T.C. ANADOLU ÜNİVERSİTESİ YAYINI NO: 2489
AÇIKÖĞRETİM FAKÜLTESİ YAYINI NO: 1460

# GÜVENLİK SİSTEMLERİ

***Yazarlar***

*Doç.Dr. Yusuf OYSAL (Ünite 1)*

*Doç.Dr. Hüseyin POLAT (Ünite 2, 4, 8)*

*Yrd.Doç.Dr. Cüneyt AKINLAR (Ünite 3, 5, 6)*

*Arş.Gör.Dr. Efnan ŞORA GÜNAL (Ünite 7)*

***Editör***

Doç.Dr. Yusuf OYSAL

**ANADOLU ÜNİVERSİTESİ**

**UZAKTAN ÖĞRETİM TASARIM BİRİMİ**

**Genel Koordinatör**
*Doç.Dr. Müjgan Bozkaya*

**Genel Koordinatör Yardımcıları**
*Doç.Dr. Hasan Çalışkan*

**Öğretim Tasarımcıları**
*Yrd.Doç.Dr. Seçil Banar*
*Öğr.Gör.Dr. Mediha Tezcan*

**Grafik Tasarım Yönetmenleri**
*Prof. Tevfik Fikret Uçar*
*Öğr.Gör. Cemalettin Yıldız*
*Öğr.Gör. Nilgün Salur*

**Kitap Koordinasyon Birimi**
*Uzm. Nermin Özgür*

**Kapak Düzeni**
*Prof. Tevfik Fikret Uçar*
*Öğr.Gör.Cemalettin Yıldız*

**Dizgi**
*Açıköğretim Fakültesi Dizgi Ekibi*

**Güvenlik Sistemleri**

ISBN
978-975-06-1157-5

1. Baskı

Bu kitap ANADOLU ÜNİVERSİTESİ Web-Ofset Tesislerinde 1400 adet basılmıştır.
ESKİŞEHİR, Mayıs 2012

# İçindekiler

# Önsöz

Teknoloji ve elektronik son yıllarda hayatımızı kaçınılmaz bir şekilde etkilemiştir. Bundan 20 yıl öncesine kadar cep telefonları lüks olarak görülürken hayatımızın en önemli ihtiyacı haline gelmiştir. İnternet bir evde olmazsa olmazlar arasındadır. Daha ilkokul seviyesinde çocuklar bilgisayar kullanmakta, arkadaşlarıyla mesajlaşmakta ve internet üzerinden tanıdıklarına resim gönderebilmektedirler. Özellikle bankacılık işlemlerinin ev ve ofis ortamında yapılması teknolojinin getirdiği kolaylıklar arasındadır. Teknolojinin getirdiği bu gibi avantajlar sayesinde toplumsal kabiliyetler artmış, daha fazla otomasyon daha fazla kazanç anlamına gelmiştir.

Teknolojideki bu yenilikler doğal olarak güvenlik sistemlerini de yenilemiştir. Gelişen elektronik, güvenlik sistemlerinin fonksiyonel bir parçası halini almıştır. Örneğin yanlış alarmı önlemek için güvenlik sistemlerinin işlevsel kabiliyeti artırılmış, çevre donanımları ile merkezi istasyonun haberleşmesi hızlandırılmış ve bina giriş-çıkışları akıllı kartlarla daha da özellikli hale getirilmiştir. Günümüzde internet-intranet elektronik marketlerden de kolaylıkla alabileceğimiz birçok alarm sistemlerinin ve kapalı devre televizyon sistemlerinin araçları haline gelmiştir.

Gelişen teknolojinin sunduğu gelişmiş ve akıllı elektronik sistemlerle zenginleşen güvenlik araçları, bu araçları kullanan güvenlik görevlilerinin birtakım teknik bilgilerle donatılması zorunluluğunu ortaya çıkarmıştır. Fakat maalesef bir güvenlik görevlisinin gelişen teknolojiye ayak uydurması ve belli bir elektronik sistem üzerinde profesyonel olması mümkün değildir. Burada yapılması gereken elektronik güvenlik sisteminin bütünü yerine kullanılmasını onlara öğretmektir. Çünkü profesyonel anlamda güvenlik görevlisinden yıllardan beri beklenen fiziksel güvenliktir. Elektronik donanımlar sadece onlara yardımcı olacak, onların işlerini kolaylaştıracak unsurlardır. Bu yüzden bir güvenlik görevlisinden bir elektronik güvenlik sisteminin kurulması, sistem ayarlarının yapılması ve çalışma mantığını bilmesi beklenmemelidir.

Bugün bile elektronik güvenliğin fonksiyonel alanına uygulanacak bilgi sınırlıdır. Örneğin, kapalı devre televizyon sistemi (CCTV) içerisinde kameraların, dijital kaydedicilerin, ışıklandırmanın ve birçok haberleşme elemanının matrissel bir organizasyonla bütünleştirildiği bilgisi olmasına rağmen tüm bu bileşenlerin nasıl biraraya getirildiğine dair teknik bir bilgiye sahip olmak zordur. Elektronik güvenlik sistemin nasıl oluşturulduğuyla ilgilenmek yerine hangi ortamda hangi elektronik sisteme ihtiyacın olduğuyla ilgilenmelidir. Bu kitabın amacı da bir mühendislik bilgisi vermek yerine, güvenlik görevlilerine çalışma hayatında yardımcı olacak sistemleri tanıtmak ve anlamasına yardımcı olmaktır. Hali hazırda kullanılabilecek tüm sistemlerin bu kitap içerisinde yer alması tabii ki mümkün değildir. Bu kitapta anlatılacak elektronik sistemlerin birçok uygulama sahası vardır ve bu cihazlar üzerinde kazanılacak tecrübeler hem güvenlik görevlilerinin işini kolaylaştıracak hem de yeni güvenlik teknolojilerine çabuk adaptasyonlarını sağlayacaktır.

Editör

Doç.Dr. Yusuf OYSAL

# 1

## Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Güvenlik sistemlerinin kullanım gerekçelerini anlatabilecek,
- Güvenlik sistemlerinin kullanım nedenlerini açıklayabilecek,
- Kuruluşları tehdit eden iç ve dış faktörleri örnekleyebilecek,
- Kuruluşların güvenlik açıklarını ve alınacak önlemleri anlatabilecek,
- Riski tanımlayabilecek,
- Risk analizinin yapılma gerekçesini ve risk analizinin yapılma aşamalarını anlatabilecek,
- Güvenlik sistemleri seçilirken dikkat edilen hususları açıklayabilecek

bilgi ve becerilere sahip olabilirsiniz.

## Anahtar Kavramlar

- Güvenlik
- Tehlike
- Tehdit
- Risk
- Önlem
- Tespit
- Değerlendirme
- Geciktirme
- Savunma
- Yönetim

## İçindekiler

# Güvenlik Sistemi Kavramları

## GİRİŞ

İnsanlar yıllar boyu kendilerini tehdit eden unsurlara karşı önlem alma ihtiyacı duymuştur. Tehdit insanları, canlıları veya kuruluşları riske sokabilecek eylem ve olaylardır. Risk ise belirli bir tehlikeli olayın meydana gelme olasılığı ile bu olaydan ortaya çıkabilecek zarar veya hasarın şiddetinin tahminidir. Risklere karşı önlem almak için kullanılan elektronik güvenlik sistemleri günlük hayatımızın bir parçası haline gelmiştir. Modern bir güvenlik sistemi yapısal olarak elektronik bileşenler dizisi olarak algılama, değerlendirme ve tepki vermek için tasarlanır. Örneğin modern güvenlik sistemi herhangi bir odadaki hareketi algılar, bu hareketin tehdit olup olmadığına karar verir ve karşı tedbirini alır. Burada insan faktörünü de unutmamak gerekir. Bahsedilen modern güvenlik sisteminin akıllı teknolojiler kullandığı varsayılmıştır. Fakat genel anlamda bir güvenlik sisteminin kulanıcıları olan güvenlik görevlileri algılanan hareketin yorumunu yapmak durumundadırlar. Bu yüzden kullanılan güvenlik sistemi hakkında karar verecek düzeyde bilgiye sahip olmalıdırlar.

Elektronik teknolojileri ve yazılım teknolojilerinin birlikte kullanılması ile geliştirilen günümüz güvenlik sistemleri daha fonksiyonel bir yapı kazanmıştır. Örneğin yanlış alarmı önlemek için güvenlik sistemlerinin işlemsel kabiliyeti artırılmış, çevre donanımları ile merkezi istasyonun haberleşmesi hızlandırılmış ve bina giriş-çıkışları akıllı kartlarla daha da özellikli hale getirilmiştir. Bugün bile elektronik güvenliğin fonksiyonel alanına uygulanacak bilgi sınırlıdır. Örneğin, kapalı devre televizyon sistemi (CCTV) içerisinde kameraların, dijital kaydedicilerin, ışıklandırmanın ve birçok haberleşme elemanının matrissel bir organizasyonla bütünleştirildiği bilgisi olmasına rağmen tüm bu bileşenlerin nasıl biraraya getirildiğine dair teknik bir bilgiye sahip olmak zordur. Elektronik güvenlik sistemin nasıl oluşturulduğuyla ilgilenmek yerine hangi ortamda hangi elektronik sisteme ihtiyacın olduğuyla ilgilenmelidir. Bundan sonraki bölümlerde günümüzde yaygın olarak kullanılan güvenlik sistem bileşenleri elektroniksel detaya girilmeden yüzeysel olarak tanıtılacaktır. Güvenlik ve koruma görevlilerine verilen bu ön bilgiler, ileride kullanacakları sistemlerin üretici firmaları tarafından daha detaylı verilecek eğitimleri aşamasında yardımcı olacaktır.

Güvenlik sistemlerinin tanıtımının yapıldığı diğer bölümleri okurken dikkat edilmesi gereken noktalar vardır. Güvenlik ana unsuru insanlar ve diğer canlıları tehdit eden unsurlara karşı alınacak önlemlerdir. Bu önlemler alınırken kullanılacak güvenlik sistemleri canlılara zarar vermemelidir. Günümüzde kullanılan televizyon ve cep telefonu gibi elektronik cihazlar bile insan sağlığına farkedilmeyecek zararlar verirken, elektornik güvenlik sistemlerinin zararsız olduğu söylenemez. Ama zararlarından bilgili ve bilinçli olma sayesinde etkilenilmeyebilir. Bu yüzden bu cihazların nasıl kullanılacağı hakkında bilgi sahibi olmak gerekir. Örneğin bir X-ışını cihaza insan vücudunun bir kısmı dahi sokulmamalıdır. Çünkü yüksek derecede radyasyon vardır.

Diğer bir konu da bu sistemler kişinin özelini ortaya dökücü şekilde kullanılmamalıdır. Örneğin kişilerin eşyaları kontrol edilirken tüm çantadakilerin çıkarılması ve diğer insanların bunu görmesi yanlıştır. İşte burada uygun bir güvenlik sistemi kullanılarak çantadaki eşyaların incelenmesi sağlanabilir. Bundan sonraki ünitelerde anlatılanların bir amacı da neyi nerede kullanacağımız konusunda bize yardımcı olmaktır. Her bölümde anlatılan güvenlik sistemlerinin hangi amaç için kullanılabileceği çok iyi anlaşılmalıdır.

# GÜVENLİK SİSTEMLERİ KULLANIMININ YASAL DAYANAĞI

Dünya nüfusunun artmasıyla birlikte kalabalık yerleşim yerlerinin oluşması, aynı yerleşim yerinde yaşayan insanlar arasında bir güvenlik sorununun da ortaya çıkmasına neden olmuştur. Gerek devlet kurumları ve gerekse özel kuruluşlar güvenlik ihtiyacını karşılamak üzere personel görevlendirmenin yanısıra gerekli görülen elektronik sistemleri de satın almaktadırlar. Bankalar, alışveriş merkezleri, fabrikalar, kuyumcular ve idari şirket binaları; kendilerine yönelik tehdit algılamaları arttığı ve faaliyetlerine müşteriler ve çalışanlar için daha güvenli bir şekilde devam etmeleri gerektiğinden, özel güvenlik görevlilerinin işlerini kolaylaştıracak kapalı devre televizyon sistemi gibi birçok güvenlik donanımlarını da güvenlik uygulamasında kullanmaktadırlar. Bu konu güncel haberlerde de yerini almaktadır. Örneğin Anadolu Ajansı'nın 06.07.2011 tarihli haberi şu şekildedir:

> "*Kadirli'de Hükümet Konağına X-Ray Cihazı Konuldu. Kadirli Kaymakamı Abdul Rauf Ulusoy, hükümet konağı girişine X-Ray cihazının konulduğunu bildirdi. Ulusoy, Anadolu Ajansı muhabirine yaptığı açıklamada, güvenlik açısından önemli bir yere sahip olan hükümet konağı girişine konulan X-Ray cihazının faaliyete geçtiğini ve vatandaşların bundan sonra işlemlerini yaptırmak için bu cihazdan geçeceklerini ifade etti. Bundan sonra hükümet konağında çalışan ve gelen vatandaşların daha rahat ve huzurlu bir şekilde olmalarını sağlamak amacıyla cihazı kurdurduklarının anımsatan Ulusoy, güvenlik açısından önceden tedbir alınmasının önemli olduğunu kaydetti.* "

Güvenlik sistemlerinin kullanılmasının hukukun üstün olduğu toplumlarda yasal bir dayanağı olması gerekir. Bunun için ülkemizde 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun çıkarılmıştır. Bu kanunun 7. maddesinin a ve f fıkralarında özel güvenlik görevlilerine bazı elektronik güvenlik sistemlerini kullanabilme yetkisi verilmiştir. Bu ifadeler şu şekilde kanunda yer almaktadır.

a) Koruma ve güvenliğini sağladıkları alanda girmek isteyenleri duyarlı kapıdan geçirme, bu kişilerin üstlerini dedektörle arama, eşyalarını X-ray cihazından veya benzeri güvenlik sistemlerinden geçirme.

f) Hava meydanı, liman, gar, istasyon ve terminal gibi toplu ulaşım tesislerinde kimlik sorma, duyarlı kapıdan geçirme, bu kişilerin üstlerini dedektörle arama, eşyaları X-ray cihazından veya benzeri güvenlik sistemlerinden geçirme.

# GÜVENLİK SİSTEMLERİNİN KULLANIM NEDENLERİ

Bilindiği üzere güvenlik ana unsuru insan ve diğer canlıların haklarını korumak olan önleyici tedbirler zinciridir. Özel güvenlik görevlilerinin öncelikli hedefi suçların önlenmesidir. Güvenlik sistemleri deyince de ses, ısı, ışık, titreşim ya da hareket bilgilerini algılayan elektromekanik cihazlar aklımıza gelmelidir. Özel güvenlik hizmetinden yararlanan kişi ve kuruluşlar karşılaşabilecekleri suç unsurlarının en aza indirilmesini beklerler. Bunun içinde öncelikle faaliyet gösterdikleri binaları ve çevreyi düzenlemeleri gerekir. Bunun için kullanılacak güvenlik cihazlarından uygun olanın belirlenmesinde olası iç ve dış tehditlerle güvenlik açıklarının belirlenmesi ve bunlara karşı risk analizinin yapılması önemli rol oynamaktadır.


**Günlük hayatta karşılaştığınız güvenlik görevlileri nerelerde bulunuyor ve hangi güvenlik sistemlerini kullanıyorlar?**


**Resim 1.1:** Güvenlik Sistemleri Seçim Prosedürü

## İç Tehditler

Şahıs, kurum veya kuruluşların karşılaşabilecekleri potansiyel tehlikeler, acil alarm durumları, maddi ve manevi uğruyabilecekleri zararların sebeplerinin belirlenmesi çalışmalarına tehdit değerlendirmeleri denir. Tehditler ilgili kurum bünyesinden de kaynaklanabilir dış faktörlere de bağlı olabilir.

İç tehditler arasında kurum çalışanlarından kaynaklanan tehditler söz konusudur. Çalışanların sayısı, eğitim ve kültür seviyeleri ve birbirlerine gösterdikleri anlayış güvenlik önlemi alınması konusunda önemli faktörlerdir. Bir kuruluşun içerisindeki çalışanların bölgesel farklılıkları önemli sorunlar oluşturabilir. Örneğin ülkemiz içerisinde kültürel olarak birbirinden farklı birçok coğrafi bölge vardır. Insan yaratılış gereği bulunduğu bölgenin insanlarına onlardan birisi olma duygusuyla daha fazla sevgi duyabilir. Aynı işe talip bir yakınının yerine başka birisinin görevlendirilmesini hazmedemeyebilir. Bu gibi örnekler genellendiğinde kuruluşun homojenliği yani çalışanların farklı bölge ilişkisi içerisinde olması unsuru gözardı edilmemelidir.

Çalışanlardan kaynaklanabilecek diğer bir tehdit etkeni de işçi-işveren ilişkisidir. Bu ilişkinin bozulmasına sebep olabilecek nedenlere bakıldığında sendikal ilişkilerin işverenin menfaatlerinin önüne geçmesi, çalışanların çok çalışıp az para almaları yani ekonomik nedenler ve çalışılan sektörün gerektirdiği hassasiyetin çalışanlara olumsuz yansımalarıdır. Güvenlik ihtiyacının artmasına neden olabilecek sektörden kaynaklanan hassasiyete örnek verecek olursak silah üreten bir firmanın alacağı güvenlik tedbirleri ile çikolata üreten bir fabrikanın güvenlik tedbirleri birbirinden çok farklı olacaktır. Özel sektörde üretimin rutin değerlerin dışına çıkması durumu da çalışanları strese sokup huzursuzlukların olmasına sebep olabilecek bir örnektir. İş yerindeki şiddet olayları, şirketlerin karşısındaki en önemli tehditlerden birisidir.

Güvenlik sadece güvenlik ve koruma sayısı açısından bakılmaması gereken bir konudur. Olası tüm tehditlere karşı alınması gereken önlemler bütünüdür. Bu kapsamda kuruluşları tehdit eden en önemli zararlardan birisi de yangındır. İç tehditler arasında ülkemizde yangın olayları sayısal olarak üst sıralarda yer alır. Yangına yol açan nedenlerin başında, üretilen madde ve kullanılan malzemelerin özelliklerine gore yanmalarını önleyici tedbirlerin alınmaması gelir. Örneğin, elektirk tesisatının tam korumalı yapılmaması, binalarda özellikle çatı kısmında ahşap kullanılması ve kirişlerin düzgün sıvanmaması, ısı tesisatlarında doğalgaz kaçağının olup olmadığının kontrol edilmemesi yangınlara davetiye çıkartmaktadır. Ülkemizde her yıl birçok fabrikada yangın çıkmaktadır. Güncel bir örnek olarak aşağıdaki haber verilebilir:

> "*Adana'da çırçır fabrikasında çıkan yangında ilk belirlemelere göre yaklaşık bin ton pamuk yandı. Çok sayıda ekip ile olaya müdahale eden itfaiye yetkilileri, yangının tamamen soğutulması için uzun süreli çalışma yapacaklarını bildirdi.*" Anadolu Ajansı [3097838] Haber Yayın Tarihi: 31.10.2011 22:00

Kuruluş sahipleri ve yöneticileri çalışanlarına güvenli bir ortam sunmak zorundadır. Güvenli bir ortamın sağlanamadığı bir iş yerinde verimlilikten, çalışma huzurundan ve nihayet ticari kazançtan bahsetmek de mümkün değildir.

## Dış Tehditler

Dış tehditler korunması hedeflenen mekân içerisindeki insanların can güvenliğine zarar verecek; şirketin varlıklarının zarar görmesine ve ticari faaliyetlerin kesintiye uğramasına neden olabilecek hırsızlık, terör olayları, organize suçlar, sabotaj gibi olası tehditlerdir.

Son yıllarda ülkemizde terör saldırıları gündemden düşmemektedir. Teröristler ülkemizin sınır bölgelerinde beklenmedik saldırılar düzenleyip askerlerimizi ve sivil halkı katlederken bu olayların ülkemizin tüm bölgelerinde olmasından endişe edilmektedir. Teröristlerin sıkça yaptığı eylemlerden birisi de sabotajdır. Sabotaj; devlete ekonomik zarar vermek için kamu ve özel kuruluşlara hasar vererek üretimi durdurmak maksadı ile yapılan eylemlere denir. Maalesef günümüzde esnafa kepenk kapatma ve iş yerlerine kalıcı ekonomik zararlar verme önemli dış tehditler arasındadır.

Teröristler araçlı ve yaya olarak binalara ya da bina yakınlarına gelerek bomba yüklü araçlarla ya da intihar saldırıları ile ağır hasarlar oluşturabilecek tehlikeler saçmaktadırlar. Bu ifadelerin yazıldığı günlerde bir annenin çocuklarını kurtarmak adına kendini feda ederek birçok insanın canını kurtardığı sonuçsuz bir intihar saldırısının haberi gazetelerde şu şekilde yer almıştır:

> ” *Bingöl'deki terör saldırısında ölen Hatice Belgin'in son anda canlı bombanın üzerine atlayıp çok daha fazla insanın can vermesini önlediği ortaya çıktı. Belgin hem 3 çocuğunun hem de onlarca insanın hayatını kurtarmış oldu.*” (Sabah Gazetesi, 31.10.2011)

Kimliği belirsiz insanlar tarafından mekan içerisine ya da dışına konulmuş ya da posta ile gönderilmiş patlayıcı içerebilecek paketler de önemli dış tehdit oluşturmaktadır. Korunan mekânın yapısından da kaynaklanan güvenlik açıklarının kullanıldığı bu tip saldırılar dikkate edilmesi gerekmektedir.

Dikkat edilmesi gereken diğer bir husus ta kuruluşun bulunduğu çevredeki adi suçların sıklığının incelenmesi gerektiğidir. Eğer korunan alanın civarında silahlı ya da bombalı hırsızlık ya da terör saldırıları oluyorsa, bu tehlikelerden çalışanların ve tesislerin zarar görmemesi gerekir. Bunun için gerekli çevresel ve fiziksel önlemler alınmalıdır.

Diğer bir konu ise güvenliği sağlanacak kurumun bünyesinde çalışan kişilerden önemli görevlerde bulunanlar için ayrı bir güvenlik zincirinin oluşturulmasıdır. Kurum hizmetlerinde kilit rol oynayan kişi ya da birimlere silahlı saldırı ve suikast gibi girişimler önemli dış tehditlerdir.

Son olarak dış tehditler konusunda gözönünde bulundurulması gereken diğer bir durum ise toplumsal olaylardır. Halkı tahrik edip galayana getirme olarak bildiğimiz suça teşvik edici faktörler günümüzde sıkça konuşulur hale gelmiştir. Burada tahrikçilerin asıl amacı önceden belirlemiş oldukları kişi ya da kurumları kötüleyerek toplumsal olayların tırmanmasına zemin hazırlamaktır. Bu sayede özellikle kamu kuruluşlarına yönelik doğrudan taşlı ya da sopalı saldırıların yapılması hedeflenmektedir. Bu duruma şu güncel olay güzel bir örnek teşkil eder:

> “*Minibüsçüler belediyeyi ateşe verdi. Adıyaman Kahta'da yeni açılan minibüs hatları, eski minibüs şoförlerini kızdırdı. Belediye önünde toplanan minibüsçülerin ateşe verdiği araç belediye binasına dalınca felaketin eşiğinden dönüldü. Adıyaman ’ın Kahta İlçesi’nde, ilçede yeni açılan hatlar için 10 yeni minibüsün sefere başlaması, mevcut minibüs şoförleri tarafından protesto edildi. Belediyenin bu yöndeki kararını protesto için Belediye’nin bulunduğu caddeye gelen şoförler, caddeyi trafiğe kapatıp, bir minibüsü ateşe verdi. Yanan minibüsün belediye giriş kapısını kapatmasının ardından alevler belediye binasına da sıçradı. Onlarca kişi indikleri giriş katında açtıkları pencereden kendilerini panikle dışarı atarken, içeride kalanlar ise güvenlik güçlerinin müdahalesinin ardından yangına müdahale eden itfaiye araçlarının merdiveniyle dışarı çıkarıldı.*” (Posta Gazetesi, 14.10.2011)

İsyan ya da ayaklanmayla başlayan toplumsal olayların masum insanların zarar görmesine sebebiyet verecek şekilde neticeler doğurabileceği bu örnekte açıkça görülmektedir.


**Günümüzde en yaygın olan dış tehditler sizce hangileridir?**

# GÜVENLİK AÇIKLARI VE ALINACAK TEDBİRLER

Güvenlik açıklarının belirlenmesi demek korunan mekân içerisindeki kritik varlıklara ya da şahışlara erişime yönelik olası sızmalara yol açabilecek fiziksel boşlukların belirlenmesi demektir. Her mekanın; mimari plan çerçevesinde bir güvenlik planlaması yapılmamış ise, mutlaka bir güvenlik açığı vardır. Olası suçlu saldırısına olanak sağlayacak bu fiziksel açıkların iyi analiz edilmesi gerekir. Bu analiz sırasında;

- Binaya olası sızma yönleri belirlenir.
- Sızma yönlerindeki mevcut fizikî engeller ve bunların geciktirme süreleri belirlenir.
- Fiziki engellerin zorluk dereceleri ve aralarındaki bağlantı özellikleri belirlenir.
- Kullanılan güvenlik tedbirlerinin sızmalara karşı gerekli tepki süresi hesaplanır.
- İlave tedbirler belirlenir

Güvenlik tedbirlerinin en önemli amacı potansiyel suçluların eylemlerinden vazgeçmelerini ya da eylemlerini gerçekleştirememelerini sağlamaktır. Bunun en kolay yolu güvenlik açıklarını kapatacak tedbirleri almaktır. Güvenlik açığını kapatacak en önemli faktör çevre düzenlemelerinde yapılacak değişikliklerdir. Bu değişiklikleri yapmamızı sağlayacak kriterler şunlardır:

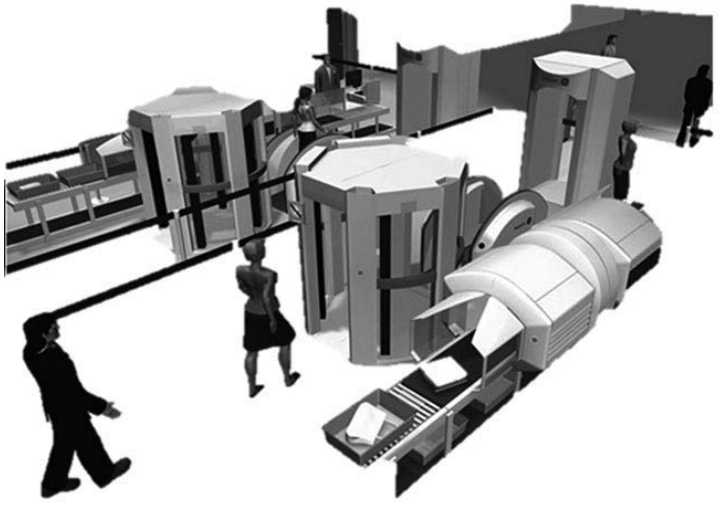
- Çevredeki kolluk veya güvenlik kuvvetlerinin konumu ve gücü
- Çevredeki işletmelerin güvenlik ihtiyacı
- Çevrede işlenen suçların cinsi ve miktarı
- Çevredeki kuruluşların aldığı güvenlik tedbirleri
- Tesislere yaklaşma yolları
- Tesislerin dış ve iç aydınlatma durumu
- Komşu binaların yakınlığı ve yapısı
- Arazini yapısı yani işletme içerisinden geçen dere, boru hattı, vs.
- Varsa sahile ya da çevre yollarına olan yakınlık
- Bölgenin iklim özellikleri
- İşletmenin dış sınır özellikleri; duvar, tel örgü, vs.
- Çevredeki trafik akışı,
- İşletme çevresinin ıssızlık durumu

Çevre düzenlemesi yaparken, sıklıkla hazırlanan yardımcı ikaz levhaları, mekânda bulunan normal kişilerin kendilerini güvende hissetmelerini sağlarken, potansiyel suçlulara eylemlerinin yüksek riskli olduğunu anlatır.

Mekânlardaki en önemli güvenlik açığı suç işleme hazırlığında olan kişilerin ıssızca girme teşebbüsünde bulunacağı erişim yolarının bulunmasıdır. Bunun için çevre düzenlerken yapılması gerekenler şunlardır:

- Binanın çevresinde görüşü azaltacak çukur, hendek ve küçük tepecikler gibi tabii toprak yapıları düzeltilmelidir.
- Binalar arasında yer alan ortak kullanım alanlarının ya da patika yolların kolayca görünülürlüğü sağlanmalıdır.
- Bahçe düzenlemesi yaparken bitki örtüsünün görünmeyen bölgeler oluşturması engellenmelidir.

