
GAZİ ÜNİVERSİTESİ
Gazi
1926

# BİLİŞİM HİZMETLERİNİN SÜREKLİLİĞİNE YÖNELİK RİSK ANALİZİ: BİR KAMU KURUMU UYGULAMA ÖRNEĞİ

**İsmail İLTER**

**YÜKSEK LİSANS TEZİ**
**YÖNETİM BİLİŞİM SİSTEMLERİ**

**GAZİ ÜNİVERSİTESİ**
**BİLİŞİM ENSTİTÜSÜ**

**ARALIK 2015**

İsmail İLTER tarafından hazırlanan "Bilişim Hizmetlerinin Sürekliliğine Yönelik Risk Analizi: Bir Kamu Kurumu Uygulama Örneği" adlı bu tez aşağıdaki jüri tarafından OY BİRLİĞİ / ~~OY ÇOKLUĞU~~ ile Gazi Üniversitesi Yönetim Bilişim Sistemleri Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

**Danışman:** Yrd. Doç. Dr. Talip KELLEGÖZ
Endüstri Mühendisliği Bölümü, Gazi Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.....

**Başkan :** Doç. Dr. İsmail KARAOĞLAN
Endüstri Mühendisliği, Selçuk Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.....

**Üye :** Öğr. Gör. Dr. Tahsin ÇETİNYOKUŞ
Endüstri Mühendisliği Bölümü, Gazi Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.....

Tez Savunma Tarihi: 25/12/2015
Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……
Doç. Dr. Nurettin TOPALOĞLU
Bilişim Enstitüsü Müdürü

## ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İsmail İLTER

25.12.2105

# BİLİŞİM HİZMETLERİNİN SÜREKLİLİĞİNE YÖNELİK RİSK ANALİZİ: BİR KAMU KURUMU UYGULAMA ÖRNEĞİ

(Yüksek Lisans Tezi)

İsmail İLTER

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Aralık 2015

## ÖZET

İş sürekliliğinin önem kazanmasıyla iş sürekliliği konusunda çeşitli çalışmalar yapılmıştır. İş sürekliliğine yönelik ulusal çalışmalar çoğalmış ve birden fazla yönetim çerçevesi ortaya çıkmıştır. Bu çalışmalardan en iyi bilineni BS25999 standardı İngiltere tarafından oluşturulmuştur. Daha sonra bölgesel standartların yerini ISO 22301 iş sürekliliği yönetim sistemi – gereksinimler standardı almıştır. Kurumlar teknolojinin gelişmesi ve yaygınlaşasıyla teknolojinin nimetlerinden faydalanabilmek için iş süreçlerinin büyük bir kısmını elektronik ortama aktarmışlardır. Müşteri bilgileri elektronik ortamlarda tutulmakta ve işlenerek müşterilere sunulmaktadır. Çalışmanın yapılacağı kurum, alışıla gelmiş kâğıt reçeteleri bile elektronik ortama aktararak e-reçete şekline getirmiştir. Öneminden dolayı bu çalışma bir kurumun bilişim hizmetlerinin sürekliliğine odaklanmıştır. Risk analizi, iş sürekliliğinde en önemli hususlardan birisidir. Bu çalışma farklı alanlarda kabul görmüş risk analizi tekniklerinin bilgi teknolojileri alanında uygulanmasının mümkün olduğunu göstermeyi amaçlamıştır. Kurum uygulamalarından AHP yöntemi ile bir uygulama seçilmiştir. Seçilen uygulama bütün bileşenleri ile bir sistem olarak ele alınmıştır. Seçilen Sistem ÖTL, HTEA ve HAZOP risk analizi teknikleri ile analiz edilmiştir. Çalışmanın çıktısı olarak üst seviye aksilikler, ön tehlike listesi, kritik sistem fonksiyonları, sistem riskleri ve risk matrisi elde edilmiştir. Sonuçların analiz edilmesi yoluyla çeşitli öneriler geliştirilmiştir.

Bilim Kodu : 902.1.121
Anahtar Kelimeler : İş sürekliliği, hizmet sürekliliği, risk analizi, bilişim, sistem, HTEA, HAZOP, ÖTL, İSO
Sayfa Adedi : 154
Danışman : Yrd. Doç. Dr. Talip KELLEGÖZ

IT SERVICES CONTINUITY RISK ANALYSIS: A PUBLIC OFFICE CASE STUDY

(M. Sc. Thesis)

İsmail İLTER

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

December 2015

## ABSTRACT

As a result of the increasing importance of business continuity, it has been studied many times. End of the studies, some national management frameworks produced. The best known of these standards is BS25999 standard which has been created by the UK standard institution. Then, the ISO 22301 business continuity management systems - Requirements standard has been replaced by regional standards. With the development and expansion of technology, Institutions transfer a large part of their business processes into electronic environment in order to benefit from the technology's blessings. Customer information is kept in electronic form and processing are presented to customers. The institution at which this study is done has transferred accustomed paper prescriptions to electronic media and transferred them to e-prescriptions. This study focused on the continuity of an organization's IT services because of its importance. Risk analysis is one of important issues in business continuity. This study aims to show that it is possible to apply some effective risk analysis techniques to the IT field. First, one of software applications used in the Institution is selected by using Analytic Hierarchy Process. The selected application is considered as a system with all its components. Selected system was analyzed by using the risk analysis techniques: Primarily Hazard Analysis, Failure Modes and Effects Analysis and Hazard and Operability Analysis. Top-level mishaps, preliminary hazard list, critical system functions, risks and risk matrix are obtained as an output of the case study. Various necessary suggestions have been developed through the analysis of the results.

Science Code : 902.1.121
Key Words : Business continuity, service continuity, risk analysis, information, system, HAZOP, FMEA, PHL, ISO
Page Number : 154
Supervisor : Asst. Prof. Talip KELLEGÖZ

# TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren tez danışmanım Yrd. Doç. Dr. Talip KELLEGÖZ'e ayrıca çalışma arkadaşlarım Abdullah ERKAN'a, Oktay YILMAZ'a, Abbas DURAK'a, M. Bora TEOMAN'a, Ramazan POLAT'a, Y. Eren ÇİFTÇİ'ye, Erkan SARIÇOBAN'a, Emre KENDİRCİOĞLU'na, Taner ALTUNTAŞ'a ve çalışmalarım sırasında desteğini esirgemeyen aileme teşekkür ederim.

# İÇİNDEKİLER

**Sayfa**

ÖZET ..... iv

ABSTRACT ..... v

TEŞEKKÜR ..... vi

İÇİNDEKİLER ..... vii

ÇİZELGELERİN LİSTESİ ..... x

ŞEKİLLERİN LİSTESİ ..... xiii

KISALTMALAR ..... xiv

1. GİRİŞ ..... 1

2. LİTERATÜR TARAMASI ..... 5

3. İŞ SÜREKLİLİĞİ ..... 21

3.1. İş Sürekliliği Yönetim Sistemi Standartları ..... 22

3.1.1. ISO 22300 iş sürekliliği terimleri ..... 22

3.1.2. TS ISO 22301 Standardı ..... 23

3.1.3. ISO/IEC 27031 Bilgi ve iletişim teknolojileri için iş sürekliliği yönergeleri ..... 31

3.1.4. BS 25999 Standardı ..... 32

4. RİSK ANALİZİ ..... 33

4.1. Tehlike Teorisi ..... 36

4.2. Tehlike Analiz Tipleri ..... 38

4.3. Tehlike Analizi Teknikleri ..... 38

4.3.1. Ön tehlike listesi ..... 39

4.3.2. Ön tehlike analizi ..... 40

4.3.3. Alt sistem tehlike analizi ..... 41

4.3.4. Sistem tehlike analizi ..... 42

**Sayfa**

4.3.5. Hata türleri ve etkileri analizi ....42

4.3.6. Tehlike ve işletilebilirlik analizi (HAZOP) ....47

4.3.7. Hata ağacı analizi ....48

4.3.8. Olay ağacı analizi ....49

4.4. Riske İlişkin ISO Standartları ....49

4.4.1. ISO 27005: Bilgi teknolojileri risk teknikleri-bilgi güvenliği risk yönetimi standardı ....50

4.4.2. ISO 31000:2009 Risk yönetimi prensipleri ve rehber ....50

4.4.3. ISO IEC 31010:2009 Risk yönetimi - risk değerlendirme teknikleri ..50

5. KAMU KURUMU HAKKINDA ....53

5.1. İçe Sunulan Bilişim Hizmetleri ....54

5.1.1. Yazılım geliştirme hizmeti ....54

5.1.2. Veritabanı hizmeti ....54

5.1.3. Elektronik posta hizmeti ....54

5.1.4. Sanallaştırma hizmeti ....55

5.1.5. Ağ hizmeti ....56

5.1.6. Veri yedekleme hizmeti ....56

5.2. Dışa Sunulan Bilişim Hizmetleri ve Uygulamalar ....58

6. RİSK ANALİZİ UYGULAMASI ....59

6.1. Risk Analizi Uygulanacak Alt Sistemin Seçilmesi ....59

6.1.1. Analitik hiyerarşi prosesi ile alt sistemin seçilmesi ....60

6.1.2. Risk analizi uygulanacak alt sistemin özellikleri ....68

6.2. Risk Analizi Uygulaması ....72

6.2.1. Ön tehlike listesi ve üst seviye aksilikler ....74

**Sayfa**

6.2.2. <Uygulama2> sisteminin HTEA ile analizi .....77

6.2.3. <Uygulama2> sisteminin HAZOP ile analizi .....82

6.3. Risk Analizi Uygulamasının Değerlendirilmesi..... 88

7. SONUÇ VE ÖNERİLER ..... 97

KAYNAKLAR ..... 100

EKLER..... 107

EK-1. FMEA Risk Analiz Tablosu..... 108

EK-2. HAZOP Risk Analizi Tablosu..... 134

ÖZGEÇMİŞ ..... 154

# ÇİZELGELERİN LİSTESİ

**Çizelge** **Sayfa**

Çizelge 2.1. İş Sürekliliği ve Riske İlişkin Örnek Çalışmalar ..... 10

Çizelge 2.2. Petro Kimya Alanındaki Örnek HAZOP Çalışmaları ..... 13

Çizelge 2.3. Güvenilirlik Alanındaki HTEA Analiz Tekniği Çalışmaları ..... 18

Çizelge 3.1. Yönetim Sistemi için PUKÖ Modeli ..... 25

Çizelge 4.1. Tehlikeli Bileşen Örnekleri ..... 37

Çizelge 4.2. Sistem Hayat Evresi ve Öncelikli Teknikler ..... 39

Çizelge 4.3. HTEA'nın Orijini ..... 43

Çizelge 4.4. Genel HAZOP parametreleri ..... 48

Çizelge 6.1. Standart Tercih Tablosu-Önem Skalası ..... 63

Çizelge 6.2. İtibar Kaybı Açısından Uygulama Karşılaştırma Matrisi ..... 63

Çizelge 6.3. Aciliyet Açısından Uygulama Karşılaştırma Matrisi ..... 64

Çizelge 6.4. Bağlantılı Sunucu Sayısına Göre Uygulama Karşılaştırma Matrisi ..... 64

Çizelge 6.5. Provizyon Sayısı Açısından Uygulama Karşılaştırma Matrisi ..... 64

Çizelge 6.6. $S_1$ Sütun Vektörü ve Hesaplama Tablosu ..... 65

Çizelge 6.7. $S_2$ Sütun Vektörü ve Hesaplama Tablosu ..... 65

Çizelge 6.8. $S_3$ Sütun Vektörü ve Hesaplama Tablosu ..... 65

Çizelge 6.9. $S_4$ Sütun Vektörü ve Hesaplama Tablosu ..... 65

Çizelge 6.10. Sütun Vektörlerinin Matris Görünümü ..... 66

Çizelge 6.11. Değerlendirme Kriterleri Karşılaştırma Matrisi ..... 66

Çizelge 6.12. Değerlendirme Kriterleri Ağırlık Vektörü ve Hesaplama Tablosu ..... 67

Çizelge 6.13. Sütun Vektörleri ile Öncelik Vektörünün Çarpılması ..... 67

Çizelge 6.14. Uygulama Puanları ..... 68

Çizelge 6.15. Risk Analizi Olasılık Ölçeği ..... 72

**Çizelge** **Sayfa**

Çizelge 6.16. Risk Analizi Şiddet Tablosu ..... 73

Çizelge 6.17. Tipik Bilgi Güvenliği Tehditleri ..... 74

Çizelge 6.18. Ön Tehlike Listesi ..... 75

Çizelge 6.19. Üst Seviye Aksilikler ve Kritik Sistem Fonksiyonları ..... 76

Çizelge 6.20. HTEA Bileşenleri için Sorular ..... 78

Çizelge 6.21. Hata Modlarını Belirlemek için Sorulan Sorular ..... 78

Çizelge 6.22. Hata Modlarının Sebeplerini Belirlemek için Sorulan Sorular ..... 78

Çizelge 6.23. Hata Modlarının Etkilerini Belirlemek için Sorulan Sorular ..... 79

Çizelge 6.24. Soğutma Alt Sistemi için Başarısızlık Modları ..... 80

Çizelge 6.25. Enerji Alt Sistemi için Başarısızlık Modları ..... 80

Çizelge 6.26. Uygulama Yazılımı için Başarısızlık Modları ..... 81

Çizelge 6.27. Bilişim Personeli için Başarısızlık Modları ..... 81

Çizelge 6.28. Sunucu Donanımı için Başarısızlık Modları ..... 81

Çizelge 6.29. Ağ Cihazları için Başarısızlık Modları ..... 82

Çizelge 6.30. VTYS Yazılımı için Başarısızlık Modları ..... 82

Çizelge 6.31. Soğutma Alt Yapısının Sistem Parametreleri ve Anahtar Kelimeleri ..... 83

Çizelge 6.32. Enerji Alt Yapısının Sistem Parametreleri ve Anahtar Kelimeleri ..... 83

Çizelge 6.33. Uygulama Yazılımının Sistem Parametreleri ve Anahtar Kelimeleri ..... 84

Çizelge 6.34. Bilişim Personelinin Parametreleri ve Anahtar Kelimeleri ..... 84

Çizelge 6.35. İşletim Sistemi için Sistem Parametreleri ve Referans Anahtar Kelimeler ..... 84

Çizelge 6.36. Sunucu Donanımı Sistem Parametreleri ve Anahtar Kelimeleri ..... 85

Çizelge 6.37. Ağ Cihazları için Sistem Parametreleri ve Referans Anahtar Kelimeler ..... 85

Çizelge 6.38. Ağ kablosunun Sistem Parametreleri ve Referans Anahtar Kelimeler ..... 85

Çizelge 6.39. VTYS Yazılımının Sistem Parametreleri ve Anahtar Kelimeleri ..... 86

**Çizelge** **Sayfa**

Çizelge 6.40. Yüksekten Düşüğe Sıralanmış İş Sürekliliği Riskleri .....88

# ŞEKİLLERİN LİSTESİ

**Şekil** **Sayfa**

Şekil 3.1. İSYS süreçlerine uygulanan PUKÖ modeli (TSE, 2013).....25

Şekil 4.1. ISO/ IEC 27005'e Göre Risk Yönetim Süreci.....34

Şekil 4.2. L Tipi Risk Matrisi .....35

Şekil 4.3. Örnek ÖTL Analiz Formu .....40

Şekil 4.4. Örnek Ön Tehlike Analiz Formu.....41

Şekil 4.5. FMEA Çeşitleri.....45

Şekil 4.6. HTEA Konsepti .....46

Şekil 4.7. Fonksiyonel Sistem Bakışı .....46

Şekil 4.8. Yapısal Sistem Bakışı.....47

Şekil 6.1. En Uygun Uygulama Seçimi için Analitik Hiyeraşi Süreci .....62

Şekil 6.2. <Uygulama2> Sistem Topolojisi.....68

Şekil 6.3. <Uygulama2> Sisteminin Mimarisi .....69

Şekil 6.4. <Uygulama2> Sisteminin Sunduğu Web Servis Şeması.....69

Şekil 6.5. <Uygulama2> Sisteminin Sunduğu Uygulama Şeması.....70

Şekil 6.6. <Uygulama2> Sistemi Fonksiyonel Görünümü .....70

Şekil 6.7. <Uygulama2> Sistemi Yapısal Görünümü.....71

Şekil 6.8. HTEA Analizi Yapılırken Kullanılan Form .....79

Şekil 6.9. HAZOP Gerçekleştirme Akış Şeması .....87

Şekil 6.10. Kullanılan HAZOP Analiz Formu.....88

Şekil 6.11. Risk Matrisi .....96

# KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

| Kısaltmalar | Açıklama |
|---|---|
| **AHP** | Analitik Hiyerarşi Prosesi |
| **BGYS** | Bilgi Güvenliği Yönetim Sistemi |
| **BİT** | Bilgi ve İletişim Teknolojileri |
| **BT** | Bilgi Teknolojileri |
| **HAA** | Hata Ağacı Analizi (Fault Tree Analysis) |
| **HTEA** | Hata Türleri ve Etkileri Analizi (FMEA) |
| **HAZOP** | Tehlike ve İşletilebilirlik Analizi (HAZOP) |
| **ISO** | Uluslararası Standart Kuruluşu |
| **ITIL** | Bilgi Teknolojileri Alt Yapı Kütüphanesi |
| **İEA** | İş Etki Analizi |
| **İSYS** | İş Sürekliliği Yönetim Sistemi |
| **MTPoD** | Maksimum Kabul Edilebilir Kesinti Süresi |
| **OAA** | Olay Ağacı Analizi (Event Tree Analysis) |
| **ÖTA** | Ön Tehlike Analizi |
| **ÖTL** | Ön Tehlike Listesi (Preliminary Hazard List) |
| **RPO** | Kabul Edilebilir Veri Kaybı |
| **RTO** | Kabul Edilebilir Kesinti Süresi |
| **UEKAE** | Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü |
| **VT** | Veri Tabanı |
| **VTSY** | Veritabanı Yönetim Sistemi |

# 1. GİRİŞ

Hızla gelişen ve değişen dünyada günlük hayatımızla beraber iş dünyası da gelişmekte ve karmaşık bir hal almaktadır. 1900'lerin başına kadar yapılan fiziki işler bilgi çağında yapılan işlerin bir parçası haline gelmiştir. Daha da somutlaştırılırsa bir binayı inşa etmek günümüzde bir veri merkezi kurmanın sadece bir adımıdır. İş kavramının karmaşıklaşması ve çok sayıda zincirleme faaliyetler sonucu ortaya çıkmasından dolayı bu faaliyetler zincirinin herhangi birinde meydana gelen bir başarısızlık yapılan işin tamamını kesintiye ya da başarısızlığa uğratabilmektedir. İş dünyasındaki rekabet ile müşterinin beklentilerinin artması gibi faktörlerden dolayı yapılan işlerdeki kesinti ya da başarısızlıkların maliyeti kurum ve kuruluşlar için çok daha ağır olabilmektedir. Taşımacılık şirketleri, 1980'lerde gerekli gördükleri durumda otobüs seferlerini bir gün veya daha fazla erteleyebilmekte[1] ve bu durumu olağan karşılamaktaydılar. Ancak günümüzde başka bir şehirdeki iş görüşmesine yetişmek isteyen bir yolcu bir günlük sefer gecikmesinde bilet ücretini talep etmekte, bir saat kadar gecikmelerde ise yolcular bu durumdan rahatsız olmaktadır. Memnuniyetsizlik yaşayan yolcular, sonraki yolculuklarında farklı şirketleri tercih ettiklerinden seferleri gecikmeli gerçekleştiren otobüs şirketleri müşteri kaybetmektedirler.

İşleri kesintiye uğratan ya da başarısız kılan olaylar planlı değildirler. Kesinti sebebi olan olaylar daha çok bazı başarısızlıklar gibi istenmeyen olaylardır. İş sürekliliğinin tam olarak sağlanabilmesi için planlanmamış istenmeyen olayların yönetilebilmesi gerekir. Bu durumda risk kavramı ortaya çıkmaktadır. Risk, istenmeyen bir olaya yönelik ve bu olayın sonuçlarının şiddetini ve meydana gelme olasılığını da içermektedir. İstenmeyen olayların olma olasılığının ve/veya olumsuz sonuçlarından kaynaklanan şiddetinin azaltılması ile işlerdeki kesintiler ve başarısızlık durumları da azalır. Kesintiler ve başarısızlıklar kabul edilebilir seviyenin altına çekildiğinde iş sürekliliği sağlanmış olur. İşleri kesintiye uğratan olayların belirlenmesi, tanımlanması, olasılığının tespiti, şiddetinin belirlenmesi, değerlendirilmesi, önlem alınması, olasılığının azaltılması, şiddetinin azaltılması ve izlenmesi risk yönetiminin aşamalarıdır. Dolayısı ile iş sürekliliği ancak başarılı bir risk yönetimi ile mümkündür. Risk analizi ise risk yönetiminin olmazsa olmaz adımıdır. Çeşitli tehlike belirleme ve risk analizi teknikleri mevcuttur. Ancak risk yönetimini yapabilmek için tek başına yeterli ve kapsayıcı ne bir analiz tipi ne de analiz tekniği mevcuttur.

[1] Kamil Koç şirketinin eski şoförlerinin anısından.

Bilgi teknolojilerinin gelişmesiyle elle yapılan birçok işlem elektronik ortama aktarılmıştır. İş süreçlerinin büyük bir kısmının elektronik ortama aktarılması ile de süreçler daha kısa zamanda daha kolay gerçekleşir olmuştur. Dolayısı ile işlem sayısı da artmıştır. İşlemlerin sayısının artması sonucunda kayıt altına alınması gerekli olan bilgi miktarı da artmıştır. Artan bilgiyi saklama ve işleme ihtiyacı; kurum ve kuruluşları teknolojiye daha bağımlı hale getirmiştir. İşverenler, ücretleri elden vermek yerine banka hesaplarına yatırmakta, çalışanlar bankadaki paralarını zorunlu olmadıkça nakit olarak çekmemektedirler. Alışverişlerin karşılığında fiziksel para yerine bankamatik kartları ve kredi kartları kullanılmaktadır. Dolayısıyla piyasada fiziksel para değil paranın kimden kime gittiği bilgisi tutulmaktadır. Şüphesiz bu bilgiler bankaların ve işletmelerin bilgi sistemlerinde tutulmaktadır. Hizmetlerinin sadece bir kısmını elektronik ortama aktaran şirketler olduğu gibi işlerini tamamen bilişim hizmetlerine dayalı yapan şirketler de bulunmaktadır. Google, Facebook ve Whatsapp gibi şirketler; yüksek oranda bilişim teknolojilerine dayalı hizmet veren şirketlere örnek gösterilebilirler. Kurum ve kuruluşlar tarafından verilen hizmetlerin büyük çoğunluğu bilişim teknolojilerine dayalı olmasa dahi kritik süreçlere ait az sayıda işlem elektronik ortama aktarılmış olduğundan yapılan işlerin kurumun bilişim teknolojilerine sıkıca bağlı olduğu söylenebilir. Toplu taşıma ve ulaştırma hizmeti veren bir havayolu şirketinin asıl işi, dolayısıyla amacı, yolcularını varacakları yere vaktinde sağlıklı koşullarda ulaştırmaktır. Ancak bilet satış, rezervasyon ve kontrol yapan *bilgi sistemlerinin* çalışmaması bütün hizmetlerin durmasına sebep olmakta ve bu durum ya uzun iş kesintilerine yol açmakta ya da büyük bir memnuniyetsizlik doğurmaktadır.

Yukarıdaki bilgiler göz önüne alındığında bir kurumun bilişim hizmetlerinin/teknolojilerinin sürekliliğinin sağlanmasının iş sürekliliği açısından kritik öneme sahip olduğu görülür. Diğer bir ifadeyle, bir kurumun iş sürekliliğini sağlamanın ön aşamalarından biri bilişim hizmetlerinin iş sürekliliğinin sağlanmasıdır. Bu amaçla Uluslararası Standart Organizasyonu (ISO) sadece *ISO 22301 iş sürekliliği yönetim sistemi* standardını oluşturmakla kalmayıp, *ISO 27031 bilgi ve iletişim teknolojileri için iş sürekliliği yönergeleri* standardını da oluşturmuştur.

Bu çalışma, bir kamu kurumunun bilişim hizmetlerine yönelik sürekliliğin dayandırılacağı risk analizini kapsamaktadır. Risk yönetiminin risk iyileştirme ve izleme aşamaları kurumun yetki ve sorumluluğundadır. Bu aşamalar hem zaman alıcı olduğundan hem de kapsamı genişleteceğinden dolayı çalışmaya dâhil edilmemiştir. Ancak iyileştirme önerileri

sunulmuştur. Gizlilik ve güvenlik kaygısından dolayı çalışmanın yapıldığı kurumun adı dâhil özel ve gizli bilgiler ya çalışmanın dışında bırakılmış ya da maskelenmiştir.

Çalışmanın ikinci bölümünde yapılan literatür taramasına yer verilmiştir. Bütüncül bir bakış açısı kazandırması açısından ve öneminden dolayı ayrı bir bölüm ayırma gereği duyulmuştur. İş sürekliliği, risk analizi, FMEA, HAZOP anahtar kelimeleri ve bunların kombinasyonları kullanılarak araştırma yapılmıştır.

Çalışmanın üçüncü bölümünde iş sürekliliğine değinilmiştir. Ayrıca *ISO 22301 iş sürekliliği yönetim sistemi* ve *ISO 27031 bilgi ve iletişim teknolojileri için iş sürekliliği yönergeleri* standartları incelenmiştir.

Çalışmanın dördüncü bölümünde tehlike ve risk analizine değinilmiştir. Tehlike analizi tipleri ve teknikleri anlatılmıştır. Yapılan çalışma için uygun olduğu düşünülen analiz teknikleri detaylandırılmıştır. Ayrıca *ISO 31000 risk yönetimi – prensipler ve kılavuzlar* ve *ISO 31010 risk yönetimi – teknikler* standartları incelenmiştir.

Çalışmanın beşinci bölümünde risk analizi yapılan kamu kurumu hakkında bilgi verilmiştir. Kuruma ait bilişim alt yapısı ile kurumun sunmuş olduğu bilişim hizmetleri anlatılmıştır.

Çalışmanın altıncı bölümünde tehlike belirleme ve risk analizi uygulaması yapılmıştır. Bütün sistem için risk analizinin yapılması mümkün olmadığından analitik hiyerarşi prosesi (AHP) ile belirlenen kriterler ışığında risk analizi yapılacak sistem (yazılım uygulaması ve ilgili bileşenler) seçilmiştir. Yapılacak olan uygulama için hangi analiz tekniklerinin daha uygun olduğuna karar verilmiştir. İlk olarak Ön tehlike listesi (ÖTL) ve üst seviye aksilikler belirlenmiştir. Daha sonra HTEA ve HAZOP analiz teknikleri ile sistem üzerindeki tehlike belirlenerek risk analiz edilmiştir.

Çalışmanın en son bölümünde sonuç ve önerilerden bahsedilmiştir. Çalışmanın amacına ulaşıp ulaşmadığı hakkında bilgi verilmiştir. Çalışmadan elde edilen bilgi ve tecrübelere dayanılarak önerilerde bulunulmuştur.

# 2. LİTERATÜR TARAMASI

Bu çalışmanın hazırlık ve uygulama aşamalarında literatür taraması yapılmıştır. Literatür taramasında görülen çalışmaların bazılarına ilgili bölümlerde konu geçtikçe değinilmiştir. Ancak bütüncül bir bakış açısı kazandırması açısından ve öneminden dolayı ayrı bir bölüm ayırma gereği duyulmuştur. Çalışmanın bu bölümünde iş sürekliliği, risk analizi, HTEA, HAZOP, AHP anahtar kelimeleri ve bunların kombinasyonları kullanılarak ulaşılan kaynaklara değinilmiştir. Bilişim hizmetlerinin sürekliliği konusunda HTEA ya da HAZOP tekniklerini kullanan herhangi bir çalışmaya ulaşılamadığından ilk olarak iş sürekliliği ve risk analizi kapsamında benzer çalışmalardan kısaca bahsedilmiştir. Ayrıca HAZOP ve HTEA tekniğini kullanan güvenilirlik çalışmalarından odaklanılmıştır.

İş sürekliliğine yönelik çalışmalar incelenirken Scopus ve diğer veritabanlarında bulunan sadece İngilizce makalelerden başlıkta "risk" ve "business continuity" geçen (tıp, filozofi, biyoloji ve ziraat hariç) risk analizine ilişkin makalelere ulaşılmıştır. Ayrıca Yükseköğretim Kurulu tez merkezinde bulunan iş sürekliliğine yönelik yüksek lisans çalışmaları da dâhil edilmiştir.

Sahebjamnia Torabi ve Mansouri (2015) Gear Box şirketinin üretim aşamalarında iş sürekliliği çalışması yapmışlardır. Yöntem olarak önemli ürün ve kritik süreçler üzerinde iş etki analizi (İEA) metodunu kullanmışlardır.

MohdRashid, Loke, ve Ooi (2014) iş sürekliliği için tedarik zinciri risk yönetimi uygulama çalışması yapmışlardır. Japonyadaki deprem ve tsunami sonrasında Malezya elektronik endüstrisinde tedarik zincirinin sağlamlığı, dayanıklılığı, esneklik ve çeviklik değerlendirilmesi yoluyla mevcut iş tedarik zinciri risk yönetimi uygulamalarını belirlemeyi amaçlamışlardır. Başarılı bir tedarik zinciri risk değerlendirmesinin iş sürekliliğini makul derecede ilerlettiğini gözlemlemişlerdir. Ayrıca tedarik zincirinin sağlamlığı, dayanıklılığı, esnekliği ve çevikliği ile firmaların sürdürebilirliğini değerlendirebilecek kavramsal bir çerçeve önermişlerdir.

Blos, Wee ve Yang (2012) çeşitli sebeplerden dolayı tedarik zincirindeki risklerin oldukça kritik olduğundan yola çıkarak iş sürekliliği ve esnekliğine yönelik tedarik zinciri risk

değerlendirmesi yapmışlardır. Tedarik zinciri esnekliği ve iş sürekliliği sağlamak amacıyla riskli bir tedarik zinciri kararının daha iyi nasıl alınabileceği konusunda genel fikir vermişlerdir.

Kawaguchi (2012) Japonyada meydana gelen deprem ve tsunami belirlenen eşik değerleri aşmış ve hasar miktarı komitelerin belirlediği üst sınırları geçmiştir. Araştırmacı bu depremden hemen sonra yerli şirketler arasında yapılan anket sonuçlarına dayanarak iş sürekliliği yönetimi açısından beklenmedik afetler sorunu üzerinde durmuştur. Beklenmedik felaket sorununun karakteristiklerini ortaya koymuşlardır.

Tammineedi (2010) BS 25999 standardına dayalı iş sürekliliği çalışmasında standarttaki adımları anlatarak iş sürekliliği yönetim sisteminin kavramsal düzeyde anlaşılmasını sağlamaya çalışmıştır. İş sürekliliğinde anahtar nitelikteki işleri Olay Öncesi Hazırlık, Olay Yönetimi ve Olay Sonrası Süreklilik şeklinde üç safhada sınıflandırmıştır. Araştırmacı tarafından risk değerlendirmesi ve iş etki analizi (İEA) de yapılmıştır.

Sakai ve diğerleri (2010) risk yönetimi ve iş sürekliliği yönetimi için bilgi ve iletişim teknolojileri (BİT) kullanımını ele almıştır. Felaket anlarında hükümet ile vatandaşlar arasında bilgi aktarımını sağlayabilecek alternatif iletişim kanallarına sahip Felaket Önleme Bilgi İletim Kontrol Merkez çözümünü ortaya koymuşlardır.

Gibb ve Buchanan (2006) çalışmalarında iş sürekliliği yönetimi programının tasarımı, uygulaması ve izlemesi için yeni bir çerçeve model önermektedir. Önerdiği model için iş etki analizi (İEA) metodunu kullanmışlardır.

Okeahalam (2006) Güney Afrika'da iş sürekliliği ve risk değerlendirme alanındaki çalışmasında ödemeler sistemlerinin işleyişi ile ilgili risklerin etkisini analiz etmiştir. Ayrıca ödemeler sisteminde iş sürekliliği yönetiminin önemini incelemek için teorik bir çerçeve önermişlerdir.

Walker (2006) dış kaynak kullanımı ve iş sürekliliği riskleri üzerinde yaptığı çalışmada şirketlerin kritik bazı iş süreçlerini Asya'ya kaydırmak suretiyle kâr paylarını arttırmaya çalıştıklarını ancak dış kaynak kullanımından kaynaklanan riskleri göz ardı ettiklerini ifade etmiştir. Araştırmacı çoğu şirketin dış kaynak kullanımına başlarken sözleşmeler ve servis

seviye anlaşması yaparak avantaj sağlamaya çalıştıklarını ancak dış kaynakların sunucu odalarındaki elektrik kesintileri gibi iş sürekliliği ihlal olaylarını dikkate almadıklarını ifade etmiştir. Araştırmacı dış kaynak kullanımında riskleri azaltmaya yönelik önerilerde bulunmuştur.

Jrad, Morawski ve Spergel (2004) iş sürekliliği planlarının reaktiften (felaket sonrası kurtarma) proaktif olmaya (felaketlere hazır olma) dönüşmesinden yola çıkarak telekomünikasyon şebekeleri için yeni bir iş sürekliliği hazır bulunurluk modeli sunmuştur. Felaketleri, doğa olayları, teknik arızalar ve insani tehditler olmak üzere üçe ayırmış ve modellemişlerdir. Potansiyel etki ve riski ölçmek ayrıca mâruziyeti azaltmaya yönelik belirli önerilerde bulunmak için bu modellerin nasıl kullanılacağını göstermişlerdir.

Literatür taramasını genişletmek ve ulusal çalışmalara da değinmek amacıyla Yükseköğretim Kurulu tez merkezindeki iş sürekliliği konulu yüksek lisans tezleri ve referans gösterilen bazı makaleler de incelenmiştir.

Yakın (2015) raylı sistemlerde risk değerlendirme tekniği için tek bir tekniğin yeterli olmadığını ifade etmiştir. Yazar İstanbul Ulaşım AŞ Bünyesindeki bir demiryolu işletmesinin yerel olarak sinyalizasyonunun yapılması sırasında karşılaşılan risklerden örnekler alarak güvenilirlik, emre amadelik sürdürülebilirlik ve emniyet (RAMS) yönetimi için HTEA ve hata ağacı analizi (HAA) teknikleri ile risk analizi yapmıştır.

Khalilov, (2015) endüstriyel tesislerin SEVESO II den SEVESO III'e geçmesine katkıda bulunmak ve örnekleme için BOTAŞ (Boru Hatları ile Petrol Taşıma) A.Ş. tesisi incelemiştir. Çalışmasında HAZOP a vurgu yapmıştır. Tesis'de bulunan eksikler belirlenmiş, kantitatif risk değerlendirmesine göre belirlenen kritik ve tehlikeli ekipmanlar ve olası risklere uygun senaryolar yazılmış ve bu senaryoların gerçekleşmesi durumunda tesisin görebileceği zararları ve ekosisteme olacak etkileri yazılım programı ile belirlemiştir. Patlama, yangın, termal ve yayılım gibi modelleri elde etmiştir.

Okumuş (2015), taşyünü üretimi sırasında oluşan hata türlerini tespit etmek için AHP, HTEA ve Taugichi tekniklerini birlikte kullanmıştır.

M. Silva, Gusmao, Poleto, L. Silva ve Costa (2014) Bilgi Güvenliği Yönteminde BT bileşenlerinin yavaşlaması, ağ ve sistem arızaları, bilgi sızıntısı ve bilgi kaybı, mali kayıplar ve iş faaliyetlerinin bozulması gibi durumları önlemek için risk değerlendirmesi yapmıştır.

Öcelan (2014) petrokimya rafinerisi benzen giderme ünitesi üzerinde tank yangını kritik olayının kök tehlikelerini belirleme ve tank yangını kritik olayını önlemeye veya bu olayın önlenememesi durumunda yangın olayının etkilerini sınırlandırılmaya yönelik insani ve teknik güvenlik tedbirlerini (bilimsel ve sistematik olarak tespit edilen) belirlemek amacıyla 11 aşamadan oluşan bir çalışma yapmıştır. Oktan artışının sağlanması amacıyla nikelli katalizör eşliğinde gerçekleşen ekzotermik hydrotreating prosesi üzerinde tehlike ve işletilebilirlik analizi (HAZOP) metodolojisi ile HAA ve olay ağacı analizi (OAA) çalışmaları birlikte gerçekleştirmiştir.

P. Ping, Xinyue, Y. Ping ve Huiling (2014) çalışmalarında iş sürekliliği analizinin iş sürekliliği yönetimi için çok önemli olduğunu ifade etmişlerdir. Çalışma, bilgi sistemleri güvenliği yönetiminde iş sürekliliği faktörlerini analiz etmektedir. İş sürekliliği hizmetleri için SPN modelinin basitleştirilmiş şekli kullanılmıştır.

Çakıl (2014) e-Ticaret Güvenliği alanındaki çalışmasında güvenlik tehditlerinden ve önlemlerinden bahsetmiştir. Çalışmanın bir bölümünde ise felaket kurtarma ve iş sürekliliği ele almıştır.

Sembiring ve Siregar (2013) çalışmalarında kurumsal mimari modelinde bir değişken olarak riski etkileyen bazı faktörleri açıklamışlardır. Felaket kurtarma merkezinde (FKM) bilgi teknolojileri (BT) risklerinin yönetimi için genel bir faktör olarak matematiksel bir fonksiyon türetmişlerdir. Bu formül ile FKM için riskler için karar verme modeli geliştirmişlerdir.

Aydemir (2013) İstanbul metrosunda iş sürekliliği çalışmasında raylı sistemlerden olan metro sistemini incelemiş ve metro istasyonlarında iş sürekliliği yönetimi hakkında bilgi vermiştir. Ayrıca kritik süreçlerin önemlerini hesaplayabilmek için AHP kullanmışlardır.

Tanrıverdi (2013) çalışmasında kimyasal proses endüstrisinde yer alan reaktörler, damıtma kolonları, ısı değiştirici, buharlaştırıcı, yoğuşturucu, Santrifüj Pompa/Kompresör, kurutucular için HAZOP formları oluşturmuştur. OAA yaparak, sistemde yıllık devam eden, durdurulan ve kontrolden çıkan olaylar hesaplamıştır. HAA yaparak, arızaya neden olabilecek tüm olayların arıza/yıl olasılıkları hesaplamıştır.

Babaarsalan (2013) TÜRPAŞ Kırıkkale Rafinerisinde, Atmosferik damıtma ünitesinde bulunan Atmosferik Damıtma Kolonuna ve giriş-çıkış hatlarına, Avrupa Komisyonu'nun V. Çerçeve Programı tarafından desteklenerek oluşturulmuş olan ARAMIS metodolojisini uygulamıştır. Aynı çalışma alanına HAZOP risk değerlendirme metodolojisini de uygulayarak Bow-tie analizinde yer alan kök nedenleri güçlendirmiştir.

Kocamustafaoğulları (2013) bilgi güvenliği prototip çalışmasında, bilgi güvenliğinin iş sürekliliğinin sağlanabilmesi için bilginin tehditlere karşı korunması olarak ifade etmiştir.

Taş (2010) HTEA çeşitlerinden biri olan proses HTEA çalışmasının mobilya endüstrisine yönelik örnek bir uygulama yapmıştır. Araştırmayı CNC makinelere sahip, kalite güvencesine yönelen bir işletmede gerçekleştirmiştir. Araştırma sonucunda, olası hata türleri ortaya çıkmış ve bu hata türleri tanımlamıştır. İşletme için hata oluşumunu önleme yönelik rehber sayılabilecek nitelikteki örnek faaliyetler yapmış ve kalitesizlik maliyetlerinin düşürülmesi sağlamıştır. Risk öncelik gösterge değerlerinde yaklaşık 3 kat azalma gerçekleşmiştir. İşletmede kalite güvencesinin sağlanmasına yönelik önemli bir gelişme sağlamıştır.

Tunçelli (2006) HTEA modeli ile en iyi kavramsal tasarım alternatiflerini seçmek ve sistem tasarım şartnamelerine karar verebilmek amacıyla helikopter pilot koltuğuna uygulamıştır. Helikopter pilot koltuğunda çıkabilecek olası arızaların ve ilgili sebeplerinin ele alınması ve çözümlenmesiyle, ürünün kalite, emniyet ve güvenilirliğini sağlamaya yönelik, tasarım aşamasında gerekli değişikliklerin yapılmasını hedeflemiştir.

Durhan (2006) tez çalışmasında iş sağlığı ve güvenliği yönetim sistemine sahip çelik boru imalatı yapan bir fabrikada, HTEA tekniği ile risk değerlendirme çalışması yürütmüştür. Uygulamanın başarılı sonuç verdiği ve yöntemin etkin olduğu değerlendirilmiştir.

Şamur (2005) tez çalışmasında, yetkili otomotiv servislerinde meydana gelen hataları anket çalışması ile saptamıştır. Hataların tekrarlanan ve önemli olanlarının belirlenmesi için Pareto Analizi uygulamıştır. Hataların meydana gelme sebebi Sebep-Sonuç (Fishbone) tekniği ile analiz edilmiştir. Bu aşamalardan sonra HTEA yöntemine geçilmiş her hatanın oluşma olasılık derecesi, şiddet derecesi ve belirleme derecesi belirlenerek risk öncelik göstergesi hesaplanmıştır. Araçta meydana gelen spesifik amortisör hatasını ortadan kaldırılması için HAA uygulamıştır.

Literatür taraması sonucunda ulaşılan iş sürekliliğine ilişkin çalışmalar kullandıkları yönteme göre analiz edilmiştir. İş sürekliliğini üst seviyede ele alıp belirli bir yöntem kullanmadan sadece iş sürekliliği yönetimine odaklananlar olduğu gibi iş sürekliliğinde detaya giren araştırmacılar daha çok iş etki analizi yöntemini kullanmışlardır. Bilişim hizmetlerinin sürekliliğine yönelik detaylı çalışmaya rastlanmamıştır. Ulaşılan iş sürekliliği ve risk analizine ilişkin çalışmaların listesi Çizelge 2.1'de verilmiştir.

Çizelge 2.1. İş Sürekliliği ve Riske İlişkin Örnek Çalışmalar

| **Yazar** | **Yıl** | **Kullanılan Analiz Tekniği** | **Kullanım Alanı** |
|---|---|---|---|
| Sahebjamnia Torabi ve Mansouri | 2015 | İş Etki Analizi (İEA) | Üretim aşamalarında önemli ürün ve kritik süreçler üzerinde iş sürekliliği analiz çalışması yapmışlardır. |
| MohdRashid, Loke, ve Ooi | 2014 | Yok | Tedarik zinciri risk yönetimi uygulama çalışması. |
| Blos, Wee ve Yang | 2012 | Yok | İş sürekliliği ve esnekliğine yönelik tedarik zinciri risk değerlenndirmesi |
| Kawaguchi | 2012 | Yok | Japonyada iş sürekliliği yönetimi açısından beklenmedik afetler. |
| Tammineedi | 2010 | İş Etki Analizi (İEA) | BS 25999 standaradına dayalı iş sürekliliği çalışması ve risk değerlendirmesi. |
| Sakai ve diğerleri | 2010 | Yok | Risk yönetimi ve iş sürekliliği yönetimi için BİT kullanımını ele almıştır. |

Çizelge 2.1. (devam) İş Sürekliliği ve Riske İlişkin Örnek Çalışmalar

| | | | |
|---|---|---|---|
| Gibb ve Buchanan | 2006 | İş Etki Analizi (İEA) | İş sürekliliği yönetimi programının tasarımı, uygulaması ve izlemesi için yeni bir çerçeve model önermiştir. |
| Okeahalam | 2006 | Yok | Güney Afrikada ödemeler sistemlerinin işleyişi ile ilgili risklerin etkisini analiz etmiştir. |
| Walker | 2006 | Yok | Dış kaynak kullanımından kaynaklanan iş sürekliliği riskleri. |
| Jrad, Morawski ve Spergel | 2004 | Yok | Telekomünikasyon şebekeleri için yeni bir iş sürekliliği hazır bulunurluk modeli sunmuştur. |

Yükseköğretim Kurulu tez merkezindeki Analitik Hiyerarşi Prosesi yöntemini kullanan yüksek lisans tezleri ve referans gösterilen iki adet makale incelenmiştir. Tedarikçi seçimi, yer seçimi ve uçak seçimi gibi çeşitli sorunlara AHP ile çözüm bulunduğu görülmüştür.

Tatar (2015) bilgi güvenliği standartlarının karşılaştırılması analitik hiyerarşi prosesi (AHP) yaklaşımını kullanmıştır. AHP metodunu kullanarak en iyi bilgi güvenliği standardını seçmeyi amaçlamıştır. Standartlarda yer alan ortak kriterler belirlenmiştir. Alternatifler Expert Choice Programı yardımı ile değerlendirilmiştir. Çalışmanın sonucunda, seçilen kriterlere göre COBIT, ISO 27001 ve ITIL'a göre üstün bulunmuştur. Ancak standartların hiçbirinin tek başına kullanıldığında bilgi güvenliğinde yüzde yüz başarı temin edemediği sonucuna varmıştır.

Kılıç (2015) bulanık-analitik hiyerarşi prosesini kullanarak İstanbul Boğazı'nda deniz kazalarının risk analizini yapmıştır. Çalışmada tüm risk kriterlerinin ağırlıklarını bularak İstanbul Boğazı'nda deniz kaza risklerini ortaya konulması amaçlanmıştır. Metot olarak Bulanık AHP seçilmiştir. Uzmanlık seviyesi yüksek 10 uzmana anket yapılarak anketlerden elde edilen değerler Bulanık AHP'den geçirilmiş ve İstanbul Boğazı'nda deniz kazalarına sebebiyet veren çeşitli ana kriter ve alt kriterlerin her birinin ağırlıkları bulunmuştur.

Civir (2015) maliyetlerin azaltılmasında nitelikli tedarikçiden ucuz ve kaliteli malzeme satın alınmasının öneminden yola çıkarak otomotiv sektöründeki tedarikçi seçimi sorununu çok ölçütlü temele dayandırılarak değerlendirmiştir. İlk aşamada otomotiv sektöründeki tedarikçi seçiminde dikkat edilmesi gereken önemli kriterleri firmalarla anket çalışması yaparak belirlemiştir. Çalışmanın ikinci aşamasında, mevcut ve aday tedarikçileri çok ölçütlü (fiyat, esneklik, kalite v.b.) yapıda değerlendirilerek göreceli olarak sıralayıp belirlenen ölçütler için en uygun tedarikçilerin seçiminde bulanık analitik hiyerarşi prosesinden yararlanmıştır.

Ünlü (2014) çalışma performansının öneminden yola çıkarak Türkiye'de mimarların performanslarını etkileyen demotivasyon kriterlerinin öncelik sırasını Analitik Hiyerarşi Prosesi ve Analitik Ağ Prosesi teknikleri ile belirlemeyi amaçlamıştır. 2012 yılında yayımlanan "Analysis of architects' demotivating factors in design firms" isimli çalışmadan aldığı demotivasyon kriterlerini Gazi Üniversitesi Mimarlık Bölümü hocalarından oluşan bir uzman grubunun görüşlerini alarak Saaty tarafından önerilen 1-9 ölçekli ikili karşılaştırmalar matrisleriyle değerlendirmiştir.

Şener (2014) firmaların tüketiciye ulaşmak için kullanacakları mecraları(reklam kanalları) dikkatli seçmeye özen göstermelerinden yola çıkarak AHP yöntemiyle hızlı tüketim malları için en etkili reklam mecrası seçim sürecini analiz etmiştir. *Nescafe 3ü1 Arada* ürünü seçmiş ve gerekli verileri bazı şirket çalışanları ile ürünün hedef kitlesi olan 18-30 yaş arası 33 birey ile yapılan ikili karşılaştırmalardan oluşan anketler sonucunda elde etmiştir. Çalışma sonucunda seçilen ürün için en etkili reklam mecrasının dijital medya olduğunu tespit etmiştir.

Kır (2012) çalışanların performans değerlendirilmesi amacıyla 360 derece performans değerlendirme sistemini analitik hiyerarşi prosesi ile bütünleştirerek tasarlanan performans değerlendirme sistemini özel bir dershanede öğretmenler üzerinde uygulamıştır.

Yılmaz (2006) havayolu şirketlerinin mevcut filolarına yeni uçak eklemeleri durumunda doğru uçak seçimini yapabilmeleri için çeşitli kriterler belirleyip uçaklar arasında karşılaştırma ve değerlendirme yapmıştır. Airbus A321-200, Airbus A320-200, Boeing B737-800, Boeing B737-900 ve Boeing B737-900X tip uçaklar arasından uçak seçimi sürecinin oluşturulmasında, çoklu kriter içeren karmaşık karar verme problemlerinin

çözümü için tasarlanan AHP modelinden yararlanmıştır. Ayrıca uygulamada belirsiz ve kesin olmayan verileri de göz önüne alarak "Bulanık AHP" uygulaması yapmış ve iki yönetimin sonuçları değerlendirmiştir.

