daha sonra klasik FMEA'nın eksiklerini gidermek için MCDM metotları kullanılmıştır. En önemli risk, depolanan verilerin yetkisiz olarak görüntülenmesi ve değiştirilmesi olarak belirlenmiştir. Bilginin gizliliğinin en önemli bilgi güvenliği kriteri olduğu sonucuna varılmıştır.

Gusmão ve ark. (2016), bulanık karar teorisini kullanan bilgi güvenliği risk analizi modeli geliştirmişlerdir. Makalede, bilgi teknolojisi sistemlerinin kötüye kullanılmasına karşılık gelen başlatıcı bir olayın meydana gelmesinin ardından olası bir kaza senaryosunda, alternatif olarak adlandırılan olay dizisini tanımlayan ve değerlendiren, bilgi güvenliği değerlendirmesi için bir risk analizi modeli önermektedir. Bu değerlendirmeyi gerçekleştirmek için çalışmada, Olay Ağacı Analizi bulanık karar teorisi ile kullanılmıştır. Önerilen modelin katkıları: Olay ve senaryo sınıflandırmasının geliştirilmesi, finansal kayıpların dikkate alınmasıyla riskin kritikliğine göre alternatiflerin sıralanması ve son olarak en yüksek düzeyde bilgi sistemi saldırılarının nedenlerine ilişkin bilgi sağlanması olarak sıralanmaktadır. Model uygulanabilirliği testi için bir veri merkezi örneği kullanılmıştır. Olayların gerçekleşme olasılıklarını belirlemeye yönelik iki farklı yöntem göz önünde bulundurularak on iki alternatif analiz edilmiştir. Veri merkezi saldırısına yönelik olay ağacı analizinde; veri merkezi saldırıları önce içeriden /dışarıdan erişim olarak iki dala ayrılmış daha sonra da kendi içlerinde her biri kasıtlı/kasıtsız saldırılar olmak üzere tekrar dallara ayrılmıştır. Çalışma sonucunda en riskli alternatifin kasıtlı dış veri tabanı hizmetleri saldırısı olduğu çıkarılmıştır.

Gusmão ve ark. (2018), Hata Ağacı Analizi ve bulanık karar teorisini kullanan siber güvenlik risk analizi modeli çalışması yapmışlardır. Bu makale, Gusmão ve ark. (2016), tarafından yürütülen ve siber güvenlik risk analizinin yapıldığı çalışmadan türetilen araştırmayı genişletmektedir. Siber saldırıların önlenmesine yönelik başarısızlıkların ve siber güvenlik

sistemlerindeki güvenlik açıklarının tespiti için hata ağacı analizi, karar teorisi ve bulanık teoriyi birleştiren bir model önermektedirler. Siber saldırı senaryolarının sebepleri karakterize etmek için FTA'yı kullanırken, finansal kayıp risklerini ve restorasyon süresinin analizini göz önüne alarak siber saldırı senaryolarını ölçmek için bulanık teoriyi kullanmaktadırlar. Bir web sitesine, e-ticarete ve kurumsal kaynak planlamasına (ERP) yönelik saldırılara karşı model geliştirilmiş, bu üç alternatife bir saldırı olması durumunda riskleri ve sonuçlarını değerlendirmek için model uygulanmıştır. Seri yayma, veri değiştirme, veri kaybı veya imhası ve hizmet kesintisi sonuçları ve hem finansal maliyetler hem de restorasyon süresi açısından değerlendirilmiştir. Model uygulaması sonuçlarına göre kullanıcıların kimlik doğrulama sorunları nedeniyle e-ticaretin, web siteleri ya da ERP'ye göre daha hassas olduğu ortaya konulmuştur.

2.3. Bilgi Güvenliğinde Risk Analizi

Karabacak ve Soğukpınar (2005), bilgi güvenliğinde risk analizi için Bilgi Güvenliği Risk Analizi Yöntemi (ISRAM) adı verilen bir yöntem önermektedir. Yöntem, bilgi güvenliği risklerini analiz etmek için nicel bir yaklaşım kullanmaktadır. Yedi adımdan oluşan yöntemde, bilgi sistemlerindeki risklerin analizi için yöneticiler ve personellerin ortak katılımıyla anket çalışması kullanılmaktadır. Anket sonrasında Arena simülasyon yazılımıyla bir risk modeli için benzetim çalışması yapılmıştır. ISRAM'ı diğer risk analiz yöntemlerinden ayıran en büyük avantajı kullanımındaki kolaylığıdır. Yöntem, anket çalışması, risk tabloları ve basit matematiksel işlemler içermektedir. Sonuçta ise, yönetici ve çalışanların ortak katılımıyla yapılan bu çalışmanın kısıtlı bir zaman dilimi için tutarlı sonuçlar verdiği görülmüştür.

Shaikh ve Siponen (2023), siber güvenlik ihlallerini takiben bilgi güvenliğinde risk analizi çalışmasında üst yönetimin gösterdiği ilginin aracılık rolü üzerine bir çalışma yapmıştır. Çalışma, siber güvenlik ihlalleri üzerine yapılan yönetimsel müdahalelerin genellikle müşteri telafisi ve kriz yönetimine odaklandığını ancak firmanın içindeki ihlallerin sistematik sorunlara işaret edebileceğini vurgulamaktadır. Sadece teknik düzeltmeler ve kontrollerle sınırlı bir müdahale, gelecekteki siber güvenliği sağlamak adına diğer yönetimsel eylemleri kısıtlayabilmektedir. Bu bağlamda, bilgi güvenliği risk değerlendirmeleri (ISRA) önemli bir rol oynamakta ve bir ihlalin ardından diğer güvenlik açıklarının tespitine yardımcı olabilmektedir. Çalışma, dikkat temelli bir perspektifle, yüksek ihlal maliyetlerinin üst yönetim ekibinin siber güvenliğe daha fazla dikkat etmesine ve ISRA gerçekleştirme olasılığını artırmasını sağlayacağını öne sürmektedir. Analiz sonuçları, siber güvenliğe olan ilginin, ihlal maliyetleri

ile ISRA gerçekleştirme kararı arasındaki ilişkiye kısmen aracılık ettiğini göstermektedir. Bu bulgular, siber güvenlik yönetiminin etkili bir şekilde gerçekleştirilmesi için üst yönetimin iş birliğinin önemini vurgulamaktadır.

2.3.1. Mobil Cihazlara Yönelik Risk Analizi

Ledermüller ve Clarke (2011), çalışmalarında mobil cihazların daha verimli çalışmasını sağlayan bir metodoloji geliştirmeyi amaçlamaktadır. Çalışmanın amacı, farklı bilgi düzeylerine sahip mobil cihaz kullanıcılarının, kullandıkları cihazlara yönelik riskleri anlamaları ve değerlendirmeleri için bir metodoloji sunmaktır. Bu yaklaşım, kullanıcıları riskler hakkında bilgilendirmek için bir mekanizma sağlamanın yanı sıra, bireysel uygulama ve hizmet kullanımına ilişkin ayrıntılı risk bilgileri de sağlamaktadır. Metodoloji kapsamında risk; varlığın değeri, tehditler ve kırılganlığının çarpımından hesaplanmaktadır. Varlığın değeri çeşitli boyutlardan kaynaklanabilmektedir. Bu değerin para olarak tahmin edilebileceği gibi aynı zamanda CIA (gizlilik, bütünlük, erişilebilirlik) olabileceği de tahmin edilebilmektedir. Yapılan risk analizi çalışması; varlık değeri kategorilerinin değerlendirilmesi, tek bir varlık değerinin hesaplanması, tehditlerin değerlendirilmesi, tek bir tehdit değerinin hesaplanması, güvenlik açığı sorularının yanıtlanması ve son olarak risk seviyesinin hesaplanması olmak üzere 6 adımdan oluşmaktadır. Varlıklar; kurumsal e-posta, kişisel e-posta, elektronik bankacılık, e-sağlık, kurumsal uzaktan erişim, kişisel uzaktan erişim, harita, navigasyon vb. kategorilere ayrılmıştır. Analiz sonucunda en yüksek risk puanlarının kurumsal e-posta ve e-sağlık uygulamasına ait olduğu sonucuna varılmıştır.

3. BİLGİ GÜVENLİĞİ

Bilgi, günümüz modern zamanında kurumsal bir kaynak olarak yeni bir statü ve değer elde etmiştir. Son yıllarda bilginin yükselişi, telekomünikasyon ve bilgi teknolojilerinin gelişmesi ile büyük bir ivme kazanmıştır. Çoğu kuruluş artık benzeri görülmemiş ölçekte fırsatlar, tehditler ve değişimle karşı karşıyadır ve bu koşullarla başa çıkabilmek için güvenilir, hızlı ve doğru bilgi şarttır (Kaye, 1995).

Bilgi güvenliği, iş sürekliliğini verimli olarak sürdürebilmek için bilginin her türlü risklerden korunması olarak tanımlanabilir (ISO, 2005). Fiziksel ve mantıksal veri erişim kontrollerini kapsamaktadır ve bilgi varlıklarının imha edilmesini, ifşa edilmesini, kaybedilmesini, hasara uğramasını veya yanlış kullanılmasını önlemeyi amaçlamaktadır.

Kuruluşun bilgi güvenliği risklerine açık olması, onun bilgi teknolojilerine bağımlılığı ile orantılıdır. Modern yaşamın hemen her alanında ihtiyaç haline gelen bilgisayarlar; ekonomik, sosyal, profesyonel hayatımızın ayrılmaz bir parçasıdır. Bilgisayar teknolojisi günümüzde; genetik mühendisliği, evren, yapay zekâ gibi alanlarda büyük potansiyel sunmaktadır. Ancak aynı zamanda bilgisayar tabanlı sistemler ve ağlar çoğu zaman kötü niyetli kişilerin kurbanı olmaktadır. Bu tür kasıtlı tehditlerin yanı sıra kasıtsız eylemler de ilgili bilgilerin kaybolmasına veya bozulmasına neden olabilmektedir (Bosworth ve Kabay, 2002). Bu nedenle, bilgi güvenliğini tehdit eden risklerin yönetilmesi gerekmektedir (Sumner, 2009). Bilgi güvenliğinin yönetilmesi; teknolojiye, proseslere ve insanlara bağlıdır. Bilgiye ait riskler sınırsızdır ve bu yönüyle diğer risklerden farklıdır (Anderson, 2003; Ashenden, 2008).

3.1. Bilgi Güvenliğinin Unsurları

Bilgi güvenliğinin üç temel unsuru olarak tanımlanan 'Gizlilik', 'Bütünlük' ve 'Erişilebilirlik' terimleri akademik literatürde ve bilgi güvenliğine yönelik uygulamalarda yaygın olarak kullanılmaktadır. Söz konusu unsurlar Şekil 3.1'de görsel olarak sunulmuştur.

Bu üç unsur sıklıkla 'CIA üçlüsü' olarak anılmaktadır. Bilgi güvenliği bu üç temel özelliğiyle tanımlansa da hiçbir zaman genel kabul olarak 'Bilgi Güvenliği = CIA' anlamına gelir denilemez (Anderson, 2003). CIA üçlüsü, günümüzde güvenliğin çok daha geniş kapsamlı operasyonel ve sosyal yönlerinin dikkate alınması gerektiği durumlarda yetersiz kaldığı için birçok kez eleştirilmiştir (Anderson, 2003; Dhillon ve Backhouse, 2000).

Bununla birlikte, CIA üçlüsünün özellikleri, bilgi güvenliğine dair sorunları ele almak için basit bir yol sunduğundan hala değer görmektedir. Bu nedenle de akademik literatür, CIA üçlüsünü kullanımda tutmakta ve çeşitli güncellemeler getirmeye çalışmaktadır (Samonas ve Coss, 2014). Örneğin; Whitman ve Mattord'a göre CIA üçgenine, doğruluk, özgünlük ve fayda karakteristikleri de eklenmelidir (Whitman ve Mattord, 2009).

Şekil 3.1. Bilgi Güvenliği Üçgeni (CIA)

Uluslararası Standardizasyon Kuruluşu (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) tarafından yayımlanan bilgi güvenliği standardına (ISO/IEC 27002:2005) göre bilgi güvenliği bilginin; gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması olarak tanımlanmaktadır (ISO/IEC 27002:2005).

Gizlilik, bilginin yetkisiz kişilerce okunmasını önlemekle ilgilidir. Örneğin bir banka müşterisi, kendi tasarruf hesabında ne kadar para olduğunun bilgisinin yetkisiz kişilerce bilinmesini istemez. Böyle bir durumun gerçekleşmesi gizlilik ihlalidir ve yasal sorunlara sebep olacaktır (Stamp, 2011).

Bütünlük, bilginin yetkisiz kişilerce değiştirilmesini önlemek ya da en azından sorunu tespit etmekle ilgilidir. Örneğin bankalar, kişilerin hesaplarındaki bakiyeyi değiştirmesini önlemek için hesap bütünlüklerini korumalıdırlar.

Gizlilik ve bütünlüğün aynı şey olmadığına dikkat edilmelidir. Yetkisiz kişilerce veriler okunamasa bile değiştirilebilir ya da silinebilirler. Böyle bir durumda değişiklik yapılmış ve o değişiklik okunamıyor ve bilinmiyor olabilir. Ancak bazen sadece sorun çıkarmak

yeterli olduğu için kötü niyetli kişiler, ne değişiklik yaptıklarıyla ilgilenmeyebilmektedir (Stamp, 2011).

Erişilebilirlik, veriye istenildiği zaman ulaşılmasıyla ilgilidir. DoS (Denial of service) saldırıları veriye erişimin önünde büyük bir engel olmaktadır. Banka örneğinden devam edecek olursak, banka ve müşteri için erişilebilirliğin engellenmesi büyük bir sorundur. Bankanın web sitesine erişilemediği bir durumda; banka müşteri işlemlerinden para elde edemez ve müşteriler de işlemlerini gerçekleştiremez. Bu da müşteri kaybına yol açabilir. Ancak bilgi güvenliğini; gizlilik, bütünlük ve erişilebilirlik olarak tanımlamak bu konu için sadece bir başlangıçtır. (Stamp, 2011).

3.2. Bilgi Güvenliğinde Risk Analizi

Risk, bir hedefe ulaşamamanın olasılığının ve sonucunun bir ölçüsüdür. Riskin bir sonuca ulaşamama olasılığı ve bu sonuca ulaşamamanın etkisi/sonucu olmak üzere iki bileşeni vardır. Bununla birlikte, başarısızlık olasılığı ve başarısızlığın sonucu genellikle kesin ve ölçülebilir parametreler olmadığından, istatistiksel veya diğer prosedürlerle tahmin edilmesi gerektiğinden riskin değerlendirilmesi her zaman için kolay değildir (Defense Systems Management College, 2000). ISO 31000 Risk Yönetimi Prosedürüne göre ise risk, belirsizliğin hedefler üzerindeki etkisidir (Purdy, 2010). Mevcut bilgi birikimine ve tahmine dayalı olduğu için risk öznel bir kavramdır. Fiziksel olarak ölçümü yapılamaz ancak olasılık tahmininde bulunabilir. Risk matematikte ise gerçekleşmesi istenilmeyen olayın meydana gelme olasılığının ve sonuçlarının çarpımı olarak karşımıza çıkmaktadır (Deighton, 2016).

Yönetim; belirlenmiş bir hedefe yönelik olarak eldeki kaynakların planlanmasını, kontrolünü, organizasyonunu sağlamak olarak tanımlanabilirken risk yönetimi; gerçekleşmesi istenilmeyen olayların olasılığının ya da onun etkisinin azaltılması için risklerin; tanımlanması, değerlendirilmesi, önceliklendirilmesi konusunda akıllıca davranma durumu olarak tanımlanabilir (Hubbard, 2020). Risk yönetiminde ilk adım risklerin değerlendirmesidir. Bu süreçte, bilgi güvenliğine dair tehditlerin etkisi ve tehditlerin gerçekleşme olasılığı değerlendirilmelidir (Sumner, 2009). Risk yönetiminin kritikliği ve maliyeti nedeniyle ciddiye alınması gereklidir. Kuruluşlar, yüksek etkili, yüksek olasılıklı risklere karşı korunmak isterler ve bu riskleri kontrol etmek için finansal kaynaklara yatırım yapabilirler. Ancak, etkisi ve olasılığı düşük riskler için aynı şeyi söylemek mümkün değildir. Bu tür riskler için risk azaltma stratejileri uygulayarak ek bir maliyet yükünün üstlenilmesi mantıklı olmamaktadır (Pinto ve ark., 2006).

Risk yönetim sürecinin ilk aşaması olan risk analizi; risk yöneticilerini bilgilendirmek için olayların olasılıklarının ve gerçekleşmesi durumundaki sonuçlarının değerlendirilmesini de içerecek şekilde risk bileşenlerinin detaylı olarak incelenmesidir (Hubbard, 2020). Risk analizi; organizasyonel misyonu desteklemek için kullanılan bilgi, insan, süreç ve teknoloji gibi kaynakların tanımlanmasını ve belgelenmesini gerektirmektedir (Choobineh ve ark. 2007). Projenin, istenilen süre ve maliyet kısıtlaması dâhilinde başarılı bir şekilde tamamlanması büyük ölçüde yüksek öncelikli acil risklerin erken tanımlanmasına bağlıdır (Datta ve Mukherjee, 2001). Elbette bir projenin başarı durumunu belirleyen birçok faktör bulunmaktadır. Ancak iyi bir risk yönetiminin gerçekleştirilmemesi durumunda projenin başarısızlıkla sonuçlanma olasılığının arttığını söylemek doğru olacaktır (Carbone ve Tippett, 2004).

Bilgi ve bilgi sistemleri kuruluşlar için oldukça önemli bir esastır. İş proseslerinin sürekli gelişen bir şekilde bilgi teknolojileriyle desteklenmesi sonucunda bilgi ve bilgi sistemleri üzerindeki riskler de çeşitlenerek artmaktadır. Özellikle kurum içi veya kurumlar arası veri alışverişi ve açık ağların giderek daha fazla kullanılmaya başlanması, bilgi ve bilgi sistemlerinin maruz kaldığı riskleri artırmaktadır. Riskleri azaltmak ve kuruluşların zarar görmesini önlemek için yeterli bilgi güvenliğinin sağlanması gerekmektedir (Disterer, 2013). Bilgi güvenliğinde risk analizinin amacı; BT kaynaklarını, olası ihlallerin zarar seviyelerine göre sıralayarak en uygun şekilde düzenlemektir (Shaikh ve Siponen, 2023).

Elektronik, basılı, sözlü vb. pek çok biçimde bulunan bilgi; soyut bir varlıktır ve bilgiyi barındıran insan, donanım, yazılım varlıkları, basılı belgelerin herhangi birinde oluşabilecek bir zafiyeti, ilişkili olduğu diğer varlıklar için tehdit unsuru olabilmektedir. Bilgi güvenliğinde risk analiz çalışmalarının tüm bu tehditler için hazırlıklı olması gerekmektedir (Ozkan ve Karabacak, 2010).

Bilgi güvenliği risklerinin değerlendirilebilmesi için nitel ve nicel pek çok risk analiz yöntemleri bulunmaktadır. Nitel yöntemler, iş süreçlerinde kolaylıkla uygulanabilen teknik olmayan birçok konunun da değerlendirilmesini sağlayan sözel ifadeleri içeren yöntemlerdir. Nicel yöntemler ise istatistiksel, matematiksel araçları ve prosedürleri (hata ağaçları, çok kriterli karar verme, bulanık mantık vb.) içeren yöntemlerdir (Patel ve ark., 2008; Ozkan ve Karabacak, 2010). Bilbao, (1992) hırsızlık, sabotaj, kişisel saldırı vb. güvenlik risklerini analiz etmek için TUAR modelini önermektedir. Bu model hata ağacı ve bulanık kümeyi kullanan nicel metoda örnek verilebilir. Kailay ve ark., (1995) ise bilgisayar güvenliği risk analizinde uygun maliyetli ve pratik olması açısından

matematiksel veya istatistiksel araçları kullanmayan nitel tabanlı bir prototip uzman sistemi kullanmışlardır. Risk analizi için yoğun nicel ölçümler içeren yöntemler çok uygun olmamaktadır. Bunun nedeni, günümüzün bilgi sistemlerinin geçmiş yılların aksine karmaşık bir yapıya ve yaygın kullanıma sahip olmasından kaynaklanmaktadır. Karmaşık ortamlar için risk modellemede kullanılan ölçütler süreci daha da zorlaştırmakta, nicel yöntemler yeterli olmamaktadır. Bu nedenle, günümüz karmaşık risk yapılarında nitel analiz yöntemleri daha uygun olmaktadır. Ancak nitel risk analizi yöntemlerinin önemli bir dezavantajı, risk modellemesinde matematik ve istatistik araçlarını kullanmadıkları için, tutarsız sonuçlar verebilmesidir. Risk analizini yürüten kişilerin fikirlerine büyük oranda bağlı olmaktadır ve göreceli sonuç verebilmektedir (Karabacak ve Soğukpınar, 2005).

3.2.1. Mobil Cihaz Tehditleri

2020 yılında dünya çapında faaliyet gösteren mobil cihaz sayısı 14 milyarın biraz üzerindeyken 2021 yılında neredeyse 15 milyara ulaşmıştır. Bu sayının 2025 yılında, 2020 yılına göre 4,2 milyar artarak 18,22 milyara ulaşması beklenmektedir (Laricchia, 2023). Mobil cihazlar içerisinde en yüksek kullanım oranı cep telefonlarına ait olup bu oran dünya nüfusunun üçte ikisinden fazlasını oluşturmaktadır. Tekil mobil kullanıcıların sayısı 2023 sonlarında yaklaşık olarak 5,60 milyara ulaşmıştır. Bu sayının içerisinde hücresel bağlantı kullanan akıllı telefonların sayısının toplam cep telefonu sayısının %84'ünü oluşturduğu belirtilmektedir (DataReportal, n.d.). Mobil teknolojiler; eğitim, sağlık, bankacılık, yönetim vb. birçok alanda değerli bilgileri elinde tutmaktadır ve bilgi güvenliği konusu kurumlar için oldukça önemli olmaktadır. Cep telefonunun hızla yaygınlaşması, dağınık yerlerdeki insanlara halihazırda kullanmakta oldukları bir teknoloji aracılığıyla ölçeklenebilir bir şekilde ulaşma kapasitesini de beraberinde getirmiştir ve bu tür cihazların bireyler ve kurumlar için oluşturduğu riskler önemli ölçüde artmıştır (Greene ve Mamic, 2015). Mobil cihazlarda, ilgili paydaşlar yöneticilerden halka kadar uzanmaktadır ve bu nedenle risk analizini hızlı, kullanıcı dostu ve etkili bir şekilde oluşturabilecek bir yaklaşım gereklidir çünkü risk analiz yöntemleri genel olarak maliyetli, uzman bilgisi gerektiren ve zaman alan bir işlemdir (Ledermüller ve Clarke, 2011). Bu artan işlevsellik yelpazesi ve erişim sağlanılan kişisel/kurumsal bilgiler, saldırganlar için giderek daha fazla odak noktası haline gelmektedir. Akıllı telefonlar popülerleştikçe ve işlem gücü PC'ye yetişmeye başladıkça, her ne kadar en son bilgilere hızlı erişimden verimli finansal faaliyetlere kadar insanların günlük yaşamına birçok

kolaylık getirse de daha fazla potansiyel güvenlik tehdidinin çözülmesi ihtiyacı ortaya çıkmaktadır. Mobil cihaz kullanımı yaygınlaştıkça virüslerin hızlı yayılması da daha mümkün hale gelmekte ve gelecekte daha büyük hasarlara yol açacağı ihtimalini doğurmaktadır (Dagon ve Martin, 2004). İnternet ve Telekom ağına maruz kaldığında; virüslerin, arka kapıların (backdoors) veya casus yazılımların (spy malwares) yayılması için yeterli sayıda kanal açılmaktadır (Li, 2011). Şu ana kadar akıllı telefonları hedef alan çok sayıda saldırı gerçekleşmiş olmakta ve gelecek vaat eden kârlar ve akıllı telefonların antivirüs çalışmalarına yönelik kısıtlamaları nedeniyle bilgisayar korsanlarının savaş alanını PC'lerden akıllı telefonlara taşıması bir trend haline gelmektedir (Dagon ve Martin, 2004).