- Otoparklarda, merdivenlerde ve alt geçitlerde maksimum görüş alanı olacak şekilde aydınlatma yapılmalıdır.
- Yayalar tarafından kullanılan yolların yönlendirmeleri ve gece aydınlatmaları düzgün yapılmalı ve yol kaybetme ihtimalini ortadan kaldıracak işaretleme, çit, farklı zemin rengi gibi tedbirler alınmalıdır.
- Binanın ana giriş kapısı yaya trafiğinin yoğun olduğu tarafa açılmalıdır.
- Balkon duvarları dışarıyı görmeye engel olmamalıdır.
- Ana girişler gizlenmeyi engelleyecek şekilde tasarlanmalıdır.
- Bina dış duvarları tırmanmaya fırsat vermeyecek pürüzsüzlükte tasarlanmalıdır.
- Ana kapıdan çıkarak, halka açık bölgeye ulaşan patika yol açık ve emniyetli olmalıdır.
- Binaların giriş-çıkışları, buralara ulaşan patikalar ve ikaz levhaları kolayca görünecek şekilde aydınlatılmalıdır.
- Her nokta en azından iki yönden aydınlatılarak gölgelenme engellenmelidir.



**Resim 1.2:** Bina Güvenliği Sistem Örnekleri


**Güvenlik ana unsuru insan ve diğer canlıların haklarını korumak olan önleyici tedbirler zinciridir. Güvenlik tedbirleri alınırkan diğer canlıların zarar görmemesine dikkat edilmelidir.**

# RİSK ANALİZİ

Genel anlamda risk belirli bir tehlikeli olayın meydana gelme olasılığı ile bu olayın sonuçlarının ortaya çıkardığı zarar, hasar veya yaralanmanın şiddetinin tahminidir. Kurumsal anlamda risk ise kurumun stratejik, mali ve operasyonel hedeflerini gerçekleştirmesini engelleyecek, her türlü olayın gerçekleşme olasılığıdır. Riskin tanımlanabilmesi için kurumsal hedeflerin belirlenmiş olması gerekir. Hedefler belirlendikten sonra bu hedeflere ulaşılmasını engelleyebilecek riskler tanımlanır, değerlendirilir ve alınacak tedbirler kararlaştırılır. Bu amaç için yapılan risk analizi son yıllarda sıkça rastlanan terör saldırıları ve hırsızlık olayları nedeniyle gerek kamu kurumlarında gerekse özel kuruluşlarda ilgi uyandıran konulardan biri olmuştur. Nedeni ve düzeyi belirsiz iç ve dış tehditlere karşı nasıl davranılacağını bilmek amacı için risk analizi çok önemlidir.

Risk analizi genel anlamda aşağıdaki safhalardan oluşur:

- Tanımlama: Risk analiz süreci, kurumun karşılaştığı risklerin tanımlanması ile başlar. Kurumsal alan üzerine etkisi olan tüm tehlikeler bunun içindedir. İşletme için sadece en bilinen felaketler değil, tüm akla gelen riskler tanımlanmalı ve kaydedilmelidir.
- Değerlendirme: Bir sonraki safha, tanımlaması yapılan risklerin önemini değerlendirmektir. Bu, iki boyutlu Etki-Olasılık hesaplamalarının etrafında çevrelenir.
- Yönetim: risklerin önem derecelerinin saptanması ile yüksek etkili ve olasılıklı risklerinin yönetilmesi için strateji geliştirmesini gerektirir.
- İnceleme: Tüm risk yönetimi süreçleri ve çıktıları yeniden gözden geçirilmeli ve devamlı olarak denetlenmelidir. Bu, risk yönetimi stratejisi ve kurumca uygulanan süreçlerin geçerlilik güncellemelerini kapsayan bir çalışmadır.

Risk analizi yaparken uygulanan yöntem ne olursa olsun aşağıdaki temel işlemler risk analizi çalışmaları arasında yer almaktadır.

- Analizin kapsamının; potansiyel riskler ve zarar görme olasılığına göre uygulanacak güvenlik tedbirlerin kapsamının belirlenmesi
- İç ve dış tehditlerin belirlenmesi için işletmenin bulunduğu bölgedeki suçlar ve alınan önlemlerle ilgili veri toplanması
- Potansiyel tehditlerin ve zararların tanımlanıp dokümente edilmesi
- Hali hazırdaki güvenlik değerlerinin belirlenmesi, yani işletmenin büyüklüğüne ve faaliyet alanının önemine göre güvenlik derecesinin belirlenmesi
- Tehditlerin oluşma olasılığının belirlenmesi
- Tehditlerin oluşması durumunda potansiyel etkilerinin belirlenmesi
- Risk seviyesinin belirlenmesi
- Analize ilişkin final dokümanının hazırlanması
- Periyodik olarak risk değerlendirme ve dokümanın güncellenme işleminin yapılması

Yapılan bu işlemlerden oluşan risk analizi özetle; bir işletmenin güvenlik tedbirlerini almadan önce hazırlanması ve devamlı olarak güncellenmesi gereken bir süreçtir. Risk analizi birbiriyle doğrudan ilgili iki konuyu kapsar. Bunlar; risk değerlendirme ve risk yönetimidir. Bu konuların biribirleri ile olan ilişkileri ve neden birbirlerini gerektirdikleri aşağıda anlatılacaktır. Burada ilgi gösterilmesi gereken konu kamu ya da özel kuruluşlarının karşılaşabilecekleri riskin niteliğini belirlemek ve bu riskleri yönetebilecek yöntemleri geliştirmektir.

**Risk analizi niçin gereklidir?**

## Risk Değerlendirme

Risk değerlendirmesi kuruluşlara iç ve dış tehditlerden kaynaklanabilecek zararları ve bunlara karşı alınacak önlemleri belirlemek amacıyla gerçekleştirilen çalışmalardır. Risk değerlendirme, özel bir suç olayının oluşması ve/veya potansiyel sonuçlarını kestirmek üzerine yapılan çalışmaları kapsar. Ülkemizde 4857 sayılı İş Kanunu'na göre her kuruluş sahibi, işyerinin ihtiyaçlarını ve koşullarını dikkate alarak tehlikeleri tanımlamak, risk değerlendirmesi ile riskleri belirlemek ve iş sağlığı ve güvenliği mevzuatına uygun olarak gerekli önlemleri almakla yükümlüdür.

İş Sağlığı ve Güvenliği Genel Müdürlüğü'nün risk değerlendirmesi konusunda hazırlamış olduğu yayında aşağıda verilen beş adımdan oluşan bir risk değerlendirme yöntemi önerilmiştir:

- Tehlikelerin belirlenmesi; işyerinde ürünlere ve iş ekipmanlarına nelerin zarar verebileceğinin belirlenmesi
- Tehlikelerin değerlendirilmesi; belirlenen tehlikelerden hangileri için ne tür önlemlerinin alınacağının ve hangileri için risk derecelendirmesinin yapılacağının tespiti
- Risklerin derecelendirmesi; riskli bulunan tehlikelerin ağırlık oranları hesaplanarak öncelik sırasının belirlenmesi
- Kontrol önlemlerinin uygulanması; önceki iki adımda belirlenen tehlikelerden kaldırılabilecek olanlar için hemen önlemler alınır ve tekrar ortaya çıkmamaları için uygun bir kontrol periyodu belirlenir. Belirli bir maliyet ve zaman gerektiren ve acil olmayan önlemler için uygulama planları yapılarak uygulanması sağlanır.
- Denetim, izleme ve gözden geçirme; risk yönetiminin tüm aşamaları ve uygulanması düzenli olarak denetlenir, izlenir ve aksayan yönler yeniden gözden geçirilir.

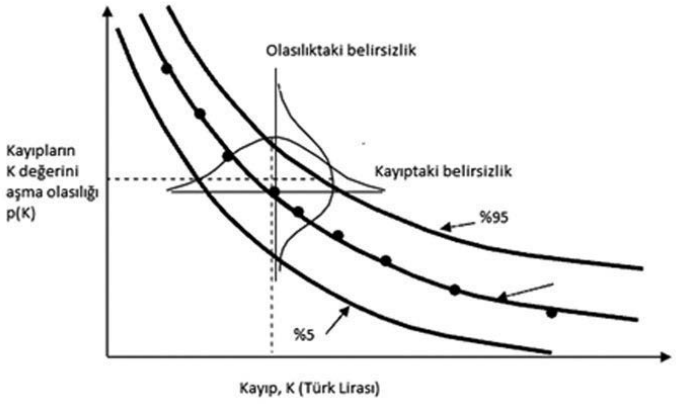
Yukarıdaki risk değerlendirme adımlarına göre, öncelikle kuruluşun karşılaşabileceği tehlikeli durumlar ve bu tehlikenin önemli olup olmadığının belirlenmesi gerekmektedir. Riski bu tehlikelere göre derecelendirirken nicel ya da nitel teknikler kullanılır.

Nicel tekniklerde risk sayısal olarak değerlendirilir. Sağlıkta, güvenlikte ve çevresel alanlarda risk genellikle yaralanma, salgın ya da ölüm gibi sonuçlarının gerçekleşme oranları ile gösterilir. Örneğin Türkiye'de şu ana kadar ölmüş 1 milyon insanlardan diyelimki 10.000 kişi kanserden ölmektedir. Burada risk $10^{-2}$ ile ifade edilir. $10^{-6}$ risk yani milyonda bir risk ihtimali genelde değerlendirmeye alınmaz. Nitel olarak risk değerlendirildiğinde riski, yüksek orta veya küçük gibi tanımlayıcı terimlerle tanımlarız. Bilim adamları ve mühendislerin belli bir riskin niteliği ve onu çevreleyen tahmini belirsizliklerin derecesi hakkında, bu değerlendirmelerden faydalanacaklara veri sağlaması gerekmektedir. Aynı zamanda bu kestirimlerin uzmanı olma konusunda hassas olmaları gerekir.

Güvenlik tedbiri alacak kurum iki uzmandan risk analizi yapmasını istediğinde, uzmanlardan birisi özel bir tehdit için "korkulacak birşey yok " derse, diğer bir uzman da "bu risk sizin radar ekranınızda olmalı" derse burada bir çelişki söz konusudur. Burada kurum nasıl bir önlem alacağını belirleyemez. Burada yapılması gereken birçok uzmanın bu konudaki görüşüne başvurup yazılan raporlarda uyum derecesinin belirlenmesidir.

Bir uzmanın belirli bir risk konusunda ne derece bir bilgi sahibi olduğunu anlamak için aşma olasılığı (EP) eğrisi oluşturulur. Bir EP eğrisi belirli kayıpların hangi olasılıkla aşıldığını gösteren eğridir. Kayıplar; uğranılan felaketin, zararın, hastalığın ya da benzeri sonuçların nakit olarak ölçülmesidir.

Özel bir örnek verecek olursak Türkiye'deki herhangi bir olası deprem için bir EP eğrisi oluşturmak istesek, risk değerlendirmesi yaparsak öncelikle maddi kaybı gerektirecek deprem sonuçları belirlenir ve belirlenen maddi zararların aşılma olasılıkları tahmin edilir. Aşağıda gösterilen EP eğrisi elde edilmiş olur. Bu eğri üzerinde olası zararların oluşması ve maddi kaybın miktarı konusunda belirsizlik ilişkisi de ele alınır. Bu belirsizlik %5 ve %95 arasında değişimle eğriye yansıtılır.




**Resim 1.3:** Aşma Olasılığı (EP) Eğrisi Örneği

Burada EP eğrisi oluşturulurken dikkat edilmesi gereken nokta olasılık ve gerçekleşen olaylara birlikte bakarak belirsizliğin derecesinin belirlenmesidir. Doğal bir afetin ya da kimyasal bir patlamanın sonuçları için EP eğrisinin elde edilmesi bir terör olayına gore daha kolaydır. Fakat her ne kadar belirli bir afetin sonuçları önceden kestirilebiliyor olsa da bu afetin sonucuna bağlı riskler ve zararların oluşmasında da belirsizlikler bulunabilir. Riski yönetme araçlarını kullanabilmek için EP eğrisi önemlidir. Uzmanlar oluşabilecek olaylar ve bunların sonuçlarını benzer olayların EP eğrileri yardımıyla tahmin edebilirler.

Geleneksel risk değerlendirme dış ve iç saldırılar ya da afetlerin kayıplarını maddi olarak ölçer. Risk algılama ise kayıplara psikolojik ve duygusal faktörler yani bu zararların insan davranışlarına olan büyük etkisi açısından bakar. Bu konuda yapılan ilk çalışmalarda insanların daha az bilgi sahibi olduğu ve zararlarından daha çok korktukları olayların en riskli olaylar olarak algılandığı sonucuna varılmıştır. Örneğin nükleer santral patlaması ve radyasyona uğrama riski en tehlikeli risktir. Bu örnekte olduğu gibi insanların duygusal ve psikolojik yaklaşımına göre riskin değerlendirmesi yapılmıştır. Son yıllarda yapılan risk değerlendirmesi çalışmaları da bu faktörlerin risk değerlendirmede etkin olduğunu göstermektedir. Toplum hala bazı aktivitelerden tehlikeli olduğu için kaçınmaktadır. Örneğin gidecekleri yere uçak yerine trenle gitmeleri, deprem olacak diye yüksek katlı evde oturmamaları, gelişen teknolojinin sunduğu elektronik cihazların kullanımı riske göre değerlendirilir. Baz istasyonlarının zarar vericeği endişesi, siyanürle altın aramanın kendilerini etkileyeceği endişe hep duygusal ve psiklojik olarak riskin değerlendirilmesi kapsamındadır.

## Risk Yönetimi

Risk yönetimi, hedeflerimizi tehdit eden riskleri ortaya çıkarmak ve onlarla baş edebilmek için atılan tüm mantıklı adımları kapsayan dinamik bir süreçtir. Kurumsal kaynaklar ve süreçler düzene sokulup riskin oluştuğu yerlerde çözümler aranır. Risk yönetimi üç önemli adımdan oluşur: (1) toplumun kabul edeceği düzeyden daha tehlikeli zararların belirlenmesi, (2) hangi kontrol etme seçeneklerinin olduğunun gözden geçirilmesi ve (3) kabul edilemeyen seviyedeki risklerin azaltılması için uygun hamlenin yapılmasına karar verilmesidir.

**SIRA SİZDE 4** **Geleneksel risk değerlendirme ile risk algılama arasındaki fark nedir?**

Gelecekte olası zararların kayıplarını azaltmak için risk yönetimi stratejileri geliştirirken risk değerlendirmeden gelen veri ile risk algılamanın ruhsal faktörlerini birleştirerek karar vermek gerekir. Fakat bu değerlendirmeler risk yöneticilerinin cevaplaması gerektiği birçok soruya cevap veremez. Örneğin hangi seviyeye kadar maruz kalınan risk kabul edilemez? Diğer bir tersine deyişle, hangi risk seviyesi güvenli kabul edilebilir? Riskin uzantısı olan olaylardaki belirsizlikler nasıl engellenir? Var olan risk azaltılırken başka riskler ortaya çıkar mı? Oluşabilecek zararlardan hangisi ile ilgilenmek diğerlerine

göre daha önemlidir? Bu tip soruların cevabı toplumsal değerlere ve önceliklere bağlıdır. Tabii ki bu risklerle uğraşmak siyasi yönetim anlayışına ve demokratik kurallara bağlıdır.

Risk yönetiminde öncelikle yapılması gereken bir işletmeyi etkileyebilecek riskler belirlendikten ve tanımlandıktan sonra bu risklere alınacak önlemlerden sorumlu kişi yani risk sahibinin belirlenmesi gereklidir.

Bundan sonraki adım ise risk raporunun hazırlanmasıdır. Bu rapor, yönetim seviyesinden çalışan seviyesine kadar sorumlu olunan alanlardaki risklerin yönetilmesinde, iç kontrol sistemlerinin etkinliğini ve önemli risklerin değerlendirilmelerini kapsamaktadır. Önemli bulunan kontrol kusurları veya zayıflıklar raporlarda tartışılmaktadır. Bunların kuruluş üzerinde ne etki gösterdiği, gösterebileceği ve nasıl arıtılacağı raporda yer almaktadır. Raporda ayrıca, mütevelli heyeti ile yönetim kademesinin risk ve kontrol konusunda açıklık ve şeffaflık esasına göre yapılması gereken iletişim yönteminin detayları bulunmaktadır.

Rapor hazırlandıktan sonraki aşama ise yıl boyunca bu rapora göre risklerin gözden geçirilip raporun güncellenmesi gerekmektedir. Bu güncellemede şu hususlara dikkat edilmelidir:

- Önemli riskler nelerdir ve bunlar nasıl tanımlanır, değerlendirilir, yönetilir?
- Raporlanmış iç kontrolde özellikle önemli kusurlar ve zayıflıklara karşı risklerin yönetilmesinde iç denetim mekanizmalarının etkinlikleri değerlendirilmelidir.
- Başarısızlık ve zayıflıkları azaltmak için gerekli adımların ivedilikle atılıp atılmadığı incelenmelidir.
- İç denetim sistemlerinin daha geniş izlenmesi için ihtiyaç olduğuna inanılan öneriler ve teknolojiler dikkate alınmalıdır.

# GÜVENLİK SİSTEMLERİNİN SEÇİMİ

Risk analizi yapılarak kuruluşun güvenlik ihtiyacı belirlenmiş olur. Hazırlanan risk raporuna göre kuruluşun hedeflerine uygun etkin bir güvenlik sisteminin bileşenlerinin seçimi önem kazanmaktadır. Etkin bir güvenlik sisteminin dört temel fonksiyonel elemanı vardır. Bunlar tespit, değerlendirme, geciktirme ve karşılık vermedir. Bu elemanlar, verilen sıraya göre görevlerini yerine getirirler.

Tespit etme sınırı aşarak işletmeye giren özel bir hareketli hedefin farkedilmesidir. Bunun için kullanılması gereken güvenlik sistemleri şunlardır:

- Belirlenen hedeflere uygun iç algılayıcılar
- Belirlenen hedeflere ugun dış algılayıcılar
- Alanlara özgü alarm kaynakları
- Sürekli bağlantılı halka veya alan çevreleyici sistemler


**Etkin bir güvenlikte olması gereken fonksiyonel elemanlar nelerdir?**

Hareketli bir sızma tespit edildiğinde değerlendirme aşamasındaki güvenlik sistemleri devreye girer. Tespit edilen hedefin görsel değerlendirmesi yapılır. Bu aşamada yapılan işler şunlardır:

- Tespit edilen şeyin tehdit olup olmadığının belirlenmesi
- Hedef hakkında ek bilgilerin elde edilmesi; hareketin yönü, hareketin hızı, hedef sayısı ve hedeflerin yanlarında bulundurdukları araçlar veya silahlar bu ek bilgiler arasındadır.
- Tespit edilen hedefe bağlı olarak güvenlik sistemlerinin yönlendirilmesi
- Güvenlik kuvvetlerine bilgi sağlanması

Değerlendirme verimli olması demek hızlı olması demektir. Bu yüzden de seçilecek güvenlik sistemlerinden hızlı bilgi alınmalı ve değerlendirme yapılmalıdır. Seçilecek güvenlik sistemleri manyetik güvenlik duvarı ve lazer algılayıcılar gibi doğrudan hedefe karşı işletmeyi korumalı veya CCTV gibi uzaktan takibini kolaylaştırıcı olmalıdır.

Eğer uzaktan takip ve müdahele gerektiren bir durum söz konusu ise bundan sonra güvenlik sisteminin yapması gereken fonksiyon geciktirme işidir. Geciktirme; güvenlik güçleri müdahele edene kadar davetsiz misafirleri yavaşlatıcı önlemler almak demektir. Bunun için bir takım bariyer sistemleri mevcuttur. Bu bariyerlerin bir kısmı insan yapımı (manyetik bariyerler gibi) veya doğal engebelerdir. Bir kısmı aktiftir ve bir kısmı da göstermelik olarak konulmuş olabilir. Bariyerlerin seçim kriteri, tehdit olarak görülen unsurların karakteristik özelliklerine bağlıdır.

Belirlenen hedefe uygulanacak son aşama ise sızan kişi ya da kişileri durdurmaktır. Bunun için karşılık verme fonksiyonu devreye girer. Karşılık verme; işletmenin değerlerini hedefin saldırısından korumaya yönelik yapılan savunma hareketleridir. Burada karşılık verme için gereken kuvvetler, silahlar, haberleşme araçları ve taktikler devreye girer. Devreye girme hızı güvenlik sistemlerin çalışma hızına ve geciktirme hızına bağlıdır. Hedef hızla hareket ediyorsa, alınacak karşı önlemler değişiklik gösterebilir.

Güvenlik sistemlerinin seçerken dikkat edilmesi gereken konu önlenmesi gereken tehlikeli durumu oluşturacak kişi kim olursa olsun, bu kişinin özel hayatını açığa çıkaracak bir elektronik sistemin seçilmesi doğru değildir. Örneğin günümüzde istihbarat elemanlarınca devletin güvenliğini sağlamak amaçlı kullanılan ses dinleme cihazlarının herhangi bir kuruluşta kullanılması özel hayata tecavüz anlamına geldiğinden doğru değildir.

Özetle güvenlik sistemlerinin seçim amacı; güvenlik çemberinin dışından başlayarak, korunan mekândaki hedef değeri yüksek varlıkları ele geçirmek, sabote etmek veya önemli kişilere zarar vermek maksatlı sızma girişimlerini;

- mümkün olduğu kadar çok geciktirmeyi,
- mümkün olan en kısa sürede tespit etmeyi,
- mümkün olan en kısa sürede önleme tepkisini vermeyi

sağlayacak çevresel düzenlemeleri yapmak ve uygun güvenlik sistem donanımlarının kurmaktır.


**Kişinin özel hayatını açığa çıkaracak bir elektronik cihazın güvenlik sistem bileşeni seçilmesi doğru değildir. Örneğin ses dinleme cihazlarının kullanılması özel hayata tecavüz anlamına geldiğinden doğru değildir.**

## Özet

Güvenlik ana unsuru insan ve diğer canlıların haklarını korumak olan önleyici tedbirler zinciridir. Özel güvenlik görevlilerinin öncelikli hedefi suçların önlenmesidir. Güvenlik sistemleri deyince de ses, ısı, ışık, titreşim ya da hareket bilgilerini algılayan elektromekanik cihazlar aklımıza gelmelidir. Özel güvenlik hizmetinden yararlanan kişi ve kuruluşlar karşılaşabilecekleri suç unsurlarının en aza indirilmesini beklerler. Bunun içinde öncelikle faaliyet gösterdikleri binaları ve çevreyi düzenlemeleri gerekir. Bunun için kullanılacak güvenlik cihazlarından uygun olanın belirlenmesinde olası iç ve dış tehditlerle güvenlik açıklarının belirlenmesi ve bunlara karşı risk analizinin yapılması önemli rol oynamaktadır

İç tehditler arasında kurum çalışanlarından kaynaklanan tehditler söz konusudur. Çalışanların sayısı, eğitim ve kültür seviyeleri ve birbirlerine gösterdikleri anlayış güvenlik önlemi alınması konusunda önemli faktörlerdir.

Dış tehditler korunması hedeflenen mekân içerisindeki insanların can güvenliğine zarar verecek; şirketin varlıklarının zarar görmesine ve ticari faaliyetlerin kesintiye uğramasına neden olabilecek hırsızlık, terör olayları, organize suçlar, sabotaj gibi olası tehditlerdir.

Genel anlamda risk belirli bir tehlikeli olayın meydana gelme olasılığı ile bu olayın sonuçlarının ortaya çıkardığı zarar, hasar veya yaralanmanın şiddetinin tahminidir. Kurumsal anlamda risk ise kurumun stratejik, mali ve operasyonel hedeflerini gerçekleştirmesini engelleyecek, her türlü olayın gerçekleşme olasılığıdır. Kuruluşların hedeflerini engelleyebilecek risklerin tanımlanabilmesi, değerlendirilmesi, yönetilmesi ve alınacak tedbirlerle incelenmesi için yapılan çalışmalara risk analizi denir. Risk analizi birbiriyle doğrudan ilgili iki konuyu kapsar. Bunlar; risk değerlendirme ve risk yönetimidir.

Risk değerlendirmesi kuruluşlara iç ve dış tehditlerden kaynaklanabilecek zararları ve bunlara karşı alınacak önlemleri belirlemek amacıyla gerçekleştirilen çalışmalardır. Risk değerlendirme, özel bir suç olayının oluşması ve/veya potansiyel sonuçlarını kestirmek üzerine yapılan çalışmaları kapsar.

Risk yönetimi, hedefleri tehdit eden riskleri ortaya çıkarmak ve onlarla baş edebilmek için atılan tüm mantıklı adımları kapsayan dinamik bir süreçtir. Kurumsal kaynaklar ve süreçler düzene sokulup riskin oluştuğu yerlerde çözümler aranır. Risk yönetimi üç önemli adımdan oluşur: (1) toplumun kabul edeceği düzeyden daha tehlikeli zararların belirlenmesi, (2) hangi kontrol etme seçeneklerinin olduğunun gözden geçirilmesi ve (3) kabul edilemeyen seviyedeki risklerin azaltılması için uygun hamlenin yapılmasına karar verilmesidir.

Risk yönetiminde öncelikle yapılması gereken bir işletmeyi etkileyebilecek riskler belirlendikten ve tanımlandıktan sonra bu risklere alınacak önlemlerden sorumlu kişi yani risk sahibinin belirlenmesi gereklidir. Bundan sonraki adım ise risk raporunun hazırlanmasıdır. Bu rapor, yönetim seviyesinden çalışan seviyesine kadar sorumlu olunan alanlardaki iç kontrol sistemlerinin etkinliğini ve önemli risklerin değerlendirilmelerini kapsamaktadır. Bu raporun güncellenmesi alınan tedbirlere karşın kuruluşların uğradığı zararlar ve olası yeni risklere gözönünde bulundurularak yapılır.

Risk analizi yapıldıktan sonraki aşama ise hazırlanan durum raporuna göre etkin güvenlik sistemlerinin seçimidir. Etkin bir güvenlik sisteminin dört temel fonksiyonel elemanı vardır. Bunlar tespit, değerlendirme, geciktirme ve karşılık vermedir. Bu elemanlar verilen sıraya göre görevlerini yerine getirirler. Tespit etme sınırı aşarak işletmeye giren özel bir hareketli hedefin farkedilmesidir. Değerlendirmenin verimli olması demek, hızlı olması demektir. Bu yüzden de seçilecek güvenlik sistemlerinden hızlı bilgi alınmalı ve değerlendirme yapılmalıdır. Geciktirme; güvenlik güçleri müdahele edene kadar davetsiz misafirleri yavaşlatıcı önlemler almak demektir. Karşılık verme ise işletmenin değerlerini hedefin saldırısından korumaya yönelik yapılan savunma hareketleridir.

Güvenlik sistemlerinin seçim amacı; korunan mekândaki hedef değeri yüksek varlıkları ele geçirmek, sabote etmek veya önemli kişilere zarar vermek maksatlı sızma girişimlerini; mümkün olduğu kadar çok geciktirmeyi, mümkün olan en kısa sürede tespit etmeyi ve mümkün olan en kısa sürede önleme tepkisini vermeyi sağlayacak çevresel düzenlemeleri yapmak ve uygun güvenlik sistem donanımlarının kurmaktır.

## Kendimizi Sınayalım

**1.** Ülkemizde güvenlik sistemlerinin kullanımının yasal dayanağı hangi sayılı kanunla belirlenmiştir?

a. 4267

b. 5188

c. 4882

d. 4857

e. 4688

**2.** Kurum çalışanlarından kaynaklanan tehditler aşağdıkaki faktörlerden hangisine bağlı değildir?

a. Çalışan sayısı

b. Çalışanların kültür seviyesi

c. İşçi-işveren ilişkisi

d. Çalışanların bölgesel homojenliği

e. Hepsi

**3.** Aşağıdakilerden hangisi dış tehditler arasında değildir?

a. Terör saldırıları

b. Hırsızlık

c. Sabotaj

d. Toplumsal olaylar

e. Grev

**4.** Aşağıdakilerden hangisi kuruluşların güvenlik tedbirleri almasını etkileyen çevresel faktörlerden değildir?

a. Çevredeki kolluk kuvvetlerinin konumu

b. Çevredeki işletmelerin güvenlik ihtiyacı

c. Çevrede işlenen suçların cinsi ve miktarı

d. Kuruluşun ürettiği ürünün cinsi

e. Kuruluşa ulaşım yolları

**5.** Aşağıdakilerden hangisi risk analizi safhalarından birisi değildir?

a. Tanımlama

b.Değerlendirme

c. Ölçme

d. Yönetim

e. İnceleme

**6.** Aşağıdakilerden hangisi risk değerlendirme aşamalarından birisi değildir?

a. Tehlikeleri tanımlama

b. Tehlikeleri algılama

c. Riskleri derecelendirme

d. Kontrol yöntemlerini uygulama

e. Gözden geçirme

**7.** Riskin psikolojik ve duygusal faktörlere gore belirlenmesine ne denir?

a. Risk yönetimi

b. Risk analizi

c. Risk değerlendirme

d. Risk algılama

e. Risk denetimi

**8.** Kuruluş hedeflerini tehdit eden riskleri ortaya çıkarmak ve onlarla baş edebilmek için atılan tüm mantıklı adımları kapsayan dinamik süreç aşağıdakilerden hangisidir?

a. Risk yönetimi

b. Risk analizi

c. Risk değerlendirme

d. Risk algılama

e. Risk denetimi

**9.** Aşağıdakilerden hangisi etkin bir güvenlik sisteminin temel fonksiyonlarından birisi değildir?

a. Tespit

b. Değerlendirme

c. Geciktirme

d. Karşılık verme

e. Öğrenme

**10.** Bir işletmenin uzmanlar tarafından belirlenen risklerden ne kadar aşımla etkilendiğini gösteren eğri hangisidir?

a. AP

b. CP

c. EP

d. OP

e. RP

## Kendimizi Sınayalım Yanıt Anahtarı

**1. b** Yanıtınız yanlış ise "Güvenlik Sistemlerinin Kullanım Nedenleri." başlıklı konuyu yeniden gözden geçiriniz.

**2. e** Yanıtınız yanlış ise "İç Tehditler" başlıklı konuyu yeniden gözden geçiriniz.

**3. e** Yanıtınız yanlış ise "Dış Tehditler" başlıklı konuyu yeniden gözden geçiriniz.

**4. d** Yanıtınız yanlış ise "Güvenlik Açıkları ve Alınacak Tedbirler" başlıklı konuyu yeniden gözden geçiriniz.

**5. c** Yanıtınız yanlış ise "Risk Analizi" başlıklı konuyu yeniden gözden geçiriniz.

**6. b** Yanıtınız yanlış ise "Risk Değerlendirme" başlıklı konuyu yeniden gözden geçiriniz.

**7. d** Yanıtınız yanlış ise "Risk Değerlendirme" başlıklı konuyu yeniden gözden geçiriniz.

**8. a** Yanıtınız yanlış ise "Risk Yönetimi" başlıklı konuyu yeniden gözden geçiriniz.

**9. e** Yanıtınız yanlış ise "Güvenlik Sistemlerinin Seçimi" başlıklı konuyu yeniden gözden geçiriniz.

**10.c** Yanıtınız yanlış ise "Risk Değerlendirme" başlıklı konuyu yeniden gözden geçiriniz.

## Sıra Sizde Yanıt Anahtarı

### *Sıra Sizde 1*

Güvenlik görevlilerine en sık alışveriş merkezlerinde, bankalarda, belediyelerde ve kamu kurum ve kuruluşlarının girişlerinde karşılaşıyoruz. En yaygın kullanılan güvenlik cihazları ise kapı detektörleri, X-ışını cihazları ve turnikelerdir. Örnekler çoğaltılabilir.