Benzer bir AHP çalışması da Kodalı ve Routroy (2006) tarafından tedarik zincirindeki tesislerin konumlarının seçilmesi üzerine yapılmıştır.

Zahir, (1991) bir kuruluşun işletme lokasyonu belirleme sorunu önceliklendirme yapılarak AHP ile ortadan kaldırmıştır.

Literatür taramasında HAZOP tekniğini kullanan çalışmalar incelenmiştir. HAZOP tekniğinin, kimya ve petrol üretim alanlarında kullanıldığı görülmüştür. Bilişim hizmetlerinin sürekliliğine yönelik HAZOP tekniğini kullanan herhangi bir çalışmaya rastlanmamıştır. Petro kimya alanında HAZOP tekniğinin kullanıldığı bazı yüksek lisans tez çalışmalarının listesi Çizelge 2.2'de verilmiştir.

Çizelge 2.2. Petro Kimya Alanındaki Örnek HAZOP Çalışmaları

| Yazar | Yıl | Kullanım Alanı |
|---|---|---|
| Khalilov | 2015 | Kimya sektöründe büyük endüstriyel kazaların önlenmesi için kullanılan risk analiz yöntemleri üzerine bir inceleme. |
| Öcelan | 2014 | Petrokimya rafinerisi benzen giderme ünitesi üzerinde iş sağlığı ve güvenliği risk analizi çalışması yapmıştır. |
| Tanrıverdi | 2013 | Kimyasal Proses Endüstrisinde riskleri belirlemiştir. |
| Babaarslan | 2013 | TÜRPAŞ Kırıkkale Rafinerisinde, Atmosferik damıtma ünitesinde bulunan Atmosferik Damıtma Kolonuna ve girişi-çıkış hatları üzerinde risk analizi yapmıştır. |

Scopus veritabanı üzerinde FMEA, HAZOP ve "reliability" kelimelerinin ikili ve üçlü kombinasyonları kullanılarak tarama yapılmış ancak sadece HTEA tekniğinin kullanıldığı güvenilirlik çalışmaları bulunabilmiştir ve ulaşılan makaleler incelenmiştir.

Yang, Zhu, Ren ve Zhang (2015) torna tezgahlarında tahsisin (dağıtım) oldukça önemli olmasına rağmen torna tezgahlarında geleneksel dağıtım yöntemlerinin orta seviye başarısızlıkları yerine sadece yüksek başarısızlık oranlarına odaklanıldığını ifade etmişlerdir. CNC torna tezgahlarının tahsis (dağıtım) problemlerini çözmek için HTEA'nın kübik dönüştürülmüş fonksiyonlarına dayalı kapsamlı bir güvenilirlik tahsisat

yöntemi sunmuşlardır. Yeni tahsis yöntemini uygulamak için bir torna tezgâh sistemi kullanmışlardır. Tahsis sonuçları yeni yöntemin eski yöntemden daha esnek olduğunu göstermiştir.

Hashim, Yoshikawa, Matsuoka, Yang (2014) Basınçlı su reaktörünün tasarımında kullanılan pasif güvenlik sistemleri, donanım arızaları ve insan hatalarının daha az ortaya çıktığı geleneksel basınçlı su reaktörünün aktif güvenlik sistemlerinden daha güvenilir olması gerektiğinden yola çıkarak gelişmiş basınçlı su reaktörlerinde kullanılan AP100 tesisinin pasif güvenlik sisteminin nicel dinamik güvenilirlik değerlendirmesini yapmışlardır. Aktif ve pasif sistemlerin güvenilirliğe ilişkin durumları karşılaştırılarak güvenilirlik değerlendirmesinde HTEA ve GO-FLOW metodolojilerini kullanmışlardır.

Q. Lin, Wang, W. Lin, Liu (2014) tıbbi cihazlar için insanın güvenirliğini HTEA yöntemiyle belirlemiş ve risk durumlarını bulanık mantık kullanarak değerlendirmişlerdir. Yapılan değerlendirme ile risk durumlarının ağırlıklarını belirlemiş ve öncelikli olarak önlem alınması gereken riskler tespit etmişlerdir.

Deveci, Esen, Hatipoğlu, Fığlalı (2014) otomobillerde kullanılan kablolardaki en ufak bozukluğun bile ciddi sorunlara yol açmasından dolayı elektrik kablolarının kesim aşamasındaki hatalarını tespit edip ve önceden gidererek sıfır hatayı amaçlamışlardır. Elektrik kablo kesme sürecinde güvenilirlik merkezli HTEA tekniğini uygulamışlardır.

Sadeghi, Karbasiyan, Navabakhsh (2014) hastalara verilen gaz bileşenlerinin hayati tehlike oluşturmasından dolayı oksijen, vakum, hava ve nitrooksit gazlarını bağlayan prizleri incelemiş vana ve yay parçalarının kritik olduğu sonucuna varmışlardır. Uygulama çalışmasında tıbbi gaz çıkışına ilişkin vana ve yay üzerinde HAA ve HTEA tekniklerini kullanarak güvenilirlik iyileştirme döngüsü yürütmüşlerdir.

Li ve Zhou (2014) kentsel gaz iletim ve dağıtım sisteminin güvenlik yönetimini geliştirmek amacıyla gaz boru hattının güvenilirlik analiz sistemini kurmuşlardır. Çok uzmanlı karar vermenin nesnellik ve belirsizliğinden kaçınmak için risk değerlerine korelasyon operatörlerini ekleyerek HTEA tekniğine kullanmışlardır.

Su, Lin, Teng ve Yang (2014) ikinci nesil elektronik kâğıt ekranların yüksek stres test ortamında başarısız olduğundan seri üretime hazır değildir. Deneme yanılma yöntemleri parametre değerlerinin belirlenip hataların giderilmesi yeni ürün geliştirmek için fazla zaman alacağından ince film transistörlü likit kristal ekran ürünlerinin güvenilirliğini artırmak için HTEA ve Taguchi yöntemlerinin birleştirildiği bir yaklaşım önermişlerdir. Uygulama sonuçları başarısızlıklar arasındaki ortalama sürenin 1867 saatten 4852 saate indiğini ve ürün geliştirme süresinin bir yılın yarısından daha fazla kısaldığını göstermiştir.

Joo, Kim ve Moon (2013) otomotiv sektöründe kullanılan parçaların birleştirilmesinde kullanılan flanş parçasının faydalı ve gerekli olmasından dolayı güvenirliliği arttırmak amacıyla dikdörtgen flanş parçalarının üretiminde süreç parametreleri ve kusurlar arasındaki ilişkiyi HTEA ile analiz etmişlerdir. İşlem durumunu optimize etmiş ve dikdörtgen flanş parçasının güvenilirliği artmışlardır.

Ling, Song ve Sun (2011) dizel motor bileşenlerinin güvenilirliğinin tahmini üzerinde çalışmışlardır. Faydalı bilgiler toplama süresini azaltmak ve tahminin verimliliğini artırmak için, tasarım HTEA ile entegre edilmiş bir yöntem önermişlerdir. Önerilen yöntemde yeni bir bileşenin güvenilirliği, yeni bileşen ile mevcut ve benzer bir bileşenin başarısızlık modları karşılaştırılarak hesaplanmıştır. Önerilen yöntemi göstermek için dizel motorun silindir başı contasının güvenilirlik tahminini örnek olarak kullanmışlardır.

Sharma, Kumari ve Kumar (2011) uçak motorunun dönen bileşeninin yükünü paylaşan rotor destek sisteminin uçak motor sisteminde hayati rol oynamasından dolayı HTEA analizi yapmayı gerekli görmüşlerdir. Modern uçak motorunun rotor destek sisteminin güvenilirliğini artırmak amacıyla MIL-STD-1629A prosedürünü kullanarak HTEA analizi gerçekleştirmişlerdir.

Sawhney ve diğerleri (2010) yalın sistem uygulayıcılarına güvenilirliği anlatmak amacıyla yalın sistemlerini sürdürmek için gerekli dört kritik kaynağa dayalı (personel, ekipman, malzeme ve program takvimi) modifiye edilmiş HTEA yaklaşımını geliştirmişlerdir.

Rebello ve Goyal (2010) çalışmalarında genişletilmiş HTEA yaklaşımına dayalı bir yazılımın güvenilirliğini ve güvenliğini değerlendirmek için nicel bir metodoloji sunmuşlardır. Gerçekleştirilen analiz, yazılım geliştirmenin başlangıç aşamasında

başlamakta ve önemli bilgilerin sağlanmasıyla yazılım geliştirmenin sonraki aşamalarında gelişmektedir. Kolay anlaşılmasından dolayı şiddet seviyelerinin fonksiyonel hata düzeyinde ele alınması önermişlerdir.

Jia, Cui ve Gao (2009) kritik sistem güvenilirliği modellemesi ve bileşen başarısızlık modları açısından kritik sistem güvenirliği analizi yapmışlardır. Sistem tehlikeli hale gelmeden önce tamir sayısı ve süresini elde etmek için İyon Kanal modelleme teorisini kullanarak güvenilirlik ve güvenlik konuları analiz etmişlerdir. Çalışmada elde edilen sonuçları göstermek için sayısal bir örnek sunmuşlardır.

Korayem ve Iravani (2008) robot güvenilirliği ve kalitesini artırmak için tasarım aşmasında HTEA ve kalite fonksiyon göçerimi gibi standart yaklaşımların uygulanmasının gerekli olduğundan yola çıkarak iki mekanik robot analiz ederek her bir robot için kritik hata türleri belirlenmiş ve müşteri istekleri doğrultusunda istenilen kalitede ürüne ulaşmışlardır.

Gollomp (2008) HTEA temelli kalite ve güvenilirlik kolaylaştırıcısı çalışması yapmıştır.

Burgazzi (2006) önemli kaza tetikleyicilerini tespit etmek amacıyla termal-hidrolik pasif sistemin güvenlik ve güvenilirlik analizi için hata türü ve etkileri analizi uygulaması yapmıştır. Hataların ortak sebeplerine karşı alınan önlemlerin sistem hata olasılıklarını kayda değer oranda azalttığını öğrenmiştir.

Zafiropoulos ve Dialynas (2005) bulanık mantık kullanarak elektronik cihazların güvenilirlik tahmini ve hata modu etkileri ve kritikliği analizi için bir metodoloji geliştirmeyi amaçlamışlardır. Güvenilirlik tahminini MIL-HDBK-217FN2 teknik dokümanına dayandırmışlar ve bileşenlerin düşük hata oranlarını korumak için sistem tasarımına yönelik bir azaltma planı geliştirmişlerdir. Bu başarısızlık oranlarını HTEA analizinde kullanmışlardır. Anahtarlamalı güç kaynağı gibi bir tipik elektronik güç cihazını analiz ederek uygun güvenilirlik endekslerini tahmin etmiş ve bulanık başarısızlık modunun risk indekslerini hesaplamışlardır.

Rhee ve Ishii (2003) riski oluşturan şiddet bileşeninin algılama ve ölçme güçlüğü ile evrensel bir skalanın olmayışından yola çıkarak bu eksiklikleri gideren ve maliyet açısından riski ölçen maliyet bazlı HTEA metodolojisini oluşturmuşlardır. Maliyet bazlı

HTEA bir sistemin genel yaşam döngüsü maliyetini düşürebilen tasarım alternatiflerini karşılaştırmada ve seçmede kullanışlıdır. Bazı senaryolardaki belirsizlikleri hesaba katmak için maliyet bazlı HTEA'yı bir Monte Carlo simülasyonu ile gerçekleştirmişlerdir.

Prasad (1991) bilgisayar veya otomobildeki bir mikroçipin paketlemesi ile ilgili benzeri görülmemiş bir başarısızlığın doğurabileceği korkunç sonuçlardan yola çıkarak entegre devre montajına temel HTEA tekniğinin uygulanışını ve karmaşık paket montajı ile çok modüllü yonga üretimi için tekniğin kullanışlı olduğunu göstermiştir.

Yuan ve Chou (1986) önerdikleri HTEA yöntemi ile network güvenilirlik indislerinin hesaplamak için ikili cebir yöntemi önermişlerdir. Paralel olarak sistem arızası frekansını hesaplamak için bir yöntem geliştirmişlerdir.

Yuan (1985) büyük ve karmaşık bir sistemlerde gelişmiş bilgisayarlara güvenmek ihtiyacından yola çıkarak bir sistemin matematiksel güvenilirlik modelinin inşasına yardımcı olacak bir HTEA uygulamak için çok genel bir algoritma sunmuştur.

Jenny (1969) optimum fazlalık miktarının hesaplanmasında kısmi hata türlerinin (Kısmi hata türleri parçaya zararlı olan fakat sisteme zararlı olmayan türlerdir) etkisini gösteren bir analiz sunmuştur. Kayıp katsayıları ve durum olasılıkları ile bir formül oluşturmuş ve durum olasılıklarının düzenlenmesi için bir model geliştirmiştir. Çalışmayı örnek bir sistem üzerinde uygulamıştır.

Literatür taramasında HTEA tekniğini kullanan çalışmalar incelenmiştir. HTEA tekniğinin, sıklıkla otomotiv, raylı sistemler ve diğer üretim alanlarında kullanıldığı görülmüştür. Bilişim hizmetlerinin sürekliliğine yönelik HTEA tekniğini kullanan herhangi bir çalışmaya rastlanmamıştır. Güvenilirlik alanında HTEA ile ilgili ulaşılan çalışmaların listesi Çizelge 2.3'te verilmiştir.

Çizelge 2.3. Güvenilirlik Alanındaki HTEA Analiz Tekniği Çalışmaları

| | | |
|---|---|---|
| Yang, Zhu, Ren ve Zhang | 2015 | CNC torna tezgahlarının tahsis (dağıtım) problemlerini çözmek için HTEA'nın kübik dönüştürülmüş fonksiyonlarına dayalı kapsamlı bir güvenilirlik tahsisat yöntemi sunmuşlardır. |
| Hashim, Yoshikawa, Matsuoka, Yang | 2014 | Gelişmiş basınçlı su reaktörlerinde kullanılan AP100 tesisinin pasif güvenlik sisteminin nicel dinamik güvenilirlik değerlendirmesini yapmışlardır. |
| Q. Lin, Wang, W. Lin, Liu | 2014 | Tıbbi cihazlar için insanın güvenirliğini HTEA yöntemiyle belirlemiş ve risk durumlarını bulanık mantık kullanarak değerlendirmişlerdir. |
| Deveci, Esen, Hatipoglu, Fi̇lali | 2014 | Otomobillerde kullanılan elektrik kablo kesme sürecinde güvenilirlik merkezli HTEA tekniğini uygulamışlardır. |
| Sadeghi, Karbasiyan, Navabakhsh | 2014 | Uygulama çalışmasında tıbbi gaz çıkışına ilişkin vana ve yay üzerinde HAA ve HTEA tekniklerini kullanarak güvenilirlik iyileştirme döngüsü yürütmüşlerdir |
| Li ve Zhou | 2014 | HTEA tekniğine kullanarak kentsel gaz iletim boru hattının güvenilirlik analiz sistemini kurmuşlardır. |
| Lin, Teng ve Yang | 2014 | İnce film transistörlü likit kristal ekran ürünlerinin güvenilirliğini artırmak için HTEA ve Taguchi yöntemlerinin birleştirildiği bir yaklaşım önermişlerdir. |
| Joo, Kim ve Moon | 2013 | Otomotiv sektöründe kullanılan dikdörtgen flanş parçalarının üretiminde süreç parametreleri ve kusurlar arasındaki ilişkiyi HTEA ile analiz etmişlerdir. |
| Ling, Song ve Sun | 2011 | Dizel motor bileşenlerinin güvenilirliğinin tahmini üzerinde çalışmışlardır. Tasarım HTEA ile entegre edilmiş bir yöntem önermişlerdir |
| Sharma, Kumari ve Kumar | 2011 | Modern uçak motorunun rotor destek sisteminin güvenilirliğini artırmak amacıyla HTEA analizi gerçekleştirmişlerdir. |
| Sawhney ve diğerleri | 2010 | Yalın sistem uygulayıcılarına güvenilirliği anlatmak amacıyla modifiye edilmiş HTEA yaklaşımını geliştirmişlerdir. |

Çizelge 2.3. (devam ) Güvenilirlik Alanında HTEA Analiz Tekniği Çalışmaları

| | | |
|---|---|---|
| Rebello ve Goyal | 2010 | Genişletilmiş HTEA yaklaşımına dayalı bir yazılımın güvenilirliğini ve güvenliğini değerlendirmek için nicel bir metodoloji sunmuşlardır. |
| Jia, Cui ve Gao | 2009 | Kritik sistem güvenilirliği modellemesi ve bileşen başarısızlık modları açısından kritik sistem güvenirliği analizi yapmışlardır. |
| Korayem ve Iravani | 2008 | Robot güvenilirliği ve kalitesini artırmak için tasarım aşmasında HTEA ve kalite fonksiyon göçerimi uygulaması. |
| Gollomp | 2008 | HTEA temelli kalite ve güvenilirlik kolaylaştırıcısı çalışması yapmıştır. |
| Burgazzi | 2006 | Önemli kaza tetikleyicilerini tespit etmek amacıyla termal-hidrolik pasif sistemin güvenlik ve güvenilirlik analizi için hata türü ve etkileri analizi uygulaması yapmıştır. |
| Zafiropoulos ve Dialynas | 2005 | Bulanık mantık kullanarak elektronik cihazların güvenilirlik tahmini ve hata modu etkileri ve kritikliği analizi için bir metodoloji geliştirmişlerdir. |
| Rhee ve Ishii | 2003 | Maliyet açısından riski ölçen maliyet bazlı HTEA metodolojisini oluşturmuşlardır. |
| Prasad | 1991 | Entegre devre montajına temel HTEA tekniğinin uygulanışını ve karmaşık paket montajı ile çok modüllü yonga üretimi için tekniğin kullanışlı olduğunu göstermiştir. |
| Yuan ve Chou | 1986) | Önerdikleri HTEA yöntemi ile network güvenilirlik indislerinin hesaplamak için ikili cebir yöntemi önermişlerdir. |
| Yuan | 1985 | Bir sistemin matematiksel güvenilirlik modelinin inşasına yardımcı olacak bir HTEA uygulamak için çok genel bir algoritma sunmuştur. |
| Jenny | 1969 | Optimum fazlalık miktarının hesaplanmasında kısmi hata türlerinin etkisini gösteren bir analiz sunmuştur. |

# 3. İŞ SÜREKLİLİĞİ

İş sürekliliği, kurum ve kuruluşların kritik fonksiyon ve süreçlerini etkileyecek olaylara karşı hazırlıklı olması ve yıkıcı olaylar meydana geldiğinde, kurumun önceden planlandığı ve test edildiği şekilde yanıt verebilmesidir (TSE, 2013).

Kritik iş süreçleri, devamlılığın sağlanamadığı durumlarda tahammül edilebilir azami kesinti süreleri içerisinde yeniden çalışır hale getirilmelidir. Kurumların ilk hedefi iş süreçlerini kesintisiz bir şekilde gerçekleştirmek olsa da planlanmamış tehlikeler (iş sürekliliği ihlal olayı) ile karşı karşıya kalmaktadırlar. İşleri kesintiye uğratan olay yangın gibi bir felaket de olabilir, personel taşıma servisinin bozulup yolda kalması gibi ufak bir olay da olabilir. İşlerin sürekliliği ve kurumun maddi manevi kayba uğramaması için kurumlar iş sürekliliği yönetim sistemini kurmalıdırlar. Kurum içerisindeki iş sürekliliği aktivitelerinin yönetildiği sisteme, iş sürekliliği yönetim sistemi denilmektedir (Dinçkan, 2008: 5).

Özellikle enerji ve elektrik alanında iş sürekliliği ülkeler tarafından ön plana alınmaktadır. Robert McDonald, enerji (elektrik) hizmetleri için güvenlik uygunluğu, güvenilirlik ve iş sürekliliği ile ilgili yeni konuları açıklamaktadır. NERC tarafından Kritik Altyapı Koruması (CIP) 002-009 standardı oluşturulmuştur. Bu standartlar, Kuzey Amerika'da yığın elektrik sistemlerini korumak için bütüncül bir güvenlik yaklaşımı uygulanmasını belirler. Bu raporda, güvenlik ve iş sürekliliği planlamasına yönelik entegre bir yaklaşım anlatılmıştır. Yazının bir bölümünde felaket yönetimi planlaması açıklanmıştır. Felaket planlama sürecinin bileşenleri ele alınmış ve risk dengelenmesi üzerinde durulmuştur (McDonald, 2008).

İş sürekliliğini yönetme amacına yönelik etkileşimli süreçler bütününe iş sürekliliği yönetim sistemi (İSYS) denir. Bazı kurumlar adı İSYS olmasa da kendilerine ait farklı yönetim sistemleri ile iş sürekliliğini sağlamışlardır. Birçok kurum direkt iş sürekliliğini amaçlamadan da iş sürekliliğinin birçok gereksinimini yerine getirebilmektedir. İş sürekliliğini amaçlayan yönetim sistemleri, bir standarda dayanmak zorunda olmasa da bazı komiteler tarafından iş sürekliliği yönetim sistemi standartları geliştirilmiştir. Ancak kurumlar iş sürekliliklerini bu standartlardan birine göre kurduklarında hem kendilerini

daha fazla güvende hissedebilir hem de kabul görürler. Dünya çapında kabul gören standartların ilklerinden biri İngiltere'de ortaya çıkan *BS 25999:2006 İş Sürekliliği Yönetimi* adındaki standarttır. ISO tarafından 2012 yılında *ISO 22301 iş sürekliliği yönetim sistemi* standardı piyasaya sürülmüştür. Dünya çapında geçerli olacak olan bu standart BS 25999:2006 standardını temel almaktadır.

## 3.1. İş Sürekliliği Yönetim Sistemi Standartları

ISO tarafından iş sürekliliğinin belirli bir standarda göre yapılabilmesi amacıyla bazı standartlar yayınlanmıştır. Bu standart ailesi içinde ISO 22300, ISO 22301, ISO 22313 numaralı standartlar bulunmaktadır. ISO 22300 numaralı standart, iş sürekliliğine yönelik terimler standardıdır. ISO 22301 numaralı standart, iş sürekliliği yönetim sistemi için gereksinimleri belirtir. ISO 22313 numaralı standart ise iş sürekliliği gereksinimlerini yerine getirebilmek için rehberdir.

### 3.1.1. ISO 22300 iş sürekliliği terimleri

ISO 22300 numaralı standart, iş sürekliliği yönetim sisteminde kullanılan terminolojinin kaynağıdır. İş sürekliliği yönetim sisteminde kullanılan bazı terimler aşağıdaki gibidir (Dinçkan, 2008, TSE, 2013).

<u>En uzun kabul edilebilir kesinti süresi-MTPoD (Maximum Tolerable Period of Disruption)</u>

Bir faaliyet, süreç veya bunların ilişkili olduğu bir bileşen için kurumun kabul edebileceği azami kesinti süresidir. Bir faaliyetin gerçekleştirilememesi sonucu oluşan yıkıcı etkilerin kabul edilemez seviyeye gelene kadarki zamandır. Bu süre kurumu zarara uğratacak eşik değerdeki süredir. Bu süre dakika cinsinden kısa olabileceği gibi gün cinsinden uzun da olabilir

<u>Kurtarma zamanı hedefi-recovery time objective (RTO)</u>

Bir ihlal olayının ardından; hizmetin yeniden verilmeye başlanma ya da faaliyetin yeniden başlatılma ya da kaynakların kurtarılma süresidir. Bu süre dolmadan hizmetler sunulabilir, bileşenler hazır ve faaliyetler gerçekleştirilebilir durumda olmalıdır.

Kurtarma noktası hedefi-recovery point objective (RPO)

Kurumun kabul edebileceği maksimum veri kaybını süre olarak ifade eder. Faaliyetin kaldığı yerden devam etmesi için bir faaliyette kullanılan bilginin tekrar dönülmesi gereken noktadır. Bu sürenin 24 saat olarak belirlenmişse gerekli durumda 24 saatlik veya daha yeni veriler kurtarılabilir olmalıdır.

İş sürekliliği planı

Kesintinin ardından karşılık vermek, kurtarma işlemini yapmak, yeniden başlangıç yapmak ve önceden tanımlanan iş seviyesini geri kazanma konusunda kuruluşa yol gösteren yazılı prosedürlerdir.

İş etkisi analizi

İşin kesintiye uğraması üzerinde etkisi olabilen faaliyetlerin ve etkilerinin analiz edilmesi sürecidir.

Tatbikat

Kuruluş için performansın değerlendirilmesi, uygulanması ve iyileştirilmesi için eğitim yapılması süreci. Test, planlanan alıştırmanın hedefi veya amaçları kapsamında "geçti" veya "kaldı" değerlendirmesini bünyesinde barındıran benzersiz ve özel bir alıştırmadır.

### 3.1.2. TS ISO 22301 Standardı

2006 yılında çalışmaları başlatılan ISO 22301 numaralı standarda en çok katkıyı Avustralya, Fransa, Almanya, Japonya, Kore Cumhuriyeti, Singapur, İsveç, Tayland, İngiltere ve Amerika Birleşik Devletleri sunmuştur. *ISO 22301 iş sürekliliği yönetim sistemi* standardı 2012 yılında ISO (223 numaralı komite) tarafından yayımlanmıştır (ISO, 2012). Bu standart iş sürekliliği için şartları belirler. Aynı standart 2013 Eylül ayında TSE tarafından Türkçeye çevrilerek TS ISO 22301:2013 numarasıyla Türk standardı olarak kabul edilmiştir. Standart kapsamında yer alan bazı kavram ve İSYS unsurları aşağıdaki gibidir (TSE, 2013).

İSYS bileşenleri

ISO 22301 numaralı standarda göre iş sürekliliği yönetim sisteminin bileşenleri beş kısımdır. Bunlar; politika, sorumlulukları tanımlanmış personel, yönetim süreçleri, dokümantasyon ve kuruluşla ilgili iş sürekliliği yönetim süreci şeklindedir.

İlgili tarafların belirlenmesi

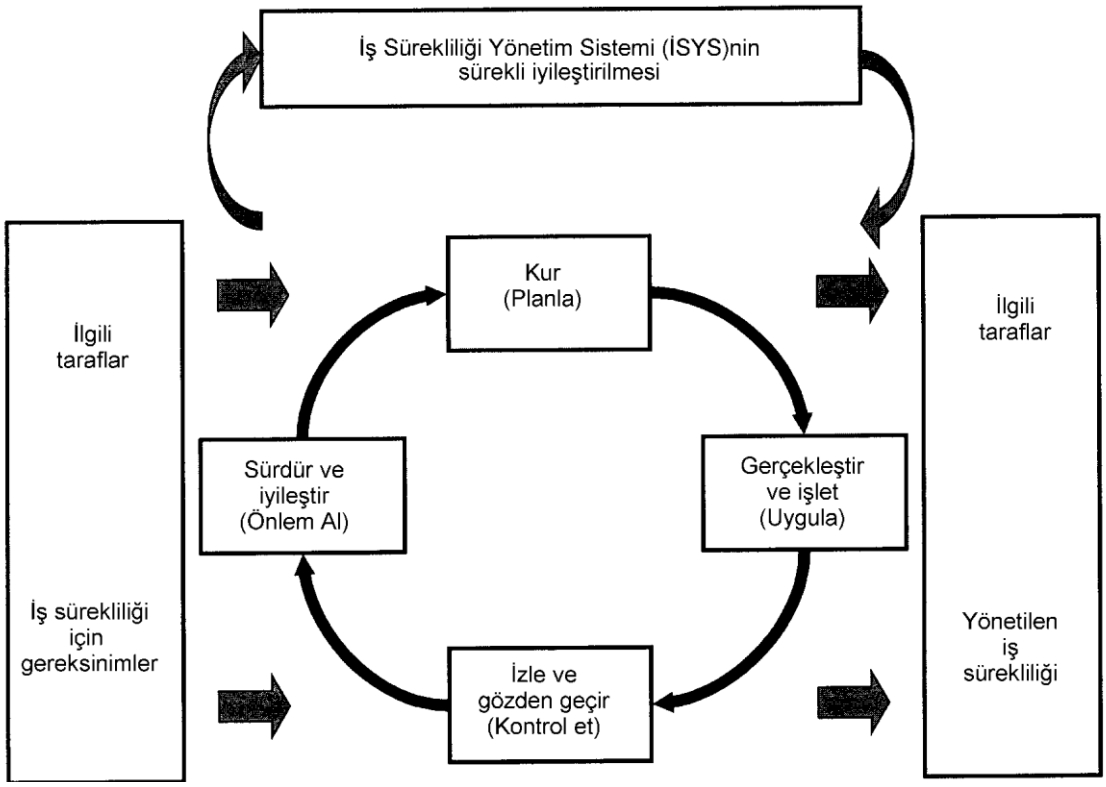
İSYS kurulum aşamasında ilgili taraflar ve ilgili tarafların gereksinimleri belirlemelidir.

Kaynaklar

İSYS'nin kurulması, gerçekleştirilmesi, sürdürülmesi ve sürekli iyileştirilmesi için gerekli olan kaynakları kurum sağlamalıdır.

Planla - uygula - kontrol et - önlem al (PUKÖ) modeli

ISO tarafından çıkarılan diğer standartlar gibi bu standart da bir kuruluşun İSYS'nin planlanmasına, kurulmasına, gerçekleştirilmesine, işletilmesine, izlenmesine, gözden geçirilmesine, sürdürülmesine ve etkinliğinin sürekli olarak geliştirilmesine Planla-Uygula-Kontrol et-Önlem al (PUKÖ) modelini uygular. Böylece, yönetim sistemi standartları arasında belli bir seviyede tutarlılık temin edilir. Şekil 3.1.'de, İSYS'nin, girdileri nasıl aldığını ve gerekli işlem ve süreçlerden geçirerek sonuçlarının nasıl ortaya çıktığı gösterilmiştir. Yönetilen iş süreçleri bu yapının çıktılardır.




Şekil 3.1. İSYS süreçlerine uygulanan PUKÖ modeli (TSE, 2013)

Çizelge 3.1.'de PUKÖ modelindeki terimlerin açıklaması gösterilmiştir.

Çizelge 3.1. Yönetim Sistemi için PUKÖ Modeli

| | |
|---|---|
| **Planla** (Tesis et) | Kuruluşun genel politikaları ve amaçlarına uygun sonuçlara ulaşılması amacıyla iş sürekliliğinin iyileştirilmesi ile ilgili iş sürekliliği politikasının, amaçlarının, hedeflerinin, kontrollerinin, süreçlerinin ve prosedürlerinin belirlenmesi. |
| **Uygula** (Gerçekleştir) | İş sürekliliği politikasının, kontrollerinin, süreçlerinin ve prosedürlerinin gerçekleştirilmesi ve yürütülmesi. |
| **Kontrol et** (Gözden geçir) | İş sürekliliği politikası ve amaçlarına karşılık performansın izlenmesi ve gözden geçirilmesi; sonuçların gözden geçirilmek üzere yönetime rapor edilmesi; düzeltme ve iyileştirme için yapılacak işlemlerin belirlenmesi ve yetki verilmesi. |
| **Önlem al** (Sürdür ve iyileştir) | Yönetimin yapacağı gözden geçirmenin sonuçlarına dayanarak ve İSYS'nin kapsamının, iş sürekliliği politikasının ve amaçlarının yeniden değerlendirilmesi suretiyle düzeltici faaliyetler yapılarak İSYS'nin sürdürülmesi ve iyileştirilmesi. |

Yasal ve düzenleme amaçlı gereksinimler

Kuruluş, yürürlükteki kanunlar ve düzenleyici mevzuat gereksinimlerini tespit edip bu gereksinimlere ulaşmak ve değerlendirmek için kuruluş bir prosedür oluşturmalı ve bu prosedüre göre yasal zorunlulukları takip etmelidir. Kurum, tabi olduğu yasal düzenlemeleri belirledikten sonra İSYS'nin kurulmasında, gerçekleştirilmesinde ve sürdürülmesinde kanun ve düzenleyici mevzuata uygunluğu sağlamalıdır ve bu uygunluğu sürdürmelidir. İlgili prosedür yazılı olmalı ve güncelliğini kuruluş sağlamalıdır. Yeni yasal zorunluluklar ve gereksinimler veya bunların değişiklikleri, ilgili taraflara duyurulmalıdır. Duyurudan daha etkin ve doğru bir yöntem ise yasal zorunluluk ya da gereksinimleri ilgili prosedürlere dönüştürüp kurumun faaliyetleri içine entegre etmektir.

İSYS'nin kapsamının belirlenmesi

Kuruluş,

- ✓ İSYS'nde yer alacak kuruluş bölümlerini belirlemeli,
- ✓ Kuruluşun misyonu, hedefleri, iç ve dış yükümlülüklerini (ilgili taraflarla ilişkili olanlar da dahil) ve yasal ve düzenleme amaçlı sorumluluklarını dikkate alarak İSYS gereksinimlerini belirlemeli,
- ✓ İSYS'nin kapsamı içerisinde yer alan ürünleri, hizmetleri ve ilgili tüm faaliyetleri tespit etmeli,
- ✓ Müşteriler, yatırımcılar, hissedarlar, tedarik zinciri ve/veya toplumun girdileri ve ihtiyaçları, beklentileri ve menfaatleri (uygun olduğu şekilde) gibi ilgili tarafların ihtiyaçlarını ve menfaatlerini dikkate almalı,
- ✓ Kuruluşun büyüklüğüne, doğasına ve karmaşıklığına uygun biçimde İSYS'nin kapsamını tanımlamalı,
- ✓ İş etkisi analizi veya risk analizi ve yürürlükteki yasal ve düzenleyici gereksinimler tarafından belirlendiği şekilde, İSYS'nin gereksinimlerini karşılayan iş ve işlemlerin sürekliliğini sağlamak için kuruluşun yeteneğini ve sorumluluğunu etkilemeyecek kapsam dışı tutulanlar gibi hususları, kapsam tanımlanırken kuruluş yazılı hale getirmeli ve açıklamalıdır.

Yönetimin desteği

Üst yönetim, aşağıdakileri yerine getirerek, İSYS konusundaki liderliğini ve desteğini göstermelidir:

- ✓ Politikaların ve amaçların, iş sürekliliği yönetim sistemi için oluşturulması ve bunların kuruluşun stratejik yönüyle uyumlu olmasının temin edilmesi,
- ✓ Kuruluşun iş süreçleri ile iş sürekliliği yönetim sistem gereksinimlerinin bütünleştirilmesinin sağlanması,
- ✓ İş sürekliliği yönetim sistemi için gerekli olan kaynakların hazır bulundurulmasının sağlanması,
- ✓ Etkili iş sürekliliği yönetim sisteminin öneminin duyurulması ve İSYS gereksinimlerine uyulması,
- ✓ İSYS'nin, düşünülen sonucu/sonuçları elde etmesinin sağlanması,
- ✓ İSYS'nin etkinliğini sürdürmek için kişilerin yönlendirilmesi ve desteklenmesi,
- ✓ Sürekli iyileştirmenin teşvik edilmesi,
- ✓ Diğer yönetim görevlerini yerine getiren personelin, kendi sorumluluk alanında liderliklerini ve işe verdikleri önemi göstermeleri için desteklenmesi.

Üst yönetim, aşağıdakileri gerçekleştirerek İSYS desteğini ortaya koyar.

- ✓ İş sürekliliği politikası oluşturarak,
- ✓ İSYS amaçlarının ve planlarının hazırlanmasını sağlayarak,
- ✓ İş sürekliliği yönetimi için görev, sorumluluk ve becerileri belirleyerek,
- ✓ İSYS'nin gerçekleştirilmesi ve sürdürülmesi için gerekli beceri ve uygun yetkiye sahip bir veya birkaç kişiyi İSYS'den sorumlu olacak şekilde belirleyip İSYS'nin kurulmasına, gerçekleştirilmesine, işletilmesine, izlenmesine, gözden geçirilmesine, sürdürülmesine ve iyileştirilmesine destek verdiğinin delilini ortaya koymalıdır.

Üst yönetim,

- ✓ Risklerin kabul edilmesi ve kabul edilebilir risk seviyeleri için kriteri tanımlayarak,
- ✓ Alıştırma ve test işlemlerinin yapılmasında etkin biçimde yer alarak,
- ✓ İSYS'nin iç denetimlerinin yapılmasını sağlayarak,
- ✓ İSYS'de yönetimin gözden geçirmesini yaparak,
- ✓ Sürekli iyileştirmeye destek verdiğini göstererek ilgili görevler için sorumlulukların ve yetkilerin belirlenmesini ve kuruluş içerisinde duyurulmasını sağlamalıdır.

Politika

Kuruluş amacına uygun, iş sürekliliği amaçlarının belirlenmesi için bir altyapı sunan, yerine getirilecek gereksinimleri karşılamaya destek verildiğini gösteren, İSYS'nin sürekli iyileştirilmesine destek verildiğini gösteren bir iş sürekliliği politikası üst yönetim tarafından oluşturulmalıdır. İSYS politikası; yazılı olmalı, duyurulmalı, ilgili tarafların kullanımına da sunulmalı, uygunluğu sürdürmek için gerektiğinde gözden geçirilmelidir.

Görev - sorumluluk ve yetkiler

Yönetim sisteminin iş sürekliliği gereksinimlerine uymasını sağlamak üst yönetimin sorumluluğundadır. Ayrıca ilgili görevler için sorumlulukların ve yetkilerin belirlenmesi ve kuruluş içerisinde duyurulması üst yönetimin sorumluluğundadır. Üst yönetim, İSYS'nin performansının üst yönetime raporlanması için sorumlulukları ve yetkileri belirlemelidir.

İş sürekliliği amaçları ve planlar

İş sürekliliği amaçlarının belirlenmesi ve kuruluş içerisindeki fonksiyonlar için ilgili kademelere duyurulması üst yönetim tarafından sağlamalıdır. Kurum, iş sürekliliği amaçları konusundaki prosedür ve ilgili belgeleri muhafaza etmelidir. Kimin sorumlu olacağı, neyin yapılacağı, hangi kaynakların gerekli olacağı, amaçlara ulaşma işleminin ne zaman tamamlanacağı, sonuçların nasıl değerlendirileceği kurum tarafından iş sürekliliği amaçlarına ulaşmak için belirlenmelidir.

Yetkinlik

Kurumda görevlendirilecek personelin verilen görevleri yerine getirebilmesi için sahip olması istenen gerekli yetkinlik belirlemelidir. Kurum işe aldığı personelin, eğitim, öğretim ve deneyim temelinde gerekli yetkinliğe sahip olduğundan emin olmalıdır. Gerektiğinde personelin yeterli düzeyde yetkinliğe sahip olması için eğitim, danışmanlık ve rotasyon yapılmalıdır. Verilen eğitimlerin, alınan danışmanlığın ve rotasyonların etkinliği de değerlendirilmelidir. İstenen yetkinliğe sahip olunduğunu gösteren delili uygun biçimde yazılmış bir bilgi şeklinde elinde bulundurmalıdır.

Farkındalık

Bu amaçla personele farkındalık eğitimi verilmelidir. Farkındalık eğitimi sonucunda personel; iş sürekliliği politikasının, İSYS'nin etkinliğine yaptığı katkının, iş sürekliliği uygunsuzluklarının olumsuz sonuçlarının, kesintiye neden olan ihlal olayları sırasında yapılması gereken görevlerinin farkında olmalıdır.

İş etki analizi (İEA)

Kurum, iş sürekliliği için resmi ve yazılı bir değerlendirme süreci oluşturmalı, gerçekleştirmeli ve sürdürmelidir. Bu süreç, hizmetleri ve hizmet bileşeni durumundaki faaliyetleri kesintiye uğratan olayların etkilerinin belirlenmesini içerir. Bu amaçla iş etki analizi formları kullanılır.

İş etki analizi şunlardan oluşur; faaliyetlerin tespit edilmesi, bu faaliyetlerin yerine getirilmemesinin zaman içerisindeki etkilerinin belirlenmesi, kabul edilebilir en düşük seviyedeki faaliyetlerin yeniden başlatılması için önceliklendirilmiş zaman cetvellerinin düzenlenmesi, söz konusu faaliyetlerin yeniden başlatılmasının etkilerinin kabul edilemez hale geldiği sürenin dikkate alınması, söz konusu faaliyetlerdeki bağımlılıkların tespit edilmesi ve kaynakların desteklenmesi.

Risk belirlemesi

İşleri kesintiye uğratan ihlal olaylarının riski hesaplanmalıdır. Bu amçla kurum yazılı bir risk metodolojisi oluşturmalı gerçekleştirmeli ve sürdürmelidir. Bu süreç, ISO 31000'e göre yapılabilir. Kurum, kritik faaliyetlerde, süreçlerde, sistemlerde, bilgide, insanlarda, varlıklarda, kurum dışındaki paydaşlarda ve sayılanları destekleyen diğer kaynaklarda kesinti yaşanması risklerini belirlemelidir. Riskler sistematik olarak analiz edilmelidir. Kesinti ile ilgili hangi risklerin işlenmesi gerektiğinin değerlendirilmesi yapılmalıdır. İş sürekliliği amacıyla ve kuruluşun risk iştahıyla orantılı risk işleme usullerini tespit etmelidir.

Riske karşı önlem

Kurum, belirlenmiş riskler için kesinti olasılığını azaltan, kesinti süresini kısaltan, kesintinin etkisini sınırlayan ön tedbirlerin alınmasını ele almalıdır. Risk iştahına göre uygun risk işlemeleri belirlenmeli ve gerçekleştirilmelidir.

İş sürekliliği planı

İş sürekliliği ihlal olaylarına karşılık vermede kullanılacak prosedürler kurum tarafından

oluşturulmalıdır. Kurum, önceden belirlenen zaman dilimlerinde faaliyetlerini nasıl sürdüreceğini veya eski haline getireceğini yazılı hale getirmelidir. Söz konusu prosedürler, anılan prosedürleri kullanacak personele yönelik olmalıdır.

ISO 22301 standardı iş sürekliliği planlarının aşağıda yazılı olanları bir arada içinde bulundurmasını ister.

- ✓ Bir ihlal olayı sırasında veya sonrasında yetkili şahıslar veya ekiplerin görev ve sorumluluklarının tanımı,
- ✓ Karşılığın verilmesi işleminin başlatılmasına yönelik prosedür,
- ✓ Aşağıdaki hususlar dikkate alınarak kesintiye neden olan ihlal olayının ilk sonuçlarının yönetilmesi konusundaki ayrıntılar,
  - Bireylerin refahı,
  - Kesintiye karşılık verilmesinde kullanılacak stratejik, taktik ve operasyonel seçenekler,
  - Öncelikli faaliyetlerde daha fazla kayıpların yaşanmasının veya öncelikli faaliyetlerin yerine getirilememesinin önlenmesi,
- ✓ Kuruluşun çalışanlarıyla, kendi bağlantılarıyla, önemli ilgili taraflarla ve acil durumda temas kurulacaklarla nasıl ve hangi koşullar altında iletişim kuracağının ayrıntıları,
- ✓ Kuruluşun, önceden belirlenen zaman dilimlerindeki öncelikli faaliyetlerini nasıl sürdüreceği veya kurtaracağı,
- ✓ Bir ihlal olayının ardından kuruluşun basına vereceği cevabın ayrıntıları aşağıdakileri içermelidir:
  - İletişim stratejisi,
  - Basın ile arada bulunması tercih edilen arayüz,
  - Bir basın ifadesinin ana hatları veya şablonu
  - Uygun sözcüler.
- ✓ İhlal olayı bittiğinde normal duruma geçiş süreci.

Tatbikat ve test

İş sürekliliği prosedürlerinin iş sürekliliği amaçlarıyla tutarlı olmasını sağlamak amacıyla iş sürekliliği prosedürleri denenmeli ve test edilmelidir. Bu kapsamda;

- ✓ Testler, İSYS'nin kapsamı ve hedefleriyle tutarlı olmalı,
- ✓ Net bir biçimde tanımlanmış amaç ve hedeflerle iyi şekilde planlanan uygun senaryolara dayanan tatbikatlar planlanmalı,
- ✓ Tatbikatlarda, tarafları da içeren kendi iş sürekliliği anlaşmalarının tümünün geçen zaman zarfında geçerliğini yönetim üstlenmeli,
- ✓ İşlemlerin kesintiye uğrama riskini en aza indiren testler yapılmalı,
- ✓ İyileştirmeleri gerçekleştirmek için sonuçları, tavsiyeleri ve faaliyetleri içeren tatbikat sonrası içeriği tanımlanmış raporlar hazırlanmalı,
- ✓ Testler, sürekli iyileştirmenin teşvik edilmesi kapsamında gözden geçirilmeli,
- ✓ Planlı aralıklarla ve kuruluş içerisinde veya kuruluşun çalıştığı ortamda önemli değişiklikler olduğunda testler yapılmalıdır.

İç denetim

Organizasyonlar, kurdukları İSYS'nin çalışıp çalışmadığını ve bu standardın gereksinimlerini karşılayıp karşılamadığını kontrol etmek amacıyla planlanan aralıklarla iç denetim yapmalıdırlar. Denetimler için sorumluluklar ve gereksinimler tanımlanmalıdır. Denetim programları yapılmalı ve gerçekleştirilmelidir. Denetim sonucunda tespit edilen uygunsuzlukları düzelmek için etkisine uygun şekilde düzeltici faaliyetler dizisi gerçekleştirilmelidir.

Yönetimin gözden geçirmesi (YGG)

İSYS üst yönetim tarafından planlanan aralıklarda ya da önemli değişikliklerde gözden geçirilmelidir. YGG toplantıları yapılmalı ve İSYS'nin yeterliliği, etkinliği ve uygunluğu konusunda emin olunmalıdır. Yönetimin gözden geçirmesi, önceki gözden geçirme işlemlerinin durumunu, iş sürekliliği yönetim sistemiyle ilgili iç ve dış konulardaki değişiklikleri, iş sürekliliği performansı konusundaki bilgiyi, uygunsuzlukları, düzeltici faaliyetleri, değerlendirme sonuçlarının izlenmesini, denetim sonuçlarını ve sürekli iyileştirme hususlarını göz önüne almalıdır.

### 3.1.3. ISO/IEC 27031 Bilgi ve iletişim teknolojileri için iş sürekliliği yönergeleri

İş sürekliliği için bilgi ve iletişim teknolojilerinin hazır bulunmasıyla ilgili olarak ISO tarafından *ISO 27031 bilgi ve iletişim teknolojileri için iş sürekliliği yönergeleri* standardı 2011 yılında yayınlanmıştır.

ISO / IEC 27031:2011 bilgi ve iletişim teknolojileri altyapı ve sistemleri üzerinde bir etkiye sahip olabilecek (ilgili güvenlik dahil) tüm ihlal olaylarını kapsar. Bu standart bilgi güvenliği ihlal olaylarının yönetimi ile BT'nin hazırda bulunurluğunu ve planlamasını içerir. Resmi ve özel bütün kurumlara uygulanabilir. İş sürekliliği için bilgi ve iletişim teknolojilerinin (BİT) hazırda bulunması amacıyla kavram ve prensipleri tanımlar. BiT'in hazırda bulunurluğu için tüm yönleriyle süreç ve metotları içeren bir çerçeve sağlar (ISO, 2011).

Rehber niteliğindeki bu standart, 9 bölümden oluşmaktadır. Standartta BT'nin iş sürekliliği içindeki rolüne değinilmiştir. BT hizmetlerinin iş sürekliliği için hazır hale getirilmesinden ve bileşenlerinden bahsedilir. BT sürekliliği prensipleri, süreklilik için gereksinimler değinilen hususlar arasındadır. Kritik BT hizmetlerinin belirlenmesi istenmiştir. İç denetim yapılması önemi vurgulanmaktadır (TSE, 2014).

### 3.1.4. BS 25999 Standardı

BS 25999 standardı iş sürekliliği yönetim sistemi standardı olarak İngiliz Standart Enstitüsü tarafından yayınlanmıştır. Standart iki parçadan oluşmaktadır. Standardın ilk parçası olan "BS 25999-1 Business Continuity Management. Code of Practice" standardı Aralık 2006 tarihinde yayınlanmıştır. Standardın rehber niteliğinde olan ikinci kısmı ise "BS 25999-2 Specification for Business Continuity Management" adıyla 2007 yılında yayınlanmıştır. ISO 22301 İş Sürekliliği Yönetim Sistemi standardının yayınlanması ile BS 25999 standardı tedavülden kaldırılmıştır (BSI, 2007).

# 4. RİSK ANALİZİ

Çalışmanın bu bölümü risk yönetimi ve özellikle tehlike belirleme ve risk analizine ayrılmıştır. Risk analizi ile ilgili tanımlar, gerekli ön bilgiler, kabul görmüş teoriler, risk yönetimine ilişkin ISO standartları, risk analizi konusunda yapılan akademik çalışmalar, tehlike analiz tipi ve teknikler bu bölümde ele alınacaktır.