Kötü niyetli saldırganların odak noktaları genellikle bilgi güvenliğinin en zayıf halkası olarak kabul edilen son kullanıcılardır. Mağdurun bilgisi dışında, cihaz kontrolünü ele geçirerek kişisel ve kurumsal verilere erişilmeye çalışılmaktadır (Çınar ve Kara 2023).

3.2.2. Kötü Amaçlı Saldırı Türleri

Kötü amaçlı saldırıların en bilinenleri; Sosyal Mühendislik, Kimlik Avı ve Ortadaki Adam olmak üzere üç türden oluşmaktadır.

- Sosyal Mühendislik: Bir senaryo oynayarak kendilerini savcı, polis, bankacı vb. gibi tanıtarak, hedef aldıkları kişilerin şahsi bilgilerini elde etmeye çalışan ikna kabiliyeti güçlü, iyi giyimli, iyi bir diksiyona sahip, aynı zamanda teknolojiyi iyi kullanabilen kötü niyetli sosyal mühendislerin uyguladığı bir tehdit türüdür. Akıllı mobil cihazlar için kullanılan sosyal mühendislik tekniği genellikle reklamlar aracılığı uygulanmaktadır. Zararlı yazılımlar, reklam yazılımlarının içine gömülmekte ve kullanıcıların isteği dışında çalıştırılabilmektedir.
- Kimlik Avı (Oltalama-Phishing): Kullanıcının akıllı mobil cihazında gerçek bir güvenli uygulama gibi davranarak kişinin oturum açma şifresini ve diğer bilgilerini ele geçirmeye çalışan sahte uygulamalardır.
- Ortadaki Adam Saldırısı (MITM): Yetkisiz kişilerin ağ bağlantıları arasına sızarak iki bağlantı arasındaki iletişimin kesilmesi, gizlice dinlenmesi ya da manipüle edilerek yanıltıcı iletişim oluşturulabilmesi şeklinde gerçekleştirilmektedir (Çınar ve Kara 2023).

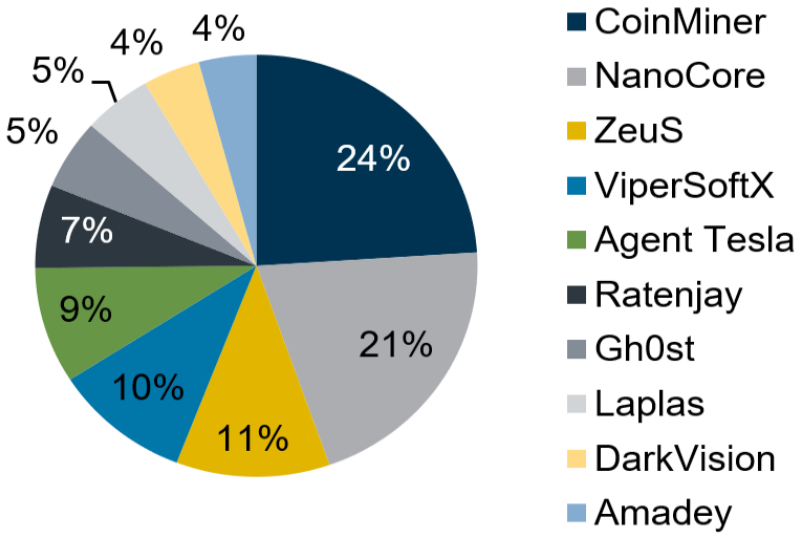
3.2.3. Kötü Amaçlı Yazılımlar

Kötü amaçlı yazılım tehditleri her zaman mevcuttur. Kötü amaçlı yazılımlar, bilgisayar sistemlerine zarar vermek, bozmak veya istismar etmek için tasarlanmıştır. Siber suçlar artarken, çeşitli kötü amaçlı yazılım türlerini anlamak ve dijital varlıkları korumak için proaktif önlemler almak çok önemli olmaktadır.

2023 Yılının En Tehlikeli Kötü Amaçlı Yazılım Saldırıları:

- Truva Atları: Truva atları, kendilerini yasal yazılım veya dosya olarak gizleyen aldatıcı kötü amaçlı yazılımlardır. Etkinleştirildiklerinde hassas verileri çalabilmekte, sistemleri çökertebilmekte ve kişisel bilgileri tehlikeye atabilmektedir. Örn; NanoCore, ZeuS, Agent Tesla, Ratenjay, Gh0st yazılımları.
- Solucanlar: Solucanlar, insan müdahalesi olmadan bir bilgisayardan diğerine yayılabilen, kendi kendini kopyalayan kötü amaçlı yazılımlardır. Bant genişliğini tüketebilmekte, istenmeyen programlar yükleyebilmekte ve hatta verileri silebilmektedirler.
- Reklam yazılımı: Kullanıcıları istenmeyen reklamlara maruz bırakan bir kötü amaçlı yazılım türüdür. Tarama davranışınızı izleyebilmekte, kişisel verilerinizi toplayabilmekte ve bilgisayar performansını bozabilmektedir.
- Cryptojacking: Bilgisayar korsanlarının, bilgisayar kaynaklarını izinsiz olarak kripto para madenciliği yapmak için kullanmasını içermektedir. Sistemi yavaşlatabilmekte ve enerji tüketimini artırabilmektedir. Örn; CoinMiner, ViperSoftX yazılımları.
- Casus Yazılım: Casus yazılımlar kullanıcıları gözetlemek ve onların bilgisi olmadan hassas bilgileri toplamak için tasarlanmıştır. İnternet etkinliklerini izleyebilmekte, tuş vuruşlarını kaydedebilmekte ve gizliliği tehlikeye atabilmektedir.
- Fidye Yazılımı: Fidye yazılımı dosyaları şifrelemekte ve dosyaları serbest bırakmak için fidye talep etmektedir. Bireyleri ve işletmeleri ciddi şekilde etkileyerek veri kaybına ve mali zarara neden olabilmektedir.
- Malvertising: Yasal web sitelerine veya reklam ağlarına kötü amaçlı reklamlar yerleştirmeyi içermektedir. Bu reklamlara tıklamak kötü amaçlı yazılım bulaşmasına yol açabilmektedir.

- Arka Kapı: Bir bilgisayar sistemine yetkisiz erişim sağlayarak saldırganların kontrolü ele geçirmesine veya hassas verileri çalmasına olanak tanımaktadır. Tespit edilmeleri ve kaldırılmaları zor olabilmektedir.
- Rootkitler: Bir bilgisayar sistemine yetkisiz erişim sağlamak ve varlıklarını maskelemek için tasarlanmıştır. Genellikle çekirdek seviyesinde çalıştıkları için kaldırılmaları zor olabilmektedir.
- Botlar ve Botnetler: Botlar, saldırganlar tarafından uzaktan kontrol edilen virüslü bilgisayarlardır. DDoS (Servis Dışı Bırakma Saldırısı) saldırıları ve diğer kötü amaçlı yazılımların yayılması gibi çeşitli siber saldırıları başlatmak için kullanılabilmektedirler. Örn; Amadey yazılımı.



Şekil 3.2. 2023 Yılının 2. Çeyreğindeki En Önemli 10 Kötü Amaçlı Yazılım (CIS, 2023).

Şekil 3.2'de 2023 yılının 2.çeyreğindeki en önemli 10 kötücül yazılım, görülme oranları ile birlikte belirtilmiştir. Sonuç olarak, dijital varlıkların korunması için farklı kötü amaçlı yazılım türlerini anlamak oldukça önemlidir. Bu tür saldırılardan korunmak için şüpheli bağlantı ve eklere tıklamamak, güvenlik duvarının etkin olduğundan emin olmak, işletim sistemi ve yazılımı güncel tutmak, güvenilmeyen kaynaklardan dosya indirmemek, dosyaları düzenli olarak çevrimdışı yedeklemek ve çevrimiçi ortamda dikkatli olmak gibi siber güvenlik uygulamalarını hayata geçirerek kötü amaçlı yazılım saldırılarının kurbanı olma riski önemli ölçüde azaltılabilmektedir (Zac, 2023; CIS, 2023).

4. METODOLOJİ

Bu bölümde, çalışmada kullanılan yöntemler tanıtılacaktır.

4.1. Hata Modu Etkileri Analizi (FMEA)

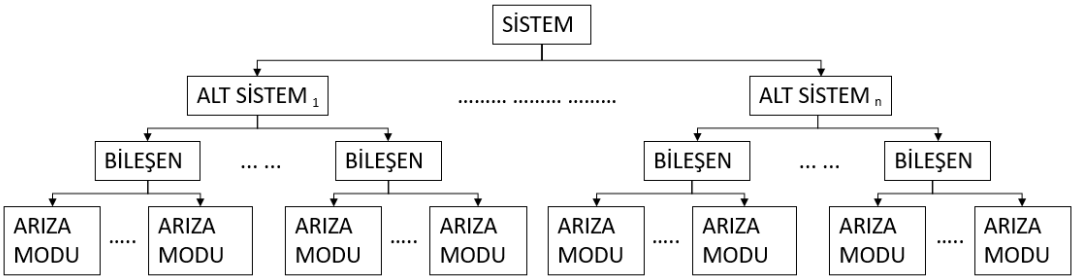
FMEA (Hata Modu Etkileri Analizi) iş açısından kritik olan sistem, tasarım, proses, konsept, yazılım ve hizmetlerde var olan ya da potansiyel hataları, müşteriye ulaşmadan önce tanımlamak, analiz etmek, etki oranını azaltmak ya da ortadan kaldırmak amacıyla kullanılan sistematik bir tekniktir. Genellikle yeni bir ürün ya da proseste, potansiyel hatalar ortaya çıkmadan önce uygulanan bir risk değerlendirme aracıdır. Belirlenen her bir potansiyel hata için ilk olarak meydana gelme olasılığı tahmin edilmekte; ikinci olarak, arızanın sonuçları (şiddeti) belirlenmekte ve üçüncü olarak, ciddi sonuçlar doğurmadan önce arızanın tespit edilme olasılığı değerlendirilmektedir. En son ise üçünün kombinasyonuna bağlı olarak eylemler gerçekleştirilmektedir. Amaç, varlık yaşam döngüsünün tüm aşamalarında tam bütünleşmiş operasyonlar, bakım, geri dönüşler, değişiklikler ve varlık bütünlüğü çözümleri sağlayarak hatayı önlemek ve varlıkları ve tesisleri en yüksek performansta çalışır durumda tutmaktır (Stamatis, 1995; Ivancan ve Lisjak, 2021). Havacılık, tıp, bilgi sistemleri, elektronik, otomotiv, kimya, enerji, hizmet, bilgi ve benzeri hangi sektörde olursa olsun, FMEA güvenilirliği sağladığı ve müşteri memnuniyetini sağlamaya yardımcı olduğu için çok önemli bir araçtır. Gerektiği şekilde yapıldığında FMEA; sorunları önceden tahmin ederek önleyebilir, maliyetleri düşürür, ürün geliştirme sürelerini kısaltır ve son derece güvenilir ürün ve hizmet süreçleri elde edilmesini sağlar (Carlson, 2012).

İnsanlar, yüksek kaliteli hizmet ve ürünler için kuruluşlardan taleplerde bulunmaktadırlar. Artan ürün karmaşıklığı ve işlevselliği ve hizmet kalitesi, kuruluşların kalite ve güvenilirliğini sürdürmesini gittikçe daha da karmaşık hale getirmektedir. Geleneksel olarak güvenilirlik, yaygın testler ve olasılıksal güvenilirlik modellemesi gibi yöntemlerin uygulanması yoluyla gerçekleştirilmektedir. Bu yöntemler ürün ve süreçlerin ileri aşamalarında uygulanmaktadır. FMEA, ürün süreç döngüsünün ilk aşamalarında olası güvenilirlik sorunlarını değerlendirmek ve bu sorunların üstesinden gelmek için önlemler almayı amaçlamaktadır. Böylece daha tasarım aşamasında iken neyin yanlış yapıldığını öngörülerek güvenilirlik artırılmış olur. Her bir hata modunu öngörmek mümkün olmasa da iyileştirme ekibi olası hata modlarının mümkün olduğunca kapsamlı

bir kaydını oluşturmalıdır. FMEA'lar ayrıca gelecekteki ürün geliştirmede kullanılmak üzere kronolojik bilgi taşımaktadır (Lipol ve Haq, 2011).

FMEA resmi bir sistem analizi metodolojisi olarak ilk kez 1960'larda NASA tarafından bariz güvenlik gereksinimleri için önerilmiştir (Sharma ve ark., 2005). Ancak yaklaşık 1977 yılında Ford otomobil üreticileri tarafından uygulandığında daha iyi tanınmıştır (Gilchrist, 1993). O zamanlardan itibaren başta havacılık olmak üzere birçok çeşitli alanlarda ürün ve proseslerde yaygın olarak kullanılmaktadır (Ebeling, 2019).

FMEA, Şekil 4.1'de gösterildiği gibi aşağıdan yukarıya bir yaklaşımdır. Yani bir seviyedeki potansiyel hata modlarıyla başladıktan sonra hemen alt sistemindeki etkiyi araştırır. Kusursuz bir FMEA analizi için hiyerarşideki tüm seviyeler sürece dâhil edilmelidir (Wang ve ark., 1995).



Şekil 4.1. Sistemin Hiyerarşik Yapısı

4.1.1 Yaygın olarak kullanılan FMEA Türleri

- Konsept FMEA: Genellikle sistem ve alt sistem seviyesinde, donanım oluşturulmadan önce erken aşamalarda hataların analizi için kullanılmaktadır. FMEA'nın bu türü, konsept aşamalarında birçok sistemin elemanları arasındaki etkileşimi içermektedir.
- Sistem FMEA: Tüm sistemin en üst düzey analizidir. Sistemle ilgili olan insan, çevre, sistem güvenliği, entegrasyonu, hataları vb. tüm konularla ilgilenmektedir. Sisteme özgü olan ve diğer seviyelerde bulunmayan, tüm sistemi bütünüyle bozabilecek arızalarla birlikte aynı zamanda arayüz ve etkileşimlerle ilgili hata modlarını da içermektedir.

- Tasarım FMEA: Genellikle alt sistem ya da bileşen seviyesindeki hataların analizinde kullanılmaktadır. Tasarımdaki eksikliklere odaklanarak iyileştirme ve ürün güvenilirliğini artırmayı içermektedir.
- Proses FMEA: Üretim ya da montaj sürecindeki hatalara odaklanmaktadır. Üretim ve montaj sürecine ek olarak malzemelerin taşınması, depolanması, etiketlenmesi gibi süreçleri de içermektedir. Bir ürünün tasarımından son halini alıncaya kadarki sürecinde güvenli bir şekilde üretilmesini sağlamaya odaklanmaktadır.
- Yazılım FMEA: Eğer yazılım, donanımı kontrol ediyorsa bu analiz geçerli olmaktadır. Yazılımdaki zayıflıkları belirlemeye, yazılım güvenlik gereksinimlerini incelemeye ve spesifikasyonları net hale getirmeye odaklanmaktadır. Amaçları; yazılım donanım arızalarının hataya dayanıklı olup olmadığını belirlemek ve sistem spesifikasyonlarındaki eksik gereksinimleri belirlemektir (Carlson, 2012; Sharma ve ark., 2018).

Geleneksel olarak, FMEA kullanılarak farklı hata modlarının risk hesaplaması, risk öncelik sayısı (RPN) geliştirilerek yapılır.

RPN, üç bileşenin çarpımı ile elde edilen değerdir:

- Bir hata modunun ortaya çıkma olasılığı (O)
- Hata modunun şiddeti (S) ve
- Hata modunun tespit edilebilirliği (D) (Mandal, 2014)

RPN hesaplamasında, üç parametre için nitel olarak belirlenen değerler nicel olarak yorumlanmaktadır.

$$RPN = OxSxD \quad (1)$$

Başlangıçta niteliksel olarak toplanan bilgiler öznel yorumlanır ve ilkinden farklı olarak niceliksel bir ölçekte kullanılır (Franceschini ve Galetto, 2001).

Ghosh (2010), RPN 80'den büyük olan hata modları için düzeltici eylemler önermektedir. Amaç, düzeltici eylem sonrasında daha düşük bir RPN sayısının elde edilmesini sağlamaktadır.

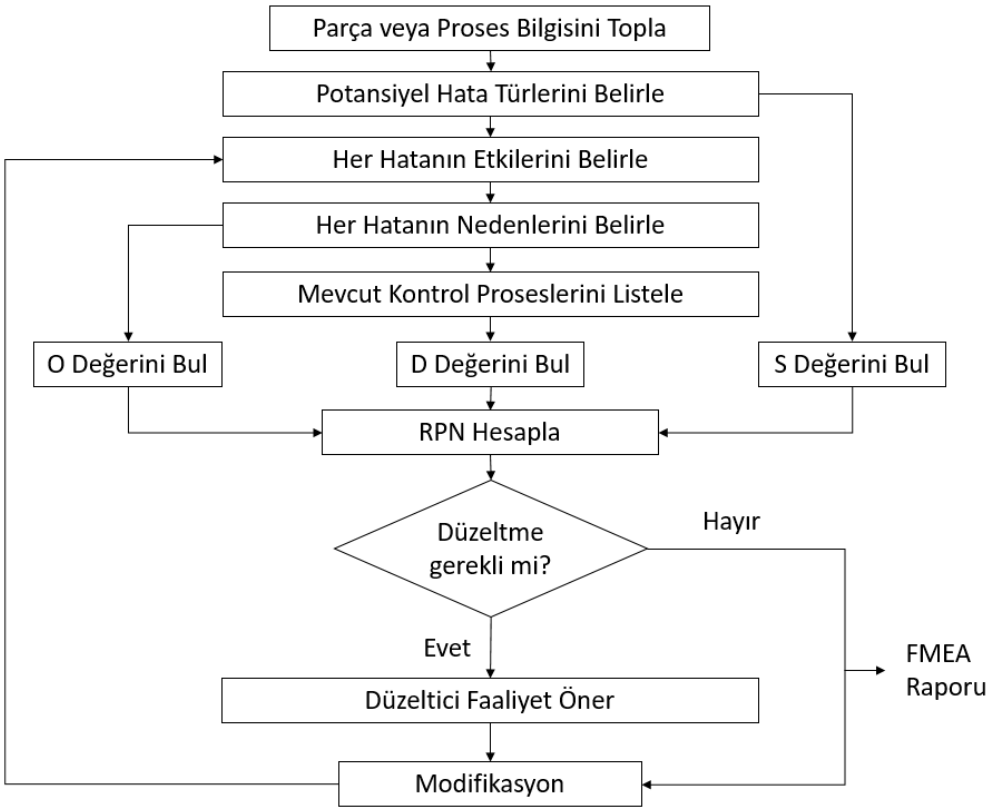
Denklem (1)'de, olasılık, ciddiyet ve tespit edilebilirlik net sayılardır, dolayısıyla RPN değerleri de doğası gereği nettir. Ancak RPN'nin hesaplanmasına yönelik bu net yaklaşımın çeşitli dezavantajları bulunmaktadır (Mandal, 2014). Her ne kadar kullanışlı görünse de klasik FMEA, özellikle kritiklik analizi söz konusu olduğunda uygulamada bazı sınırlamalar ortaya çıkarmaktadır (Xu ve ark., 2002).

4.1.2. FMEA Prosesi Adımları

FMEA prosesi işlem adımları:

1. Sistemin işleyişiyle ilgili genel bilgiler toplanmalıdır.
2. Sistemin işleyişindeki gereklilikler ve potansiyel hataların nerelerde olabileceği belirlenmelidir. Sistemdeki risklerin daha iyi tespiti için sistem, daha sonra entegre edilecek şekilde ayrıştırılabilir. Her bir işlev için potansiyel hata modları belirlenmelidir.
3. Belirlenen her hata için etkiler tanımlanıp bu etkilerin dikkatli bir şekilde seviyesi belirlenmelidir. Modifikasyon kararı sonrası geri dönülecek adım bu adımdır.
4. Her hatanın nedenleri belirlenmelidir. Nedenler olasılık değerinin belirlenmesinde etkilidir. 10 puanlık bir ölçek, olasılığı çok düşük ihtimalden (1) çok yüksek ihtimale (10) kadar tahmin edebilir.
5. Hataların tespit edilebilirlik değeri belirlenmelidir. Tespit edilebilirlik ne kadar yüksek ise risk o kadar düşük olmaktadır.
6. Belirlenen O, S ve D değerleri kullanılarak RPN hesaplanmalıdır.
7. RPN değerlerine bağlı olarak düzeltici faaliyet gerektirmeyen hata modları için FMEA raporu yazılarak gerekli modifikasyonlar yapılmalıdır.
8. RPN değerlerine bağlı olarak kabul edilebilir risk sınırını aşan riskler için düzeltici faaliyet önerilmelidir.
9. Başka bir FMEA döngüsü ile riskleri yeniden değerlendirilmelidir (Stamatis, 1995; Sharma, 2005; ASQ, 2016; Asllani ve ark., 2018).

FMEA prosesi akış şeması Şekil 4.2'de sunulmuştur.



Şekil 4.2. FMEA Prosesi Akış Şeması (Sharma, 2005).