### *Sıra Sizde 2*

Hırsızlık, terör olayları, organize suçlar, sabotaj gibi tehlikeli faaliyetler sıkca karşılaşılan dış tehditlerdir.

### *Sıra Sizde 3*

Nedeni ve düzeyi belirsiz iç ve dış tehditlere karşı nasıl davranılacağını bilmek amacı için risk analizi çok önemlidir. Risk analizi yapılarak olası riskler ve bu riskleri önleyici ya da etkisini azaltıcı güvenlik sistemlerinin bileşenleri belirlenir.

### *Sıra Sizde 4*

Geleneksel risk değerlendirme dış ve iç saldırılar ya da afetlerin kayıplarını maddi olarak ölçer. Risk algılama ise kayıplara psikolojik ve duygusal faktörler yani bu zararların insan davranışlarına olan büyük etkisi açısından bakar.

### *Sıra Sizde 5*

Etkin bir güvenlik sisteminin dört temel fonksiyonel elemanı vardır. Bunlar tespit, değerlendirme, geciktirme ve karşılık vermedir.

## Yararlanılan Kaynaklar

Pearson, R.L. (2007). **Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions**, Butterworth-Heinemann, Elsevier.

Grossi P. ve Kunreuther H. (2005). **Catastrophe Modeling: A New Approach to Managing Risk.** Boston: Springer.

İş Sağlığı ve Güvenliği Genel Müdürlüğü. (2007). **5 Adımda Risk Değerlendirmesi,** Ankara: Çalışma ve Sosyal Güvenlik Bakanlığı Genel yayın No: 140.

Yücel, T. (1983). **Yapısalcılık ve Tarihsel Süreç İçinde İnsan,** İstanbul: Can Yayınları.

Pickett K.H.S. (2010). **The Internal Auditing Handbook**, Londra: Wileyt.

## Yararlanılan İnternet Kaynakları

www.ozelguvenlikdunyasi.com

# 2

## Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Elektronik alarm sistemlerini anlatabilecek,
- Elektronik alarm sistemlerinin çeşitlerini açıklayabilecek,
- Hırsız alarm sistemlerini ve bileşenlerini tanımlayabilecek,
- Yangın alarm sistemlerini ve bileşenlerini tanımlayabilecek

bilgi ve becerilere sahip olabilirsiniz.

## Anahtar Kavramlar

- Elektronik
- Alarm
- Hırsız Alarm Sistemi
- Manyetik Kontak
- Hareket Algılayıcı
- Yangın Alarm Sistemi
- Duman Detektörü
- Gaz Detektörü
- Alev Detektörü
- Siren ve Flaşör

## İçindekiler

# Elektronik Alarm Sistemleri

## GİRİŞ

Kitabın bu ünitesinde, güvenliğin sağlanması ve arttırılması amacı için bir araya gelerek sistemi oluşturan farklı cihazlardan bahsedilecektir. Elektronik alarm sistem bileşenleri, temel amaçları güvenliği sağlamak olan güvenlik elemanlarına ya da kolluk kuvvetlerine yardım amacı ile kullanılan cihazlardır. Elektronik alarm sistemleri içerisinde yer alan cihazlar, bu bölümde ayrı ayrı incelenecektir.

Bu bölümde elektronik alarm sistemleri iki başlık altında incelenecektir:

- Hırsız Alarm Sistemleri: Elektronik parçaların bir araya gelmesi ile hırsızlık, gasp ve sabotaj olaylarına karşı korunmayı ve yetkisiz giriş anında gerek siren ya da flaşör ile gerekse telefon sesli ya da kısa mesajı ile belirlenen numaralara bilgi vermeyi amaçlayan sistemlerdir.
- Yangın Alarm Sistemleri: Herhangi bir teknik sorun, sabotaj ya da dikkatsizlik sonucu çıkabilecek yangına başlangıç aşamasında müdahale etmeyi, bazı durumlarda ise yangına sebep olabilecek kusurları tespit etmeyi ve önlem almayı kolaylaştıran, duman ya da gaz zehirlenmelerine karşı güvenliği sağlayan sistemlerdir.

**Resim 2.1:** Bütünleşik Alarm Panelleri

Ev ve iş yerlerinin hırsızlık, gasp ya da sabotaj olaylarına karşı korunması için güvenlik görevlilerinden her zaman faydalanmak mümkün olmayabilir. Gerek ev ya da iş yerinin konumunun uygunsuzluğu ve gerekse maliyet faktörü, güvenliğin önemli olduğu durumlarda kullanılacak elektronik alarm sistemlerinin tasarlanması ihtiyacını doğurmuştur. Zaman içerisinde güvenliği sağlamak için cihazlar, tek tek değil de, birlikte kullanılmaya başlanmış ve güvenlik sistemleri doğmuştur. Güvenlik sistemleri kurulumu bir kez yapılan ve sonrasında çok az bir bakım ile senelerce görevlerini yerine getiren cihazlardan oluşmaktadır.

Farklı cihazların birleşimi ile oluşturulan sistem, hırsız alarm sistemleri olarak da adlandırılmaktadır. Sistemin asıl amacı, içerisine kurulduğu mekâna zorla girmek isteyen herhangi bir şahsı algılamak ve siren ya da flaşör ile belirlenen mekâna yetkisiz bir giriş olduğunu görevlilere bildirmektir. Yakın çevrede güvenlik görevlilerinin olmaması durumunda sistem bağlantıları gerekli birimlere telefon yolu ile de bilgi vermeyi sağlar.

Güvenlik sistemleri, temelde güvenlik görevlilerine ve kolluk kuvvetlerine yardımı amaç-lamaktadır. Yetkisiz bir giriş olduğunu siren, flaşör ya da telefon ses mesajı ya da kısa mesaj ile öğrenen güvenlik görevlileri ya da kolluk kuvvetleri derhal belirlenen mekâna giderek gerekli işlemleri yaparlar. Bu sayede hırsızlık, gasp ya da sabotaj olaylarına karşı önlem arttırılmış olur. Bazı durumlarda sadece hırsız alarm sisteminin mekânda kurulu olması bile, caydırıcı etkisi ile hırsızlık, gasp veya sabotaj olaylarını önlemede yardımcı olmaktadır.

Ev ve iş yerlerimize hırsızlık, gasp ya da sabotaj olaylarından belki de daha fazla zarar veren bir olay da yangın çıkmasıdır. Elektronik alarm sistemlerinin bir başka özelliği ise yangın durumunda gerekli birimleri uyarmak ve yangın söndürme sistemlerini ivedi olarak devreye almaktır.

Sistem parçalarının bir bölümü yangını daha oluşmadan önlemek amacı ile kullanılır. İçeride yaşayanları kurtarmaya yönelik bu cihazlar gaz detektörleri olarak adlandırılır. Temel amaçları, ortama yayılan doğalgaz ya da tüp gazı algılayarak, yangın oluşmadan ortamda yaşayanları genellikle ses ve flaşör ile uyarmaktır. Böylelikle, yangın çıkmasa dahi, gaz zehirlenmelerine karşı da önlem alınmış olur. Yangın alarm sistemleri de kitabın bu bölümünde incelenecek parçalar ile daha iyi anlaşılacaktır.

Hırsız alarm sistemleri ile yangın alarm sistemlerinin bileşenleri birbirinden farklıdır. Gerekli olduğu durumlarda kullanılacak olan bu bileşenleri temelde üç kategoride toplamak mümkündür.

- **Giriş Cihazları**: Görevleri, çevreden topladıkları bilgileri merkeze iletmektir. Her sistem için kullanılan giriş cihazları birbirinden farklı olabilir. Sistemde hangi giriş cihazlarının kullanılacağı, sistemi projelendiren ekip tarafından, mekânın özelliklerine ya da kanuni zorunluluklara bağlı olarak belirlenir.
- **Değerlendirme Cihazları**: Tüm giriş cihazlarından gelen verileri değerlendirerek gerekli durumlarda alarm işleminin başlatılmasını sağlayan ana merkezlerdir. Bir ana merkez olmaksızın alarm sisteminin kurulması mümkün değildir. Sistemin beyni olarak değerlendirilebilir.
- **Çıkış Cihazları**: Değerlendirme cihazları tarafından gelen alarm sinyalini dışarıya vermekle görevlidirler. Acil durumda çalışırlar. Sirenler, flaşörler, telefon arayıcıları, internet modülünün bir bölümü bu cihazlar kapsamındadır. Merkezden sinyal almadıkça görev yapmazlar.

# HIRSIZ ALARM SİSTEMLERİ

Hırsızlık, gasp ve sabotaj uyarı ve önleme sistemleri, elektronik alarm sistemleri içerisinde güvenliğimize yönelik en önemli cihazlardan oluşur. Basit anlamda bir alarm sistemi, ev ya da iş yerlerinin içeriden, dışarıdan ya da her iki yönden de korunmasına yöneliktir. Ev ya da işyerine hırsızlık, sabotaj ya da gasp amacı ile girmek isteyen yetkisiz şahıslara mani olmak amacı ile tasarlanmıştır. İyi bir alarm sistemi yetkisiz şahsın içeri girmesine mani olmalı ve aynı zamanda da ışık ya da ses ile çevreyi uyarmalıdır.

Sistemin son yıllarda eklenen en önemli özelliği, herhangi bir zorlama ya da yetkisiz giriş durumunda ev ya da iş yeri sahibini, alarm merkezini ya da kolluk kuvvetlerini telefon yardımı ile gerek sesli mesaj gerekse kısa mesaj ile uyarmasıdır. İnternet kullanımının yaygınlaşması ile hırsız alarm sistemleri, gerekli donanımlara sahipse, internet üzerinden de raporlama yaparak, uzak kullanıcılara bilgi vermektedir. Bu sayede sistemin kurulduğu mekânın durumunu bölge bölge ve tüm algılayıcılardan gelen mesajları anında görme imkânı mevcuttur.

Hırsız alarm sistemini oluşturan bileşenleri,

- Alarm Kontrol Paneli,
- Manyetik Kontaklar,
- Hareket Algılayıcılar,
- Cam kırılma detektörleri,
- Ağırlık detektörleri,
- Siren ve Flaşörler,
- Telefon Arayıcılar,
- Işınlı Bariyer Detektörleri,
- Panik Butonları,
- Uzaktan Kumandalar,
- İnternet Modülü
- Kablolar,
- Kablosuz Cihazlar,
- Aküler,

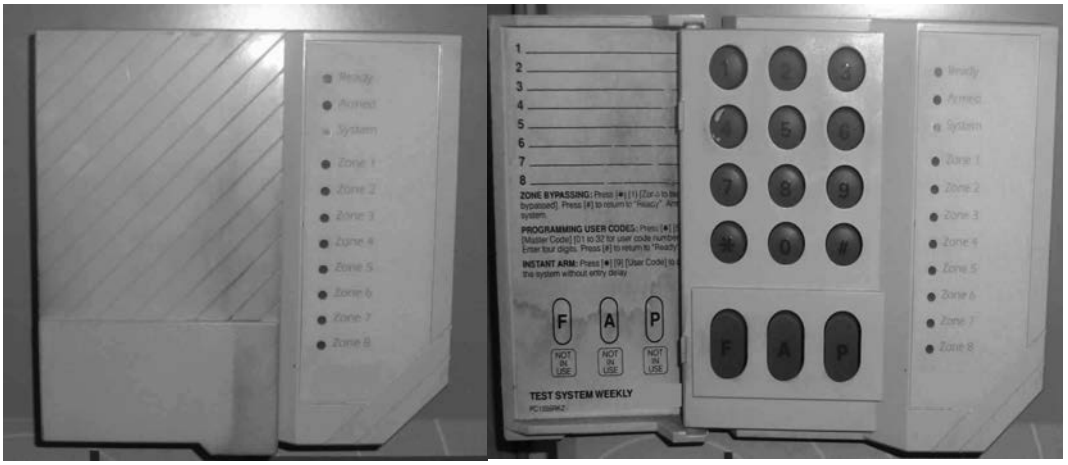
olarak sıralayabiliriz. Bir sistemin kurulması için yukarıda belirtilen parçaların tamamını kullanmak gerekmeyebilir. Sistemin kurulması istenen mekânın özelliklerine bağlı olarak daha az parça ile oluşturulan sistemler de yeterli gelmektedir. Şimdi sırası ile sistemi oluşturan bu parçaları inceleyelim.

## Alarm Kontrol Paneli

Ünitenin ilerleyen sayfalarında konu olacağı gibi, alarm kontrol panelleri, sadece hırsızlığa karşı önlem olmakla kalmayıp, aynı zamanda yangın, acil sağlık sorunları gibi durumlarda da bizlere yardımcı olmaktadır. Herhangi bir alarm sisteminin beyni olarak çalışan parça olmaksızın sistemin kurulumu da gerçekleştirilemez.

Alarm kontrol panellerini temelde iki farklı kategoride ele almak mümkündür. Bu kategoriler aynı zamanda kurulumun yapıldığı firma ile de belirlenmektedir. Ev ya da iş yerimize hırsız alarm sistemi monte ettirmek istediğinizde, karar vermeniz gereken en önemli nokta, kurulacak sistemin tek başına çalışan bir sistem mi, yoksa bir merkeze bağlı çalışan bir sistem mi olması gerektiğidir.


**Çevrenizdeki ev ya da iş yerlerini inceleyerek, hangilerinde alarm sistemi olduğunu belirlemeye çalışın. Mekanda alarm sistemi bağlı bulunduğunu belli eden bir dış cihaz ya da uyarı levhası olup olmadığını kontrol ediniz.**




**Resim 2.2:** Alarm Kontrol Panelleri

Eğer tek başına çalışan bir sistem bizim ihtiyacımızı karşılayacaksa, sistem herhangi yetkisiz bir girişi rapor etmek için bir merkezi aramayacak, sadece bizim istediğimiz kişi ya da kurumlara bilgi verecektir. Diğer açıdan, sistem bir firma güvencesi ile kurulacak olursa, alarm durumunda bağlı bulunduğu merkeze bilgi verecek ve firma görevlileri gerekli işlemleri yapacaktır. Merkeze bağlı alarm sistemleri, ev ya da iş yerini, alarm sistemi devrede bulunduğu zamanlarda bilgisayar yardımı ile sürekli izleme imkânı ve aksilik durumunda hızlı hareket etme önceliğini sunmaktadırlar.

Seçilen duruma göre alarm kontrol panelleri de değişecektir. Eğer tek başına çalışan bir sistem düşünülüyorsa, alarm kontrol panelinin daha basit bir yapıda olması yeterlidir. Merkeze bağlı sistemlerde ise daha teknolojik ve içerisinde internet modülü bulunan cihazlar kullanılmaktadır.

Alarm kontrol panelleri, ev ya da işyerinin tüm bölümlerinden gelen sinyalleri toplayan ve değerlendiren cihazlardır. Bir hırsız alarm sistemi kurulmadan önce ev ya da işyeri incelenerek farklı bölümlere ayrılır. Bu bölümlere "alan (zone)" adı da verilir. Tüm bu bölümlere gerekli görülen hareket algılayıcıları, manyetik cam ve kapı kontakları, cam kırılma detektörleri, ağırlık algılayıcıları, ışın bariyerleri yerleştirilir. Bu algılayıcıların her birinden gelen kablolar alarm kontrol panelinde toplanır. Eğer kablosuz haberleşme kullanılacaksa, alarm kontrol paneli kablosuz bir alıcı içerir. Panel, aktif olduğu durumda, kendisine bağlı tüm algılayıcılardan gelen sinyalleri değerlendirir. Herhangi bir algılayıcıdan normal dışında bir sinyal gelmesi, o bölgeye yetkisiz bir giriş olduğunu gösterir. Bu durumda panel kendisine bağlı bulunan sireni ve flaşörü çalıştırır. Eğer merkeze bağlı bir sistem kullanılıyorsa merkeze, tek başına çalışan bir sistem kullanılıyorsa daha önceden tanımlanan numaralara ses mesajı ya da kısa mesaj ile bilgi verir.

Alarm kontrol paneli üzerinde genellikle şifre girmeyi sağlayan bir numara takımı ve kendisine bağlı bulunan cihazları ve bölgelerin durumunu gösteren dijital bir ekran mevcuttur. Bazı durumlarda dijital ekran yerine bölgelerin durumu, yanıp sönen ledler ile de gösterilmektedir. Cihaz üzerindeki numara takımı ile yanlışlıkla yetkili bir giriş, yetkisiz gibi görünürse alarm çalma işleminin ertelenmesi ya da durdurulması için daha önceden belirlenen şifrenin girilmesi sağlanır. Tuş takımı dokunmatik olan ya da LCD gösterge ile bilgilendirme yapan çeşitli modelleri mevcuttur. Karar verme merkezi olan ve alarm sistemine dâhil tüm cihazların direk bağlandığı panel, telefon arama modülünü de içermektedir.

Alarm kontrol paneli aynı zamanda, acil durumlarda gerekli kapıların, kepenk ya da panjurların kapanması ya da açılması için de programlanabilir özelliktedir.


**Resim 2.3 :** Alarm Kontrol Paneli

## Manyetik Kontaklar

Manyetik kontaklar, genellikler kapı ve pencere gibi açılabilen elemanlara yerleştirilir. Manyetik kontakların iki farklı çeşidi mevcuttur.

İlk çeşit manyetik kontaklar bir batarya ve hoparlör sistemi ile kendi üzerinde siren barındırır. Hiçbir bağlantı gerekmeksizin sadece üzerinde bulunduğu kapı ya da pencere yetkisiz açıldığında üzerinde bulunan sireni aktif hale getirerek ses ile uyarıda bulunur. Bu çeşit manyetik kontaklarda dikkat edilmesi gereken en önemli nokta, manyetik kontak üzerinde yerleşik bulunan bataryanın azalması ve bitmesidir. Bu durumda manyetik kontak devre dışı kalır ve öngörülen faaliyetini gerçekleştiremez.

İkinci grup manyetik kontaklar ise hırsızlık alarm sistemleri içerisinde kullanılan manyetik kontaklardır. Bu grup bir kablo yardımı ile ya da kablosuz olarak alarm kontrol paneli ile sürekli bağlantı halindedir. Üzerinde yerleşik bulunduğu kapı ya da pencere açıldığında, herhangi bir ses ya da ışık uyarısı yapmaz. Bu kontak türü, açılma ya da kapanma uyarısını alarm kontrol merkezine gönderir. Yapılan hareketin acil ya da yetkisiz bir giriş ya da çıkış olduğuna karar verecek merci burada alarm kontrol panelidir. Alarm kontrol paneli gerekli sinyali alır ve kendisine daha önceden programlanmış şekilde işleme geçer. Kablo ile bağlantı sağlanan manyetik kontak beslemesi alarm kontrol paneli tarafından sağlandığı için batarya azalması ya da bitmesi sorunu yoktur. Kablosuz olarak sinyalleşme sağlanan durumlarda ise manyetik kontak üzerinde haberleşme için gerekli enerjiyi sağlayan bir batarya mevcuttur. İlk çeşit manyetik kontaklarda olduğu gibi, bataryanın azalması ya da bitmesi, kontağın çalışmaması anlamına gelir.

**Resim 2.4:** Kapı ve Pencere Kontakları ve Kullanımı

Manyetik kontaklar üzerinde yerleşik bulundukları kapı veya pencerenin açıldığı ya da kapandığına manyetik olarak karar verirler. Gerekli manyetik ortamı oluşturmak için kapı ya da pencerenin hem

açılan, hem de sabit bölgesine birbirinin tam karşısına gelecek şekilde yerleştirilen iki parçadan oluşur. Yerleştirme şeklinde dikkat edilecek nokta, kapı ya da pencere kanadı kapalı durumda iken her iki parçanın da üst üste bulunması gerekliliğidir.

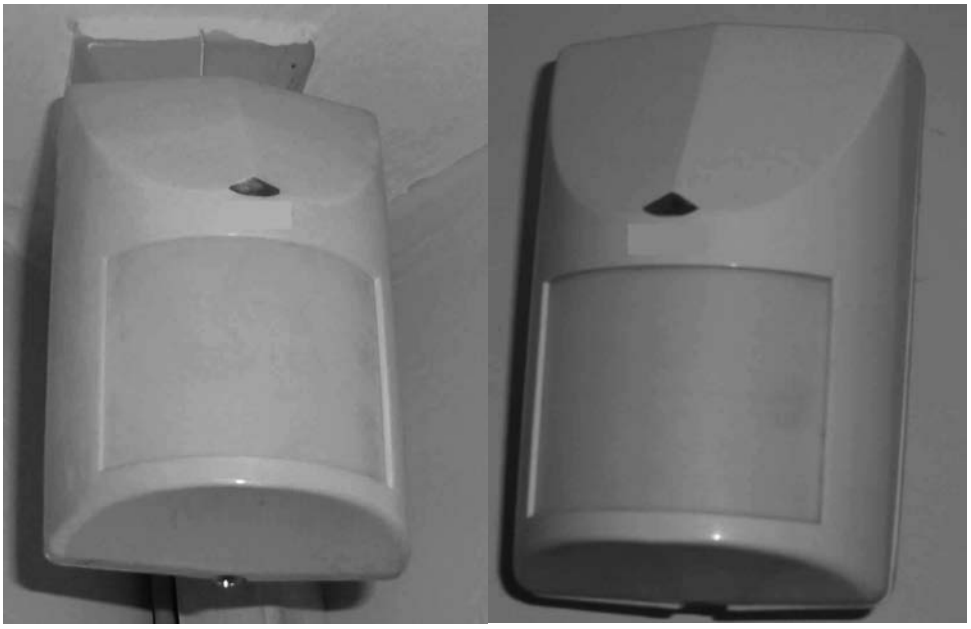
Doğru yerleşim ve eğer gerekli ise bataryaların tam bakımlı ve dolu olması, manyetik kontakların görevlerini eksiksiz yerine getirmesini sağlamakta, kapı ve pencerelerden yetkisiz girişlerde zamanında uyarı vermektedir.

Güvenliği sağlanacak alana ve üzerinde kullanılacak ekipmana göre, gömme tip manyetik kontaklar, minik tip manyetik kontaklar ya da kepenk tipi manyetik kontaklardan uygun olan seçilebilir.

## Hareket Algılayıcılar

Hareket algılayıcıların çalışma prensiplerini basitçe açıklamamız gerekirse, hareket gördüğü zaman kendisine bağlı bulunan uçlara sinyal gönderen basit cihazlardan bahsetmemiz mümkündür. Cihazın basitliğine rağmen, kullanımı oldukça yaygın ve gereklidir. Bir hırsız alarm sistemi kurulumu yapılırken, kesinlikle kullanılması gereken cihazlardandır.

Alarm kontrol paneli ile ilgili bölümde, hırsız alarm sistemleri döşenirken, ev ya da iş yerinin farklı bölgelere ayrıldığından bahsedilmişti. Tüm bu bölgelere yetkisiz bir giriş olup olmadığını algılayan cihazlar, doğru yerleştirilmiş hareket algılayıcılarıdır.



**Resim 2.5:** Hareket Algılayıcılar

Hareket algılayıcılar için en büyük problem, yanlış yerleştirme sorunudur. Algılayıcının yerleştirildiği bölge içerisindeki tüm alan, algılayıcı tarafından izlenebilir olmalıdır. Bölge içerisinde algılayıcı tarafından izlenemeyen bir alan, yetkisiz girişin burada yapılması ve hırsızlık alarm sisteminin hiçbir uyarı vermemesi anlamına gelmektedir. Hareket algılayıcılar, analog ya da dijital olarak hareketi algılayabilmektedir. Görüş açısına göre dar açılı hareket algılayıcılar, tavan tipi hareket algılayıcılar mevcuttur. Gerekli görüldüğü durumlarda görüş açısını ayarlayabilmek ya da bölgenin tamamını kontrol altına alabilmek için, uygun olan hareket algılayıcısı seçilmelidir.

Hareket algılayıcılar da iki farklı çeşitte incelenebilir. İlk çeşit, hareket gördüğü an kendisinin direk olarak bağlı bulunduğu aydınlatma ürününü ya da sireni tetikleyen, alarm kontrol panelinden bağımsız çalışan algılayıcılardır.

Hırsızlık alarm sistemlerinde kullanılan hareket algılayıcılar ise, aynı manyetik kontaklarda olduğu gibi, alarm kontrol paneline kablolu ya da kablosuz olarak bağlı çalışır. Yerleştirildiği bölgede herhangi bir hareket gördüğü an, bağlı bulunduğu alarm kontrol paneline sinyal göndererek bilgi verir. Bundan sonra yapılacak işleme, alarm kontrol paneli karar verir.

Kablosuz çalışan hareket algılayıcılar üzerinde bir batarya yardımı ile veri alış verişinde bulunur. Bataryanın azalması ya da bitmesi, hareketin algılanamamasına ya da algılanan hareketin alarm kontrol paneline gönderilememesine sebep olur.

Hareket algılayıcılar için önemli bir problem de evcil hayvan beslenen ev ya da iş yerleridir. Evcil hayvanlar sürekli hareket halinde olacaklarından algılayıcı alarm kontrol paneline sürekli sinyal göndermek durumunda kalacaktır. Bu durumda evcil hayvanın bulunduğu bölgede hareket algılayıcı kullanmak anlamsız olacaktır. Bu sorunu önlemek için evcil hayvan bağışıklı hareket algılayıcılar geliştirilmiştir. Bu tür algılayıcılar belirli bir ağırlığın altındaki hareketli cisimlere sinyal yaratmamaktadır. Bu sayede sadece yetkisiz şahıs girişlerinde alarm kontrol paneline sinyal göndermektedir.

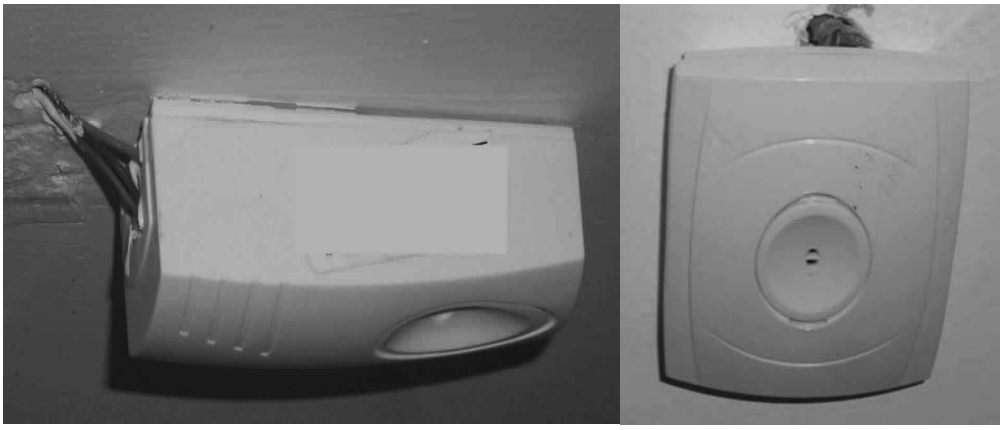
**Resim 2.6:** Hareket Algılayıcı

İç mekânda olduğu gibi, dış mekânda kullanılan hareket algılayıcılar da mevcuttur. Dış mekânda kullanılan hareket algılayıcılarda sağlıklı sonuç alınabilmesi hava şartlarına da bağlıdır.