Daha önce iş sürekliğini ele almayan organizasyonlar, işe ait potansiyel etkileri ve riskleri hafife alma eğilimindedirler. Başarılı olacak herhangi bir iş sürekliliği yönetim programı sağlam ve kesin iş risklerinin analizine dayanmalıdır (Nosworthy, 2000).

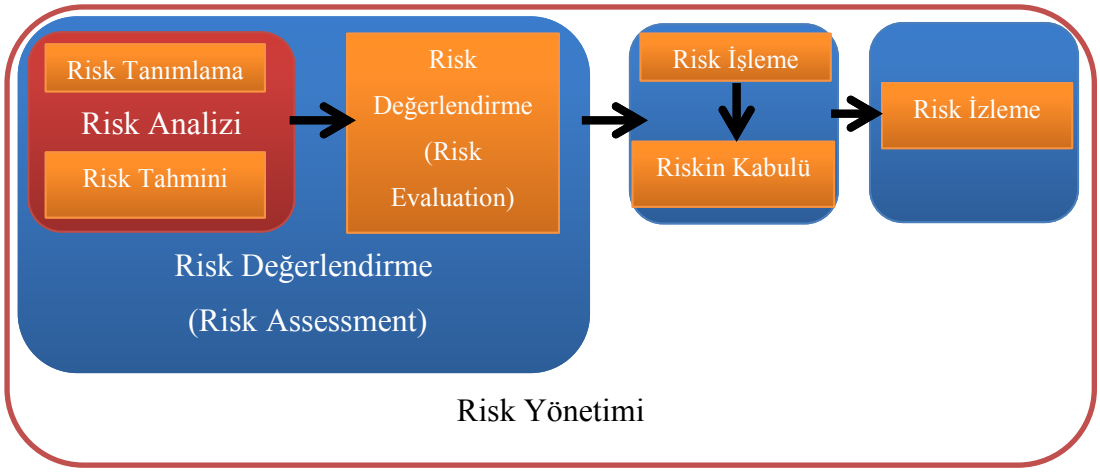
Risk, sıklıkla kullanılan bir kelimedir. Riskin günlük hayatta kullanımı kadar mühendislik, finans ve bilim alanında da yer edinmiştir. Risk kelimesi İngilizce karşılığı "Risk" olup ilk defa 1600 lü yıllarda kullanılmıştır. Kelimenin kökeni Latince riziko (risicum) ya da Arapça rızık ("رزق") köklerinden türetilmiştir (Ansell ve Wharton, 1992: 4-5). Rızık rassal ve istenen olumlu bir durumdur. Riziko ise, bir balıkçının kayalıklı alanla karşılaşması gibi istenmeyen olumsuz bir olaydır. ISO 31000 / ISO Rehber 73'te risk belirsizliğin bir nesne üzerindeki etkisi olarak tanımlanmıştır.

Risk, kullanım alanına göre farklı anlamlar içerse de en genel anlamıyla bir olayın etkisi (şiddeti) ile olasılığının fonksiyonudur (Fazil, 2005: 2 ,Rebello ve Goyal, 2010). Riski tanımlayan fonksiyon Eş. 4.1'de gösterilmiştir.

Risk = f [ (tehlikenin şiddeti), (tehlikenin olasılığı)] (4.1)

Bazı kaynaklarda risk, "Risk=OlasılıkxŞiddet" şeklinde basit fonksiyon olarak da tanımlanmaktadır. Risk ile belirsizlik yakın anlama sahip olsalar da arada belirgin bir fark vardır. Risk hassas bir şekilde ölçülebilmekte ve nicel değer alabilmektedir. Belirsizlik ise kesin olarak ölçülemeyen durumların ifadesidir (Knight, 1921: 19).

Şekil 4.1'de risk yönetimi sürecinin aşamaları görülmektedir[2] (ISO, 2008, 2009a). Çalışmanın bu bölümünde sadece risk tanımlama ve risk analizi aşamalarına yoğunlaşılacaktır. Tehlike teorisinden, tehlike analiz tiplerinden ve risk analiz tekniklerinden bahsedilecektir.




Şekil 4.1. ISO/ IEC 27005'e Göre Risk Yönetim Süreci

Riskin rol oynamadığı herhangi bir durum düşünmek zordur. Risk; hava durumu, sağlık, fiyatlar, deprem ve yangın ile ilgili olabilir (Rennie, 1961).

Risk analizi; ortamdaki tehlikeleri belirleyen, onların kritik değişkenler ve fonksiyonlar üzerindeki etkilerini araştıran ve koruma amaçlı mekanizma ve stratejiler geliştiren bir süreçtir (Kahraman, 2009).

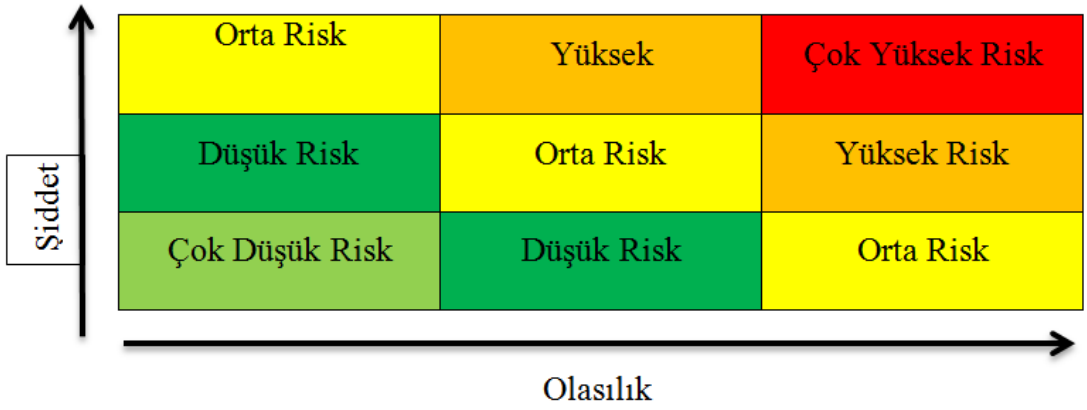
Risk analizi, riskin anlaşılmasını amaçlayan yöntemler bütünüdür denilebilir. Burada risk stratejik kararda ele alınan bir parametre ile ilgilidir (Arman, 1997: III).

Risk analizi, riskin anlaşılabilirliğini geliştirmeyi sağlar. Risk değerlendirmesine ve risklerin işlenmesi gerekip gerekmediği konularında kararlar alabilmek için ve en uygun risk işleme stratejileri ve yöntemlerini belirleyebilmek için girdi sağlamaktadır. Risk analizi ayrıca farklı tip ve seviyelerdeki riskler içeren ve bunlar arasında tercih yapılması gereken kararlara da bir girdi sağlayabilir (ISO, 2009a).

[2] Risk yönetimine ait faaliyetler farklı şekilde guruplandırılabilse de genel olarak bu 5 aşamadan oluşmaktadır.

Risk analizi; risklerin nedenleri ve kaynaklarını, onların olumlu ve olumsuz sonuçlarını ve bu sonuçların meydana gelme olasılığı gibi konuları içerir. Sonuçları ve olasılığını etkileyen faktörler belirlenmelidir. Bir olay birden fazla sonuç doğurabilir ve birden fazla hedefi etkileyebilir. Mevcut kontroller ve bunların etkinlik ve verimliliği de dikkate alınmalıdır (ISO, 2009a).

Tehlikeler belirlendikten sonra bu tehlikelerin şiddeti ve olasılığı da dikkate alınarak risk analizi yapılır. Riskleri belirlemek için risk matrisi kullanılabilir. Şekil 4.2'de L tipi Risk Matrisi görülmektedir. Olasılığı ve şiddeti düşük olan bir tehlikenin riski çok düşük; olasılığı ve şiddeti yüksek olan bir tehlikenin riski ise çok yüksek olarak ortaya çıkacaktır.




Şekil 4.2. L Tipi Risk Matrisi

Risk analizinin sistem hayat çevriminin erken safhalarında yapılması önemlidir. Bir proje sonuca yakın risk analizine tabi tutulduğunda riskler analiz edilse de riskleri ortadan kaldırmak için çok geç kalınmış olunabilir. Akademik bir çalışmada yazılım projesi risk yönetimi konusunda 20 tane araştırma projesi incelemiş ve bunları birbiriyle karşılaştırmıştır. Ulaşılan bulgularla hayat çevriminin daha erken aşamalarına odaklanılması gerektiği ifade edilmiştir. Proje öncesi aşamalarda daha az risk analizi çalışması yapıldığı görülmüştür (Erdem ve Younis, 2012).

Labuschagne ve Eloff, (1998) belirli bir iletişim oturumu için Global Risk Değerini (GRV) belirlemeyi amaçlamışlardır. GRV çeşitli tekil risk faktörlerinin birleştirilmiş halidir. Tipik risk faktörleri, iletişim oturumunun kaynak ve hedef adresleri olarak ifade edilebilir. İnternet protokol paketlerinin bileşenleri analiz edilerek normal durumdan farklı akan ağ trafiğinde tehditler saptanmaya çalışılmıştır. Araştırmacılar, GRV değerlerini

hesaplayabilmek için bazı kurallar oluşturmuş, bilgisayar korsanlarından gelebilecek tehditlerin riskini 0-1 arasında hesaplamışlardır.

## 4.1. Tehlike Teorisi

Sistem güvenilirliği ve düşük risk için tehlikelerin belirlenmesi ve ortadan kaldırılması şarttır. Tehlike teorisini doğru anlamak ve tehlikeleri sistematik bir şekilde belirlemek gerekmektedir. Sistem tehlike analizleri sonucunda sistem, alt-sistem ve bileşenlerin sahip oldukları tehlikeler ortaya çıkar. Tehlike teorisini anlamak amacıyla bazı kavramları açıklamak gerekmektedir (Booher, 2003: 499).

Kaza (accident)

Malzeme, ekipman, kargo, insan v.b. unsurlarda hasara, yaralanmaya veya ölüme neden olan, planlanmamış, istenmeyen, beklenmeyen olaydır.

Aksilik (mishap)

Ölüm, yaralanma, meslek hastalığı, ekipman veya çevrede kayıp ve hasarlara neden olan planlanmamış olay, kaza. Aksilik kazayı da içeren geniş bir anlama sahiptir. Risk ise, bir aksiliğin ortaya çıkma olasılığı ve şiddetinin ifadesi olduğundan aksiliğin ölçülmüş hali denebilir.

Tehlike (hazard)

Ölüm, yaralanma, meslek hastalığı, ekipman veya çevrede kayıp ve hasarlara neden olabilecek potansiyel durumdur. Aksiliğin ön şartını oluşturan durumdur. Tehlike, bazı değişimler sonucunda aksiliğe (kaza) dönüşmektedir.

Tehlike basit anlamda bir risk kaynağıdır. Risk, bir kayıp veya yaralanmanın olasılığı ile bu kayıp veya kazanın şiddetinin bileşimidir. Tehlike ise kazanın kaynağıdır. Eş. 4.2'de risk ile tehlikenin arasındaki ilişki gösterilmiştir. Formülden de anlaşılacağı üzere önlemler (kontrol) ne kadar artarsa artsın tehlike olduğu müddetçe risk hiçbir zaman sıfır olmaz (Kaplan ve Garrick, 1981).

$$Risk = \frac{Tehlike\ (Hazard)}{Önlem\ (Safegurads)} \tag{4.2}$$

Tehlikenin bileşenleri

Detaylı incelendiğinde tehlikenin üç bileşeninin olduğu görülür (Mansourov ve Campara, 2010: 126). Bunlar; (1) tehlikeli eleman (TE), (2) tetikleyici mekanizma (TM), (3) hedef ve tehdittir (H/T).

Tehlikeli eleman tehlikeye asıl sebep olan temel tehlikeli kaynaktır. Bir tesisteki patlayıcı özelliğe sahip kimyasal maddeler tehlikeli elemana örnektir. Tetikleyici mekanizma tehlikeli elemanı harekete geçiren tehlike bileşenidir. Hedef ve tehdit ise tehlikede zarar gören yani olumsuz etkilenen bileşendir. Bu bileşen aksiliğin çıktısıdır ve şiddeti belirler.

Tehlikeyi daha iyi anlayabilmek için Çizelge 4.1'de bileşenlerine ayrılmış bazı tehlikeler verilmiştir. Bilişim hizmetlerinin sürekliliği göz önüne alındığında hedef/tehdit, tehlikeli elemanın kendisi olabilmektedir. Bir tehlikede birden fazla tetikleyici mekanizma ya da hedef bileşeni olabilmektedir. Böyle bir durumda tetikleyici mekanizmaların doğru sırada gerçekleşmesi gerekmektedir.

Çizelge 4.1. Tehlikeli Bileşen Örnekleri

| **Tehlikeli Eleman** | **Tetikleyici Mekanizma** | **Hedef/Tehdit** |
|---|---|---|
| İşletim Sistemi | Virüs bulaşması | Bilgisayardaki dosyaların silinmesi |
| Elektrik | Elektriğin kesilmesi | Verinin kaybedilmesi |
| Router Yazılımı | Yanlış yapılandırma | Ağ bağlantısının kesilmesi |
| Kullanıcı | Fazla sayıda istek | Sunucunun çökmesi |

## 4.2. Tehlike Analiz Tipleri

Sistemin çevirim safhası kabaca üçe ayrılabilir. Sistem çevrimi tasarımdan başlar ve operasyon safhasına geçilir. Ömrü dolan sistemin operasyon safhası biter ve kullanım dışı bırakma (imha ya da devre dışı bırakma) safhası ile son bulur. Sistemdeki tüm tehlikeleri ortaya çıkarabilmek için tasarımdan ölüme değin sistemin bütün ömrünü analiz etmek gerekir. Çevrim safhasına ve hedefine göre tehlike analizleri farklılık gösterir. Sistem güvenliğinin sağlanması amacıyla farklı safhalarda farklı analizler gerçekleştirilmektedir. Risk analizi ilk olarak kavramsal sistem tasarımı aşamasında başlatılmalı, riskler ortaya çıkarılmalıdır. İlerleyen safhalarda detaylı tasarım ortaya çıkınca buna yönelik daha detaylı tehlike analiz yapılır. Operasyon safhasında işlemlere yönelik tehlike analizleri yapılır. Alt sistemlerin mevcudiyeti durumunda sistemler arası tehlikeleri belirlemek için arayüzlere yönelik tehlike analizi yapılır. Sistemin gereksinimleri karşılayıp karşılamadığı konusunda ve çalışanların sağlıklarına yönelik tehlikeler de analiz edilir.

## 4.3. Tehlike Analizi Teknikleri

Tehlike analizinde kullanılabilecek çok sayıda analiz tekniği vardır. Bazı analiz teknikleri diğer teknikler üzerinde değişiklikler yapılarak elde edilmiştir. Çalışmanın bu bölümünde kabul görmüş tehlike analiz teknikleri anlatılacaktır. Bu teknikler; ön tehlike listesi (ÖTL), ön tehlike analizi (ÖTA), Alt Sistem Tehlike Analizi (ASTA), Sistem Tehlike Analizi (STA), İşlem ve Destek Tehlike Analizi (İDTA), Güvenlik Gereksinimleri Analizi (GGA), hata türleri ve etkileri analizi (HTEA), tehlike ve işletilebilirlik analizi (HAZOP), hata ağacı analizi (HAA) ve olay ağacı analizidir (OAA). Bu teknikler tehlike ve güvenilirlik analizinin temel yapıtaşını oluşturmaktadır.

Analiz tekniklerinin kullanımı amacına ve sistem hayat safhasına göre değişiklik göstermektedir. Çizelge 4.2'de Sistem hayat safhaları ve bu safhalarda önerilen öncelikli analiz teknikleri verilmiştir. (Ericson, 2005: 53).

Çizelge 4.2. Sistem Hayat Evresi ve Öncelikli Teknikler

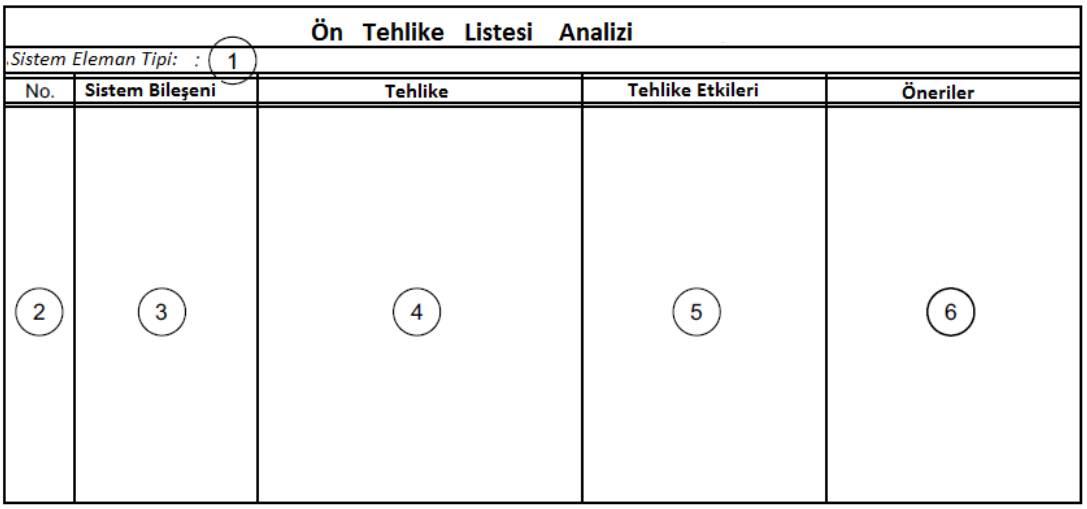
| Sistem Hayat Evresi | Odaklanılan Tehlike | Öncelikli Tekniği |
|---|---|---|
| Kavramsal tasarım | Sistem tehlikeleri | ÖTL (PHL) |
| Ön tasarım | Sistem tehlikeleri | ÖTA (PHA) |
| Detaylı sistem tasarımı | Alt sistem tehlikeleri | ASTA (SSHA) |
| Entegre sistem tasarımı | Entegre sistem tehlikeleri | STA (SHA) |
| Kullanım tasarımı | Kullanım tehlikeleri | O&SHA |
| Tasarım, test ve güvenlik gereksinimleri | Gereksinimler/testler | GGA (SRCA) |

### 4.3.1. Ön tehlike listesi

Ön tehlike listesi (ÖTL), kavramsal ve ön tasarım aşamalarında uygulanan bir tehlike analiz tekniğidir. Bu analizin en önemli avantajı, kısa sürede kolayca ve düşük maliyetle uygulanabilmesidir. Potansiyel tehlikelerin belirlenmesi amacıyla kullanılır. ÖTL, analiz tipleri için bir başvuru noktası ya da başlangıç noktası olarak görülebilir. Bu teknik, kavramsal tasarım ve ön tasarım aşamaları sırasında uygulanmaktadır. ÖTL detaylı ve derinlemesine değerlendirmeler için bir tehlike belirleme yöntemi değildir. Başlangıç tehlike listesini oluşturulması amaçlanır (Cho, 1998).

ÖTL, bilinen ve potansiyel tehlikeleri listeler. Analist, tehlikeler konusunda sahip olduğu bilgiyi kullanarak teknik personelle görüşmesi sonucunda sistemin tasarımında bulunan tehlikeleri belirler. ÖTL sonucunda istenirse tehlikelerin nedenleri ve sınıflandırılması da yapılabilir. Bu analiz tekniğinde detaylı bilgiye ihtiyaç yoktur. İhtiyaç duyulan bilgi benzer sistemlerden ve kontrol listelerinden sağlanabilir. Analist ÖTL analizi sonucunda çıktı olarak tehlike listesini ve üst seviye aksilikler listesini elde eder.

Kolaylık sağladığı için ÖTL'in uygulanmasında bir analiz formu kullanılır. Şekil 4.3'te ÖTL tekniği için kullanılabilecek örnek bir analiz formunun görüntüsü verilmiştir (Ericson, 2005: 61).




Şekil 4.3. Örnek ÖTL Analiz Formu

Analiz formunda (1) ile gösterilen alana sistem elemanının tipi yazılır (sistem donanımı, sistem yazılımı, enerji kaynakları). Formun (2) ile gösterilen alanına tehlike takibi için kullanılacak tehlike sıra numarası yazılır. Formun (3) ile gösterilen alanına sistem elemanının alt bileşeni yazılır. Formda (4) ile gösterilen alana belirlenen tehlike yazılır. Formda (5) ile gösterilen alana tehlikenin neden olduğu aksilikler yazılır. Formun (6) ile gösterilen alanına önemli bilgiler ve öneriler yazılır.

### 4.3.2. Ön tehlike analizi

Ön tehlike analiz (ÖTA) tekniği, sistem tasarımı konusunda detaylı bilgi olmadığında tehlikelerin, onlarla ilişkili nedensel faktörlerin, etkilerinin, risk seviyelerinin ve onları azaltacak tasarım ölçümlerinin tanımlanması amacıyla yapılan bir güvenlik analizidir. Amaç, güvenliğin sağlanması amacıyla sistem geliştirme sürecinin erken safhalarında tasarımı olumlu etkilemek veya sistem üzerinde hızlı bir risk analizi gerçekleştirmektir. ÖTA, ÖTL tekniği tarafından belirlenen tehlikelerin analizinin yanı sıra yeni tehlikelerin de tanımlanması amacıyla gerçekleştirilir. ÖTA aynı zamanda tasarıma güvenlik açısından odaklanılması amacıyla kritik güvenlik fonksiyonları ile üst seviye aksilikleri de belirler. Sistemin boyutu ve çalışmanın maliyeti ne olursa olsun ÖTA tekniğinin kullanımı özellikle tavsiye edilmektedir. Tehlikelerin tanımlanması amacıyla en sık kullanılan analiz tekniği ÖTA'dır. Çoğu durumda ÖTA sistemin içerdiği tehlikelerin büyük bir kısmını tanımlar. Kalan tehlikeler ise genellikle daha detaylı tasarım bilgilerinin sağlanması veya daha uzun

analiz süresi harcanmasıyla ileri analiz tekniklerinin kullanımı yoluyla tespit edilebilecek tehlikelerdir. (Nolan, 2014: 139).

ÖTA analizinde kullanılan risk analiz formu için iyi bir örnek Şekil 4.4'de verilmiştir. Analiz formunda (1) ile gösterilen alana analiz edilen sistem yazılır. Analiz formunda (2) ile gösterilen alana alt sistem ya da fonksiyonun adı yazılır. Analiz formunda (3) ile gösterilen alana analist bilgileri, (4) ile gösterilen alana analiz tarihi, (5) ile gösterilen alana referans için kullanılacak tehlike sıra numarası yazılır. Analiz formunda (6) ile gösterilen alana belirlenen tehlikeler yazılır. Analiz formunda (7) ile gösterilen alana tehlikenin nedenleri (tetikleyici olaylar) yazılır. Formda (8) ile gösterilen alana tehlikenin neden olabileceği aksilikler, (9) ile gösterilen alana tehlikenin etkin olabileceği safha ya da kip, (10) ile gösterilen alana tehlikenin başlangıç risk değeri, (11) ile gösterilen alana tehlikeleri azaltacak öneriler yazılır. Analiz formunda (12) ile gösterilen alana önleyici tedbirler uygulandıktan sonraki risk değeri, (13) ile gösterilen alana gerekli diğer bilgi ve tecrübeler, (14) ile gösterilen alana tehlikenin açık, kapalı ya da devam edip etmediğine ilişkin bilgi yazılır (Ericson, 2005: 79-80).

| Sistem Alt-sistem/Fonksiyon (1) (2) | | | Ön Tehlike Analizi | | | | Analist: (3) Tarih: (4) | | |
|---|---|---|---|---|---|---|---|---|---|
| No. | Tehlike | Nedenleri | Etkileri | Mod | BRİ | Tavsiyeler | SRİ | Düşünceler | Durum |
| (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) | (13) | (14) |

Şekil 4.4. Örnek Ön Tehlike Analiz Formu

### 4.3.3. Alt sistem tehlike analizi

Alt sistem tehlike analizi (ASTA), alt sistem seviyesinde uygulanan detaylı bir tehlike analiz tekniğidir. Daha önceden belirlenmiş tehlikelerin alt-sistem seviyesinde daha detaylı değerlendirilmesi için alt sistem tehlike analizi tekniği uygulanır. ASTA süreci ÖTA süreciyle aynıdır. Aralarındaki tek fark ASTA'nın sistemin en alt bileşenlerine kadar tümüne uygulanmasıdır. Detaylı tasarım bilgilerine sahip olunması ve/veya analize yeterince zaman ayrılabilmesi durumunda ASTA uygulanabilir. ASTA, tehlikelerin nedensel faktörlerini kök neden seviyesine kadar revize eder. ASTA sürecinde sistemde

bulunan ve analiz edilmesi gereken tüm alt bileşenler için birer adet analiz formu oluşturulur (Roland ve Brian, 1990: 213-218).

### 4.3.4. Sistem tehlike analizi

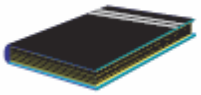
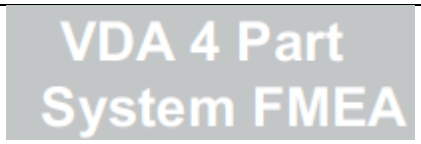
Sistem tehlike analizi (STA), alt sistemlerin entegrasyonundan kaynaklanan tehlikelere yönelik bir çalışmadır. STA; arayüz ve kritik güvenlik fonksiyonlarına odaklanarak, sistem seviyesinde risk ve güvenlik uyumluluğunu analiz eden bir tekniktir. Sistemin bütününü analiz ederek daha önce yapılmış olan ASTA'ların entegrasyonunu gerçekleştirir. STA, her tip sisteme detaylı tasarım aşamasında veya kullanım dâhil sonraki aşamalarda uygulanabilir. STA, alt sistem tehlike analizi sürecinde tespit edilmemiş olan ve birden fazla alt-sistemin etkileşimi sonucu ortaya çıkan tehlikeler ve riskleri tanımlar. Analizin yaklaşımı alt sistemler arasındaki ara yüzlerin incelenmesi şeklindedir. STA, alt sistem ve bileşenler arasındaki ara yüzlere ve kritik güvenlik fonksiyonlarına odaklanarak riskin ve sistem düzeyindeki güvenlik uyumluluğunun değerlendirilmesi amacıyla yapılan bir analiz metodolojisidir. STA, sistem düzeyinde tüm tehlikelerin anlaşıldığından, nedensel faktörlerin belirlenip azaltıldığından ve toplam sistem riskinin bilinip kabul edildiğinden emin olur (Roland ve Brain, 1990: 218-222).

### 4.3.5. Hata türleri ve etkileri analizi

Hata türleri ve etkileri analizi (HTEA), ilk uygulandığı alan uçuş kontrol sistemleridir. Amerika Birleşik Devletlerinde 1950 yıllarında kullanılmaya başlanan HTEA analiz tekniği 1960'lı yıllarından sonra havacılık sanayinde önemli bir yer edinmiştir. Daha sonra bu analiz tekniği Ford otomotiv şirketi tarafından kullanılmıştır. Otomotiv sektöründe bu analiz tekniği ile oldukça başarılı sonuçlar elde edilmiştir (Akın, 1998: 12).

HTEA'nın kökeni ve kullanım alanlarına ait kronolojik sıralama Çizelge 4.3'te verilmiştir. (Bertsche, 2007: 99).

Çizelge 4.3. HTEA'nın Orijini

| | | |
|---|---|---|
| 1963 | NASA (Apollo projesi) |  |
| 1965 | Havacılık ve havacılıkla ilgili yapılar (MIL-STD 1629A*) |  |
| 1975 | Nükler teknoloji |  |
| 1978 | Otomotiv endüstrisi (Ford) |  |
| 1980 | Almanya'da standardizasyon |  |
| 1986 | Otomotiv endüstrisinde ileri uygulamaları |  |
| 1990 | Elektronik ve yazılım geliştirmede uygulaması |  |
| 1996 | Sistem HTEA'nın geliştirilmesi |   |

HTEA, bilinen veya beklenen hata türlerini ve bunların sebeplerini ve etkilerini tanımlamada, tanımlanan hata türlerinin sıralanmasında ve hata türlerinin ortadan kaldırılmasında yardımcı olur. HTEA'nın esas amacı, bilinen ya da beklenen hataların müşteriye ulaşmasını önlemektir. Bu nedenle, her hata riski değerlendirilmeli ve riskler sıralanmalıdır (Chin, Wangb, Poona ve Yangc, 2009)

HTEA kendi tasarım amacını yerine getirmeyen bileşenlerin, sistemlerin veya süreçlerin hata belirleme yollarını tanımlamak için kullanılan bir tekniktir (ISO, 2009b).

HTEA'nın esas amacı; hata /arıza türlerini, etkilerini ve kritikliklerini kararlaştırmak, ürünün kritik (tehlikeli) hata/arızalarını belirlemek, hataları, kusurları, arızaları ve kritikleri ortadan kaldıracak veya en aza indirecek; değişiklikleri, yöntemleri ve testleri uygulayarak, ürünü en son mükemmel haline getirmeyi başarmaktır (Stamatis, 2003: 28).

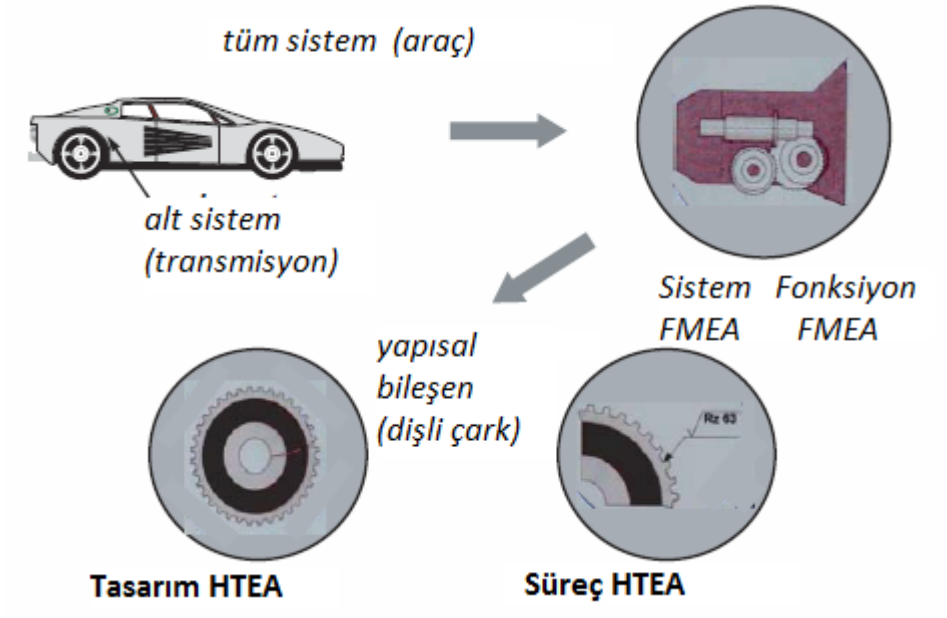
HTEA hakkında yayınlanmış ilk standartlardan biri olan Amerikan MIL-STD 1629A (Hata Türü, Etkileri ve Kritiklik Analizi Uygulaması Prosedürü)'nde HTEA "Sistemdeki her bir olası hata türünün, sonuçlarını veya etkilerini belirlemek ve önemlerine göre her bir hata türünü sınıflandırmak için analiz edildiği bir prosedürdür" şeklinde tanımlamıştır.

HTEA; neyin nasıl ve hangi sıklıkla başarısız olacağını cevaplar. Ayrıca bu başarısızlıkların etkilerini de değerlendirir. Bu sonuçlara ulaşabilmek için sistem tasarımı, işlemsel kısıtlar, başarısızlık modları ve sıklıkları hakkında bilgi sahibi olunması gerekmektedir.

HTEA, alt-sitem, montaj, bileşen veya fonksiyonların potansiyel başarısızlık modları üzerinde durur. HTEA, daha çok donanım ve sürecin değerlendirilmesine yöneliktir. Bileşenlerin başarısızlık hızları da göz önüne alınırsa incelenen alt-sitem veya bileşene ilişkin olasılıklar da elde edilebilir. Genellikle bileşen düzeyindeki başarısızlık oranları mevcut olduğu için HTEA da bileşen seviyesinde uygulanır. HTEA, tek bir bileşenin başarısızlıklarını göz önüne alır. Bu yüzden çoklu bileşen başarısızlık kombinasyonlarını incelemede yetersiz kalmaktadır. HTEA, başarısızlıkların dışında kalan radyasyon gibi olayların sonucu ortaya çıkabilecek tehlikeleri de tanımlayamaz. Bu nedenle HTEA tehlike analizlerinde tek başına yetersizdir (Ericson, 2005: 235-236).

HTEA'nın detayına geçmeden önce "başarısızlık modu" kavramını açıklamak gerkmektedir. Başarısızlık modu bir sistem bilşeninin başarısızlığının türüdür. Diğer bir ifadeyle başarısızlık oluştuğunda içinde bulunduğu durumdur. Sistem bileşeni olarak bir vida ele alınırsa vidanın paslanması yani paslanmış olma durumu vida için bir başarısızlık modudur (hata türü).

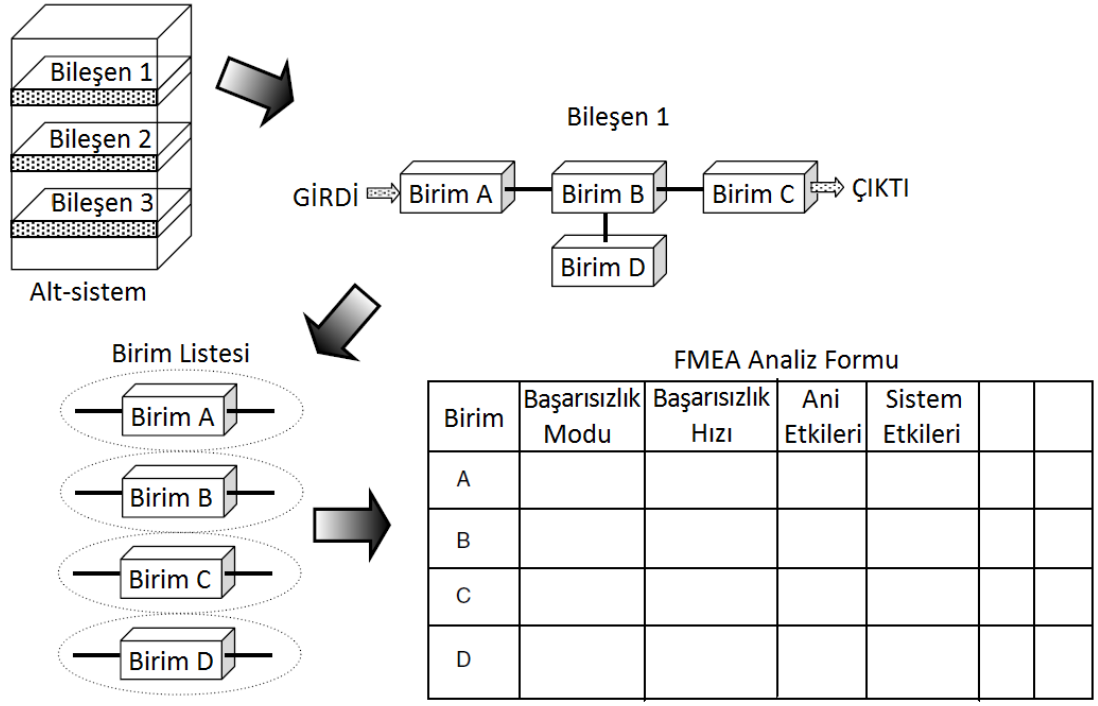
Sistemin tipine ve karmaşıklığına göre HTEA çeşitli prosedürlerden oluşmaktadır. Şekil 4.5'te çeşitli HTEA prosedürlerinin görünümü verilmiştir (Bertsche, 2007: 101).




Şekil 4.5. FMEA Çeşitleri

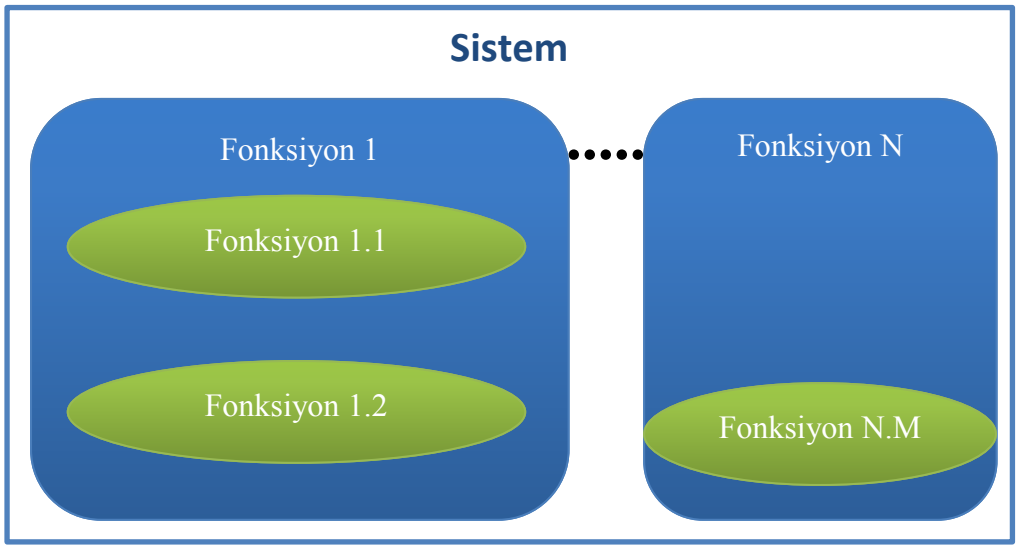
HTEA sürecinde alt sistem bileşenlerine ayrılır ve ihtiyaç duyulursa bu bileşenler de bir alt bileşene (birim) ayrıştırılır. Her biri diğerlerinden ayrışık olarak (izole edilerek) analiz edilmesi amacıyla HTEA formunun ilk sütununda listelenir. İkinci sütunda ise ilgili birim için söz konusu olabilecek potansiyel başarısızlık modları listelenir. Bu yolla alt-sistem yukardan aşağı doğru analiz edilmiş olur. Birimler donanım parçası veya bileşen olabileceği gibi fonksiyon da olabilir. Şekil 4.6'da örnek bir HTEA süreci gösterilmiştir (Ericson, 2005: 237-239).

HTEA'nın analiz ettiği birincil sistem yapıtaşları sistem donanımı ve sistem fonksiyonlarıdır. HTEA'nın sistem fonksiyonları bakış açısı, yapılması zorunlu olan fonksiyonel görevleri sistemin nasıl yerine getirmesi gerektiğini tanımlar. HTEA'nın sistem yapısı bakış açısı ise sistem operasyonlarını yerine getiren donanımlara fonksiyonların nasıl implemente edileceğini tanımlar.



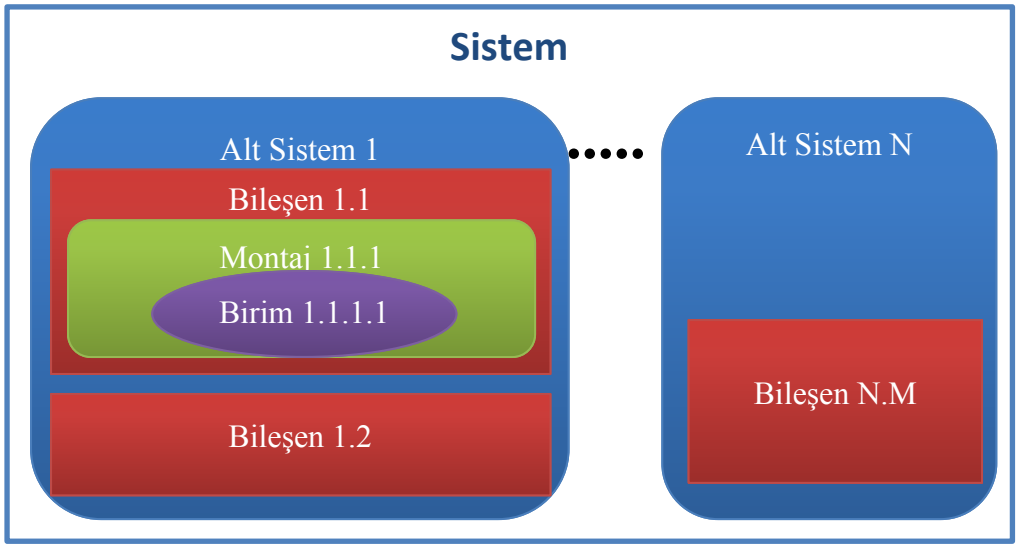

Şekil 4.6. HTEA Konsepti

Şekil 4.7'de bir sistemin fonksiyonel görünümü gösterilmiştir.




Şekil 4.7. Fonksiyonel Sistem Bakışı

Şekil 4.8'de bir sistemin yapısal görünümü gösterilmiştir. Sistem alt sistemlere, alt sistem bileşenlere, bileşenler montaja ve montaj birimlere ayrıştırılır.




Şekil 4.8. Yapısal Sistem Bakışı

### 4.3.6. Tehlike ve işletilebilirlik analizi (HAZOP)

HAZOP, Tehlike ve İşletilebilirlik (HAZard and OPerability) kelimelerinden oluşan bir kısaltmadır. Planlanmış veya mevcut ürün, süreç, prosedür veya sistemin yapılandırılmış ve sistematik olarak incelenmesidir. İnsan, ekipman, çevre ve / veya örgütsel amaçlara karşı riskleri tanımlamak için kullanılan bir tekniktir. Çalışma ekibinin mümkünse riskin azaltılması için bir çözüm sağlaması beklenir. HAZOP, temelde, tasarım aşamasında ya da çalışma esnasında, tasarımın, sürecin, prosedürün ya da sistemin hangi adımında başarısızlık olabileceğine göre kılavuz kelimelerinin kullanıldığı nitel bir tekniktir. HAZOP, ekip tabanlı bir teknik olup beyin fırtınası toplantıları şeklinde gerçekleştirilir. Genellikle toplantılar çoklu disipline sahip bir ekip tarafından yürütülmektedir. HAZOP tekniği başlangıçta kimyasal işlem sistemlerini analiz için geliştirilmiştir, ancak farklı sistemler ve karmaşık işlemler gibi konuları da kapsayacak şekilde genişletilmiştir. Bunlar arasında, mekanik ve elektronik sistemler, prosedürler, yazılım sistemleri ve hatta örgütsel değişiklikler ve yasal sözleşme tasarımı ve incelemeleri bulunmaktadır (ISO, 2009b). HAZOP, sistem tehlikelerinin belirlenmesinde “Daha fazla”, “Yok”, “Daha az” gibi referans anahtar kelimeleri ve sistem parametrelerini (hız, akış, basınç) kullanır.

HAZOP, Sistem, alt-sistem, montaj, bileşen, ekipman, yazılım, prosedür, çevre ve insan hatalarına uygulanabilir. Süreç veya sistemin her bir parçası için hedeften sapmaların olup olmayacağının incelenmesini kapsar. Sapma ve sonuçlarının sistemin güvenliği ve etkin

çalışması üzerinde olumsuz bir etkisinin olup olmayacağına yönelik değerlendirme yapılır. HAZOP sürecinde referans anahtar kelimelerle sistem parametrelerini karşılaştırılır. Karşılaştırma sonucunda tehlikelere neden olacak potansiyel sistem sapmaları belirlenmeye çalışılır. HAZOP'un başarısında referans anahtar kelimeler ile sistem parametrelerinin belirlenmesi çok kritiktir (Ericson, 2005: 267-268).

HAZOP yöntemine ilişkin genel sistem parametreleri Çizelge 4.4'te verilmiştir (Nolan, 2014b: 133-141).

Çizelge 4.4. Genel HAZOP parametreleri

| | | |
|---|---|---|
| ✓ Akış | ✓ Hizmet hataları | ✓ Aksiyon |
| ✓ Seviye | ✓ Anormal operasyon | ✓ Bilgi |
| ✓ Basınç | ✓ Prosedürler | ✓ Sıra |
| ✓ Sıcaklık | ✓ Statik | ✓ Güvenlik önlemleri |
| ✓ Geçirgenlik | ✓ Yedek ekipman | ✓ Global |
| ✓ Rölyef sistemi | ✓ Örnekleme | |
| ✓ Korozyon | ✓ Zaman | |

### 4.3.7. Hata ağacı analizi

Hata ağacı anlizi (HAA), istenmeyen bir olayın ("tepe olay" olarak adlandırılır) nedenlerinin analizinde kullanılan bir tekniktir. Nedensel faktörler tümdengelimli olarak tanımlanır, mantıklı bir şekilde organize edilir ve ağaç diyagramında nedensel faktörleri ve üst olay arasındaki mantıksal ilişkiyi temsili olarak resmederek gösterir. Hata ağacı, hataya (tepe olaya) götüren potansiyel nedenleri ve yolları belirlemek için nitel ya da bilgisi verilen nedensel olayların olasılıklarını, tepe olayın olasılığını hesaplamak için nicel kullanılabilir. Bu yöntem, hatanın olası nedenlerini belirlemek için ve/veya bir sistemin tasarım aşamasında farklı tasarım seçenekleri arasından seçim yapmak için kullanılabilir. Büyük hataların nasıl ortaya çıktığını ve esas olaya, farklı yolların göreceli olarak nasıl etki ettiğini görmek için çalışma aşamasında kullanılabilir. Bir hata ağacı farklı olayların bir araya gelerek hatayı nasıl meydana getirdiğini analiz etmek için kullanılabilir (ISO, 2009b).

HAA, Bell Laboratuarlarında çalışan Watson ve Mearns tarafından geliştirilmiş olup tekniğin analitik gücü ve başarısı ticari uçak ve nükleer güç endüstrisinde kendisini kanıtlamıştır. HAA ile bilinen genel bir hataya yol açan hata yolları araştırılmaktadır. Bu nedenle HAA ile tümden gelim yöntemi izlenir. HAA her tip sisteme, hayat çevriminin her aşamasında uygulanabilir. Hata yollarında yer alan tehlikelerin neden-sonuç ilişkilerinin modellenmesi amacıyla mantık kapıları ve hata olaylarını kullanan grafiksel modeller ile hata ağaçları oluşturulur. Grafiksel model, matematiksel modele çevrilebilir. Hata ağacının geliştirilmesi süreci, bir önceki yapının sürekli güncellendiği iteratif bir süreçtir (Ericson, 2005: 183-189).

### 4.3.8. Olay ağacı analizi

Olay Ağacı Analizi (OAA), başlangıç olayını takip eden farklı kaza senaryolarının modellemesi, hesaplaması ve sıralamasında kullanılabilir. Nicel analizler, kontrollerin kabul edilebilirlik analizine katkı sağlar. Sıklıkla çoklu önlemlerin olduğu hataları modellemek için kullanılır. OAA, kayıp veya kazanç getiren başlangıç olaylarını modellemek için kullanılabilir. Ancak, koşul olarak kazancı optimize etmek için sıklıkla karar ağacı modellenmiştir (ISO, 2009b).

OAA, olay ağacı adı verilen mantık temeline dayalı görsel bir ağaç yapısı kullanır. OAA, tek bir tetikleyici olayın neden olabileceği çok çeşitli sonuçları ortaya koyabilmektedir. Ayrıca her bir sonuca ilişkin ortaya çıkma olasıklarını hesaplayabilmektedir. OAA her türlü alt-sistem, sistem, bileşen ve yazılımın tetikleyici olaydan sonra meydana gelebilecek aksilikleri modelleyebilir. OAA ek olarak olasılık ve HAA konusunda bilgi sahibi olunması gerekmektedir.

## 4.4. Riske İlişkin ISO Standartları

Çalışmanın bu bölümünde risk yönetimi ve risk analizi ile ilgili ISO tarafından yayınlanmış standartlara değinilmiştir. Bu standartlar *ISO 27005:Bilgi Teknolojileri Risk Teknikleri-Bilgi Güvenliği Risk Yönetimi Standardı*, *ISO31000:2009 Risk Yönetimi Prensipler ve Rehber* ve *ISO IEC 31010:2009 Risk Yönetimi Risk Değerlendirme Teknikleri*dir.

### 4.4.1. ISO 27005: Bilgi teknolojileri risk teknikleri-bilgi güvenliği risk yönetimi standardı

ISO 27000 ailesinin her bir üyesinin odaklandığı bir konu vardır. Kurumlar ve kuruluşlar bilgi güvenliği altyapısını oluşturmak ve dokümantasyon yapılarını geliştirmek-düzenlemek istiyorsa temel olarak ISO 27001'i kullanırlar. ISO 27001 Bilgi Güvenliği Yönetim Sistemi planlama, uygulama, kontrol et ve önlem al adımlarından oluşan sürekli geliştirilen bir sistem sunar. ISO 27001 risk yönetimi kısmındaki tanımlar kullanılarak hangi kısımlara kontrol uygulanacağı tespit edilir. ISO 27001 Bilgi güvenliği hususunda büyük resmi verir. Eğer özel olarak risk yönetimi ile ilgileniliyorsa *ISO / IEC 27005:Bilgi Teknolojileri Risk Teknikleri* ve *ISO / IEC 31000 Risk Yönetimi- Prensip ve Rehber* standardı incelenmeli ve uygulanmalıdır.