4.1.3. FMEA Avantaj ve Dezavantajları

FMEA'in avantajları;

1. Daha yüksek güvenlik, güvenilirlik ve kalite sağlayarak ürün ve prosesler için geliştirilmiş olan tasarımlara katkı sağlamak,
2. Tüketici memnuniyetinin artırılmasına katkıda bulunmak, .
3. Ürün geliştirme süreleri, yeniden tasarım ve garanti maliyetlerini azaltarak maliyet tasarrufuna katkıda bulunmak,
4. İsrafı ve katma değeri olmayan işlemleri azaltmak,
5. Sürekli iyileştirmenin uygulanmasına teşvik etmektir.

Ek olarak, Tasarım aşamasındaki ürünlerin tasarım evriminin metodolojik olarak belgelenmesi yeteneğinden dolayı tasarımcılar bu yöntemi cazip bulmaktadır (Franceschini ve Galetto, 2001; Lipol ve Haq, 2011).

Ancak Klasik FMEA analizinin bazı dezavantajları da bulunmaktadır:

1. RPN hesaplamasında; olasılık, şiddet ve tespit edilebilirlik çarpımı sonucunda sıralama her zaman mantıklı sonucu vermeyebilir. Şiddeti daha az olan bir durum daha yüksek bir RPN değerine sahip olabilir. Örneğin, (O, S, D) endeksleri sırasıyla (8,1,1) olan bir durum ile (2,2,2) olan durumlarda Her iki durum için de RPN değeri '8' olacaktır. Bunun nedeni, karakteristik hata modu indekslerinin sıralı niteliksel ölçeklerde ifade edilmesi ve tüm endeks ölçeklerinin eşit önem seviyesine sahip olduğu varsayımıdır.
2. Parametre değerlerine atanan rakamlar oransal olarak bir bilgi vermemektedir. Sadece bir değerin diğerinden daha iyi veya daha kötü olduğu bilgisini taşımaktadır. Örneğin; '2' derecesi, '1' derecesinden iki kat daha kötüdür demek değildir. Ancak çarpma işlemi onlara böyle bir yorumlama getirmektedir.
3. FMEA ekibi iyi bir bilgi birikimine sahip ve multidisipliner yapıda olmalıdır. Genel olarak, birkaç kişinin katıldığı bir beyin fırtınası oturumu fikir aşamasından sonuca kadar sürece dâhil olan kişiler gereklidir. Bu da yüksek maliyete yol açmaktadır ve FMEA'nın daha geniş bir kapsamda uygulanmasını engellemektedir. FMEA değerlendirmesinin bilgisayarda etkin bir şekilde otomasyonu için uzman deneyiminin dâhil edilebileceği bir sistemin geliştirilmesi çok faydalı olacaktır.
4. FMEA'da hatalar ve onlara ait parametreler çoğunlukla dilsel değişkenlerle tanımlanabilen, kesinlik içermeyen ifadelerdir. Ayrıca çoğu sistem zamanla değişikliğe uğrar ve bu değişime ilişkin değerlendirmeler de doğal dilsel değişkenlerle tanımlanmaktadır. Klasik FMEA bu değerlendirmeyi karşılayamamaktadır.
5. Klasik FMEA ile dilsel değerlendirmelerin birleştirilmesi ve birkaç hata modunun aynı anda oluşmasının dağılımlarını elde etmek oldukça zor olmaktadır.
6. Sayısal verilerin yorumlanması RPN'in basitleştirilmesini sağlar ve hesaplama kolaylığı sağlar ancak aynı zamanda anlamından uzaklaşma riskini de artırır (Franceschini ve Galetto, 2001; Xu ve ark., 2002).

Bu tür dezavantajların üstesinden gelmek için birçok yöntem bulunmaktadır, bulanık mantık da bunlardan birisidir. Bulanık mantık, kesin olmayan ve yaklaşık analize izin vererek bu durumlarda sistem güvenilirliğini karakterize etmek için etkili bir araç sağlar, mümkün olmadığı yerde kesinliği zorlamaz (Bowles ve Pelaez, 1995).

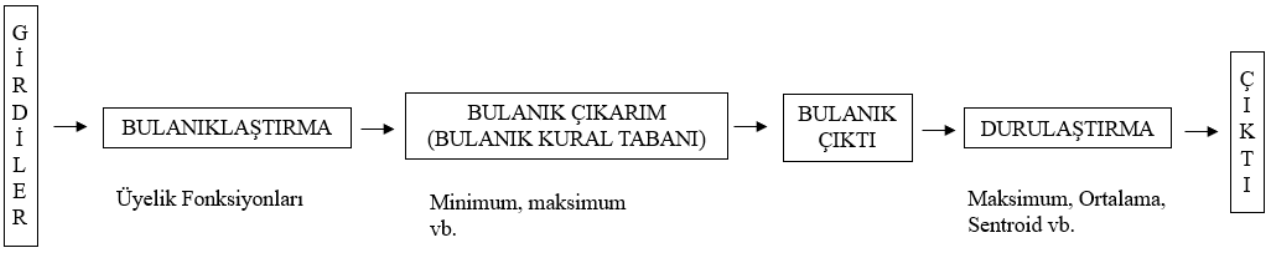
4.2. Bulanık FMEA

Çalışmanın bu bölümünde bulanık mantık, bulanık kümeler ve bulanık FMEA tanıtılacaktır.

4.2.1. Bulanık Mantık

Aristo tarafından öne sürülen klasik mantık, insanların akıl yürütme yoluyla vardığı sonuç ya da aldığı kararlar gibi net olan doğru veya yanlış önermelerle ilgilenmektedir. Klasik mantıkta her bir önerme zıttıyla vardır. Her önermeyi bir değişken temsil etmekte ve bu değişkenlerin kombinasyonları da doğru veya yanlış olmak üzere sadece bir doğruluk değerine sahip olmaktadır. Yani klasik mantıkta hiçbir zaman bir şey aynı anda hem doğru hem de yanlış olamaz. Bu mantık, insan aklı ile kolayca algılanamayan ve çözümlenemeyen olaylarda çeşitli idealleştirme ve kabuller yoluyla problemlere çözüm bulunmasını kolaylaştırmıştır. Ancak gerçek hayatta ideal olanı elde etmek mümkün olmamaktadır. Sistem karmaşıklığı arttıkça, çözüm kolaylığı sağlamak için kabuller yapılmaya başlanır bu kabuller her ne kadar büyük ve karmaşık problemlerin çözümünü kolaylaştırsa da kesinlik içerdiklerinden sonucu gerçekten uzaklaştırır. Halbuki gerçek dünya sürekli olarak karmaşıklık içermektedir. Kabuller ve varsayımlar içeren öngörüler, gerçek dünyada ölçümlerin yerini tam olarak tutamazlar. Bulanık mantıkta kabullere gerek duyulmadığından sonuçtan bu şekilde bir sapma yaşanmamaktadır. Bu noktada insanlar; yaklaşık olanı düşünme, eksik ya da yanlış bilgiler üzerinde tutarlı sonuçlara varabilme yeteneğini kullanmaktadırlar. Buna rağmen her karmaşık problem bulanık mantık ile çözülür demek de çok doğru olmayacaktır. Bulanık mantık, problemler için sözel olarak akılcı ilişkilerle çözüm arayan bir yöntem olarak sunulmaktadır. Bulanık sistemde amaç girdileri çıktılara mantık kuralları ile bağlamaktır (Chen ve Pham, 2000; Şen, 2020).

Bulanık mantığı daha iyi ifade edebilmek için Şekil 4.3'te gösterildiği gibi bulanık çıkarım modeli akış şemaları kullanılmaktadır.



Şekil 4.3. Bulanık Çıkarım Modeli Akış Şeması (Metaxiotis ve ark., 2003; Sharma, 2005).

Modele ilişkin temel bileşenler:

- Bulanıklaştırma: Uygun dilsel ifadeler ile model girdi ve çıktılarının bulanıklaştırılması işlemi yapılır (‘düşük’, ‘orta’, ‘yüksek’ vb. gibi).
- Bulanık kural tabanı: Her kuralda, girdi ve çıktı değişkenlerinin değer aralıklarından belirli kısımlar birbirleriyle ilişkilendirilir. Bu aşamada, uzman görüşlerine ek olarak önceki çalışmalardan da yararlanılabilmektedir.
- Bulanık çıkarım sistemi: Yazılan kurallarda öncül kısımdaki şartların ardıl kısımda karşılığını bulmak için çeşitli çıkarımların yapılmasını sağlar. (Eğer-İse şeklinde yazılan bulanık kurallarda; ‘Eğer ’den sonra öncül; ‘İse ’den sonra ardıl gelmektedir.) Burada ilgili bir kuralın, yazılan kurallar içerisinde denk geldiği karşılıklarının bir harmanlanması yapılarak verilen girdi değişkenlerinin sayısal değerleri için çıktı değişkeni için bulanık çıkarım elde edilir.
- Durulaştırma: Bulanık olarak elde edilen çıktı değişkeni durulaştırılarak kesin bir sayı elde edilir (Sharma, 2005; Şen, 2020).

Temel bulanık sistemde bulanıklaştırma ve durulaştırma işlemlerini yapan birimler bulunmamaktadır ve sistem tamamen bulanık ifadelerden oluşmaktadır. Daha sonra bulanık sistemin, sayısal girdiler içeren durumlarda kullanılabilmesi için bulanıklaştırma birimi eklenmiş; sonuçların mühendislik uygulamalarında sayısal olarak yorumlanabilmesi için de durulaştırma birimi eklenmiştir (Şen, 2020).

4.2.2. Bulanık Küme Teorisi

Klasik küme teorisinde, bir eleman hakkında hem deterministik hem de stokastik durumlar için net olarak iki ifade kullanılabilir: Bir eleman kesin olarak bir kümeye aittir ya da değildir. Ancak bulanık kümelerde böyle bir kesinlikten bahsedilmemektedir. Bulanık küme, net olarak sınırları belirlenmemiş kümedir (Alizadeh, 2013).

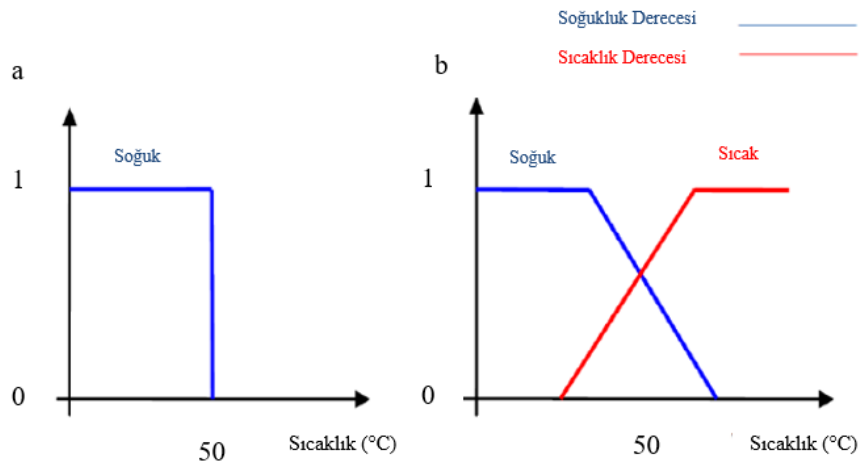
Bulanık küme, sistem ve mantık kavramları ilk olarak Lotfi Askerzadeh (Zadeh, 1965) tarafından literatüre kazandırılmıştır. Zadeh, bir elemanın bir kümeye 0 ile 1 arasında değişen üyelik derecesinde ait olma durumunu savunmaktadır. İlk zamanlar kesin bir şekilde reddedilen bulanık mantığın öneminin anlaşılması 1975 yılında Mamdani ve Assilian tarafından yapılan buhar makinasının kontrolünün bulanık sistem ile modellenmesi çalışmasının başarılı sonuç vermesi sayesinde olmuştur. Bu gelişme sonrasında bulanık sistemler birçok sektörde kullanılmaya başlanmıştır (Şen, 2020).

Olasılık ve istatistikte; "Bu varlığın, bu kümenin üyesi olma olasılığı nedir?" sorusu sorulduğunda, nihai sonuç ya “Varlık, kümeye aittir.” ya da “Varlık, kümeye ait değildir.” olacaktır. Varlığın, kümenin elemanı olma olasılığının %90 olduğu durumda, “Varlık, bu kümenin üyesidir.” cevabını veren bir kişinin doğru tahminde bulunma şansı %90’dır. Bu durum, varlığın kümeye %90 üye olduğu ve %10 da üye olmadığı anlamına gelmez. Yani bir elemanın hem bir kümede olmasına hem de olmamasına klasik küme teorisinde izin verilmez. Gerçek hayat problemlerinin çoğu klasik küme ile açıklanamadığı için kısmi üyelikleri kabul eden bulanık küme ile açıklanmaktadır (Chen ve Pham, 2000).

Bulanık küme teorisi, çoğu belirsiz olan doğal dilsel kavramların çeşitli türlerdeki bulanık kümelerle temsil edilmesine ve bunların belirli amaçlar doğrultusunda çok çeşitli şekillerde manipüle edilmesine olanak tanımaktadır. Dilsel değişkenler belirsiz olmalarının yanında anlamları ve yorumlamaları da bir bağlama bağlı olmaktadır. Örneğin bir mesafenin uçakla, arabayla ya da yürüyerek katedilmesi o mesafenin farklı yorumlanmasına sebep olacaktır. Ya da genç ve yaşlı kavramları farklı türdeki canlılara bakıldığında farklı yorumlanmakta; hatta astronomide gök cisimlerine uyarlandığında çok daha farklı yorumlanmaktadır. Benzer şekilde ucuz, pahalı, çok pahalı vb. kavramlar yalnızca uygulandıkları öğelere değil aynı zamanda alıcının refahına ve bir dizi başka koşula da bağlı olmaktadır. Hatta aynı koşullar altında bile kişiden kişiye farklılık gösterebilmektedir, bu konuda örnekler sayısızdır (Klir ve Yuan, 1995).

Bulanık küme aşağıda verildiği şekilde bazı özelliklere sahiptir. Buna göre genel olarak bir bulanık kümede;

- Üyelik derecesi 1’e eşit olan en az bir öge bulunmalıdır, yani bulanık küme normal olmalıdır. Ancak çıktı bulanık kümesinde normallik aranmamaktadır.
- Üyelik derecesi 1’e eşit olan ögenin en yakınında olan sağdaki ve soldaki ögelerin üyelik dereceleri 1’den 0’a kadar sürekli olarak azalmalıdır. Bu şekilde değerde artmadan azalma olması durumu monotonluk olarak belirtilmektedir. Bulanık kümede monotonluk aranmalıdır.
- Üyelik derecesi 1’e eşit olan ögenin sağında ve solunda eşit uzaklıktaki ögelerin üyelik derecesi eşit olmalıdır, buna bulanık kümenin simetrik olması denir. Ancak her bulanık kümede simetriklik aranmaz (Şen, 2020).



Şekil 4.4. (a) Klasik Küme (b) Bulanık Küme (Jain, 2012).

Şekil 4.4'te klasik küme ile bulanık küme arasındaki fark gösterilmektedir. Klasik kümede sadece dikdörtgen üyelik derecesi fonksiyonu bulunurken bulanık kümede değişik üyelik derecesi fonksiyonları bulunmaktadır. Şekil 4.4'te bulanık küme için üçgen üyelik fonksiyonu gösterilmektedir. Klasik kümede 30°C soğuk kabul edilirken bulanık kümede 30°C 'nin soğukluk derecesi 0,85 olup aynı zamanda 30°C 'nin sıcaklık derecesi 0,15'tir. Yani 30°C %85 soğuk iken, %15 de sıcaktır (Jain, 2012).

4.2.3 Üyelik Fonksiyonları

Üyelik fonksiyonları $\mu A(x)$ ile gösterilmektedir ve belirli bir bulanık değişkene ait noktaların derecesini temsil eden bir fonksiyondur (Jain, 2012).

A ⊂ E alt kümesi bulanık olmayan bir küme ise üyelik fonksiyonu:

$$\mu_A(\mathrm{x}) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases} \quad (2)$$

Burada $\mu_A(x)$, x değişkeninin A kümesindeki üyeliğidir. Yani, bir x değişkeni A kümesine sadece "aittir" ($\mu_A(x)$= 1) veya "ait değildir" ($\mu_A(x)$= 0). Ancak bulanık küme teorisi için bu uygunluk kavramı aşağıdaki gibi sunulmaktadır:

$$A = \{(x, \mu_A(\mathrm{x}), \mid \mathrm{x} \epsilon E)\} \quad (3)$$

$\mu_A(x)$: x değişkeninin A kümesindeki üyelik derecesi

A : Sıralı çift (x, $\mu A_{(x)}$) tarafından oluşturulan bulanık küme

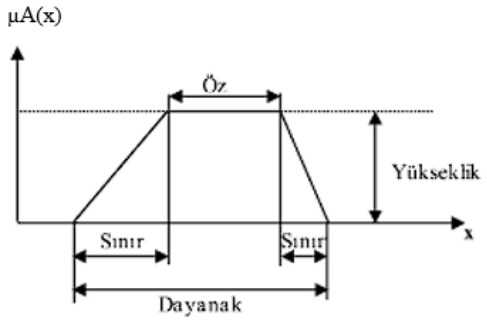
x : İlgili değişken

E : Evrensel Küme

Üyelik fonksiyonu, *E* evrensel kümesine ait bir *x* elemanının *A* alt kümesine ait olma derecesini ifade eden bir fonksiyondur. Geleneksel kümelerden farklı olarak [0, 1] sürekli aralığını kullanmakta ve bu aralıktaki değerler üyelik derecesi olarak adlandırılmaktadır. 0 sayısı *x* elemanının kümenin üyesi olmadığını gösterirken, 1 sayısı *x*'in kümenin tam üyesi olduğunu ve bu iki değer arasındaki herhangi bir sayı ise *x*'in kümeye üyelik derecesini ya da kısmi üyeliğini göstermektedir (Bojadziev ve Bojadziev, 2007; Maués ve ark., 2019).

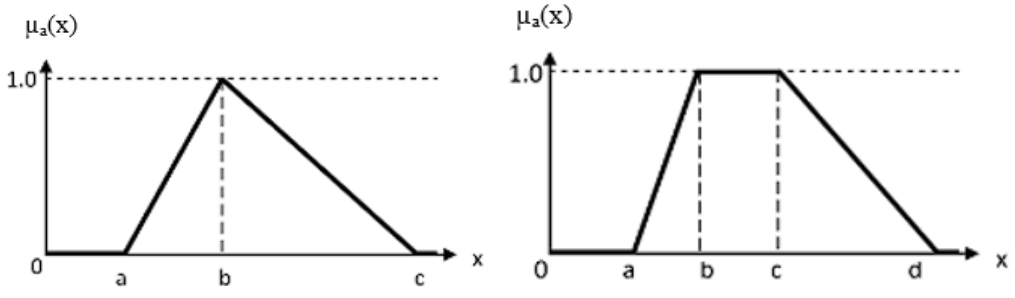
Üyelik fonksiyonu bölümleri; öz, dayanak, sınır gibi tanımlarla ifade edilmektedir.

$\mu A(x) = 1$ olan bölümler 'öz' olarak adlandırılırken alt kümenin bütün elemanlarını içeren aralık ise 'dayanak' olarak adlandırılmaktadır. Normal bir bulanık kümede en az bir tane öz bulunmalıdır. Üyelik derecesi (0,1) açık aralığında değişen elemanlar ise 'sınır' olarak adlandırılan bölümde yer almaktadır. Sekil 4.5.'te yamuk üyelik fonksiyonunun bölümleri gösterilmektedir (Şen, 2020).

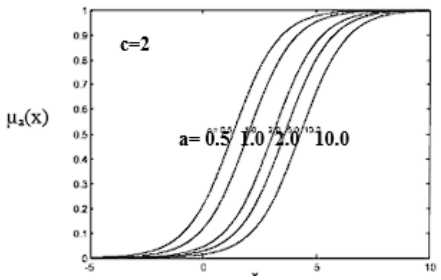


Şekil 4.5. Üyelik Fonksiyonu Bölümleri (Şen, 2020).

Üyelik fonksiyonunun uygun seçilmesi çözüm için oldukça önemlidir. Seçimde; kolay anlaşılabilirlik, kolay kullanım ve verimlilik göz önünde bulundurulabilir. Literatürde; üçgen, yamuk, sigmoid gibi çeşitli üyelik fonksiyonları bulunmaktadır. Şekil 4.6'da sırasıyla üçgen, yamuk ve sigmoid üyelik fonksiyonları gösterilmektedir (Jain, 2012; Şen, 2020).



a b



c

Şekil 4.6. (a) Üçgen, (b) Yamuk ve (c) Sigmoid Üyelik Fonksiyonları (Şen, 2020).

Üçgen üyelik fonksiyonu en basit üyelik fonksiyonu olarak kabul edilmektedir ve tek bir öz değeri bulunmaktadır. Yamuk üyelik fonksiyonunda, üçgen üyelik fonksiyonundan farklı olarak öz tek bir değer değildir. Ancak b=c olması durumunda üçgen üyelik fonksiyonu ortaya çıkmaktadır. Sigmoid üyelik fonksiyonunda a ve c olmak üzere iki farklı değişken bulunmakta ve a değeri sağ ve sol tarafa açıklık gösterdiğinden negatif olarak çok küçük olan ya da pozitif olarak çok büyük bulanık kelimeleri anlatmak için bu bulanık fonksiyondan yararlanılmaktadır (Şen, 2020).

Şekil 4.6'da gösterildiği gibi, üçgen üyelik fonksiyonunun, a <b <c olan bir alt ve üst sınır ve bir merkez değeri bulunmaktadır; fonksiyon taban değerler ve yükseklik değeri olmak üzere üç parametre ile tanımlanmaktadır (Khairuddin ve ark., 2021).