SIRA SİZDE 2 **Hareket algılayıcılar, son yıllarda hırsız alarm sistemlerinden farklı olarak bir cihaza daha bağlı ve sıkça karşımıza çıkmaktadır. Bu cihazın nasıl çalıştığını gözlemleyerek bulmaya çalışınız.**

## Cam Kırılma Detektörleri

Cam kırılma detektörleri, bulunduğu ortamdaki cam kırılmasını algılayıp alarm kontrol paneline bildiren cihazlardır. İçerisinde cam bulunan bölgelere yerleştirilir. Yetkisiz giriş, eğer camın kırılması ile olacaksa, detektör bunu algılayarak alarm kontrol paneline bildirir. Camın kırılması iki farklı metotla anlaşılır. Bu metotlardan ilki, camın kırılması esnasında çıkan sestir. Detektör bu sesi algılayarak gerekli sinyali gönderir. İkinci metot ise darbe ve şok dalgası analizidir. Kapalı bir ortamdaki camın birden kırılması ile içeride oluşan basınç değişimini algılayan detektör, alarm kontrol merkezine gerekli sinyali gönderir.



**Resim 2.7:** Cam Kırılma Detektörleri

Cam kırılma detektörü de, diğer cihazlarda olduğu gibi, alarm kontrol paneline sinyali kablolu ya da kablosuz olarak gönderebilir.

## Ağırlık Detektörleri

Ağırlık detektörleri zemin altına yerleştirilerek belli bir ağırlığın üzerindeki cisimleri algılayan elektronik sistemlerdir. Tabana yerleştirilen ağırlık detektörü ile ortam tabanında olacak küçük bir ağırlık farklılığı, alarm kontrol paneline iletilir.

Ağırlık detektörü, sinyal gönderme ağırlığı açısından ayarlanabilir yapıya sahiptir. Aynen hareket algılayıcılarda olduğu gibi, ağırlık detektörleri de evcil hayvanlara karşı ayarlanır. Böylece, evcil hayvanın ağırlığını aşan durumlarda panel bilgilendirilir.

## Siren ve Flaşörler

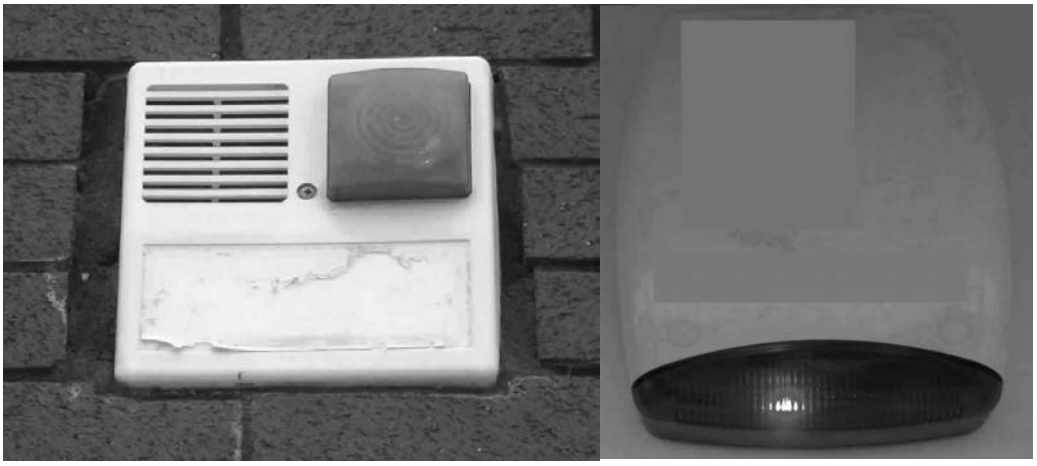
Başlangıçta, hırsız alarm sisteminin ana kumanda paneli olan alarm kontrol panelinin bir merkeze bağlı olup olmama durumu belirlenmelidir. Eğer tek başına çalışan bir hırsız alarm sistemi var ise, siren ve flaşör daha önemli bir görev üstlenmektedir.

Sirenler, dâhili ve harici olarak iki bölümde incelenebilir. Dahili sirenler ev ya da iş yerinin içerisinde bulunan, nispeten daha az ses çıkışına sahip cihazlardır. Alarm kontrol paneli ile bağlantısı sayesinde çalma işlemini bu panelden emir alarak gerçekleştirir. Dahili sirenler üzerinde bir elektronik devre ile ses çıkartmaya yardımcı bir hoparlör bulunur. Bazı modellerde ledler ile aydınlatma sağlayan flaşör devreler de mevcuttur.

Harici sirenler ise, ev veya işyerinin dışında bulunan, genellikle herkes tarafından kolayca görünebilecek bir yere monte edilen cihazlardır. Ses çıkışları yüksektir. Çalması durumunda dikkati o ev ya da iş yerine çekmek ve güvenlik personeli ya da kolluk kuvvetlerine yetkisiz girişin yapıldığı yeri belli edebilmek amacı ile üzerlerinde flaşör adı verilen yerleşik bir aydınlatma sistemi bulunur. Bir çok harici siren içerisindeki yerleşik aküden beslenir. Böylelikle elektrik kaynağının kesilmesi, çalma durumunu ve flaşörün yanmasını engellemez.

Hem dâhili, hem de harici sirenler çalma ve üzerlerindeki flaşörü yakarak uyarı verme eylemlerini alarm kontrol merkezine bağlı olarak gerçekleştirirler. Tüm kaynaklardan veri toplayan alarm kontrol merkezi, aksi giden bir durumda ilk olarak siren ve flaşör ile uyarı verir.

Sirenler için en belirleyici özellik ne kadar yüksek ses verdikleridir. Etraftaki güvenlik görevlilerini ve kolluk kuvvetlerini uyarmak için çıkartılan sesin yüksek olması gerekmektedir. Bu sebeple sirenler üzerinde yerleşik bulunan hoparlörler yüksek seviyede sesi uzun süre yayınlayabilmek için tasarlanmıştır. Çıkarttıkları ses miktarı, ses ölçüsü olan desibel ile ölçülür.



**Resim 2.8:** Harici Siren ve Flaşör Örnekleri

Dâhili sirenler genellikler alarm kontrol paneli yakınlarına, harici sirenler ise ev veya iş yerinin ana giriş kapısının üzerine yerleştirilerek, aynı zamanda mekânın hırsız alarm sistemi ile korunduğunu da gösterirler. Bu vasıta ile caydırıcı etkiye de sahip olurlar.

## Telefon Arayıcılar

Herhangi bir merkeze bağlı olup olmamasından bağımsız olarak, hırsızlık alarm sistemleri, gerekli durumlarda daha önceden belirlenen numaraları arayarak sesli mesajı ya da cep telefonlarına kısa mesajı iletebilir. Sesli veya kısa mesaj alıcıları çoğu zaman tek numaradan fazladır. Bunun için sistemin bağlı bulunduğu mekânda telefon hattının bulunması ve telefon hizmetinin veriliyor olması gereklidir.

Bir merkeze bağlı sistemlerde alarm kontrol paneli üzerindeki bilgiler (manyetik cam-kapı kontaklarının durumu, hareket algılayıcılarından gelen raporlar, ağırlık ya da cam kırılma detektörlerinin bildirdiği problemler) bu merkez tarafından da anında görüntülenmektedir. Bu sebeple herhangi bir uyarı durumu, sirenlerin ve flaşörlerin devreye girmesinden önce bu merkezde bulunan bilgisayarda uyarının kaynağı ile birlikte görüntülenmektedir. Bundan dolayı herhangi bir numaraya sesli veya yazılı mesaj gönderilmesi çok gerekli olmayabilir.

Fakat bir merkeze bağlı olmadan çalışan sistemlerde telefon arayıcıların önemi ortaya çıkmaktadır. Herhangi bir cihazdan bir uyarı sinyali alan alarm kontrol paneli, daha önceden kendisine belirtilen numaralara bilgi verir. Bilgi verme işi sesli mesajla veya kısa mesajla olabilir. Bu durumda arama yapılan numaralar genellikle ev ya da işyerinin sahibi, özel bir güvenlik şirketinin telefonu ya da kolluk kuvvetlerinin telefonudur.

Cep telefonlarının yaygınlaşması ile telefon arayıcılar da normal hat ile çalışan telefon arayıcılar ve GSM aramayı gerçekleştiren arayıcılar olarak çeşitlendirilebilir. GSM aramayı gerçekleştirebilmek için arayıcı üzerinde bulunan haberleşme kartının desteklediği operatörün kapsama alanı içerisinde bulunması gereklidir. Hangi telefon arayıcının uygun olacağı, tamamen aranacak numaralar ve sesli ya da kısa mesaj gönderme durumuna göre değişiklik gösterir.


**Telefon arayıcıların hizmet verebilmesi için, bu cihaza hizmet veren bir telefon hattının faal olarak bulundurulması gereklidir. Telefon hattı olmadan arama yapılamaz.**

## Kablolama

Hırsız alarm sistemlerinde tüm cihazların alarm kontrol merkezi ile haberleşmesi son derece önemlidir. Sadece bir cihazın bile haberleşmesinde aksilik olması, o cihazın bulunduğu bölgedeki yetkisiz bir girişe karşı önlem alınamaması anlamına gelir. Bir alarm sisteminin düzgün çalışması, bağlı bulunduğu tüm bölgelerde eksiksiz bağlantı ile sağlanır.

Hırsız alarm sistemi kablosu denince aklımıza, bina içerisinde tesisatta bulunan ve cihazların sinyallerini alarm kontrol merkezine taşıyan esnek kontrol ve iç bağlantı kabloları gelmektedir. Kabloların dış yüzeyi PVC bir kaplama ile kaplıdır. Bu kaplama, kabloyu dış etkilerden mümkün oldukça korumak amacı ile kullanılır. Dış kaplamanın üzerinde kablonun üretici firması, kablonun metresi ve kablonun tipi belirli aralıklarla yazılıdır. Kablonun metresinin dış kaplama üzerinde yazılması sayesinde, kullanılan kablo metrajı daha kolay belirlenmektedir.

Kablo, içerisinde kullanılan iç kablo sayısına, PVC kaplamanın altında sarma bandı korumasına, bakır örgü tellerle ekran tatbik edilmesine, iç kabloların sarmallık durumuna göre çeşitlere ayrılır. Her bir kablonun kullanım yeri ve hatasız veri taşıma mesafesinin uzunluğu birbirinden farklıdır. Sistem oluşturulurken doğru yerde doğru kablonun da kullanılması sistemin sağlıklı çalışması açısından önemlidir.

## Işınlı Bariyer Detektörleri

İki parçadan oluşan bu detektör, bir taraftan gönderilen infrared ışının, diğer parçadaki fotoledler tarafından algılanması esasına bağlı çalışır. Detektör devreye alındıktan sonra araya giren herhangi bir şahıs ya da nesne ışının kesilmesine yol açacaktır. Bu da alarm kontrol paneline sinyal gönderilmesine sebep olacaktır.

Genellikle dış mekân kullanımına yönelik olan ışınlı bariyer detektörlerinin, kapı ve pencereler için kullanılan tipleri de mevcuttur. İlk çıkan sürümlerinde kar veya yağmur yağması ışının kesilmesine ve hatalı sinyal üretimine neden olsa da, yeni nesil ışınlı bariyer detektörlerinde problem çözülmüştür. Işınlı bariyer detektörlerinin infrared ışın yerine lazer ışını gönderen modelleri de son kullanıcılara sunulmuştur.


**Hareket algılayıcılarda olduğu gibi, ışınlı bariyer detektörleri de son yıllarda, hırsız alarm sistemlerinden farklı bir amaç ile karşımıza çıkmaktadır. Bu amacın ne olduğunu özellikle otomatik giriş sistemine sahip bariyer ya da garaj kapılarını inceleyerek bulmaya çalışınız.**

## Panik Butonları

Alarm kontrol paneline direk bağlı olan panik butonları, herhangi bir cihazdan bir sinyal gelmemesine rağmen, alarmı devreye almak için kullanılır. Genellikle dışarıdan yardım istemek amacı ile yerleştirilir. Bankalar, döviz büroları, kuyumcular gibi hırsızlık ya da gasp olayının daha sık rastlandığı yerlerde, hırsızlık veya gasp olayı ile karşılaşıldığında, kullanıcı panik butonuna basarak alarmı devreye alır ve bu sayede özel güvenlik şirketlerinden ya da kolluk kuvvetlerinden yardım istenir. Panik butonunun, dışarıdan kolayca görünmeyecek ama kullanıcılar tarafından kolaylıkla erişilebilecek bir yere yerleştirilmesi uygundur.

## Uzaktan Kumandalar

En basit amacı, alarm sistemini devreye almak veya devreden çıkartmaktır. Devreden çıkartma işleminde kullanılmak için eğer gerekiyorsa üzerinde, alarm kontrol panelinde bulunana benzer, bir numara takımı barındırır. Bazı modellerinde üzerindeki ledler ile alarm kontrol merkezi ile veri haberleşmesinin gücü görüntülenebilir. Gelişmiş modellerde gerekli butonlar yardımıyla uzaktan kumanda sayesinde alarm çalıştırılabilir, çalışan alarm susturulabilir ya da sistem sıfırlanabilir. Uzaktan kumanda cihazı üzerinde

bir panik butonu da bulundurabilir. Yerleşik bulunan batarya ile enerji ihtiyacını karşılar. Bataryanın azalması ya da bitmesi durumunda uzaktan kumanda işlevi devre dışı kalır.

## İnternet Modülü

Alarm kontrol panelindeki bilgilere dışarıdan internet hattına sahip bir bilgisayar ile erişmeyi amaçlayan bir bileşendir. Ev veya işyerindeki internet hattına genellikle RJ45 konnektör ile ya da kablosuz olarak bağlanır. Gerekli ayarların yapılması ile ev veya iş yeri dışından internete bağlı bir bilgisayar ile alarm kontrol paneline bağlantı sağlanır. Bağlantı aşamasında yetkisiz erişimleri engellemek amacı ile kullanıcı adı ve şifre doğrulaması yapılır. Alarm kontrol paneli ile bağlantı yapıldıktan sonra tüm izleme işlemleri ile birlikte, alarmın devreden çıkartılması, devreye alınması, panik çağrısının yapılması ve bunun gibi birçok işleme, alarm kontrol panelinin izin verdiği düzeyde erişim sağlanır.


**İnternet modülünün çalışabilmesi için karşı merkeze bağlı olan bir internet hattına ihtiyaç vardır. Internet hattı ile bağlı olmayan merkezlerde bu modülden faydalanmak mümkün değildir.**

## Aküler

Herhangi bir hırsızlık, sabotaj veya gasp anında kötü niyetli kişilerin hırsız alarm sistemi kurulu bir mekânda yapacakları ilk iş şehir gerilimini keserek, ev ya da işyerini elektriksiz bırakmak olacaktır. Bu sebeple hırsız alarm sistemlerinin her durumda faal olabilmesi gereklidir. Bundan dolayı sistemlerin, içlerinde bir akü barındırması ve şehir elektriğinin kesilmesi durumunda bu akü ile beslenmesi gerekmektedir.

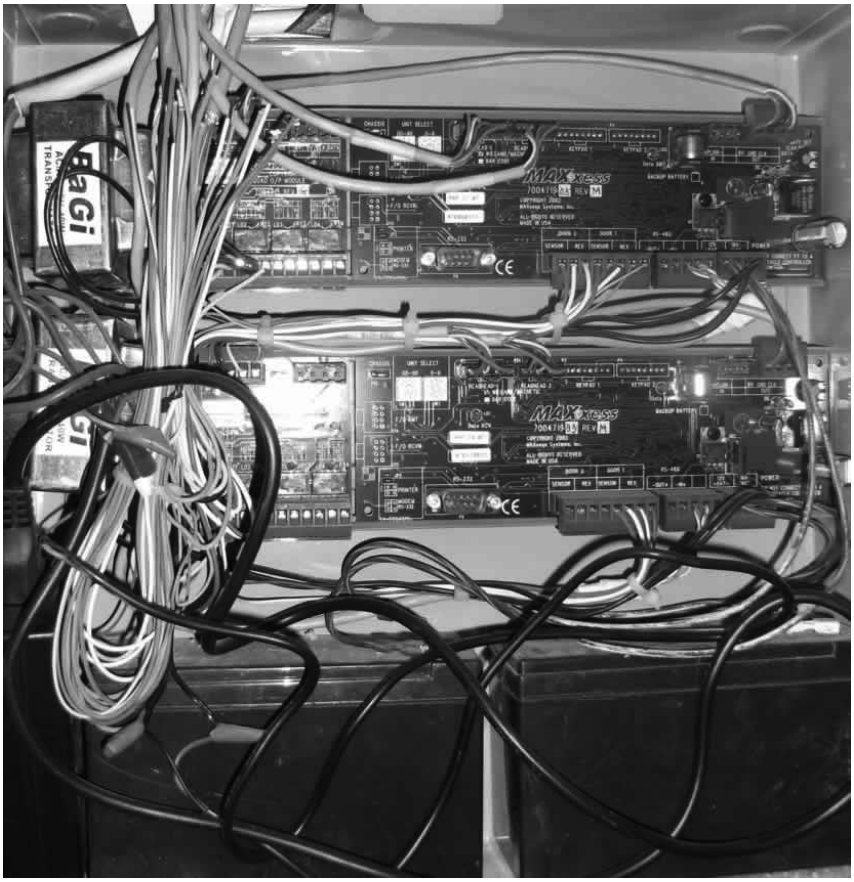
Hırsız alarm sisteminin en önemli parçasının alarm kontrol paneli olduğundan bahsedilmişti. Tüm diğer cihazlar bilgilerini bu panele göndermekte ve panel tarafından değerlendirilen bilgiler neticesinde gerek varsa siren ve flaşör devreye alınmakta, telefon arayıcı gerekli numaraları aramaktadır. Bu sebeple ilk olarak alarm kontrol paneli içerisinde yerleşik bir akü bulunması gereklidir. Bunun dışında siren ve flaşör de kendi aküsüne sahip olabilir.

Eğer alarm kontrol paneli ile diğer cihazlar arasındaki haberleşme kablosuz sağlanıyorsa, her cihaz kendi aküsüne ya da bataryasına sahip olmak zorundadır.

## Kablosuz Haberleşme

Eğer hırsız alarm sistemindeki cihazların, alarm kontrol paneli ile haberleşmeleri kablosuz olarak sağlanacaksa, sistemin tüm bileşenleri kablosuz sisteme uygun cihazlardan seçilmelidir. Bu durumda alarm kontrol paneli tüm cihazlardan gelen verileri her biri için ayrı frekans kullanarak değerlendirecek ve bölge ve cihaz ayırımını gerçekleştirecektir. Panele bilgi gönderen tüm cihazlar da kendilerine ait frekanstan sinyal göndererek durumları hakkında bilgiyi alarm kontrol paneline ileteceklerdir.

Cihazlar arası kablosuz haberleşme sağlanacaksa, enerji ihtiyacı da genelde cihazlarda yerleşik bulunan pil ya da bataryalardan sağlanacak ve gerektiğinde bu bataryalar şehir gerilimi ile şarj edilecektir.



**Resim 2.9:** Alarm İç Tesisatı ve Aküler

## YANGIN ALARM SİSTEMLERİ

Konaklama, toplanma, eğitim, sağlık hizmeti, ticaret, ofis, endüstriyel, depolama, cezaevi, ev gibi amaçlarla kullanılan tüm binalarda, yangına sebep olacak bir aksaklığı veya yangın olayını başlamadan ya da başlangıç aşamasında henüz tehlikeli bir boyuta ulaşmadan önlemeyi amaçlayan sistemlerdir. Yangın alarm sistemleri tüm bina için özel bir projelendirme ile kurulur. Bu projelendirme, mekânın farklı bölgelere (zone) bölünmesi ve gerekli algılayıcının gerekli bölge ya da bölgelere kurulmasını sağlar. Burada dikkat edilecek nokta, tüm bölgelerde aynı cihaza ihtiyaç duyulmamasıdır. Doğalgaz boru hattının geçtiği bölgelerde gaz detektörü kullanılması gerekirken, gaz hattı bulunmayan bölgelerde böyle bir detektörün yerleştirilmesi gereksiz olacaktır. Duman, ısı ve sabit ısı detektörleri de kendilerine ihtiyaç duyulan bölgelere yerleştirilir.

Sistem en basit şekilde tarifle, yangını çıkmadan ya da başlangıç aşamasında algılayarak çeşitli detektörlerden gelen bilgileri işleyen bir ana kumanda paneli ve gerektiğinde kullanılmak üzere kumanda paneline bağlı bulunan siren ve flaşörden oluşur.

Yangın alarm sistemlerinde önemli olan yangının başlangıç aşamasında veya henüz yangın oluşmadan oluşturabilecek nedeni anlayarak uyarı vermesi ve eğer gerekiyorsa yangın söndürme sistemlerini devreye sokmasıdır. Uyarı yapılmadan geçen her saniye öncelikle insan hayatına ve devamında mala zarar verecektir. Uyarı yapıldıktan sonra ise önemli olan doğru bölgeye müdahale edilmesi gerekliliğidir. Yangın alarm sistemlerinin yangın olayının ya da riskinin bulunduğu bölgeyi doğru göstermesi gereklidir. Yangın alarm sistemleri, bölge bilgisinin alınmasına göre iki farklı kategoride incelenebilir:

- **Klasik Yangın Alarm Sistemleri**: Sistemde yangın olan ya da yangına sebep olabilecek gaz veya duman çıkışını algılayan detektörün işaret ettiği bölge alarm paneli üzerinde görüntülenir. Bina katlar şeklinde ayrıldıysa, sadece ihbarın geldiği katın bölgesi genellikle panel üzerindeki ledlerle gösterilir.
- **Adresli Yangın Alarm Sistemleri**: Klasik yangın alarm sistemlerine göre daha gelişmiş olan sistemde, genellikle LCD ekran üzerinde bölge adresi ve sinyal gönderen detektör tipi görüntülenir. Klasik sisteme göre daha kesin şekilde ilk müdahale yapılması sağlanır.

Her ne kadar evler ve küçük iş yerleri ya da müstakil ticarethaneler için keyfi de olsa, devlet daireleri, eğitim kurumları, fabrikalar ve büyük ticari işletmeler, alışveriş merkezleri gibi birçok yapı için yangın alarm sistemi kurulması yasal bir zorunluluktur. Yangın alarm sistemlerinin nasıl yerleştirileceği konusunda yönetmelikler de çeşitli bakanlıklar tarafından yayınlanan teknik şartnamelerde açıklanmıştır.


**Teknik şartnameler konusunda detaylı bilgi almak ve şartnameleri incelemek için www.bayindirlik.gov.tr internet sitesi ziyaret edilebilir.**

Yangın, sabotaj sonucu oluşabileceği gibi, teknik bir hata ya da dikkatsizlik sonucu da meydana gelebilir. Mutfakta kullanılan fırın ve ocağın yanması, sıcak su ihtiyacı için kullanılan şofben ürünü, ısınma ve sıcak su sağlamak için kullanılan kombi ya da kat kaloriferi ürünleri gerekli olan ısı enerjisini son yıllarda katı yakıttan daha çok yanıcı sıvı gazlar ile sağlamaktadır. Bu gaz ev ya da işyeri içerisinde doğalgaz ya da yer altına gömülü likit gaz tanklarından bir tesisat yardımıyla gerekli cihazlara ulaşabileceği gibi, tüplerden direk bağlı oldukları cihazlara da aktarılabilmektedir. Aktarım sırasında tesisatta oluşabilecek en ufak aksilik, bu çok yanıcı gazın havaya karışması anlamına gelir. Havaya karışan gaz eğer önlem alınmazsa, herhangi bir ateş kaynağı ile temas ettiği an patlamaya ve arkasından da yangına sebep olur.

Yangına sebep olan bir diğer sebep ise kullanıcıların dalgınlıkları ya da dikkatsizlikleridir. Ocakta bırakılan bir çaydanlık, elektrik kaynağı ile bağlantısı kesilmeden bulundurulan ütü, devrilmiş bir elektrikli ısıtıcı gibi ürünler ve üzerinden gereğinden fazla yük çekilen prizler yangına sebep olmadan önce yoğun duman çıkışı ile yangını belli eder.

Sabotaj sonucunda yangının çıkma riskine karşı önlemi hırsız alarm sistemleri ile de azaltabiliriz. Komple bir alarm sistemi kurmak istediğimizde, hırsız alarm sistemi ile yangın alarm sistemini beraber düşünmeliyiz. Yangın alarm sistemlerinde, hırsız alarm sistemlerine ek olarak gelen cihazlar ile yangın çıkmadan önce uyarı ve önlem alma ya da yangının başlangıç anında uyarı ve yangını önlemeye yönelik işlemler yapılmaktadır.

Yangın alarm sistemlerindeki cihazları,

- Yangın Alarm Panelleri,
- Gaz detektörleri,
- Duman detektörleri,
- Isı detektörleri,
- Işınlı Bariyer Detektörleri,
- Alev ve Kıvılcım Detektörleri,
- Siren ve flaşörler,
- Işıklı Yönlendirme Panoları,
- Yangın Alarm Butonları (Kır-Bas Butonlar)
- Telefon Arayıcılar ve İnternet Modülleri,
- Kablolar, Kablosuz Cihazlar, Aküler,

olarak sıralayabiliriz. Aynı hırsız alarm sistemlerinde, sistemin kurulumunda olduğu gibi, yangın alarm sistemlerinin kurulumu için de tüm parçaların kullanımı gerekmez. Kurulum sırasında kullanılacak parçalar, sistemin kurulacağı mekânın özelliklerine göre seçildiği kadar, kanuni zorunluluk nedeniyle yapılan sistemlerde gerekli kanun maddelerine bağlı kalmak zorunludur. Gerektiğinde sistemi teşkil etmek için kullanılabilecek bu cihazlara kısaca göz atalım.

## Yangın Alarm Panelleri

Yangın alarm panelleri, aynen hırsız alarm sistemlerinde kullanılan ve tüm cihaz bağlantılarını üzerinde toplayan alarm kontrol panelleri gibi çalışmaktadır. Bütünleşik alarm sistemlerinde hırsız alarm kontrol paneli, aynı zamanda yangın alarm kontrol paneli olarak da görev yapar. Bu durumda hırsız alarm sistemi cihazları gibi, tüm yangın alarm sistemi cihazları da kablolu ya da kablosuz şekilde alarm kontrol paneline bağlanmak ve gerekli durumlarda sinyal göndermek zorundadır.

Daha önce bahsedildiği gibi, tüm bölgeler için detektörlerin doğru yerleşimi yapıldıktan sonra, bu cihazlar kablolu ya da kablosuz şekilde yangın alarm paneli ile bağlantıya geçirilir. Gaz detektörleri, duman detektörleri, ısı ve sabit ısı detektörleri, ışınlı bariyer sistemleri bölgeleri bazında panele bağlanırlar. Bağlanan aletler arasında yangın butonları olarak adlandırılan kır-bas butonlar da mevcuttur. Yangın alarm paneli tüm cihazlardan gelen verileri sürekli inceler. Herhangi bir detektör ya da yangın butonundan bir sinyal geldiğinde, kendisine bağlı bulunan tüm siren ve flaşörleri devreye sokar. Hırsız alarm sistemlerinden farklı olarak siren ve flaşör yerleştirilmesi tüm bölgeler, koridor ve merdivenler için ayrı ayrı yapılır. Yangın alarm paneli değerlendirme yaparak sadece yangın olayı ya da riski bulunan bölgedeki siren ve flaşörü çalıştırabilir.

Yangın alarm paneli bağlantılı olarak, eğer varsa, yangın söndürme sistemini de devreye sokar. Gerekli durumlarda bina içerisindeki yangın ekibine, güvenlik görevlilerine bilgi verir. Üzerinde yerleşik telefon arama modülü bulunuyorsa daha önceden belirlenen numaralara ve şehir itfaiyesine bilgi vererek acil müdahale imkânı sağlar.

Yangın alarm paneli, sistemin klasik yangın alarm sistemi veya adresli yangın alarm sistemi olmasına bağlı olarak üzerindeki ledler ya da LCD ekran vasıtasıyla uyarı alınan bölgeyi işaret eder. Yangın uyarısı anında üzerinde yerleşik bulunan hoparlörü vızıltı (buzzer) verecek şekilde kullanarak uyarı ses ile de yayınlar. Hızlı ve doğru müdahale yapılması için alarm anında bu panel ziyaret edilerek yangın ile ilgili bölge bilgisine ulaşılır.

Yangın alarm panelinin ön kısmında ledler veya LCD gösterge ile bilgi almayı sağlayan birimin yanı sıra, alarmı devreye alma, kapatma, susturma, sirenleri çalıştırma ya da kapatma, detektörleri test etme, sistemi sıfırlama gibi işlevlerde kullanılacak tuşlar da mevcuttur. Eğer sistem hırsız alarm sistemi ile beraber kullanılıyorsa bu işlevler, ortak kullanılan tuş takımı ile sağlanır.