### 4.4.2. ISO 31000:2009 Risk yönetimi prensipleri ve rehber

"ISO 31000 Risk Yönetimi Prensipler ve Rehber" standardı, risk yönetimi konusunda kurum ve kuruluşlara kurumsal risklerini tanımaları, analiz etmeleri ve bu risklerini azaltmalarına yönelik çalışmalarında kılavuzluk yapar. ISO 31000 standardı temelde risklerin belirlenmesini ve bu risklere zamanında müdahale ile risklerin tehlikeye dönüşmeden azaltılması ya da tamamen ortadan kaldırılmasını hedeflemektedir. Standartta yer alan maddeler risk yönetiminin sistemli ve kapsamlı bir biçimde nasıl yapılabileceğini anlatmaktadır. ISO 31000 Risk Yönetimi Standardı kurum ve kuruluşların risklerinden doğan maliyetlerini azaltmak, kurumsal değerlerini arttırmak ve yöneticilere kurumsal planlamalarında hedeflerini tutturmalarına yardımcı olmak amacıyla oluşturulmuştur. Diğer pek çok standartta olduğu gibi sertifikasyon amacıyla oluşturulmamıştır.

### 4.4.3. ISO IEC 31010:2009 Risk yönetimi - risk değerlendirme teknikleri

ISO 31000 ailesinin temeli olarak bu standarttan bahsedilebilir. Hangi risk değerlendirme tekniğinin seçileceği ve nasıl uygulanacağı bu standartta ayrıntılı olarak anlatılmıştır. Risk değerlendirmesi, risk analizi ve işleme işlemlerinin tamamıdır. Farklı riskler için uygulanabilecek farklı araç ve teknikler vardır. Risk değerlendirmesi; risklerin anlaşılması, sonuçları ve ihtimalleri ile ilgili bilgilendirmeyi yapar. Bu da kurum ve kuruluşların ileride yapmayı planladıkları bir projeye başlayıp başlamama kararını almasını, tespit edilen

mevcut bir riskin müdahale gerektirip gerektirmediğini, tespit edilmiş bir risk varsa ve eğer düzeltme gerekecekse hangi seçeneklerin olduğu, hangi seçeneklerin öncelikli uygulanması gerektiği gibi pek çok konuda kurumların alacakları kararlarda yardımcı olur. Bu standart da ISO 31000 gibi sertifikasyon amaçlı değildir.

# 5. KAMU KURUMU HAKKINDA

<Çalışmanın Yapıldığı Kurum>, kanun ile kurulmuş bir kamu kuruluşudur. Başkanlık merkez teşkilâtı, ana hizmet birimleri ile danışma ve yardımcı hizmet birimlerinden oluşmaktadır. <Çalışmanın Yapıldığı Kurum>'un merkez ve taşra teşkilâtının her türlü bilişim hizmetlerini yürütme görevi <BT Birimi>ne verilmiştir. Bu birimin ayrıca <müşteri> veri tabanını oluşturması, diğer kamu idarelerinin veri tabanları ile entegrasyonunu sağlaması, <müşteri> veri tabanı bilgilerinin güncelliğini sağlaması gerekmektedir. <Çalışmanın Yapıldığı Kurum> için gerekli yazılım ve donanım altyapılarını plânlamak, geliştirmek, kurmak, işletmek, yenilemek, bu altyapıların güvenliğini ve sürekliliğini sağlamak üzere gerekli önlemleri almak da <BT Birimi>ne kanunla verilmiş görevler arasındadır. <Çalışmanın Yapıldığı Kurum> verdiği hizmetlere ilişkin süreçlerin büyük bir kısmını elektronik ortama çektiği için bilişim hizmetleri kurum için hayati derecede önem arz etmektedir. Birçok kamu kurum ve kuruluşunda bilgi işlem birimleri daire başkanlığı seviyesinde oluşturulmasına rağmen <Çalışmanın Yapıldığı Kurum>'da bilişim hizmetlerini yürütmesi amacıyla Genel Müdürlük kurulmuştur. Bilgi teknolojilerinin <Çalışmanın Yapıldığı Kurum> için öneminden dolayı <BT Birimi> ana hizmet birimlerinden sayılmıştır. Bu bilgiler ışığında neden <Çalışmanın Yapıldığı Kurum>'un bilişim hizmetlerine yönelik risk analizinin yapıldığı daha çok anlaşılacaktır.

<Çalışmanın Yapıldığı Kurum>'da 25 bin civarı personel bulunmaktadır. Otuz binden fazla dış kurum ya da kuruluş <Çalışmanın Yapıldığı Kurum> bilgi sistemlerine online bağlantı sağlamaktadır. Banka ve tüm Türkiye Cumhuriyeti vatandaşlarının erişebildiği 50'den fazla e-devlet uygulamaları bulunmaktadır. <Çalışmanın Yapıldığı Kurum>'un sunmuş olduğu bilişim hizmetleri, toplumun tamamını ilgilendiren büyük ölçekli hizmetlerdir.

<Çalışmanın Yapıldığı Kurum>'da en yaygın kullanılan programlama dili Java'dır. Destek hizmetlerine yönelik[3] hazır alınan yazılımlar ise .Net veya PHP gibi programlama dillerinde yazılmış olabilmektedir. Kurum, <müşteri> verilerini ana sunucuda tutmaktadır. Mevcut durumda ana sunucunun haricinde de VTYS çalıştıran açık sistem sunucuları bulunmaktadır.

[3] Yemek hizmetleri için kullanılan tabldot uygulaması

## 5.1. İçe Sunulan Bilişim Hizmetleri

Çalışmanın bu bölümünde, <BT Birimi>nin diğer iç birimlere ve iç kullanıcılara sunmuş olduğu bilişim hizmetleri ele alınacaktır. Bu hizmetlerin hepsi detaylı olarak anlatılmayacak olup genel olarak değinilecektir. Kurum içi sunulan bilişim hizmetleri yazılım ve sistem olarak iki ana gruba ayrılmaktadır. E-posta hizmeti, veri tabanı hizmeti, sanallaştırma hizmeti, veri yedekleme hizmeti ile ağ ve güvenliği hizmeti başlıca sistem gurubu bilişim hizmetleridir.

### 5.1.1. Yazılım geliştirme hizmeti

<BT Birimi> bünyesinde çok sayıda daire başkanlığı yazılım geliştirmektedir. Bu daire başkanlıklarından Kurumsal Yazılımlar Daire Başkanlığı; personel, doküman yönetim sistemi gibi kurumun kendi içinde kullandığı uygulamaları geliştirmektedir. 2013 yılından itibaren <Çalışmanın Yapıldığı Kurumdaki> uygulamaların entegrasyonu ve modernizasyonu amacıyla Entegrasyon Projesi, bir Daire Başkanlığı bünyesinde yürütülmektedir. Projenin bir amacı kurumdaki yazılımların modernizasyonu ve entegrasyonu iken diğer bir amacı ise kurumsal mimariyi oluşturmaktır. Proje sonrasında <Çalışmanın Yapıldığı Kurumdaki> uygulama sayısı azalmakla birlikte bu uygulamaların geliştirilmesi uluslararası yazılım geliştirme yöntemlerine göre yapılacaktır. Hali hazırda proje kapsamında süreçler analiz edilmiş ve amaçlanan uygulamalar için tasarımlar hazırlanmıştır.

### 5.1.2. Veritabanı hizmeti

Kurumda <müşteri> bilgilerinin tutulduğu veritabanları bulunmaktadır. Bu veri tabanlarının üzerinde çalıştığı donanım ve VTYS ler çok çeşitlilik arz etmektedir. Kurumda 10'un üzerinde <A marka>, 5 adet <B marka>, 2 adet <C marka>, 3 adet <D marka> VTYS üzerinde koşan veritabanı bulunmaktadır.

### 5.1.3. Elektronik posta hizmeti

<BT Birimi>, kurum personeline elektronik posta hizmeti sunmaktadır. 25 bin civarındaki kurum personelinin tamamına eposta adresi sağlanmıştır. Eposta sunucusu olarak <B

şirketinin posta sunucusu> kullanılmaktadır. Posta sunucuları <X marka işletim sistemi> sunucusu üzerinde koşmaktadır. Kurum çalışanları ister masa üstü e-psota istemcisi üzerinden isterlerse web e-posta ara yüzü üzerinden e-posta hesaplarına ulaşabilmektedirler. Kuruma paydaşlardan ve diğer ilgili taraflardan çok sayıda e-posta gelmekte ve çok sayıda e-posta gitmektedir.

### 5.1.4. Sanallaştırma hizmeti

Sanallaştırma çok geniş bir konu olmakla birlikte genel olarak donanım, yazılım, uygulama, ağ, depolama gibi farklı katmanlardaki kaynakları birbirinden yalıtarak kullanılmasını sağlayan yazılım teknolojisi olarak tanımlanabilir.

*Tanım 1*: Sanallaştırma, donanımı ve yazılımı paylaştırma veya birleştirme, kısmi ya da bütün makine simülasyonu, benzetim, zaman paylaşımı vb. metotları kullanarak bilişim kaynaklarını bir veya daha fazla işletim ortamına sunmak için kombine eden veya ayrıştıran bir teknolojidir (Naveed, 2012).

*Tanım 2*: Sanallaştırma, uygulamaları ve altında yatan bileşenleri, onları destekleyen donanımdan soyutlamak ve bu kaynakların mantıksal veya sanal bir görüntüsünü sunmak için geliştirilen teknolojilerdir (Kusnetzky, 2011).

Web uygulamalarının üzerinde çalıştığı 700'den fazla ön sunucu bulunmaktadır. <A yazılım teknolojisi ile yazılan> uygulamalar için <X Uygulama Sunucusu>, <B yazılım teknolojisi ile yazılan> uygulamaları için <Y Uygulama Sunucusu> kullanılmaktadır. Uygulama sunucuları kümeleme (cluster) yapıda olduğu için sistem üzerinde yedekli olarak çalışabilmektedirler. Bu sistemler 230 $m^2$ büyüklüğündeki ana veri merkezi ve 400 $m^2$ büyüklüğündeki ikincil BT sistem odalarında bulunmaktadır. Ancak kısa süre sonra bu veri merkezleri ömürlerini doldurdukları için kapatılacak ve kullanılmayacaklardır. Kurum uçtan uca yenilenmiş veri merkezi çalışmalarını bitirmek üzeredir.

Kurumda sunucu sanallaştırması platformu; x86 sanallaştırma sunucuları, SAN depolama ağı ve IP ağından meydana gelmektedir. Kurumda sunucu sanallaştırma yazılımı olarak <X marka sanallaştırma platformu> kullanılmaktadır.

### 5.1.5. Ağ hizmeti

Kurum bilgi sistemleri ağı; tüm bilgi sistemleri hizmet ve cihazlarını birbirlerine bağlayan, güvenliği tam olarak sağlanmış her türlü ağ cihazları, fiziksel bağlantıları (kablolama), yazılımları ve bu ağın kesintisiz çalışması için gerekli diğer yan donanımların tanımlandığı alandır. Kurum ağı; sanallaştırma sunucuları, fiziksel sunucular, saldırı engelleme sistemleri (IPS), ana veri tabanı sunucuları (Mainframe), yük dengeleyiciler, anahtarlar, yönlendiriciler, veri eşleştirme araçları ve depolama sistemlerinden oluşmaktadır.

Ağ, erişim sağlayan personel ve cihazlar dikkate alınarak yetkilendirilmektedir, ölçeklendirilmektedir ve sürekli kontrol edilebilir durumdadır. Bu kapsamda <Çalışmanın Yapıldığı Kurum> ağı 3 mantıksal bölümde ele alınmıştır ve yapılandırılmıştır. Böylece ağ modüler olarak düzenlenmiş ve BT güvenlik ve yetkilendirmelerinin uygun olarak yapılması için temel oluşturulmuştur.

Bu alandaki <Çalışmanın Yapıldığı Kurum> ağı taşra teşkilatını da içine alan büyük bir yapıyı oluşturması ve arada kiralık hatların ve kontrol edilemeyen fiziksel alanların oluşabileceği düşünülerek uçtan uca yönlendirme ve yapılandırmaların uygun olarak yapılması, yetkisiz cihazların ağ kaynaklarına erişiminin engellenmesi önem arz etmektedir. Bu kapsamda da ağ erişim kontrol sistemi taşra teşkilatına genişletilmiştir ve ağa bağlanan her cihazın, kurum envanterine kayıtlı, içinde sadece izin verilen yazılımların bulunduğu, anti-virüs ve işletim sistemi yamalarının güncel olduğu görüldükten sonra ağ kaynaklarından faydalanması sağlanmaktadır.

Kullanıcı ağı üzerinde ağ erişim sistemi kurulmuştur ve yetkisiz cihazların ağa erişimi engellenmektedir. Ağ erişim sistemi olmaksızın, ağın ölçeklenmesi ve güvenliğinin tam olarak sağlanması imkânsızdır. Tesis edilen ağ erişim sisteminde donanım çözümü oluşturulmuştur ve yetkili cihazların fiziksel adresleri ağa tanımlanarak işlem yapılmaktadır.

### 5.1.6. Veri yedekleme hizmeti

Yedeği alınacak ortam Sistem Yönetimi Şube Müdürlüğüne “Yedekleme ve Geri Yükleme Talep Formu” ile iletilen yedekleme talepleri değerlendirilir, yedeklenmesi

kararlaştırılanlar mevcut Yedekleme Planına eklenir. < İlgili Şube Müdürlüğü>, belirlenen politika çerçevesinde sistemlerin ve verilerin yedeklerini alır. Yedekler kapasite, performans ve öncelik kısıtlarına göre disk ya da teyp ortamına alınabilir. Yedek alma planına göre yedeklemelerin yapıldığı günlük olarak kontrol edilir. Alınan yedekler de "tamamlandı" olarak işaretlenir.

Yedeği alınan tüm veri kümeleri kurumun başka bir lokasyonunda kasa içerisinde saklanır. Saklanan veri, yerine yedekleme planında belirtilen sürede yenisi geldiğinde kasadan çıkartılır. Yedekleme birimine tekrar yedekleme aracı olarak kullanılmak üzere gönderilir. İletim kurum personeli tarafından kurum aracı ile gerçekleştirilir.

<İlgili Şube Müdürlüğü> yedeği alınan tüm verileri asgari altı ayda bir en az farklı iki tarihteki yedeklerinden geri yükleyerek geri yükleme testlerini gerçekleştirir. Geri yükleme testleri bu iş için ayrılmış test sistemleri üzerinde gerçekleştirilir. Geri yükleme test sistemleri yazılım geliştirme test sistemlerinden ayrık ve bağımsızdır. Geri yükleme testlerine ilişkin kayıtlar imzalı olarak tutulur ve <İlgili Kurul> tarafından kontrol edilir.

Herhangi bir veri kümesinin ya da sistemin yedeğinin geri yüklenmesi ilgili veri sahibi ya da işletmeninin yazılı iznine tabidir. <İlgili Şube Müdürlüğü> yazılı talebi alınmamış herhangi bir geri yükleme çalışmasını gerçekleştirmez. Talep yazılarında hangi tarihli yedeğe dönüleceği ve geri yüklemenin ne zaman ve nasıl gerçekleştirilmesinin talep edildiği açıkça yer alır. Geri yükleme öncesinde, geri yüklemenin acil olmaması durumunda, verilerin ya da sistemin geri yükleme öncesindeki son halinin yedeği de alınır ve geri yükleme ancak bundan sonra başlatılabilir.

Yazılım gruplarının oluşturdukları verilerin standart büyüklüklere sahip olmaması ve periyotlarının düzenli olmaması sebebiyle bu verilerin yedeklemesinin ve saklamasının sorumluluğu ile ilgili politikaların hazırlanması ilgili yazılım gruplarına bırakılmıştır. Yedeklemelerin alındığı medyaların 2 (iki) kopyası yedekleme yönetimine ilgili yazılım grubu tarafından teslim edilecektir.

Herhangi bir veri kümesinin ya da sistemin yedeğinin geri yüklenmesi ilgili veri sahibi ya da işletmeninin yazılı iznine tabidir. <İlgili Şube Müdürlüğü> yazılı talebi alınmamış herhangi bir geri yükleme çalışmasını gerçekleştirmez. Talep yazılarında hangi tarihli

yedeğe dönüleceği ve geri yüklemenin ne zaman ve nasıl gerçekleştirilmesinin gerektiği açıkça yer alır. Geri yükleme öncesinde, geri yüklemenin acil olmaması durumunda, verilerin ya da sistemin geri yükleme öncesindeki son halinin yedeği de alınır ve geri yükleme ancak bundan sonra başlatılabilir.

Yedekleme yönetimi tarafından yedeği alınan tüm verileri asgari altı ayda bir en az farklı iki tarihteki yedeklerinden geri yükleyerek geri yükleme testlerini gerçekleştirir. Geri yükleme testleri bu iş için ayrılmış test sistemleri üzerinde gerçekleştirilir. Geri yükleme test sistemleri yazılım geliştirme test sistemlerinden ayrık ve bağımsızdır. Geri yükleme testlerine ilişkin kayıtlar imzalı olarak tutulur ve <ilgili Kurul> tarafından kontrol edilir.

## 5.2. Dışa Sunulan Bilişim Hizmetleri ve Uygulamalar

Çalışmanın bu bölümünde, <Çalışmanın Yapıldığı Kurum>'un dışarıya vermiş olduğu bazı hizmetlerin bilişim yönü ele alınacaktır.

Kurumda intranet ve internette sağlık, sigortalılık, insan kaynakları gibi alanlarda kullanılan 300'den fazla web uygulaması hizmet vermektedir.

Vatandaşlara sunulan sağlık hizmetlerinin omurgasını oluşturan uygulama grubu <Çalışmanın Yapıldığı Kurum> bünyesinde 2007 yılında hayata geçirilmiş ve güncellenmesine devam edilmektedir. Sistem, sağlık hizmet kullanımına ait bilgilerin elektronik ortamda kayda alınmasını sağlayarak hak sahiplerinin sunulan hizmetlerden iyi bir şekilde yararlanmasını ve sağlık hizmet sunucularının bütün süreçlerde kaliteli veri üretebilmesini sağlamıştır. Ayrıca sağlık kuruluşlarına yapılacak ödeme işlemleri daha doğru, hızlı ve etkin hale getirilmiştir. Bunların yanı sıra, kapsamlı ve güvenilir istatistiki verilerin elde edilmesi, geleceğe yönelik doğru sağlık harcaması öngörüleri, risk analizleri ve harcama kalemlerinde değişiklik takiplerinin sağlanması da sağlık uygulama gurubu ile mümkün hale gelmiştir. Sağlık uygulama gurubu, <Uygulama1>, <Uygulama2> ve <Uygulama3> alt uygulamalarından oluşmaktadır.

# 6. RİSK ANALİZİ UYGULAMASI

Çalışmanın bu bölümünde risk analizi uygulaması yapılacaktır. Kurumun bilgi sistemleri çok büyük ve karmaşık olduğundan mevcut sistemin bir alt sistemi üzerinde risk analizi yapılacaktır. İlk olarak risk analizi için alt sistem seçimi yapılacak seçilen sistem hakkında bilgi verilecektir. İkinci olarak seçilen bu alt sistem ile ilgili literatürde kabul görmüş tehlike / risk analiz teknikleri kullanılarak analiz yapılacaktır. Risk analizi uygulaması sırasında kurum ile ilgili gizli bilgiler varsa maskelenecektir. Son olarak risk analizi yoluyla elde edilen sonuçlar değerlendirmeye tabi tutulacaktır.

## 6.1. Risk Analizi Uygulanacak Alt Sistemin Seçilmesi

Çalışmanın bu bölümünde risk analizi uygulanacak alt sistemin nasıl seçildiği anlatılacak ve sistem hakkında bilgi verilecektir.

Gerek iş sürekliliği gerek BT sürekliliği olsun başlangıç noktası bileşen değil süreçler olmalıdır. Tümevarım yöntemi ile direk sistem bileşenlerinden başlayarak yola çıkmak büyük sistemler için doğru değildir. İş sürekliğini amaçlayan bir noktadan başlayan ve daha sonra süreç, faaliyet, uygulama, yazılım ve donanım şeklinde detaya inen tümdengelim yaklaşımı ile iş sürekliliğine başlamak çoğunlukla daha doğru bir yaklaşımdır. Ancak hem kurum ve kuruluşların süreçlerini düzgün bir şekilde ortaya çıkarmamış olmaları hem de süreçler ile süreç BT bileşenleri arasındaki ilişkileri tespit etmemeleri sebebiyle bu yöntem mümkün olmamaktadır. Orta Doğu Teknik Üniversitesi tarafından yayınlanan bir makalede, BT kapsamındaki risk analizlerinde sadece donanımlara ve yazılımlara odaklanıldığında yönetimsel birçok riskin göz ardı edildiği ifade edilmiştir. Süreç modeli kullanılarak nasıl risk analizi yapılabileceği konusunda bir öneri getirilmiştir. Önerilen metotta, bilgi güvenliği yönetim sistemi (BGYS) kapsamının belirlenmesinin ardından, varlık envanterine geçilmeden önce bu kapsam içerisinde yer alan süreçlerin ortaya konulması ve modellenmesi önerilmektedir. Süreçlerin belirlenmesi ve yazılı hale getirilmesi varlıkların daha sağlıklı ve eksiksiz bir şekilde belirlenmesini de sağlayacağı ifade edilmiştir. Önerilen metotta sadece donanım ve yazılım gibi varlıklara odaklanmak yerine modellenmiş süreçlerden yola çıkılarak belirlenmiş olan varlıklardaki

açıklıklar ve bu açıklıklar kullanan tehditler ortaya konmaktadır (Karabacak ve Özkan, 2010).

Çalışmanın yapıldığı kurumun içe ve dışa sunmuş oldu çok sayıda bilişim hizmeti mevcuttur. Sunulan bilişim hizmetlerinin çeşitliliği ve sayıca fazla olması sebebiyle mevcut sistemin tamamına değil de iş sürekliliğini etkileyebilecek bir alt sisteme risk analizi uygulanacaktır. Daha önceki akademik çalışmalarda bezer şekilde bir kurumdaki web servisler[4] veya uygulamalar üzerinde risk analizi yapılmıştır. Akademik bir çalışmada yazar, e-iş uygulamaları için web servislerin önemli olduğu üzerinde durmuştur. Kritik görevler için birleşik web servislerinin[5] eksikliklerinin web servislerinin yedekli yapısı kurularak telafi edilebileceğini iddia etmektedir. Birleşik bir web servisin sık ve ciddi hatalarını önlemenin anahtarının, servis kalitesinin değerlendirilmesi ve uygun kalite özelliklerine sahip web servislerin seçimi olarak görülmüştür. Çalışmada, yedekli servis bileşimlerinin kalitesini değerlendirmek için dış web servislerinin kullanımı ile ilgili risk analizi yoluyla yeni bir yaklaşım önermişlerdir. Son olarak, hesap-başarı oranını, tepki süresini ve ilgili web hizmetlerinin yürütme maliyetini dikkate alan iyileştirilmiş bir seçim algoritması tanımlamışlardır (Kokash ve D'Andrea, 2007).

Çalışmanın yapıldığı kurumda 300'den fazla uygulama bulunmaktadır. Bu uygulamalar ile <Çalışmanın Yapıldığı Kurum>, iç ve dış süreçlerinin büyük bir bölümünü elektronik ortamda yürütmektedir. Kurum iç hizmetlerine yönelik uygulamalardaki kesintilerin etkisi kurum dışına sunulan hizmetlerin etkisi kadar fazla değildir. Kurum tarafından vatandaşlara sunulan hizmetlerde kesinti olduğunda bu kesintilerin maddi ve manevi etkisi daha yüksek olmaktadır. Özellikle toplumun tamamını ilgilendirmesi açısından sağlık uygulamalarındaki kesintiler, hem kuruma itibar kaybı gibi zararlar hem de vatandaşlara maddi veya manevi zararlar vermektedir.

### 6.1.1. Analitik hiyerarşi prosesi ile alt sistemin seçilmesi

Sağlık uygulamalarının <Uygulama1>, <Uygulama2> ve <Uygulama3> alt sistemleri vardır. Bu alt sistemlerin her biri <Çalışmanın Yapıldığı Kurum>'un sunmuş olduğu

[4] Yapısal açıdan bakıldığında bir web servis ile bir web uygulaması arsındaki fark web uygulamasında fazladan kullanıcı ara yüzünün olmasıdır. Bir web servis ile web uygulaması bileşenleri açısından aynıdır.
[5] Birleşik web servis birden fazla web servisin paralel ya da seri şekilde bir araya gelmesinden oluşan web servistir. Orijinal kaynakta "composit web service" şeklinde geçmektedir.

hizmetlerin elektronik süreçlerini gerçekleştirmektedir. <Uygulama1> uygulaması ile sağlık sigortacılığı hak sahiplerinin ilaç temini ve reçete işlemlerine ilişkin elektronik süreçler yürütülmektedir. <Uygulama1> uygulaması eczane ve ilaç temini yapan kurum ve kuruluşlar tarafından kullanılmaktadır. İlaç temini yapan eczacılardan kurum ile protokol yapmış olanlara <Çalışmanın Yapıldığı Kurum> tarafından sisteme giriş amacıyla kullanıcı adı ve şifre verilir. <Uygulama2> uygulaması ile sağlık sigortacılığı hak sahiplerinin sağlık teşhis ve tedavilerine ilişkin elektronik süreçler yürütülmektedir. <Uygulama2> uygulamasını çoğunlukla sağlık sunucuları ve merkezindeki kurum personeli kullanmaktadır. Kamu sağlık sunucularına ek olarak kurum ile anlaşma yapmış özel sağlık sunucuları ve üniversite hastanelerine de <Uygulama2> uygulamasını kullanmaları amacıyla sistem kullanıcı adı ve şifre verilmektedir. <Uygulama3> uygulaması ile sağlık sigortacılığı hak sahiplerinin optik ortez ve protez teminine ilişkin elektronik süreçler yürütülmektedir. Hekim tarafından gözlük camı ve çerçeve reçeteleri yazılmış olan sağlık hak sahipleri kurum ile anlaşmalı optisyenlere gittiklerinde <Uygulama3> uygulaması üzerinden işlemleri yürütülmektedir.

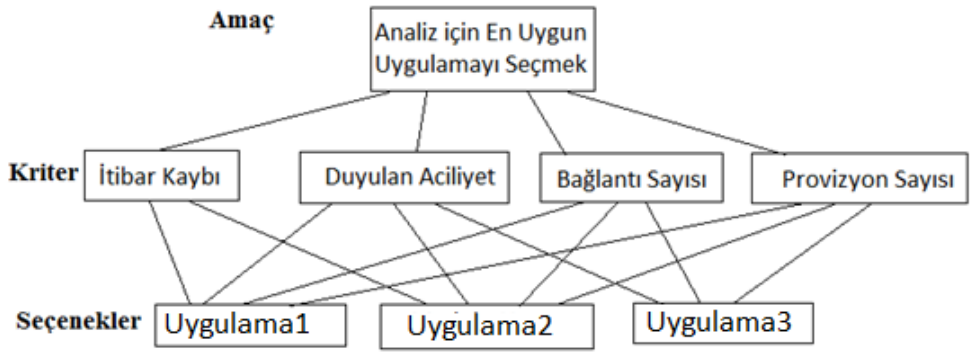
Risk analizi uygulaması yapılması amacıyla <Uygulama1>, <Uygulama2> ve <Uygulama3> uygulamalarından birinin seçilmesi gerekmektedir. Uygulama seçimi sırasında dört belirgin değerlendirme kriteri ortaya çıkmaktadır. Bunlar; kesinti olduğunda kaybedilecek itibar, sağlık hak sahibinin uygulama tarafından yapılacak işleme duyduğu aciliyet, uygulamalara bağlanan çevrimiçi sağlık sunucu sayısı ve uygulama üzerinden gerçekleştirilen provizyon sayısıdır. Sağlık uygulamalarındaki iş sürekliliği kesintileri <Çalışmanın Yapıldığı Kurum>'a para gibi maddi kayıplar yaşatmadığından maddi kayıplar değerlendirme kriteri olarak ele alınmayacaktır. Uzman bakış açısı ve tecrübelerle <Uygulama3> uygulamasının en son sırada yer aldığı görülebiliyor. Ancak <Uygulama1> ve <Uygulama2> uygulamalarının her ikisi de hem itibar kaybı hem aciliyet hem de provizyon sayısı açısından birbirlerine yakındırlar.

Risk analizi yapmak üzere sağlık uygulamalarından birinin seçilmesi gerekmektedir. Rastgele bir uygulama seçmek yerine karar vermek için bilimsel bir yol izlenecektir. Bu kapsamda uygulamalar arasından risk analizi için en uygun olanı seçmek üzere analitik hiyerarşik süreci (AHP) kullanılacaktır.

AHP hakkında kısaca bilgi vermek gerekmektedir. AHP, ilk olarak 1968 de ortaya atılmış olup 1977den itibaren çoklu kriterlere dayalı karar verme süreçlerinde kullanılmaktadır. AHP önceden tanımlanmış bir karar skalası kullanır.

AHP sürecinde ilk olarak problem tanımlanır. Problem belirlenirken değerlendirmeye tabi tutulacak karar noktaları ve karar vermek için değerlendirme kriterleri belirlenir. İkinci olarak karşılaştırma matrisleri oluşturularak önem dağılımları belirlenir. Sütun vektörleri bir araya getirilerek matris oluşturulur. Sütun vektörleri ile değerlendirme kriterlerinin ağırlık değerleri çarpılarak sonuca ulaşılır.

AHP sürecini modellenecek olursa; en iyi uygulamanın seçilmesine karar vermek hedeftir. İtibar kaybı, uygulamaya duyulan aciliyet, uygulamaya anlık bağlantı yapan sunucu sayısı ve uygulama üzerinden alınan provizyon sayısı değerlendirme kriterleridir. <Uygulama1>, <Uygulama2> ve <Uygulama3> uygulamaları ise karar verilecek seçeneklerdir. En uygun uygulamanın seçimi için AHP modellemesi Şekil 6.1'de gösterilmiştir.




Şekil 6.1. En Uygun Uygulama Seçimi için Analitik Hiyerarşi Süreci

Alternatifin karşılaştırılması için makul bir zemin oluşturması amacıyla oluşturulan standart tercih tablosu Çizelge 6.1'de gösterilmiştir (Saaty, 1990: 54).

Çizelge 6.1. Standart Tercih Tablosu-Önem Skalası

| Önem Değerleri | Değer Tanımları |
|---|---|
| 1 | Eşit Önemde |
| 3 | Biraz Daha Önemli (Az Üstünlük) |
| 5 | Oldukça Önemli (Fazla Üstünlük) |
| 7 | Çok Önemli (Çok Üstünlük) |
| 9 | Son Derece Önemli (Kesin Üstünlük) |
| 2,4,6,8 | Ara Değerler (Uzlaşma Değerleri) |

Matrislerin oluşturulmasında ilgili uzmanların görüşleri alınmıştır. Ayrıca iki kriter için uygulamaların sayısal değerlere sahip olması da karşılaştırma matrislerinin oluşturulmasında kolaylık sağlamıştır. Bu nedenle tutarsızlık oranları çok düşük çıkmıştır. Önem skalası kullanılarak ilk olarak itibar kaybı, aciliyet, çevrimiçi bağlantılı sağlık sunucu sayısı ve provizyon sayısı kriterlerine göre uygulama karşılaştırma matrisleri oluşturulmuştur. En alt satırlarda her sütunun aldığı değerlerin toplamı gösterilmiştir. Çizelge 6.2'de itibar kaybı açısından uygulama karşılaştırma matrisi, Çizelge 6.3'te aciliyet açısından uygulama karşılaştırma matrisi, Çizelge 6.4'te online bağlantılı sağlık sunucu sayısı açısından uygulama karşılaştırma matrisi ve Çizelge 6.5'te provizyon sayısı açısından uygulama karşılaştırma matrisi gösterilmiştir. Tutarsızlık oranı hesaplamaları ayrıca yapılmış ve her tablonun altına eklenmiştir.

Çizelge 6.2. İtibar Kaybı Açısından Uygulama Karşılaştırma Matrisi

| | **Kriter 1: İtibar Kaybı** | | |
|---|---|---|---|
| **Uygulamalar** | <Uygulama1> | <Uygulama2> | <Uygulama3> |
| <Uygulama1> | 1 | 1/4 | 2 |
| <Uygulama2> | 4 | 1 | 6 |
| <Uygulama3> | 1/2 | 1/6 | 1 |
| Toplam | 11/2 | 34/24 | 9 |
| Tutarsızlık Oranı: %1 | | | |

Çizelge 6.3. Aciliyet Açısından Uygulama Karşılaştırma Matrisi

| | **Kriter 2: Aciliyet** | | |
|---|---|---|---|
| **Uygulamalar** | <Uygulama1> | <Uygulama2> | <Uygulama3> |
| <Uygulama1> | 1 | 1/5 | 3 |
| <Uygulama2> | 5 | 1 | 7 |
| <Uygulama3> | 1/3 | 1/7 | 1 |
| Toplam | 19/3 | 47/35 | 11 |
| Tutarsızlık Oranı: %6,8 | | | |

Çizelge 6.4. Bağlantılı Sunucu Sayısına Göre Uygulama Karşılaştırma Matrisi

| | **Kriter 3: Online Bağlantılı Sağlık Sunucu Sayısı** | | |
|---|---|---|---|
| **Uygulamalar** | <Uygulama1> | <Uygulama2> | <Uygulama3> |
| <Uygulama1> | 1 | 8 | 5 |
| <Uygulama2> | 1/8 | 1 | 1/2 |
| <Uygulama3> | 1/5 | 2 | 1 |
| Toplam | 53/40 | 11 | 13/2 |
| Tutarsızlık Oranı: %6 | | | |

Çizelge 6.5. Provizyon Sayısı Açısından Uygulama Karşılaştırma Matrisi

| | **Kriter 4: Provizyon Sayısı** | | |
|---|---|---|---|
| **Uygulamalar** | <Uygulama1> | <Uygulama2> | <Uygulama3> |
| <Uygulama1> | 1 | 1/2 | 9 |
| <Uygulama2> | 2 | 1 | 9 |
| <Uygulama3> | 1/9 | 1/9 | 1 |
| Toplam | 28/9 | 29/18 | 19 |
| Tutarsızlık Oranı: %5,6 | | | |

Karşılaştırma matrisleri oluşturulduktan sonra değerlendirme kriterleri açısından uygulamaların önem dağılımları için $S_1$, $S_2$, $S_3$ *ve* $S_4$ sütun vektörleri hesaplanmıştır. Bunun için öncelikle karşılaştırma matrisinin sütunlarındaki değerler sütun toplamlarına bölünmüş, satır toplamları bulunmuş ve bu değerlerin aritmetik ortalamaları alınarak $S_1$, $S_2$, $S_3$ *ve* $S_4$ sütun vektörünün elemanları elde edilmiştir. Çizelge 6.6'da $S_1$ sütun vektörünün

elemanları ve hesaplanması, Çizelge 6.7'de $S_2$ sütun vektörünün elemanları ve hesaplanması, çizelge 6.8'de $S_3$ sütun vektörünün elemanları ve hesaplanması ile çizelge 6.9'da $S_4$ sütun vektörünün elemanları ve hesaplanması gösterilmiştir.

Çizelge 6.6. $S_1$ Sütun Vektörü ve Hesaplama Tablosu

| | **Kriter 1: İtibar Kaybı** | | | | $S_1$ |
|---|---|---|---|---|---|
| **Uygulamalar** | <Uygulama1> | <Uygulama2> | <Uygulama3> | Satır Top | Satır Ort |
| <Uygulama1> | 2/11=0,1818 | 3/17=0,1764 | 2/9=0,2222 | 0,5804 | 0,1935 |
| <Uygulama2> | 8/11=0,7272 | 12/17=0,7060 | 6/9=0,6667 | 2,0996 | 0,6999 |
| <Uygulama3> | 1/11=0,0910 | 2/17=0,1176 | 1/9=0,1111 | 0,3196 | 0,1066 |

Çizelge 6.7. $S_2$ Sütun Vektörü ve Hesaplama Tablosu

| | **Kriter 2: Aciliyet** | | | | $S_2$ |
|---|---|---|---|---|---|
| **Uygulamalar** | <Uygulama1> | <Uygulama2> | <Uygulama3> | Satır Top | Satır Ort |
| <Uygulama1> | 3/19=0,1580 | 7/47=0,1490 | 3/11=0,2727 | 0,5797 | 0,1932 |
| <Uygulama2> | 15/19=0,7894 | 35/47=0,7447 | 7/11=0,6364 | 2,1705 | 0,7235 |
| <Uygulama3> | 1/19=0,0526 | 5/47=0,1063 | 1/11=0,0909 | 0,2498 | 0,0833 |

Çizelge 6.8. $S_3$ Sütun Vektörü ve Hesaplama Tablosu

| | **Kriter 3: Online Bağlantılı Sağlık Sunucu Sayısı** | | | | $S_3$ |
|---|---|---|---|---|---|
| **Uygulamalar** | <Uygulama1> | <Uygulama2> | <Uygulama3> | Satır Top | Satır Ort |
| <Uygulama1> | 40/53=0,7547 | 8/11=0,7272 | 10/13=0,7692 | 2,2511 | 0,7503 |
| <Uygulama2> | 5/53=0,0943 | 1/11=0,0909 | 1/13=0,0769 | 0,2621 | 0,0874 |
| <Uygulama3> | 8/53=0,1510 | 2/11=0,1819 | 2/13=0,1539 | 0,4868 | 0,1623 |

Çizelge 6.9. $S_4$ Sütun Vektörü ve Hesaplama Tablosu

| | **Kriter 4: Provizyon Sayısı** | | | | $S_4$ |
|---|---|---|---|---|---|
| **Uygulamalar** | <Uygulama1> | <Uygulama2> | <Uygulama3> | Satır Top | Satır Ort |
| <Uygulama1> | 9/28=0,3214 | 9/29=0,3104 | 9/19=0,4737 | 1,1055 | 0,3685 |
| <Uygulama2> | 18/28=0,6429 | 18/29=0,6207 | 9/19=0,4737 | 1,7373 | 0,5791 |
| <Uygulama3> | 1/28=0,0357 | 2/29=0,0689 | 1/19=0,0526 | 0,1572 | 0,0524 |

$S_1$, $S_2$, $S_3$ *ve* $S_4$ sütun vektörleri hesaplandıktan sonra *w* vektörü ile çarpılması amacıyla matris haline getirilmiştir. Çizelge 6.10'da sütun vektörlerinin bir araya getirilmesiyle oluşturulan matris gösterilmektedir. Tablonun satırlarında uygulamalar ve sütunlarında ise değerlendirme kriterleri verilmiştir. Satır ile sütunun kesişimindeki hücrede ise her bir uygulama için değerlendirme kriterlerinin hesaplanması sonucunda ulaşılan değerler verilmiştir.

Çizelge 6.10. Sütun Vektörlerinin Matris Görünümü

| | **Kriterler** | | | |
|---|---|---|---|---|
| **Uygulamalar** | İtibar Kaybı | Aciliyet | Online Bağlantılı S.Sunucu Sayısı | Provizyon Sayısı |
| <Uygulama1> | 0,1935 | 0,1932 | 0,7503 | 0,3685 |
| <Uygulama2> | 0,6999 | 0,7235 | 0,0874 | 0,5791 |
| <Uygulama3> | 0,1066 | 0,0833 | 0,1623 | 0,0524 |

İtibar kaybı, aciliyet, online bağlantılı sağlık sunucu sayısı ve provizyon sayısı değerlendirme kriterlerinin ağırlıkları eşit değildir. Değerlendirme kriterlerinin ağırlıklarının hesaplanması amacıyla, $w_1$, $w_2$, $w_3$, $w_4$ ağırlıklarının hesaplanıp *w* vektörünün bulunması gerekmektedir. *w* öncelik (ağırlık) vektörünü hesaplamak için ilk olarak Çizelge 6.11'de gösterildiği gibi değerlendirme kriterlerinin karşılaştırma matrisi oluşturulmuştur.

Çizelge 6.11. Değerlendirme Kriterleri Karşılaştırma Matrisi

| **Kriterler** | İtibar Kaybı | Aciliyet | Online Bağlantılı Sunucu Sayısı | Provizyon Sayısı |
|---|---|---|---|---|
| İtibar Kaybı | 1 | 1/2 | 5 | 5 |
| Aciliyet | 2 | 1 | 5 | 5 |
| Online Bağlantılı Sunucu Sayısı | 1/5 | 1/5 | 1 | 1 |
| Provizyon Sayısı | 1/5 | 1/5 | 1 | 1 |
| Toplam | 17/5 | 19/10 | 12 | 12 |
| Tutarsızlık Oranı: %2,2 | | | | |

Değerlendirme kriterlerinin öncelik (ağırlık) vektörleri hesaplanmıştır. Bunun için öncelikle karşılaştırma matrisinin sütunlarındaki değerler sütun toplamlarına bölünmüş, satır toplamları bulunmuş ve bu değerlerin aritmetik ortalamaları alınarak $w_1, w_2, w_3$ *ve* $w_4$ ağırlık değerleri hesaplanmıştır. Hesaplamaların nasıl yapıldığı ve bulunan *w* vektörü Çizelge 6.12'de gösterilmiştir.

Çizelge 6.12. Değerlendirme Kriterleri Ağırlık Vektörü ve Hesaplama Tablosu

| **Kriterler** | İtibar Kaybı | Aciliyet | Online Bağlantılı Sunucu Sayısı | Provizyon Sayısı | *w* vektörü |
|---|---|---|---|---|---|
| İtibar Kaybı | 5/17=0,2941 | 5/19=0,2631 | 5/12=0,4167 | 5/12=0,4167 | 0,3476 |
| Aciliyet | 10/17=0,5883 | 10/19=0,5263 | 5/12=0,4167 | 5/12=0,4167 | 0,4870 |
| Online Bağlantılı Sunucu Sayısı | 1/17=0,0588 | 2/19=0,1053 | 1/12=0,0833 | 1/12=0,0833 | 0,0827 |
| Provizyon Sayısı | 1/17=0,0588 | 2/19=0,1053 | 1/12=0,0833 | 1/12=0,0833 | 0,0827 |

Son olarak her bir değerlendirme kriteri ve uygulama için hesaplanan *S* sütun vektörleri matris formatında bir araya getirilmiş ve *w* ağırlık vektörü ile çarpılmıştır. Şekil 6.13'te sütun vektörleri ile *w* öncelik vektörünün çarpma işlemleri gösterilmiştir.

Çizelge 6.13. Sütun Vektörleri ile Öncelik Vektörünün Çarpılması

| | **Kriterler** | | | | |
|---|---|---|---|---|---|
| **Uygulamalar** | İtibar Kaybı | Aciliyet | Online Bağlantılı Sunucu Sayısı | Provizyon Sayısı | Toplam |
| <Uygulama1> | 0,1935x0,3476 | 0,1932x0,4870 | 0,7503x0,0827 | 0,3685x0,0827 | =0,25387376 |
| <Uygulama2> | 0,6999x0,3476 | 0,7235x0,4870 | 0,0874x0,0827 | 0,5791x0,0827 | =0,65074929 |
| <Uygulama3> | 0,1066x0,3476 | 0,0833x0,4870 | 0,1623x0,0827 | 0,0524x0,0827 | =0,09537695 |

Analitik hiyerarşi prosesinin uygulanması ile sağlık uygulamalarının hangisi için risk analizi yapılması gerektiği kararına varılmıştır. Uygulamalar ve alınan puanlar Çizelge 6.14'te gösterilmiştir. <Uygulama2> uygulaması 0,6507 (%65.07) puan ile belirgin farkla ön plana çıkmıştır. Çıkan sonuca göre risk analizi çalışması <Uygulama2> uygulaması ve bileşenleri üzerinde gerçekleştirilecektir.

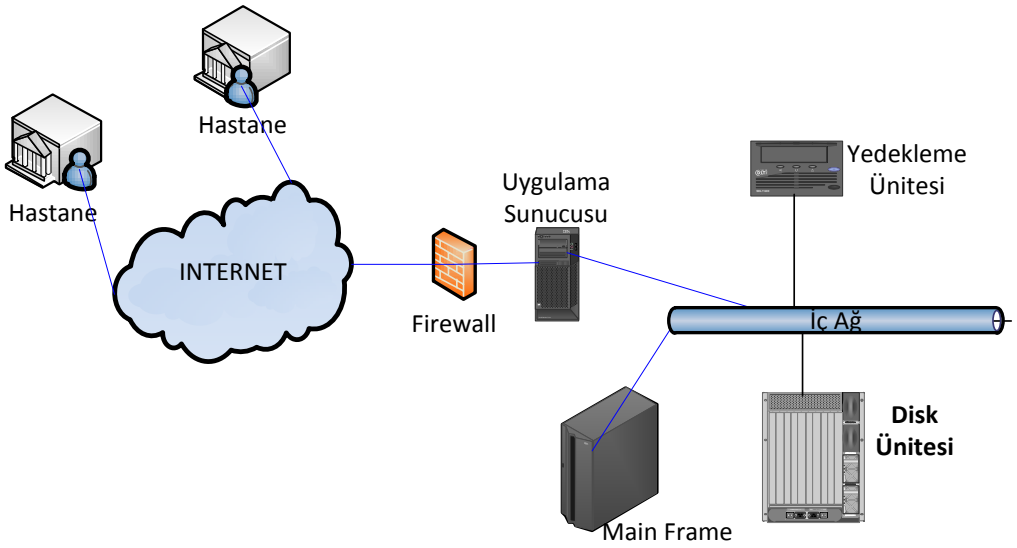
Çizelge 6.14. Uygulama Puanları

| Uygulamalar | Puan | |
|---|---|---|
| <Uygulama1> | 0,2537 | %25.38 |
| <Uygulama2> | 0,6507 | %65.07 |
| <Uygulama3> | 0,0952 | %09.53 |

### 6.1.2. Risk analizi uygulanacak alt sistemin özellikleri

Risk analizi yapılmak üzere sağlık uygulamaları AHP ile değerlendirmeye tabi tutulduğunda en uygun uygulama <Uygulama2> uygulaması çıkmıştır. Çalışmanın bu bölümünde <Uygulama2> uygulaması hakkında tehlike / risk analizinde kullanılan bazı yapısal ve fonksiyonel bilgiler verilecektir.

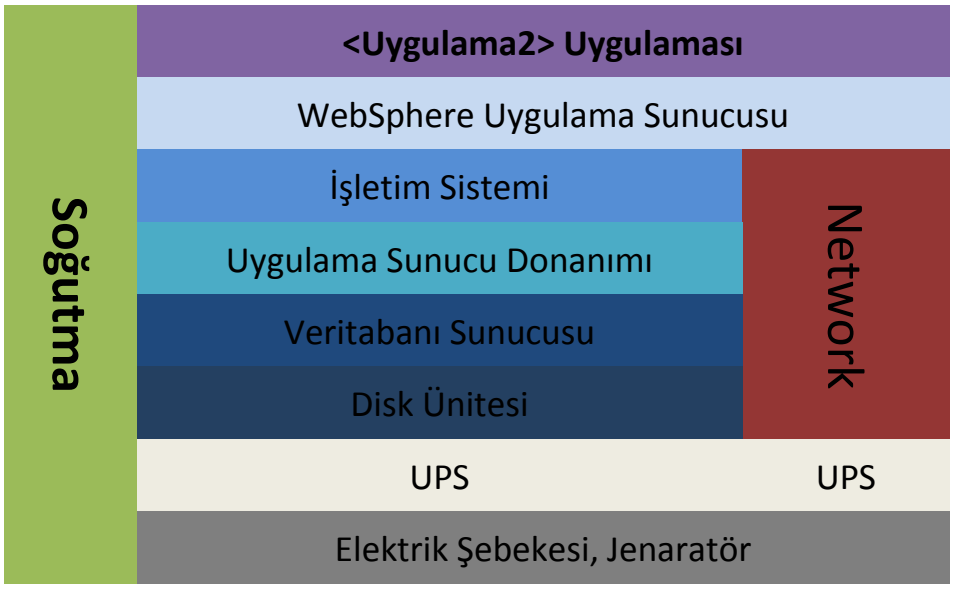
<Uygulama2> uygulamasının kendisi, uygulama sunucusu, sunucu üzerinde çalışan işletim sistemi, sunucu donanımı, ağ bileşeni ve veritabanı; risk analizi uygulanacak sistem[6] olarak ele alınacaktır. Şekil 6.2'de risk analizi uygulanacak sisteminin topolojik görünümü ve sistem bileşenleri gösterilmiştir.