Bulanık A kümesinin a, b ve c parametreleri için tanımlanmış üçgen üyelik fonksiyonunun matematiksel gösterimi:

$$\mu_A(\mathrm{x}) = \begin{cases} 0, & x < a \\ \frac{x-a}{b-a}, & a \le x \le b \\ \frac{c-x}{c-b}, & b \le x \le c \\ 0, & x > c \end{cases} \quad (3)$$

Bulanık A kümesinin a, b, c ve d parametreleri için tanımlanmış yamuk üyelik fonksiyonunun matematiksel gösterimi:

$$\mu_A(\mathrm{x}) = \begin{cases} 0, & x < a \\ \frac{x-a}{b-a}, & a \le x \le b \\ 1, & b \le x \le c \\ \frac{c-x}{d-c}, & c \le x \le d \\ 0, & x > d \end{cases} \quad (4)$$

Bulanık A kümesinin a ve c parametreleri için tanımlanmış sigmoid üyelik fonksiyonunun matematiksel gösterimi (Şen, 2020):

$$\mu_A(\mathrm{x}) = \frac{1}{1+ae^{-(x-c)}} \quad (5)$$

4.2.4. Bulanık Kümelerde İşlemler

Kesişim kümesi A ve B bulanık kümelerinin elemanlarının üyelik derecesi minimum olanları olarak ifade edilmektedir. Matematiksel olarak gösterimi:

$$\mu_{(A\cap B)}(\mathrm{x}) = \min\big(\mu_A(\mathrm{x}), \mu_B(\mathrm{x})\big), x \in \mathrm{E} \quad (6)$$

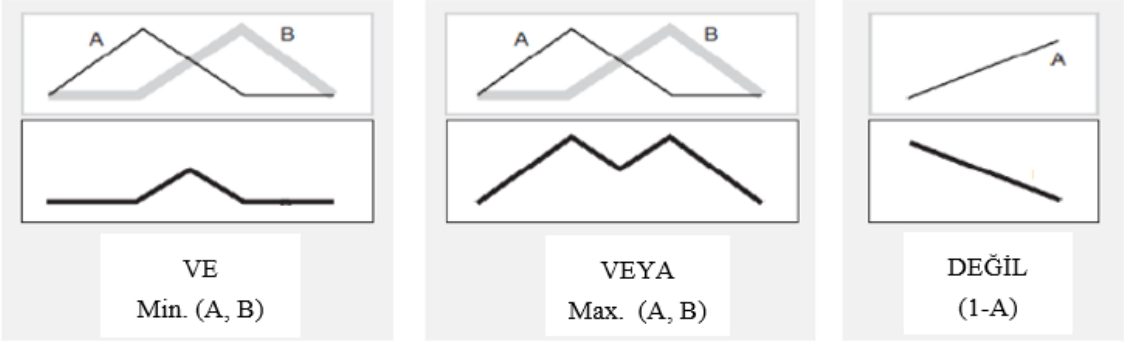
Birleşim kümesi A ve B bulanık kümelerinin elemanlarının üyelik derecesi maksimum olanları olarak ifade edilmektedir. Matematiksel olarak gösterimi:

$$\mu_{(A\cup B)}(\mathrm{x}) = \max\big(\mu_A(\mathrm{x}), \mu_B(\mathrm{x})\big), \mathrm{x} \in \mathrm{E} \quad (7)$$

Bulanık A kümesine ait x elemanının üyelik derecesi ile aynı kümenin tümleyenine (değili) ait üyelik derecesinin toplamı 1'e eşit olmaktadır. Matematiksel olarak gösterimi:

$$\overline{\mu_A}(x) = 1 - \mu_A(x) \quad (8)$$

Şekil 4.7'de sırasıyla; 've', 'veya', 'değil' mantıksal operatörlerin grafik gösterimleri bulunmaktadır. İlk satırda fonksiyon grafikleri yar alırken ikinci satırda ilgili mantıksal operatörlere göre grafikler gösterilmektedir.



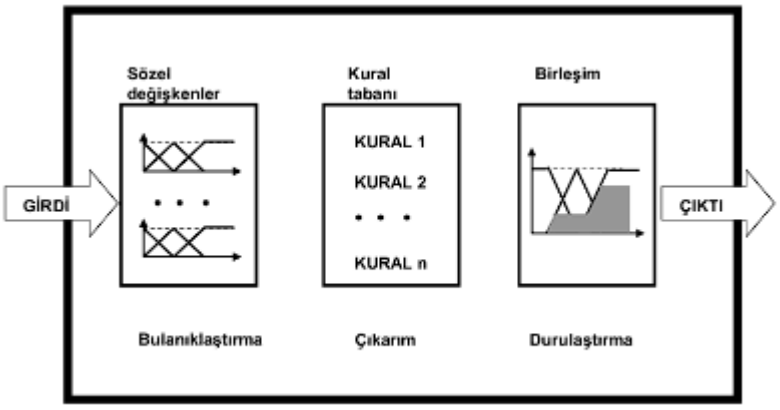
Şekil 4.7. Mantıksal Operatörlerin Grafik Gösterimi (Alizadeh, 2013).

4.2.5. Bulanık Çıkarım Sistemleri (BÇS)

Literatürde, en bilinenleri Mamdani Modeli ve Tagaki-Sugeno Modeli olmak üzere çeşitli Bulanık Çıkarım Sistem modelleri bulunmaktadır.

4.2.5.1. Mamdani Tipi BÇS

Mamdani Modelinin temel özelliği hem öncüllerin hem de sonuçların tümünün bulanık olmasıdır. Bu modelde bulanık girdiler bir kural tabanı ile bulanık çıktılar ile bağlanmaktadır. Şekil 4.8'de Mamdani Modeli yapısı gösterilmektedir.



Şekil 4.8. Mamdani Modeli Yapısı (Şen, 2020).

Mamdani Modeli işlem basamakları:

1. Bulanıklaştırma İşlemi: Girdi değişkenleri, kural tabanında kullanılmak için üyelik fonksiyonları yardımıyla bulanıklaştırılır.
2. Çıkarım Yapılması: Mantıksal operatörlerden 've' operatörü kullanılarak öncüldeki tüm üyelik dereceleri için en küçük değerler ya da bu değerlerin çarpımı alınır. Bu aşamada seçilen yönteme göre en küçükleme ya da çarpım olarak iki farklı çıkarım elde edilir. Daha sonra üyelik fonksiyon eğrisi elde edilen seviyelerden kesilerek ardıl kısım için çıktı oluşturulur.
3. Kuralların Birleştirilmesi: Tüm kurallar için ortak bir çıkarım yapılması amacıyla 'veya' operatörü kullanılarak bir önceki adımda kesilen bulanık çıkarım fonksiyonları birleştirilir, yani en büyükleme işlemi yapılır. Bu aşamada ortaya çıkan bulanık kümenin konveks olmasından ve normalliğinden söz edilememektedir.
4. Durulaştırma İşlemi: Bulanıklaştırmanın tam tersi olan bu işlem, kuralların birleştirilmesi sonucunda ortaya çıkan şekilden anlamlı bir sayısal ifade elde

edilmesidir. Eğri altında kalan alanın ağırlık merkezi sonuç değeri için yaygın olarak kullanılmaktadır (Buriboev ve ark.,2019; Şen, 2020).

Bulanık çıkarım yapılması adımında önce en küçükleme sonra en büyükleme (EK-EB) ya da önce çarpım sonra en büyükleme (Çarpım-EB) olmak üzere iki yöntem bulunmaktadır. Genel olarak girdi sayısının çok olduğu bulanık çıkarımlarda Çarpım-EB metodu tercih edilmemektedir. Çünkü üyelik dereceleri $0 \leq \mu \leq 1$ olduğundan bu sayıların çarpımları da çok küçük olacağından çıkarımın anlamlılığını olumsuz etkileyecektir. Ancak EK-EB yönteminde de en küçük üyelik derecesi dışında olan girdi üyelik dereceleri dikkate alınmamaktadır (Şen, 2020).

Durulaştırma yöntemi için çeşitli kurallar uygulanmaktadır. Literatürde kullanılan durulaştırma yöntemlerinden bazıları aşağıda verilmektedir.

- En Büyük Üyelik Kuralı: Yükseklik yöntemi olarak da adlandırılan bu yöntemin uygulanabilmesi için çıktı bulanık kümesinin tepe noktaları bulunmalıdır. Bu tepe noktalarından en yüksek olanı çıktı değer olarak kullanılır.
- Ortalama En Büyük Üyelik Kuralı: En büyük üyelik kuralına çok benzemektedir. Birden fazla en büyük üyelik derecesi olması durumunda bu değerlerin ortalaması alınır.
- Aritmetik Ortalama Kuralı: Çıktı bulanık kümesi *n* adet eşit aralığa bölünür. Her bir bulanık kümenin eşit ağırlığının olduğu kabul edilerek aritmetik durulaştırma işlemi yapılır.
- Ağırlıklı Ortalama Kuralı: Simetrik olan üyelik fonksiyonları için kullanılan bir yöntemdir. Üyelik dereceleri ağırlık katsayısı olarak kullanılarak durulaştırma yapılır.
- Ağırlık Merkezi Kuralı: Genellikle en çok tercih edilen yöntemdir. Ağırlık merkezi durulaştırma yöntemi için kullanılan formül aşağıdaki gibidir (Şen, 2020):

$$Z = \frac{\int \mu c(z) z dz}{\int \mu c(z) dz} \tag{9}$$

4.2.5.2. Tagaki-Sugeno Tipi BÇS

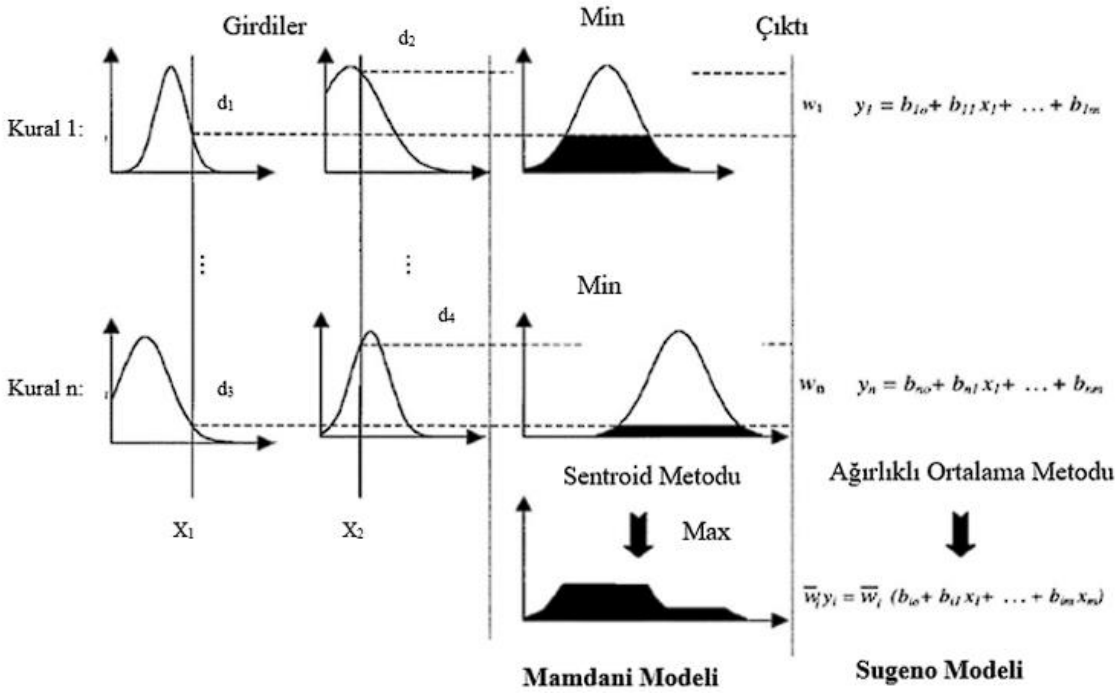
1985 yılında Takagi-Sugeno-Kang tarafından geliştirilen Takagi-Sugeno Modeli, çıktı değerinin bulanık küme olmadığı durumlarda kullanılmakta ve modelde bulanık sistemin çıktısı giriş değişkenlerinin bir fonksiyonu olarak temsil edilmektedir. Mamdani Modeli

işlem basamaklarının ilk 3 adımı bu model için de geçerlidir. Sugeno tipi bulanık modellemede çıktı üyelik fonksiyonları sadece lineer ya da sabit olabilmektedir. Girdileri 'G_1' ve 'G_2' olan ve Çıktısı 'Ç' olan bir bulanık kural için Tagaki-Sugeno modeli için örnek bir kural aşağıdaki gibi olacaktır:

Kural: Eğer G_1 'Çok Düşük' ise ve G_2 'Yüksek' ise Ç = f (G_1, G_2)

Yöntemde, üyelik dereceleri ağırlık olmak üzere ağırlıklı ortalama alınarak sonuç elde edilir (Alizadeh, 2012; Maués ve ark., 2019; Şen, 2020).

Bulanık sistemde tüm kurallar ve uygulanacak yöntemler belirlendikten sonra veriler, bulanık sistemde işlenerek bir çıktı değeri elde edilir. Daha sonra bulanık sistem kullanılarak veriler için daha önce yazılmış uygun kurallar üzerinden işlemler yapılır. Örneğin; Şekil 4.9'da X_1 ve X_2 verileri için daha önce yazılmış olan kurallar arasından bu verilerin içerisinde yer aldığı (Kural 1, … Kural n) üzerinden işlemler yapılır. X_1 verisinin kural 1'de ilgili fonksiyonu kestiği nokta değerine ait (d_1) üyelik derecesi ile X_2 verisinin kural 1'de ilgili fonksiyonu kestiği nokta değerine ait (d_2) üyelik derecesinin minimumları alınarak yamuk bulanık küme elde edilir. Aynı işlemler X_1 ve X_2 değerlerinin denk geldiği diğer bulanık n adet kural için de yapıldıktan sonra elde edilen yamuk çıktılar birleştirilerek sonuçta konveks ve normal olmayan bulanık yamuk model elde edilir (Şen, 2020).

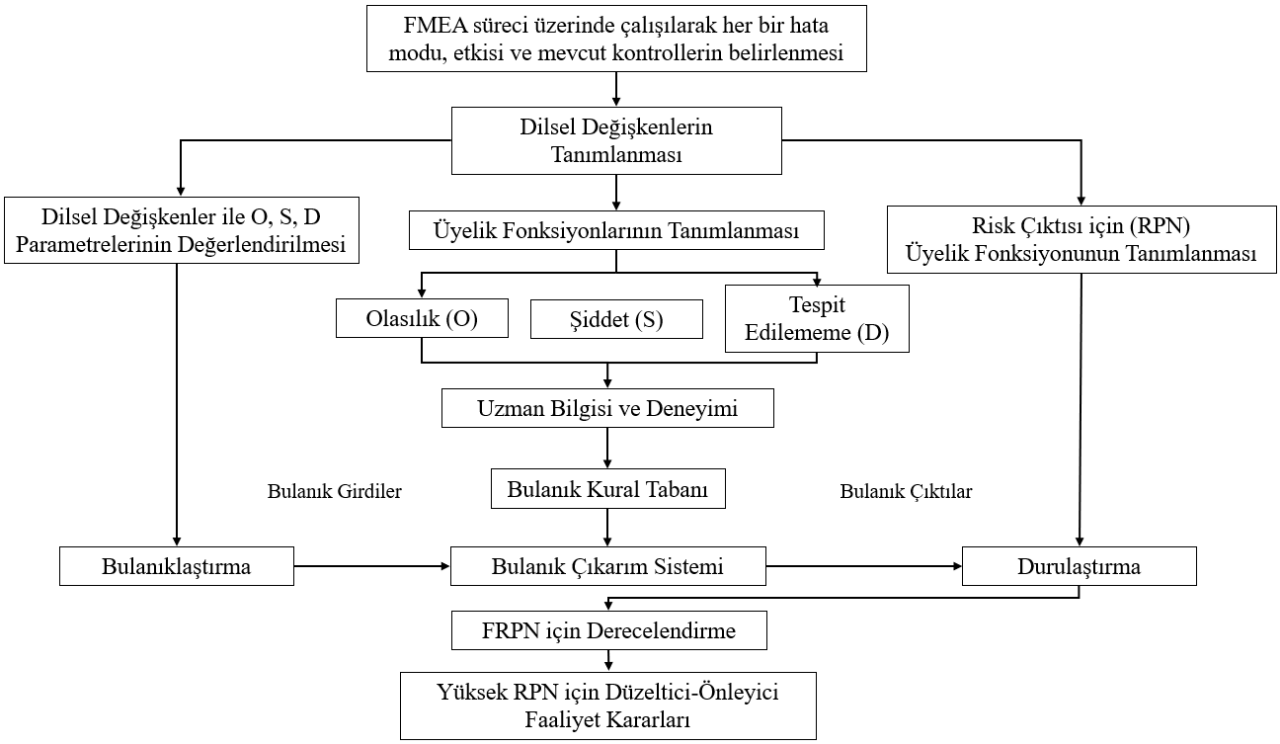


Şekil 4.9. Sırasıyla min (ve) ve max (veya) kullanan Mamdani ve Sugeno bulanık çıkarım sistemi (Buriboev ve ark., 2019).

4.2.6. Bulanık FMEA Prosesi

Bulanık FMEA, bilginin kesin olmadığı durumlarda girdi parametrelerini (O, S ve D değerleri) uygun üyelik fonksiyonları ile bulanıklaştırılarak ve 'Eğer-İse' kuralını kullanarak Klasik FMEA'nın dezavantajlarını minimize etmeyi sağlayan bilgi tabanlı bir yaklaşım tekniğidir (Balaraju ve ark., 2019).

Bulanık FMEA için proses akış şeması Şekil 4.10'daki gibi özetlenebilir:



Şekil 4.10. Bulanık FMEA Tekniği Prosesi (Chanamool ve ark., 2016; Balaraju ve ark., 2019).

Bulanık FMEA Prosesi için;

- Bulanık FMEA analizi yapılacak konu için uzman görüşleri ve önerileri yardımıyla hata modları ve potansiyel etkilerinin belirlenmesi gerekmektedir.
- Her bir girdi değişkeni için dilsel değişkenler tanımlanmalı ve bu parametrelerin üyelik fonksiyonları belirlenmelidir. Ayrıca bu aşamada RPN değeri için de üyelik fonksiyonu belirlenmelidir.
- Girdi değişken kombinasyonlarının tümünü kapsayacak şekilde üyelik fonksiyonları tanımlanmalıdır.
- Bulanık çıkarım sistemi kullanılarak durulaştırma işlemi yapılmalı ve FRPN değerleri önceliklendirilmelidir.
- Son olarak da yüksek RPN değerleri için düzeltici ya da önleyici faaliyetler önerilmelidir (Chanamool ve ark., 2016).

5. UYGULAMA

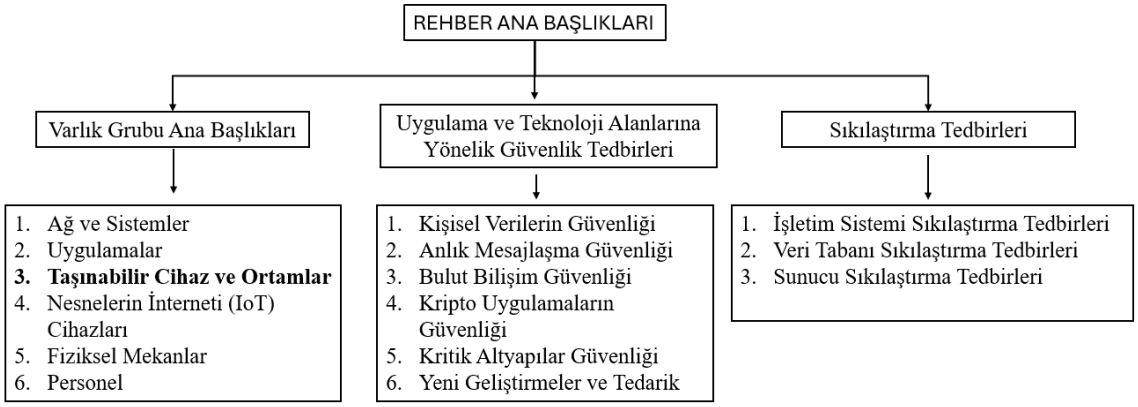
Kurumlarda, bilgi varlıklarının güvenliğinin sağlanması, korunması, yönetimi, belgelendirilmesi gibi işlemlerin başarılı bir şekilde sürdürülmesi için Uluslararası Standardizasyon Kuruluşu olan ISO tarafından ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardının 2005 yılında ilk sürümü yayınlanmıştır. Yıllar içerisinde gelişen teknoloji ve değişen gereksinimlerle birlikte standart, 2013 ve 2022 yıllarında revize edilmiştir. Standartta, bilgi varlıklarını korumak ve bu varlıklara yönelik riskleri belirlemek için genel bir çerçeve sunulmaktadır. Ayrıca ISO/IEC 27001'de belirtilen güvenlik gereksinimleri için öneriler sunmak adına ISO/IEC 27002 standardı geliştirilmiştir (ISO/IEC 27002, 2005; ISO/IEC 27001, 2024). Ancak her ne kadar ISO 27002'de BGYS gereksinimlerinin karşılanması için ISO 27001 detaylandırılmış olsa da varlık gruplarının ve kritiklik derecelerinin belirlenmesi, boşluk analizlerinin yapılması için yöntemlerin seçimi kurumlara bırakılmıştır.

Bilgi güvenliğine yönelik çalışmaların yıllar içinde öneminin anlaşılmasıyla birlikte bu çalışmalar geliştirilmeye ve detaylandırılmaya başlanmıştır. Bu noktada ülkemizde de 2020 yılında Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi hazırlanmıştır. Rehberde, kurumların bilgi ve iletişim güvenliğinde varlıkların kritiklik derecelerine göre alınması gereken genel tedbirler belirlenmiş, bu tedbirlerin uygulanabilirliğinin denetimi için de ayrıca bir denetim rehberi yayımlanmıştır (Bilgi ve İletişim Güvenliği Rehberi, 2020; Bilgi ve İletişim Güvenliği Denetim Rehberi, 2021).

Tez çalışması kapsamında 2020 yılında Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberinde yer alan Varlık Gruplarına Yönelik Güvenlik Tedbirleri ana başlıklarından biri olan 'Taşınabilir Cihaz ve Ortam Güvenliği' alt başlığı üzerinde çalışma yapılmıştır (Bilgi ve İletişim Güvenliği Rehberi, 2020).

Rehber; Varlık Gruplarına Yönelik Güvenlik Tedbirleri, Uygulama ve Teknoloji alanlarına Yönelik Güvenlik Tedbirleri ve Sıkılaştırma Tedbirleri olmak üzere 3 temel başlıktan oluşmaktadır. Şekil 5.1'de rehberde yer alan temel başlıklar ve alt grupları gösterilmektedir. Varlık grupları kendi içerisinde; Ağ ve Sistemler, Uygulamalar, Taşınabilir Cihaz ve Ortamlar, Nesnelerin İnterneti (IoT) Cihazları, Fiziksel Mekânlar ve

Personel olmak üzere 6 alt gruba ayrılmıştır. Diğer temel başlıklar da kendi içerisinde alt başlıklardan oluşmaktadır (Bilgi ve İletişim Güvenliği Rehberi, 2020).



Şekil 5.1. Bilgi Güvenliği Rehberi Ana Başlıkları (Bilgi ve İletişim Güvenliği Rehberi, 2020).

Rehbere göre öncelikle ilgili kurumdaki varlıklara göre varlık grupları belirlenmektedir. Belirlenen varlık gruplarına kritiklik düzeylerine göre çeşitli tedbir maddeleri yöneltilmektedir. Daha sonra bu varlık grupları için sırasıyla güvenlik ve sıkılaştırma tedbirlerinin uygulanabilirliği değerlendirilmektedir. Dolayısı ile ilk aşama varlık gruplarına yönelik çalışmanın yapılması olmaktadır. Çalışmada ilk aşamada yer alan varlık gruplarına yönelik güvenlik tedbir maddeleri kullanılmıştır.