Yangın eğer elektrik kontağından çıkmışsa, doğal olarak mekânın gerilimi sigortaların atması sunucunda kesilecektir. Böyle bir durumda algılayıcıları çalıştırmak, acil durum aydınlatmalarını devreye sokmak, gerekli siren ve flaşörü çalıştırmak, yangın alarm panelinin görevleri arasındadır. Bu sebeple, yangın alarm panelinin üzerinde elektrik kesilmelerinde sistemi besleyecek aküler mevcuttur.


**Resim 2.10:** Yangın Alarm Panelleri

## Gaz Detektörleri

Yangın alarm sistemlerinde, yangına sebep olabilecek problemlere karşı da uyarılar bulunduğundan bahsedilmişti. Gaz detektörleri, yangına sebep olabilecek gaz kaçakları ile ilgili uyarıyı sağlayan cihazlardır. Özellikle mutfak içerisinde bulunan fırın ve ocağın beslenmesi, su ya da mekân ısıtmasının sağlanması için kullanılan doğalgaz veya lpg, tutuşabilir gazlar sınıfındandır. Bu tür gazların ortamda normal değerden fazla bulunması, elektrik kontağı ya da alevle temas etmesi durumunda patlama ve beraberinde yangın oluşumuna sebep olacaktır. Gaz detektörleri, tutuşabilir gazların normalden fazla değerde olduğunu algıladıkları an sinyal yaratmaktadırlar.

İki farkı çeşit gaz detektöründen bahsetmek mümkündür. Birinci tip gaz detektörleri, bir yangın alarm sistemine bağlı olmaksızın çalışan, genellikle ev ya da küçük iş yerlerinde gaz hattı yakınına yerleştirilen, normalden fazla gaz çıkışında üzerinde bulunan ledler ve hoparlör yardımıyla sesli ve ışıklı uyarı veren cihazlardır. Şehir gerilimi ile çalışabildikleri gibi üzerlerinde yerleşik bulunan pillerden güç alarak da çalışırlar.

İkinci tip gaz detektörleri ise, yangın alarm sistemlerine bağlı kullanılan gaz detektörleridir. Bu çeşit gaz detektörleri de diğer çeşitte olduğu gibi gaz hatlarının bulunduğu ortamlara konumlandırılırlar. Hava içerisinde normalden fazla tutuşabilir gaz tespit ettiklerinde yangın alarm paneline sinyal göndererek aksiliği belli ederler. Bu durumda siren ve flaşörü çalıştırma görevi yangın alarm panelinindir.

Gaz detektörleri, hava içerisindeki tutuşabilir gaz oranı normale düştüğünde alarm vermeyi ya da yangın alarm paneline sinyal göndermeyi keserler.


**Evinizde fırın-ocak için kullanılan gaz tipini araştırınız. Eğer doğalgaz ya da lpg tüpü kullanılıyorsa, gaz detektörü ile güvenliği arttırınız.**

**Resim 2.11:** Gaz Detektörü

## Duman Detektörleri

Bu detektörler ortamda duman bulunduğunda devreye girerler. Bu detektörlerin, dumanı algılama yöntemine göre üç farklı çeşiti mevcuttur. Bunlar şu şekilde sıralanabilir:

- **Optik Duman Detektörleri**: Bu tür detektörlerde fotoelektrik algılama prensibinden faydalanılır. Detektörün içerisine giren duman tarafından içeride bulunan ışığın kırılması ya da emilmesi sonucunda algılama sağlanır. Bu sayede detektör, ortamda duman bulunduğunu anlayarak alarmı devreye sokar ve yangın alarm paneline sinyal gönderir.
- **İyonize Duman Detektörleri**: Görünebilir ve görünemez gaz parçacıklarını içerisinde bulundurduğu radyoaktif madde ile algılayan detektör tipidir. Özellikle fazla duman parçacığı çıkartan yüksek enerjili yangınlarda, optik duman detektörüne göre daha kesin sonuçlar vermektedir.
- **Video Duman Detektörleri**: Bu tip duman detektörleri, bir video kamera ve görüntü değişimi algılama yazılımı ile birlikte çalışmaktadır. Genellikle bu detektörün kullanımında ortamdaki güvenlik kameralarının üzerine görüntüyü işlemeye yönelik bir yazılım yüklenmektedir. Görüntüde olacak bir değişim, yangın uyarısı olarak algılanmaktadır.

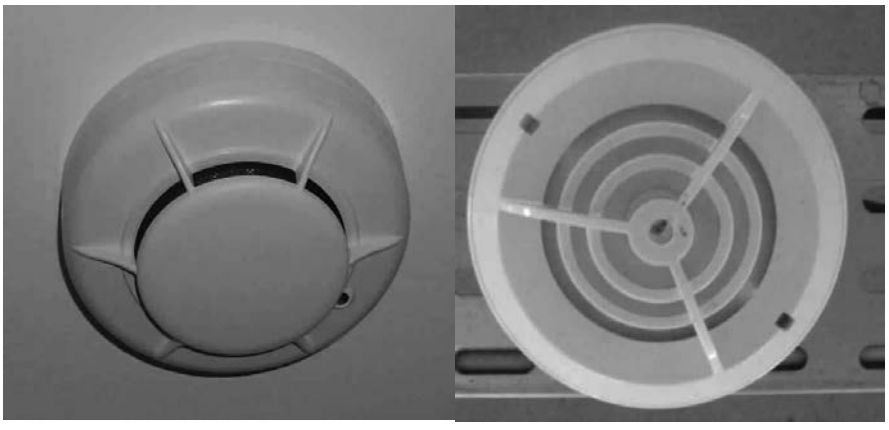
**Resim 2.12:** Çeşitli Duman Detektörleri

Duman detektörleri, ısı detektörlerine göre daha hızlı algılama yeteneğine sahiptirler. Duman detektörlerinin normal şartlarda kullanım yerleri duman, toz ya da buhar bulunmayan genel mahallerdir. Ortamda bulunan buhar, araba egzoz dumanı, boya parçaları ya da tesislerde üretimden kaynaklanan dumanlar yanlış algıya ve yanlış alarm sinyali yaratılmasına sebep olmaktadır. Otel odalarına yerleştirilen duman detektörlerinin çoğu sigara dumanından etkilenerek yanlış sinyal göndermekte ve paniğe yol açmaktadır. Genellikle bir adet duman detektörü ile 70-100 $m^2$ büyüklüğündeki alanlarda algılama yapmak mümkündür.

## Isı Detektörleri

Ortamın ısısındaki değişimlere göre algılama yapan ısı detektörleri de dört farklı çeşitte kullanıma sunulmaktadır. Bunlar;

- **Isı Artış Detektörleri**: İçerisinde bulunduğu ortam ısısının belirli bir zaman aralığındaki değişimine göre algılama yapan detektör tipidir. Kısa bir zaman aralığında ortamda fazla bir ısı artışı söz konusu ise yangın olayından ya da en azından başlangıcından söz etmek mümkündür. Bu durumda ısı artış detektörü hızlı ısı artışını algılayarak yangın alarm paneline sinyal gönderir. Bu sayede yangın, henüz başlangıç aşamasındayken önlenebilir.
- **Sabit Isı Detektörleri**: Ortam ısısı ayarlanan bir değere ulaştığın an detektör sinyal verir ve yangın alarm panelini bilgilendirir. Ayarlanan ısı değeri genellikle yangın tarafından yükseltilebilecek kadar yüksek bir değer olmalıdır. Aksi durumda herhangi bir ısı kaynağından gelecek ısı yükselmesi bile detektörün yanlış sinyal yaratmasına yok açacaktır.
- **Sabit Isı ve Isı Artış Detektörleri**: Hem ortam ısısının ani değişimini, hem de ortam ısısının belirli bir değerin üzerine çıkmasını kontrol eden yukarıdaki her iki detektörün de özelliklerini bünyesinde barındıran detektör tipidir.
- **Termoelektrik Tip Isı Detektörleri**: Isı değişiminin, detektör içerisindeki devrenin direncinin değiştirmesi esasına dayalı algılama yapan detektör tipidir. Isı artış ya da sabit ısı detektörü olarak kullanılabilmektedir. Hızlı algılama yapılması gereken mekânlarda kullanımı daha uygundur.



**Resim 2.13:** Isı Detektörleri

Isı detektörleri normal şartlarda içerisinde yoğun şekilde buhar, toz, duman, egzoz gazı bulunan ortamda kullanılır. Duman detektörleri tarafından yanlış sinyal yaratılabilecek bu ortamlarda, bölüm güvenliği ısı detektörleri tarafından sağlanır. Bir ısı detektörü ile 30-50 $m^2$ büyüklüğünde alanlar için algılama yapılabilir. Yangın anında ısınan havanın ortamdaki soğuk hava ile karışarak seyreleceği göz önüne alınırsa, yüksek tavanlı mekânlarda ısı detektörlerinin daha sık yerleştirilmesi uygundur.

Isı detektörlerinin de tek başlarına çalışan modelleri mevcuttur. Üzerinde yerleşik bataryası, hoparlör ve led uyarı sistemi olan bu detektör tipi ile hiçbir yangın alarm sistemine bağlı olmaksızın ısı değişimleri algılanarak siren ve flaşör ile uyarı sağlanır.

## Işınlı Bariyer Detektörleri

Yangın alarm sistemlerinde kullanılan ışınlı bariyer detektörleri, hırsız alarm sistemlerinde kullanılan ışınlı bariyer detektörlerinin kullanımı ile çalışma prensibi olarak aynı fakat kullanım mantığı olarak biraz farklıdır.

Bu sistemde kullanılan ışınlı bariyer detektörleri de infrared ya da lazer ışını yayan bir verici ve karşı tarafta da bu ışını algılayan fotoled alıcı bulunmaktadır. Hırsız alarm sistemlerinde kullanılan ışınlı bariyer detektörlerinde ışının bir insan veya nesne ile kesilmesi sonucunda sistem, yetkisiz bir girişe karar verip alarmı aktif hale getirmekteydi. Bu sistemin hatasız çalışması için kar, yağmur ya da dumandan etkilenmemesi, daha büyük nesneler tarafından ışın kesintiye uğradığı zaman sinyali aktif hale getirmesi gerekliydi.

**Resim 2.14:** Işınlı Bariyer

Yangın alarm sistemlerinde kullanılan ışınlı bariyer detektörlerinde ise araya giren dumanın ışını kesmektedir. Böylelikle olası bir yangın başlangıcına karşı önlem almak gerekmektedir.

## Alev ve Kıvılcım Detektörleri

Ortamda bulunan kıvılcımın yangına sebep olması ya da yangın başlangıcında yayılan alevin algılanması esası ile çalışan detektör tipleridir.

Kıvılcım detektörleri, kıvılcım sonucunda patlamaların ve devamında büyük yangınların baş göstereceği yerlerde kullanılır. Özellikle yakıt gibi birden alev almaya müsait maddelerin saklandığı depolarda ya da pompalarında kullanılan kıvılcım detektörlerinin verimli çalışması için karanlık ortama ihtiyaç vardır.

Alev detektörleri, alevi algılama metotlarına göre kızılötesi, ultraviyole ya da her ikisi ile birlikte çalışan detektörler olarak gruplandırılabilir. Farklı kimyasal maddeler tarafından başlatılan yangınların algılanması ve yangın alarm paneline gerekli uyarı sinyalinin gönderilmesi amacı ile kullanılır. Kullanılacak olan detektör çeşidi, tamamen kullanılacak mekânda bulunan maddelerin kimyasal özelliklerine göre seçilir.

## Siren ve Flaşörler

Hırsız alarm panellerinde siren ve flaşörleri incelerken, dahili ve harici sirenlerin herhangi bir hırsızlık, gasp ya da sabotaj durumunda dışarıdaki özel güvenlik elemanlarını ya da kolluk kuvvetlerini uyarmak amacı ile kullanıldıkları belirtilmişti. Yangın alarm sistemlerinde ise sirenler ve flaşörler daha çok içeride bulunan insanları uyarmaya yöneliktir.

**Resim 2.15:** Yangın Siren ve Flaşör Örnekleri

Yangın anında binanın tahliyesinin sağlanması amacı ile siren ve flaşörlerle uyarı yapılmalıdır. Bu sayede içeride bulunan insanların kendilerine en yakında bulunan yangın tahliye kapısını kullanarak binayı terk etmeleri amaçlanmaktadır. Bu sebeple, yangın alarm sistemlerinde siren ve flaşör kullanımı, hırsız alarm sistemlerinden sayı olarak çok daha fazladır.

Hırsız alarm sistemlerinde alarm kontrol paneline bağlı dahili veya harici bir sirenden bahsederken, yangın alarm sistemlerinde tüm alarm bölgelerini ayrı ayrı uyarmayı sağlayacak kadar çok siren ve flaşör kullanılması gerekmektedir.

Siren ve flaşör yerleşimi, yangın alarm paneline direk bağlı olmasından ziyade, her bölgede ayrı ayrı ve yangın alarm butonlarının her birine bağlı şekilde yapılmalıdır. Böylece, yangın alarm panelinden gelen sinyal olmasa dahi, yangını fark eden ve uyarı vermek isteyen herhangi bir kişi de bu butonu kullanarak siren ve flaşörü devreye alabilecektir.

## Işıklı Yönlendirme Panoları

En basit kullanımı ile ışıklı yönlendirme panoları, yangın anında tahliyeyi sağlayacak aydınlatmayı sunmak ve üzerindeki yönlendirme ile mekanı tahliye edecek insanları doğru güzergâhlara göndermek için kullanılır. Üzerlerinde bulunan bataryalar ile bina içerisindeki gerilim kesilmesinde dahi yönlendirme ve aydınlatmayı sağlayacaklardır.

Üzerlerinde led lambası bulunan yönlendirme panoları ise, daha çok, çok katlı ve büyük kompleksler için uygundur. Yangın anında birden fazla çıkışa sahip olan mekânlarda yangının çıkış bölgelerine göre tahliye edilecek şahısları en zararsız yollara sevk ederek tahliye etmek gerekmektedir. Yangın alarm paneline bağlı çalışan ledli yönlendirme panoları, gerekli yolu panelden gelen sinyallere göre göstererek tehlikesiz tahliyeye imkân sağlamaktadır.

## Yangın Alarm Butonları

Bu butonlar yangın anında detektörlerden sinyal gelmemesi durumunda, yangını fark eden şahısların alarmı el ile çalıştırması için kullanılmaktadır. Mekanda bulunan şahısların hatayla alarm sistemini devreye sokarak gereksiz paniğe yol açmamaları için, butonun üzerinin bir cam koruması mevcuttur. Bu durumda yangın alarm butonları, kır-bas buton olarak da adlandırılır. Yangını fark eden şahıs, alarmı aktif hale getirmek için öncelikle bu koruyucuyu kırmalı, arkasından butona basmalıdır.


**Resim 2.16:** Farklı Yangın Alarm Butonları

Buton genellikle kendisine bağlı bulunan siren ve flaşör ile birlikte bulunur. Yangın alarm butonuna basıldığında yangın alarm paneline, hangi bölgedeki butonun basıldığına dair bilgi giderken, bağlı bulunan siren ve flaşör de devreye girer. Böylelikle bölge içerisindeki şahısların tahliyesi sağlanır.

DİKKAT **Yangın alarm butonlarının kır-bas tipi olanlar tek kullanımlıktır. Üzerindeki cam ya da koruyucu kırılarak faal hale getirilen butonun, alarm susturulduktan ve tehlike geçtikten sonra yenisi ile değiştirilmesi gereklidir.**

SIRA SİZDE 4 **Hırsız alarm sistemlerinde kullanılan panik butonları ile yangın alarm sistemlerinde kullanılan yangın alarm butonlarının benzer ve farklı özelliklerini belirleyiniz.**

## Telefon Arayıcılar ve İnternet Modülleri

Yangın alarm sistemlerinde bulunan telefon arayıcılar ve internet modülleri de, hırsız alarm sistemlerindeki görevlerinin aynısını gerçekleştirmekle yükümlüdür. Telefon arayıcılar, alarm durumunda kendilerine bağlı bulunan telefon hattını kullanarak daha önceden belirlenen numaraları ve eğer programlandıysa itfaiyeyi arayarak bilgi vermektedir.

İnternet modülü ile de iki taraflı olarak, hem sistem dışarıdan izlenebilmekte, hem de acil durumda modülün diğer ucundan hangi bölgede yangın ya da benzeri bir uyarı olduğu ile ilgili detaylı bilgi alınabilmektedir. Her iki sistem de yangın alarm paneline bağlantılı olarak, genellikle panel ile aynı kutuda bulunur.

SIRA SİZDE 5 **Daha önceki bilgilerimizden, telefon arayıcıların ve internet modülünün çalışabilmesi için, yangın alarm sisteminin bağlı bulunduğu mekanın hangi alt yapı özelliklerine sahip olması gerektiğini belirtiniz.**

## Kablolar, Kablosuz Cihazlar ve Aküler

Yangın alarm sistemlerinde kablolama, sistemin en önemli noktasıdır. Tüm birimlerin yangın alarm paneline bağlı çalışması gerekliliğinden daha önce bahsetmiştik. Tüm bu birimlerin iletişimi eğer kablolu olarak sağlanacaksa kablolarda da dikkat edilmesi gereken noktalar mevcuttur. Yangın anında kablonun enerji ve bilgi iletimini kesmeyecek kadar dayanıklı olması bu gerekliliklerin başında gelir.

Yangın şartlarında, yüksek ısı ve alev altındayken, veri ve enerji iletimini sağlamayı saatlerce sürdüren kablolar, özellikle büyük binalarda tesisat kablosu olarak da kullanılmakta, böylece sadece yangın alarm sisteminin değil, aynı zamanda asansör, havalandırma cihazları, aydınlatma gibi hayati öneme sahip donanımların da çalışır durumda olması sağlanmaktadır.

Yangın kabloları söz konusu olunca, kablonun yangını iletmeme özelliği de önemlidir. Tahmin edilebileceği gibi kablolar, tesisat ile tüm binayı kuşatmaktadır. Bir bölgede baş gösteren bir yangın, tesisat kabloları eğer alevi taşıyacaksa, çok kısa zamanda binanın tüm bölgelerine sıçrayacaktır. Diğer durumda ise belki de yangın sadece bir ya da yakınındaki birkaç bölgede kalacak ve yangın söndürme sistemleri ve itfaiye yardımı ile kolayca söndürülecektir. Bu da binanın tamamının yanmaktan kurtulması anlamına gelecektir.

Yangın kablolarındaki bir diğer önemli husus, yangın anında kablonun yanması neticesinde çıkan gazın insan sağlığı açısından etkisidir. Yangına dayanıklı kablolar, çok yoğun ısı ve alev altında belli bir süre sonra, kablo yanmaya dahi başlasa, açığa çıkan gaz insan sağlığını tehdit etmeyecek şekilde üretilmektedir.

Yangın alarm sistemlerinde eğer kablosuz haberleşme seçilecek olursa, yangın alarm panelinde tüm cihazlardan gelen verileri algılayacak bir kablosuz alıcı bulunmalıdır. Bu durumda tüm diğer çevre cihazları da kablosuz veri iletimine olanak sağlayacak yapıda olmalıdır.

Kablosuz cihazlarda en büyük sorun, daha önce hırsız alarm sistemlerinde de bahsedildiği gibi, cihazların bataryalarının azalması ya da bitmesidir. Bu durumda cihazlar görevlerini yerine getirememektedir. Cihazlar üzerinde bulunan bataryaları şehir gerilimi ile şarj etmek suretiyle bu sorunun üstesinden gelinmeye çalışılmaktadır. Cihazların elektrik kesilmesinde de görevlerini eksiksiz yerine getirmeleri için akülerden de faydalanılır. Özellikle yangın alarm paneli bir akü ile canlandırılarak, kesintisiz işlem sağlanır.

## Özet

Elektronik alarm sistemleri, güvenliği sağlamak, insanları ve mekanları korumak amacı ile bir araya getirilen bir çok cihazın birleşimi ile oluşan bütünleşik yapılardır. Her ne kadar sistemin oluşturulması için kullanılan cihazların, sistem içine girmeden tek başlarına kullanılan modelleri mevcut olsa da, tam bir güvenlik çemberi yaratmak için gerekli görüldüğü durumlarda tümünden faydalanmak seçeneği işlemleri kolaylaştıracaktır.

Elektronik alarm sistemi kurulumdan önce mekânın incelenmesi ve projelendirilmesi, hem maliyet hem de sistemin doğru çalışması için gereklidir. Proje aşamasında sistemin kurulacağı mekân bölgelere (zone) ayrılır. Bölgelerin durumuna göre gerekli algılayıcılar, gereği kadar sıklıkta yerleştirilir. Tüm algılayıcılar bir merkezde toplanır. Bu merkezin özelliği, algılayıcılardan gelen mesajlara gore alarm sistemini devreye alıp almayacağına karar vermektir. Elektronik alarm sisteminin beyni olarak da düşünebileceğimiz bu cihaz, kendisine bağlı bulunan siren ve flaşör, telefon arayıcı, internet modülünü kullanarak gerekli uyarı ve haberleşmede bulunur. Bu merkezin, bir ya da gerektiğinde daha fazla akü ile desteklenerek, kesintisiz çalışması sağlanır.

Kitabın bu ünitesinde elektronik alarm sistemlerini iki başlık altında incelenmiştir. İlk kısımda hırsız alarm sistemleri ve sistemi oluşturan cihazlar incelenmiştir. Hırsız alarm sistemleri, güvenliği sağlanmak istenen mekâna kurulumu yapıldıktan sonra hırsızlık, gasp ya da sabotaj amacı ile yetkisiz girişleri algılamaya yönelik cihazlardan oluşur. Hareket algılayıcılar, cam ya da kapı kontakları, ağırlık detektörleri, ışınlı bariyer sistemleri, cam kırılma detektörleri ile algılanan yetkisiz giriş, alarm kontrol merkezine bildirilir. Alarm kontrol merkezi kendisine bağlı bulunan siren ve flaşörü devreye sokar. Üzerinde yerleşik bulunan telefon arayıcı ile gerekli numaralara gerekli bilgileri iletir. Üzerinde yerleşik internet modülü bulunan alarm kontrol merkezleri ise, hangi detektörün, hangi bölge içerisinde ne tür bir uyarı verdiğini uzak kullanıcıya kesin şekilde bildirmeyi amaçlar. İnternet modülü sayesinde uzak kullanıcı alarm panelinin yönetimini de gerçekleştirebilir. Hırsız alarm sistemlerinde bir avantaj da panik butonlarının kullanımıdır. Genellikle gizli bir konuma yerleştirilen panik butonları ile ev ya da işyeri sahipleri veya çalışanları herhangi bir gasp ya da sabotaj olayında, hiçbir detektör algısına gerek kalmaksızın alarmı devreye sokma ve dışarıya bir aksilik olduğunu bildirme şansına sahiptir. Hırsız alarm sistemlerinin çoğu zaman kolluk kuvvetleri veya özel güvenlik şirketleri ile bağlantısı da bulunmaktadır.

Bu ünitede anlatılan ikinci elektronik alarm sistemi ise yangın alarm sistemleridir. Yangın alarm sistemleri, sadece yangın anında değil, yangın oluşumuna sebep olabilecek herhangi bir aksilikte de bizleri uyarmayı amaçlayan bir sistemdir. Özellikle gaz ya da duman detektörleri bu amaç için çok faydalıdır. Sistem kurulumu yapıldıktan sonra çeşitli detektörler ile gaz kaçağı, duman çıkışı, kıvılcım ya da alevlenme takip edilmektedir. Tüm detektörler yangın alarm paneline direk bağlıdır. Aksi bir durumda detektörlerden gelen sinyaller, yangın alarm paneli tarafından değerlendirilir ve gerekli ise alarm devreye alınır. Yangın alarm panelinin, yangın alarmı durumunda, siren ve flaşörü devreye almak, telefon ya da internet bağlantısı ile dış kullanıcılara bilgi vermek gibi görevleri vardır. Yangın alarm panelinin bunlara ek olarak tahliye işlemini kolaylaştırmak için gerekli uyarı panolarına gerekli mesaj ve yönlendirme bilgilerini iletme, varsa yangın söndürme sistemlerini devreye alma fonksiyonları da vardır. Sistem algılayamasa da yaygın olarak kullanılan yangın alarm butonları ile sistemin istenildiği anda devreye alınması imkânı vardır.

Elektronik alarm sistemlerinin incelendiği bu bölümde, sistemi oluşturan birçok farklı cihazdan bahsedilmiştir. Herhangi bir sistemi oluşturmak için bu bahsedilen cihazların tümünün aynı anda kullanılması şart değildir. Sistemin güvenli ve sağlıklı çalışması için, oluşturulurken hangi parçaların kullanılacağı uzman kişiler tarafından belirlenmektedir. Bazı durumlarda ise sistemin hangi parçalardan oluşacağı, teknik şartnamelerle bakanlıklar bazında belirlenmektedir.

İnsan sağlık ve güvenliği için çalışan elektronik alarm sistemleri, bizlerin daha güvenli ve sağlıklı bir ortamda yaşaması için artık lüks değil gereklilik olarak değerlendirilmelidir.

## Kendimizi Sınayalım

**1.** Aşağıdakilerden hangisi hırsız alarm sistemi cihazlarından biri değildir?

a. Hareket Algılayıcılar

b. Isı Detektörleri

c. Manyetik Kontaklar

d. Cam Kırılma Detektörleri

e. Ağırlık Detektörleri

**2.** Cam kırılma detektörleri, cam kırılma eylemini hangi yöntem ile algılar?

a. Duman çıkışı ile

b. Cam parçalarını görerek

c. Kıvılcım çıkışı ile

d. Basınç farkı ile

e. Ortam ısısındaki değişim ile

**3.** Hangi siren tipi dış mekana yerleştirilerek uyarı sağlanır?

a. Dahili Siren

b. Optik Siren

c. Harici Siren

d. Giriş Sireni

e. Vızıltı Sireni (buzzer)

**4.** Telefon arayıcıların çalışması için aşağıdakilerden hangisi sağlanmalıdır?

a. Alarm paneli üzerinde tuş takımı bulunmalı

b. Dahili sirene bağlı olmalı

c. Sistem bir güvenlik merkezine bağlı olmalı

d. Harici sirene bağlı olmalı

e. Çalışan bir telefon hattına bağlı olmalı

**5.** Hırsız alarm sistemlerinde uzaktan kumanda aşağıdaki hangi eylemi gerçekleştiremez?

a. İnternet modülüne bağlanmak

b. Panik alarmını çalıştırmak

c. Sistemi sıfırlamak

d. Sistemi kapatmak

e. Sistemi devreye almak

**6.** Aşağıdakilerden hangisi yangın alarm sistemi cihazlarından biri değildir?

a. Isı Detektörleri

b. Duman Detektörleri

c. Panik Butonları

d. Hareket Algılayıcılar

e. Gaz Detektörleri

**7.** Aşağıdakilerden hangisi bir ısı detektörü tipi değildir?

a. Isı Artış Detektörleri

b. Isı Dengeleme Detektörleri

c. Sabit Isı Detektörleri

d. Sabit Isı ve Isı Artış detektörleri

e. Termoelektrik Tip Isı Detektörleri

**8.** Yangın Alarm Paneli, alarm durumunda aşağıdakilerden hangisini yapmaz?

a. Sireni çalıştırmak

b. Flaşörü çalıştırmak

c. Telefon araması yapmak

d. Acil durum aydınlatmasını kapatmak

e. İnternet modülü ile dışarıya bilgi vermek

**9.** Elektronik alarm sistemlerinde aküye ne zaman ihtiyaç duyulur?

a. Elektrik kesintisi olduğunda

b. Detektörler sinyal verdiğinde

c. Telefon arayıcı hattı bulamadığında

d. Internet bağlantısı kesildiğinde

e. Ortam aydınlatması yetersiz olduğunda

**10.** Yangın alarm sistemleri döşenirken kullanılacak kablo, yangın anında aşağıdaki hangi özelliği sağlamaz?

a. Uzun süre daha veri iletimini sağlamalı

b. Yandığında insan sağlığına zarar vermemeli

c. Yangını taşımamalı

d. Yandıktan sonra kablo renkleri görünebilmeli

e. Uzun süre daha enerji iletimini sağlamalı

## Kendimizi Sınayalım Yanıt Anahtarı

**1. b** Yanıtınız yanlış ise "Hırsız Alarm Sistemleri" başlıklı konuyu yeniden gözden geçiriniz.

**2. d** Yanıtınız yanlış ise "Hırsız Alarm Sistemleri - Cam Kırılma Detektörleri" başlıklı konuyu yeniden gözden geçiriniz.

**3. c** Yanıtınız yanlış ise "Hırsız Alarm Sistemleri – Siren ve Flaşörler" başlıklı konuyu yeniden gözden geçiriniz.

**4. e** Yanıtınız yanlış ise "Hırsız Alarm Sistemleri – Telefon Arayıcılar" başlıklı konuyu yeniden gözden geçiriniz.

**5. a** Yanıtınız yanlış ise "Hırsız Alarm Sistemleri – Uzaktan Kumandalar" başlıklı konuyu yeniden gözden geçiriniz.

**6. d** Yanıtınız yanlış ise "Yangın Alarm Sistemleri" başlıklı konuyu yeniden gözden geçiriniz.

**7. b** Yanıtınız yanlış ise "Yangın Alarm Sistemleri – Isı Detektörleri" başlıklı konuyu yeniden gözden geçiriniz.

**8. d** Yanıtınız yanlış ise "Yangın Alarm Sistemleri – Yangın Alarm Paneli" başlıklı konuyu yeniden gözden geçiriniz.

**9. a** Yanıtınız yanlış ise "Yangın Alarm Sistemleri – Kablolar, Kablosuz Cihazlar ve Aküler" başlıklı konuyu yeniden gözden geçiriniz.