Şekil 6.2. <Uygulama2> Sistem Topolojisi

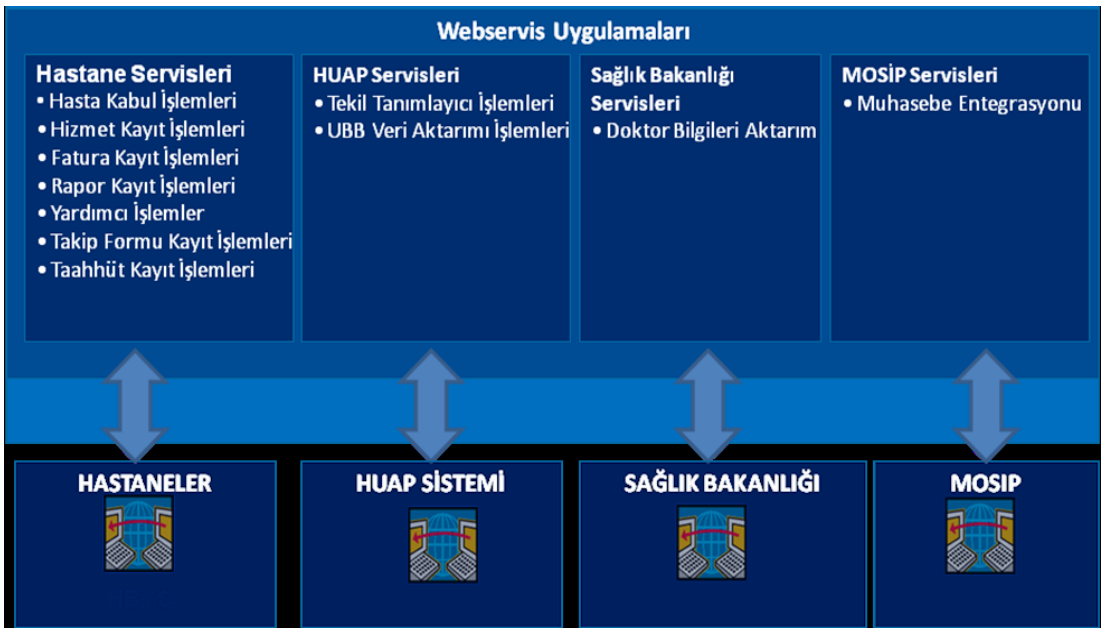
<Uygulama2> sisteminin mimarisi Şekil 6.3'te gösterilmiştir.

[6] Tanımı yapılan sistem <Çalışmanın Yapıldığı Kurumun> bilişim sistemlerinin bir alt kümesidir.




Şekil 6.3. <Uygulama2> Sisteminin Mimarisi

Şekil 6.4'te <Uygulama2> uygulamasının diğer web servislerle entegrasyonu gösterilmiştir. Şekil 6.5'te ise <Uygulama2> uygulamasının diğer web uygulama bileşenleri gösterilmiştir.



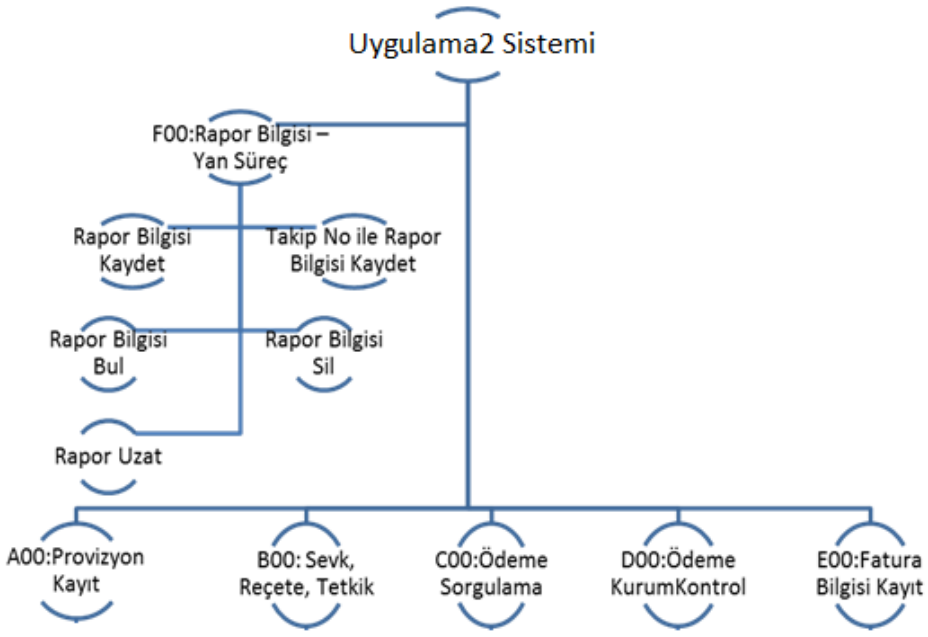

Şekil 6.4. <Uygulama2> Sisteminin Sunduğu Web Servis Şeması




Şekil 6.5. <Uygulama2> Sisteminin Sunduğu Uygulama Şeması

Şekil 6.6'da risk analizi yapılacak olan uygulamanın fonksiyonel görünümü gösterilmiştir.

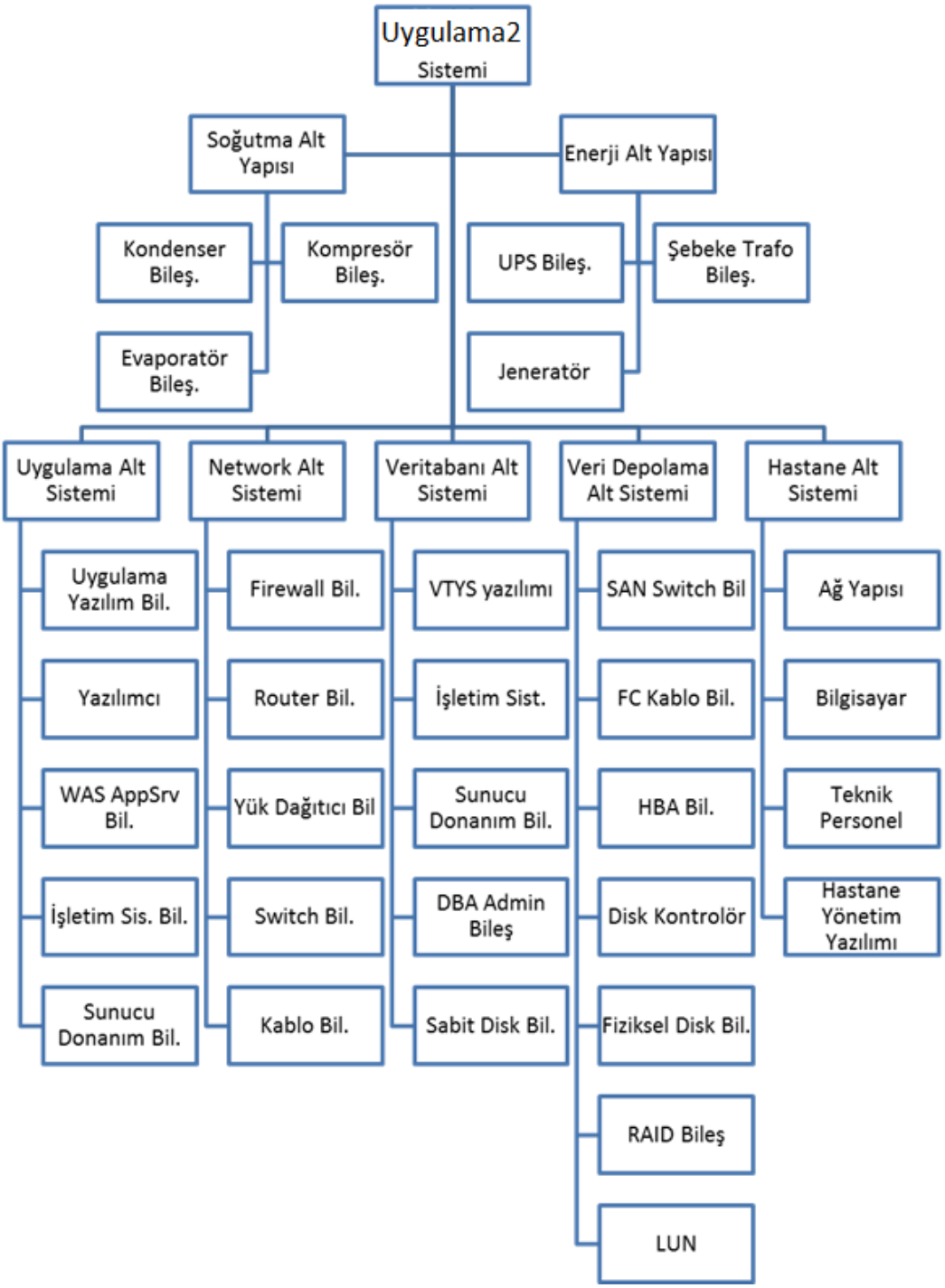
Bu bilgiler Fonksiyonel HTEA yapılabileceğini göstermek üzere verilmiştir.




Şekil 6.6. <Uygulama2> Sistemi Fonksiyonel Görünümü

Şekil 6.7' de risk analizi yapılacak olan uygulamanın yapısal görünümü gösterilmiştir. Bu yapısal görünüm birçok web uygulamasında birbirine benzemektedir. Kuruma özel olan

bileşen marka, model, yapılandırma bilgileri vb. gizliliğinden ve gerek duyulmadığından verilmemiştir.




Şekil 6.7. <Uygulama2> Sistemi Yapısal Görünümü

## 6.2. Risk Analizi Uygulaması

Çalışmanın bu bölümünde, kabul görmüş analiz teknikleri kullanılarak seçilen alt sistem için risk analizi yapılacaktır. Risk analizi tekniklerinden sadece birini uygulayarak sistemdeki tüm riskleri ortaya çıkarmak mümkün değildir. Akademik bir çalışmada küçük organizasyonlar için bile tam bir risk modelinin aşırı derecede kompleks olduğu ve bu yüzden keşfedilmemiş bazı zayıflıkların her zaman olabileceğini ifade etmiştir. Bir organizasyonun risk analizi gereksinimlerinin tamamının karşılanması tek bir metotla mümkün değildir (Zibigniew ve Ciechanowic, 1997).

Çalışmanın önceki bölümlerinde ifade edildiği gibi risk, bir olayın şiddeti ve olasılığının çarpımıdır. Çalışma kapsamında gerçekleştirilen analiz çalışmasında nitel yöntemlerle olasılık ve şiddet skalalar şeklinde ifade edilmiştir. Çalışma kapsamında gerçekleştirilen risk analizi çalışmasının başarısını arttırmak için çeşitli yöntemlerin entegre bir şekilde uygulanması gerekmektedir. Çalışma kapsamında gerçekleştirilen risk analizinde tehlikelerin olasılıklarını belirleyebilmek için kullanılan göstergeler Çizelge 6.15'te verilmiştir.

Çizelge 6.15. Risk Analizi Olasılık Ölçeği

| Olasılık İfadesi | Frekans | Derecesi |
|---|---|---|
| Çok Yüksek: Hata hali hazırda gerçekleşmiş olabilir. | Saatte 1 kez | 10 |
| | Günde 1 kez | 9 |
| Yüksek: Kısa sürede hata tekrar eder. | Haftada 1 kez | 8 |
| | Ayda 1 kez | 7 |
| Orta: Hata orta ya da uzun sürede tekrar eder. | Yılda 1 kez | 6 |
| | 3 Yılda 1 kez | 5 |
| | 5 Yılda 1 kez | 4 |
| Düşük: Hata ancak uzun süre sonra tekrar eder. | 10 Yılda 1 kez | 3 |
| | 15 Yılda 1 kez | 2 |
| Uzak ihtimal: Hatanın oluşmayacağı varsayılır. | 20+ Yılda 1 kez | 1 |

Eğer bir olay, ortalama saate bir kez meydana gelecekse olma olasılığı çok yüksek olarak kabul edilmiştir. Meydana gelme ihtimali en yüksek olan olayların derecesi tabloya göre

“10” olarak verilmiştir. Eğer bir olay, yirmi yılda bir kez meydana gelecekse olma olasılığı uzak ihtimal olarak kabul edilmiştir. Meydana gelme ihtimali en düşük olan olayların derecesi tabloya göre “1” olarak verilmiştir. Çalışma kapsamında gerçekleştirilen risk analizinde tehlikelerin etkilerini belirleyebilmek için kullanılan etki değerleri Çizelge 6.16’da verilmiştir (IsecT, 2015).

Çizelge 6.16. Risk Analizi Şiddet Tablosu

| Etki | Etkinin Ciddiyeti | Derecesi |
|---|---|---|
| **Felaket** | Uygulama uzun süre hizmet veremez ve veriler zarar görür. Kurum itibarı ciddi şekilde sarsılır. | **10** |
| **Aşırı Derece** | Veriler zarar görür ve hizmet bir süre aksar. Kurum itibarı ciddi şekilde sarsılır. | **9** |
| **Çok Yüksek** | Veriler zarar görür uygulama hizmeti kısa süre aksar. Kurum itibarı ciddi şekilde sarsılır. | **8** |
| **Yüksek** | Veriler zarar görmez ancak uygulama hizmeti uzun süre aksar. Kurum itibarı ciddi şekilde sarsılır. | **7** |
| **Orta** | Veriler zarar görmez ancak uygulama hizmeti bir süre aksar. Kurum itibarı sarsılır. | **6** |
| **Düşük** | Veriler zarar görmez ancak uygulama hizmeti kısa bir süre aksar. Kurum itibarı sarsılır. | **5** |
| **Çok Düşük** | Veriler zarar görmez ancak uygulama hizmeti uzun süre yavaşlar. Kurum itibarı sarsılır. | **4** |
| **Önemsiz** | Veriler zarar görmez ve uygulama hizmeti kısa süre yavaşlar. Kurum itibarı sarsılabilir. | **3** |
| **Neredeyse Yok** | Uygulama hizmeti kısa süreli performans kaybı hariç devam eder. Kısmen hissedilebilir. | **2** |
| **Yok** | Uygulama hizmeti planlanan şekilde devam eder. | **1** |

Kullanılan olasılık ve şiddet tabloları uzman görüşü alınarak oluşturulmuştur. Eğer bir olay meydana geldiğinde uygulama planlandığı şekilde çalışmasına devam ediyorsa etkisinin olmadığı düşünülür ve etkinin ciddiyetine en düşük derece olan “1” verilir. Eğer olay oluştuğunda uygulama uzun süre hizmet veremez, veriler zarar görür ve kurum itibarı ciddi şekilde sarsılırsa bu olayın etkisinin felaket olduğu söylenir. Felaket olayının etkisinin ciddiyeti tabloya göre “10” olarak verilmiştir. Tehlikeler belirlendikten sonra ekipte bulunan kişilere söz konusu tablolar verilerek her bir tehlike için olasılık ve şiddet değerleri belirlenmiştir.

### 6.2.1. Ön tehlike listesi ve üst seviye aksilikler

İlk olarak <Uygulama2> sisteminin ÖTL ile üst seviye aksilikleri belirlenmiştir. Çalışmada kontrol listesi olarak ISO / IEC 27005 Bilgi Güvenliği Risk Yönetimi standardının Ek-C bölümünde yer alan örnek tehditler listesinden faydalanılmıştır (ISO, 2008). Çizelge 6.17'de Risk yönetimi standardından alınmış tehditlerin listesi gösterilmiştir.

Çizelge 6.17. Tipik Bilgi Güvenliği Tehditleri

| Tip | Tehdit |
|---|---|
| Fiziksel Hasar | Yangın<br>Sıvı ile temas<br>Kirlenme<br>Büyük kaza<br>Ekipman ya da cihazların tahribatı<br>Kir, korozyon donma |
| Doğa Olayları | İklim olayları, Sismik olaylar, Volkanik olaylar<br>Meteorolojik olaylar, Sel |
| Temel hizmetlerin kaybı | Klima veya su temin sistemi arızası<br>Güç kaynağı kaybı<br>İletişim ve haberleşme arızaları |
| Radyasyon dolayısı ile bozulmalar | Elektromanyetik radyasyon,<br>Termal radyasyon<br>Elektromanyetik şiddetli darbeler |
| Bilginin Yanlış Kişilerce Ele Geçirilmesi | Sinyallerin kesişme tehlikesi<br>Uzaktan casusluk, Dinleme<br>Medya veya belgelerin hırsızlığı<br>Ekipman hırsızlığı<br>Atılan medyadan bilgiyi geri elde etme<br>Bilgi sızdıran açıklama<br>Güvenilir olmayan kaynaklardan elde edilen veriler,<br>Donanım ile oynanması<br>Yazılım ile oynanması<br>Pozisyon algılama |
| Teknik arızalar | Ekipman arızası<br>Ekipman aksaklığı<br>Bilgi sisteminin doygunluğu<br>Yazılımın kusurlu çalışması<br>Bilgi sistemlerinin bakımının ihmali |
| Yetkisiz İşlemler | İzinsiz ekipmanın kullanımı<br>Hileli yazılım kopyalama<br>Sahte veya kopyalanmış yazılım kullanımı<br>Verilerin bozulması<br>Yasadışı verilerin işlenmesi |
| Fonksiyonların ele geçirilmesi | Kullanımdaki hatalar<br>Hakların kötüye kullanımı<br>Hakların taklidi<br>İşlemlerin reddi<br>Personele erişememe durumu |

Bu tehdit listesi ve edinilmiş tecrübelerden yararlanılarak analiz yapılacak olan sistemle ilgili ön tehlike listesi elde edilmiştir. Çizelge 6.18'de elde edilen ön tehlikeler gösterilmiştir.

Çizelge 6.18. Ön Tehlike Listesi

| **Ön Tehlike Listesi Analizi** | | | | |
|---|---|---|---|---|
| **No** | **Bileşen** | **Tehlike** | **Etkileri** | **Öneriler** |
| 1 | Klima | Yüksek basınçlı akışkandan dolayı klimanın soğutma yapamaması | Veri merkezinin ısınması ve uygulamanın yavaşlaması | Yok |
| | | Klimanın iç ve dış bölümlerinin toz ve kirden dolayı tıkanması. | Veri merkezinin ısınması ve uygulamanın yavaşlaması | Yok |
| | | Klima sisteminde hava akışının olmaması. | Veri merkezinin ısınması ve uygulamanın yavaşlaması | Yok |
| | | Klimanın sürekli çalışması | Gereksiz yere soğutma ve ısıtma yaparak bozulması. | Yok |
| | | Klima motorunun mekanik arızalanması | Veri merkezinin ısınması ve uygulamanın yavaşlaması ya da durması | Yok |
| 2 | Güç bileşeni | Enerji biriminden güç çıkışının olmaması | Sisteme güç gitmez ve uygulama hizmet veremez. | Yok |
| | | Beklenmedik elektrik kesintileri | Sisteme güç gitmez ve uygulama kapanır. | Yok |
| | | Güç biriminden gelen düşük ya da dalgalı gerilim | Sistem bileşenleri arızalanır. | Yok |
| | | Yanlış şalterin kapatılması | Sistemde güç kesintisi olur ve sunucular zarar görür. | Yok |
| 3 | Uygulama Yazılımı | Metotlar / Fonksiyonlar başlamaz | Uygulama başlamaz | Yok |
| | | Metotlar / Fonksiyonlar çalışmaz | Uygulama çalışmaz | Yok |
| | | Metot/fonksiyon gecikmeli çalışır | Uygulama yavaşlar | Yok |
| | | Metotlar yanlış çalışır | Uygulama yanlış sonuç verir. | Yok |
| | | Metotların kırılması, beklenmedik şekilde sonlanması | Uygulama sürekliliği kaybolur. | Yok |
| 4 | Personel | Hastalanma | Problemler zamanında giderilemez. | Yok |
| | | İşe geç gelme | Bazı sorunlara vaktinde müdahale edilemez. | Yok |
| | | Yanlış işlem ya da operasyon gerçekleştirme | Uygulama hata verir veya kapanır. | |

Çizelge 6.18. (devam) Ön Tehlike Listesi

| | | | | |
|---|---|---|---|---|
| 4 | Personel (devam) | İşten ayrılma | Bazı sorunlara vaktinde müdahale edememe veya iş planlarının aksaması. | Yok |
| 5 | İşletim Sistemi | Sunucuya virüs bulaşması | Uygulama yavaşlar ya da çalışmaz | Yok |
| | | Sunucunun çökmesi | Uygulama çalışmaz | Yok |
| | | Yanlış yapılandırılma | Sunucu çalışmaz | Yok |
| | | Bellek Hatası | Sunucu hata verir | Yok |
| 6 | Sunucu Donanımı | Sunucu bileşenlerinin fiziksel arızalanması | Uygulama yavaşlar ya da çalışmaz | Yok |
| | | Sunucunun zamanla yavaşlaması | Uygulama yavaşlar | Yok |
| | | Bellek hatası | Sunucu hata verir | Yok |
| 7 | Ağ cihazları | Fiziksel arıza sonucunda ağ bağlantısı kesilmesi | Uygulamanın erişilebilirliği kaybolur. | Yok |
| | | Ağ cihazlarını yanlış yapılandırılma | Uygulamanın erişilebilirliği kaybolur. | Yok |
| | | Ağ cihazlarının zamanla yavaşlaması | Uygulamaya erişim yavaşlar. | Yok |
| | | Ağ cihazlarının başarısız firmware yükseltmesi | Uygulamanın erişilebilirliği kaybolur. | Yok |
| 8 | VTYS Yazılımı | VTYS yazılımının yavaşlaması | Uygulama yavaşlar ya da çalışmaz | Yok |
| | | VTYS yazılımının yanlış yapılandırılması | Veritabanına erişilemez ve uygulama çalışmaz | Yok |
| | | VTYS yazılımına başarısız yama yüklemesi | Uygulama yavaşlar ya da kısa süre çalışmaz | Yok |
| | | Tablonun kilitlenmesi | Uygulama yeni kayıt yapamaz | Yok |
| | | Table Space ya da diskin dolması | Uygulama yeni kayıt yapamaz | Yok |

Üst seviye aksilikler ve kritik sistem fonksiyonları Çizelge 6.19'da gösterilmiştir.

Çizelge 6.19. Üst Seviye Aksilikler ve Kritik Sistem Fonksiyonları

| **No** | **İş Sürekliliğini Aksatıcı Üst Seviye Aksilikler** | **Kritik Sistem Fonksiyonları** |
|---|---|---|
| 1. | Enerjiden kaynaklı iş sürekliliğini aksatıcı aksilikler. | Sisteme enerji sağlama süreci |
| 2. | Soğutma sisteminden kaynaklı iş sürekliliğini aksatıcı aksilikler. | Veri merkezini soğutma süreci |

Çizelge 6.19. (devam) Üst Seviye Aksilikler ve Kritik Sistem Fonksiyonları

| | | |
|---|---|---|
| 3. | Siber saldırı kaynaklı veri kaybına da sebep olan iş sürekliliğini aksatıcı aksilikler. | Güvenliği sağlama |
| 4. | Bilişim personelinin çalışma sürekliliğini aksatıcı aksilikler. | Bilişim personelinin çalışma sürekliliği |
| 5. | Bilişim personelinin yanlış işleminden kaynaklı iş sürekliliğini aksatıcı aksilikler. | Bilişim perosnelinin işlemleri yüksek doğrulukta yapması |
| 6. | Donanımsal arızalardan kaynaklı iş sürekliliğini aksatıcı aksilikler. | Sistem bakımı ve yenileme süreci |
| 7. | Değişiklik yönetimi olmamasından kaynaklı iş sürekliliğini aksatıcı aksilikler. | Değişiklik yönetim süreci |
| 8. | Konfigürasyon yönetiminin olmamasından kaynaklı iş sürekliliğini aksatıcı aksilikler. | Konfigürasyon yönetimi süreci |
| 9. | Gereksinimlerin belirlenmemesinden kaynaklı iş sürekliliğini aksatıcı aksilikler. | Gereksinim belirleme süreci |
| 10. | Tasarım ve planlama yapılmamasından kaynaklı iş sürekliliğini aksatıcı aksilikler. | Analiz ve tasarım süreci |
| 11. | Sistem ile etkileşen personelin yetersiz eğitime sahip olması. | Eğitim süreci |

### 6.2.2. <Uygulama2> sisteminin HTEA ile analizi

<Uygulama2> sisteminde risk analizi uygulamak için ön tehlike listesi analizinin yanı sıra kullanılacak ikinci teknik olarak HTEA seçilmiştir. Hem genel bir kabul görmesi hem de başarılı sonuçlar üretmesi seçilmesinde en önemli etkenlerdir.

HTEA analizi yaparken ilk olarak sistem alt sistemlere ayrılmalıdır. Daha sonra alt sistemler ise bileşenlere ayrılmıştır. Çalışma kapsamında sistem bileşenleri ve fonksiyonlarını belirlemek için sorulan sorular Çizelge 6.20'de gösterilmiştir.

Çizelge 6.20. HTEA Bileşenleri için Sorular

| **Bileşenler Belirlenirken Sorulan Sorular** |
|---|
| Bu bileşenin/fonksiyonun birincil amacı nelerdir? |
| Bu bileşenin/fonksiyonun ne yapması beklenir? |
| Bu bileşenin/fonksiyonun neler yapmaması gerekir? |
| Arayüzde hangi fonksiyonlar gerçekleşir? |
| İş sürekliliği ile ilgili hangi işlev ya da özellikler bu bileşen/fonksiyon için önemlidir? |

Çalışma kapsamında bileşenlerin hata modlarının tespit edilmesi için sorulan sorular Çizelge 6.21'de gösterilmiştir.

Çizelge 6.21. Hata Modlarını Belirlemek için Sorulan Sorular

| **Hata Modları Belirlenirken Sorulan Sorular:** |
|---|
| Bu bileşen/operasyon amaçlanan işlevinden nasıl başarısız olur? |
| Ne şekilde bu bileşen istenmeyen bir fonksiyonu gerçekleştirir? |
| Bu bileşenle ilgili ne yanlış gidebilir? |
| Arayüzle ilgili ne yanlış gidebilir? |
| Geçmişte bu bilşenle ilgili neler yolunda gitmedi? |
| Bu bileşen hangi şekilde kötüye kullanılır ya da istismar edilir? |
| Bu sistem ya da bileşenle ilgili endişen var mı? |

Risk analizi yapılırken belirlenen hata modlarının sebeplerini ortaya çıkarmak için sorulan sorular Çizelge 6.22'de gösterilmiştir.

Çizelge 6.22. Hata Modlarının Sebeplerini Belirlemek için Sorulan Sorular

| **Hata Modlarının Sebepleri Belirlenirken Sorulan Sorular** |
|---|
| Hata nasıl meydana gelebilir? |
| İşlemin başarısız olmasını ne sebep olabilir? |
| Hata neden meydana gelir? |
| Hataya sebep olabilecek materyal, yöntem veya çevresel unsur var mı? |

Risk analizi yapılırken belirlenen hata modlarının etkilerini ortaya çıkarmak için sorulan sorular Çizelge 6.23'te gösterilmiştir.

Çizelge 6.23. Hata Modlarının Etkilerini Belirlemek için Sorulan Sorular

| **Hata Modlarının Etkileri Belirlenirken Sorulan Sorular** |
|---|
| Bu hatanın Sonuçları ne olur? |
| Bu hatanın dar kapsamda ve kısa zamanda etkileri nelerdir? |
| Bu hatanın <Uygulama2> sistemi üzerindeki etkisi nedir? |
| Bu hata olursa sağlık hak sahipleri nasıl etkilenir? |
| Bu hata <Uygulama2> sisteminin diğer bileşenlerini nasıl etkiler? |

HTEA analizi yapmak için alt sistemlerin her biri analiz edilmiş ve sistem bileşenleri elde edilmiştir. Sistem bileşenlerinin her biri için Ericson (2005) tarafından önerilen ve Şekil 6.8'de gösterilen analiz formu doldurulmuştur. Her bir bileşen için potansiyel hata modu, hata modunun sebebi, etkileri ve uygulama üzerindeki etkileri belirlenmiştir. Daha sonra uzman kişilerle görüşülerek belirlenen hata modlarının olasılığı ve ciddiyeti tespit edilmiştir (Bknz. Çizelge 6.15 ve 6.16).

| **Sistem:** Medula-Hastane | | | **Alt Sistem:** | | | **Mod/Safha:** Operasyon | | | **FMEA Analizi** |
|---|---|---|---|---|---|---|---|---|---|
| **No Bileşen** | **Potansiyel Başarısızlık Modu** | **Potansiyel Etkileri** | **Uygulama Üzerindeki Etkiler** | **Ciddiyet** | **Nedensel Faktörler** | **Olasılık** | **Mevcut Kontroller** | **Risk** | **Önerilen Kontroller** |
| | | | | | | | | | |

Şekil 6.8. HTEA Analizi Yapılırken Kullanılan Form

HTEA analizi sırasında bileşenlerin başarısızlık modları elde edilmiştir. Soğutma alt sistemine ait bileşenler için elde edilen başarısızlık modları Çizelgel 6.24'te gösterilmiştir.

Çizelge 6.24. Soğutma Alt Sistemi için Başarısızlık Modları

| **Soğutma Alt Yapısı ile ilgili Başarısızlık Modları** |
|---|
| Yüksek basınçlı akışkan |
| Yoğunlaştıramama |
| Tıkanma / Tıkanıklık |
| Çalışmıyor, hava akışı yok |
| Sürekli çalışma |
| Mekanik arıza |
| Isı alışverişi yapamama |

Enerji alt sistemine ait bileşenler için elde edilen başarısızlık modları Çizelge 6.25'te gösterilmiştir.

Çizelge 6.25. Enerji Alt Sistemi için Başarısızlık Modları

| **Enerji Alt Yapısı ile ilgili Başarısızlık Modları** |
|---|
| Güç çıkışı yok |
| Elektrik kesildikten kısa süre sonra kapanması |
| Elektrik kesilir kesilmez kapanması |
| UPS devreye girmiyor. |
| UPS Şarj olmama |
| Alternatör gerilim üretmez |
| Düşük ya da dalgalı gerilim |
| Motor kısa süre sonra durur |
| Güç dalgalanması |
| Yanlış şalterin kapatılması |
| Sigorta atması |
| Elektrik iletmeme |

Uygulama yazılımına ait bileşenler için elde edilen başarısızlık modları Çizelge 6.26'da gösterilmiştir.

Çizelge 6.26. Uygulama Yazılımı için Başarısızlık Modları

| **Uygulama Yazılımı ile ilgili Başarısızlık Modları** |
|---|
| Metotlar / fonksiyonlar başlamaz |
| Güvenirliğinin kaybolması |
| Metotlar / fonksiyonlar çalışmaz |
| Metot/fonksiyonlar gecikmeli çalışır |
| Metotlar yanlış çalışır |
| Metotların kırılması, beklenmedik şekilde sonlanması |

Bilişim personeline elde edilen başarısızlık modları Çizelge 6.27'de gösterilmiştir.

Çizelge 6.27. Bilişim Personeli için Başarısızlık Modları

| **Bilişim Personeli ile ilgili Başarısızlık Modları** |
|---|
| Hastalanma |
| İşe geç gelme |
| İşten ayrılma |
| Yanlış kod yazma |

Sunucu donanımı için elde edilen başarısızlık modları Çizelge 6.28'de gösterilmiştir.

Çizelge 6.28. Sunucu Donanımı için Başarısızlık Modları

| **Sunucu Donanımı ile ilgili Başarısızlık Modları** |
|---|
| Fiziksel arıza |
| Yavaşlama |
| Çalışmama |
| Bellek hatası |
| Kaynak çakışması |
| Kesme isteği çakışması |

Ağ alt sistemine ait bileşenler için elde edilen başarısızlık modları Çizelge 6.29'da gösterilmiştir.

Çizelge 6.29. Ağ Cihazları için Başarısızlık Modları

| **Ağ Cihazları ile ilgili Başarısızlık Modları** |
|---|
| Fiziksel arıza |
| Yanlış yapılandırılma |
| Yavaşlama |
| Donma / durma |
| Başarısız firmware yükseltmesi |

VTYS bileşenine için elde edilen başarısızlık modları Çizelge 6.30'da gösterilmiştir.

Çizelge 6.30. VTYS Yazılımı için Başarısızlık Modları

| **VTYS Yazılımı ile ilgili Başarısızlık Modları** |
|---|
| Yavaşlama |
| Güvenirliğinin kaybolması |
| Yanlış yapılandırma |
| Başarısız yama yüklemesi |
| Tablonun kilitlenmesi |
| Table Space ya da diskin dolması |

HTEA analizi sonuçları çalışmanın bir numaralı ekinde (Ek-1) verilmiştir.

### 6.2.3. <Uygulama2> sisteminin HAZOP ile analizi

HAZOP analizi yapmak için öncesinde sistem parametreleri ve referans anahtar kelimeler ortaya konmalıdır. Çalışmanın bu bölümünde ilk olarak sistemin alt sistemlerine ait sistem parametresi ve referans anahtar kelimeler belirlenmiştir.

Sistem parametreleri ve referans anahtar kelimelerin belirlenmesi için bileşenler üzerinde kurumun ilgili bölümlerinde çalışan bilişim uzmanı ve diğer alanlarda uzman personeller ile beyin fırtınası toplantıları yapılmıştır. Soğutma alt yapısına ait sistem parametreleri ve referans anahtar kelimeler, Çizelge 6.31'de gösterilmiştir.

Çizelge 6.31. Soğutma Alt Yapısının Sistem Parametreleri ve Anahtar Kelimeleri

| **Soğutma Alt Yapısı ile İlgili Sistem Parametreleri ve Referans Anahtar Kelimeler** | |
|---|---|
| **Sistem Parametresi** | **Referans Anahtar Kelime** |
| Akışkan sıvı miktarı | Çok |
| | Az |
| Tıkanma / Tıkanıklık | Var |
| Yoğunlaştırma | Başarısız |
| | Yok |
| Kondenser içi basınç | Çok |
| | Az |
| Hava akışı | Düşük |
| | Yok |
| Isı alış verişi | Düşük |

Enerji alt yapısına ait sistem parametreleri ve referans anahtar kelimeler, Çizelge 6.32'de gösterilmiştir.

Çizelge 6.32. Enerji Alt Yapısının Sistem Parametreleri ve Anahtar Kelimeleri

| **Enerji Alt Yapısı ile İlgili Sistem Parametreleri ve Referans Anahtar Kelimeler** | |
|---|---|
| **Sistem Parametresi** | **Referans Anahtar Kelime** |
| Şarj olma | Başarısız |
| Güç çıkışı | Yok |
| Güç sağlama süresi | Kısa |
| Otomatik devreye girme | Başarısız |
| Güç Girişi | Yok |
| | Dalgalı |
| Voltaj | Düşük |
| Motorun çalışma süresi | Kısa |
| Şalterin kapatılması | İstemsiz / yanlışlıkla |
| İletmek/iletim | Başarısız |

Uygulama yazılımına ait sistem parametreleri ve referans anahtar kelimeler, Çizelge 6.33'de gösterilmiştir.

Çizelge 6.33. Uygulama Yazılımının Sistem Parametreleri ve Anahtar Kelimeleri

| **Uygulama Yazılımı ile İlgili Sistem Parametreleri ve Referans Anahtar Kelimeler** | |
|---|---|
| **Sistem Parametresi** | **Referans Anahtar Kelime** |
| Durması | Zamansız |
| İşlem Süresi | Uzun |
| Sonuçların güvenilirliği | Yok |
| Başlatma | Başarısız |
| Sonlandırma | Başarısız |

Bilişim personelinin sistem parametreleri ve referans anahtar kelimeleri, Çizelge 6.34'te gösterilmiştir.

Çizelge 6.34. Bilişim Personelinin Parametreleri ve Anahtar Kelimeleri

| **Bilişim Personeli ile İlgili Sistem Parametreleri ve Referans Anahtar Kelimeler** | |
|---|---|
| **Sistem Parametresi** | **Referans Anahtar Kelime** |
| İşe gelme (Sisteme Erişim) | Geç |
| Algoritma oluşturma | Yanlış |
| Kod yazma süresi | Uzun |
| Fonksiyon kullanımı | Yanlış |
| (Çalışma) sürekliliği | Yok |

İşletim sistemine ait sistem parametreleri ve referans anahtar kelimeler, Çizelge 6.35'te gösterilmiştir.

Çizelge 6.35. İşletim Sistemi için Sistem Parametreleri ve Referans Anahtar Kelimeler

| **Sistem Parametresi** | **Referans Anahtar Kelime** |
|---|---|
| Süreklilik | Yok |
| Yapılandırma | Yanlış |
| Başlatma | Başarısız |
| Çalışma performansı | Düşük |

Sunucu donanımına ait sistem parametreleri ve referans anahtar kelimeler, Çizelge 6.36'da gösterilmiştir.

Çizelge 6.36. Sunucu Donanımı Sistem Parametreleri ve Anahtar Kelimeleri

| **Sunucu Donanımı ile İlgili Sistem Parametreleri ve Referans Anahtar Kelimeler** | |
|---|---|
| **Sistem Parametresi** | **Referans Anahtar Kelime** |
| Fiziksel bütünlük | Yok / bozuk |
| Çalışma performansı | Düşük |
| Başlatma | Başarısız |

Ağ cihazlarına ait sistem parametreleri ve referans anahtar kelimeler, Çizelge 6.37'de gösterilmiştir.

Çizelge 6.37. Ağ Cihazları için Sistem Parametreleri ve Referans Anahtar Kelimeler

| **Ağ Cihazları ile İlgili Sistem Parametreleri ve Referans Anahtar Kelimeler** | |
|---|---|
| **Sistem Parametresi** | **Referans Anahtar Kelime** |
| Fiziksel bütünlük | Yok / bozuk |
| Yapılandırma | Yanlış |
| Çalışma performansı | Düşük |
| Süreklilik | Yok |
| SSL bağlantısı | Başarısız |

Ağ kablolarının sistem parametreleri ve referans anahtar kelimeleri, Çizelge 6.38'de gösterilmiştir.

Çizelge 6.38. Ağ kablosunun Sistem Parametreleri ve Referans Anahtar Kelimeler

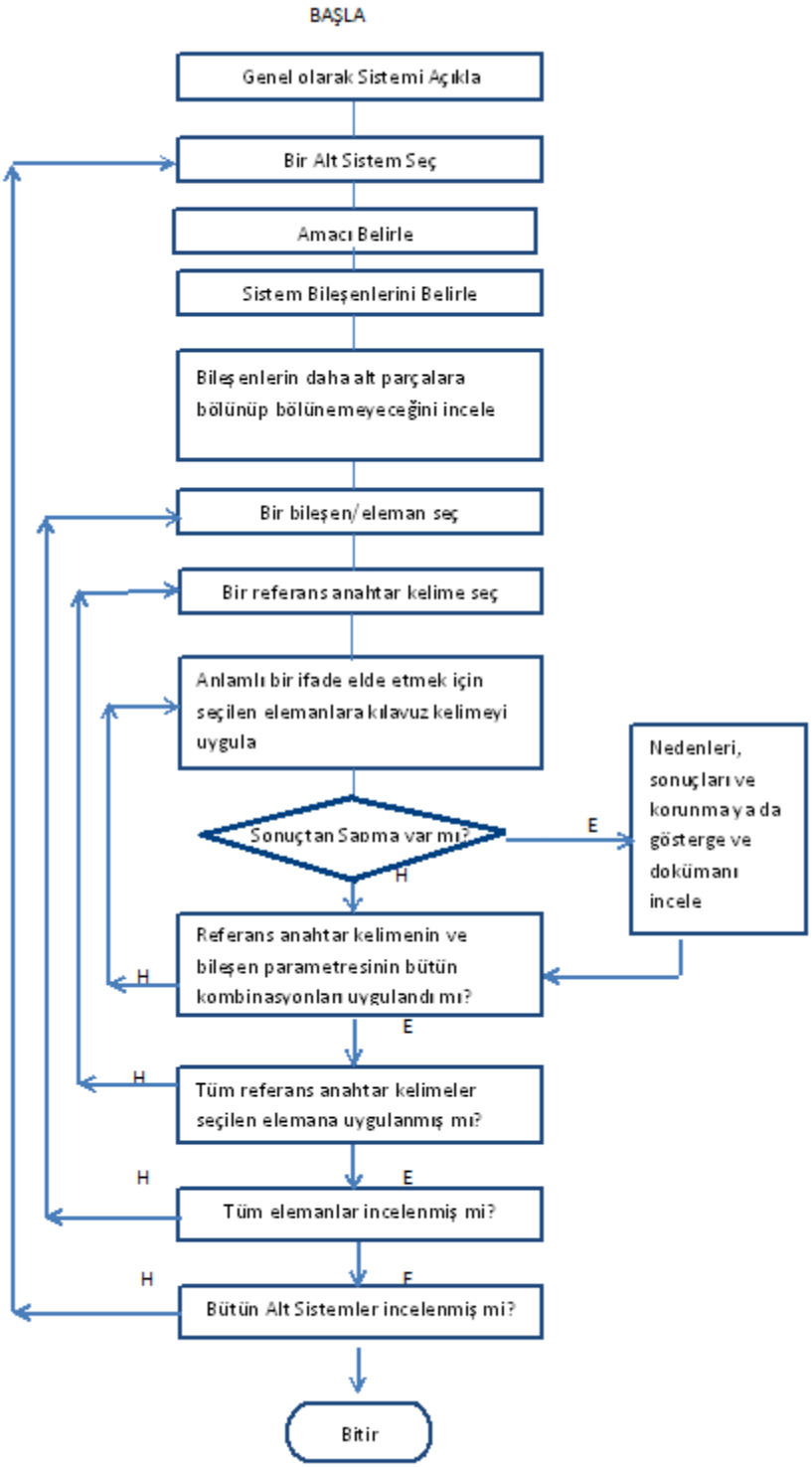
| **Sistem Parametresi** | **Referans Anahtar Kelime** |
|---|---|
| Fiziksel bütünlük | Yok / bozuk |
| Parazit | Var |
| Sinyal | Zayıf |

VTYS yazılımının sistem parametreleri ve referans anahtar kelimeleri, Çizelge 6.39'da gösterilmiştir.

Çizelge 6.39. VTYS Yazılımının Sistem Parametreleri ve Anahtar Kelimeleri

| **VTYS Yazılımı ile İlgili Sistem Parametreleri ve Referans Anahtar Kelimeler** | |
|---|---|
| **Sistem Parametresi** | **Referans Anahtar Kelime** |
| Verilerin güvenirliği | Yok |
| İşlem süresi | Uzun |
| Yapılandırma | Yanlış |
| Veri | Yok |
| Tabloya ekleme işlemi | Başarısız |

Şekil 6.9'da HAZOP analizinin gerçekleştirme adımları gösterilmiştir (IEC, 2001). Analizin amacı bilişim sistemlerinin sürekliliği olarak belirlenmiştir. İlk olarak sisteme ait alt sistemler belirlenmiştir ve her bir alt sistem sırasıyla ele alınmıştır. Dikkate alınan alt sistem bileşenlerine ayrılmıştır. Her bir bileşen için olası sistem parametreleri tespit edilmiştir. Seçilen sistem parametresi referans anahtar kelime ile birleştirilmiştir. Daha sonra bu işlem bütün bileşenlerin her bir sistem parametresi ve referans anahtar kelime için tekrarlanmıştır.




Şekil 6.9. HAZOP Gerçekleştirme Akış Şeması

HAZOP analizinde kullanılan ve Ericson (2005) tarafından önerilen analiz formu Şekil 5.10'da gösterilmiştir.

| Sistem: Medula Hastane | | Alt Sistem: Soğutma Alt Yapısı | | | HAZOP ANALİZİ | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sıra No / Bileşen | Fonksiyon /Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Rik | Öneriler ve Düşünceler |
| 1 <Sistem Bileşeni> | | <Sistem Parametresi> | <Anahtar Kelime 1> | | | | | | | |
| | | | <Anahtar Kelime 2> | | | | | | | |

Şekil 6.10. Kullanılan HAZOP Analiz Formu

Yapılan çalışmanın HAZOP analiz formları ikinci ekte (Ek-2) verilmiştir.

## 6.3. Risk Analizi Uygulamasının Değerlendirilmesi

Yapılan analiz sonucunda sistemde bulunan tehlikeler ciddiyet (Bknz. Çizelge 5.15) ve olasılık (Bknz. Çizelge 5.16) tablosuna göre puanlandırılmıştır. Sistemde 108 adet tehlike bulunmuş ve çok benzer olanlar çıkarılarak 96 adet tekil risk elde edilmiştir. Tehlikeler risk puanlarına yüksekten düşüğe doğru göre sıralanmıştır. En yüksek risk siber saldırı sonucunda verilerin silinmesi veya bozulması sonucunda uygulamanın hizmet verememesi olup değeri 70 (yetmiş) olarak bulunmuştur. En düşük risk değeri ise hastanelerde izin verilen uzunluktan daha uzun kablo kullanmadan kaynaklı ağ kablosunda parazit oluşması ve hastane bilgisayarlarının uygulamaya erişirken gecikmeler yaşaması olup risk puanı 6 (altı) olarak bulunmuştur. Sistemde bulunan tehlikelerin risk puanlarına yüksekten düşüğe doğru göre sıralanışı Çizelge 6.40'ta gösterilmiştir.