Uygulama yapılan kurumda, varlık grupları içerisinden Taşınabilir Cihaz ve Ortam Güvenliği alt başlığının seçilme nedenlerinin başında;

- Tüm kurum çalışanlarının taşınabilir cihazları ve ortamları (taşınabilir bilgisayarlar, taşınabilir depolama aygıtları, harici diskler, usb bellekler vb.) günlük iş süreçlerinde aktif olarak kullanıyor olması, yani varlık sayısının oldukça fazla olması,
- Veri ve sistemlere uzaktan erilebilmek amacıyla uzaktan çalışma durumlarında akıllı kartların (taşınabilir ortam) kullanılması,
- Taşınabilir Cihaz ve Ortamlara bağımlı varlık gruplarının ve varlıkların sayısının ve kritikliğinin diğerlerine göre yüksek olması önemli olmaktadır.

Varlık sayısının fazlalığı varlıkların güvenliklerinin kontrol edilebilirliğini de oldukça zorlamaktadır. Bu kullanımlardan doğabilecek güvenlik zafiyetlerinin iyi anlaşılıp

önlenebilmesi için uzmanların görüşleri de dikkate alınarak ilgili konu başlığında çalışma yapılmasına öncelik verilmiştir.

Uzman görüşleri ve literatür örnekleri kullanılarak yapılan bu çalışma için Bulanık FMEA yöntemi kullanılmıştır. Rehberde, Şekil 5.1'de gösterilen her bir alt başlık için gerekli olan güvenlik tedbirleri yer almaktadır. Hata modları belirlenirken, Taşınabilir Cihaz ve Ortam Güvenliği Başlığında yer alan güvenlik tedbirleri incelenerek çalışma yapılan kurum için uygulanabilir olan 21 adet hata modu seçilmiştir. Bkz. Ek-1 Hata Modları Anket Listesi.

Çalışma, bir kurumdaki ISO 27001 BGYS Ekip üyeleri ile yürütülmüştür. Üyeler, dış denetimi gerçekleştirilen ISO 27001 BG denetimi kapsamında gereksinimler için çalışmalar yapmakta ve ek olarak CBDDO Bilgi Güvenliği İç Denetim Çalışmasını yürütmektedirler. Ekipte yer alan; 2 üye kıdemli uzman, 3 üye uzman ve 2 üye de uzman yardımcısı unvanına sahiptir. Ekip üyeleri içerisinde 4 kişi bilgisayar mühendisi, 2 kişi elektrik-elektronik mühendisi, 1 kişi ise endüstri mühendisidir. Uzmanların ekiple birlikte çalışma süresi minimum 2 yıldır. Ekip üyelerinin unvanlarının çeşitliliği ve bilgi güvenliği konusunda farklı tecrübe düzeylerine sahip olması analizde de değişkenlerin yorumlanması konusunda çeşitlilik meydana getirmiştir.

Hata modlarının olasılık, şiddet ve tespit edileme parametrelerinin yüksek olması durumunda güvenlik zafiyetleri ortaya çıkma ihtimali artmaktadır. Aşağıda, çalışmada seçilen hata modlarına yönelik O, S, D değerlerinin yüksek olması durumunda doğabilecek zafiyetlerden bazıları örneklendirilmiştir:

- Kritik verilere erişen cihazlara ait kullanım politikasının olmaması ya da olması halinde de çalışanlara gerektiği şekilde tebliğ edilmemesi durumunda; çalışanların eriştikleri kritik verilerin işlenmesi, korunması gibi talimatları gerektiği şekilde uygulayamaması durumu ortaya çıkabilir. Bunun sonucunda da veri sızıntıları, veri güvenliği zafiyetleri, verilerin yetkisiz kişilerin kullanımına geçmesi durumları ile karşı karşıya kalınabilir. Yani bilgi güvenliğinin; gizlilik, bütünlük, erişilebilirlik unsurlarından en az biri zarar görebilir.
- Kritik verilerin zarar görmeleri sonucunda kurum itibarı olumsuz etkilenir, bu durum hukuki yükümlülüklerin artmasına sebep olabilir.
- Bilgi güvenliği unsurlarındaki eksiklikler, süreçlerin kesintiye uğramasına sebebiyet verebilir. Süreçteki aksamalar sonucunda çeşitli cezai yaptırımlar ortaya çıkabilir.

- Çalışanların bilgi güvenliği konusunda yeterli bilgi sahibi olmaması durumunda, çalışanlar bilinçsiz bir şekilde riskli davranışlarda bulunabilir, bunun sonucu yukarıda belirtilen bir dizi olumsuzlukları beraberinde getirebilir.
- Cihazlara gerekli yazılım kurulum kısıtlarının getirilmemesi durumunda da kötücül yazılımlarının yayılma riski artmaktadır. Bu da en küçüğü sistem performansının düşmesi olmak üzere beraberinde birçok sorunu getirmektedir.
- Yazılım kurulum kısıtları haricinde cihazlar için gerekli güvenlik yazılımlarının yüklenmemesi durumunda da cihazlar zararlı yazılımlara karşı açık hale gelmektedir (Eminağaoğlu ve Gökşen, 2009; Bilgi ve İletişim Güvenliği Rehberi, 2020).

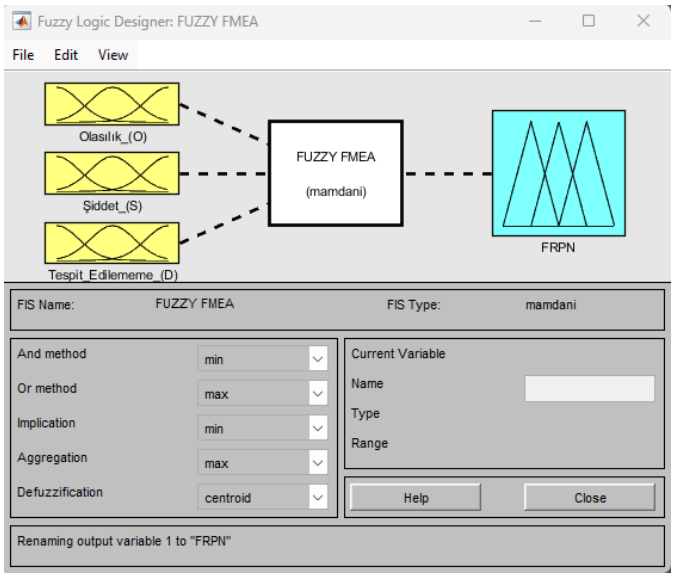
Bu gibi zafiyetlerin önlenebilmesi ya da etkisinin minimize edilebilmesi için mevcut durum risk analizleri doğru bir şekilde yapılmalı ve yorumlanmalıdır.

Çalışmada önce klasik RPN hesaplaması yapılmıştır. Karar vericilerden RPN risk puanı için 'Çok Düşük', 'Düşük', 'Orta', 'Yüksek' ve 'Çok Yüksek' olmak üzere 5'li ölçekte bir değerlendirme yapmaları istenilmiştir. Bu risk puanı aralıkları tüm olasılıkları içerecek şekilde Çizelge 5.5'te gösterildiği şekilde renklendirilmiştir.

Çalışmada, Matlab paket programı (Versiyon: MatlabR2024a) içerisindeki Bulanık Mantık (Fuzzy Logic) Modülü kullanılmıştır. Şekil 5.2'de Matlab Fuzzy Logic Designer Fuzzy FMEA Modülü arayüzü gösterilmektedir.

Uygulanan Bulanık FMEA temel olarak;

- Olasılık, Şiddet ve Tespit Edilememe olmak üzere üç girdi değişkeninden,
- Girdi değişkenlerini üyelik dereceleriyle birlikte dönüştüren bulanıklaştırma arayüzünden,
- Birçok sayıda Eğer-İse kuralını içeren kural tabanından ve
- Bulanık sonuçların çıktısını içeren arayüzden oluşmaktadır.



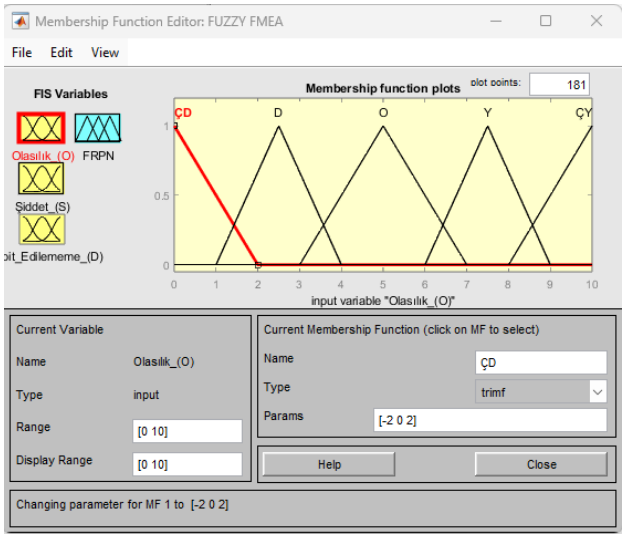
Şekil 5.2. Matlab Fuzzy Logic Designer Fuzzy FMEA Modülü

Tespit edilebilirlik arttıkça risk azalacağından bu tanım için 'Tespit Edilememe' ifadesi kullanılmıştır. Dolayısı ile olasılık, şiddet değerlerinde olduğu gibi tespit edilememe değeri düşük ise risk de düşük olacaktır.

Çalışmada girdi ve çıktı değişkenlerinin tümünün bulanık sayı olması sebebiyle Mamdani Tipi bulanık çıkarım sistemi kullanılmıştır. Bulanık çıkarım yapılırken girdi parametreleri arasından en küçük olan üyelik derecelerinin belirleyici olması istendiğinden ve girdi parametre sayısının nispeten çok olduğu düşünüldüğünden Çarpım-EB metodu yerine EK-EB metodu kullanılmıştır. Durulaştırma aşamasında en yaygın kullanıma sahip olan ve fizik bakımından da anlamlı olan ağırlık merkezi (sentroid) metodu kullanılmıştır.

Girdi arayüzünde, her bir girdi için bulanıklaştırma işlemi yapılırken üyelik fonksiyonlarının tipi ve parametre değerleri belirlenmektedir. Kesin değerler, bu aşamada bulanık değerlere dönüştürülerek işlenmektedir. Doğru üyelik fonksiyonlarının belirlenmesi, bulanıklaştırma aşamasında kritik bir faktör olarak öne çıkmaktadır. Bu aşamada üyelik fonksiyonu seçiminde en çok tercih edilen fonksiyonlardan biri olan üçgen üyelik fonksiyonu tercih edilmiştir. Üyelik derecesi 1'e eşit olan öz değerinin 1 adet olması istenildiğinden bu üyelik fonksiyonu seçilmiştir. Bu tercih karar vericilerin inisiyatifinde olup fonksiyonun tepe noktasının birden fazla istenilmesi durumunda yamuk üyelik fonksiyonu da seçilebilirdi. O, S ve D değerlerinin 1-10 arasında olması yani dar bir aralıkta olması bu seçimde etkili olmuştur. Alt aralıklardaki geçiş değerlerinin birbirine tam olarak teğet olmaması, üyelik fonksiyonundaki geçişlerin daha uzlaştırıcı bir çözüm sunmasını sağlamaktadır. Şekil 5.3'te Matlab bulanık mantık arayüzünde 5

dilsel ölçekten biri olan olasılık girdisine ait ‘Çok Düşük (ÇD)’ seviyesi için parametreler gösterilmektedir.



Şekil 5.3. Matlab Bulanık Mantık Girdi Arayüzü – Olasılık (O) girdisine ait ‘Çok Düşük (ÇD)’ seviyesi için parametrelerin gösterimi

Karar vericilerin öznel değerlendirmeleri ile olasılık, şiddet ve tespit edilememe parametreleri ile bulanık değerlendirme yapılabilmesi için öncesinde belirli dilsel değişkenler kullanılarak parametrelerin her biri için bulanık aralıklar belirlenmelidir. Çeşitli ölçeklendirme kılavuzları mevcuttur ve bu makalede önerilen modelde dilsel değişkenlerin seçiminde; Xu ve ark., (2002); Mandal (2014); Silva ve ark., (2014); Chanamool ve ark., (2016) örnek olmak üzere literatür incelenmiş olup her bir girdiye ait genellikle 5 farklı ya da 10 farklı dilsel ölçeklerin kullanıldığı görülmüştür. Bu tez çalışmasında O, S ve D parametreleri için karar vericilerden daha hassas değerlendirme yapılabilmesi için 10’lu dilsel ölçekte değerlendirme yapmaları istenilmiştir, dolayısı ile üyelik fonksiyonu için girdi değerleri 1-10 arası puanlanmıştır. Puanlama yapılırken kullanılan açıklamalar için yine ilgili literatür örnekleri kullanılmıştır. Sonrasında ise Chanamool ve ark. (2016) çalışmasında uygulandığı şekilde bu dilsel değişkenler; 1=Çok Düşük (ÇD), 2-3= Düşük (D), 4-6= Orta (O), 7-8= Yüksek (Y) ve 9-10= Çok Yüksek (ÇY) olacak şekilde 5 seviyede gruplanmıştır. Ek 2’de anket puanları ve açıklamaları detaylı olarak gösterilmektedir. Bulanık kuralların belirlenmesi aşamasında her bir parametre için tüm dilsel değişken değerlerinin kombinasyonlarının yazılması gerekmektedir. Her parametre için 10 dilsel seviyenin olması durumunda kombinasyon 10^3 olacaktır ki bu da 1000 adet bulanık kural yazılması anlamına gelmektedir. Ancak bu çalışmada 1000 adet kuralın yazılması durumu risk puanlarının yayılımı dikkate

alındığında çok anlamlı olmamaktadır. Bu yüzden dilsel değişkenler 5 seviyede gruplanmıştır. Dolayısı ile sonuçta 5^3=125 adet kural tanımlanmıştır.

7 karar vericiden alınan olasılık, şiddet ve tespit edilememe girdi değerleri için ortak tekil değer elde edilirken merkezi eğilim ölçülerinden medyan kullanılmıştır. Medyan dışında sıklıkla kullanılan bir diğer yöntem olan geometrik ortalamanın tercih edilmemesinin nedeni uzmanların bazı hata modları için çekimser kalıp boş bıraktıkları anket değerleri bulunmasından dolayıdır.

Girdilere ait üyelik fonksiyonları aşağıda gösterilmektedir:

$$\mu(O,S,D)_{\text{ÇD}} = \begin{cases} \frac{x+2}{2}, & -2 \le x \le 0 \\ \frac{2-x}{2}, & 0 \le x \le 2 \\ 0, & x < -2; x > 2 \end{cases}$$

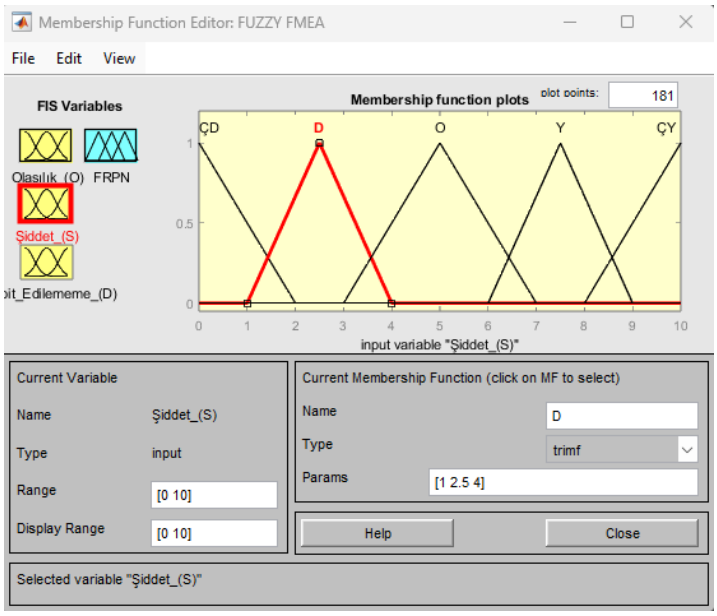
$$\mu(O,S,D)_{\text{D}} = \begin{cases} \frac{x-1}{1,5}, & 1 \le x \le 2,5 \\ \frac{4-x}{1,5}, & 2,5 \le x \le 4 \\ 0, & x < 1; x > 4 \end{cases}$$

$$\mu(O,S,D)_{\text{O}} = \begin{cases} \frac{x-3}{2}, & 3 \le x \le 5 \\ \frac{7-x}{2}, & 5 \le x \le 7 \\ 0, & x < 3; x > 7 \end{cases}$$

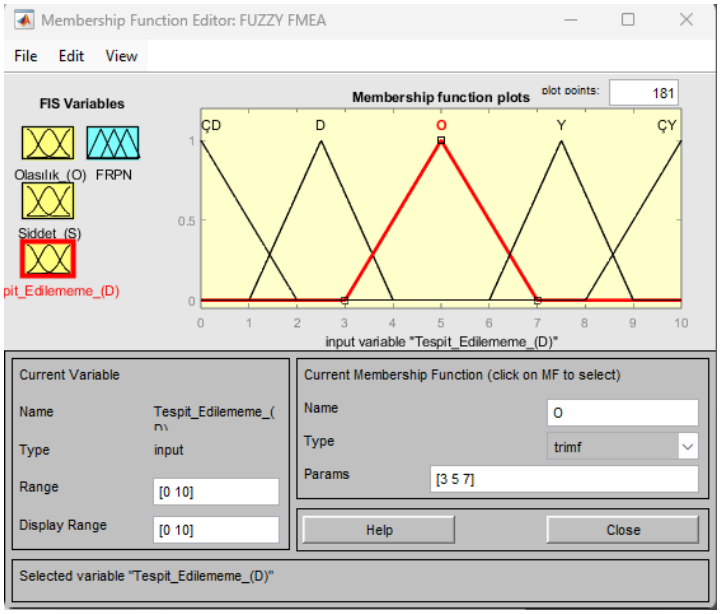
$$\mu(O,S,D)_{\text{Y}} = \begin{cases} \frac{x-6}{1,5}, & 6 \le x \le 7,5 \\ \frac{9-x}{1,5}, & 7,5 \le x \le 9 \\ 0, & x < 6; x > 9 \end{cases}$$

$$\mu(O,S,D)_{\text{ÇY}} = \begin{cases} \frac{x-8}{2}, & 8 \le x \le 10 \\ \frac{12-x}{2}, & 10 \le x \le 12 \\ 0, & x < 8; x > 12 \end{cases}$$

Girdilere ait üyelik fonksiyonlarında yer alan değerler Matlab bulanık mantık arayüzünde tanımlanmıştır. Şekil 5.4 ve Şekil 5.5'te sırasıyla şiddet girdisine ait düşük seviye ve tespit edilememe girdisine ait orta seviye için parametreler gösterilmektedir.



Şekil 5.4. Şiddet (S) girdisine ait 'Düşük (D)' seviyesi için parametrelerin gösterimi.



Şekil 5.5. Tespit Edilememe (D) girdisine ait 'Orta (O)' seviyesi için parametrelerin gösterimi.

Girdilere ait parametreler, değer aralıkları, üyelik fonksiyonu tipi vb. belirlendikten sonra çıktı fonksiyonuna ait değerler girilmiştir.

Literatür örnekleri incelendiğinde çıktı parametresi için de tıpkı girdi parametrelerinde olduğu gibi 5'li ya da 10'lu ölçeklerin kullanıldığı görülmüştür. Çalışma özelinde, 10'lu ölçek için risk puanları için dilsel tanımlamaların çok dar aralıklar içerdiğinden risk aralıklarını iyi temsil etmediği düşünülmüştür ve 5'li ölçek ile değerlendirme yapılmıştır.

Bulanık aralıklar girdi parametrelerinde olduğu gibi Çok Düşük(ÇD), Düşük(D), Orta(O), Yüksek(Y) ve Çok Yüksek (ÇY) olmak üzere kategorize edilmiştir. Karar vericiler risk aralıklarını, RPN değerindeki yığılmaları göz önüne alarak belirlemişlerdir. RPN değerleri öncesinde klasik bir risk analizi çalışması için yaklaşık risk puanı sınırları Çizelge 5.1'deki gibi belirlenmiştir:

Çizelge 5.1. RPN İçin Belirlenen Değer Aralıkları ve Hata Modu Frekans Değerleri

Klasik FMEA için RPN Değer Aralıkları							
Alt Sınır				**Üst Sınır**	**Tanım**	**Kısaltma**	**Frekans**
0	<=	RPN Değeri	<	20	Çok Düşük	ÇD	7
20	<=	RPN Değeri	<	40	Düşük	D	4
40	<=	RPN Değeri	<	80	Orta	O	5
80	<=	RPN Değeri	<	100	Yüksek	Y	3
100	<=	RPN Değeri	<	200	Çok Yüksek	ÇY	2

Ancak bu çalışmada RPN frekans dağılımları bu aralıkta istenilen sonucu vermemektedir. Çünkü karar vericiler hata modları RPN değerlerini yorumlarken hesaplanmış olan risk puanlarına bağlı olarak risk puanlarının 'Orta' derecede riskler çevresinde yığılması gerektiğini vurgulamışlardır.

Çizelge 5.1'de hata modlarının küçükten büyüğe sıralanmış şekilde RPN değerleri verilmektedir ve bu değerlerin tekrar sayıları gösterilmektedir. 21 hata modu için hesaplanan 21 RPN değerinin medyan değeri 36'dır. RPN değerleri için yığılmalar ve karar vericilerin yorumları doğrultusunda yeni aralıklar belirlenmiştir.

Yaklaşık risk puanlarının sınırlandırılması ileride yapılacak olan uygun bulanık aralıkların belirlenmesi için belirleyici olmuştur. Dolayısı ile yeni aralıklar belirlenirken değerler arasında simetrik fark olmasına dikkat etmek yerine verilerin nerelerde yığılma gösterdiği ve karar vericilerin hangi risk düzeylerini kabul edilebilir düzey olduğu kararı etkili olmuştur. Daha sonra yeni aralıklar Çizelge 5.2'deki gibi güncellenmiştir:

Çizelge 5.2.Yeni RPN Değer Aralıkları

Klasik FMEA için RPN Değer Aralıkları							
Alt Sınır				**Üst Sınır**	**Tanım**	**Kısaltma**	**Frekans**
10	<=	RPN Değeri	<	18	Çok Düşük	ÇD	4
18	<=	RPN Değeri	<	40	Düşük	D	7
40	<=	RPN Değeri	<	84	Orta	O	5
84	<=	RPN Değeri	<	126	Yüksek	Y	3
126	<=	RPN Değeri	<	200	Çok Yüksek	ÇY	2

İstenilen çan eğrisine yakın yığılma görüntüsü böylece elde edilmiş olmaktadır yani en çok tekrar eden değerler orta risk düzeyine doğrudur ve bulanık çıktı değer aralıkları belirlenirken yukarıdaki tabloya benzer aralıklar bulanıklaştırılmıştır. Örneğin 18-40 değer aralıkları Çizelge 5.2'de belirtildiğine göre düşük risk düzeyi tanımına dâhil olmasına rağmen bu aralıkta yığılma 35 RPN değerinden sonra olmaktadır. Klasik FMEA yapıldığında, 'düşük' seviye risk grubuna dâhil edilmiş olan 18-40 aralığında yer alan RPN değerleri, bulanık FMEA yapıldığında hem 'düşük' seviye hem de 'orta' seviyeli risk tanımlamasına üye olacaktır. Ayrıca RPN değerlerindeki yığılmanın 35 RPN değeri sonrasında olduğu göz önüne alınarak bu puanlar 'orta' seviyeli risk tanımlamasında daha yüksek üyelik derecesine sahip olacak ve bu durumda net sınırlar yerine bulanık sınırlar belirlenmiş olacaktır.