**10. d** Yanıtınız yanlış ise "Yangın Alarm Sistemleri – Kablolar, Kablosuz Cihazlar ve Aküler" başlıklı konuyu yeniden gözden geçiriniz.

## Sıra Sizde Yanıt Anahtarı

### *Sıra Sizde 1*

Herhangi bir mekânda hırsız alarm sistemi var ise, alarm kontrol paneline bağlı olan harici siren ve flaşör dışarıdan kolayca fark edilecek, görülebilecek bir yere yerleştirilir. Bu genellikle ana giriş kapısının üzeridir. Hırsız alarm sistemi eğer bir güvenlik firması tarafıdan kurulduysa, firmanın adını da barındıran bir uyarı levhasını da görmek mümkündür.

### *Sıra Sizde 2*

Hareket algılayıcılar, son yıllarda aydınlatma sistemlerinde de sıklıkla kullanılmaktadır. Üzerine yerleştirilen hareket algılayıcı ile aydınlatma sistemi hareket algıladığı an aktif hale gelmektedir.

### *Sıra Sizde 3*

Işınlı bariyer detektörleri otomatik kapanma özelliğine sahip bariyer sistemleri ya da garaj kapılarında kullanılır. Genellikle kapının bir cisim veya bir araç üzerine kapanmasını önlemek için kullanılır. Site, otopark ya da alışveriş merkezleri girişlerinde bu detektörlere kolayca rastlanabilir.

### *Sıra Sizde 4*

Her iki sistemde kullanılan butonların ortak özellikleri, alarm sistemini devreye sokmaktır. Butona basıldığında gerek hırsız alarm kontrol paneline gerekse yangın alarm paneline uyarı giderek sistemler aktif hale gelir. Aralarındaki temel fark ise, hırsız alarm sistemlerindeki panik butonunun genellikle gizli, yangın alarm sistemlerindeki ihbar butonunun ise görünebilir ve kolay ulaşılır yerlere yerleştirilmesidir.

### *Sıra Sizde 5*

Telefon arayıcının faal çalışması için çalışır halde hizmet veren bir telefon alt yapısına, internet modülünün devreye alınabilmesi için ise çalışır halde bir internet bağlantısına ihtiyaç vardır.

## Yararlanılan Kaynaklar

Pearson, R.L. (2007). **Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions**, Butterworth-Heinemann, Elsevier.

## Yararlanılan İnternet Kaynakları

http://www.bayindirlik.gov.tr

http://megep.meb.gov.tr

http://mevzuat.meb.gov.tr

http://tr.wikipedia.org

# 3

## Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Giriş Kontrol Sistemleri bileşenlerini örneklerle açıklayabilecek,
- Turnikeli, kartlı ve biyometrik sistemlerin yapısını ve çeşitlerini anlatabilecek,
- Dedektörlü ve X-Işını sistemlerin yapısını açıklayabilecek,
- RFID sistemler ile araç plaka tanıma sistemlerinin yapısını ve çeşitlerini özetleyebilecek

bilgi ve becerilere sahip olabilirsiniz.

## Anahtar Kavramlar

- Turnikeli Sistemler
- Biyometrik Sistemler
- X-Işını Sistemler
- Araç Plaka Tanıma Sistemleri
- Kartlı Sistemler
- Dedektörlü Sistemler
- RFID Sistemler

## İçindekiler

# Bina Giriş Kontrol Sistemleri

## GİRİŞ

Elektronik güvenlik sistemleri çatısı altında bulunan giriş kontrol sistemleri, günümüzde devlet ve özel sektördeki tüm kurum ve kuruluşların çeşitli güvenlik sorunlarına karşı çalışanlarını ve ziyaretçilerini denetim ve kontrol altına almaları için vazgeçilmez bir güvenlik sistemi haline gelmiştir. Personel, ziyaretçi veya kötü niyetli kişilerden kaynaklanabilecek olumsuz olayları engellemenin ilk adımı, kişilerin sadece izin verilen alanlara girebilmelerini sağlamaktır. Giriş kontrol sistemi, temel olarak kişinin kimliğini, giriş zamanını ve nereye gireceğini belirlemekte, denetlemekte ve uygulamaktadır.

Binaların sayısı, büyüklükleri, kullanıcı sayısı ve kullanım amacı da sistemin güvenlik boyutunda belirlenmesi için önemli etkenlerdir. Oteller, rezidanslar, alışveriş merkezleri, hastaneler, eğitim kurumları, metro ve tren istasyonları, hava alanları, askeri tesisler hatta hapishaneler birbirinden farklı güvenlik gereksinimlerine sahiptir. Binaya en uygun sistemin uygulanabilmesi için bir dizi tespit ve değerlendirme çalışması yapılmalıdır. Bu çalışmanın ana maddelerini aşağıdaki şekilde sıralamak mümkündür.

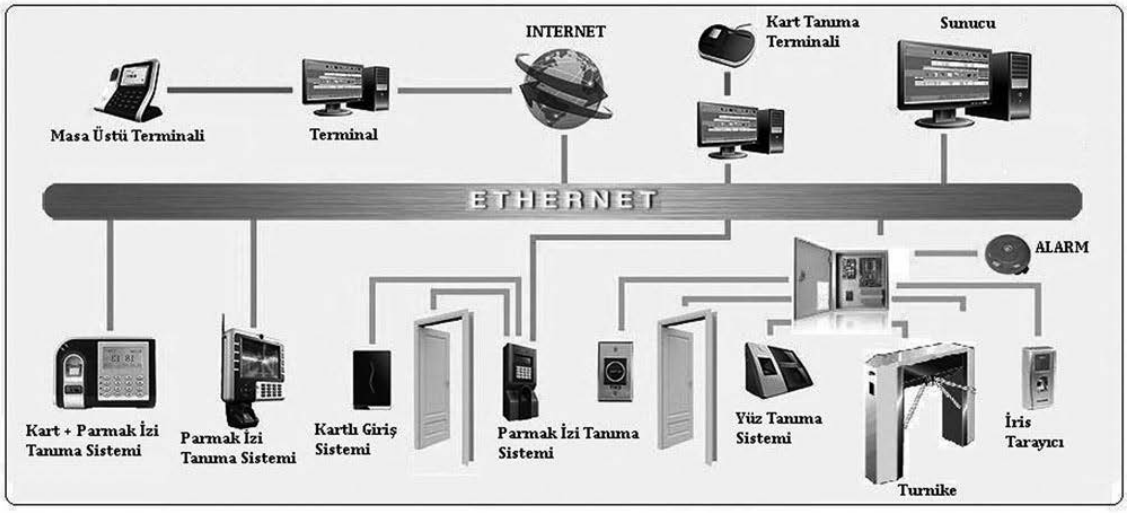
- Bina analiz edilerek izleme ve raporlama gereksinimleri belirlenir.
- Uygulanacak güvenlik tedbirleri belirlenir ve sistemin binadaki görüntülü kamera sistemi, yangın alarm sistemi, otomasyon sistemi, asansör sistemi gibi sistemlere uyumu için gereksinimler belirlenir.
- Güvenlik senaryoları tartışılır, can emniyeti gereksinimleri ile herhangi bir uyumsuzluk olup olmadığı araştırılır ve eğer bir uyumsuzluk varsa giderilecek çözümler belirlenir.
- İleriye yönelik büyüme ve genişleme gereksinimleri değerlendirilir.

Giriş kontrol sistemlerinde her farklı kişi için farklı yetki seviyeleri de belirlenebilmektedir. Bu sayede binadaki tüm personelin ve dışarıdan gelenlerin hareketi kontrol edilebilmekte ve gerektiği takdirde kullanılacak mekânlara, gerek zaman kısıtı gerekse giriş kısıtı getirilebilmektedir. Giriş kontrol sistemlerinde personel ve ziyaretçilerin bilgileri tutularak güvenlik senaryolarının uygulanmasını sağlayan çeşitli güvenlik yönetim yazılımları da kullanılmaktadır. Sistem, kişinin belirlenen yetkiler kapsamında hareket etmesini sağlayarak yetki dışına çıkması durumunda güvenlik merkezine çeşitli alarm düzeylerinde ikazlar gönderebilmektedir.

Giriş kontrol sistemlerinin, yukarıda belirtilen işlevlerin yanı sıra gelişen teknoloji ve artan talepler doğrultusunda farklı kullanım şekillerine de uyumlu olarak çalışması gerekmektedir. Günümüzde biyometrik sistemlerle uyumlu olarak kullanılmaya başlandığı gibi, personelin devamlılığını kontrol eden sistemlerin, ziyaretçilerin bina içerisindeki çeşitli yerlere girişlerini de kontrol eden aynı zamanda yüksek güvenliğin gerekli olduğu noktalarda, kart okutulmasının yanında kameralardan alınan görüntülerle, sistemin veritabanında bulunan fotoğraf bilgisini kontrol ederek maksimum güvenliğin sağlandığı noktalara gelinmiştir. Dâhili ağ ve internet ortamlarından kontrol edilebilmeyle birlikte, dünyanın herhangi bir bölgesinden haberleşme ve entegrasyonu da sağlanabilmektedir.

Bina giriş kontrol sistemlerinde farklı kullanım alanları için farklı çözümleri olmasına karşın, temel olarak sistemde akıllı kartlar, yakınlık (proximity) kartlar, mifare kartlar gibi geçiş alanında kullanılan

yetkilendirilmiş kartlar ve bu kartları okuyan donanımlar, parmak izi tanıma alanında kullanılan parmak izi okuyucu, yüz tanıma sistemi gibi biyometrik sistemler ve hidrolik bariyer, mantar bariyer, kollu bariyer ve daha pek çok modelde bariyer sistemleri ile turnike sistemleri, kapı kontrol sistemleri gibi mekanik elemanlar bulunmaktadır.




**Resim 3.1:** Bina Giriş Kontrol Sistemi ve Personel Devam Kontrol Sistemi Yapısı

Bütün bu elektronik ve mekanik donanımların bağlı bulunduğu bilgisayar yazılımları da bina giriş kontrol sistemleri için en önemli bileşenlerdendir. Kartlı veya biyometrik sistemler, kapı, bariyer, turnike gibi giriş noktalarına monte edilerek bilgisayar yazılımı yardımıyla gerçekleştirilen yetkilendirmeyle hangi personelin giriş yapacağını belirlemektedir.

Bina giriş kontrol sistemlerini iki ana başlık altında toplamak mümkündür.

- Kişi Giriş Kontrol Sistemleri
- Araç Giriş Kontrol Sistemleri

Bu ünite içerisinde bina giriş kontrol sistemlerinde kullanılan bileşenler alt başlıklar içerisinde kısaca ele alınacak olup, kitabın diğer ünitelerinde ise bu bileşenler daha ayrıntılı olarak anlatılacaktır.

# KİŞİ GİRİŞ KONTROL SİSTEMLERİ

Kontrolün yapılacağı sistemin insan odaklı olduğu durumu bu başlık altında toplamak mümkündür. Bina girişi yapacak olan kişinin üzerinde taşıdığı veya yanında getirdiği eşyalarının da kontrolü bu sistemler tarafından yapılmaktadır. İstenmeyen eşyaların binaya girmesi bu aşamada engellenebilmektedir. Ziyaretçi, personel veya kötü niyetli kişileri belirleme amaçlı olan bu sistemde, personel takip, ziyaretçi kaydı gibi kısımların yanında, yemekhane kontrol sistemi, yurt yoklama sistemi gibi binaların yapısına göre çalışabilecek sistemlerle entegre olarak da kullanılabilmesi mümkündür.

Kişi odaklı olan bu kontrol sisteminin en önemli özelliği kişinin bina girişini yaptıktan sonra da izlenebilmesidir. Yetkisi dâhilinde bina içerisindeki hareketi sağlanmakta ve yetki dışına çıkması engellenmektedir. Günümüzde en çok kullanılan Kişi giriş kontrol sistemleri çeşitlerini iki alt başlık altında sıralayabiliriz:

- İnsan Kontrol Sistemleri
    - Turnikeli Sistemler
    - Kartlı Sistemler
    - Biyometrik Sistemler (Parmak izi, iris-retina, ses tanıma, yüz tanıma vb.)

- Eşya Kontrol Sistemleri
    - Dedektörlü Sistemler
    - X-Işını Sistemler

Şimdi bu sistemleri alt başlıklar halinde inceliyelim.

## İnsan Kontrol Sistemleri

### *Turnikeli Sistemler*

Büyük alışveriş merkezleri girişlerinde, metro ve tren istasyonlarında, fabrikalarda ve daha pek çok mekan girişlerinde oldukça yaygın olarak kullanılan sistemlerdir. Üst araması yapmak, kişilerin biletle geçiş yaptığına emin olmak ya da personel devam kontrol sistemlerinden faydalanabilmek için turnikeli giriş sistemleri kullanılmaktadır. Kullanım amaçlarına göre birçok turnike çeşiti vardır. Bunlar içerisinde, günümüzde en yaygın olarak kullanılanlarını aşağıdaki şekilde sıralamak mümkündür:

- Kartlı Turnikeler
- Parmak İzli Turnikeler
- Fotoselli Turnikeler
- Kelebek Turnikeler
- Üç Kollu (tripod) Turnikeler
- Boy Turnikeler
- Jetonlu Turnikeler
- VIP Turnikeler

Kartlı ve parmak izli olan turnikeler daha çok fabrikalarda personel devam kontrol sistemi amaçlı olarak da kullanılmaktadır. Parmak izi ya da yakınlık kart okuyucu terminaller turnikelerin üzerine yerleştirilebilmektedir. Bunların yanında mifare kart okuyucu, yakınlık kart okuyucu, parmak izi okuyucu ve çeşitli şifreli okuyucular bağlanarak güvenli geçiş sağlanabilmektedir. Örneğin, yemekhane girişlerinde çalışanların turnikelerden okuyucu terminaller vasıtasıyla geçiş yapmaları sağlanabilmekte, personelin öğünlerini, yemekhaneye giriş saatlerini, yabancı kişi girişlerini takip etmek ve raporlamak mümkün olabilmektedir.

Özürlü ya da VIP turnikeler tek kollu turnikelerdir. Açık konumdayken kolay geçiş yapılabilmekte ve geçişlerin kolaylaştırılması açısından farklı amaçlarla kullanılabilmektedirler. Acil durumlarda tahliye amaçlı olarak, engelli kişilere kolay geçiş sağlamak ya da çıkışlarda kalabalığın hızlı şekilde çıkışını sağlamak üzere yaygın olarak kullanılan turnike sistemlerindendir.

Üç kollu (tripod) turnikeler daha çok personel girişlerinde, stadyum gibi mekânlarda ise boy turnikeleri kullanılmaktadır. Boy turnikeler döner kapıları andırmaktadır. Diğer turnike çeşitlerinde olduğu gibi sadece bel hizasında değil, baştan aşağıya döşenmiş kollardan oluşmakta ve bir insan boyundadırlar. Bu durumda geçişler daha yavaş olmakta, kişiler tek tek ve sıkı bir kontrolle içeri alınmaktadırlar.

**Resim 3.2:** Turnikeli Giriş Sistemi

Turnike Sistemleri, diğer güvenlik sistemleriyle iç içe kullanılmaktadır. Turnike üzerine yerleştirilebilen bir okuyucu ünite vasıtasıyla alınan veri, bilgisayar kontrollü sistemlerle yorumlandıktan sonra geçiş hakkı var ise turnikenin tetiklenmesiyle geçiş sağlanabilmekte, aksi takdirde geçiş hakkı sağlanamamaktadır. Aynı zamanda Turnike Sistemlerinde tek yön veya çift yön çalıştırılabilme özelliği de mümkün olabilmektedir.

Birçok turnike modeli artık yuvarlatılmış köşeli, çarpma ya da düşmelere karşı insanların yaralanma riskini en aza düşürecek şekilde tasarlanmaktadır. Elektrik arızası gibi durumlarda ise, kolların otomatik olarak serbest kalması sayesinde geçişlerin aksamaması sağlanmaktadır. Aşağıda günümüzde kullanılmakta olan birkaç turnike sistemi fotoğrafı gösterilmektedir.

**Resim 3.3:** Boy, Üç Kollu, VIP turnike örnekleri

Görüldüğü üzere pekçok farklı mekânda, değişik amaçlarla da olsa en çok kullanılan bina giriş sistemlerinden biri, turnikeli sistemlerdir. Kullanımı pratik ve yerleşimi kolaydır. Diğer güvenlik sistemleriyle kolayca entegre olabildiklerinden, eskimeyen ve yenilenen yaşam alanlarına kolaylıkla uyum sağlayan sistemlerdir.

Hürriyet Gazetesi'nin 08.01.2008 tarihli haberinde konuyla ilgili olarak örnek bir kullanım anlatılmaktadır. İlgili haber:

> *"İzmir Mimar Sinan Anadolu Teknik, Teknik ve Endüstri Meslek Lisesinde öğrencilerin ders saatlerinde okul dışına çıkmalarını engellemek amacıyla turnike sistemi kuruldu. Okul Müdürü Mehmet Gürses, öğrencilerin okula düzenli devam etmelerini ve güvenliklerini sağlamak amacıyla turnike sistemi oluşturduklarını belirtti. Okuldaki her öğrencinin fotoğraflı manyetik kartı bulunduğunu anlatan Gürses, şu bilgileri verdi:*
>
> *"Öğrenci kartını sisteme gösterdiğinde çıkış izni yoksa turnike dönmediği için dışarı çıkamıyor. Sistem sayesinde güvenlik görevlisi ya da nöbetçi öğretmenlerle, öğrenci arasında tartışma yaşanmasının önüne geçmiş oluyoruz. Öğrenci dilediği saatte dışarı çıkamadığı için, okul dışında art niyetli kişilerle karşılaşma riski de ortadan kalkıyor. Veli, öğrencinin öğlen tatilinde dışarı çıkmasını istiyor ve mesuliyetini üzerine alıyorsa, dilekçe vererek bunu sağlayabiliyor."*

*Öğrencilerin, ailenin bilgisi ve izni olmadan okula gelmemesi durumununda da gerekli hassasiyeti gösterdiklerini ifade eden Gürses, "Böyle durumlarda velinin cep telefonuna kısa mesaj gönderiyoruz. Öğrencilerimizin güvenli bir şekilde eğitim hayatlarını sürdürmeleri bizim için önemli" dedi."*

## *Kartlı Sistemler*

Kartlı Sistemler, giriş kontrolü yapılmak istenen yerlerde her türlü personel giriş/çıkış, personel ziyaretçi giriş kontrol ve denetinin yapılmasını sağlar. Aynı zamanda personel devam kontrol sistemleri (PDKS) ile uyumlu olacak şekilde çeşitli fabrikalar, hastaneler, okullar gibi pekçok bina giriş sistemlerinde kullanılabilmektedir. Kartlı sistemlerde ana öğe kartın kendisidir. Günümüzde, mifare kart, yakınlık kartı, plastik kart gibi kartlar çeşitli sistemlerde yaygın olarak kullanılmaktadır.

Genel olarak akıllı kart olarak isimlendirilen kartlardan olan mifare kartlar, içinde yazılım yüklü olan elektronik çipli kartlardır. Tüm donanım, mifare kartın içine gömülü olarak yerleştirildiğinden diğer manyetik araçlardan ya da su dökülmesi veya güneşe maruz kalma gibi koşullardan etkilenmemektedir. Mifare karttaki bilgiler çalınamamakta ve kopyalanamamaktadır. Dolayısıyla bilgilerin bozulması da mümkün değildir ve güvenlik yüksek düzeyde sağlanmaktadır.

Yakınlık (proximity) kartlar, çoğunlukla çalışanların belli alanlara erişimlerini sınırlandırmak amaçlarıyla kullanılan kartlardır. Bu kartları da bir çeşit akıllı kart olarak isimlendirmek mümkündür. Yakınlık kartlarda geçiş izinleri dışında kişilerin kimlik bilgileri, sigorta numaraları gibi isteğe bağlı ekstra bilgiler de yer alabilmektedir. Yakınlık kartlar bu bilgileri yaptıkları işlemle birlikte saat ve tarih belirterek ana bilgisayara gönderebilmektedir.

Plastik kartlar ise, kişi bilgilerinin manyetik bantlar içerisinde yer aldığı, daha basit düzeyde güvenlik sistemlerinde kullanılan kartlardır. Daha çok alışveriş mağazalarında kullanılan, yapılan her alışveriş sonrası bir takım puanların biriktiği, bazı dönemlerde karta özel avantajların olabildiği sistemlerde kullanılan kartlardandır. Plastik kart sistemleri sıklıkla bilgisayar teknolojisini kullanan ve geniş veritabanına sahip olan sistemlerde kullanılmaktadır.

Günümüzde yaygın olaran kullanılan kartlı sistemleri, bağımlı kartlı sistemler ve bağımsız kartlı sistemler olmak üzere ikiye ayırmak mümkündür.

Bağımsız kartlı sistemler; herhangi bir bilgisayar ya da ekstra bir kontrol ünitesi olmadan kendi başına çalışan sistemlerdir. Bir kart okuyucu, tuş takımı ya da yakınlık okuyucuya, elektrikli bir kilit sisteminin kumanda edilebilmesi esasına dayanarak çalışmaktadır. Bu tür sistemler çoğunlukla yüksek güvenlik gerektirmeyen giriş noktalarında sadece kart veya şifre sahibi olan kişilerin giriş/çıkış hareketlerinin sağlanması amacıyla kullanılmaktadır. Sonraki aşamada bir bilgisayar ekranından izlenmeyen sistemlerdir.


**Resim 3.4:** Öncelikli (Proximity) Kart ve Kartlı Sistem Örneği

Bağımlı kartlı sistemler; bir bilgisayara bağlı olarak çalışan sistemlerdir. Kartlı giriş sistemi ile kontrol altına alınan kapı, bariyer veya turnike gibi giriş ünitesine yakınlık kartları okuyabilen okuyucuların monte edilmesi ile çalışmaktadır. Bu okuyucular sistemin ana kontrolünü sağlayan bir ana kontrol kartı üzerine yerleştirilmiştir. Ana kontrol kartı, bilgisayar ile doğrudan bağlantı kurabilmekte ve bilgisayar üzerinde gelen komutları kilitlere, okuyuculara ve kullanılan diğer donanımlara iletmektedir. Bu sistemin bağımsız durumlu sistemlerden en önemli farkı, kişilerin giriş/çıkış kontrollerinin yanında geliş gidiş saatleri, işe geç kalınıp kalınmadığı, bina içinde personelin konumu gibi birçok özellik bilgisayar yazılımı vasıtasıyla kaydedilebilmektedir. Hatta herhangi bir yangın durumunda sistem eğer yangın alarm sistemi ile entegre edilmişse bütün kapı kilitlerinin açılmasını da sağlayabilmektedir.


**Resim 3.5:** Farklı Kartlı Sistem örnekleri

Kartlı sistemlerin günümüzde yaygın olarak kullanımına örnek olarak Akşam Gazetesi'nin 17.11.2011 günkü haberi verilebilir. İlgili haber:

> *"Son yıllarda yaşanan istihbarat sızmaları Genelkurmay Başkanlığı'nı harekete geçirdi. Karargâh, bu girişimlere karşı önlemlerini en üst düzeye çıkardı. 'Kozmik oda', 'Harekât ve İstihbarat Merkezi' gibi yüksek güvenliğin gerektirdiği birimlerde özel güvenlik kalkanı devreye girdi. Görevli personel, bu alanlara ancak 'parmak izi, göz ve yüz tanıma' sistemi ile geçiş yapabiliyor. Türkiye genelinde bulunan 14 kozmik odanın tüm güvenlik kriterleri yenilendi. Ana karargâh başta olmak üzere kuvvet, ordu ve kolordu komutanlıklarında personelin bir başka birime geçişini sınırlandıran 'akıllı kart' uygulaması başlatıldı. Bu sisteme göre karargâh içindeki bir personelin, rütbesi ne olursa olsun kartı yetkili değilse bir başka birime geçiş yapmasımümkün değil. O personelin ilgili birime geçişi ancak kartının yetkilendirilmesi ile sağlanıyor.*
>
> *Sistem Genelkurmay ve MSB binalarının yer aldığı ana karargâhta uygulanıyor. Ana karargâhta 'akıllı kart' uygulaması ile sadece Genelkurmay Başkanı Org. Necdet Özel, Genelkurmay İkinci Başkanı Org. Hulusi Akar, korgeneral rütbesindeki 'J başkanları', Genelkurmay Genel Sekreteri, generaller ve stratejik birimlerde çalışan subayların 'tam yetkilendirilmiş' geçiş kartı bulunuyor. Aynı güvenlik önlemi ana karargâhtaki nizamiyeler için de uygulanıyor. Personelin hangi nizamiyeleri kullanacağı, misafirlerini hangi nizamiyelerden alacağı da belirlendi. Üst düzey subay da olsa bir personel ancak geçiş izni olan nizamiyeyi kullanabiliyor."*

## *Biyometrik Sistemler*

İnsan vücüdunda davranışlarında kimliğini ele verebilecek birçok detay bulunmaktadır. Biyometrik Sistemler, bu detaylara bakarak karşısındaki kişinin gerçekten istenen kişi olduğunu anlamaya çalışmaktadır. Bu detaylardan bazılarını aşağıdaki şekilde sıralamak mümkündür.

- **Parmak İzi**: Parmakların üzerinde yer alan izler olup, kişiye özgü bir özelliğe sahiptir.
- **Dinamik İmza**: Sadece imzanın şekli değil, kalemin hangi noktalardan daha hızlı geçtiği veya kalem ucunun nerelerde daha çok basınç uyguladığı sezilebilmektedir.

- **Yüz Geometrisi**: Yüzün tanımına veya burun, dudak, göz gibi belli bir bölümüne bakılarak kişinin kimliği doğrulanabilmektedir.
- **İris Tanıma**: Gözdeki iris tabakasının ortaya koyduğu şeklin, tamamen kişiye özgü oluşu prensibine dayanmaktadır.
- **Retina Analizi**: Gözün retina tabakasındaki toplardamarların haritasının çıkarılması vasıtasıyla kimlik doğrulamasının yapılmasıdır.
- **El ve Parmak Geometrisi**: El ve parmakların duruşuna ve geometrisine bakarak değerlendirme yapılmasıdır.
- **El Damar Analizi**: El üzerindeki toplardamarların haritasının çıkarılmasına dayanarak kimlik doğrulamasının yapılmasıdır.
- **Kulak Formu**: Kulağın görünen kısmının formunu analiz ederek, sesin sahibinin doğru kişi olup olmadığının kontrol edilmesidir.
- **Ses Analizi**: Ses tonu ve tınısını analiz ederek, sesin sahibinin doğru kişi olup olmadığının kontol edilmesidir.
- **DNA Analizi**: Kullanıcının genetik kompozisyonunu analiz ederek kimlik doğrulamasının yapılmasıdır.
- **Tuş Vuruşları**: Klavye üzerindeki tuşlara vuruş hızının ve temposunun kişiye özgü bir karakter yaratması ve bu tuş vuruşlarına dayanarak kimlik doğrulamasının yapılmasıdır.

Biyometrik Sistemler, günümüz teknolojisinde sürekli kendini geliştiren sistemlerdendir. Bu sistemler gelişen yüksek teknolojinin ışığında yapılan araştırmalar sonucu insan bedeninde bulunan taklit edilemez unsurlar ile dijital cihazların çalıştığı bir yapı olarak tasarlanmıştır. Bu cihazların ortaya çıkmasındaki en büyük etken, *"nasıl daha güvenli ve anti müdahalesi en az olan bir kontrol yapısı oluşturabiliriz?"* olmuştur. İnsan odaklı bu olan bu sistemlerin günümüz güvenlik teknolojileri içerisinde en yaygın olanlarını şu şekilde sıralayabiliriz:

- Parmak izi tanıma
- Avuç içi, el üstü damar tanıma
- İris, retina tanıma
- Yüz tanıma
- Ses tanıma
- Çok modelli biyometri

Bu sıraladığımız teknolojiler içerisindeki son maddede belirtilen çok modelli biyometrik sistemlerin anlamı, farklı biyometrik sistemleri bir arada yani birden fazla biyometrik sistem çeşitini birlikte kullanmaktır. Örnek verecek olursak, parmak izi, insan nüfusunun yaklaşık %10 luk bir kısmında aşınmış, yaralanma, tahriş veya tanınamaz durumdadır. Böyle bir durumda sistemin sadece parmak izi odaklı olması bir takım sıkıntıları beraberinde getirecek olup, sadece parmak izine bakmaksızın, yüz tanıma sistemiyle birlikte birleştirilmiş bir çok-modelli biyometrik sistem daha güvenli geçiş sağlanmasını mümkün kılabilmektedir.