Çizelge 6.40. Yüksekten Düşüğe Sıralanmış İş Sürekliliği Riskleri

| No | Sistemdeki İş Sürekliliği Tehlike ve Riskleri | Risk |
|---|---|---|
| 1. | Siber saldırı ya da SQL injection sonucunda verilerin güvenirliliğin kaybolması ile uygulamanın güvenilir bir şekilde hizmet verememesi. | 70 |
| 2. | Sabotaj yada istemsiz işlem kaynaklı verilerin silinmesi sonucunda verilere erişilememesi ve uygulamanın hizmet verememesi. | 60 |
| 3. | Tablonun kilitlenmesi sonucunda VTYS yazılımı tabloya ekleme yapamadığı için uygulama yeni kayıt yapamaması ve bir süre hizmet verememesi. | 56 |

Çizelge 6.40. (devam) Yüksekten Düşüğe Sıralanmış İş Sürekliliği Riskleri

| | | |
|---|---|---|
| 4. | Bozuk disk yerine sağlam diskin değiştirilmesi kaynaklı verilerin silinmesi ya da bozulması sonucunda ve uygulamanın hizmet verememesi. | 54 |
| 5. | Şebeke elektriği kesildikten kısa süre sona UPS sisteme güç veremez. Sunucu ve diğer donanımların kapanmasıyla uygulama hizmetinin durması. | 45 |
| 6. | Yangın, sıvı ile temas ya da elektrik kesintisi kaynaklı ağ cihazlarının donanım arızası sonucunda ağ trafiğinin kesilmesiyle uygulamaya erişilemez. | 42 |
| 7. | Eksik analiz ve tasarım yapılmamasından kaynaklı yazılımcının yanlış algoritma oluşturması ve metotların çalışmaması sonucunda uygulamanın yanlış hizmet vermesi. | 40 |
| 8. | Yapılan işlerin prosedürünün olmaması, aşırı iş yükü, motivasyon eksikliği veya yetersiz eğitimden kaynaklı veri depolama cihazlarının yanlış yapılandırılması ile veri trafiğinin kesilmesi veya yavaşlaması sonucunda uygulamanın veri tabanına erişememesi veya yavaş erişmesi. | 40 |
| 9. | Klima kondenserinde akışkan sıvı miktarının gereğinden çok olmasından kaynaklı veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulamanın yavaşlaması veya durması. | 36 |
| 10. | Klima kondenserinde akışkan sıvı miktarının gereğinden az olmasından kaynaklı veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulamanın yavaşlaması veya durması. | 36 |
| 11. | Klima kondenser içi basıncın gereğinden çok olmasından kaynaklı veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulamanın yavaşlaması veya durması. | 36 |
| 12. | Klima kondenser içi basıncın gereğinden az olmasından kaynaklı veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulamanın yavaşlaması veya durması. | 36 |
| 13. | Redresör arızasından dolayı şebeke elektriği kesildiğinde şarj olmayan UPS sisteme güç veremez. Sunucu ve diğer donanımların kapanmasıyla uygulamanın hizmet verememesi. | 36 |
| 14. | İnvertör veya emniyet sigortasının atması kaynaklı şebeke elektriği kesildiğinde UPS sisteme güç veremez. Sunucu ve diğer donanımlar kapanmasıyla uygulamanın hizmet verememesi. | 36 |
| 15. | Prosedürün olmaması veya eğitim eksiğinden kaynaklı WAS uygulama sunucusunun başarısız yapılandırması sonucunda uygulama hizmet verememesi, hata vermesi. | 36 |
| 16. | Yapılan işlerin prosedürünün olmaması, aşırı iş yükü, motivasyon eksikliği veya yetersiz eğitimden kaynaklı ağ cihazlarının yanlış yapılandırılması ile ağ trafiğinin kesilmesi veya yavaşlaması sonucunda uygulamaya erişilememesi veya yavaş erişilmesi. | 36 |

Çizelge 6.40. (devam) Yüksekten Düşüğe Sıralanmış İş Sürekliliği Riskleri

| | | |
|---|---|---|
| 17. | Sabotaj ya da RAID yapısının bozulmasından kaynaklı LUN yapılandırmasının silinmesi sonucunda verilerin bozulması ayrıca veri tabanına erişilememesi ve uygulamanın hizmet verememesi. | 36 |
| 18. | Direk ısıya maruz kalan ya da dar ve havasız alanlara monte edilen klima kondenserinin klima gazını yoğunlaştıramamasından kaynaklı veri merkezinin ısınması sonucunda içindeki sistemlerin ısınması ve uygulamanın yavaşlaması. | 35 |
| 19. | Yangın, yıldırım ya da kullanıcı hatası nedenlerinden dolayı güvenlik duvarının fiziksel bütünlüğünün bozulması ve uygulamaya erişilememesi. | 35 |
| 20. | Yapılan işlerin prosedürünün olmaması, aşırı iş yükü, motivasyon eksikliği veya yetersiz eğitimden kaynaklı güvenlik duvarının yanlış yapılandırılması ile ağ trafiğinin kesilmesi sonucunda uygulamaya erişilememesi. | 35 |
| 21. | Değişen anahtarın güvenlik duvarına girilmemesi kaynaklı başarısız SSL bağlantısı sonucunda uygulamaya erişilemez. | 35 |
| 22. | Yük dağıtıcının elektrik kesintisi veya donanım arızası sonucu erişim isteklerinin sunucuya ulaşamaması ve uygulamanın hizmet verememesi. | 35 |
| 23. | Omurga ağ anahtarının elektrik kesintisi veya donanım arızasından kaynaklı iç ağ trafiği sunuculara ulaşmaz ve uygulama hizmet veremez. | 35 |
| 24. | Güç kesintisi, yanlış prosedür veya yanlış sürüm kaynaklı başarısız firmware yükseltmesi sonucunda disk kontrolörün veri ağı ile bağlantısının kesilmesi veya yavaşlaması ile uygulama hizmet veremez veya yavaş hizmet verir. | 35 |
| 25. | Yetersiz eğitim ya da aşırı iş yükü sonucunda yazılımcının kod içerisinde fonksiyonun yanlış bir şekilde kullanılmasıyla uygulamanın çalışmaması, yanlış çalışması veya beklenmedik şekilde sonlanması. | 32 |
| 26. | Yazılım içindeki parametrik SQL kodundan kaynaklı işlem sürelerinin uzaması ve uygulama yavaş hizmet vermesi. | 32 |
| 27. | Klima evaporatörünün kirlenmesi, tıkanması veya korozyonu kaynaklı ısı alış verişi düşük olur. Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlaması veya durması. | 30 |
| 28. | Elektrik tesisatın yanmasından kaynaklı sunucular kapanıp veriler zarar görmesi ve uygulamanın uzun süre hizmet verememesi. | 30 |
| 29. | Fonksiyonların yanlış kullanımından veya yazım yanlışından dolayı uygulama yazılımının zamansız durması ve hizmet verememesi. | 30 |
| 30. | SQL injection kaynaklı güvenirliliğin kaybolması sonucunda uygulamanın güvenilir bir şekilde hizmet verememesi. | 30 |

Çizelge 6.40. (devam) Yüksekten Düşüğe Sıralanmış İş Sürekliliği Riskleri

| | | |
|---|---|---|
| 31. | Fonksiyonların yanlış kullanımından veya yazım yanlışından dolayı uygulama başlatıldıktan kısa süre sonra kapasitesini doldurması ve hizmet verememesi. | 30 |
| 32. | Düşük maaş, aşırı iş yükü veya motivasyon eksikliğinden kaynaklı yetiştirilmiş uygulama geliştirici bilişim personelinin işten ayrılması sonucunda yeni uygulama sürümünün vaktinde devreye girememesi veya hatalı sürümün ortaya çıkması. | 30 |
| 33. | Sunucunun çökmesinden kaynaklı server.pid dosyası sistemde kalır. İlgili JVM (ler) başlayamadığından uygulama da başlamaması ve hizmet verememesi. | 30 |
| 34. | Yapılan işlerin prosedürünün olmaması, aşırı iş yükü, motivasyon eksikliği veya yetersiz eğitimden kaynaklı yük dağıtıcının yanlış yapılandırılması sonucunda uygulamaya erişilememesi. | 30 |
| 35. | Yapılan işlerin prosedürünün olmaması, aşırı iş yükü, motivasyon eksikliği veya yetersiz eğitimden kaynaklı başarısız yama yüklemesi sonucunda VTYS yazılımı çalışmadığı için uygulamanın veritabanına erişememesi ve hizmet verememesi. | 30 |
| 36. | Yapılan işlerin prosedürünün olmaması, aşırı iş yükü, motivasyon eksikliği veya yetersiz eğitimden kaynaklı başarısız yapılandırma sonucunda VTYS yazılımı çalışmadığı ya da yavaş çalıştığı için uygulamanın veritabanına erişememesi ve hizmet verememesi veya yavaş hizmet vermesi. | 30 |
| 37. | Yapılan işlerin prosedürünün olmaması, aşırı iş yükü, motivasyon eksikliği veya yetersiz eğitimden kaynaklı başarısız yapılandırma kaynaklı VT işletim sisteminin çalışmaması ya da VTYS yazılımını çalıştıramadığı ya da yavaş çalıştırdığı için veritabanına erişilmeyebilir. Uygulama hizmet vermez veya yavaş verir. | 30 |
| 38. | Desteğin bitmesi, elektrik kesintisi ya da eksik sürücü (dosya) kaynaklı uygulama sunucusu işletim sisteminin başlayamaması sonucunda uygulamanın hizmet verememesi. | 30 |
| 39. | Yangın, yıldırım veya kullanıcı hatalarından dolayı yönlendiricinin fiziksel bütünlüğünün bozulmasıyla uygulamaya erişilememesi. | 28 |
| 40. | Yıpranma, ısınma veya korozyon kaynaklı yük dağıtıcının çalışma performansının düşmesiyle yönlendirme hızlı yapılamaz ve uygulama yavaş hizmet verir. | 28 |
| 41. | Yıldırım, yüksek güç veya yangın kaynaklı fiziksel SAN switch arızası sonucunda veri trafiği kesilmesi ve uygulamanın hizmet verememesi. | 27 |
| 42. | Titreşim, elektrik kesintisi veya destek anlaşmasının bitmesinden kaynaklı aynı RAID yapılandırması içinde çoklu diskin bozulması sonucunda veri tabanına erişilememesi ve uygulamanın hizmet verememesi. | 27 |

Çizelge 6.40. (devam) Yüksekten Düşüğe Sıralanmış İş Sürekliliği Riskleri

| | | |
|---|---|---|
| 43. | Klima kondenserinin yanlış yere montajından veya kirli ortamdan kaynaklı veri merkezi ve içindeki sistemlerin ısınması ve uygulama yavaşlaması. | 25 |
| 44. | Klima kompresöründe oluşan zararlı kimyasal eriyikler ya da termostatın yanlış ayarlanmasından kaynaklı veri merkezi ve içindeki sistemlerin ısınması ve sonucunda uygulamanın yavaşlaması veya durması. | 25 |
| 45. | Yazılım içindeki elverişsiz SQL kodundan kaynaklı işlem sürelerinin uzaması ile uygulama hizmetinin yavaşlaması veya bir süre sonra durması. | 25 |
| 46. | İşletim sistemindeki veya çalışma ortamındaki eksik kütüphanelerden dolayı uygulama başlatılamaması ve hizmet verememesi. | 25 |
| 47. | DDOS gibi hizmet aksatıcı siber saldırılar sonucunda bağlantı sınırlarının aşılmasıyla uygulamanın yeni ve gerçek kullanıcılardan gelen isteklere cevap verememesi. | 25 |
| 48. | Ulaşım sorunu, kötü hava şartları veya düzensiz iş planından kaynaklı veri tabanı yöneticisinin işe geç gelmesi sonucunda sorunlara geç müdahale etmesi ve uygulama hizmetinin kesintiye uğraması. | 25 |
| 49. | Aşırı iş yükü, düşük maaş, motivasyon eksikliği, mobbing, emeklilik veya askerlikten dolayı VT yöneticisinin işten ayrılması sonucunda uygulama hizmetinin kesintiye uğraması. | 25 |
| 50. | Standartlarının ve gereksinimlerinin olmamasından kaynaklı Hastana Bilgi Yönetim Sisteminin düşük performansı ve hataları sonucunda <Uygulama2> ile iletişiminin yavaşlaması ve sağlık hak sahiplerinin işlemlerinin gecikmesi. | 25 |
| 51. | Klima kompresörüne güç girişi olmaması, rulmanın sıkışması veya termik atması kaynaklı veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulamanın yavaşlaması veya durması. | 24 |
| 52. | Yapılan işlerin prosedürünün olmaması, aşırı iş yükü, motivasyon eksikliği veya yetersiz eğitimden kaynaklı başarısız yama yüklemesi sonucunda WAS uygulama sunucusu çalışmaması dolayısı ile uygulamanın hizmet vermemesi. | 24 |
| 53. | Yıpranma, ısınma, toz, kir veya korozyon kaynaklı ağ yönlendiricisinin çalışma performansının düşmesiyle ağ trafiğinin yavaşlaması ve uygulamanın yavaş hizmet vermesi. | 24 |
| 54. | Temassızlık, yanlış montaj ya da donanım arızalanması sonucu uygulama sunucusunun çalışmaması ve uygulama hizmet verememesi. | 21 |
| 55. | Yıpranma, ısınma, toz, kir veya korozyon kaynaklı güvenlik duvarının çalışma performansının düşmesiyle ağ trafiğinin yavaşlaması ve uygulamanın yavaş hizmet vermesi. | 21 |
| 56. | Yıldırım, yüksek güç veya yangın kaynaklı VTYS sunucu donanımının fiziksel bütünlüğünün bozulmasıyla veritabanına erişilememesi ve uygulamanın hizmet verememesi. | 21 |

Çizelge 6.40. (devam) Yüksekten Düşüğe Sıralanmış İş Sürekliliği Riskleri

| | | |
|---|---|---|
| 57. | Eksik yazılım analiz, tasarımı veya aşırı iş yükü kaynaklı yazılım kod yazmanın uzun sürmesi sonucunda yeni yazılım projesinin ya da yeni sürümünün vaktinde devreye alınamaması. | 20 |
| 58. | Yapılan işlerin prosedürünün olmaması, aşırı iş yükü, motivasyon eksikliği veya yetersiz eğitimden kaynaklı uygulama sunucusunun başarısız yapılandırılması ile uygulamanın hizmet verememesi, veya hata vermesi. | 20 |
| 59. | Ağ kablosu ile elektrik kablosunun yakın geçmesi veya yalıtım olmamasından kaynaklı ağ kablosunda parazit oluşması ve uygulama hizmet verirken gecikmelerin olması. | 20 |
| 60. | Gereğinden uzun kablo kullanmadan kaynaklı ağ kablosunda parazit oluşması ve uygulama hizmet verirken gecikmelerin oluşması. | 20 |
| 61. | Aşırı iş yükü, olumsuz çalışma şartları ve zayıf bünyeden kaynaklı veri tabanı yöneticisinin işe geç gelmesi sonucunda sorunlara geç müdahale edilmesi ve uygulama hizmetinin kesintiye uğraması. | 20 |
| 62. | Güç kesintisi, yanlış prosedür veya yanlış sürüm kaynaklı yük dağıtıcının başarısız firmware yükseltmesi sonucunda erişim isteklerinin sunuculara iletilememesi veya yavaş iletilmesi ile uygulamanın hizmet verememesi veya yavaş hizmet vermesi. | 20 |
| 63. | Yıldırım, yüksek güç, korozyon veya yangın kaynaklı fiziksel disk arızası sonucunda disk üzerindeki verilerin bozulması ve uygulamanın hizmet verememesi. | 20 |
| 64. | Yetersiz eğitim, sabotaj, aşırı iş yükü veya prosedürün olmamasından kaynaklı RAID yapılandırmasının silinmesi sonucunda veri tabanına erişilememesi ve uygulamanın hizmet verememesi. | 20 |
| 65. | Bozuk geçiş anahtarından dolayı şebeke elektriği kesildiğinde UPS devreye girmemesi sonucunda sunucu ve diğer donanımlar kapanmasıyla uygulamanın hizmet vermemesi. | 18 |
| 66. | Jeneratör AVR arızasından dolayı sisteme düşük voltaj gitmesi ve sistemin kapanıp arızalanması. | 18 |
| 67. | Etiketleme olmamasından veya insan hatasından kaynaklı yanlış şalterin kapatılması sonucunda sisteme güç girişi olmayacağı için sunucular kapanması ve uygulamanın hizmet verememesi. | 16 |
| 68. | Donanım arızası veya virüs bulaşması sonucunda işletim sistemi çalışmasını sürdüremediğinde uygulama hizmet verememesi. | 16 |
| 69. | Düşük performanslı RAID yapılandırması veya düşük hızlı disklerden kaynaklı işlem sürelerinin uzaması ve uygulamanın yavaş hizmet vermesi. | 16 |

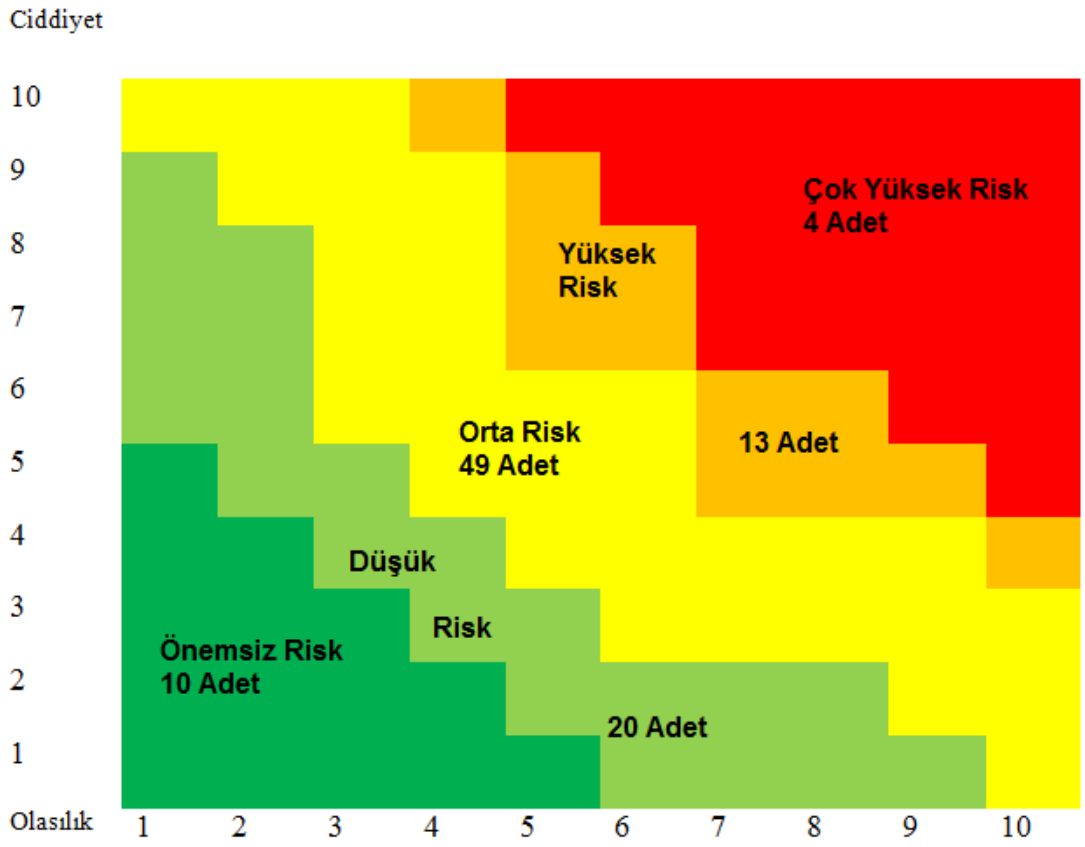
Çizelge 6.40. (devam) Yüksekten Düşüğe Sıralanmış İş Sürekliliği Riskleri

| | | |
|---|---|---|
| 70. | Güç kesintisi, yanlış prosedür veya yanlış sürüm kaynaklı HBAnın başarısız firmware yükseltmesi sonucunda sunucunun veri ağı ile bağlantısının kesilmesi veya yavaşlaması ile uygulamanın hizmet verememesi veya yavaş hizmet vermesi. | 16 |
| 71. | Güç kesintisi, ısınma, yanlış prosedürün izlenmesi veya yanlış sürümden kaynaklı güvenlik duvarının başarısız firmware yükseltmesi sonucunda ağ trafiğinin yavaşlaması veya kesilmesi ile uygulamaya erişimin yavaşlaması veya kesilmesi. | 14 |
| 72. | Güç kesintisi, ısınma, yanlış prosedürün izlenmesi veya yanlış sürümden kaynaklı ağ yönlendiricisinin başarısız firmware yükseltmesi sonucunda ağ trafiğinin yavaşlaması veya kesilmesi ile uygulamaya erişimin yavaşlaması veya kesilmesi. | 14 |
| 73. | Güç kesintisi, ısınma, yanlış prosedürün izlenmesi veya yanlış sürümden kaynaklı yük dağıtıcının başarısız firmware yükseltmesi sonucunda ağ trafiğinin yavaşlaması veya kesilmesi ile uygulamaya erişimin yavaşlaması veya kesilmesi. | 14 |
| 74. | Güç kesintisi, ısınma, yanlış prosedürün izlenmesi veya yanlış sürümden kaynaklı ağ anahtarının başarısız firmware yükseltmesi sonucunda ağ trafiğinin yavaşlaması veya kesilmesi ile uygulamaya erişimin yavaşlaması veya kesilmesi. | 14 |
| 75. | Kapasite planlaması olmamasından kaynaklı hastane bilgisayar ve ağ yapısında bir sorun oluştuğunda teknik personel sayısının az olması nedeniyle sorunların uzun süre devam etmesi ve uygulamaya erişilememesi. | 14 |
| 76. | Toz, kir, ısınma ve yıpranma kaynaklı donanım yavaşlaması sonucunda VTYS sunucusunun ve uygulama hizmeti yavaşlaması veya kısa süre sonra durması. | 12 |
| 77. | Sigorta atması, ikaz trafosunun yanması, mıknatıs manyetizmasının azalmasından dolayı jeneratörün güç üretmemesi sonucunda ve sunucuların kapanması ve uygulamanın hizmet verememesi. | |
| 78. | Veri depolama ağındaki Fiber optik (FC) kablonun kopması ya da yerinden çıkması sonucunda veri trafiği kesilmesi ve uygulamanın hizmet verememesi. | 12 |
| 79. | Yangın, korozyon, yüksek güç veya insan hatasından kaynaklı ağ bağlantısının kesilmesi sonucunda hastane bilgisayarlarının uygulamaya erişememesi ve sağlık hak sahiplerine hizmet verilememesi. | 12 |
| 80. | Ağ kablolarının elektrik kabloları aynı kanaldan geçmesinden kaynaklı ağ kablosunda parazit oluşması sonucunda hastane bilgisayarlarının uygulamaya erişememesi ve sağlık hak sahiplerine hizmet verilememesi. | 12 |
| 81. | Yangın, korozyon, yüksek güç veya insan hatasından kaynaklı hastanedeki bilgisayarların fiziksel arızalanması sonucunda hastane çalışanlarının uygulamaya erişememesi ve sağlık hak sahiplerine hizmet verilememesi. | 12 |

Çizelge 6.40. (devam) Yüksekten Düşüğe Sıralanmış İş Sürekliliği Riskleri

| | | |
|---|---|---|
| 82. | Toz, kir, ısınma, yıpranma veya korozyon kaynaklı hastanedeki bilgisayarların yavaşlaması sonucunda uygulamaya erişimin yavaşlaması ve sağlık hak sahiplerine sunulan hizmetler aksaması. | 12 |
| 83. | Virüs bulaşmasından kaynaklı hastane bilgisayarlarının arızalanması sonucunda bilgisayarların çalışmaması ve hastane personelinin uygulamaya erişememesi. | 12 |
| 84. | Yanlış seçim veya yetersiz eğitimden dolayı hastane teknik personelinin yeterli beceriye sahip olmaması sonucunda oluşan sorunların uzun süre devam etmesi ve uygulamaya kısa sürede erişilememesi. | 12 |
| 85. | Ulaşım sorunu, kötü hava şartları veya düzensiz iş planından kaynaklı hastane teknik personelinin işe geç gelmesi sonucunda hastane bilgisayarlarında ve ağ yapısındaki sorunların uzun süre devam etmesi ve uygulamaya erişilememesi. | 12 |
| 86. | Ulaşım sorunu, kötü hava şartları veya düzensiz iş planından kaynaklı yazılım geliştiren personelin işe geç gelmesi uygulamanın sürekliliği için ciddi bir tehlike teşkil etmemektedir. | 10 |
| 87. | Yakıt devresi tıkanması, ayarsız enjektörler veya emme kanallarının tıkanmasından kaynaklı jeneratörün sisteme güç girişi sağlayamaması sonucunda sunucular kapanması ve uygulamaların hizmet verememesi. | 9 |
| 88. | Fazla sayıda modül ya da uygulamadan kaynaklı virüs bulaşması ile işletim sisteminin yavaşlaması ve sonucunda uygulama hizmeti yavaşlaması. | 9 |
| 89. | Toz, kir, ısınma, yıpranma veya korozyon kaynaklı uygulama sunucusu donanımının yavaşlaması sonucunda uygulama hizmetinin yavaşlaması veya bir süre sonra durması. | 9 |
| 90. | Yıldırım, yangın, yüksek güç girişi, sıvı teması veya insan hatasından dolayı fiziksel SAN switch arızası sonucunda veri trafiği kesilmesi ve uygulamanın hizmet verememesi. | 9 |
| 91. | Yıpranma, ısınma veya korozyon kaynaklı SAN switch yavaşlaması ve uygulamanın yavaş hizmet vermesi. | 9 |
| 92. | Kullanıcı hatası, ezilme veya gerilme kaynaklı ağ kablosunun fiziksel bütünlüğünün bozulması sonucunda veri trafiği kesilmesi ve uygulamanın hizmet verememesi. | 8 |
| 93. | Diskin dolması sonucunda VTYS yazılımı tabloya ekleme yapamadığı için uygulama yeni kayıt yapamaması. | 7 |
| 94. | Table spacenin dolması sonucunda VTYS yazılımı tabloya ekleme yapamadığı için uygulamanın yeni kayıt yapamaması. | 7 |
| 95. | Hatalı motor devri veya sargılardaki kopmalardan kaynaklı jeneratörün sisteme dalgalı güç vermesi sonucunda sunucu ve ağ cihazlarının arızalanması ve uygulamanın hizmet verememesi. | 6 |
| 96. | Gereğinden uzun kablo kullanmadan kaynaklı ağ kablosunda parazit oluşması ve hastane bilgisayarlarının uygulamaya erişirken gecikmeler yaşaması. | 6 |

Ciddiyet (Bknz. Çizelge 6.15) ve olasılık (Bknz. Çizelge 6.16) tabloları kullanılarak risk matrisi oluşturulmuştur. Dokuzdan küçük riskler önemsiz olarak gösterilmiştir. Risk matrisinde 9-16 puan aralığındakiler düşük, 16-36 puan aralığındakiler orta, 36-49 puan aralığındakiler yüksek ve 49 puan ve üstündeki riskler ise çok yüksek risk olarak belirlenmiştir. Şekil 6.11'de risk matrisi gösterilmiştir. On tane önemsiz, yirmi tane düşük, 49 tane orta, 13 tane yüksek ve 4 tane çok yüksek risk bulunmuştur.




Şekil 6.11. Risk Matrisi

# 7. SONUÇ VE ÖNERİLER

İş dünyasında rekabet edebilmek için hem yatırım projelerinde hem de çalışma sırasında karşılaşılan tehlikelerin önceden belirlenmesi ve değerlendirilmesi gerekmektedir. Tehlikelerin tespiti ve bunları önceliklendirme ihtiyacına en iyi çözümlerden birisi risk analizidir. Bu nedenle risk analizi rekabeti ve iş sürekliliğini önemseyen herkes için ihtiyaç haline dönüşmüştür.

Risk analizinin amacı; sistemde meydana gelmesi muhtemel tehlikeleri gerçekleşmeden proaktif bakış açısıyla olaylara yaklaşarak belirlemek, kaynağında yok etmek ya da olasılığını ya da şiddetini azaltmaya yönelik faaliyetler belirleyerek sürekli iyileştirmelerle olası riskleri azaltmaktır.

Çalışma sırasında risk analizi ile ilgili standartlar ve akademik çalışmalar incelenmiştir. İncelenen standartlardan bazıları; *ISO 22301 iş sürekliliği yönetim sistemi* ve *ISO 27031 bilgi ve iletişim teknolojileri için iş sürekliliği yönergeleri* standartlarıdır. Ayrıca *ISO 31000 risk yönetimi – prensipler ve kılavuzlar* ve *ISO 31010 risk yönetimi – teknikler* standartları ve akademik çalışmalar incelenerek HTEA ve HAZOP hakkında detaylı bilgiler elde edilmiştir. Akademik çalışmalarda risk analizinin daha çok sistem güvenliğine yönelik yapıldığı görülmüştür. Ancak az sayıda da olsa da iş sürekliliğine değinen çalışmalara rastlanmıştır.

Çalışmanın özünü bilişim sistemlerinde iş sürekliliğine yönelik risk analizi oluşturmaktadır. Bütün sistem için risk analizinin yapılması mümkün olmadığından öncelikle AHP yöntemi ile risk analizi yapılan uygulama seçilmiştir.

Akademik çalışmalar incelendiğinde iyi bir risk analizi için tek bir tekniğin yeterli olmadığı anlaşılmıştır. Uygulama çalışmasında ilk olarak üst seviye aksiliklerin belirlenmesine karar verilmiş ve ÖTL analiz tekniği uygulanarak ön tehlike listesi oluşturulmuştur.

Çalışma kapsamında kullanılan diğer bir risk analizi tekniği olarak HTEA'nın seçilmesinde hem genel bir kabul görmesi hem de başarılı sonuçlar üretmesi etkili olmuştur. HTEA

uygulaması için ilk olarak bileşenleri, fonksiyonları, hata modlarını, hataların etkilerini ve nedenlerini belirlemek için sorular hazırlanmıştır. Sistem alt sistemlere ayrılmış ve alt sistemler de personel, veritabanı, kablo ve disk gibi detaylı bileşenlere ayrılmıştır. Uzman ekiplerle yapılan beyin fırtınası toplantılarında iş sürekliliği ihlal olaylarına sebep olabilecek bileşenlerin hata modları, hataların etkileri, nedenleri ve öneriler ortaya konulmuştur.

HAZOP analizi için ilk olarak alt sistemlere ait sistem parametresi ve referans anahtar kelimeler belirlenmiştir. Her bir alt sistem için sistem parametreleri ve referans anahtar kelimeleri belirlemek için bileşenler üzerinde beyin fırtınası yapılmıştır. Sistem parametreleri ve referans anahtar kelimeler belirlendikten sonra her seferinde sisteme ait alt sistemlerden biri seçilmiştir. Alt sistem bileşenlerine ayrılmıştır. Seçilen bileşen ele alınıp bu bileşen için geçerli olan sistem parametreleri belirlenmiştir. Seçilen her bir sistem parametresi referans anahtar kelime ile birleştirilmiştir. Bu yolla anlamlı tehlikeler tanımlanıp tanımlanamayacağı araştırılmıştır.

Yapılan çalışma sonucunda hem HAZOP hem de HTEA'nın bilişim sistemlerinin sürekliliğine yönelik risk analizi için uygun olduğu görülmüştür. Ancak bu analiz tekniklerinin uygulanması ve analiz formları ihtiyaç halinde değiştirilerek kullanılabilir. Sistemin çalışmasını engelleyecek ya da yavaşlatacak, işin sürekliliğine zarar verebilecek unsurlar risk analizi metotları kullanılarak belirlenmiştir. Riskleri azaltarak sürekli iyileştirme ile kurumun mevcut durumundan daha iyi bir seviyeye çıkması için yapılacak işler belirlenmeye çalışılmıştır.

Risklerin yüksek puana sahip büyük bir kısmının altyapı ve enerji sorunlarından kaynaklandığı görülmüştür. Bu nedenle kurum veri merkezini elverişli binalara kurmalıdır. Risklerden yüksek puana sahip başka bir bölüm, insan hatası olduğundan (yanlış işlemden kaynaklı) önleyici tedbir olarak bilişim personeli düzenli eğitime tabi tutulmalı ve personelin becerileri geliştirilmelidir. Kurum; bilişim personellerinin istihdamından önce doğru kişinin seçilmesi ve istihdam sırasında ise gerekli eğitimin verilmesi, görev ve sorumlulukların net bir şekilde belirlenmesi gibi hususlarda çalışma yapmalıdır.

Operasyon sırasında sonuçlardan sapmanın nedensel faktörleri; ilgili konuda prosedürün olmaması ya da bir standarda dayandırılmamasıdır. Kuruma ve iş sürekliliğini amaçlayan

diğer kurumlara, işleri prosedürlere dökmeleri ayrıca değişiklik yönetimi ve konfigürasyon yönetimi yapmaları şiddetle önerilmektedir.

Bilişim hizmetinde kronik kesintiler olan kurumlar, belirli ve sıkıntı verici bu hizmet kesintilerinin kök nedenlerini bulmak ve gidermek için hata ağacı analiz (HAA) tekniklerini kullanabilirler. Enerji ve soğutma alt yapısında meydana gelen bir olayın sebep olabileceği hizmet kesintilerini ortaya çıkarabilmek için olay ağacı analizini (OAA) kullanmalıdırlar. Uygulanabilirliğini kolaylaştırmak ve süreci hızlandırmak amacıyla bilişim hizmetlerinin risk analizi konusunda daha fazla teorik ve pratik çalışma yapılması önerilmektedir.

Bilgi teknolojilerine yönelik uluslararası[7] standartlar ile yönetim çerçeveleri[8] birbirleriyle hem kesişmekte hem de biri diğerinin tamamlamaktadır. Bu standart ve yönetim çerçevelerinin her birinde iş sürekliliği direk ya da başka adlarda[9] gereksinim olarak belirtilmektedir. Bu nedenle kurumlar gerçek anlamda iş sürekliliği uygulamak istediklerinde bilgi güvenliği tedbirlerini, iş sürekliliği planlarını, konfigürasyon yönetimini, değişiklik yönetimini, kapasite yönetimini ve rol yönetimini de içeren entegre yönetim sistemi kurmaları ve işletmeleri önerilmektedir.

[7] ISO /IEC 20000, ISO / IEC 27001, ISO / IEC 27031, ISO 22301 ve SPICE gibi BT standartları.
[8] En iyi bilenen ve yaygın ITIL, COBIT ve CMMI gibi yönetim çerçeveleri.
[9] Hizmet sürekliliği yada iş sürekliliği için hazır bulunurluk gibi ifadeler geçmektedir.

# KAYNAKLAR


Akın, B. (1998). *Hata Türü ve Etkileri Analizi*, İstanbul: Bilim Teknik Yayınevi, 12.

Ansell, J., and Wharton, F. (1992). *Risk: Analysis, Assessment and Management*, John Wiley and Sons, 4-5.

Arman, T. (1997). *Rrisk Analizine Giriş*, İstanbul: Alfa Basım Yayım, III.

Aydemir, Z. (2013). *İstanbul Metrosunda İş Sürekliliği*, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Babaarsalan, N. (2013). *Petrol Rafinerisinde Atmosferik Damıtma Kolonunda Kaza Riski Değerlendirmesi*, Yüksek Lisans Tezi, Ankara Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Bertsche, B. (2007). *Reliability in Automotive and Mechanical Engineering*, Springer, 98-118.

Blos M.F., Wee H.M., and Yang W.-H. (2012). Supply Chain Risk Management: Resilience and Business Continuity, *Intelligent Systems Reference Library*, 33, 219-236.

Booher, H. R. (2003). *Handbook of Human Systems Integration*, John Wiley & Sons, 499.

Burgazzi, L. (2006). Failure mode and effect analysis application for the safety and reliability analysis of a thermal-hydraulic passive system, *Nuclear Technology*, 156 (2), 150-158.

Chin, K. S., Wang, Y.M., Poona, G. K. K., and Yangc, J.B. (2009). "Failure mode and effects analysis using a group-based evidential reasoning approach", *Computers & Operations Research*, 36 (6), 1768–1779.

Cho, F. L. , American Society of Mechanical Engineers , (1998, July). "*Risk assessment technologies, and transportation, storage, and disposal of radioactive materials*". Paper presented at ASME/JSME Joint Pressure Vessels and Piping Conference,22-23

Ciechanowicz, Z. (1997). Risk analysis: requirements, conflicts and problems, *Computer and Security*, 16 (3), 223-232.

Civir, P. (2015). *Otomotiv Sektöründe Tedarikçi Seçiminde AHP-Bulanık AHP Karşılaştırması*, Yüksek Lisans Tezi, Kocaeli Üniversitesi / Fen Bilimleri Enstitüsü, 43-46.

Çakıl, G. (2014). *E-Ticaret Güvenliği*, , Yüksek Lisans Tezi, Okan Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Çakmak, M. (2015). *Demir-Çelik Sektöründe Bulanık Hata Türleri Ve Etkileri Analizi (FUZZY FMEA) Yöntemi İle Risk Değerlendirme Uygulaması*, Yüksek Lisans Tezi, Karabük Üniversitesi Fen Bilimleri Enstitüsü, Karabük.

Deveci, H.C., Esen, H., Hatipoğlu, T., ve Fiğlali, N. (2014). Implementation of reliability-centred FMEA in a cable cutting process, *International Journal of Quality Engineering and Technology*, 4 (4), 334-351.

Dinçkan, A. (2008). *Bgys-0009 İş Sürekliliği Yönetim Sistemi Kurulumu*, TUBITAK UEKAE, 5-6.

Durhan, D. (2006). *Hata Türü Ve Etkileri Analizi (FMEA) Ve Bir Uygulama*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Erdem, O. A., and Younis, A. E. (2012). Yazılım Projelerinde Risk Yönetimi, *Gazi Üniversitesi Bilişim Teknolojileri Dergisi*, 5 (1), 1-5.

Ericson C. A. (2005). *Hazard Analysis Techniques for System Safety*, (Second Edition), John Wiley and Sons, 53-269.

Fazil, A. (2005). A Primer on Risk Assessment Modelling: Focus on Seafood Products, Food and Agriculture Organization of the United Nations, 2.

Gibb, F., and Buchanan, S. (2006). A Framework For Business Continuity Management, *International Journal of Information Management*, 26 (2),128–141.

Gollomp, B. (2008). A look back - Quality and reliability facilitator – FMEA, *IEEE Instrumentation and Measurement Magazine*, 11 (2), 58-59.

Hashim, M., Yoshikawa, H., Matsuoka, T., and Yang, M. (2014). Quantitative dynamic reliability evaluation of AP1000 passive safety systems by using FMEA and GO-FLOW methodology, *Journal of Nuclear Science and Technology*, 51 (4), 526-542.

International Electronic Commision (2001), *Hazard and operability studies– Application guide*, IEC, 11.

International Organization for Standardization (2008). *Information Security Risk management*, ISO , 39-40.

International Organization for Standardization. (2009). *Risk management — Principles and guidelines*, ISO , 12-21.

International Organization for Standardization (2009). *Risk management — Risk assesment techniques*, ISO , 18.

İnternet: British Standarts Institute, "Published Standards" http://standardsdevelopment.bsigroup.com/Home/Search?searchText=25999#tabs-materials, Son Erişim Tarihi: 10.10.2015.

İnternet: IsecT, "FMEA Analiz Formu", http://www.iso27001security.com/ISO27k_FMEA_spreadsheet.xlsx Son Erişim Tarihi: 22.11.2015.

İnternet: ISO, "News 21012 - Business continuity - ISO 22301 when things go seriously wrong", http://www.iso.org/iso/news.htm?refid=Ref1602, Son Erişim Tarihi:12.05.2015.

İnternet: ISO, "Guidelines for information and communication technology readiness for business continuity", http://www.iso.org/iso/catalogue_detail?csnumber=44374, Son Erişim Tarihi:13.05.2015.

Jia, X.-J., Cui, L.-R., and Gao, S. (2009). Safety-critical system reliability modeling and their analyses in terms of effects of component failure modes, *Journal of Beijing Institute of Technology (English Edition)*, 18 (4), 502-506.

Jenny, J.A. (1969). The Effect of Partial Failure Modes on Reliability Analysis, *IEEE Transactions on Reliability*, R-18 (4), 175-180.

Joo, B., Kim S., Kim, S., and Moon, Y.H. (2013). FMEA for the reliability of hydroformed flanged part for automotive application, *Journal of Mechanical Science and Technology*, 27 (1), 63-67.

Jrad A., Morawski T., and Spergel L. (2004). A model for quantifying business continuity preparedness risks for telecommunications networks, *Bell Labs Technical Journal*, 9 (2), 107-123.

Kahraman, Ö. (2009), *Bir Otomobil Fabrikasında İSG Alanında FMEA Yöntemi İle Risk Analizi*, Yüksek Lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya, 9.

Kaplan, S., Garrick, B. J. (1981). On The Quantitative Definition of Risk, *Risk Analysis*, 1 (1), 11-12.

Karabacak, B., ve Özkan, S. (2010, Şubat). *Bilgi Güvenliği Yönetim Sistemi için Süreç Tabanlı Risk Analizi*, III. Ağ ve Bilgi Güvenliği Sempozyumunda sunuldu, Ankara

Kawaguchi H. (2012). Treatment of unexpected risk on business continuity management learned from the Great East Japan Earthquake, *Journal of Disaster Research*, 7 (4), 376-385.

Khalilov, A. (2015). *Büyük Endüstriyel Kazaların Önlenmesi İçin Kullanılan Risk Analiz Yöntemleri Üzerine Bir İnceleme*, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, 87.

Kılıç, İ. (2015). *Bulanık-Analitik Hiyerarşi Sürecini Kullanarak İstanbul Boğazı'nda Deniz Kazaları Risk Analizi*, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, 47-48.

Kır, İ. (2012). *Performans Değerlendirmede Ahp Yaklaşımı Ve Eğitim Sektöründe Bir Uygulama*, Yüksek Lisans Tezi, Çukurova Üniversitesi Fen Bilimleri Enstitüsü, 80-83.

Knight, F. H. (1921). *Risk, uncertainty and profit*, Beard Books, 19.

Kocamustafaoğulları, M. (2013). *Bilgi Güvenliği Farkındalığı Ve Uygulama Seviyesi Değerlendirmek İçin Bilgi Güvenliği Prototip Uygulaması*, Yüskek Lisans Tezi, Çankaya Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Kodalı, R., and Routroy, S. (2006). Decision Framework for Selection of Facilities Location in Competitive Supply Chain, *Journal of Advanced Manufacturing Systems*, 5 (1), 89-110.

Kokash, N., and D'Andrea V. (2007). *Evaluating Quality of Web Services: A Risk-driven Approach,* University of Trento, Trento Italy.

Korayem, M.H., and Iravani, A. (2008). Improvement of 3P and 6R mechanical robots reliability and quality applying FMEA and QFD approaches, *Robotics and Computer-Integrated Manufacturing*, 24 (3), 472-487.

Kusnetzky, D. (2011). *Virtualization A Manager's Guide*, Sebastopol : O'Reilly, 1.

Labuschagne, L., and Eloff, J.H.P. (1998). The Use of Real-Time Risk Analysis to Enable Dynamic Activation of Countermeasures, *Computer and Security*, 17 ( 4), 347-357.

Li, S., and Zhou, W. (2014). Reliability analysis of urban gas transmission and distribution system based on FMEA and correlation operatör, *Frontiers in Energy*, 8 (4), 443-448.

Ling, D., Song, W., and Sun R. (2011). A reliability prediction method for diesel engine components based on FMEA, *Eksploatacja i Niezawodnosc*, 49 (1), 63-67.

Lin Q., Wang D., Lin W., and Liu H. (2014). Human reliability assessment for medical devices based on failure mode and effects analysis and fuzzy linguistic theory, *Safety Science*, 62, 248–256.

Mansourov, N., and Campara, D. (2010). *System Assurance: Beyond Detecting Vulnerabilities*, MK/OMG Press, 126.

McDonald, R. (2008). CHS-III, New Considerations for Security Compliance Reliability and Business Continuity, *Conference Papers*, Paper No.08 B1, 978-1-4244-2148.

Mohd Rashid A.H., Loke S.-P., and Ooi K.-B. (2014). Strengthening supply chain risk management for business continuity: A case study approach, *International Journal of Management and Enterprise Development*, 13 (3-4), 278-301.

Naveed, Y. (2012). *Comparison of Virtualization Performance: VMWare and KVM*, Master Thesis, Oslo University College Department of Informatics, Oslo, 15.

Nolan, D. P. (2014b*). Safety and Security Review for the Process Industries Application of HAZOP, PHA, What-If and SVA Reviews*, gulf professıonal publishing, 133-141.

Nolan, D.P. (2014). *Handbook of Fire and Explosion Protection Engineering Principles*, William Andrew, 139.

Nosworthy, J. (2000). A Practical Risk Analysis Approach: Managing BCM Risk, *Computers & Security*, 19 (7), 596-614.

Okeahalam C.C. (2006), Payment systems, risk assessment and business continuity management in South Africa, *International Journal of Risk Assessment and Management*, 6 (4-6), 472-490.

Okumuş, F. (2015). *Taşyünü Üretim Tesisinde Hata Türü Ve Etkileri Analizi İle Taguchi Deney Tasarımının Birlikte Uygulanması*, Yüksek Lisans Tezi, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, Kocaeli.

Öcelan, S. (2014). *Petrokimya Tesislerinde İş Sağlığı Ve Güvenliği İle İlgili Risk Faktörleri Ve Risk Değerlendirmesi*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Rebello, S., and Goyal, N.K. (2010). Software system reliability and safety assessment: An extended FMEA approach, *International Journal of Reliability and Safety*, 4 (4), 366-380.

Rhee, S.J., and Ishii, K. (2003). Using cost based FMEA to enhance reliability and serviceability, *Advanced Engineering Informatics*, 17 (3-4), 179-188.

Ping, P., Xinyue, M., Ping, Y., and Huiling, Z. (2014, November). *Reliability Analysis of Business Continuity Based on SPN in Information System Security Management*, paper presented at Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Guangzhou China.

Rennie, R. A. (1961). The Measurement of Risk, *The Journal of Insurance*, 28 (1), 5.

Roland, E., and Brian, M. (1990). *System Safety Engineering and Management*, John Wiley & Sons, 213-218.

Prasad S. (1991). Improving Manufacturing Reliability in IC Package Assembly Using the FMEA Technique, *IEEE Transactions on Components, Hybrids, and Manufacturing Technology*, 14 (3), 452-456.

Saaty, T. L. (1990). *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*, RWS, 54.

Sadeghi, M., Karbasiyan, M., Navabakhsh M. (2014). Designing a model for reliability improvement with FTA and FMEA techniques on medical gas outlet, *International Journal of Logistics Systems and Management*, 18 (3), 322-342.

Sahebjamnia, N., Torabi, S.A., and Mansouri, S.A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience, *European Journal of Operational Research*, 242 (1), 261-273.

Sakai K., Takaki Y., Sumita J., Saito K., and Miyazaki T. (2010), Use of ICT for risk management and business continuity management and R&D initiatives NTT Technical Review, 8 (1), .

Sawhney, R., Subburaman, K., Sonntag C., Venkateswara Rao P.R., and Capizzi C. (2010). A modified FMEA approach to enhance reliability of lean systems, *International Journal of Quality and Reliability Management*, 27 (7), 832-855.

Sembiring, J. and Siregar, M. H. (2013). A Decision Model for IT Risk Management on Disaster Recovery Center in an Enterprise Architecture Model, *Procedia Technology*, 11,1142-1146.

Sharma, V., Kumari, M., and Kumar, S. (2011). Reliability improvement of modern aircraft engine through failure modes and effects analysis of rotor support system, *International Journal of Quality and Reliability Management*, 28 (6), 675-687.

Silva, M., Gusmao, A., Poleto, T., Silva, L. C., and Costa, A. (2014) "A multi dimensional approach to information security risk management using FMEA and fuzzy theory", *International Journal of Information Management,* 34 (6), 733–740.

Stamatis, D. H. (2003). *Failure mode and effects analysis – FMEA from theory to execution*, ASQC Quality Pres, 28.

Su, C.-T., Lin, H.-C., Teng, P.-W., and Yang, T. (2014). Improving the reliability of electronic paper display using FMEA and Taguchi methods: A case study, *Microelectronics Reliability*, 54 (6-7), 1369-1377.

Şamur, M. (2005). *Otomotiv Servislerinde FMEA Ve FTA Hata Önleme Tekniklerinin Uygulanması*, Yüksek Lisans Tezi, Marmara Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Şen, S. (2015). *Kentiçi Raylı Sistemlerde Hat Bakımlarının Planlanması, Yönetimi Ve Risk Değerlendirmesi*, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Şener, Ç. (2014). *Reklam Mecrası Seçimi: Hızlı Tüketim Malları Sektöründe AHS Yöntemi İle Bir Uygulama*, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Tammineedi R.L. (2010). Business continuity management: A standards-based approach, *Information Security Journal*, 19 (1), 36-50.

Tanrıverdi, N. (2013). , *Kimyasal Proses Endüstrisi İçin Risk Değerlendirme*, Yüksek Lisans Tezi, Ankara Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Taş, Y. (2010). *Hata Türü Ve Etkileri Analizi (FMEA) Tekniğinin Mobilya Endüstrisine Yönelik Uygulaması*, Yüksek Lisans Tezi, İstanbul Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Tatar, N. (2015). *Bilgi Güvenliği Standartlarının Analitik Hiyerarşi Prosesi Yaklaşımı İle Karşılaştırılması*, Yüksek Lisans Tezi, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Tunçelli, S. (2006). *Helikopter Tasarım Sürecinde Pilot Koltuğu Tasarım Kavram Hata Türü Ve Etkileri Analizi (HTEA)*, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Türk Standartlar Enstitüsü. (2013). *İş Sürekliliği Yönetim Sistemi-Gereksinimler* Ankara: TSE, 1-19.

Türk Standartlar Enstitüsü. (2014). *Bilgi ve İletişim Teknolojileri için İş Sürekliliği Yönergeleri*, Ankra:TSE, 1-29.

Ünlü, T. (2014). *Mimarları Etkileyen Demotivasyon Kriterlerinin Analitik Hiyerarşi Proses(AHP) Ve Analitik Ağ Prosesi(ANP) İle Ağırlıklandırılması*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Walker A. (2006). Business continuity and outsourcing - moves to take out the risk, *Network Security*, 2006 (5), 15-17.

Yang Z., Zhu Y., Ren H., and Zhang Y. (2015). Comprehensive reliability allocation method for CNC lathes based on cubic transformed functions of failure mode and effects analysis, *Chinese Journal of Mechanical Engineering (English Edition)*, 28 (2), 315-324.

Yakın, İ. (2015). *Demiryolu Sinyalizasyonunda Güvenilirlilik Emre Amadelik Sürdürülebilirlik Ve Emniyet (RAMS) Yönetimi Ve FMEA - FTA Analizi Uygulaması*, Yüksek Lisas Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Yılmaz, S. (2006). *Uçak Seçim Kriterlerinin Değerlendirilmesinde AHP Ve Bulanık AHP Uygulaması*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Yuan, J., and Chou, S.-B. (1986). Boolean algebra method to calculate network system reliability indices in terms of a proposed FMEA, *Reliability Engineering*, 14 (3), 193-203.

Yuan, J. (1985). A strategy to establish a reliability model with dependent components through FMEA, *Reliability Engineering*, 11 (1), 37-45.

Zafiropoulos, E.P., and Dialynas, E.N. (2005). Reliability prediction and failure mode effects and criticality analysis (FMECA) of electronic devices using fuzzy logic, *International Journal of Quality and Reliability Management*, 22 (2), 183-200.

Zahir, M.S. (1991). Incorporating The Uncertainty of Decision Judgements in The Analytic Hierarchy Process, *European Journal of Operational Research*, 53 (2), 206-216.