Çizelge 5.2'de yer alan alt ve üst sınır değerleri aynı zamanda hesaplanmış olan RPN değerleridir. Bunun sebebi sınır değerlerin bir alt ve bir üst sınırlara dâhil edilmesini kolaylaştırmak içindir. Böylece örneğin, 18 RPN değeri hem 'ÇD' hem de 'D' risk seviyesine üye olacaktır.

Çıktı için üçgen üyelik fonksiyonları:

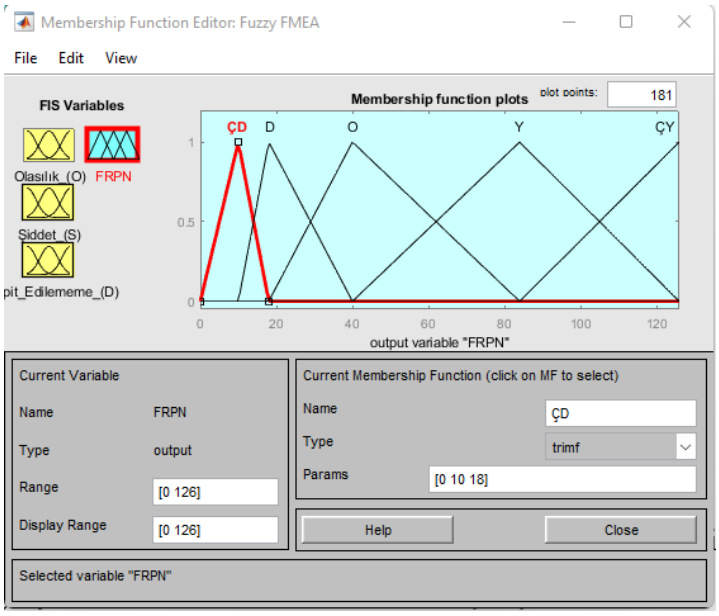
$$\mu(O,S,D)_{\text{ÇD}} = \begin{cases} \frac{x}{10}, & 0 \le x \le 10 \\ \frac{18-x}{8}, & 10 \le x \le 18 \\ 0, & x < 0; x > 18 \end{cases}$$

$$\mu(O,S,D)_{\text{D}} = \begin{cases} \frac{x-10}{8}, & 10 \le x \le 18 \\ \frac{40-x}{22}, & 18 \le x \le 40 \\ 0, & x < 10; x > 40 \end{cases}$$

$$\mu(O,S,D)_{\text{O}} = \begin{cases} \frac{x-18}{22}, & 18 \le x \le 40 \\ \frac{84-x}{44}, & 40 \le x \le 84 \\ 0, & x < 0; x > 18 \end{cases}$$

$$\mu(O,S,D)_{\text{Y}} = \begin{cases} \frac{x-40}{44}, & 40 \le x \le 84 \\ \frac{126-x}{42}, & 84 \le x \le 126 \\ 0, & x < 40; x > 126 \end{cases}$$

$$\mu(O,S,D)_{\text{ÇY}} = \begin{cases} \frac{x-84}{42}, & 84 \le x \le 126 \\ \frac{200-x}{74}, & 126 \le x \le 200 \\ 0, & x < 84; x > 200 \end{cases}$$



Şekil 5.6. Çıktı Değişkenine Ait Üyelik Fonksiyonu

Matlab programına çıktı değişkenine ait parametrelerin girilmesiyle Şekil 5.6.'daki gibi simetrik olmayan üçgen üyelik fonksiyonları oluşturulmuştur.

Kural tabanının oluşturulduğu modül ise Şekil 5.7'de gösterilmiştir. Bu modülde, birçok Eğer-İse kuralı belirlenebilmektedir. Çalışmada her bir girdi için 5 seviye bulunduğundan 5^3=125 adet bulanık kural belirlenmiştir. En uygun olan kuralların bulunması, modelin başarısını artıracak en önemli unsurlardan biri olmaktadır. Tüm bulanık kurallar Ek 3'te gösterilmektedir.

Kural tabanı oluşturulurken doğru kuralın yazılması oldukça önemlidir. Çalışmanın en başında, girdi parametrelerinin dilsel değişken sayısının 10'lu ölçekte yazıldıktan sonra bulanık dilsel aralıklarının 5'li ölçekte hesaplamaların yapılması durumu karışıklığa sebep olabilmektedir. Bu karışıklığı önlemek için karar vericilerin puanlarının 5'li ölçek için gruplandırılmış değerlerinin geometrik ortalamaları kullanılmıştır. Bu aşamada karar vericilere ait puanların aritmetik ortalama değerleri ile geometrik ortalama değerleri neredeyse aynı sonucu vermekteydi. İki puanlama sistemi de tamamen karar vericiye yardımcı olmak amacıyla kullanıldığından ve sonuçlarda bu işlem özelinde anlamlı bir fark olmadığından tercihen çok büyük ve çok küçük sayılardan etkilenmeyen geometrik ortalama değerlerinden yararlanılmıştır. Çizelge 5.3'te karar vericilerin puanlarının aritmetik ve geometrik ortalamaları gösterilmektedir.

Çizelge 5.3. Karar Vericilerin Puanlarının Aritmetik Ortalama ve Geometrik Ortalama Değerleri

Karar Vericilerin Puanları (KVP)	5'li Ölçekte Karşılıkları	5'li Ölçekte Dilsel Tanımları	KVP Aritmetik Ortalama Değerleri	KVP Geometrik Ortalama Değerleri
1	1	ÇD	1,00	1,00
2	2	D	2,50	2,44
3				
4	3	O	5,00	4,93
5				
6				
7	4	Y	7,50	7,48
8				
9	5	ÇY	9,50	9,48
10				

Karar vericilerin puanlarının geometrik ortalamalarından yararlanılarak tüm ihtimaller için RPN hesaplaması yapılmış ve çıkan sonuçlar bulanık kuralların belirlenmesinde belirleyici olmuştur. Çizelge 5.4'te ilk 35 kural için bu değerlendirme gösterilmektedir.

Çizelge 5.4. İlk 35 Kural için Örnek RPN değerlendirmeleri

Kural No	O	S	D	RPN
1	1,0	1,0	1,0	1,00
2	1,0	1,0	2,4	2,40
3	1,0	1,0	5,0	5,00
4	1,0	1,0	7,5	7,50
5	1,0	1,0	9,5	9,50
6	1,0	2,4	1,0	2,40
7	1,0	2,4	2,4	5,76
8	1,0	2,4	5,0	12,00
9	1,0	2,4	7,5	18,00
10	1,0	2,4	9,5	22,80
11	1,0	5,0	1,0	5,00
12	1,0	5,0	2,4	12,00
13	1,0	5,0	5,0	25,00
14	1,0	5,0	7,5	37,50
15	1,0	5,0	9,5	47,50
16	1,0	7,5	1,0	7,50
17	1,0	7,5	2,4	18,00
18	1,0	7,5	5,0	37,50
19	1,0	7,5	7,5	56,25
20	1,0	7,5	9,5	71,25

Çizelge 5.4. İlk 35 Kural için Örnek RPN değerlendirmeleri (devamı)

Kural No	O	S	D	RPN
21	1,0	9,5	1,0	9,50
22	1,0	9,5	2,4	22,80
23	1,0	9,5	5,0	47,50
24	1,0	9,5	7,5	71,25
25	1,0	9,5	9,5	90,25
26	2,4	1,0	1,0	2,40
27	2,4	1,0	2,4	5,76
28	2,4	1,0	5,0	12,00
29	2,4	1,0	7,5	18,00
30	2,4	1,0	9,5	22,80
31	2,4	2,4	1,0	5,76
32	2,4	2,4	2,4	13,82
33	2,4	2,4	5,0	28,80
34	2,4	2,4	7,5	43,20
35	2,4	2,4	9,5	54,72

Çizelge 5.4'teki renklendirmeler için tüm O*S*D değerleri için renklendirilmiş RPN matrisi kullanılmıştır. Bu matris Çizelge 5.5'te gösterilmektedir. Olasılık, şiddet ve tespit edilememe girdilerinin tüm değerleri için renklendirilen matrisin oluşturulmasında 3 girdi parametresi iki boyutta gösterileceği için matris iki aşamada oluşturulmuştur. İlk aşamada olasılık ve tespit edilememe girdileri için bir matris oluşturulmuştur. Bu çalışma özelinde, karar vericilerden alınan olasılık girdisine ait tüm değerler 1-3 puanları arasında olduğu için olasılık değerleri için bu değer aralıkları kullanılmış olup şiddet ve tespit edilememe için böyle bir kısıtlama yapılmamıştır ve 1-10 arası tüm puanlar yazılmıştır.

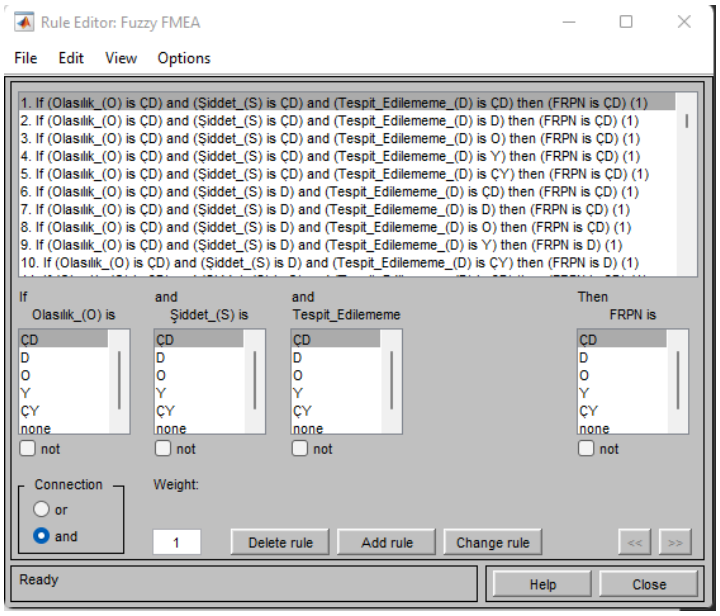
Çizelge 5.5. Risk Puanlarına göre renklendirilmiş RPN matrisi

O*D		TESPİT EDİLEMEME									
		1	2	3	4	5	6	7	8	9	10
OLASILIK	1	1	2	3	4	5	6	7	8	9	10
	2	2	4	6	8	10	12	14	16	18	20
	3	3	6	9	12	15	18	21	24	27	30

O*S*D		ŞİDDET									
		1	2	3	4	5	6	7	8	9	10
OLASILIK* TESPİT EDİLEBİLİRLİK	1	1	2	3	4	5	6	7	8	9	10
	2	2	4	6	8	10	12	14	16	18	20
	3	3	6	9	12	15	18	21	24	27	30
	4	4	8	12	16	20	24	28	32	36	40
	5	5	10	15	20	25	30	35	40	45	50
	6	6	12	18	24	30	36	42	48	54	60
	8	8	16	24	32	40	48	56	64	72	80
	9	9	18	27	36	45	54	63	72	81	90
	10	10	20	30	40	50	60	70	80	90	100
	12	12	24	36	48	60	72	84	96	108	120
	14	14	28	42	56	70	84	98	112	126	140
	15	15	30	45	60	75	90	105	120	135	150
	16	16	32	48	64	80	96	112	128	144	160
	18	18	36	54	72	90	108	126	144	162	180
	20	20	40	60	80	100	120	140	160	180	200
	21	21	42	63	84	105	126	147	168	189	210
	24	24	48	72	96	120	144	168	192	216	240
	27	27	54	81	108	135	162	189	216	243	270
	30	30	60	90	120	150	180	210	240	270	300

Sonuçta; Çizelge 5.5'te yer alan maksimum O*S*D değeri 10*10*10=1000 yerine 3*10*10=300 olarak yazılmıştır.

Kuralların oluşturulması aşamasında ise hesaplanan yaklaşık değerler ile birlikte karar vericilerin subjektif değerlendirmelerinden yararlanılmıştır ve her bir kural için ortak tek bir sonuç elde edilerek bu değerler Şekil 5.7'de gösterildiği şekilde kural düzenleyici arayüzüne girilmiştir.



Şekil 5.7. Kural Tabanının Oluşturulması

Şekil 5.7'de ilk 10 kural Matlab kural düzenleyici arayüzünde gösterilmektedir. Kural tabanı oluşturulurken belirlenmiş olan 125 adet kural 'Kural Belirleyici' modülüne birer birer girilmiş ve kurallar 've' operatörü ile birleştirilmiştir.

Örneğin;

8. Kural: Olasılık(O) 'Çok Düşük' ve Şiddet (S) 'Düşük' ve Tespit Edilememe(D) 'Orta ise Risk 'Çok Düşük' olmaktadır.

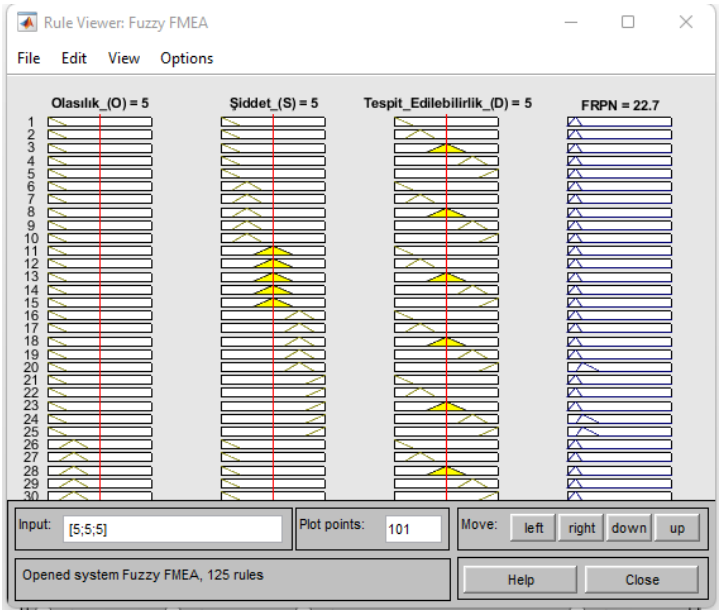
17. Kural: Olasılık(O) 'Çok Düşük' ve Şiddet (S) 'Yüksek' ve Tespit Edilememe(D) 'Düşük' ise Risk 'Düşük' olmaktadır.

39. Kural: Olasılık(O) 'Düşük' ve Şiddet (S) 'Orta' ve Tespit Edilememe(D) 'Yüksek' ise Risk 'Yüksek' olmaktadır.

55. Kural: Olasılık(O) 'Orta' ve Şiddet (S) 'Düşük' ve Tespit Edilememe(D) 'Çok Yüksek' ise Risk 'Orta' olmaktadır.

93. Kural: Olasılık(O) 'Yüksek' ve Şiddet (S) 'Yüksek' ve Tespit Edilememe(D) 'Orta ise Risk 'Çok Yüksek' olmaktadır.

Tüm bulanık kurallar belirlendikten sonra Mamdani bulanık çıkarım sisteminin son aşaması olan durulaştırma işlemi yapılmıştır. Durulaştırma işlemi için Şekil 5.8'de gösterilen 'Kural Görüntüleyici' arayüzü kullanılmıştır. Girdi değerlerinin yazılması gereken bölüme, FRPN değeri hesaplanılması istenen hata modunun girdilerinin medyan değerleri girilerek en başta kural tanımlama arayüzünde belirlenen hesaplama metodu kullanılarak (bu çalışma için sentroid) durulaştırma işlemi gerçekleştirilmiştir.



Şekil 5.8. Matlab Kural Görüntüleyici Arayüzü

Şekil 5.9. Bulanık Mantık Sonuç Ekranı- Hata modu 21 için FRPN değeri.

Şekil 5.9.'de gösterilen hata modu 21 için girdi değerleri (3,8,3) iken FRPN=47,9 olarak hesaplanmıştır. Bu şekilde her bir hata modu için FRPN değerleri hesaplanmış ve Çizelge 5.6'da anket sonuç değerleri gösterilmiştir.

Çizelge 5.6 Anket Sonuçları

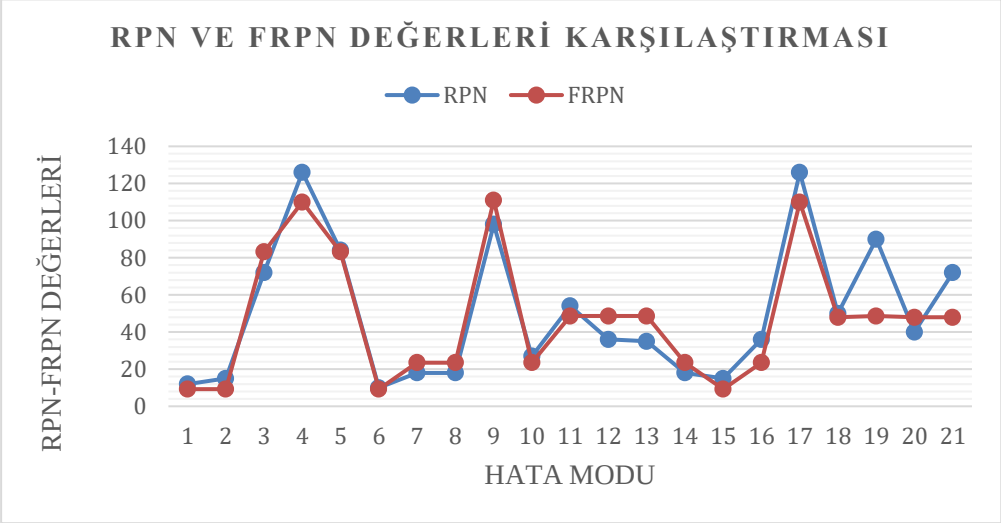
Hata Modu No	MEDYAN			RPN	FRPN
	O	S	D		
1	1	4	3	12	9,24
2	1	5	3	15	9,24
3	2	9	4	72	83,20
4	2	9	7	126	110,00
5	3	7	4	84	83,20
6	1	10	1	10	9,24
7	1	9	2	18	23,50
8	2	9	1	18	23,50
9	2	7	7	98	111,00
10	1	9	3	27	23,50
11	2	9	3	54	48,60
12	2	9	2	36	48,60
13	1	10	4	35	48,60
14	1	9	2	18	23,50
15	1	6	3	15	9,24
16	2	6	3	36	23,50
17	2	9	7	126	110,00
18	2	5	5	50	47,90
19	3	6	5	90	48,60
20	2	10	2	40	47,90
21	3	8	3	72	47,90

Elde edilen FRPN değerlerinin hesaplanmasında, karar vericilerin görüşleri ve Çizelge 5.4'te yapılan hesaplamalar yardımıyla yazılan bulanık kurallar belirleyici olmuştur. Yazılmış olan 125 adet bulanık kuralın çıktı değerlerinin değiştirilmesiyle sonuçların da değiştiği gözlemlenmiştir, sonuçta uygun kurallar Ek 3'teki gibi belirlenmiştir.

Çizelge 5.4'teki sonuçlara bakıldığında örneğin, 18. ve 19. hata modlarında klasik RPN değeri üç girdi değişkeninin çarpımı olarak hesaplandığından 18. ve 19. hata modlarına ait RPN değerleri arasındaki fark oldukça fazladır. Ancak FRPN değerlerine bakıldığında ise bu puanların birbirlerine çok yakın olduğu görülmüştür. Bunun sebebi ise bulanık değer aralıklarının 2-3 = Düşük, 4-5-6 = Orta seviye olarak belirlenmesinden ve bulanık kuralların yazılırken 18. ve 19. hata modlarına ait girdi değerlerinin aynı seviyeye denk gelmesinden ve yazılan bulanık kurallar ile de benzer aralıklarda olan bu girdi değerlerinin yine sonuçta benzer çıktı aralıklarına denk gelmesinden kaynaklanmaktadır.

Aralarındaki ufak fark ise bu değerlerin aralıktaki üyelik derecelerinin farklı olmasından dolayıdır. Bu örneklere bakılarak bulanık FMEA öncesinde klasik RPN değeri yüksek olan 19 numaralı hata modunun yüksek risk içerdiği sonucuna varılırken FRPN değeri dikkate alındığında aynı hata modunun risk puanının o kadar da yüksek olmadığı için önceliğin diğer yüksek FRPN değerine sahip hata modlarına verilebileceği söylenebilir. Ancak bu örnek dışında; 4, 9, 17 numaralı hata modlarına bakıldığında ise hem RPN değerlerinin hem de FRPN değerlerinin oldukça yüksek olduğunu ve bu hata modlarının yüksek risk içerdiği için öncelik verilmesi gerektiği söylenebilir. Sonuçta, RPN ve FRPN değerlerinin büyük oranda benzerlik göstermesine rağmen farklı olduğu hata modlarının olduğunu söylemek mümkün olmaktadır. Çalışmada, bulanık risk hesaplamasının yapılmasıyla kısmen de olsa farklı sonuçların çıkabileceği görülmüştür.

Çalışmada son olarak hesaplanmış olan RPN ve FRPN değerleri için bir kıyaslama yapılmıştır. Bu kıyaslamadan beklenen şey iki değerin birbirleriyle benzerlik göstermesidir. Şekil 5.10.'da klasik ve bulanık RPN değerlerinin karşılaştırmalı olarak gösterildiği bir grafik sunulmaktadır.



Şekil 5.10. RPN ve FRPN Değerleri Karşılaştırması

Grafik incelendiğinde, bu değişkenler arasında benzer bir eğilim olduğu ve bir değişkenin değeri arttığında diğer değişkenin de genellikle arttığını görülmektedir. İki değişken arasındaki bu benzer hareketlilik olması gereken bir durumdur. Çünkü bulanık FMEA, klasik FMEA'nın dezantajlarını gidererek yeni bir yaklaşım sunsa da temelde her iki yöntemde de uzmanlardan alınan olasılık, şiddet ve tespit edilememe girdileri kullanılmaktadır. Sadece bulanık yaklaşımda sınır değerler klasik FMEA'de olduğu gibi

kesin bir tanımlamaya dâhil olmak yerine alt-üst aralıklara belirli üyelik derecesinde dâhil olduğundan daha makul sonuçlar sunmaktadır.