Biyometrik Sistemleri, diğer güvenlik sistemlerinden ayıran en önemli özelliklerini aşağıdaki şekilde sıralamak münkündür:

- **Benzersizlik**: Biyometrik sistemler bireylerin kendilerine özgü özellikleri etrafında geliştirilmiştir. İki kişinin aynı biyometrik veriyi paylaşım oranı hemen hemen sıfırdır.

- **Paylaşılamazlık**: Biyometrik özellik bireyin içsel bir özelliği olduğundan yinelenmesi veya paylaşılması mümkün değildir. (Yüzünüzü veya elinizin bir kopyasını başkasına veremezsiniz.)
- **Kopyalanamazlık**: Günümüz teknolojisi ile biyometrik özelliklerin tespiti sadece canlı bireyler üzerinden olmaktadır. Sahtesinin taklit edilmesi mümkün değildir.
- **Kayıp edilemezlik**: Bir bireyin biyometrik özelliği sadece ciddi bir kaza durumunda kaybedilebilir.

Hürriyet gazetesinin 19 Temmuz 2009 tarihinde yayınlanan sayısında Nilgün Karataş'ın Güvenlik Endüstrisi Sanayi ve İşadamları Derneği Başkanı İbrahim Uzelli ile yaptığı röportajın makalesinde, günümüzde parmak izi okuyan sistemlerin çok yaygın olarak kullanılmasına karşın, kopyalanma riski bulunduğuna dikkat çekilmiş, insanların birbirine benzemeyen parmak damar yapısının çok daha güvenli bir sistem olarak görüldüğü belirtilmiştir. Aynı zamanda, özel bir alıcı sayesinde parmak damar tanıması yapılabildiği, bunun ATM'lerde, bilgisayarda kullanımının mümkün olduğu belirtilmiştir.

Biyometrik sistemlerin çalışma aşamalarını kayıt ve tanıma aşaması olarak ikiye ayırmak mümkündür. Sistem, karakteristik biyometrik özelliği içeren bir veritabanına (kayıtlı bilgiler) dayanmaktadır. Veritabanı ya merkezidir ya da manyetik kartlar üzerine işlenerek dağıtılmıştır. Kayıt aşamasında biyometrik karakteristik veritabanına eklenir. Cihaz tarafından taranarak kişinin biyometrik unsur, kompakt ve belirgin dijital temsili oluşturulmaktadır. Buna şablon (template) denir. Şablon veritabanına kaydedilir.

Tanıma aşamasında ise, sistem erişim noktasındaki kişinin biyometrik özelliği alınır ve şablon ile karşılaştırılır. Tarama sonucu ile optimize edilmiş dijital temsilin eşleşme sonucuna göre kişi, ya kabul edilir ya da reddedilir. Sistemin genel performansı, depolama, hız ve eşleştirmedeki doğruluk payı ile belirlenir. Ayrıca mevcut şablona göre, cihazın veriyi tarama zamanı da belirleyici unsurlardandır. Şablonun boyutu büyük olduğu takdirde, tarama ve eşleştirme süresi buna bağlı olarak uzayacaktır.

Aşağıda biyometrik temelli sistemlerden bazılarının fotoğraflarını görebilirsiniz.

**Resim 3.6:** Parmak İzi Okuma, Yüz Tanıma ve İris Tanıma Sistemleri Örnekleri

Güvenlik gereksinimlerinin en üst düzeyde olması gereken kurum ve kuruluşlarda, biyometrik sistemlerin kullanımı gün geçtikçe artmaktadır. Akşam gazetesinin 17.11.2011 tarihli haberinde Genelkurmay Başkanlığı'nda alınan güvenlik tedbirlerindeki radikal değişim şu şekilde anlatılmıştır:

> *"Türk Silahlı Kuvvetleri istihbarat sızmalarına karşı teknolojik kalkan oluşturdu. 14 kozmik odanın tüm güvenlik kriterleri yenilendi. Genelkurmay, istihbarat sızmalarına karşı teknolojik kalkan oluşturdu. Türkiye genelinde bulunan 14 kozmik odanın tüm güvenlik kriterleri yenilendi. Bu alanlara artık 'parmak izi, göz ve yüz tanıma' sistemi ile geçiş yapılabiliyor. 4 aylık çalışma sonrasında binin üzerindeki tanıma, yeni kod ve şifre getirilirken, kozmik oda personelinin görev tanımı 'gizli'den 'gizli gizli'ye yükseltildi. Bu kurullarda görevyapan TSK personelinin kozmik büro görev talimatnamesi yeniden*

*belirlendi. Olası savaş, kriz ve doğal afet durumunda devlet büyüklerinden işadamlarına kadar önemli isimlerin nerede ve nasıl korunacağına dair planlar güncellendi."*

Biyometrik sistemleri daha ayrıntılı olarak, kitabın 6. ünitesi içerisinde "Biyometrik Temelli Güvenlik Sistemleri" başlığı altında inceliyebilirsiniz.

## Eşya Kontrol Sistemleri

### *Dedektörlü Sistemler*

Tehlikeli cisimlerin yoğunluğunu tespit eden, sesli ve ışıklı uyarı veren cihazlardır. Çoğunlukla hava alanları, alışveriş merkezleri, otogarlar, hastaneler, okullar, kamu kurum ve kuruluşları, belediyeler, iş merkezleri, fabrikalar, spor tesisleri gibi fazla sayıda insanın giriş çıkış yapabilecekleri binaların girişlerinde kullanılan sistemlerdir. Giriş yapan kişinin üzerinde taşıdığı eşyaların çeşitli istenmeyen maddelerin kontrolünün yapıldığı bu sistemleri kendi içinde ikiye ayırmak mümkündür.

- El Dedektörleri
- Kapı Dedektörleri

El dedektörleri, bir şahıs kontrolünde, genellikle girişi yapılacak binanın güvenlik görevlisi kontrolünde kullanılmaktadır. Bilinen metal dedektörleri ile aynı şekilde çalışmaktadır. Kontrolü yapılacak kişinin üzerinde kullanılırken, kontrol edilen bölgeye paralel şekilde tutulmalıdır. El dedektörleri, kapı dedektörlerine göre, kontrol edilen kişinin vücudunda metal bulunan bölgeyi tam olarak işaretlemesi açısından daha avantajlıdır. Aynı zamanda, elle yapılan aramalar, insanlar arasında daha az tepkiyle karşılanmakta ve caydırıcı etkisi daha yüksek olmaktadır.


**Resim 3.7:** El Dedektörü

Kontrol kutusu, elektronik sinyal, pil ve mikroişlemciden oluşan el dedektörleri, gönderdiği titreşimlerin geri dönüş süresini ölçerek çalışmaktadır. Alternatifi olan X-Işını cihazları gibi radyasyon yaymadıkları için kullanım alanları oldukça fazladır.

Hassasiyeti için üzerinden ayar yapılabilen bu cihazlarda, bozuk para, küpe, anahtarlık ve kemer tokası gibi günlük kullanımdaki metallere karşı duyarsız hale getirilebilmekte ve bu sayede girişlerin yoğun olduğu binalarda kuyrukların oluşması engellenebilmektedir.


**El dedektörü, kontrol yapılacak şahsın vücuduna 2.5 cm ile 7.5 cm arasında bir mesafede tutulmalı ve kişinin baş kısmına tutulmamalıdır.**

Kapı dedektörleri ise bina girişlerinin yoğun olduğu yerlerde, insan hareketliliğini aksatmadan güvenlik seviyesini arttıran sistemlerdir. Tehlikeli cisimlerin metal yoğunluğunu tespit eden bu cihazlar, sesli ve ışıklı olarak güvenlik görevlisine uyarı vermekte ve aynı zamanda giriş yapan kişi sayısını ekranda göstermektedir. El dedektörlerinde olduğu gibi kapı dedektörlerinde de hassasiyet ayarı ayarlanabilmekte, bozuk para, küpe, kemer tokası ve anahtarlık gibi insanın üzerinde genel olarak bulunabilecek metallere karşı sinyal vermesi engellenebilmektedir.

**Resim 3.8:** Kapı Dedektörü

Herhangi bir binaya giriş yapan kişilerin tek tek aranması yerine bu işlemi saniyeler içerisinde geçekleştiren kapı dedektörleri, zamandan olduğu kadar kullanılacak personelin sayısını azaltarak maliyetten de tasarruf sağlamaktadır. Binanın girişinin yapıldığı kontrol noktalarında kullanılan bu sistemlerde, kişilerin bir sıra ile geçiş yapılması istenmektedir. Sırada bekleyen kişilerin en az 1.5m geride beklemesi gerekmektedir. Kapı dedektörlü sistemler, ortalama dakikada 50-60 kişinin giriş yapabileceği şekilde hassas tarama yapmaktadır.

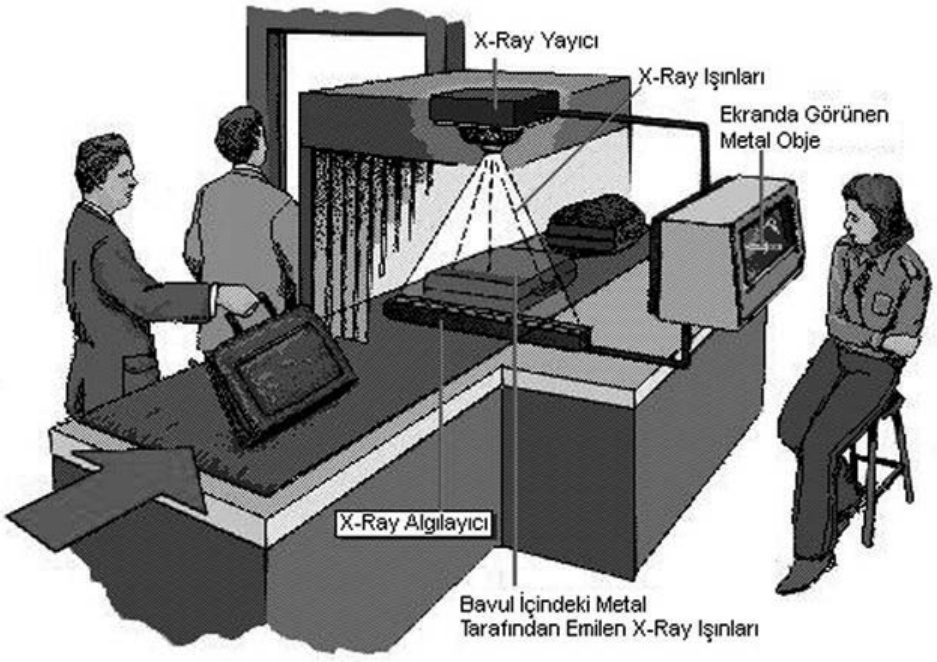
## *X-Işını Sistemler*

Bina girişinde, kişinin eşyalarının kontrolünün yapıldığı sistemlerden olan X-Işını sistemleri de dedektörlü sistemlerde olduğu gibi yaygın olarak kullanılan sistemlerdendir. Genellikle dedektörlü sistemlerle paralel olarak kullanılmaktadır. Hava alanlarında, toplu taşıma işlerinin yapıldığı alanlarda yaygın olarak kullanılmaktadır. Bina girişi sırasında, kişilerin üzerinin taranması kısmı dedektörlü sistemler tarafından yapılırken kişilerin üzerinde bulunan, çanta, bavul gibi eşyaların içlerinin sadece metal araması değil, silah, bomba gibi tehlikeli malzemelerin bulunmasında kullanılan sistemlerdir. Fiziksel aramaya göre dört kat hızlı olup, kişilerin özel eşyalarının halkın içinde kontrol edilmemesini sağlar.

X-Işını cihazı, farklı modelleri olmakla birlikte genel olarak, kontrol edilen çantaya X ışık dalgaları gönderir, geriye zayıf dönen X ışık dalgaları dedektör filtresinden geçirilir. Güçlü olan 2. dalga X ışınları 2. detektöre ulaşır. Makine bu iki dedektörden aldığı verileri ekrana yansıtarak içindeki organik, inorganik ve metal objelerin ekranda görünmesini sağlar.

Monitörü gözden geçiren güvenlik elemanının mutlaka eğitimli olması ve hangi renklerin hangi nesneleri temsil ettiğini iyi bilmesi gerekmektedir. Bazı güvenlik kontrollerinde sadece bıçak, silah gibi belirgin objeler değil, aynı zamanda, birleştirildikleri zaman bir patlayıcıya dönüştürülebilecek objeleri güvenlik elemanı tespit edebilecek kapasitede olmalıdır.

Özellikle X-Işını cihazı konusunda havaalanlarında yaşanan bir başka sorun ise, yolcuların filmlerini, kasetlerini, silinebilecekleri gerekçesiyle X-Işını cihazı içine bırakmak istememeleridir. Artık günümüzde üretilen tüm güvenlik amaçlı X-Işını cihazları *"film safe"* yani, filmler için güvenli olarak imal edilmektedir. X-Işını cihazı içinde bulunan radyasyon, filmleri etkileyecek kadar yüksek düzeyde değildir.




**Resim 3.9:** X-Işını (X-Ray) Sistemi Yapısı

Dizüstü bilgisayarlar gibi elektronik cihazlar, genellikle çok küçük parçalardan oluştuğu için X-Işını cihazından geçmiş olsalar bile, içerisine bir bombanın parçalarının yerleştirilip yerleştirilmediğini kontrol etmek amacıyla güvenlik görevlileri tarafından, cihazı açmanız ve çalıştırmanız istenebilir. Ancak çalışan bir dizüstü bilgisayar içine bile bir bomba yerleştirmek mümkün olduğundan, özellikle yüksek güvenlikli bölgelerde kimyasal maddeleri algılayan cihazlar da kullanılmaktadır.

Oldukça düşük miktarda radyasyon yayan güvenlik amaçlı X-Işını cihazları etrafında bulunmak, sağlık açısından herhangi bir sorun yaratmamaktadır. Piyasada, farklı özelliklerde ve ölçülerde bulunan X-Işını cihazı fiyatları, kullanılan özelliklere, hassasiyetine, çalışma hızına, vb. etmenlere göre farklılık göstermektedir.

Röntgen cihazlarında kullanılan donanım X-Işını cihazlarında da aynıdır. X-Işını $10^8$ ile $10^{12}$ cm'lik kısa dalga boylu elektromanyetik ışınlardır. Bu cihazların kullanımında, kullanan personel ve yolcular bir televizyondan daha az miktarda radyasyona maruz kalmalarına rağmen, çalışanlara dozimetre kullanmaları önerilmektedir. Cihazın tünelinin etrafında, cihazdan çıkan radyasyonu önlemek için kurşun levhalar, giriş ve çıkışlarda da boşluk bırakmayacak şekilde kurşun viril perdeler bulunmaktadır. Ancak ne olursa olsun kontrol edilen eşyaların cihaza giriş ve çıkışları esnasında, perdelerin arasından bir miktar radyasyon çıkışı insan sağlığı açısından tehlike arz etmektedir. Dozimetre kullanımı genellikle zorunlu tutulmaktadır. Dozimetre veya radyakmetre olarak isimlendirilen cihaz, maruz kalınan radyasyon miktarını ölçmektedir. Radyasyonun vücut üzerindeki ölçüsü rem veya milirem birimleriyle gösterilmektedir.


**Bir saatte alınan 600 rem öldürücüdür.**

X-Işını sistemlerin günümüzde güvenlik tedbirlerini arttırıcı etken olduğuna dair, Kocaeli Büyükşehir Belediyesine ait olan kaçırılan deniz otobüsü olayının ardından, İDO'nun aldığı önlemleri içeren 15.11.2011 gününe ait Bölge Gazetesi'nin şu haberi X-Işını sistemlerinin önemini bir kere daha göz önüne getirmektedir:

*"Geçtiğimiz günlerde yasadışı bölücü örgüt tarafından kaçırılan Kocaeli Büyükşehir Belediyesi'ne ait Kartepe Deniz Otobüsü'nün ardından gözler İDO'ya çevrildi. Kaçırıldıktan sonra güvenlik güçleri tarafından etkisiz hale getirilen ve üzerinde patlayıcı çıkan teröristin güvenlik cihazlarından rahatlıkla geçmesi ise güvenlik zaafiyeti olarak dikkat çeken unsur.*

*Birçok vatandaş tarafından ulaşım olarak tercih edilen İDO'nun ise deniz otobüslerine binişlerde güvenlik çemberini genişlettiği ve yolcuların ellerinde bulunan en ufak poşetleri bile cihazlardan geçirdiği son günlerde görülmekte. X-Ray cihazlardan geçen vatandaşlarda sıkı bir arama yapan ve en ufak bir olumsuzlukta eskisinden daha özen ile korunan İDO'nu' bu uygulamasından en çok yine vatandaş memnun olmakta."*

Burada anlatılan X-Işını sisteminin detaylarını kitabın 4. ünitesi olan "X-Işını Cihazları" başlığı altında daha ayrıntılı olarak inceleyebilirsiniz.

# ARAÇ GİRİŞ KONTROL SİSTEMLERİ

Giriş kontrol sistemleri altında bu başlık içerisinde, giriş yapacak kişinin araçla birlikte giriş yaptığı zamanlarda kullanılacak olan sistemler anlatılmaktadır. Sistemin ana merkezi araç odaklı olduğu için, araca özel olan belirleyici unsurlar belirlenerek veya araç üzerine bir takım elektronik sistemlerin yerleştirilmesiyle oluşan sistemler kullanılmaktadır. Araç giriş kontrol sistemlerinde araç, bariyere yaklaşırken aracın bilgisi sistem tarafından çok kısa bir sürede alınır ve değerlendirilir, araç geçiş yetkisine sahipse, bilgisayar sistemi, bariyere açma sinyalini gönderir ve bariyerin açılarak aracın geçişine izin verilir. Yapılan işlem, tarih, saat ve giriş kapısı bilgisiyle birlikte kaydedilir ve gerektiğinde raporlanabilir.

Sistemler, kamu ve özel sektör kuruluşlarında, konut sitelerinde, üniversitelerde, limanlarda, özel otoparklarda askeri tesislerde yaygın olarak kullanılmaktadır. Sistemler on-line (uygulandığı anda) veya off-line (sonradan kaydedilebilir) olarak kullanılabilir, kart sahiplerine zaman ve kapılar bazında yetkiler verilebilir, hangi kapıdan hangi araçların hangi tarih ve saatlerde geçiş yapabileceği sistemde tanımlanabilir. İstendiği takdirde sisteme bilgisayar bağlanabilir ve eğer yetkiye sahipse, on-line olarak sistem bilgilerine erişilebilir, giriş çıkış raporları alınabilir ve sistem yönetilebilir.

Girişin güvenli ve hızlı yapılması önem arzetmektedir. Araç giriş kontrol sistemlerini iki gruba ayırmak mümkündür:

- Radyo Frekanslı Tanıma Sistemleri (RFID Sistemler)
- Araç Plaka Tanıma Sistemleri

## Radyo Frekanslı Tanıma Sistemleri (RFID Sistemler)

İlk olarak 1940'lı yıllara dayanan RFID sistemler; İngilizce açılımı *"Radio Frequency Identification"* kelimelerinin kısaltmasından oluşmaktadır. Türkçe ifade ile *"Radyo Frekanslı Tanımla"*; nesneleri radyo dalgaları ile tanımlamak için kullanılan teknolojilere verilen genel isimdir. Bir RFID sistem, etiketler (elektronik bilgi çipleri), etiket okuyucular, anten ve uygulama yazılımı ve bilgilerin depolandığı veritabanından oluşmaktadır. Etiket tarafından gönderilen veri, kimlik, konum bilgisi gibi çeşitli verilerden oluşabilmektedir. Okuyucu, alıcı anteni yoluyla etiketin göndermiş olduğu veriyi alır, haberleşme için geliştirilmiş yazılımı kullanarak veriyi işler ve işlenen veri depolamak üzere veritabanına kaydeder. Okuyucu ve etiket arasında bu haberleşme anında bazen çarpışmalar (çakışmalar) gerçekleşebilmektedir. Bu çarpışmaları gidermek için, çarpışma önleyici algoritmalar RFID sistemlerde yaygın olarak kullanılmaktadır.

RFID sistemlerinde temel olarak, RFID etiketi ve RFID okuyucusu en kritik bileşenlerdir. RFID etiketi, üç çeşitten oluşmaktadır:

- Pasif (etkisiz)
- Yarı pasif (yarı etkin)
- Aktif (etkin)

**Resim 3.10:** RFID Sistem örneği

En ucuz etiket çeşidi olan pasif etiketler, kendi güç kaynakları olmayan, okuyucunun gücüyle çalışan etiketlerdir. Yarı pasif etiketler ise, gelen sinyalden güç almaya gerek bırakmayacak kadar küçük bir pil bulunduran etiketlerdir. Daha geniş okunma alanına sahip bu etiketler, daha güvenilir oldukları gibi, okuyucuya daha çabuk cevap verebilirler.

Aktif etiketler ise, diğer çeşitlerinden farklı olarak devrelerini çalıştırmalarını ve cevap sinyali üretmelerini sağlayan kendi güç kaynaklarına sahiptirler. Bu özellikleri ile yüksek performans sergilerler ancak maliyetleri de diğerlerinden daha yüksektir.

Aslında tipik bir RFID etiketinin okunma mesafesi birçok etkene bağlıdır. Operasyonun sıklığı, okuyucunun gücü, diğer RF araçlarıyla çakışması vs. bu etkenler arasında sayılabilir. Genelde düşük frekanslı etiketler 0,33 m ve daha az uzaklıktan okutulabilir. Yüksek frekanslı etiketler 1 m'den, UHF olarak bilinen daha yüksek frekanslı etiketler ise 3-7 metreden okunabilmektedir.

**Resim 3.11:** RFID Etiket örnekleri

RFID sistemlerde en önemli konulardan biri de frekans bantlarıdır. RFID, düşük frekans (LF) 125–134 kHz, yüksek frekans (HF) 13.56 MHz, ultra yüksek frekans (UHF) 860–960 MHz, 2.45 GHz ve süper yüksek frekans (SHF) 5,8 GHz frekanslarında kullanılabilmektedir. Her ülke kendi radyo frekans kullanımını düzenlemektedir. Bu standart RFID'nin 865 - 868 MHz frekans bandında, *"Söylemeden Dinle"* (LBT) protokolü ile 2 Watt'a varan güç seviyeleri ile kullanılmasını öngörmektedir. Bu standart pek çok Avrupa ülkesinde kabul edilmiş ve yerel düzenlemelere yerleştirilmiştir. Türkiye'de ise, 06.03.2004 tarihli ve 25394 sayılı Resmi Gazetede yayınlanan *"Kısa Mesafe Erişimli Telsiz Cihazlarının (KET) Kurma ve Kullanma Esasları Hakkındaki Yönetmelik"* uyarınca, RFID sistemleri 865,6 - 867,6 MHz frekans bandında maksimum 500mW (0.5W) güç seviyesi ile uygulanabilmesi onaylanmıştır. Daha

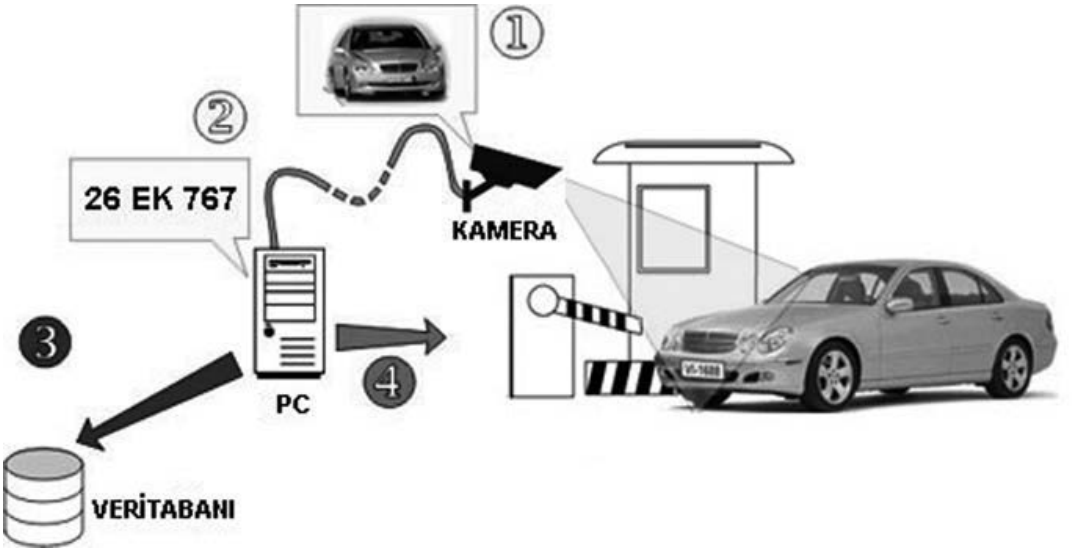
sonra 16 Mart 2007 tarihli Resmi Gazete'de yayınlanan yeni KET yönetmeliği ile 865,6-867,6 MHz. bandı arasında kullanım gücü 2 Watt olarak yenilenmiş ve Avrupa standartlarına çekilmiştir.

Bir RFID sistem uygulaması yapılacaksa, öncelikle uygulamanın yapılacağı ülkenin izin verdiği frekans seçenekleri belirlenmelidir. Frekans belirlendikten sonra, ne kadarlık bir okuma mesafesinin olacağı öncelikli kriterlerden biridir. Sonraki aşamada ise, etiket çeşiti yani pasif, yarı pasif veya aktif mi olacağı belirlenerek sistem tasarlanmalıdır.

**SIRA SİZDE 1 Yaşadığınız şehirde bulunan büyük bir alışveriş merkezine gittiğinizi düşünün. Geçtiğiniz giriş kontrol sistemlerini gözlemleyiniz.**

## Araç Plaka Tanıma Sistemleri

Plaka tanıma sistemleri, araç üzerinde bulunan plakayı dijital yöntemlerle okuyarak araçları tanımlamaktadır. Aracın plakası, bu amaca özel bir plaka tanıma kamerasıyla okunmakta ve elde edilen görüntüler sayısallaştırılarak bilgisayar ortamında ilgili yazılım vasıtasıyla işlenmektedir. Yine bilgisayar ortamında bulunan veritabanı içerisinde, okunan plakanın giriş yetkisinin olup olmadığına bakılarak geçiş kapılarına yetkilendirme yapılarak aracın geçişi sağlanmaktadır. Resim 3.12'de sistemin çalışma şekli gösterilmektedir.




**Resim 3.12:** Araç Plaka Tanıma Sistemi ve çalışma adımları

Sistemin donanım boyutunda kameraların önemi büyüktür. Gece karanlık ortamlarda da aynı gündüz koşulları gibi çalışmaya devam etmesi için, kızıl ötesi özelliklere sahip kameralar da kullanılabilmektedir. Aynı zamanda, yazılım ortamında kullanılan dijital filtreler sayesinde sistem, gece-gündüz, yaz-kış ve farklı ışık koşullarında da sorunsuz çalışabilmektedir. Araç plaka tanıma sistemleri günümüzde birçok ortamda kullanılmaktadır. Otoyollardaki araçların hız kontrolünün yapılması, köprü geçiş kotrolünde kullanılan sistemler gibi örneklerde araç durağan bir konumda değil, hareketli pozisyonda olmaktadır. Böyle durumlarda kullanılan kameraların kalitesi, plaka tanıma yazılımının çalışma performansı açısından oldukça önemlidir. Bu konu başlığı altında incelediğimiz sistemde, araç durağan pozisyonda olacağı için sistemin başarımı çok daha yüksek olmaktadır.