# EKLER

EK-1. FMEA Risk Analiz Tablosu

| **Sistem:** <Uygulama2> | | | **Alt Sistem:** Soğutma Alt Yapısı | | | **Mod/Safha:** Operasyon | | | **FMEA Analizi** |
|---|---|---|---|---|---|---|---|---|---|
| **No Bileşen** | **Potansiyel Başarısızlık Modu** | **Potansiyel Etkileri** | **Uygulama Üzerindeki Etkiler** | **Ciddiyet** | **Nedensel Faktörler** | **Olasılık** | **Mevcut Kontroller** | **Risk** | **Önerilen Kontroller** |
| 1 Kondenser | Yüksek Basınçlı Akışkan | -Kondenserin kapanması<br>-Kompresörün arızalanması<br>-Veri merkezinin ısınması | Uygulama yavaşlar.<br>Uzun sürede hizmet durur | 6 | -Basınç koruma elamanının bozulması<br>-Fazla akışkan/gaz dolumu | 7 | -Yedeklilik<br>-Bakım | 42 | -Gaz veya sıvının miktarının kontrolü<br>-Basınç koruma elemanına bakım yapma |
| | Yoğunlaştıramama | -Kompresörün arızalanması<br>-Veri merkezinin ısınması | Uygulama yavaşlar.<br>Uzun sürede hizmet durur | 5 | -Direk ısıya maruz kalma<br>-Dar havasız alanlara monte etme | 7 | -Yedeklilik<br>-Bakım | 35 | -Sundurma yapılabilir |
| | Tıkanma / Tıkanıklık | -Kompresörün arızalanması<br>-Veri merkezinin ısınması | Uygulama yavaşlar.<br>Uzun sürede hizmet durur | 5 | -Yanlış seçilen montaj yeri | 5 | -Yedeklilik<br>-Bakım | 25 | -Mevsim şartlarına göre daha sık temizleme |
| 2 Kompresör | Çalışmıyor hava akışı yok | - Veri merkezi ısınır<br>-Sunucu ve diskler ısınır | Uygulama yavaşlar<br>Uzun sürede hizmet durur | 6 | -Elektrik Kesik<br>-Termik atması<br>-Kesici Şalter kapalı | 4 | -Yedeklilik | 24 | -Sürekli fiziksel kontrol<br>-Nöbet sistemi |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 2 Kompresör (devam) | Sürekli Çalışma | -Soğutma yapamaz<br>- Veri merkezi ısınır<br>-Sunucu ve diskler ısınır | Uygulama yavaşlar<br>Uzun sürede hizmet durur | 4 | -Eksik soğutucu akışkan<br>-Termostatın yanlış ayarlanması<br>-Yoğunlaşmayan gazlar | 6 | -Yedeklilik | 24 | -Sürekli fiziksel kontrol<br>-Nöbet sistemi |
| | Mekanik Arıza | Sunucu ve diskler ısınır | Uygulama yavaşlar<br>Uzun sürede hizmet durur | 5 | Yoğunlaşmayan gazların varlığı<br>-Kondenserden sıvı taşması<br>-Zararlı kimyasal eriyikler<br>- Motorun rulmanı sıkışmış<br>- Dönüş hattından yüksek sıcaklıkta sıvı girişi<br>-Liqid haldeki soğutucunun kompresöre girmesi<br>-Terminale yanlış bağlantı | 5 | -Yedeklilik | 25 | Yok |
| 3 Evoporatör | Isı alışverişi yapamama | - Veri merkezi ısınır<br>-Sunucu ve diskler ısınır | Uygulama yavaşlar<br>Uzun sürede hizmet durur | 5 | -Tıkanma<br>-Kirlenme<br>-Korozyon<br>-Borudaki kaçak<br>-Fanın bozulması | 6 | 3 Aylık periyodik bakım<br>-Yedeklilik | 30 | Yok |

EK-1. (devam) FMEA Risk Analiz Tablosu

| **Sistem:** <Uygulama2> | | | **Alt Sistem:** Enerji Alt Yapısı | | | **Mod/Safha:** Operasyon | | | **FMEA Analizi** |
|---|---|---|---|---|---|---|---|---|---|
| **No Bileşen** | **Potansiyel Başarısızlık Modu** | **Potansiyel Etkileri** | **Uygulama Üzerindeki Etkiler** | **Ciddiyet** | **Nedensel Faktörler** | **Olasılık** | **Mevcut Kontroller** | **Risk** | **Önerilen Kontroller** |
| 4 UPS | Güç çıkışı yok | Sisteme güç gitmez | Elektrik kesilir kesilmez uygulama hizmet veremez | 9 | -İnvertör sigortası atmış<br>-Emniyet sigortası atmış<br>-Çıkışın kısa devre olması | 4 | -Yedeklilik<br>-Periyodik bakım<br>-Otomasyon kontrolü | **36** | -STS anahtarı |
| | Elektrik kesildikten kısa süre sonra kapanması | Sisteme güç gitmez | Elektrik kesildikten kısa süre sonra uygulama hizmet veremez | 9 | -Ömrü azalmış akü<br>-Çok sayıda yeniden şarj olma | 5 | -Yedeklilik<br>-Bakım | **45** | Dinamik UPS sistemi ya da hibrit UPS sistemi |
| | Elektrik kesilir kesilmez kapanması | Sisteme güç gitmez | Elektrik kesildikten kısa süre sonra uygulama hizmet veremez | 9 | Aküler devre dışı | 3 | -Yedeklilik<br>-Bakım | **27** | Yok |
| | Sadece By-Pass modunda çalışması ve yükün UPS üstüne geçmemesi. | Sisteme güç gitmez | Elektrik kesilir kesilmez uygulama hizmet veremez | 8 | UPS çıkışına bağlı yük cihaz gücünün üzerinde | 4 | -Yedeklilik | **32** | Yok |
| | UPS devreye girmiyor. | Sisteme güç gitmez | Elektrik kesilir kesilmez uygulama hizmet veremez | 9 | Bozuk geçiş anahtarı | 2 | -Yedeklilik<br>-Bakım | **27** | Çift besleme |
| | Şarj olmama | Sisteme güç gitmez | Elektrik kesilir kesilmez uygulama hizmet veremez | 9 | -Redresör arızası (AC -> DC)<br>-Şarj devresinin bozulması | 4 | -Yedeklilik<br>-Bakım | **36** | Yok |
| 5 Jeneratör | Alternatör gerilim üretmez | Sisteme güç gitmez | Uygulama hizmet veremez | 4 | -Sigorta atmış<br>-İkaz trafosu yanmış olabilir<br>-Manyetizma gitmiş olabilir | 3 | -Yedeklilik<br>-Bakım | **12** | Yok |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 5 Jeneratör (devam) | Düşük ya da dalgalı gerilim | Sistem bileşenleri arızalanır | Uygulama hizmet veremez | 3 | -Motor devir ayarı hatalı<br>-Sargılarda kopukluk | 2 | -Yedeklilik<br>-Bakım<br>-UPS | **6** | Yok |
| | Motor kısa süre sonra durur | Sisteme güç gitmez | Motor durduktan sonra uygulama hizmet veremez | 3 | Yakıt devresi tıkalı ya da hava var<br>-Yakıt filtresi tıkalı<br>-Enjektörler ayarsız<br>-Emme kanalları tıkalı | 3 | -Yedeklilik<br>-Bakım<br>-UPS | **9** | Yok |
| 6 Şebeke Trafosu | Güç dalgalanması | Sistem bileşenleri arızalanır | Uygulama hizmet veremez | 4 | -Yıldırım<br>-Kısa devre<br>-Topraklama yok | 5 | -UPS<br>-Topraklama | **20** | Yok |
| | Yanlış şalterin kapatılması | Sisteme güç gitmez | UPS devreye girer Kısa süre sonra uygulama hizmet veremeyebilir | 4 | -Etiketleme yok | 4 | -Etiketleme | **16** | -Prosedür oluşturma<br>-Dedike personel oluşturma |
| | Sigorta atması | Sisteme güç gitmez | UPS devreye girer Kısa süre sonra uygulama hizmet veremeyebilir | 5 | -Bireysel su ısıtıcı vb. kullanma<br>-Aşırı yük<br>- Kısa devre | 7 | -Uyarı | **35** | -Uyarılar arttırılabilir ve kullanıcılar bilinçlendirilebilir |
| 6.1 Şebeke tesisatı | Elektrik iletmeme | Sisteme güç gitmez | Uygulama hizmet veremeyebilir | 10 | -Kopukluk<br>-Tesisatın yanması | 3 | -Bakım<br>-Kontrol<br>-Paratoner testi | **30** | Su ve kanalizasyon tesisatının ayrıştırılması |

EK-1. (devam) FMEA Risk Analiz Tablosu

| **Sistem:** <Uygulama2> | | | **Alt Sistem:** Uygulama Alt Sistemi | | | **Mod/Safha:** Operasyon | | | **FMEA Analizi** |
|---|---|---|---|---|---|---|---|---|---|
| **No Bileşen** | **Potansiyel Başarısızlık Modu** | **Potansiyel Etkileri** | **Uygulama Üzerindeki Etkiler** | **Ciddiyet** | **Nedensel Faktörler** | **Olasılık** | **Mevcut Kontroller** | **Risk** | **Önerilen Kontroller** |
| 7 Uygulama Yazılımı | Metotlar / Fonksiyonlar başlamaz | Uygulama başlamaz | Uygulama hizmet vermez | 5 | Eksik kütüphane | 5 | Yok | **25** | Kontrol listesi oluşturulabilir |
| | Güvenirliğinin kaybolması | Veri değiştirme | Uygulama yanlış hizmet verir | 10 | SQL injection | 2 | Oracle Xml Gateway | **20** | Yok |
| | Metotlar / Fonksiyonlar çalışmaz | Uygulama çalışmaz | Uygulama hizmet vermez | 5 | -Web servislerin DNS adı yerine IP adresi girilmiştir.<br>-Fonksiyonel test yapılmamış. | 7 | DNS adları tercih ediliyor | **35** | Değişiklik yönetimi |
| | Metot/fonksiyon gecikmeli çalışır | Uygulama yavaşlar | Uygulama gecikmeli hizmet verir | 5 | Yazılım Kodu Parametrik SQL içerir | 5 | SQL optimizasyonu<br>-Transaction Cost hesaplaması | **25** | Tasarım yeniden gözden geçirilmeli<br>-Kod anallizi yapılmalı |
| | Metotlar yanlış çalışır | Metotlar yanlış sonuç üretir | Uygulama hatalı hizmet verir | 7 | -Yanlış analiz<br>-Yanlış tasarım - Yanlış algoritma oluşturma<br>-Hatalı sabit değerler ve parametreler<br>-Yanlış veri tipi dönüştürme<br>-Formüllerin yanlış yazılması<br>-Fonksiyonların yanlış kullanımı | 7 | | **49** | -Analiz<br>-Tasarım<br>-Test<br>-Eğitim |
| | Metotların kırılması beklenmedik şekilde sonlanması | Uygulama sürekli çalışamaz | Uygulama sürekli hizmet veremez | 5 | -Yazım yanlışı<br>-Yanlış algoritma<br>-Validasyon (doğrulama) yapılmaması | 6 | | **30** | -Kod yazma standardı<br>-Test<br>-Eğitim |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 8 Yazılımcı | Hastalanma | Problemler zamanında giderilemeyebilir | Uygulama tam hizmet veremez | 3 | -Aşırı iş yükü<br>-Olumsuz çalışma şartları<br>-Zayıf bünye | 7 | Yok | **21** | Yok |
| | İşe geç gelme | | Uygulama hizmet verir | 1 | -Ulaşım servisinin kaza yapması<br>-Düzensiz iş planı | 10 | Yok | **10** | Yok |
| | İşten ayrılma | -Problemler giderilemez<br>-Değişiklik yapılamaz | Uygulama tam hizmet veremez | 5 | -Aşırı iş yükü<br>-Düşük maaş<br>-Motivasyon eksikliği | 6 | Yok | **30** | -Özlük haklarında iyileştirme<br>-Çalışma şartlarının iyileştirilmesi<br>-Düzenli iş planı ve isteklendirme |
| | Yanlış kod yazma | -Metotlar yanlış çalışır<br>-Metotlar çalışmaz | -Uygulama hizmet veremez<br>-Uygulama hatalı hizmet verir | 8 | -Yetersiz eğitim<br>-Eksik veya analiz | 5 | Yok | **40** | Kapasite planlaması<br>-Eğitim<br>-Prosedür oluşturma<br>-Kod yazma standardı ve kuralları<br>-Kapasite planlama |
| | Emekli Olma | -Problemler giderilemez<br>-Değişiklik yapılamaz | Uygulama sürekli ve tam hizmet veremez | 5 | -Emeklilik süresinin dolması<br>-Yaşlılık | 3 | Yok | **15** | |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 9 WAS Application Sunucusu | İsteklere cevap verememe | Kullanıcılar Uygulamaya Giremez | Uygulama Çalışmaz | 5 | -Aşırı istek<br>-Web Konteyner dolması | 7 | -İzleme<br>-Yedeklilik | **35** | |
| | Yanlış yapılandırılma | Uygulama Sunucusu Çalışmaz | Uygulama çalışmaz | 6 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 6 | -İzleme<br>-Yedeklilik | **36** | -Değişiklik yönetimi<br>-Konfigürasyon yönetimi<br>-Prosedür oluşturma |
| | Eksik yapılandırma | -Uygulama Sunucusu Çalışmaz -Kullanıcılar Uygulamaya Giremez | -Uygulama çalışmaz<br>-Uygulama Erişilmez Olur | 6 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü | 6 | -İzleme<br>-Yedeklilik | **24** | -Değişiklik yönetimi<br>-Konfigürasyon yönetimi<br>-Prosedür oluşturma |
| | Belleğin dolması | Kullanıcılar Uygulamaya Giremez | Uygulama hizmet vermez | 5 | Çöp toplayıcı (grabage collector) çalışmaz | 3 | -İzleme<br>-Yedeklilik | **15** | -Konfigürasyon yönetimi<br>-Prosedür oluşturma<br>-Kontrol listesi |
| | WebSphere Server1 Node1 Başlayamaz | WAS sunucusu başlamaz | Uygulama hizmet vermez | 5 | Ani sistem çökmesi sonucu | 7 | Yok | | Kontrol noktası oluşturulmalı: server1.pid dosyasının silinmesi |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 10 İşletim Sistemi | Virüs bulaşması | Sunucu Yavaşlar | Uygulama Yavaşlar | 3 | -Kullanıcı Hatası<br>-Antivirüs eksik | 3 | Yok | **9** | Antivirüs kurulması |
| | Çökmesi | Sunucu çalışmaz | Uygulama hizmet vermez | 8 | -Yazılım hatası<br>-Virüs bulaşması<br>-Donanım arızası | 2 | Yedeklilik | **16** | -Antivirüs kurulmalı<br>-Test ortamı hazırlanmalı<br>-Sıklaştırma politikaları oluşturulmalı |
| | Yanlış yapılandırılma | Sunucu çalışmaz | Uygulama hizmet vermez | 5 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 4 | Yedeklilik | **20** | -Prosedür oluşturulmalı<br>-Personelin motivasyonu arttırılmalı<br>-Düzenli eğitim verilmeli |
| | Bellek Hatası | Sunucu hata verir | Uygulama hizmet vermez | 3 | Sistem belleğinde hata tespiti ya da düzeltmesi olmadan çalışan yazılımlar (Leakage) | 3 | Yedeklilik | **9** | -Sıklaştırma politikası ve kontrol listesi oluşturulmalı<br>-Test prosedürleri oluşturulmalı |
| | Donması | Sunucu yavaşlar | Uygulama çok yavaş hizmet verir sonrasında durur | 3 | -Bellek Hatası<br>-Isınma<br>-Fazla sayıda uygulama | 3 | -Yedeklilik<br>-Soğutma sistemi | **9** | -Sıklaştırma politikası ve kontrol listesi oluşturulmalı |
| | Çalışmama | Sunucu çalışmaz | Uygulama hizmet vermez | 8 | -Donanım arızası<br>-Desteğinin bitmesi<br>-Başarısız yama yüklemesi<br>-Eksik Sürücü<br>-Virüs bulaşması | 2 | -Yedeklilik<br>-Bakım destek anlaşmaları | **16** | -Yazılım yönetimi prosedürü oluşturulmalı |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 11 Sunucu Donanımı | Fiziksel Arıza | Sunucu çalışmaz | Uygulama hizmet vermez | 7 | -Sıvı ile temas<br>-Yüksek nem<br>-Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Eskime<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 2 | Yedeklilik | **14** | -Bakım<br>-Yedek malzeme |
| | Yavaşlama | Sunucu yavaşlar | Uygulama çok yavaş hizmet verir sonrasında durur | 3 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | 3 | Yedeklilik | **9** | -Bakım |
| | Çalışmama | Sunucu çalışmaz | Uygulama hizmet vermez | 3 | -Güç girişi yok<br>-Temassızlık<br>-Fiziksel arıza<br>-Yanlış montaj | 2 | Yedeklilik | **6** | -Kontrol listesi<br>-Düzenli eğitim verilmesi |
| | Bellek hatası | Sunucu hata verir | Uygulama hizmet vermez | 3 | - Sistem belleğinde hata tespiti ya da düzeltmesi olmadan çalışan yazılımlar | 2 | Donanım bellek hatası tespiti | **6** | -Yedek RAM bulundurulmalı |
| | Kaynak çakışması Kesme isteği çakışması | Sunucu hata verir | Uygulama hizmet vermez | 3 | -Uyumsuz bileşen<br>-Çevre bileşenlerin aynı kesme isteği sinyalini veya DMA kanallarını veya giriş çıkış adreslerini kullanması | 2 | Yok | **6** | IRQ kanalını değiştir |

EK-1. (devam) FMEA Risk Analiz Tablosu

| **Sistem:** <Uygulama2> | | | **Alt Sistem:** Ağ Alt Sistemi | | | **Mod/Safha:** Operasyon | | | **FMEA Analizi** |
|---|---|---|---|---|---|---|---|---|---|
| **No Bileşen** | **Potansiyel Başarısızlık Modu** | **Potansiyel Etkileri** | **Uygulama Üzerindeki Etkiler** | **Ciddiyet** | **Nedensel Faktörler** | **Olasılık** | **Mevcut Kontroller** | **Risk** | **Önerilen Kontroller** |
| 12 Güvenlik Duvarı | Fiziksel arıza | -Ağ bağlantısı kesilir | Uygulamaya erişim yapılamaz | 7 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Eskime<br>-Sıvı ile temas<br>-Yüksek nem<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 5 | Yedeklilik | **35** | -Acil Müdahale ekibi<br>-Yedek modül stoğu |
| | Yanlış yapılandırılma | -Erişim isteğini engeller<br>-Ağ bağlantısı kesilir | -Uygulama hizmet vermez<br>-Uygulamaya erişilmez | 5 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 7 | Yok | **35** | -Konfigürasyon yönetimi<br>-Değişiklik yönetimi<br>-Prosedür oluşturulmalı<br>-Test ortamı oluşturulmalı |
| | Yavaşlama | Güvenlik duvarı yavaşlar | Uygulama yavaş hizmet verir | 2 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | 8 | İzleme | **16** | -Yük testleri<br>-Periyodik bakım<br>-Yedeklilik arttırılmalı |
| | Donma / Durma | -Erişim isteği engellenir<br>-Ağ bağlantısı kesilir | -Uygulama hizmet vermez<br>-Uygulamaya erişilmez | 7 | -DDOS atağı | 4 | -ISP'den DDOS hizmeti alınmakta | **28** | -Kara liste oluşturulmalı ve güncellenmeli |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 12 Güvenlik Duvarı (devam) | Başarısız firmware yükseltmesi | Firewall çalışmaz | Uygulamaya erişilemez | 7 | -Güç kesintisi<br>-Isınma<br>-Yanlış sürüm | 2 | Yok | **14** | Test ortamı |
| | Başarısız SSL bağlantısı | -Bağlantı kurulamaz | Uygulamaya erişim yapılamaz | 6 | Firewall'a değişen anahtar (key) girilmemesi<br>-Başarısız SSL handshake | 6 | Yok | **36** | -Değişiklik yönetimi<br>-Kurumlar arası protokol ekine ilgili madde eklenmeli |
| 13 Yönlendirici | Fiziksel arıza | -Ağ bağlantısı kesilir | Uygulamaya erişim yapılamaz | 7 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Eskime<br>-Sıvı ile temas<br>-Yüksek nem<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 5 | Yok | **35** | Yedeklilik |
| | Yanlış yapılandırma | -Erişim isteğini engeller<br>-Ağ bağlantısı kesilir | -Uygulama hizmet vermez<br>-Uygulamaya erişilmez | 6 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 6 | Yok | **36** | -Eğitim<br>-Test ortamının oluşturulması<br>-Değişiklik yönetimi<br>-Yedeklilik<br>-Konfigürasyon yönetimi |
| | Yavaşlama | Yönlendirici yavaşlar | Uygulama yavaş hizmet verir | 3 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | 8 | Yok | **24** | -Yedeklilik<br>-Yönlendirici modülünü arttırma |
| | Başarısız firmware yükseltmesi | Yönlendirici çalışmaz | Uygulamaya erişilemez | 7 | -Güç kesintisi<br>-Isınma<br>-Yanlış sürüm | 1 | Yok | **7** | Yok |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 13 Yönlendirici (devam) | Yönlendirme protokol uyuşmazlığı | Ağ trafiğinin kesilmesi | Uygulamaya erişilemez | 7 | Farklı marka cihaz kullanımı | 4 | Yok | **28** | -Aynı marka network cihazı kullanılmalı |
| 14 Yük Dağıtıcı | Fiziksel arıza | -Ağ bağlantısı kesilir | Uygulamaya erişim yapılamaz | 7 | -Sıvı ile temas<br>-Yüksek nem<br>-Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Eskime<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 5 | Yedekli yapı | **35** | Yedeklilik |
| | Yanlış yapılandırılma | -Ağ bağlantısı kesilir<br>-Erişim kaybolur | -Uygulama hizmet vermez<br>-Uygulamaya erişilmez | 6 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 7 | | **42** | -Eğitim<br>-Test ortamının oluşturulması<br>-Değişiklik yönetimi<br>-Yedeklilik<br>-Konfigürasyon yönetimi |
| | Yavaşlama | Yük dağıtıcı yavaşlar | Uygulama yavaş hizmet verir | 4 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | 7 | -Yedeklilik | **28** | Bakım |
| | Başarısız firmware yükseltmesi | Yük dağıtıcı çalışmaz | Uygulamaya erişilemez | 6 | -Güç kesintisi<br>-Isınma<br>-Yanlış sürüm | 1 | | **6** | Yok |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 15 Switch / Anahtar (Omurga ve Kenar) | Fiziksel arıza | -Ağ bağlantısı kesilir | Uygulamaya erişim yapılamaz | 7 | -Toz/Kir<br>-Sıvı ile temas<br>-Yüksek nem<br>-Isınma<br>-Yıpranma<br>-Eskime<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 6 | Yok | **42** | -Yedeklilik<br>-Acil müdahale ekibi<br>-Yedek modül malzeme stoğu |
| | Yanlış yapılandırılma | -Ağ bağlantısı kesilir | -Uygulamaya erişilmez | 6 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 7 | Yok | **42** | -Eğitim<br>-Prosedür<br>-Değişiklik yönetimi<br>-Konfigürasyon eğitimi<br>-Test ortamı |
| | Yavaşlama | Switch yavaşlar | Uygulama yavaş hizmet verir | 4 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | 8 | Yok | **28** | -Modül arttırılır<br>-Bakım<br>-Düzenli ve sistematik izleme yapılması |
| | Başarısız firmware yükseltmesi | Switch çalışmaz | Uygulamaya erişilemez | 7 | -Yanlış prosedürün izlenmesi<br>-Güç kesintisi<br>-Isınma<br>-Yanlış firmware sürümü | 5 | Yok | **35** | -Prosedür oluşturulmalı<br>-Yedeklilik<br>-Test ortamı<br>-Değişiklik yönetimi |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 16 Kablo | Kopması / Kesilmesi | Erişimin kaybedilmesi | Uygulamaya erişilemez | 4 | -Sabotaj<br>-Yanlışlıkla kopma | 1 | | **4** | Kabloların kanallardan geçirilmesi |
| | Fiziksel deformasyon | Veri paketlerinde kayıp yaşanır | Uygulama hizmeti yavaşlar veya başarısız işlemler meydana gelir | 3 | -Isı farkı<br>-Gerilme<br>-Basınç | 2 | | **6** | Kabloların kanallardan geçirilmesi |
| | Parazit oluşması | Veri paketlerinde kayıp yaşanır | Uygulama hizmeti yavaşlar veya başarısız işlemler meydana gelir | 3 | -Elektrik kabloları ile yakın geçmesi<br>-İzolasyon olmaması | 3 | | **9** | Veri kablosunun elektrik kanallarından farklı kanallardan geçirilmesi veya izolasyonu |
| | Sinyalin zayıflaması | Veri paketlerinde kayıp yaşanır | Uygulama hizmeti yavaşlar veya başarısız işlemler meydana gelir | 3 | Normalden uzun kablo kullanımı | 1 | | **3** | Kontrol oluşturulmalı |
| | Yerinden Çıkma | Erişimin kaybedilmesi | Uygulamaya erişilemez | 4 | -Farkında olmadan ya da istemsizce çıkarılması | 2 | | **8** | Uyarı mesajları |

EK-1. (devam) FMEA Risk Analiz Tablosu

| **Sistem:** <Uygulama2> | | | **Alt Sistem:** Veritabanı Alt Sistemi | | | **Mod/Safha:** Operasyon | | | **FMEA Analizi** |
|---|---|---|---|---|---|---|---|---|---|
| **No Bileşen** | **Potansiyel Başarısızlık Modu** | **Potansiyel Etkileri** | **Uygulama Üzerindeki Etkiler** | **Ciddiyet** | **Nedensel Faktörler** | **Olasılık** | **Mevcut Kontroller** | **Risk** | **Önerilen Kontroller** |
| 17<br>VTYS Yazılımı | Yavaşlama | -Kullanıcılar uygulamaya giremez<br>- Kullanıcı memnuniyetsizliği | Uygulama yavaş hizmet verir | 5 | -Aşırı istek bağlantı isteği<br>-Uygulama içindeki VT bağlantılarının sonlandırılmaması gibi yazılım içindeki elverişsiz SQL kodu<br>-REORG yapılmaması | 6 | VT bakımı | **30** | -İş (mevzuat) birimleriyle kapasite planlaması yapılmalı<br>-SQL optimizasyonu<br>-Düzenli VT bakımı |
| | Güvenirliğinin kaybolması | -Değişmiş, yanlış veya bozuk veri<br>- Verinin Silinmesi | Uygulama hatalı hizmet verir<br>- Uygulama hizmet veremez | 10 | -SQL injection<br>-Siber saldırı | 7 | Oracle Xml Gateway kullanılmakta | **70** | *Siber güvenlik tedbirleri<br>-Yedeklerin daha kısa süreyle online yedeklenmesi<br>-VT güvenlik duvarı |
| | Yanlış yapılandırma | Veritabanına erişilemez | Uygulama hizmet veremez | 5 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 6 | | **30** | -Eğitim<br>-Motivasyon oluşturma<br>-Değişiklik yönetimi<br>-Konfigürasyon yönetimi<br>-Detaylı (uyarıları da içeren) prosedürler oluşturulmalı |
| | Başarısız yama yüklemesi | VTYS çalışmaz | Uygulama hizmet veremez | 5 | -Güç kesintisi<br>-Isınma<br>-Prosedüre uyulmaması<br>-Yanlış sürüm | 6 | | **30** | -Eğitim<br>-Motivasyon oluşturma<br>-Değişiklik yönetimi<br>-Detaylı (uyarıları da içeren) yama yönetimi prosedürü oluşturulmalı |
| | Tablonun kilitlenmesi | VTYS tabloya yazamaz | -Uygulama yeni kayıt yapamaz<br>-Uygulama hizmet veremez | 7 | -Uygulama içinde yanlış SQL kodu | 6 | | **42** | -SQL optimizasyonu<br>-Uygulamaların VT tasarımlarının gözden geçirilmesi |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 17 VTYS Yazılımı (devam) | Table Space ya da diskin dolması | VTYS tabloya yazamaz | -Uygulama yeni kayıt yapamaz- Uygulama hizmet veremez | 2 | -Veritabanı bakımının vaktinde yapılmaması | 7 | | **14** | -Otomatik büyüme table space çekilmesi |
| | Okuma yazmada fazla gecikme | -Kullanıcılar uygulamaya giremez - Kullanıcı memnuniyetsizliği | Zaman aşımı nedeniyle uygulama başarısız işlem | 4 | -Düşük hızlı diskler -Düşük RAID seviyesi -Fazla Veri | 4 | Hızlı disk kullanımı | **16** | -Hızlı disk kullanımı teknik şartnamelerde zorunluluk olarak belirtilmeli -Sistem kurma çalışmalarında RAID türlerinden performanslı olanın (R10 gibi) tercih edilmesi şart koşulmalı |
| 18 İşletim Sistemi | Çalışmama | -Sunucu çalışmaz | Uygulama hizmet vermez | 7 | -Donanım arızası -Desteğinin bitmesi -Eksik Sürücü | 3 | Yedeklilik | **21** | Yok |
| | Başarısız yama yüklemesi | Sunucu çalışmaz | Uygulamaya erişilemez | | -Güç kesintisi -Isınma -Yanlış sürüm | | | | -Değişiklik yönetimi -Konfigürasyon yönetimi -Detaylı (uyarıları da içeren) yama yönetim prosedürü oluşturulmalı |
| | Yanlış yapılandırılma | Sunucu çalışmaz | Uygulama hizmet vermez | 6 | -Yetersiz eğitim -Prosedür yok ya da eksik -Konfigürasyon yönetimi yok -Motivasyon eksikliği -Aşırı iş yükü -Dalgınlık | 5 | | **30** | -Eğitim -Motivasyon oluşturma -Değişiklik yönetimi -Konfigürasyon yönetimi -Detaylı (uyarıları da içeren) prosedürler oluşturulmalı |
| | Çökmesi | Sunucu çalışmaz | Uygulama hizmet veremez | 7 | -Donanım arızası -Yazılım hatası -Virüs bulaşması | 3 | Yedeklilik | **21** | Yok |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 19 Sunucu Donanımı | Fiziksel Arıza | -VTYS çalışmaz | Uygulama hizmet vermez | 7 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Eskime<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 2 | Bakım destek anlaşması | **14** | Yedeklilik |
| | Yavaşlama | -Kullanıcılar uygulamaya giremez<br>- Kullanıcı memnuniyetsizliği | Uygulama yavaş hizmet verir | 6 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | 3 | Bakım | **18** | Sıcaklık ve nem değerlerinin kontrolü |
| | Başarısız firmware yükseltmesi | Sunucu çalışmaz | Uygulamaya erişilemez | 7 | -Güç kesintisi<br>-Isınma<br>-Yanlış sürüm | 4 | | **28** | -Değişiklik yönetimi<br>-Konfigürasyon yönetimi<br>-Detaylı (uyarıları da içeren) yama yönetim prosedürü oluşturulmalı |
| | Çalışmama | Sunucu çalışmaz | Uygulama hizmet vermez | 7 | -Temassızlık<br>-Fiziksel arıza<br>-Yanlış montaj | 2 | Yedeklilik | **14** | -Kontrol listesi<br>-Düzenli eğitim verilmesi |
| | Bellek hatası | Sunucu hata verir | Uygulama hizmet vermez | 7 | -Temassızlık<br>- Sistem belleğinde hata tespiti ya da düzeltmesi olmadan çalışan yazılımlar | 2 | Donanım bellek hatası tespiti | **14** | -Yedek RAM bulundurulmalı |
| | Kaynak çakışması Kesme isteği çakışması | Sunucu hata verir | Uygulama hizmet vermez | 7 | -Uyumsuz bileşen<br>-Çevre bileşenlerin aynı kesme isteği sinyalini veya DMA kanallarını veya giriş çıkış adreslerini kullanması | 1 | Yok | **7** | IRQ kanalını değiştir |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 20<br>DBA Admin<br>(VT Yöneticisi) | Sağlık sorunları | -Sorunlara vaktinde müdahale edilemez | Uygulama tam ve doğru bir şekilde hizmet veremeyebilir | 5 | -Aşırı iş yükü<br>-Olumsuz çalışma şartları<br>-Zayıf bünye | 4 | | **20** | -Yedekli personel arttırılmalı<br>-Uzaktan erişim |
| | İşe Geç Gelme | -Sorunlara vaktinde müdahale edilemez | Uygulama tam ve doğru bir şekilde hizmet veremeyebilir | 5 | -Ulaşım servisinden kaynaklanan sorunlar<br>-Düzensiz iş planı<br>-Motivasyon eksikliği<br>-Kötü hava şartları | 5 | | **25** | -Nöbet |
| | İşten Ayrılma | -Problemler giderilemez<br>-Değişiklik yapılamaz<br>-Sorunlara vaktinde müdahale edilemez | Uygulama tam ve sürekli hizmet veremez | 5 | -Aşırı iş yükü<br>-Düşük maaş<br>-Motivasyon eksikliği<br>-Askerlik<br>-Emekli olma | 5 | | **25** | -Özlük hakları<br>-Çalışma şartlarının iyileştirilmesi<br>-Prosedürler oluşturularak kişiye bağımlılığın azaltılması<br>-Yedekli personel<br>-Konfigürasyon yönetimi |
| | Yanlış işlem yapma | -VTYS çalışmaz | -Uygulama hizmet veremez | 6 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 6 | | **36** | -Eğitim<br>-Gereksiz iş yükünün azaltılması<br>-Yapılan işlerin prosedürünün oluşturulması<br>-Konfigürasyon yönetimi |

EK-1. (devam) FMEA Risk Analiz Tablosu

| **Sistem:** <Uygulama2> | | | **Alt Sistem:** Veri Depolama Alt Sistemi | | | **Mod/Safha:** Operasyon | | | **FMEA Analizi** |
|---|---|---|---|---|---|---|---|---|---|
| **No Bileşen** | **Potansiyel Başarısızlık Modu** | **Potansiyel Etkileri** | **Uygulama Üzerindeki Etkiler** | **Ciddiyet** | **Nedensel Faktörler** | **Olasılık** | **Mevcut Kontroller** | **Risk** | **Önerilen Kontroller** |
| 21<br>SAN Switch | Fiziksel Arıza | -VTYS sunucusunun veri depolama ünitesine bağlantısı kesilir. | Uygulama hizmet vermez | 9 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Eskime<br>-Yüksek güç girişi<br>-Sıvı ile temas<br>-Yüksek nem<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 1 | -Yeklilik<br>-Soğutma sistemi | **9** | -Mesh toploji ile çoklu yol oluşturulabilir ve yapı istendiği kadar genişletilebilir. |
| | Yanlış yapılandırma | -VTYS sunucusunun veri depolama ünitesine bağlantısı kesilir. | Uygulama hizmet veremez | 8 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 5 | SAN Switchler arasındaki otomatik yapılandırma senkronizasyon kapalı | **40** | -İleri SAN yönetim eğitimi<br>-Yapılandırma prosedürü oluşturulmalı<br>-Konfigürasyon yönetimi oluşturulmalı<br>-İş yükü hafifletilmeli<br>-Yapılandırma için uzman ve dedike personel seçilmeli. |
| | Yavaşlama | -VTYS ve disk ünitesi asasındaki bağlantı yavaşlar | Uygulama yavaş hizmet verir | 3 | -Toz/Kir<br>-Firmware bug<br>-Isınma<br>-Yıpranma<br>-Korozyon | 3 | Yedeklilik<br>-Soğutma sistemi | **9** | -Mesh toploji ile çoklu yol oluşturulabilir ve yapı istendiği kadar genişletilebilir.<br>-Yama yönetimi ve takibi yapılmalı |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 21<br>SAN Switch<br>(devam) | Başarısız firmware yükseltmesi | SAN switch çalışmaz ya da yavaş çalışır | Uygulama yavaş hizmet verir ya dahizmet veremez. | 5 | -Yanlış prosedürün izlenmesi<br>-Güç kesintisi<br>-Isınma<br>-Yanlış firmware sürümü | 4 | Yedeklilik | **20** | Test ortamı kurulmalı |
| | SAN switchin kapanması | VTYS Disk ünitesine erişememe | Uygulama hizmet veremez | 8 | -Güç kesintisi | 7 | Yedeklilik | **56** | -Düzenli aralıklarla izleme ve kontrol mekanizması oluşturulmalı<br>-Otomatik uyarı mesajları ayarlanmalı |
| 22<br>Fiber Kablo | Bükülme/Ezilme | Veri paketlerinde kayıp yaşanır | Uygulama hizmeti yavaşlar veya başarısız işlemler meydana gelir | 4 | -Isı farkı<br>-Gerilme<br>-Basınç | 2 | Yedeklilik | **8** | -Düzenli aralıklarla izleme ve kontrol mekanizması oluşturulmalı<br>-Otomatik uyarı mesajları ayarlanmalı |
| | Porttan çıkması | VTYS sunucusu ve disk ünitesine erişimin kaybedilmesi | Uygulamaya erişilemez | 3 | -Sabotaj<br>-Yanlışlıkla çıkma | 3 | Yedeklilik | **9** | -Düzenli aralıklarla izleme ve kontrol mekanizması oluşturulmalı<br>-Otomatik uyarı mesajları ayarlanmalı |
| | Kopma | VTYS sunucusu ve disk ünitesinin bağlantısının kopması | -Uygulamaya erişilemez<br>-Uygulama hizmet veremez | 4 | -Sabotaj<br>-Yanlışlıkla kopma | 2 | Yedeklilik | **8** | -Düzenli aralıklarla izleme ve kontrol mekanizması oluşturulmalı<br>-Otomatik uyarı mesajları ayarlanmalı |
| 23<br>HBA | Fiziksel Arıza | Sunucu ile SAN switch arasındaki bağlantı kopar | -Uygulama hizmet veremez | 9 | -Isınma<br>-Yıpranma<br>-Eskime<br>-Sıvı ile temas<br>-Yüksek nem<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 1 | -Yedeklilik (Çoklu HBA) | **9** | -Düzenli aralıklarla izleme ve kontrol mekanizması oluşturulmalı<br>-Otomatik uyarı mesajları ayarlanmalı |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 23<br>HBA (devam) | Başarısız firmware yükseltmesi | HBA çalışmaz veya yavaş çalışır | -Uygulama yavaşlar veya kısa süre sonra hizmet veremez | 4 | -Yanlış prosedürün izlenmesi<br>-Güç kesintisi<br>-Isınma<br>-Yanlış firmware sürümü | 4 | Yedeklilik | **16** | Test ortamı kurulmalı |
| | Sağlam HBA nın sistemde online gözükmemesi | HBA çalışmaz | Sunucunun veri ünitesine erişimi kesilir. Uygulama hizmet veremez. | 3 | -Temassızlık<br>-Yerinden çıkma | 3 | Yedeklilik | **9** | -Düzenli aralıklarla izleme ve kontrol mekanizması oluşturulmalı<br>-Otomatik uyarı mesajları ayarlanmalı |
| 24<br>Disk Kontrolör | Fiziksel arıza | -Disklere erişilemez<br>-Veritabanına erişilemez | -Uygulama hizmet veremez | 10 | -Toz/Kir<br>-Isınma<br>-Sıvı ile temas<br>-Yıpranma<br>-Eskime<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 3 | -Yedeklilik<br>-Proaktif uyarı sistemi | 30 | Düzenli “healt check” test prosedürü |
| | Başarısız firmware yükseltmesi | -Yavaşlar<br>-Disklere erişilemez<br>-Veritabanına erişilemez | -Uygulama hizmet veremez veya yavaşlar | 7 | -Yanlış prosedürün izlenmesi<br>-Güç kesintisi<br>-Isınma<br>-Yanlış firmware sürümü | 5 | Yedeklilik | 35 | Test ortamı<br>Sistem odasının sıcaklığı sık sık kontrol edilmeli,<br>Ani sıcaklık değişimlerinde SMS le uyarı |
| | Disk kontrolör Yönetim yazılımın hata vermesi | Disk ünitesi yönetilemez | -Uygulama hizmet vermeye devam eder ancak disk yönetimi yapılamaz. | 2 | Yazılım içindeki bug | 2 | Yedeklilik | 4 | Düzenli “healt check” test prosedürü<br>-Bakım destek anlaşmalarının yenilenmesi |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No<br>Bileşen | Potansiyel<br>Başarısızlık<br>Modu | Potansiyel<br>Etkileri | Uygulama<br>Üzerindeki Etkiler | Ciddiyet | Nedensel<br>Faktörler | Olasılık | Mevcut<br>Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 25<br>Fiziksel Disk | Fiziksel arıza | -Veri bozulur<br>-Veritabanına erişilemez | -Uygulama hizmet veremez | 10 | -Titreşim sarsıntı<br>-Sıvı teması<br>-Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Eskime<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 2 | Veri yedekleme | 20 | Verinin senkronize yedeklenmesi |
| 26<br>RAID | Yanlış yapılandırma | Yanlışlıkla düşük seviye yapılandırma sonucunda performans kaybı oluşur | -Uygulama yavaş hizmet verir | 3 | -Yetersiz eğitim<br>-Prosedür yok ya da eksik<br>-Konfigürasyon yönetimi yok<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 3 | Yok | **9** | -Sistem kurulum ve konfigürasyon yönetimi prosedürünün oluşturulması<br>-Yeniden yüksek seviye RAID yapılandırması yapılabilir |
| | Yanlış Diskin Değiştirilmesi | -Disklere erişilemez<br>-Veritabanına erişilemez | -Uygulama hizmet veremez | 9 | -Yetersiz eğitim<br>-Sabotaj<br>-Prosedür yok ya da eksik<br>-Motivasyon eksikliği<br>-Aşırı iş yükü<br>-Dalgınlık | 6 | Kullanıcı hatasını önlemeye yönelik gömülü disk değiştirme prosedürü mevcut. | **54** | -Eğitim verilmeli<br>-İşlemler için prosedür oluşturulmalı<br>-Yüksek seviyeli RAID yapısı kullanılmalı<br>-Çalışan üzerindeki fazla ya da gereksiz iş yükü kaldırılmalı<br>-Çalışan motive edilmeli<br>-RAID ve pooling yapılandırması kullanılabilir. |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 26<br>RAID (devam) | Çoklu Disk Hatası | -RAID yapısı bozulur<br>-Veri bozulur<br>-Disklere erişilemez<br>-Veritabanına erişilemez | -Uygulama hizmet veremez | 9 | -Titreşim sarsıntı<br>-Isınma<br>-Yıpranma<br>-Yüksek güç girişi<br>-Elektrik kesintisi | 3 | Hotspare disk tutulmaktadır<br>-Veri yedeklemesi | **27** | -Yüksek seviyeli RAID yapısı kullanılmalı<br>-Hotspare disk sayısı arttırılmalı.<br>-Yedekte disk bekletilmeli<br>-RAID ve pooling yapılandırması kullanılabilir<br>- Verinin senkronize yedeklenmesi |
| | RAID yapılandırmasının kaybedilmesi | -Disklere erişilemez<br>-Veritabanına erişilemez | -Uygulama hizmet veremez | 9 | -Sabotaj<br>-Aşırı iş yükü | 2 | Yok | **18** | Raid yapılandırmasını iki kişi aynı anda yapacak şekilde Administratör rolü iki kişiye paylaştırılabilir. |
| 27<br>LUN | LUN yapılandırmasının silinmesi | -Veri silinir<br>-Veritabanına erişilemez | Uygulama hizmet veremez | 9 | -Sabotaj<br>-Aşırı iş yükü<br>-RAID yapılandırmasının silinmesi | 4 | Yedekleme | **36** | Verinin senkronize yedeklenmesi |

EK-1. (devam) FMEA Risk Analiz Tablosu

| **Sistem:** <Uygulama2> | | | **Alt Sistem:** Hastane Alt Sistemi | | | **Mod/Safha:** Operasyon | | | **FMEA Analizi** |
|---|---|---|---|---|---|---|---|---|---|
| **No Bileşen** | **Potansiyel Başarısızlık Modu** | **Potansiyel Etkileri** | **Uygulama Üzerindeki Etkiler** | **Ciddiyet** | **Nedensel Faktörler** | **Olasılık** | **Mevcut Kontroller** | **Risk** | **Önerilen Kontroller** |
| 28<br>Ağ Yapısı | Ağ kabloların kopması / kesilmesi | Erişimin kaybedilmesi | Uygulamaya erişilemez | 2 | -Sabotaj<br>-Yanlışlıkla kopma | 6 | Kanaldan geçmesi | **12** | Wifi network |
| | Ağ kablolarında parazit oluşması | Veri paketlerinde kayıp yaşanır | Uygulama hizmeti yavaşlar veya başarısız işlemler meydana gelir | 3 | -Elektrik kabloları ile yakın geçmesi<br>-İzolasyon olmaması | 4 | Yok | **12** | Kanallar ayrılmalı ya da izolasyon yapılmalı |
| | Switch ve kabinetin ısınması | Bağlantı yavaşlar | Uygulamaya erişim yavaşlar veya başarısız işlemler meydana gelir | 4 | -Kapalı dar alan<br>-Soğutma yok | 5 | Yok | **20** | Ağ kabineleri ve montaj yerleri için standart geliştirilmeli |
| | Sinyalin zayıflaması | Veri paketlerinde kayıp yaşanır | Uygulamaya erişim yavaşlar veya başarısız işlemler meydana gelir | 2 | Normalden uzun kablo kullanımı | 3 | Yok | **6** | Uzun kablo kullanımı tespit edilmeli ve standart getirilmeli |
| | Kablonun yerinden çıkması | Erişimin kaybedilmesi | Uygulamaya erişilemez | 2 | -Elverişsiz kablo tesisatı<br>-Sabotaj<br>-Yanlışlıkla çıkma | 6 | Yok | **12** | Kapalı kanallardan geçmeli |
| 29<br>Bilgisayar | Fiziksel Arıza | Bilgisayarın açılmaması | -Uygulamaya erişememe<br>-Sağlık sigortası hak sahibi memnuniyetsizliği | 2 | -Sıvı ile temas<br>-Yüksek nem<br>-Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Eskime<br>-Yüksek güç girişi<br>-Bakım eksikliği<br>-Elektrik kesintisi<br>-Korozyon | 6 | Bakım | **12** | Bilgisayarlara periyodik bakım<br>-Thin client kullanımı |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 29 Bilgisayar (devam) | Yavaşlama | Uygulama ekranında gezinme ve menü geçişleri uzun sürer | -Uzun süren işlem süreleri<br>-Sağlık sigorta memnuniyetsizliği | 2 | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | 6 | Yok | **12** | -Thin client kullanımı<br>-Gereksiz uygulamaların kaldırılması |
| | Virüs bulaşması | Uygulama ekranında gezinme ve menü geçişleri uzun sürer | -Uzun süren işlem süreleri<br>-Sağlık sigortası hak sahibi memnuniyetsizliği | 2 | -Koruma yok<br>-Kontrolsüz USB disk kullanma | 8 | Anti virüs | **16** | -Antivirüs güncelleme takibi<br>-USB kullanımı kısıtlanmalı |
| | Bellek hatası | Bilgisayar hata verir | -Uygulamaya erişememe<br>-Sağlık sigortası hak sahibi memnuniyetsizliği | 2 | -Temassızlık<br>- Sistem belleğinde hata tespiti ya da düzeltmesi olmadan çalışan yazılımlar | 6 | | **12** | Yok |
| | Kaynak çakışması Kesme isteği çakışması | Bilgisayar hata verir | -Uygulamaya erişememe<br>-Sağlık sigortası hak sahibi memnuniyetsizliği | 2 | -Uyumsuz bileşen<br>-Çevre bileşenlerin aynı kesme isteği sinyalini veya DMA kanallarını veya giriş çıkış adreslerini kullanması | 3 | BIOS kontrolü | **6** | Yok |
| 30 Teknik Personel | Geç müdahale | Sorunların uzun süre devam etmesi | -Uygulamaya Erişememe<br>-Sağlık sigortası hak sahibi memnuniyetsizliği | 2 | -Yetersiz eleman<br>-Aşırı iş yükü | 7 | | **14** | Personel kapasite planlaması |
| | Yanlış/Bozuk operasyon işlem | Sorunların uzun süre devam etmesi | -Uygulamaya Erişememe<br>-Sağlık sigortası hak sahibi memnuniyetsizliği | 2 | -Yetersiz eğitim<br>-Eksik prosedür | 7 | | **14** | -Eğitim<br>-Prosedür oluşturulmalı |
| | Çözümün uzun sürmesi | Sorunların uzun süre devam etmesi | -Uygulamaya Erişememe<br>-Sağlık sigortası hak sahibi memnuniyetsizliği | 2 | -Yetersiz eğitim<br>-Eksik prosedür | 7 | | **14** | -Eğitim<br>-Prosedür oluşturulmalı |

EK-1. (devam) FMEA Risk Analiz Tablosu

| No Bileşen | Potansiyel Başarısızlık Modu | Potansiyel Etkileri | Uygulama Üzerindeki Etkiler | Ciddiyet | Nedensel Faktörler | Olasılık | Mevcut Kontroller | Risk | Önerilen Kontroller |
|---|---|---|---|---|---|---|---|---|---|
| 31 Hastane Bilgi Yönetim Yazılımı | Yazılımın yavaş çalışması | Web servisleri yavaş kullanır | -Sağlık sigortası hak sahibi memnuniyetsizliği | 3 | | 5 | | **15** | Standart getirilmeli |