Grafikte, 18-21 hata modlarında RPN değerlerinde farklılık olmasına rağmen FRPN değerlerinin büyük oranda sabit kalması dikkat çekmektedir. Bunun nedeninin bulanık kuralların belirlenirken girdi değişken aralıklarının bu hata modlarında benzer sonuçları vermesinden kaynaklandığı düşünülmektedir. RPN ve FRPN değerlerinin her ne kadar benzer olması beklense de FRPN değerlerinin farklı olduğu noktaların olması da beklenen bir durumdur. Bulanık yaklaşım ile karar vericilerin seçimleri doğrultusunda bir karar verildiğinden daha gerçekçi bir değerlendirme yapıldığını söylemek mümkündür.

Ayrıca; RPN değerinin, FRPN değerini ne kadar iyi tahmin edebileceğini anlamak için RPN ve FRPN değerlerinin sıralanmış veriler olması nedeniyle bu iki değerin karşılaştırılması için Spearman Korelasyon katsayısı kullanılmıştır. Korelasyon katsayısının 0,924 olması ($p=0,001$) korelasyonun anlamlı olduğunu, RPN ve FRPN değerleri arasında pozitif yönde çok güçlü bir ilişki olduğunu göstermektedir.

Anket sonuçlarının belirlenmesinin ardından çıkan risk puanları kendi aralarında öncelik sırasına göre (büyükten küçüğe) sıralanmıştır ve böylece hangi risklere öncelik verilmesi gerektiği belirlenmiştir.

6. SONUÇ VE ÖNERİLER

Bilgi güvenliğine yönelik riskler sayısızdır. Teknolojinin hızlı evrimi, sürekli olarak yeni tehdit unsurlarının ve zayıflıkların ortaya çıkmasına yol açmaktadır. Bilgi hem bireyler hem de kurumlar için son derece kıymetli bir unsur olup kurumların, bilgi varlıklarının ve süreçlerin korunması adına daha proaktif ve etkili önlemler alması gerekmektedir. Bilgi güvenliği, sadece varlık koruması açısından değil, aynı zamanda bireylerin ve kurumların güvenilirliği ve sürdürülebilirliği için de kritik bir role sahiptir. Bu nedenle, bilgi güvenliğinin sağlanması, risklerin önceden tahmin edilip etkin bir şekilde yönetilmesine bağlıdır. Bilgi güvenliğine yönelik risklerin sürekli izlenmesi ve değerlendirilmesi gerekmektedir. Bilgi güvenliği stratejilerinin sürdürülebilir ve dinamik hale getirilmesi, organizasyonların bu değişen tehditlere karşı daha dirençli olmalarını sağlamak için oldukça önemlidir.

Bu çalışma, taşınabilir cihaz ve ortam güvenliği açısından mevcut önemli riskleri belirleme ve değerlendirme amacını taşımaktadır. Çalışmada, en çok tercih edilen risk analiz yöntemlerinden biri olan bulanık FMEA yöntemi kullanılmıştır. Geleneksel risk yönetimi yaklaşımlarının yanı sıra, bulanık FMEA yönteminin kullanılması, belirsizlik ve karmaşıklıkla başa çıkma kapasitemizi artırabilmektedir. Bilgi güvenliği alanında uzman 7 kişi ile çalışılmış ve uzmanlardan 21 adet hata modu için değerlendirme yapmaları istenmiştir. Risk değerlendirmesi için olasılık, şiddet ve tespit edilebilirlik girdileri 10 farklı dilsel ölçekte sunulmuştur. Uzmanların farklı disiplinlerden gelmesi ve farklı tecrübe düzeyleri; hata modlarının yorumlanması aşamasında değerlendirilen olasılık, şiddet ve tespit edilebilirlik girdilerinin farklı yorumlanmasına ve değerlendirilmesine neden olmuştur.

Karar vericilerin olasılık değerlendirmelerine bakıldığında, hata modlarının ilgili kurumda görülme olasılığı ya da olayların meydana gelme sıklığı düşük olduğu için 1-3 değer aralıkları dışında bir puan verilmediği görülmüştür. Ancak olasılığın aksine şiddet ve tespit edilebilirlik girdileri için 1-10 değerlerinin hepsinin kullanıldığı görülmüştür. Bilgi güvenliğinde küçük bir güvenlik açığı bile büyük sorunlara yol açabileceğinden ve bu tür farklı yorumlamalara açık bir konu olduğundan karar vericilerin şiddet ve tespit edilebilirlik değerlendirmelerinin farklı yorumlandığı sonucuna varılmıştır.

Farklılık her hata modu için geçerli olmamakla birlikte örneğin; ‘Kritik seviyeli ağlarda kullanılan taşınabilir cihazların, internete bağlı veya kurum dışı sistemlerde kullanılması’ olarak belirlenen 20 numaralı hata modu karar vericiler tarafından farklı yorumlanmış; şiddet ve tespit edilebilirlik değerleri arasındaki açıklık değeri en yüksek bu hata modunda gözlenmiştir. Karar vericilerin cevaplarındaki bu çeşitlilik beklenen bir durum olmakla beraber sonuçta elde edilen anket puanları kullanılarak aykırı değerlerin yer almaması adına her bir girdinin medyan değerleri üzerinden hesaplamalar yapılmıştır.

Ayrıca çalışmada, klasik RPN hesaplaması ile bulanık RPN sonuçları karşılaştırılmış ve iki değerin birbiriyle oldukça tutarlı olduğu sonucuna varılmıştır.

Risk hesaplamaları sonucunda kurumlarda, elde edilen çıktılar ile bir yol haritası oluşturulmakta, risk önceliklendirilmeleri ve zaman-maliyet analizleri yapılmaktadır. Bu noktada öncelik verilmesi gereken risklerin doğru belirlenmesi, yapılan analizlerin doğruluğunu desteklemektedir. Bilgi güvenliği konusunda ise risklerin doğru önceliklendirilmesi kritik bir öneme sahiptir.

Çalışma sonucunda hata modları bulanık Risk Öncelik Puanlarına göre sıralandığında, yüksek öncelik verilmesi gereken 5 hata modu;

1. Tamire verilen taşınabilir bilgisayarlarda bulunan verinin silinmemesi,
2. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, belgelerin kurumsal olarak yetkilendirilmemiş kişilerde veya kişisel olarak kullanılan cihazlarda bulundurulması,
3. Taşınabilir ortamlar üzerinde yer alan kritik bilginin/verinin şifreli olarak saklanmaması,
4. Kritik veriye erişen cihazlara çeşitli yazılım kurulum kısıtlarının getirilmemesi,
5. Cihazı uzaktan fabrika ayarlarına döndürüp içindeki veriyi silebilecek bir mekanizmanın kullanılmaması, olarak belirlenmiştir.

Bu risklerin azaltılması ve kontrol altına alınması için etkili önlemlerin alınması gerekmektedir. Özellikle, tamire verilen taşınabilir bilgisayarlarda bulunan verinin silinmemesi gibi durumlar, ciddi güvenlik tehditleri oluşturabilir ve bu konuda alınacak önlemler büyük önem taşımaktadır. Taşınabilir ortam içerisindeki veriler bilgi güvenliği prosedür veya politikalarında belirtildiği şekilde ve belirtildiği süre boyunca saklanmalıdır. Ortam, her türlü olumsuz fiziksel etkilere karşı korunmalıdır. Kullanım politikaları merkezi olarak yönetilmeli ve sürekli olarak güncellenmelidir. Yetkilendirme ve kimlik yönetimi açısından da cihazlar merkezi olarak yönetilmelidir.

Gizli ve ticari bilgilerin sızması durumu da kurumları bir dizi olumsuz etkileşimle karşı karşıya bırakmaktadır. Finansal kayıplara, müşteri bilgilerinin kötüye kullanılmasına, hukuki maliyetlere, rekabet avantajı kaybına, ticari sır ve stratejik bilgilerin yetkisiz kişilerce kötüye kullanılmasına, kurum itibarının olumsuz etkilenmesine ve kötü amaçlı yazılımların veya siber saldırıların, silinmiş verilere erişilmesine sebep olmaktadır. Bu tür sorunlarla karşılaşmamak için, güvenlik politikalarının güçlendirilmesi, güvenlik yazılımlarının kullanılması, düzenli güvenlik denetimlerinin yapılması ve güncel teknolojik çözümlerin benimsenmesi gibi önlemler alınmalıdır. Organizasyonlar, güvenlik stratejilerini ve politikalarını sürekli olarak yenilemeli ve geliştirmelidir. Ayrıca, personel eğitimine ve farkındalığını artırmaya yönelik çabaların dinamik bir şekilde sürdürülmesi, bilgi güvenliği kültürünün oluşturulmasında kritik bir rol oynamaktadır. Bu, organizasyonların siber tehditlere karşı daha dirençli ve adaptasyon kabiliyeti yüksek bir yapıya sahip olmalarını sağlayabilmektedir.

Sıralanan risklerin gerçekleşmesi durumunda doğabilecek sorunlara bakıldığında aslında tüm hata modlarının hemen hepsinin birbiriyle bağlantılı olduğu görülmektedir. Yani hata modlarından birinin riskinin yüksek olması durumu beraberinde birçok zafiyeti getirmektedir. Öncelikli olarak FRPN değeri yüksek olan hata modlarına öncelik verilmesi gerekse de bilgi güvenliği konusunda en ufak bir açıklığın devasa geri dönülmez sonuçları olabilmektedir. Dolayısıyla en düşük FRPN değerine sahip hata modunun bile oldukça önemli olduğunu ve göz ardı edilemeyecek durumlar olduğu söylenebilir.

Sonuçların klasik FMEA ile tutarlı olduğunu göz önünde bulundurarak, bulanık FMEA'nın bu alandaki etkinliği ortaya konulmuştur. Korelasyon katsayısı 0,924 seviyesinde olup, bu da bulanık FMEA'nın geleneksel yöntemle güçlü bir uyum içinde olduğunu göstermektedir. Benzer işlemlerden geçen bu iki yöntemin birbiriyle uyumlu olması beklenmekle birlikte aynı zamanda sınır değerler için bulanık yöntemde farklılıkların olması da beklenmektedir. Çünkü sınır RPN değerleri aynı anda bir alt ve bir üst sınırına üye olmaktadır. Üyelik derecelerinin oranları ve bu çalışma özelinde kullanılan metoda göre (EK-EB) de girdi değişkenleri içerisinde en küçük olan belirleyici olmaktadır. Böylece çalışmada sonucun büyük oranda klasik FMEA ile benzerlik göstermesi beklenirken klasik yöntemden ayrıldığı noktaların da gözlenmesi beklenmiş ve sonuçların da bunu doğruladığı görülmüştür. Sonuçta, bulanık FMEA'nın karmaşık ve

belirsiz durumların değerlendirilmesinde geleneksel yöntemlere göre daha etkili bir araç olduğu söylenebilmektedir.

Güvenlik tehditleriyle karşı karşıya kalan birçok varlık bulunmaktadır. Ancak çalışmanın kapsamı taşınabilir cihaz ve ortam güvenliği ile sınırlandırılmıştır. Gelecekte, daha birçok varlık grupları üzerinde (Ağ ve Sistem Güvenliği, Uygulama ve Veri Güvenliği, Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği, Personel Güvenliği, Fiziksel Mekânların Güvenliği) risk değerlendirme çalışması yapılabilir ve bu çalışmalar kurumların hangi risklere öncelik vermesi gerektiği hakkında oldukça yardımcı olabilmektedir. Varlık grupları için risk analizi çalışması yapılmasından sonra da Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri ve Sıkılaştırma Tedbirleri başlıkları altında yer alan her bir alt başlık için de aynı çalışmanın yapılabilir ve riskler önceliklendirilebilir. Bu tür geniş kapsamlı bir güvenlik değerlendirmesi, kurumların bütünlüklerini ve güvenlik stratejilerini daha etkili bir şekilde geliştirmelerine yardımcı olabilmektedir.

7. KAYNAKLAR

Alizadeh Khameneh, M. A., Tree detection and species identification using LiDAR data, https://www.researchgate.net/publication/285593710_Tree_Detection_and_Species_Identification_using_LiDAR_Data (Erişim Tarihi: **3 Mart 2024**).

Alizadeh, S. S., Solimanzadeh, Y., Mousavi, S., and Safari, G. H., Risk assessment of physical unit operations of wastewater treatment plant using fuzzy FMEA method: a case study in the northwest of Iran. Environmental Monitoring and Assessment, 194(9), (**2022**) 609.

Amos, Z., How Ransomware Can Evade Antivirus Software, https://gca.isa.org/blog/how-ransomware-can-evade-antivirus-software (Erişim Tarihi: **3 Mart 2024**).

Anderson, J. M., Why we need a new definition of information security. Computers & security, 22(4) (**2003**) 308-313.

Ashenden, D., Information Security management: A human challenge?. Information security technical report, 13(4) (**2008**) 195-201.

Asllani, A., Lari, A., and Lari, N., Strengthening information technology security through the failure modes and effects analysis approach. International Journal of Quality Innovation, 4 (**2018**) 1-14.

ASQ, Failure mode effect analysis (FMEA), http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html **(**Erişim tarihi: **27 Kasım 2023)**

Balaraju, J., Raj, M. G., and Murthy, C. S., Fuzzy-FMEA risk evaluation approach for LHD machine–A case study. Journal of Sustainable Mining, 18(4) (**2019**) 257-268.

Bidgoli, H., Handbook of information security, information warfare, social, legal, and international issues and security foundations, Vol. 2, John Wiley & Sons, **2006**.

Bilbao, A., TUAR-a model of risk analysis in the security field. In Proceedings 1992 International Carnahan Conference on Security Technology: Crime Countermeasures, IEEE, Atlanta, GA, USA, **1992**, 65-71.

Bojadziev, G., and Bojadziev, M., Fuzzy logic for business, finance, and management Vol. 12, World Scientific. **1997.**

Bosworth, S., and Kabay, M. E. (Eds.)., Computer security handbook. John Wiley & Sons, **2002.**

Bowles, J. B., and Peláez, C. E., Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis. Reliability engineering & system safety, 50(2) (**1995**) 203-213.

Buriboev, A., Kang, H. K., Ko, M. C., Oh, R., Abduvaitov, A., and Jeon, H. S., Application of fuzzy logic for problems of evaluating states of a computing System, *9*(15) (**2019**) 3021.

Carbone, T. A., and Tippett, D. D., Project risk management using the project risk FMEA, *16*(4) (**2004**) 28-35.

Carlson, C. S., Effective FMEAs: Achieving safe, reliable, and economical products and processes using failure mode and effects analysis, Vol. 1, John Wiley & Sons, **2012.**

Center for Internet Security, Top 10 malware Q2 2023. CIS. https://www.cisecurity.org/insights/blog/top-10-malware-q2-2023 **(**Erişim tarihi: **3 Aralık 2023)**

Chanamool, N., and Naenna, T., Fuzzy FMEA application to improve decision-making process in an emergency Department, 43 (**2016**) 441-453.

Chen, G., and Pham, T. T., Introduction to fuzzy sets, fuzzy logic, and fuzzy control systems, CRC press, Boca Raton, 2000.

Chiozza, M. L., and Ponzetti, C., FMEA: a model for reducing medical errors. Clinica chimica acta, 404(1) (**2009**) 75-78.

Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J., Management of information security: Challenges and research directions. Communications of the Association for Information Systems, 20(1) (**2007**) 57.

Cinar, A. C., and Kara, T. B., The current state and future of mobile security in the light of the recent mobile security threat reports. Multimedia Tools and Applications, 82(13) (**2023**) 20269-20281.

Dagon, D., Martin, T., and Starner, T., Mobile phones as computing devices: The viruses are coming!, 3(4) (**2004**) 11-15.

Datareportal, Digital around the world Global digital insights. https://datareportal.com/global-digital-overview#:~:text=Global%20mobile%20adoption&text=The%20latest%20data%20reveal%20that,5.60%20billion%20in%20October%202023 (Erişim tarihi: **03 Aralık 2023**)

Datta, S., and Mukherjee, S. K., Developing a risk management matrix for effective project planning—an empirical study, 32(2) (**2001**) 45-57.

de Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Poleto, T., and Costa, A. P. C. S., Information security risk analysis model using fuzzy decision theory. International Journal of Information Management, 36(1) (**2016**) 25-34.

de Gusmão, A. P. H., Silva, M. M., Poleto, T., e Silva, L. C., and Costa, A. P. C. S., Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory, *43* (**2018**) 248-260.

Defense Systems Management College, Acquisition Strategy Guide. Government Printing Office., US, **2000.**

Deighton, M., Facility integrity management: effective principles and practices for the oil, gas and petrochemical industries. Gulf Professional Publishing, **2016.**

Dhillon, G., and Backhouse, J., Risks in the use of information technology within organizations, *16*(1) (**1996**) 65-74.

Disterer, G., ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security 4(2) (**2013**).

Ebeling, C. E., An introduction to reliability and maintainability engineering. Waveland Press. NYC, **2019.**

Eminağaoğlu, M., ve Gökşen, Y. Bilgi güvenliği nedir, ne değildir? Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri, 11, (**2009**) 01-15.

Ershadi, M. J., and Forouzandeh, M., Information Security Risk Management of Research Information Systems: A hybrid approach of Fuzzy FMEA, AHP, TOPSIS and Shannon Entropy. J. Digit. Inf. Manag., 17(6) (**2019**) 321.

Franceschini, F., and Galetto, M., new approach for evaluation of risk priorities of failure modes in FMEA. International journal of production research, 39(13) (**2001**) A 2991-3002.

Ghosh M., Process failure mode effects analysis (PFMEA),

Gilchrist, W., Modelling failure modes and effects analysis. International Journal of Quality & Reliability Management, 10(5) (**1993**).

Global Cybersecurity Alliance, How Ransomware Can Evade Antivirus Software , https://gca.isa.org/blog/how-ransomware-can-evade-antivirus-software **(**Erişim tarihi: **3 Mart 2024)**

Greene, L., and Mamic, I., The future of work: Increasing reach through mobile technology International Labour Organization No. 994867513402676 (**2015**).

https://www.processexcellencenetwork.com/lean-six-sigma-business-performance/articles/process-failure-mode-effects-analysis-pfmea **(**Erişim tarihi: **27 Kasım 2023)**

Hubbard, D. W., The failure of risk management: Why it's broken and how to fix it. John Wiley & Sons., **2020.**

International Standards Organization (ISO). ISO/IEC 17799 information technology security techniques: code of practice for information security management. Geneva: ISO; **2005.**

ISO, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, www.iso.org/standard/27001 **(**Erişim tarihi: **3 Mart 2024)**

Ivančan, J., and Lisjak, D. New FMEA risks ranking approach utilizing four fuzzy logic systems. Machines, 9(11) (**2021**) 292.

Jain, M. K., An Efficient Expert System Generator for Qualitative Feed-Back Loop Analysis. BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 3(1) (**2012**) 5-18.

Kailay, M. P., and Jarratt, P., RAMeX: a prototype expert system for computer security risk analysis and management. Computers & Security, 14(5) (**1995**) 449-463.

Karabacak, B., and Sogukpinar, I., ISRAM: information security risk analysis method. Computers & Security, 24(2) (**2005**) 147-159.

Kaye, David. The importance of information. Management Decision 33(5) (**1995**): 5-12.

Khairuddin, S. H., Hasan, M. H., Hashmani, M. A., and Azam, M. H., Generating clustering-based interval fuzzy type-2 triangular and trapezoidal membership functions: A structured literature review. Symmetry, 13(2) (**2021**) 239.

Kim, M.H., Toyib, W., and Park, M.G., An Integrative method of FTA and FMEA for software security analysis of a smart phone. KIPS Transactions on Computer and Communication Systems 2(12) (**2013**) 541-552.

Klir, G., and Yuan B., Fuzzy sets and fuzzy logic. Vol. 4. New Jersey: Prentice hall, **1995.**

Laricchia, F., Number of mobile devices worldwide 2020-2025. Statista. https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/ **(**Erişim tarihi: **3 Aralık 2023)**

Ledermüller, T., and Nathan L. C., Risk assessment for mobile devices. Trust, Privacy and Security in Digital Business: 8th International Conference, TrustBus 2011, Toulouse, France, August 29-September 2, 2011, Proceedings 8. Springer Berlin Heidelberg, **2011.**

Li, B., Smartphone, promising battlefield for hackers 8(1) (**2011**) 89-110.

Li, X., Li, H., Sun, B., and Wang, F., Assessing information security risk for an evolving smart city based on fuzzy and grey FMEA. Journal of Intelligent & Fuzzy Systems, 34(4) (**2018**) 2491-2501.

Lipol, L. S., and Haq, J., Risk analysis method: FMEA/FMECA in the organizations. International Journal of Basic & Applied Sciences, 11(5) (**2011**) 74-82.

Mandal, S., and Maiti, J., Risk analysis using FMEA: Fuzzy similarity value and possibility theory based approach. Expert Systems with Applications, 41(7) (**2014**) 3527-3537.

Maués, L. M. F., Sá, J. A. S. D., Costa, C. T. D., Kern, A. P., and Duarte, A. A. A. M., Construction duration predictive model based on factorial analysis and fuzzy logic. Ambiente Construído, 19 (**2019**) 115-133.

Mendonça Silva, M., Poleto, T., Camara e Silva, L., Henriques de Gusmao, A. P., and Cabral Seixas Costa, A. P., A grey theory based approach to big data risk management using FMEA. Mathematical Problems in Engineering, 2016 (**2016**).

Metaxiotis, K., Psarras, J., and Samouilidis, E., Integrating fuzzy logic into decision suppport systems: current research and future prospects. Information management & computer security, 11(2) (**2003**) 53-59.

Ozkan, S., and Karabacak, B., Collaborative risk method for information security management practices: A case context within Turkey. International Journal of Information Management, 30(6) (**2010**) 567-572.

Patel, S. C., Graham, J. H., and Ralston, P. A., Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. International Journal of Information Management, 28(6) (**2008**) 483-491.

Pinto, C. A., Arora, A., Hall, D., and Schmitz, E., Challenges to sustainable risk management: case example in information network security. Engineering Management Journal, 18(1) (**2006**) 17-23.

Purdy, G., ISO 31000: 2009—setting a new standard for risk management. Risk Analysis: An International Journal, 30(6) (**2010**) 881-886.

Samonas, S., and Coss, D., The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3) (**2014**).

Schmittner, C., Gruber, T., Puschner, P., and Schoitsch, E., Security application of failure mode and effect analysis (FMEA). In Computer Safety, Reliability, and Security: 33rd International Conference, SAFECOMP 2014, September 10-12, 2014. Proceedings 33 Springer International Publishing, Florence, Italy, 2014, p. 310-325.

Shaikh, F. A., and Siponen, M., Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security, 124 (**2023**) 102974.

Sharma, K. D., and Srivastava, S., Failure mode and effect analysis (FMEA) implementation: a literature review. J Adv Res Aeronaut Space Sci, 5(1-2) **(2018**) 1-17.

Sharma, R. K., Kumar, D., and Kumar, P., Systematic failure mode effect analysis (FMEA) using fuzzy linguistic modelling. International journal of quality & reliability management, 22(9) (**2005**) 986-1004.

Silva, M. M., de Gusmão, A. P. H., Poleto, T., e Silva, L. C., and Costa, A. P. C. S., A multidimensional approach to information security risk management using FMEA and fuzzy theory. International Journal of Information Management, 34(6) (**2014**) 733-740.

Stamatis, D. H., Failure mode and effect analysis, Quality Press, **2003**.

Stamp, M., Information security: principles and practice, John Wiley & Sons, **2011.**

Sumner, M., Information security threats: a comparative analysis of impact, probability, and preparedness. Information Systems Management, 26(1) (**2009**) 2-12.

Şen, Zekai. Bulanık mantık ilkeleri ve modelleme. Su Vakfı, **2020.**

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Denetim Rehberi,
https://cbddo.gov.tr/SharedFolderServer/Projeler/File/BG_Denetim_Rehberi.pdf
(Erişim tarihi: **3 Mart 2024).**

TS EN ISO/IEC 27002 Bilgi teknolojisi- Güvenlik teknikleri- Bilgi güvenliği kontrolleri için uygulama prensipleri (**2017**).

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi,
https://cbddo.gov.tr/SharedFolderServer/Projeler/File/BG_Denetim_Rehberi.pdf
(Erişim tarihi: **3 Mart 2024)**

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf (Erişim tarihi: **3 Ocak 2024**).

Wang, J. B. Y. J., J. B. Yang, and P. Sen. Safety analysis and synthesis using fuzzy sets and evidential reasoning. Reliability Engineering & System Safety 47.2 (**1995**): 103-118.

Whitman ME, Mattord HJ. Principles of information security. 3rd ed. Thompson Course Technology; **2009.**

Xu, Kai, et al. Fuzzy assessment of FMEA for engine systems. Reliability engineering & system safety 75.1 (**2002**): 17-29.

Yang, Zaili, Steve Bonsall, and Jin Wang. Fuzzy rule-based Bayesian reasoning approach for prioritization of failures in FMEA. IEEE Transactions on Reliability 57.3 (**2008**): 517-528.

Zadeh, L. A., Fuzzy sets, Inf Control, 8(3) (**1965**) 338–353

EKLER

Ek 1- Hata Modları Anket Listesi

	Hata Modları	O	S	D
1	Kurum verisine erişen taşınabilir bilgisayarlar için tanımlanmış kullanım politikası eksikliği.			
2	Kurumun, mobil cihaz üzerinden e-posta ve/veya VPN gibi kurumsal servislere erişim izni vermeden önce politikayı çalışanlara tebliğ			
3	Kritik veriye erişen cihazlara çeşitli yazılım kurulum kısıtlarının getirilmemesi.			
4	Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgelerin kurumsal olarak yetkilendirilmemiş kişilerde veya kişisel olarak kullanılan cihazlarda bulundurulması.			
5	Cihazı uzaktan fabrika ayarlarına döndürüp içindeki veriyi silebilecek bir mekanizmanın kullanılmaması.			
6	Taşınabilir bilgisayarlar için gerekli güvenlik yazılımlarının yüklenmemesi.			
7	Zararlı yazılımdan korunma uygulamalarına ait politikaların merkezi olarak yönetilmemesi.			
8	Zararlı yazılımlardan korunma uygulamasının üretici veya ilgili kurum tarafından önerilen şekilde yapılandırılmaması ve güncel tutulmaması.			
9	Tamire verilen taşınabilir bilgisayarlarda bulunan verinin silinmemesi.			
10	Taşınabilir bilgisayarlar için çalınma ve kaybolma riskine karşı disk şifreleme yapılmaması.			
11	Kritik veriye erişim imkânı olan taşınabilir bilgisayarlarda, harici depolama ortamlarının okuma ve yazma özelliklerinin devre dışı bırakılmış olmaması.			
12	Kritik veriye erişen cihazların merkezi olarak yönetilmemesi. (Bu durum farklı kullanıcı grupları veya departmanlar arasında farklı güvenlik ayarlarına neden olabilir.)			
13	Güvenlik politikasının kritik veriye erişen cihazlara yüklenmiş olmaması.			
14	Merkezi yönetim sisteminin, güvenlik yamaları yüklenmemiş ya da üzerinde kara listeye alınmış uygulama/uygulama sürümü barındıran taşınabilir bilgisayarların sisteme erişiminin engellememesi.			
15	Taşınabilir ortam yönetimine ilişkin en az fiziksel koruma ve saklama ile ilgili gereksinimler, yedekleme, el değiştirme ve imha hususlarını içeren kullanım politikası hazırlanıp uygulanmaması.			
16	Taşınabilir ortamların, olumsuz fiziksel etkilere karşı üretici tarafından tavsiye edilen saklama ve kullanım koşullarına uyumlu olarak			
17	Taşınabilir ortamlar üzerinde yer alan kritik bilginin/verinin şifreli olarak saklanmaması.			
18	Kullanım süresi dolmuş taşınabilir ortamların veri sızıntılarını önlemek amacıyla güvenli olarak imha edilmemesi.			
19	Taşınabilir ortam içindeki bilginin/verinin saklanması gereken süre göz önünde bulundurularak güvenli şekilde yedeklenmemesi.			
20	Kritik seviyeli ağlarda kullanılan taşınabilir cihazların, internete bağlı veya kurum dışı sistemlerde kullanılması.			
21	Kaba kuvvet saldırılarından korunmak için kurum tarafından belirlenecek sayıda hatalı giriş denemesi sonrası cihaz belleğinde bulunan verilerin silinmemesi.			

Ek 2- Anket Puanlarının Belirlenmesi

OLASILIK				
5'li Ölçek	**Puan**	**Kısaltma**	**Tanım**	**Açıklama**
ÇY	10	K	Kesin Gerçekleşme Olasılığı	Hata günde en az bir kez meydana gelir ya da neredeyse her an hata vardır.
	9	NK	Hata Neredeyse Kaçınılmaz	Hata öngörülebilecek şekildedir.
Y	8	ÇY	Çok Yüksek Oluşma Olasılığı	Hata her 3-4 günde bir tekrarlar.
	7	OY	Oldukça Yüksek Oluşma Olasılığı	Hata sıklıkla meydana gelir.
O	6	Y	Yüksek Oluşma Olasılığı	Haftada 1 hata meydana gelir.
	5	NY	Nispeten Yüksek Oluşma Olasılığı	Hata neredeyse ayda bir meydana gelir.
	4	OD	Orta Dereceli Oluşma Olasılığı	Hata ara sıra meydana gelir ya da her 3 ayda 1 hata meydana gelir.
D	3	DO	Düşük-Orta Dereceli Oluşma Olasılığı	Hata nadiren meydana gelir ya da yılda 1 hata meydana gelir.
	2	D	Düşük Oluşma Olasılığı	Neredeyse hiç hata meydana gelmez.
ÇD	1	ÇD	Çok Düşük Oluşma Olasılığı	Kimse en son ne zaman hata meydana geldiğini hatırlamaz.

ŞİDDET				
5'li Ölçek	**Puan**	**Kısaltma**	**Tanım**	**Açıklama**
ÇY	10	SD	Son Derece Tehlikeli	Tüm sistemin herhangi bir ön uyarı olmaksızın tamamen çökmesi. Sistemin çalışmasını askıya alır ve/veya hükümet düzenlemelerine uymamayı içerir.
	9	KD	Kritik Derecede Tehlikeli	Hata büyük veya kalıcı bir soruna neden olabilir ve/veya hükümet düzenlemelerine/standartlarına uymamayı içerir.
Y	8	ÖD	Önemli Derecede Tehlikeli	Hizmet birincil işlev kaybıyla çalışamaz durumdadır, sistem çalışmaz.
	7	ÇY	Çok Yüksek Derecede Tehlikeli	Ön uyarı sonrası ciddi sistem kesintisi, hizmet kesintisi yaşanması.
O	6	YD	Yüksek Derecede Tehlikeli	Hata küçük ya da orta dereceli bir hasara neden olabilir ancak ciddi derecede müşteri memnuniyetsizliğini beraberinde getirir ve/veya büyük sistem problemi yüksek onarım maliyeti ya da önemli derecede yeniden işleme maliyetine yol açar.
	5	OY	Orta-Yüksek Derecede Tehlikeli	Önemli sistem sorunları meydana gelebilir.
	4	T	Tehlikeli	Hata bazı müşteri memnuniyetsizliklerine neden olabilir ve/veya belirli sistem sorunları meydana gelebilir.
D	3	DO	Düşük-Orta Derecede Tehlikeli	Hata çok küçük bir soruna neden olabilir veya hiç sorun yaratmayabilir ancak müşterileri rahatsız edebilir ve/veya sistemde/proseste küçük değişiklikler yapılarak onarılabilecek sistem aksamaları meydana gelebilir.
	2	HT	Hafif Tehlikeli	Hata çok küçük önemsiz sorunlara neden olabilir veya hiç sorun yaratmayabilir ve müşteriler bu sorunu fark etmeyebilirler.
ÇD	1	TY	Tehlike Yok	Hatanın sistem üzerinde herhangi bir etkisi ve tehlikesi yoktur.

TESPİT EDİLEMEME				
5'li Ölçek	**Puan**	**Kısaltma**	**Tanım**	**Açıklama**
ÇY	10	ŞY	Tespit Edime Şansı Yoktur	Hatanın tespiti son derece zordur ve genellikle fark edilemez.
	9	GO	Güvenilir Olmayan Tespit Edilebilirlik Şansı	Hatayı tespit etmek için bilinen bir mekanizma yoktur.
Y	8	ÇZ	Çok Zor Tespit Edilebilirlik Şansı	Hata ancak kapsamlı bir inceleme ile tespit edilebilir. Ancak bu mümkün değil ya da çok zordur.
	7	Z	Zor Tespit Edilebilirlik Şansı	Hata, tespit edilebilir ancak genellikle geç veya zor bir şekilde fark edilir.
O	6	OZ	Orta-Zor Derecede Tespit Edilebilirlik Şansı	Hata manuel olarak tespit edilebilir ancak bunun için herhangi bir süreç yoktur, tespit edilebilirlik tamamen şansa bırakılmıştır.
	5	OD	Orta Derecede Tespit Edilebilirlik Şansı	Çifte kontroller veya denetimler için bir süreç vardır ancak otomatik değildir ve/veya sadece bir örneğe uygulanır.
	4	OY	Orta-Yüksek Tespit Edilebilirlik Şansı	Hata, ortalamanın üzerinde bir kolaylıkla tespit edilebilir.
D	3	Y	Yüksek Tespit Edilebilirlik Şansı	Sürecin %100 denetimi/gözden geçirilmesi söz konusudur ancak otomatik değildir.
	2	ÇY	Çok Yüksek Tespit Edilebilirlik Şansı	Sürecin %100 denetimi/gözden geçirilmesi söz konusudur ve otomatiktir.
ÇD	1	NK	Neredeyse Kesin Tespit Edilebilirlik Şansı	Hatayı önleyen otomatik 'kapatmalar' veya kısıtlamalar bulunmaktadır.

Ek 3- Bulanık Kural

	BULANIK KURAL			
	O	**S**	**D**	**Risk**
1	ÇOK DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
2	ÇOK DÜŞÜK	ÇOK DÜŞÜK	DÜŞÜK	ÇOK DÜŞÜK
3	ÇOK DÜŞÜK	ÇOK DÜŞÜK	ORTA	ÇOK DÜŞÜK
4	ÇOK DÜŞÜK	ÇOK DÜŞÜK	YÜKSEK	ÇOK DÜŞÜK
5	ÇOK DÜŞÜK	ÇOK DÜŞÜK	ÇOK YÜKSEK	ÇOK DÜŞÜK
6	ÇOK DÜŞÜK	DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
7	ÇOK DÜŞÜK	DÜŞÜK	DÜŞÜK	ÇOK DÜŞÜK
8	ÇOK DÜŞÜK	DÜŞÜK	ORTA	ÇOK DÜŞÜK
9	ÇOK DÜŞÜK	DÜŞÜK	YÜKSEK	DÜŞÜK
10	ÇOK DÜŞÜK	DÜŞÜK	ÇOK YÜKSEK	DÜŞÜK
11	ÇOK DÜŞÜK	ORTA	ÇOK DÜŞÜK	ÇOK DÜŞÜK
12	ÇOK DÜŞÜK	ORTA	DÜŞÜK	ÇOK DÜŞÜK
13	ÇOK DÜŞÜK	ORTA	ORTA	DÜŞÜK
14	ÇOK DÜŞÜK	ORTA	YÜKSEK	DÜŞÜK
15	ÇOK DÜŞÜK	ORTA	ÇOK YÜKSEK	ORTA
16	ÇOK DÜŞÜK	YÜKSEK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
17	ÇOK DÜŞÜK	YÜKSEK	DÜŞÜK	DÜŞÜK
18	ÇOK DÜŞÜK	YÜKSEK	ORTA	DÜŞÜK
19	ÇOK DÜŞÜK	YÜKSEK	YÜKSEK	ORTA
20	ÇOK DÜŞÜK	YÜKSEK	ÇOK YÜKSEK	ORTA
21	ÇOK DÜŞÜK	ÇOK YÜKSEK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
22	ÇOK DÜŞÜK	ÇOK YÜKSEK	DÜŞÜK	DÜŞÜK
23	ÇOK DÜŞÜK	ÇOK YÜKSEK	ORTA	ORTA
24	ÇOK DÜŞÜK	ÇOK YÜKSEK	YÜKSEK	ORTA
25	ÇOK DÜŞÜK	ÇOK YÜKSEK	ÇOK YÜKSEK	YÜKSEK
26	DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
27	DÜŞÜK	ÇOK DÜŞÜK	DÜŞÜK	ÇOK DÜŞÜK
28	DÜŞÜK	ÇOK DÜŞÜK	ORTA	ÇOK DÜŞÜK
29	DÜŞÜK	ÇOK DÜŞÜK	YÜKSEK	DÜŞÜK
30	DÜŞÜK	ÇOK DÜŞÜK	ÇOK YÜKSEK	DÜŞÜK
31	DÜŞÜK	DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
32	DÜŞÜK	DÜŞÜK	DÜŞÜK	ÇOK DÜŞÜK
33	DÜŞÜK	DÜŞÜK	ORTA	DÜŞÜK
34	DÜŞÜK	DÜŞÜK	YÜKSEK	ORTA
35	DÜŞÜK	DÜŞÜK	ÇOK YÜKSEK	ORTA
36	DÜŞÜK	ORTA	ÇOK DÜŞÜK	ÇOK DÜŞÜK
37	DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK
38	DÜŞÜK	ORTA	ORTA	ORTA
39	DÜŞÜK	ORTA	YÜKSEK	YÜKSEK

Ek 3- Bulanık Kural (devamı)

	Olasılık	Şiddet	Tespit Edilememe	Risk
40	DÜŞÜK	ORTA	ÇOK YÜKSEK	YÜKSEK
41	DÜŞÜK	YÜKSEK	ÇOK DÜŞÜK	DÜŞÜK
42	DÜŞÜK	YÜKSEK	DÜŞÜK	ORTA
43	DÜŞÜK	YÜKSEK	ORTA	YÜKSEK
44	DÜŞÜK	YÜKSEK	YÜKSEK	ÇOK YÜKSEK
45	DÜŞÜK	YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK
46	DÜŞÜK	ÇOK YÜKSEK	ÇOK DÜŞÜK	DÜŞÜK
47	DÜŞÜK	ÇOK YÜKSEK	DÜŞÜK	ORTA
48	DÜŞÜK	ÇOK YÜKSEK	ORTA	YÜKSEK
49	DÜŞÜK	ÇOK YÜKSEK	YÜKSEK	ÇOK YÜKSEK
50	DÜŞÜK	ÇOK YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK
51	ORTA	ÇOK DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
52	ORTA	ÇOK DÜŞÜK	DÜŞÜK	ÇOK DÜŞÜK
53	ORTA	ÇOK DÜŞÜK	ORTA	DÜŞÜK
54	ORTA	ÇOK DÜŞÜK	YÜKSEK	DÜŞÜK
55	ORTA	ÇOK DÜŞÜK	ÇOK YÜKSEK	ORTA
56	ORTA	DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
57	ORTA	DÜŞÜK	DÜŞÜK	DÜŞÜK
58	ORTA	DÜŞÜK	ORTA	ORTA
59	ORTA	DÜŞÜK	YÜKSEK	YÜKSEK
60	ORTA	DÜŞÜK	ÇOK YÜKSEK	YÜKSEK
61	ORTA	ORTA	ÇOK DÜŞÜK	DÜŞÜK
62	ORTA	ORTA	DÜŞÜK	ORTA
63	ORTA	ORTA	ORTA	YÜKSEK
64	ORTA	ORTA	YÜKSEK	ÇOK YÜKSEK
65	ORTA	ORTA	ÇOK YÜKSEK	ÇOK YÜKSEK
66	ORTA	YÜKSEK	ÇOK DÜŞÜK	DÜŞÜK
67	ORTA	YÜKSEK	DÜŞÜK	YÜKSEK
68	ORTA	YÜKSEK	ORTA	ÇOK YÜKSEK
69	ORTA	YÜKSEK	YÜKSEK	ÇOK YÜKSEK
70	ORTA	YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK
71	ORTA	ÇOK YÜKSEK	ÇOK DÜŞÜK	ORTA
72	ORTA	ÇOK YÜKSEK	DÜŞÜK	YÜKSEK
73	ORTA	ÇOK YÜKSEK	ORTA	ÇOK YÜKSEK
74	ORTA	ÇOK YÜKSEK	YÜKSEK	ÇOK YÜKSEK
75	ORTA	ÇOK YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK
76	YÜKSEK	ÇOK DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
77	YÜKSEK	ÇOK DÜŞÜK	DÜŞÜK	DÜŞÜK
78	YÜKSEK	ÇOK DÜŞÜK	ORTA	DÜŞÜK
79	YÜKSEK	ÇOK DÜŞÜK	YÜKSEK	ORTA

Ek 3- Bulanık Kural (devamı)

	Olasılık	Şiddet	Tespit Edilememe	Risk
80	YÜKSEK	ÇOK DÜŞÜK	ÇOK YÜKSEK	ORTA
81	YÜKSEK	DÜŞÜK	ÇOK DÜŞÜK	DÜŞÜK
82	YÜKSEK	DÜŞÜK	DÜŞÜK	ORTA
83	YÜKSEK	DÜŞÜK	ORTA	YÜKSEK
84	YÜKSEK	DÜŞÜK	YÜKSEK	ÇOK YÜKSEK
85	YÜKSEK	DÜŞÜK	ÇOK YÜKSEK	ÇOK YÜKSEK
86	YÜKSEK	ORTA	ÇOK DÜŞÜK	DÜŞÜK
87	YÜKSEK	ORTA	DÜŞÜK	YÜKSEK
88	YÜKSEK	ORTA	ORTA	ÇOK YÜKSEK
89	YÜKSEK	ORTA	YÜKSEK	ÇOK YÜKSEK
90	YÜKSEK	ORTA	ÇOK YÜKSEK	ÇOK YÜKSEK
91	YÜKSEK	YÜKSEK	ÇOK DÜŞÜK	ORTA
92	YÜKSEK	YÜKSEK	DÜŞÜK	ÇOK YÜKSEK
93	YÜKSEK	YÜKSEK	ORTA	ÇOK YÜKSEK
94	YÜKSEK	YÜKSEK	YÜKSEK	ÇOK YÜKSEK
95	YÜKSEK	YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK
96	YÜKSEK	ÇOK YÜKSEK	ÇOK DÜŞÜK	ORTA
97	YÜKSEK	ÇOK YÜKSEK	DÜŞÜK	ÇOK YÜKSEK
98	YÜKSEK	ÇOK YÜKSEK	ORTA	ÇOK YÜKSEK
99	YÜKSEK	ÇOK YÜKSEK	YÜKSEK	ÇOK YÜKSEK
100	YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK
101	ÇOK YÜKSEK	ÇOK DÜŞÜK	ÇOK DÜŞÜK	ÇOK DÜŞÜK
102	ÇOK YÜKSEK	ÇOK DÜŞÜK	DÜŞÜK	DÜŞÜK
103	ÇOK YÜKSEK	ÇOK DÜŞÜK	ORTA	ORTA
104	ÇOK YÜKSEK	ÇOK DÜŞÜK	YÜKSEK	ORTA
105	ÇOK YÜKSEK	ÇOK DÜŞÜK	ÇOK YÜKSEK	YÜKSEK
106	ÇOK YÜKSEK	DÜŞÜK	ÇOK DÜŞÜK	DÜŞÜK
107	ÇOK YÜKSEK	DÜŞÜK	DÜŞÜK	ORTA
108	ÇOK YÜKSEK	DÜŞÜK	ORTA	YÜKSEK
109	ÇOK YÜKSEK	DÜŞÜK	YÜKSEK	ÇOK YÜKSEK
110	ÇOK YÜKSEK	DÜŞÜK	ÇOK YÜKSEK	ÇOK YÜKSEK
111	ÇOK YÜKSEK	ORTA	ÇOK DÜŞÜK	ORTA
112	ÇOK YÜKSEK	ORTA	DÜŞÜK	YÜKSEK
113	ÇOK YÜKSEK	ORTA	ORTA	ÇOK YÜKSEK
114	ÇOK YÜKSEK	ORTA	YÜKSEK	ÇOK YÜKSEK

Ek 3- Bulanık Kural (devamı)

	Olasılık	Şiddet	Tespit Edilememe	Risk
115	ÇOK YÜKSEK	ORTA	ÇOK YÜKSEK	ÇOK YÜKSEK
116	ÇOK YÜKSEK	YÜKSEK	ÇOK DÜŞÜK	ORTA
117	ÇOK YÜKSEK	YÜKSEK	DÜŞÜK	ÇOK YÜKSEK
118	ÇOK YÜKSEK	YÜKSEK	ORTA	ÇOK YÜKSEK
119	ÇOK YÜKSEK	YÜKSEK	YÜKSEK	ÇOK YÜKSEK
120	ÇOK YÜKSEK	YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK
121	ÇOK YÜKSEK	ÇOK YÜKSEK	ÇOK DÜŞÜK	YÜKSEK
122	ÇOK YÜKSEK	ÇOK YÜKSEK	DÜŞÜK	ÇOK YÜKSEK
123	ÇOK YÜKSEK	ÇOK YÜKSEK	ORTA	ÇOK YÜKSEK
124	ÇOK YÜKSEK	ÇOK YÜKSEK	YÜKSEK	ÇOK YÜKSEK
125	ÇOK YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK	ÇOK YÜKSEK