EK-2. HAZOP Risk Analizi Tablosu

| **Sistem:** <Uygulama2> | | **Alt Sistem:** Soğutma Alt Yapısı | | | **HAZOP ANALİZİ** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Sıra No / Bileşen** | **Fonksiyon/Amaç/ işlem** | **Parametre** | **Referans Anahtar Kelime** | **Sonuç/ sapma** | **Neden** | **Tehlike** | **Olasılık** | **Şiddet** | **Risk** | **Öneriler ve Düşünceler** |
| 1 Kondenser | Soğutarak gazdan sıvıya dönüştürme | Akışkan sıvı miktarı | Çok | Kompresörün arızalanması sonucu soğutma yok | -Fazla akışkan dolumu | Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlar veya durur. | 6 | 6 | 36 | -Gaz veya sıvının miktarının düzenli kontrolü |
| | | | Az | Yetersiz soğutma | -Eksik akışkan dolumu<br>-Kaçak olması | Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlar. | 6 | 6 | 36 | -Gaz veya sıvının miktarının düzenli kontrolü |
| | | Tıkanma / Tıkanıklık | Var | Yetersiz soğutma | -Yanlış seçilen montaj yeri<br>-Kirli ortam | Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlar. | 5 | 5 | 25 | -Mevsim şartlarına göre daha sık temizleme |
| | | Yoğunlaştırma | -Başarısız<br>-Yok | Yetersiz soğutma | -Direk ısıya maruz kalma<br>-Dar havasız alanlara monte etme | Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlar. | 7 | 5 | 35 | -Sundurma yapılabilir |
| | | Kondenser içi basınç | Çok | Kompresörün arızalanması sonucu soğutma yok | Basınç koruma elemanının bozulması | Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlar veya durur. | 6 | 6 | 36 | -Gaz veya sıvının miktarının düzenli kontrolü |
| | | | Az | Yetersiz soğutma | -Eksik akışkan dolumu<br>-Kaçak olması | Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlar. | 6 | 6 | 36 | -Gaz veya sıvının miktarının düzenli kontrolü |
| 2 Kompresör | Havayı sıkıştırma gazı devir daim yapma | Hava akışı | Düşük | Yetersiz soğutma | -Zararlı kimyasal eriyikler<br>-Termostatın yanlış ayarlanması | Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlar veya durur. | 5 | 5 | 25 | Bakımın mevsime göre sıklaştırılması |
| | | | Yok | Soğutma yok | -Güç yok<br>-Rulman sıkışması<br>-Termik atması | Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlar veya durur. | 4 | 6 | 24 | -Sürekli fiziksel kontrol<br>-Nöbet sistemi |
| 3 Evoporatör | Soğutma sıvısını gaza dönüştürerek (buharlaştırarak) çevresini soğutma | Isı alış verişi | Düşük | Soğutma başarısız | -Tıkanma<br>-Kirlenme<br>-Korozyon<br>-Fanın bozulması | Veri merkezi ve içindeki sistemlerin ısınması sonucunda uygulama yavaşlar veya durur. | 6 | 5 | 30 | 3 Aylık periyodik bakım yeterli |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| **Sistem:** <Uygulama2> | | **Alt Sistem:** Enerji Alt Yapısı | | | **HAZOP ANALİZİ** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Sıra No / Bileşen** | **Fonksiyon/Amaç/ işlem** | **Parametre** | **Referans Anahtar Kelime** | **Sonuç/ sapma** | **Neden** | **Tehlike** | **Olasılık** | **Şiddet** | **Risk** | **Öneriler ve Düşünceler** |
| 4<br>UPS (KGK) | Kesintisiz elektrik enerjisi sağlamak | Şarj olma | Başarısız | UPSin sisteme güç verebilecek enerjiye sahip olmaması | -Redresör arızası (AC -> DC)<br>-Şarj devresinin bozulması | Şebeke elektriği kesildiğinde şarj olmayan UPS sisteme güç veremez. Sunucu ve diğer donanımlar kapanmasıyla uygulama hizmet veremez. | 4 | 9 | 36 | Yok |
| | | Güç çıkışı | Yok | UPSin sisteme güç sağlayamaması | İnvertör veya emniyet sigortasının atması | Şebeke elektriği kesildiğinde UPS sisteme güç veremez. Sunucu ve diğer donanımlar kapanmasıyla uygulama hizmet veremez. | 4 | 9 | 36 | -STS anahtarı eklenebilir |
| | | Güç sağlama süresi | Kısa | UPS sisteme güç verebilecek enerjiye sahip olmaması | Akü ömrünün bitmesi | Şebeke elektriği kesildikten kısa süre sona UPS sisteme güç veremez. Sunucu ve diğer donanımların kapanmasıyla uygulama hizmeti kesilir. | 5 | 9 | 45 | -Dinamik UPS sistemi ya da hibrit UPS sistemi |
| | | Otomatik devreye girme | Başarısız | Elektrik kesintisinde UPSin devreye girmemesi | -Bozuk geçiş anahtarı | Şebeke elektriği kesildiğinde UPS devreye girmez. Sunucu ve diğer donanımlar kapanmasıyla uygulama hizmet veremez. | 2 | 9 | 18 | Çift besleme |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 5 Jeneratör | Benzini yakarak elektrik enerjisi üretmek | Güç | Başarısız | Sisteme güç gitmez | -Sigorta atmış<br>-İkaz trafosu yanmış olabilir<br>-Manyetizma gitmiş olabilir | Sigorta atmasından dolayı jeneratör güç üretmeyebilir. Uygulama hizmet veremez | 3 | 4 | 12 | Kontrol |
| | | | Dalgalanma | Sisteme güç gitmez | -Motor devir ayarı hatalı<br>-Sargılarda kopukluk | Jeneratör motorundaki sorunlardan dolayı sisteme dalgalı güç gider. | 2 | 3 | 6 | Dalgalı güç UPS tarafından kesilmektedir. Düzenli kontrol |
| | | Voltaj | Düşük | Sistem zarar görebilir | AVR arızası | Jeneratör avr arızasından dolayı sisteme düşük voltaj gider ve sistem kapanabilir arızalanabilir. | 2 | 9 | 18 | |
| | | Motorun çalışma süresi | Kısa | Sisteme güç girişi olmayacağı için sunucular kapanır. | -Yakıt devresi tıkalı<br>-Enjektörler ayarsız<br>-Emme kanalları tıkalı | Sisteme güç girişi olmayacağı için sunucular kapanır ve uygulamalar hizmet veremez. | 3 | 3 | 9 | |
| 6 Şebeke Trafosu | Elektrik enerjisi iletiminin kontrolünü sağlamak | Şalterin kapatılması | İstemsiz / Yanlışlıkla | Sisteme güç girişi olmayacağı için sunucular kapanır. | -Etiketleme yok<br>-Dalgınlık | Sisteme güç girişi olmayacağı için sunucular kapanır ve uygulamalar hizmet veremez. | 4 | 4 | 16 | -Prosedür oluşturma<br>-Dedike personel oluşturma |
| 6.1 Şebeke Tesisatı | Elektrik enerjisini iletmek | İletmek | Başarısız | Sunucular kapanır veriler zarar görebilir. | -Kopukluk<br>-Tesisatın yanması | Tesisatın yanmasından kaynaklı sunucular kapanıp veriler zarar görebilir ve uygulama uzun süre hizmet veremez. | 3 | 10 | 30 | Su ve kanalizasyon tesisatının veri merkezinden ayrılması |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| **Sistem:** <Uygulama2> | | **Alt Sistem:** Uygulama Alt Sistemi | | | **HAZOP ANALİZİ** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Sıra No / Bileşen** | **Fonksiyon/Amaç/ işlem** | **Parametre** | **Referans Anahtar Kelime** | **Sonuç/ sapma** | **Neden** | **Tehlike** | **Olasılık** | **Şiddet** | **Risk** | **Öneriler ve Düşünceler** |
| 7 Uygulama Yazılımı | Web arayüzü ile veritabanı üzerinde ekleme, silme, güncelleme veya okuma işlemlerinin yapılmasını sağlama | Durması | Zamansız | Uygulamaya erişilemez | -Yazım yanlışı<br>-Fonksiyonların yanlış kullanımı | Uygulama yazılımının zamansız durduğunda hizmet verilemez | 6 | 5 | 30 | -Fonksiyonel testlerin yapılması<br>-Test ortamının kurulması |
| | | İşlem Süresi | Uzun | Uygulama yavaşlar | Yazılım içindeki elverişsiz SQL kodu. | İşlem sürelerinin uzaması ile hizmet yavaş verilir yada bir süre sonra hizmet durur. | 5 | 5 | 25 | -SQL optimizasyonu<br>-Tasarım yeniden gözden geçirilmeli<br>-Kod anallizi yapılmalı |
| | | Sonuçların güvenilirliği | Yok | Güvenilmez sonuçlar | -SQL injection<br>-Eksik veya yanlış analiz<br>-Eksik veya yanlış tasarım | SQL injection sonucunda güvenirliliğin kaybolması ile uygulama güvenilir bir şekilde hizmet veremez. | 3 | 10 | 30 | |
| | | Başlatma | Başarısız | Uygulamaya erişilemez | Eksik kütüphane | Uygulama başlatılamadığı için hizmet verilemez | 5 | 5 | 25 | Kontrol listesi |
| | | Sonlandırma | Başarısız | İşlemler birikir | -Yazım yanlışı<br>-Fonksiyonların yanlış kullanımı | Uygulama başlatıldıktan kısa süre sonra kapasitesini doldurur ve hizmet veremez. | 6 | 5 | 30 | |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 8 Yazılımcı | -Uygulama yazılımının kodlarını yazmak ve yazılımdaki sorunları gidermek | İşe gelme | Geç | Yok | -Ulaşım sorunları<br>-Kötü hava şartları<br>-Düzensiz iş planı | Yazılımcının işe geç gelmesi uygulamanın sürekliliği için bir tehlike teşkil etmemektedir. | 10 | 1 | 10 | -Nöbet<br>-Uzaktan erişim<br>-İş planlarının düzenlenmesi |
| | | Algoritma oluşturma | Yanlış | Metotlar çalışmaz veya yanlış hizmet verir | -Eksik veya yanlış analiz<br>-Eksik veya yanlış tasarım | Eksik analiz sonucunda yazılımcının yanlış algoritma oluşturması ve metotların çalışmaması veya yanlış çalışması | 5 | 8 | 40 | Yazılımların analiz ve tasarımlarının düzenli yapılması |
| | | Kod yazma süresi | Uzun | Proje/değişiklik zamanında bitmez | -Düzensiz iş planı<br>-Eksik veya yanlış analiz<br>-Eksik veya yanlış tasarım | Analiz eksiği veya aşırı iş yükü sonucunda yazılım projesi ya da yeni sürümü vaktinde devreye giremez | 5 | 4 | 20 | Yazılımların analiz ve tasarımlarının yapılarak yazılımcılara düzenli iş planı oluşturulmalı. |
| | | Fonksiyon kullanma ve parametre ekleme | Yanlış | Fonksiyon çalışmaz ya da yanlış çalışır | -Yetersiz eğitim<br>-Yanlış personel seçimi<br>-Aşırı iş yükü | Yazılım kodu içerisinde fonksiyonun yanlış bir şekilde kullanılmasıyla uygulama çalışmaz, yanlış çalışır veya beklenmedik şekilde sonlanır | 4 | 8 | 32 | -Eğitim<br>-Yazılım geliştirme prosedürünün oluşturulması |
| | | (Çalışma) sürekliliği | Yok | Gerekli değişiklikler yapılamaz veya sorunlu sürümler ortaya çıkar | -Düşük maaş<br>-Aşırı iş yükü<br>-Motivasyon eksikliği | Yetiştirilmiş personelin işten ayrılması sonucunda yeni sürümü vaktinde devreye giremez veya hatalı sürüm ortaya çıkar. | 6 | 5 | 30 | -Özlük hakları<br>-Çalışma şartlarının iyileştirilmesi<br>-Prosedürler oluşturularak kişiye bağımlılığın azaltılması<br>-Yedekli personel<br>-Konfigürasyon yönetimi |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 9 WAS Application Sunucusu | Uygulama yazılımını çalıştırmak ve kullanıcılara web arayüzü oluşturmak Veritabanına bağlantı sağlamak | Yama yapma | Başarısız | WAS uygulama sunucusu çalışmaz | -Prosedür yok ya da eksik<br>-Eksik eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Başarısız yama yüklemesi sonucunda WAS uygulama sunucusu çalışmaz dolayısı ile uygulama hizmet vermez | 4 | 6 | 24 | -Detaylı yama yönetimi prosedürünün oluşturulması<br>-Konfigürasyon yönetimi<br>-Prosedür oluşturma |
| | | Yapılandırma | Yanlış | WAS uygulama sunucusu çalışmaz veya kısmen çalışır | -Prosedür yok ya da eksik<br>-Eksik eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Başarısız yapılandırma ile uygulama hizmet vermez, kısmen hizmet verir veya hata verir. | 6 | 6 | 36 | -Değişiklik yönetimi<br>-Konfigürasyon yönetimi<br>-Prosedür oluşturma |
| | | Başlatma | Başarısız | Node1Server1 çalışmaz | Server1.pid dosyasının mevcudiyeti<br>-Crash | İlgili JVM (ler) başlayamadığından uygulama da başlamaz ve hizmet veremez. | 6 | 5 | 30 | Kontrol noktası oluşturulmalı: server1.pid dosyasının silinmesi |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 10 İşletim Sistemi | Sunucu donanımı üzerinde koşarak WAS çalışması için çalışma ortamı sağlamak | Süreklilik | Yok | İşletim sistemi çalışmaması | -Donanım arızası | Donanım arızası veya virüs bulaşması sonucunda işletim sistemi çalışmasını sürdüremediğinde uygulama hizmet veremez. | 2 | 8 | 16 | Yok |
| | | Yapılandırma | Yanlış | İşletim sistemi çalışmaz veya WAS uygulama sunucusunun çalışmasını engeller | -Prosedür yok ya da eksik<br>-Eksik eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Başarısız yapılandırma ile uygulama hizmet vermez, kısmen hizmet verir veya hata verir. | 4 | 5 | 20 | -Eğitim<br>-Prosedür<br>-Konfigürasyon yönetimi<br>-Değişiklik yönetimi |
| | | Başlatma | Başarısız | İşletim sisteminin çalışamaması | -Donanım arızası<br>-Eksik sürücü<br>-Desteğin bitmesi | İşletim sisteminin başlaması başarısız olduğunda uygulama hizmet veremez. | 2 | 7 | 14 | Yok |
| | | Çalışma performansı | Düşük | İşletim sisteminin yavaşlaması | -Fazla sayıda gereksiz modül ya da uygulama | Virüs bulaşması ile işletim sistemi yavaşlar ve sonucunda uygulama hizmeti yavaşlar. | 3 | 3 | 9 | -Sıklaştırma politikası ve kontrol listesi oluşturulmalı |
| 11 Sunucu Donanımı | Elektronik verileri işleyerek çıktılara dönüştürmek | Fiziksel bütünlük | Yok/Bozuk | Sunucu çalışmaz | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yangın vb. nedenlerden sunucu donanımının fiziksel bütünlüğünün bozulmasıyla uygulama hizmet veremez. | 2 | 7 | 14 | Topraklama hattı periyodik olarak kontrol edilmeli.<br>Veri merkezi olmaya uygun binalar kullanılmalı |
| | | Çalışma performansı | Düşük | Sunucu donanımın yavaşlaması | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | Donanımın yavaşlaması sonucunda uygulama hizmeti yavaşlar veya kısa süre sonra durur. | 3 | 3 | 9 | -Bakım |
| | | Başlatma | Başarısız | Sunucu çalışmaz | -Donanım arızası<br>-Temassızlık<br>-Yanlış montaj | Donanım arızalanması sonucu sunucu çalışmaz ve uygulama hizmet veremez. | 3 | 7 | 21 | -Kontrol listesi<br>-Düzenli eğitim verilmesi |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| **Sistem:** <Uygulama2> | | **Alt Sistem:** Network Alt Sistemi | | | **HAZOP ANALİZİ** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Sıra No / Bileşen** | **Fonksiyon/Amaç/ işlem** | **Parametre** | **Referans Anahtar Kelime** | **Sonuç/ sapma** | **Neden** | **Tehlike** | **Olasılık** | **Şiddet** | **Risk** | **Öneriler ve Düşünceler** |
| 12 Firewall (Güvenlik Duvarı) | Ağ trafiğini kontrol ederek izin vermek ya da engellemek | Fiziksel bütünlük | Yok/Bozuk | Güvenlik duvarının çalışmaması | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yangın vb. nedenlerden güvenlik duvarının fiziksel bütünlüğünün bozulmasıyla uygulamaya erişilemez. | 5 | 7 | 35 | -Yedeklilik<br>-Acil müdahale ekibi |
| | | Yapılandırma | Yanlış | -Erişim isteği engellemesi<br>-Ağ trafiği kesilmesi | -Prosedür yok ya da eksik<br>-Eksik konfigürasyon yönetimi<br>-Yetersiz eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Yanlış yapılandırma sonucu ağ trafiği engellenir veya kesilir; uygulamaya erişilemez. | 7 | 5 | 35 | -Düzenli eğitim<br>-Test ortamının kurulması ve yapılandırmaların test edilmesi |
| | | Çalışma performansı | Düşük | Güvenlik duvarının yavaşlaması | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | Güvenlik duvarının çalışma performansının düşmesiyle ağ trafiği yavaşlar ve uygulama yavaş hizmet verir. | 7 | 3 | 21 | -Yedeklilik<br>-Performans testi |
| | | Süreklilik | Yok | -Ağ trafiğinin kesilmesi | -Donanım arızası<br>-Elektrik kesintisi | Elektrik kesintisi sonucu ağ trafiğinin kesilmesiyle uygulamaya erişilemez. | 5 | 7 | 35 | -Yedeklilik<br>-izleme ve uyarı sistemi |
| | | | | -Bağlantı sayısı dolması | -DDOS atağı | Siber saldırı sonucu bağlantı sınırlarının aşılmasıyla uygulama yeni ve gerçek isteklere cevap veremez. | 4 | 7 | 25 | -izleme ve uyarı sistemi<br>-Siber güvenlik önlemleri |
| | | Firmware yükseltmesi | Başarısız | Ağ trafiğinin kesilmesi veya yavaşlaması | -Isınma<br>-Güç kesintisi<br>-Yanlış prosedürün izlenmesi<br>-Yanlış sürüm | Güç kesintisi, yanlış prosedür veya yanlış sürüm kaynaklı başarısız firmware yükseltmesi sonucunda ağ trafiğinin yavaşlaması veya kesilmesi ile uygulama erişim yavaşlar veya erişim olmaz. | 2 | 7 | 14 | Test ortamı |
| | | SSL bağlantısı | Başarısız | Bağlantı kurulamaması | -Değişen anahtarın girilmemesi | Şifre uyuşmazlığı veya başarısız SSL handshake kaynaklı başarısız SSL bağlantısı sonucunda uygulamaya erişilemez. | 7 | 5 | 35 | Değişiklik yönetimi ve koordinasyon planı |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 13 Router | L3 katmanında IP veri paketlerini yönlendirerek hedefe ulaşmasını sağlamak | Fiziksel bütünlük | Yok/Bozuk | -Yönlendiricinin çalışmaması | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yangın vb. nedenlerden yönlendiricinin fiziksel bütünlüğünün bozulmasıyla uygulamaya erişilemez. | 7 | 4 | 28 | Yedeklilik |
| | | Yapılandırma | Yanlış | Ağ trafiği kesilir veya yavaşlar | -Prosedür yok ya da eksik<br>-Eksik konfigürasyon yönetimi<br>-Yetersiz eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Prosedürün olmaması veya yetersiz eğitim kaynaklı yanlış yapılandırma sonucu uygulamaya erişilemez veya yavaşlar. | 6 | 6 | 36 | -İzleme ve uyarı sistemi<br>-Siber güvenlik önlemleri<br>-Test ortamı<br>-Değişiklik yönetimi<br>-Konfigürasyon yönetimi |
| | | Çalışma performansı | Düşük | Yönlendiricinin yavaşlaması | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | Yıpranma, ısınma veya korozyon kaynaklı yönlendiricinin çalışma performansının düşmesiyle ağ trafiği yavaşlar ve uygulama yavaş hizmet verir. | 3 | 8 | 24 | -Bakım |
| | | Süreklilik | Yok | Ağ trafiği kesilir. | -Donanım arızası<br>-Elektrik kesintisi | Elektrik kesintisi veya donanım arızası sonucu ağ trafiğinin kesilmesiyle uygulamaya erişilemez. | 7 | 6 | 42 | Yedeklilik |
| | | Firmware yükseltmesi | Başarısız | Ağ trafiğinin kesilmesi veya yavaşlaması | -Isınma<br>-Güç kesintisi<br>-Yanlış prosedürün izlenmesi | Güç kesintisi, yanlış prosedür veya yanlış sürüm kaynaklı başarısız firmware yükseltmesi sonucunda ağ trafiğinin yavaşlaması veya kesilmesi ile uygulama erişim yavaşlar veya erişim olmaz. | 2 | 7 | 14 | Test ortamı |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 14 Load Balancer (Yük Dağıtıcı) | Erişim isteklerini sunucu kümesi üyelerine dağıtmak | Fiziksel bütünlük | Yok/Bozuk | -Yük dağıtıcının çalışmaması | -Yangın<br>-Yıldırım<br>-Sıvı ile temas<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yangın vb. nedenlerden yük dağıtıcının fiziksel bütünlüğünün bozulmasıyla uygulamaya erişilemez. | 4 | 5 | 20 | -Bakım<br>-Varsa yedek modül stoğu |
| | | Yapılandırma | Yanlış | -Erişim isteklerinin üye sunucular arasında düzgün dağıtılamaması | -Eksik konfigürasyon yönetimi<br>-Prosedür yok ya da eksik<br>-Yetersiz eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Prosedürün olmaması veya yetersiz eğitim kaynaklı yanlış yapılandırma sonucu uygulamaya erişim olmaz. | 6 | 5 | 30 | -Eğitim<br>-Test ortamı<br>-Değişiklik yönetimi<br>-Konfigürasyon yönetimi |
| | | Çalışma performansı | Düşük | Yük dağıtıcının yavaşlaması | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | Yıpranma, ısınma veya korozyon kaynaklı yük dağıtıcının çalışma performansının düşmesiyle yönlendirme hızlı yapılamaz ve uygulama yavaş hizmet verir. | 7 | 4 | 28 | Bakım |
| | | Süreklilik | Yok | Üye sunuculara erişim istekleri dağıtılamaması | -Donanım arızası<br>-Elektrik kesintisi | Elektrik kesintisi veya donanım arızası sonucu erişim istekleri sunucuya ulaşmaz ve uygulama hizmet veremez. | 5 | 7 | 35 | Bakım |
| | | Firmware yükseltmesi | Başarısız | -Erişim isteklerinin üye sunucular arasında dağıtılamaması | -Isınma<br>-Güç kesintisi<br>-Yanlış prosedürün izlenmesi | Güç kesintisi, yanlış prosedür veya yanlış sürüm kaynaklı başarısız firmware yükseltmesi sonucunda erişim isteklerinin sunuculara iletilememesi ile uygulama hizmet veremez. | 2 | 7 | 14 | Test ortamı |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 15 Switch (Ağ Anahtarı) | L2, katmanında veri paketlerini doğru porta yönlendirerek hedefe ulaşmasını sağlamak | Fiziksel bütünlük | Yok/Bozuk | -Ağ anahtarının çalışmaması | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yangın vb. nedenlerden ağ anahtarının fiziksel bütünlüğünün bozulmasıyla uygulamaya erişilemez. | 6 | 7 | 42 | -Acil müdahale ekibi<br>-Yedek modül stoğu |
| | | Yapılandırma | Yanlış | -İç ağ trafiğinin kesilmesi veya yavaşlaması | -Prosedür yok ya da eksik<br>-Eksik konfigürasyon yönetimi<br>-Yetersiz eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Prosedürün olmaması veya yetersiz eğitim kaynaklı yanlış yapılandırma sonucu ağ trafiğinin kesilmesiyle uygulamaya erişim olmaz veya yavaş olur. | 6 | 5 | 35 | -Eğitim<br>-Test ortamı<br>-Değişiklik yönetimi<br>-Konfigürasyon yönetimi |
| | | Çalışma performansı | Düşük | Ağ trafiğinin yavaşlaması | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | Yıpranma, ısınma veya korozyon kaynaklı ağ trafiğinin yavaşlamasıyla uygulama yavaş hizmet verir. | 7 | 3 | 21 | Bakım |
| | | Süreklilik | Yok | İç ağ trafiğinin kesilmesi | -Donanım arızası<br>-Elektrik kesintisi | Elektrik kesintisi veya donanım arızası kaynaklı iç ağ trafiği sunuculara ulaşmaz ve uygulama hizmet veremez. | 5 | 7 | 35 | -Acil müdahale ekibi<br>-Yedek modül stoğu |
| | | Firmware yükseltmesi | Başarısız | -İç ağ trafiğinin kesilmesi veya yavaşlaması | -Isınma<br>-Güç kesintisi<br>-Yanlış prosedürün izlenmesi | Güç kesintisi, yanlış prosedür veya yanlış sürüm kaynaklı başarısız firmware yükseltmesi sonucunda erişim isteklerinin sunuculara iletilememesi veya yavaş iletilmesi ile uygulama hizmet veremez veya yavaş hizmet verir. | 2 | 7 | 14 | Test ortamı |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 16<br>Ağ kablosu | L1 katmanında veri paketlerini elektriksel olarak iletmek | Fiziksel bütünlük | Yok/Bozuk | Ağ bağlantısının kesilmesi | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yangın vb. kaynaklı ağ bağlantısının kesilmesi sonucu uygulamaya erişilmez. | 4 | 5 | 20 | Kabloların kanallardan geçirilmesi |
| | | Parazit | Var | Veri paketlerinde kayıp | Ağ kablosu ile elektrik kablosunun yakın geçmesi veya yalıtım olmaması | Elektrik kabloları aynı kanaldan geçme kaynaklı ağ kablosunda parazit oluşur ve uygulama hizmet verirken gecikmeler olur. | 4 | 5 | 20 | Veri kablosunun elektrik kanallarından farklı kanallardan geçirilmesi veya izolasyonu |
| | | Sinyal | Zayıf | Veri paketlerinde kayıp | Uzun kablo kullanılması | Gereğinden uzun kablo kullanmadan kaynaklı ağ kablosunda parazit oluşur ve uygulama hizmet verirken gecikmeler olur. | 4 | 5 | 20 | Azami kablo uzunluğu için kontrol noktası oluşturulmalı |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| **Sistem:** <Uygulama2> | | **Alt Sistem:** Veritabanı Alt Sistemi | | | **HAZOP ANALİZİ** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Sıra No / Bileşen** | **Fonksiyon/Amaç/ işlem** | **Parametre** | **Referans Anahtar Kelime** | **Sonuç/ sapma** | **Neden** | **Tehlike** | **Olasılık** | **Şiddet** | **Risk** | **Öneriler ve Düşünceler** |
| 17<br>VTYS<br>Yazılımı | Veritabanını erişebilir kılmak, ekleme, silme ve güncelleme yapmak ... yönetmek | İşlem süresi | Uzun | Cevapların gecikmesi | -Düşük RAID seviyesi<br>-Düşük hızlı disk | Düşük seviyeli RAID ya da düşük hızlı disk kaynaklı işlem süreleri uzar ve uygulama yavaş hizmet verir. | 4 | 4 | 16 | Disk alım şartnamelerine yüksek hızlı disk için madde eklenmeli. |
| | | | | | -Yazılım içindeki (Parametrik) SQL kodu | Yazılım içindeki parametrik SQL kodundan kaynaklı işlem süreleri uzar ve uygulama yavaş hizmet verir. | 8 | 4 | 32 | -SQL optimizasyonu<br>-Yük ve performans testi<br>-Yazılım geliştirme prosedürü |
| | | Verilerin güvenirliği | Yok | Sonuçlara güvenilememesi | -SQL injection<br>-Siber saldırı | SQL injection sonucunda güvenirliliğin kaybolması ile uygulama güvenilir bir şekilde hizmet veremez. | 7 | 10 | 70 | -Siber saldırı önlemleri<br>-Kısa aralıklarla online veri yedeklemesi<br>-VT firewall |
| | | Yama yapma | Başarısız | VTYS yazılımının çalışmaması | -Prosedür yok ya da eksik<br>-Eksik eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Başarısız yama yüklemesi sonucunda VTYS yazılımı çalışmadığı için uygulama veritabanına erişemez ve hizmet veremez. | 6 | 5 | 30 | -Detaylı yama yönetimi prosedürü (uyarıları da içeren) geliştirilmeli<br>-Eğitim<br>-Gereksiz iş yükünün azaltılması<br>-Motivasyon |
| | | Yapılandırma | Yanlış | VTYS yazılımın çalışmaması, yavaş çalışması veya veritabanına erişilememesi | -Prosedür yok ya da eksik<br>-Eksik eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Başarısız yapılandırma sonucunda VTYS yazılımı çalışmadığı ya da yavaş çalıştığı için uygulama veritabanına erişemez ve hizmet veremez veya yavaş hizmet verir. | 6 | 5 | 30 | -Detaylı yama yönetimi prosedürü (uyarıları da içeren) geliştirilmeli<br>-Eğitim<br>-Gereksiz iş yükünün azaltılması<br>-Motivasyon |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 17 VTYS Yazılımı (devam) | Veritabanını erişebilir kılmak, ekleme, silme ve güncelleme yapmak ... yönetmek | Tabloya ekleme işlemi | Başarısız | Yeni kayıt yapılamaması | -Tablonun kilitlenmesi (dead lock) | Tablonun kilitlenmesi sonucunda VTYS yazılımı tabloya ekleme yapamadığı için uygulama yeni kayıt yapamaz uzun sürede hizmet veremez. | 8 | 7 | 56 | -SQL optimizasyonu<br>-Uygulamanın VT tasarımının gözden geçirilmesi |
| | | | | | Diskin dolması | Diskin dolması sonucunda VTYS yazılımı tabloya ekleme yapamadığı için uygulama yeni kayıt yapamaz uzun sürede hizmet veremez. | 1 | 7 | 7 | -Kapasite yönetimi<br>-Anlık uyarı mesajları |
| | | | | | -Table spacenin dolması | Table spacenin dolması sonucunda VTYS yazılımı tabloya ekleme yapamadığı için uygulama yeni kayıt yapamaz uzun sürede hizmet veremez. | 1 | 7 | 7 | Otomatik grow |
| | | Veri | Yok | Verilere erişilememesi | -Sabotaj<br>-Çok fazla kullanıcının silme yetkisinin olmasından dolayı istemsizce silinmesi | Sabotaj yada istemsiz işlem kaynaklı verilerin silinmesi sonucunda verilere erişilemez ve uygulama hizmet veremez. | 6 | 10 | 60 | -Bilgi güvenliği tedbirleri<br>-Audit<br>-Yetki düzenlemesi<br>-Test ortamı |
| 18 İşletim Sistemi | Sunucu donanımı üzerinde koşarak WAS çalışması için çalışma ortamı sağlamak | Süreklilik | Yok | İşletim sistemi çalışmaması | -Donanım arızası | Donanım arızası veya virüs bulaşması sonucunda işletim sistemi çalışmasını sürdüremediğinde veritabanına ulaşılamaz ve uygulama hizmet veremez. | 3 | 7 | 21 | Yedeklilik arttırılabilir |
| | | Yapılandırma | Yanlış | İşletim sistemi çalışmaması veya VTYS yazılımını çalıştıramaması | -Prosedür yok ya da eksik<br>-Eksik eğitim<br>-Aşırı iş yükü<br>-Motivasyon eksikliği<br>-Dalgınlık | Başarısız yapılandırma kaynaklı işletim sistemi yada VTYS çalışmadığı ya da yavaş çalıştığı için veritabanına erişilmeyebilir. Uygulama hizmet vermez veya yavaş verir. | 5 | 6 | 30 | -Eğitim<br>-Prosedür<br>-Konfigürasyon yönetimi<br>-Değişiklik yönetimi |
| | | Başlatma | Başarısız | İşletim sisteminin çalışmaması | -Donanım arızası<br>-Eksik sürücü<br>-Desteğin bitmesi | Donanım arızası ya da eksik sürücü kaynaklı işletim sisteminin başlayamaması sonucunda uygulama hizmet veremez. | 3 | 5 | 30 | Test ortamı |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 19 Sunucu Donanımı | Elektronik verileri işleyerek çıktılara dönüştürmek | Fiziksel bütünlük | Yok/Bozuk | Uygulama veri tabanına erişemez | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | VTYS sunucu donanımının fiziksel bütünlüğünün bozulmasıyla veritabanına erişilemez ve uygulama hizmet veremez. | 3 | 7 | 21 | -Enerji ve soğutma alt yapısının güçlendirilmesi<br>-Sıcaklık ve nem değerlerinin sensörlerle kontrolü |
| | | Çalışma performansı | Düşük | Sunucu donanımın yavaşlaması | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | Toz, kir, ısınma ve yıpranma kaynaklı donanım yavaşlaması sonucunda VTYS ve uygulama hizmeti yavaşlar veya kısa süre sonra durur. | 3 | 4 | 12 | -Bakım ve yenileme |
| 20 DBA (Veri Tabanı Yöneticisi) | VTYS yazılımı ile veritabanını yönetmek. | İşe gelme<br>Sisteme erişim | Geç | Sorunlara vaktinde müdahale edememe | -Ulaşım sorunları<br>-Kötü hava şartları<br>-Düzensiz iş planı | Ulaşım sorunu, kötü hava şartları veya düzensiz iş planı kaynaklı veri tabanı yöneticisinin işe geç gelmesi sorunlara geç müdahale edilir ve uygulama hizmeti kesintiye uğrar. | 5 | 5 | 25 | -Nöbet<br>-Uzaktan erişim<br>-İş planlarının düzenlenmesi |
| | | Sağlık sorunu | Var | Sorunlara vaktinde müdahale edememe<br>-Görevleri zamanında yapamama | -Aşırı iş yükü<br>-Olumsuz çalışma şartları<br>-Zayıf bünye | Aşırı iş yükü, olumsuz çalışma şartları ve zayıf bünye kaynaklı veri tabanı yöneticisinin işe geç gelmesi sonucunda sorunlara geç müdahale edilir ve uygulama hizmeti kesintiye uğrar. | 4 | 5 | 20 | -Yedekli personel<br>-Nöbet<br>-Uzaktan erişim |
| | | Çalışma sürekliliği | Yok | -Gerekli değişikliğin zamanında yapılamaması<br>-Sorunlara vaktinde müdahale edilememesi | -Aşırı iş yükü<br>-Düşük maaş<br>-Motivasyon eksikliği<br>-Mobbing<br>-Emeklilik<br>-Askerlik | VT yöneticisinin işten ayrılması sonucunda uygulamanın hizmet vermesi kesintiye uğrayabilir. | 5 | 5 | 25 | -Özlük hakları<br>-Çalışma şartlarının iyileştirilmesi<br>-Prosedürler oluşturularak kişiye bağımlılığın azaltılması<br>-Yedekli personel<br>-Konfigürasyon yönetimi |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 22 Fiber Kablo | SAN switch, depolama ünitesi ve sunucular arasında bağlantı sağlamak | Fiziksel bütünlük | Yok/Bozuk | Veri trafiğinin kesilmesi | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Kablonun fiziksel bütünlüğünün bozulması sonucunda veri trafiği kesilir ve uygulama hizmet veremez. | 2 | 4 | 8 | -Düzenli aralıklarla izleme ve kontrol mekanizması oluşturulmalı<br>-Otomatik uyarı mesajları ayarlanmalı |
| | | Veri iletme | Başarısız | Veri trafiğinin kesilmesi | -Kopma<br>-Yerinden çıkması | Kablonun kopması ya da yerinden çıkması sonucunda veri trafiği kesilir ve uygulama hizmet veremez. | 3 | 4 | 12 | -Düzenli aralıklarla izleme ve kontrol mekanizması oluşturulmalı<br>-Otomatik uyarı mesajları ayarlanmalı |
| 23 HBA | FC kablo üzerinden bağlantı yapılması için arayüz sağlamak | Fiziksel bütünlük | Yok/Bozuk | Sonucunun veri depolama ağı ile bağlantısının kesilmesi | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yıldırım, yüksek güç veya yangın kaynaklı fiziksel SAN switch arızası sonucunda veri trafiği kesilir ve uygulama hizmet veremez. | 1 | 9 | 9 | -Düzenli aralıklarla izleme ve kontrol mekanizması oluşturulmalı<br>-Otomatik uyarı mesajları ayarlanmalı |
| | | Firmware yükseltmesi | Başarısız | Veri trafiğinin kesilmesi veya yavaşlaması | -Isınma<br>-Güç kesintisi<br>-Yanlış prosedürün izlenmesi | Güç kesintisi, yanlış prosedür veya yanlış sürüm kaynaklı başarısız firmware yükseltmesi sonucunda sunucunun veri ağı ile bağlantısının kesilmesi veya yavaşlaması ile uygulama hizmet veremez veya yavaş hizmet verir. | 4 | 4 | 16 | Test ortamı kurulmalı |
| 24 Disk Controller | Disk ünitesinin fiziksel disklere erişimini sağlamak | Fiziksel bütünlük | Yok/Bozuk | Veri trafiğinin kesilmesi | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yıldırım, yüksek güç veya yangın kaynaklı fiziksel SAN switch arızası sonucunda veri trafiği kesilir ve uygulama hizmet veremez. | 3 | 9 | 27 | Düzenli “healt check” test prosedürü oluştutulmalı |
| | | Firmware yükseltmesi | Başarısız | Veri trafiğinin kesilmesi veya yavaşlaması | -Isınma<br>-Güç kesintisi<br>-Yanlış prosedürün izlenmesi | Güç kesintisi, yanlış prosedür veya yanlış sürüm kaynaklı başarısız firmware yükseltmesi sonucunda disk kontrolörün veri ağı ile bağlantısının kesilmesi veya yavaşlaması ile uygulama hizmet veremez veya yavaş hizmet verir. | 5 | 7 | 35 | -Test ortamı<br>Sistem odasının sıcaklığı sık sık kontrol edilmeli,<br>-Ani sıcaklık değişimlerinde SMS le uyarı |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 25<br>Fiziksel Disk | Veri okumak ve yazmak | Fiziksel bütünlük | Yok/Bozuk | -Veri bozulması<br>-Veri tabanına erişilememesi | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yıldırım, yüksek güç veya yangın kaynaklı fiziksel disk arızası sonucunda disk üzerindeki veriler bozulur ve uygulama hizmet veremez. | 2 | 10 | 20 | Verinin online ve kısa aralıklarla yedeklenmesi |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılı | Şidde | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 26 RAID | Performans ve yedeklilik amacıyla fiziksel diskleri guruplamak ve yönetmek için arayüz oluşturmak | Bozuk disk değiştirme | Farklı | Disklere erişilememesi | -Prosedürün olmaması<br>-Yetersiz eğitim<br>-Aşırı iş yükü | Bozuk disk yerine sağlam diskin değiştirilmesi sonucunda veri tabanına erişilemez ve uygulama hizmet veremez. | 6 | 9 | 54 | -Eğitim verilmeli<br>-İşlemler için prosedür oluşturulmalı<br>-Yüksek seviyeli RAID yapısı kullanılmalı<br>-Çalışan üzerindeki fazla ya da gereksiz iş yükü kaldırılmalı<br>-Çalışan motive edilmeli<br>-RAID ve pooling yapılandırması kullanılabilir. |
| | | Yapılandırma | silinmesi | RAIDin bozulması<br>-Verinin bozulması<br>-Disklere erişememe | -Yetersiz eğitim<br>-Sabotaj<br>-Aşırı iş yükü<br>-Prosedürün olmaması | RAID yapılandırmasının silinmesi sonucunda veri tabanına erişilemez ve uygulama hizmet veremez. | 2 | 10 | 20 | Raid yapılandırmasını iki kişi aynı anda yapacak şekilde Administratör rolü iki kişiye paylaştırılabilir. |
| | | | Düşük seviye | Veri okuma yazmanın yavaşlaması | -İhtiyaç gereksiniminin planlanmaması<br>-Prosedürün olmaması | Disklerin düşük seviye bir RAID ile yapılandırmanın sonucunda disklere okuma yazma yavaşlar ve uygulama yavaş hizmet verir. | 3 | 3 | 9 | -Sistem kurulum ve konfigürasyon yönetimi prosedürünün oluşturulması<br>-Yeniden yüksek seviye RAID yapılandırması yapılabilir |
| | | Bozulan disk sayısı | Çok | RAIDin bozulması<br>-Verinin bozulması<br>-Disklere erişememe | -Yıpranma<br>-Titreşim<br>-Elektrik kesintisi<br>-Destek anlaşmasının eksikliği | Aynı RAID yapılandırması içinde çoklu diskin bozulması sonucunda veri tabanına erişilemez ve uygulama hizmet veremez. | 3 | 9 | 27 | -Yüksek seviyeli RAID yapısı kullanılmalı<br>-Hotspare disk sayısı arttırılmalı.<br>-Yedekte disk bekletilmeli<br>-RAID ve pooling yapılandırması kullanılabilir<br>- Verinin senkronize yedeklenmesi |
| 27 LUN | SAN storage üzerinde mantıksal disk bölümleri oluşturmak | LUN yapılandırılması | İstemsiz silinmesi | Verilerin bozulması | -RAID yapısının bozulması<br>-Sabotaj<br>-Aşırı iş yükü | LUN yapılandırmasının silinmesi sonucunda veri tabanına erişilemez ve uygulama hizmet veremez. | 4 | 9 | 36 | Verinin online ve kısa aralıklarla yedeklenmesi |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| **Sistem:** <Uygulama2> | | **Alt Sistem:** Hastane Alt sistemi | | | **HAZOP ANALİZİ** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Sıra No / Bileşen** | **Fonksiyon/Amaç/ işlem** | **Parametre** | **Referans Anahtar Kelime** | **Sonuç/ sapma** | **Neden** | **Tehlike** | **Olasılık** | **Şiddet** | **Risk** | **Öneriler ve Düşünceler** |
| 28<br>Ağ Yapısı | Hastanedeki bilgisayarların <Uygulama2> uygulamasına erişmesini sağlamak | Fiziksel bütünlük | Yok/Bozuk | Ağ bağlantısının kesilmesi | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yangın vb. kaynaklı ağ bağlantısının kesilmesi sonucu hastane bilgisayarları uygulamaya erişemezler. | 6 | 2 | 12 | -Kanallar ayrılmalı ya da izolasyon yapılmalı |
| | | Parazit | Var | Veri paketlerinde kayıp | Ağ kablosu ile elektrik kablosunun yakın geçmesi veya yalıtım olmaması | Elektrik kabloları aynı kanaldan geçme kaynaklı ağ kablosunda parazit oluşur ve hastane bilgisayarları uygulamaya erişirken gecikmeler yaşanır. | 4 | 3 | 12 | Kanallar ayrılmalı ya da izolasyon yapılmalı |
| | | Sinyal | Zayıf | Veri paketlerinde kayıp | Uzun kablo kullanılması | Gereğinden uzun kablo kullanmadan kaynaklı ağ kablosunda parazit oluşur ve hastane bilgisayarları uygulamaya erişirken gecikmeler yaşanır. | 3 | 2 | 6 | Ağ kabloları için uzunluk standardı oluşturulmalı ve mevcutlar tespit edilmeli |
| 29<br>Bilgisayar | <Uygulama2> uygulamasını kullanmak için ortam sağlamak veya arayüz oluşturmak (internet tarayıcı) | Fiziksel bütünlük | Yok/Bozuk | Bilgisayarın çalışmaması | -Yangın<br>-Yıldırım<br>-Yüksek güç<br>-Korozyon<br>-Kullanıcı hatası | Yangın vb. nedenlerden dolayı hastanedeki bilgisayarın fiziksel bütünlüğünün bozulmasıyla hastane personeli uygulamaya erişemez. | 6 | 2 | 12 | -Bilgisayarlara periyodik bakım<br>-Thin client kullanımı |
| | | Çalışma performansı | Düşük | Bilgisayar donanımın yavaşlaması | -Toz/Kir<br>-Isınma<br>-Yıpranma<br>-Korozyon | Hastanedeki bilgisayarların yavaşlaması sonucunda uygulamaya erişim yavaşlar ve sağlık hak sahiplerine sunulan hizmetler aksar. | 6 | 2 | 12 | -Thin client kullanımı<br>-Gereksiz uygulamaların kaldırılması |
| | | Başlatma | Başarısız | Bilgisayar çalışmaz | -Virüs bulaşması<br>-Çökmesi | Donanım arızalanması sonucu bilgisayarlar çalışmayabilir ve hastane personeli uygulamaya erişemez. | 6 | 2 | 12 | -Antivirüs güncelleme takibi<br>-USB kullanımı kısıtlanmalı |

EK-2. (devam) HAZOP Risk Analizi Tablosu

| Sıra No / Bileşen | Fonksiyon/Amaç/ işlem | Parametre | Referans Anahtar Kelime | Sonuç/ sapma | Neden | Tehlike | Olasılık | Şiddet | Risk | Öneriler ve Düşünceler |
|---|---|---|---|---|---|---|---|---|---|---|
| 30 Teknik Personel | Hastane bilgisayar ve ağ yapısına bakım yapmak ve sorunlara müdahale ederek personelin <Uygulama2> uygulamasına erişebilmesini sağlamak | Personel sayısı | Az | Sorunlara zamanında müdahale edememe | Kapasite planlaması olmaması | Hastane bilgisayar ve ağ yapısında bir sorun oluştuğunda teknik personel sayısının az olmasından dolayı sorunlar uzun süre devam eder ve uygulamaya erişilemez. | 7 | 2 | 14 | Kapasite planlamasının yapılması |
| | | Yeterli beceri | Yok | Ağ ve bilgisayar problemlerinin zamanında giderilememesi | -Yetersiz eğitim<br>-Yanlış seçim | Teknik personel yeterli beceriye sahip olmadığında oluşan sorunlara oluştuğunda sorunlar uzun süre devam eder ve uygulamaya erişilemez. | 6 | 2 | 12 | -Eğitim<br>-Seçim kriterlerinin düzenlenmesi |
| | | İş gelme | Geç | Ağ ve bilgisayar problemlerine geç müdahale | -Ulaşım sorunları<br>-Kötü hava şartları<br>-Düzensiz iş planı | Hastane bilgisayar ve ağ yapısında bir sorun oluştuğunda teknik personelin işe geç gelmesinden dolayı sorunlar uzun süre devam eder ve uygulamaya erişilemez. | 6 | 2 | 12 | -İş planlarının gözden geçirilmesi<br>-Vardiyalı çalışma<br>-Yedekli personel |
| 31 Hastane Bilgi Yönetim Yazılımı | <Uygulama2> ile entegre şekilde hastaların kabul ve tedavi işlemlerinin takibini yapmak. | Çalışma performansı | Düşük | <Uygulama2> ile iletişimi yavaşlar | -Test ve standart getirilmemesi | Hastana Bilgi Yönetim Sisteminin düşük performansından kaynaklı <Uygulama2> ile iletişimi yavaşlar ve sağlık hak sahiplerinin işlemleri gecikir. | 5 | 5 | 25 | Hastana Bilgi Yönetim Sistemi için bazı gereksinimler belirlenmeli. |

# ÖZGEÇMİŞ

## Kişisel Bilgiler


| | | |
|---|---|---|
| Soyadı, adı | : | İLTER, İsmail |
| Uyruğu | : | T.C. |
| Doğum tarihi ve yeri | : | 18.01.1986 Tuzluca |
| Medeni hali | : | Evli |
| Telefon | : | 0 (312) 595 87 70 |
| e-mail | : | iilter@ s g k .gov.tr |


| Eğitim Derecesi | Okul | Mezuniyet yılı |
|---|---|---|
| Lisans | Yıldız Teknik Üniversitesi/ EHM Mühendisliği | 2008 |
| Lise | Çapa Anadolu Öğretmen Lisesi | 2003 |

| İş Deneyimi, Yıl | Çalıştığı Yer | Görev |
|---|---|---|
| 2008 | THY | Yolcu hizmetleri memuru |
| 2008-2011 | Albaraka | Sistem Yöneticisi |
| 2011-devam ediyor | S G K | Uzman |

## Yabancı Dil

İngilizce

## Yayınlar

## Diğer Tezler

**1.** İlter, İ., Baltat, H. (2014) "İnteraktif bilgi teknolojileri yönetim sistemi ve hizmet sunmu genel müdürlüğünde örnek bir uygulama", Uzmanlık Tezi

## Hobiler

Masa Tenisi, Fotoğrafçılık, Teknoloji



*GAZİ GELECEKTİR...*