**İNTERNET Plaka tanıma sistemleri ile ilgili olarak daha ayrıntılı bilgi almak için http://tr.wikipedia.org/wiki/Otomatik_plaka_tanıma adresini ziyaret edebilirsiniz.**

Bina giriş kontrol sistemleri altında incelenen araç giriş kontrolünü sağlayan sistemin ana bileşenlerini şu şekilde sıralamak mümkündür:

- Yüksek çözünürlüklü, düşük ışık hassasiyetli plaka tanıma sistemine özel kızıl ötesi aydınlatmalı kamera
- Video yakalama donanımı ve elektronik kontrol sistemi
- Plaka tanıma yazılımı
- Bilgilerin depolandığı veritabanı

Son yıllarda bilim ve teknoloji alanlarındaki çalışmalar daha yüksek kalitede algoritmalar ve donanımların geliştirilmesine olanak sağlamış, plaka tanıma sistemlerini daha yaygın kullanılır hale getirmiştir. Sistemin yazılımı aşağıdakilere benzer zorluklarla başa çıkabilmelidir:

- Uzaklık ve/veya kameraya bağlı düşük resim çözünürlüğü
- Kamera odaklanma problemleri, bulanıklık
- Ortamın aydınlığı, düşük zıtlık, gölgeler
- Görüntünün örneğin çamur sebebi ile engellenmesi
- Değişik yazı stilleri
- Aldatıcı ve kanun dışı plakaları ayırdedebilme
- Ülkeye bağlı olarak benzer plakaları ayırtedilebilme
- Tüm bu işlemleri uygulamada kabul edilebilir bir karmaşıklıkta yapma


**"Araç Plaka Tanıma Sistemleri" günümüzde pek çok alanda kullanılmaktadır. Giriş kontrol sistemleri haricinde nerelerde kullanıldığını araştırınız.**

Takvim gazetesinin 16 Eylül 2011 tarihli şu haberi, plaka tanıma sistemlerinin günümüzde farklı alanlarda kullanımınını göz önüne getirmektedir:

> *"Terörle mücadelede yeni bir dönem başlatan Hükümet, bölge halkını rahatlatmaya devam ediyor. Bu kapsamda Doğu ve Güneydoğu'da güvenlik için yapılan yol kontrolleri artık tarih oluyor... Yıllardır süren uygulama yerine 'plaka tanıma sistemi' devreye girecek. Türkiye'de ilk kez Hakkâri'de denenecek sistemle aranan veya istihbarat kapsamında 'şüpheli' listesinde yer alan araçların plakaları, mobese sistemine işlenecek. Kontrol noktasına gelen araç eğer sistemde kayıtlıysa, mobese kameraları uyarı vererek güvenlik ekiplerini uyaracak. Bu şekilde artık sadece şüpheli araçlara 'dur' denilecek. Sistemde kaydı bulunmayan bir araçla ilgili ihbar ve ya anlık istihbarat gelmesi halinde ise araç durdurulacak ve gerekli işlemeler yapılabilecek. Plaka tanıma sistemiyle aranan veya şüpheli araçlar dışında vatandaş hiç bir şekilde durdurulmayacak."*

Anadolu Ajansı'nın 01.11.2011 tarihli haberinde ise Kastamonu'nun İlçe Jandarma Komutanlığı girişine Plaka Tanıma Sistemli güvenlik sisteminin kurulduğuna dair haberde, şüpheli araç tespitini hızlı ve kolay bir şekilde yapıldığı anlatılmıştır. İlgili haber:

> *"Kastamonu'nun Çatalzeytin İlçe Jandarma Komutanlığı önüne Plaka Tanıma Sistemi (PTS) kuruldu. Aselsan tarafından "Jevus projesi" kapsamında geliştirilen PTS'nin amacının güzergâhtan geçen sisteme kayıtlı olan şüpheli araçların tespit edilmesi olduğu öğrenildi. Jandarma Genel Komutanlığı veri tabanında kayıtlı olan araçların tamamının kontrol altında olacağı sistem ile trafikte seyir halinde bulunan araçların çalıntı olup olmadığı, herhangi bir suça karışıp karışmadıkları, tescil, muayene ve ceza gibi durumlarını araçlar trafikte durdurulmadan tespit edilebilecek. Sistemin montaj işlerinde görevli olan Aselsan teknisyeni Serdar Kahvecioğlu'nun verdiği bilgiye göre sistem 14 metreden saniyede 40 fotoğraf çekebilecek teknolojik donanıma sahip."*

## Özet

Bu ünitede “Elektronik Güvenlik Sistemleri” başlığı altında bulunan “Bina Giriş Kontrol Sistemleri”, iki alt başlık altında ayrıntılı olarak anlatılmıştır. İlk olarak turnikeli, kartlı ve biyometrik sistemler ile dedektörlü ve X-Işını sistemleri “Kişi Giriş Kontrol Sistemleri olarak anlatılmıştı. RFID ve araç plaka tanıma sistemleri ise “Araç Giriş Kontrol Sistemleri” olarak ele alınmıştır. Öncelikle bir Bina Giriş Kontrol Sistemi’nin belirlenmesinde binaya en uygun güvenlik sisteminin seçilebilmesi için yapılması gereken bir dizi tespit ve değerlendirme çalışmasının yapılması oldukça önemlidir. Bu konu kitabın ilk bölümünde ayrıntıları ile anlatılmıştı. Aynı zamanda sistemin diğer elektronik güvenlik sistemleri ile uyumlu olacak şekilde çalışabilmesi de bir diğer önemli unsurlardandır.

Turnikeli sistemler, diğer güvenlik sistemleri ile iç içe kullanılması ve pratik olup yerleşiminin kolay olması yönleriyle yaygın olarak kullanılan sistemlerdendir. Kartlı sistemler, personel devam kontrol sistemleriyle uyumlu olabilmesi yönüyle ve çeşitliliğiyle oldukça fazla kullanım alanına sahiptirler.

Biyometrik sistemler ise yüksek derecede güvenlik gerektiren yerlerde, benzersizliğiyle, paylaşılamaz oluşuyla, kopyalanamazlığıyla ve kayıp edilemez oluşuyla tercih edilebilmektedir.

İnsanlar giriş yaparken üzerlerinde istenmeyen maddeleri yanlarında taşıyabilmektedirler. Bu tür durumlarda ise “Eşya Kontrol Sistemleri” devreye girmektedir. Dedektörlü sistemler, caydırıcılık etkisinin yüksek oluşuyla ve alternatifi olan X-Işını sistemlere göre radyasyon yaymadığı için kullanım alanları oldukça fazladır.

X-Işını sistemler, dedektörlü sistemler ile birlikte kişilerin üzerindeki eşyaların ayrı, kişilerin ayrı taranması amacıyla etkin olarak kullanılmaktadır. Fiziksel aramaya göre dört kat daha hızlı olması ve özel eşyaların açılıp kontrol edilmesi gibi durumları ortadan kaldırması sayesinde hava alanları gibi girişlerin yoğun olarak yapılan yerlerde yaygın olarak kullanılmaktadır.

Araç girişlerinin kontrol edildiği, araç odaklı sistemler ise Radyo Frekanslı Tanıma Sistemleri (RFID Sistemler) ve Araç Plaka Tanıma Sistemleri olarak ikiye ayrılmaktadır. Arka planda bilgisayara bağlı olan bu iki sistemde de bariyerli kapı istenilen aracın girişini yapmasını sağlamaktadır.

RFID sistemde pasif, yarı pasif ve aktif olmak üzere üç farklı etiket (elektronik bilgi çipi) çeşiti vardır. Etiketin üzerinde güç kaynağı olmayan pasif etikette sistem okuyucunun gücüyle çalışmaktadır. Yarı pasif ve aktif olan etiketlerde, kendine has bir güç kaynağı bulunması okuyucuya daha çabuk cevap verebilmektedirler. Aktif etiketlerde ise, kendi devrelerini çalıştırmasının yanında cevap sinyali üretmelerini sağlayan kendi güç kaynaklarının bulunması sayesinde yüksek performans sergileyebilmektedirler. Tabiki bu yüksek performans diğer etiketlere oranla daha fazla bir maliyet gerektirmektedir.

Etiket ile okuyucu arasındaki radyo frekansı, sistemin çalıştığı ülkenin izin verdiği frekans ölçülerinde olmalıdır.

Araç üzerinde herhangi bir ekstra elektronik sistem yerleştirilmeksizin sadece araçta standart olarak bulunan plakanın kamera vasıtasıyla dijital yöntemlerle okunmasına dayanan sistemleri “Araç Plaka Tanıma Sistemleri” başlığı altında toplamak mümkündür.

Bariyerin, sadece giriş yetkisi olan araçlara karşı açılması sağlanmaktadır. Araç Plaka Tanıma Sistemleri, kamera, video yakalama donanımı ve elektronik kontrol sistemi, plaka okuma yazılımı ve bilgilerin depolandığı veritabanından oluşmaktadır. Sistem, ortamın aydınlığı, kameranın kalitesi, plaka üzerindeki çamur vs. etkenler, aldatıcı ve kanun dışı plakaların kullanımı gibi bir takım zorluklarla karşılaşabilmektedir. Otoyollardaki araçların hız kontrolünün yapılması, köprü geçiş kotrolünde kullanılan sistemler gibi örneklerde araç durağan bir konumda değil, hareketli pozisyonda olmaktadır. Böyle durumlarda kullanılan kameraların kalitesi, plaka tanıma yazılımının çalışma performansı açısından oldukça önemlidir.

Bilim ve teknolojideki gelişmelerle birlikte, sistemin algoritmasının da gelişmesi sayesinde bu tip zorlukların üstesinden gelebilmesi sağlanabilmektedir.

## Kendimizi Sınayalım

**1.** Bir binaya en uygun giriş kontrol sisteminin belirlenmesi için aşağıdaki maddelerden hangisinin yapılmasına ihtiyaç duyulmamaktadır?

a. Bina analiz edilmeli, izleme ve raporlama gereksinimleri belirlenmelidir.

b. Uygulanacak güvenlik tedbiri belirlenmelidir.

c. Sistemin binadaki diğer güvenlik sistemleri ile uyumu için gereksinimler belirlenmelidir.

d. Güvenlik senaryoları tartışılmalı, herhangi bir uyumsuzluk oluşuyorsa, giderilecek çözümler belirlenmelidir.

e. Güvenlik görevlileri ile toplantı yapılarak nöbet değişimleri belirlenmelidir.

**2.** Yemekhane binasına kurulması gereken en uygun giriş kontrol sistemi aşağıdakilerden hangisidir?

a. Boy Turnike

b. VIP Turnike

c. Kartlı Turnike

d. El Dedektörlü Sistem

e. Kapı Dedektörlü Sistem

**3.** Aşağıdaki biyometrik sistemlerden hangisi doğruluk açısından en güvenilirdir?

a. Parmak İzi Tanıma

b. Avuç İçi Tanıma

c. Ses Tanıma

d. İris Tanıma

e. Çok Modelli Biyometri

**4.** Aşağıdakilerden hangisi biyometrik sistemlerin özelliklerinden değildir?

a. Benzersiz olması

b. Paylaşılamaz olması

c. Kayıp edilemez olması

d. Bozulamaz olması

e. Kopyalanamaz olması

**5.** Kapı dedektörleri ile el dedektörleri arasında bir tercih yapılacak olursa, aşağıdaki durumların hangisinde el dedektörleri tercih edilebilir?

a. Sesli uyarı verme durumunda

b. Işıklı uyarı verme durumunda

c. Bir güvenlik görevlisi kontrolüne bağlı olma durumunda

d. Problemli bölgeyi tam olarak işaretlemesi durumunda

e. Fazla insan geçişi olması durumunda

**6.** Aşağıdaki sistemlerden hangileri birlikte kullanılırsa güvenlik açısından en uygun örnek olur?

a. Jetonlu Turnike – Yüz Tanıma

b. VIP Turnike – Ses Tanıma

c. Kapı Dedektörü – X-Işını Sistem

d. El Dedektörü – Kapı Dedektörü

e. El Dedektörü – Parmak İzli Turnike

**7.** Alışveriş yapılan mağazalarda müşterilere verilen kartlar aşağıdaki kart çeşitlerinden hangisidir?

a. Kredi Kartı

b. Telefon Kartı

c. Yakınlık Kartı

d. Mifare Kart

e. Plastik Kart

**8.** Aşağıdaki giriş kontrol sistemlerinin hangisinde kamera kullanılması şarttır?

a. Dedektörlü Sistem

b. RFID Sistem

c. Kartlı Sistem

d. Turnikeli Sistem

e. Araç Plaka Tanıma Sistemi

**9.** Aşağıdaki Giriş Kontrol Sistemlerinin hangisinde bilgisayar yazılımına ihtiyaç yoktur?

a. Araç Plaka Tanıma Sistemi

b. El Dedektörlü Sistem

c. Biyometrik Sistem

d. Yüz Tanıma Sistemi

e. Bağımlı Kartlı Sistem

**10.** Aşağıdakilerden hangisi Araç Plaka Tanıma Sistemlerinin karşılaşabileceği zorluklardan biri değildir?

a. Aracın cinsinin tespiti

b. Değişik yazı stilleri

c. Uzaklık

d. Düşük Resim Çözünürlüğü

e. Ortamın aydınlığı, gölgeler

## Kendimizi Sınayalım Yanıt Anahtarı

**1. e** Yanıtınız yanlış ise "Giriş" başlıklı konuyu yeniden gözden geçiriniz.

**2. c** Yanıtınız yanlış ise "Turnikeli Sistemler" başlıklı konuyu yeniden gözden geçiriniz.

**3. e** Yanıtınız yanlış ise "Biyometrik Sistemler" başlıklı konuyu yeniden gözden geçiriniz.

**4. d** Yanıtınız yanlış ise "Biyometrik Sistemler" başlıklı konuyu yeniden gözden geçiriniz.

**5. d** Yanıtınız yanlış ise "Dedektörlü Sistemler" başlıklı konuyu yeniden gözden geçiriniz.

**6. c** Yanıtınız yanlış ise "Kişi Giriş Kontrol Sistemleri" başlıklı konuyu yeniden gözden geçiriniz.

**7. e** Yanıtınız yanlış ise "Kartlı Sistemler" başlıklı konuyu yeniden gözden geçiriniz.

**8. e** Yanıtınız yanlış ise "Araç Plaka Tanıma Sistemleri" başlıklı konuyu yeniden gözden geçiriniz.

**9. b** Yanıtınız yanlış ise "Dedektörlü Sistemler" başlıklı konuyu yeniden gözden geçiriniz.

**10. a** Yanıtınız yanlış ise "Araç Plaka Tanıma Sistemleri" başlıklı konuyu yeniden gözden geçiriniz.

## Sıra Sizde Yanıt Anahtarı

### *Sıra Sizde 1*

Alışveriş merkezlerinde en sık karşılaşılan giriş kontrol sistemleri X-Işını cihazı, kapı dedektörleri ve el detektörleridir. Bazı alışveriş merkezlerinin kapılarında turnikeler de bulunmaktadır.

### *Sıra Sizde 2*

Araç plaka tanıma sistemleri gününüzde birçok ortamda kullanılmaktadır. Otoyollardaki araçların hız kontrolünün yapılması, köprü geçiş kotrolü gibi hareketli araçlar için de kullanılmaktadır.

## Yararlanılan Kaynaklar

Pearson, R.L. (2007). **Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions**, Butterworth-Heinemann, Elsevier.

## Yararlanılan İnternet Kaynakları

http://www.resmigazete.gov.tr

http://en.wikipedia.org

http://www.cacsecurity.com/

http://www.perkotek.com

http://www.guvenlikkamerasistemleri.org

http://www.aktifzaman.com.tr

http://www.dtksoft.com

http://www.guvenlikdanismanlik.com

http://www.onikibilgi.com

http://hurarsiv.hurriyet.com.tr

http://www.senkronguvenlik.com.tr

http://www.voles.com.tr

http://www.eec.com.tr

http://www.guvenliksistemleri.gen.tr

http://www.teta.com.tr/

http://www.biometricnewsportal.com

http://www.kontrolsis.com

http://www.emrealtun.com/

http://www.aa.com.tr/

http://www.takvim.com.tr

http://www.bolge.com.tr

# 4

## Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- X-Işını cihazı ve çalışma prensibini anlatabilecek,
- X-Işını cihazları çeşitlerini ve kullanım alanlarını özetleyebilecek,
- X-Işını cihazlarının kullanımında dikkat edilmesi gereken noktaları açıklayabilecek,
- X-Işını cihazlardaki radyasyon ve bundan korunma yollarını örnekleyebilecek

bilgi ve becerilere sahip olabilirsiniz.

## Anahtar Kavramlar

- Röntgen
- X-Işını
- Elektro manyetik spektrum
- Backscatter (Geri yansıma)
- Radyasyon
- Film, Termolüminans ve Yüzük Dozimetreler
- T.A.E.K.

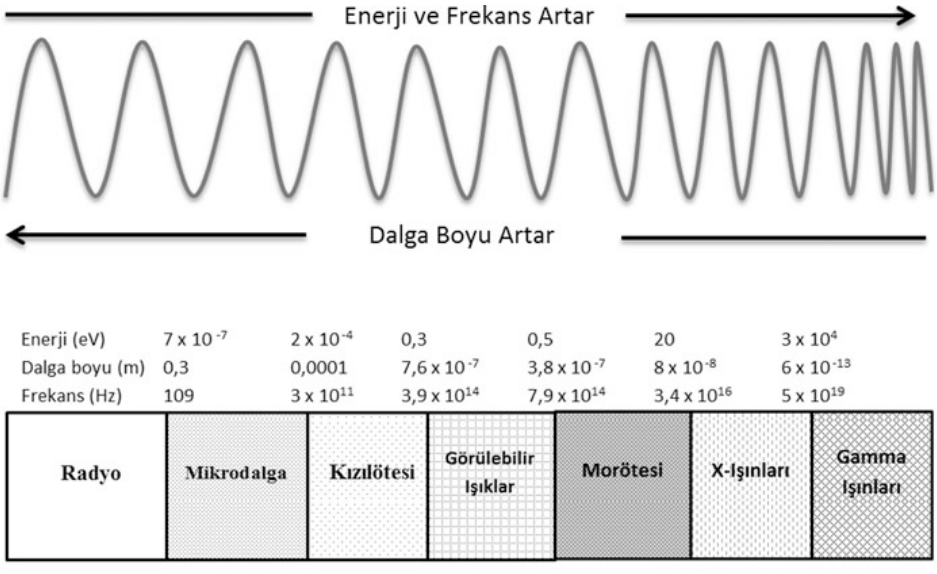
## İçindekiler

# X-Işını Cihazları

## GİRİŞ

Güvenlik sistemlerinin önemli bir parçası da X-Işını cihazlarıdır. Güvenlik hizmetlerinin yerine getirilebilmesi için aramalarda oluşabilecek rahatsızlıkların en aza indirilmesinde X-Işını cihazları kullanılmaktadır. Bu araçlar sayesinde uyuşturucu, silah, patlayıcı veya patlayıcı düzenekleri v.b. gibi suç teşkil edebilecek maddelerin tespiti kolaylıkla mümkün olmaktadır.

Alman bilim adamı Wilhem Conrad Röntgen tarafından bir deney sırasında varlığı tesadüfen keşfedilen bu ışınlar, İngilizce'de tanımlanamayan nesneler için kullanılan X öneki ile kullanılmış ve X-Işını olarak isimlendirilmiştir. X-Işınları gözle görülmeyen ancak son derece delici olan salınımlı sinyallerdir. Düşük dalga boylu, yüksek frekanslı bu ışınlar radyoaktif özellik taşımaktadır.




**Resim 4.1:** Elektromanyetik Spektrum.

Elektromanyetik spektrum, ışınların dalgaboyu, enerji ve frekanslarına göre sıralandığı bir görüntü dizisidir. Burada radyo dalgalarının frekansı, sırasıyla mikrodalga, kızılötesi, görülebilir ışıklar, morötesi, X ışınları ve Gamma ışınlarından düşük ancak buna karşılık dalga boyu büyüktür. X-Işını ya da Röntgen ışını gözle görülen ışığın dalgaboyundan küçüktür. Aynı zamanda bu ışın, elektronları ve atomik çekirdekleri saptırdığından, tıbbi amaçlı ve moleküllerin tam yapılarının araştırılması için 20.yy'nin başlarından beri kullanılmaktadır. Görülebilir ışıkların bulunduğu frekans aralığı dışında kalan diğer ışınlar insan gözüyle görülememekte olup etkileri farklı şekillerde hissedilmektedir.

# X-IŞINI VE X-IŞINI CİHAZLARININ ÇALIŞMA ŞEKLİ

Alman fizikçi Wilhelm Conrad Röntgen, laboratuvarında Hittrof-Crookes tüpü adı verilen, bir pompa yardımıyla içindeki hava basıncı atmosferik basıncın milyonda birine düşürülmüş, iki ucunda anot ve katot metalleri bulunan tüpün iki ucuna akım kaynağı bağladığında yeşil renkte bir floresan ışığı elde etmiştir. 8 Kasım 1895 günü Hittrof-Crookes tüpü ile çalışırken masanın üzerindeki "baryum platinosiyanür" kristallerinin floresan ışıdığını fark etmiştir. Devam eden çalışmaları sonucunda floresan ışımasına tüpten ekrana doğru düzgün bir yol izleyen fakat görünmeyen bir ışınımın neden olduğu sonucuna varmıştır. Bu ışın bugünkü adıyla bilinmeyen ışın manasında X-Işını olarak tarihe geçmiştir.

Günümüzde X-Işını tabanlı cihazlar kaynak olarak X-Işını tüplerini kullanmaktadır. Temelde X-Işını tüpü vakum ortamına alınmış anot ve katot gerilimleri altında, katot tarafında kaynak flaman ve anot tarafında hedef metalden oluşmaktadır. Anot katot gerilimi kilovolt mertebesinde büyük bir gerilimdir. Flamandan akan elektronlar yüksek gerilim altında hedef metale doğru hızlandırılarak çarptırılır. Bu büyük çarpışmadan dolayı elektronların enerjisinin büyük bölümü ısıya dönüşmekle birlikte bir kısmı da bugün birçok alanda kullandığımız X ışınlarına (röntgen ışınları) dönüşür. Bu ışınlar da yararlanılmak istenen alanlarda farklı enerji düzeylerinde üretilerek güvenlik sistemlerinde, tıpta ve endüstrinin birçok kolunda kullanılmaktadır.

Hedef metal olarak atom numarası büyük olan ve erime sıcaklığı yüksek olan Tungsten elementi kullanılır. Üretilen X ışınlarının şiddeti, kilovolt cinsinden elektriksel değeri ve uygulama süresine göre değişmektedir. Gerilim değeri arttırıldığında ışınların gönderildiği maddenin üzerine etkisi daha yoğun olmaktadır.

X-Işını cihazları; insan, nesne ya da araçların sabit bir X-Işını kaynağından geçirilmesi sonucunda içeriği hakkında bilgi veren cihazlardır. Bu cihazlarda bir X-Işın kaynağı ve bunun karşısında gönderilen ışınları algılayan dedektörler bulunmaktadır. İnsan, nesne ya da araçlardan geçen ışınlar foto-diyot denilen dedektörler yardımıyla algılanarak görüntülenebilmektedir.

X-Işınları Wilhelm Conrad Röntgen tarafından keşfedildikten sonra çok farklı alanlarda kullanıla gelmiştir. Bunlardan bazılarını aşağıdaki gibi sıralayabiliriz:

1. Tıpta teşhis ve tedavi aracı olarak kullanılmaktadır. Radyoskopi ve radyografi gibi işlemlerde X-Işınlarından elde edilen düşük dalga boylu sert ışınlarından yararlanılmaktadır. Aynı şekilde farklı işlemler sonucunda elde edilen X-Işınları kanser tedavisinde ve bazı tıbbi operasyonlarda da kullanılmaktadır.
2. Maddenin yapısı, örneğin kristal yapısı ve organik maddelerin moleküler yapısının incelenmesinde sıklıkla kullanılan bir araçtır.
3. Teknik olarak malzeme kontrollerinde, örneğin bir maddenin içeriğinin araştırılmasında içerisinde hava boşluğu olup olmamasında, yapım hatalarının saptanmasında kullanılmaktadır.
4. Kimyasal maddelerin içerisindeki az miktarda bulunan maddelerin analizinde kullanılmaktadır.
5. Fizikte yeni elementlerin incelenmesinde kullanılmaktadır.
6. Güvenlik açısından kişilerin, eşyaların ya da araçların içerisinde gizlenmiş yabancı maddelerin (uyuşturucu, silah, patlayıcı veya patlayıcı düzenekleri) tespitinde sıklıkla kullanılmaktadır.

Dedektörlerin elde ettiği sinyaller çeşitli filtreleme işlemlerinden sonra görüntü işleme teknikleri yardımıyla dilim görüntüler oluşturulmakta, elde edilen bu dilim görüntüler ise sonradan birleştirilerek nesnelerin içeriğinin bir görüntüsü elde edilmektedir.

**Resim 4.2:** X-Işını Cihazı

X-Işınlı güvenlik kontrol sistemleri ilk kullanılmaya başlandığında siyah beyaz görüntü verebilen basit cihazlardı. Bu cihazlardan sadece malzemenin, çantanın içindekilerin fiziksel şekli hakkında bilgi alınabilmekteydi. Daha sonraları elde edilen bu görüntüler yeterli olmayınca, 90'lı yılların başlarında üreticiler tarama alanı içerisindeki nesnelerin kimyasal yapısı hakkında da bilgi verebilecek yani onların organik ya da inorganik maddeler olup olmadıklarının belirlenebileceği teknikler üzerinde çalışıp kullanıcılara bu bilgileri verebilecek çok enerjili sistemler geliştirdiler. Bu sistemler, oluşturulan görüntü üzerinde operatörlerin madde tanımlamasını kolaylaştırıcı bazı uygulamaları içermektedir. Bu tanımlamada malzemelere renk kodlaması uygulanmakta, örneğin titanyum, krom, demir, çelik, kalay, kurşun, bakır, gümüş, altın gibi atom numarası 18'den büyük olan ağır elementler (inorganik maddeler) mavi renklendirme ile alüminyum gibi atom numarası 10 ile 18 arasında olan orta ağırlıktaki elementler (karışık grup) yeşil renklendirme ile ve atom numaraları 10'un altında olan hidrojen, karbon, nitrojen, oksijen, nitrogliserin, akril, kağıt, tekstil ürünleri, tahta ve su gibi organik maddeler de turuncu ile görünmektedir.

2000'li yıllara doğru ise bu cihazlarda daha büyük gelişmeler yaşanmaya başlanmıştır. Yeni gelişmeler sonucunda X-Işını cihazları, güvenlik operatörlerine çantaların şüpheli olup olmadığı hakkında karar vermesinde yardımcı olmaya yarayan ve görüntüler üzerine şüpheli olabilecek bölgeleri işaretleyen sistemler ile birlikte daha verimli hale gelmişlerdir.

Havaalanlarında kullanılan X-Işını cihazları genel olarak çift enerjili X-Işını sistemleridir. Bu sistemlerde 140-160 kilovolt tepe (KVP) aralığında X-Işını gönderen tek bir kaynak bulunur. KVP ölçü birimi X-Işınının maddelere nüfuz etme (penetrasyon) miktarını ifade eder. KVP oranı arttıkça taranan maddeye nüfuz eden X-Işını miktarı artar.

X-Işınları taranan cisim üzerinden geçtikten sonra bir dedektör tarafından toplanır. Dedektörde toplanan düşük enerjili X-Işınları bir filtre yardımıyla engellenir. Geriye kalan yüksek enerjili X-Işınları ikinci bir detektöre çarptırılılmaktadır. Düşük enerjili yani organik nesneler, bilgisayar devresi yardımıyla karşılaştırmalı olarak diğer nesnelerden ayrıştırılır ve bu şekilde tespitleri mümkün olur. Farklı malzemeler farklı seviyelerde X-Işınlarını emdiğinden, X-Işını cihazı güvenlik görevlileri tarafından kullanıldığında onlara çanta, valiz ya da kişilerin üzerindeki nesneleri ayırt edebilme imkânı sunar. Bu ögeler genellikle nesnelerden geçen ışının vermiş olduğu farklı tepkilere göre 3 ana kategoriye göre renklendirilirler. Bu kategoriler şunlardır:

1. Organik
2. İnorganik (Organik olmayan)
3. Metal

X-Işını cihazı üreticileri tarafından inorganik ve metal nesneleri belirtmek için kullanılan renkler farklılık gösterseler de, hepsinde organik neslerin temsili için turuncu tonları kullanılmaktadır. Bunun en önemli nedeni patlayıcı maddelerin çoğunlukla organik maddelerden yapılmasıdır. Cihaz operatörleri sadece silah, bıçak gibi şüpheli nesneleri ayırt etmek için değil, patlayıcı aygıt ya da maddeleri ayırt etmek için de eğitilmektedirler. Patlayıcı maddeler piyasada ticari olarak değil, terörist ya da eylemciler tarafından üretilen nesneler olup, boru tipi bomba, elektronik kontrollü bomba gibi farklı çeşitlerde olabilmektedir. Biçimsel olarak farklılık gösteren patlayıcı maddelerin bu yüzden tanınması ve tespiti son derece önemlidir.

Yaygın kanaatin aksine X-Işını cihazları film ve elektronik ortamlara zarar vermemektedir. Gerçekte tüm modern X-Işını cihazları film ve eletronik ortamlara zarar vermeyecek biçimde tasarlanmakdır. Bunun anlamı tarama cihazlarında gönderilen X-Işınının radyasyon miktarı fotoğrafik filmlere zarar vermeyecek kadar azdır. Diğer yandan elektronik ortamdaki bilgiler, fotoğrafik filme göre radyasyona daha dayanıklı olduklarından bu ışınlardan hiç etkilenmemektedirler. Ancak tomografi gibi bazı yüksek enerjili X-Işını cihazları fotoğrafik film materyallerine zarar vermektedir.

Dizüstü bilgisayarlar gibi elektronik aygıtların içerisine gizlenebilecek bombanın tespiti, göreceli olarak bir valize gizlenmiş bombanın tespitinden zor olabilmektedir. Bu yüzden kontroller esnasında görevliler, dizüstü ya da PDA gibi bilgisayarların çalıştırılmasını kişilerden isteyebilmektedirler. Bu aygıtların çalışıyor gibi gözükmesi bile güvenli olup olmadığının tespiti için yeterli olmayabilir. Bu nedenle birçok havaalanında “kimyasal dinleyici” olarak tabir edilen bir kutuya yerleştirilmiş otomatik kimyasal laboratuvarlar bulunmaktadır. Rastsal aralıklarla ya da şüpheli bir durumda elektronik aygıtın üzerinden bir bez yardımıyla örnek alınır ve kimyasal dinleyici tarafından bu örneğin analizi yapılarak bomba yapımında kullanılabilecek kimyasal kalıntı tespiti yapılmaya çalışılır. Herhangi bir kalıntıya rastlanılması halinde dinleyici güvenlik görevlilerini potansiyel bomba uyarısında bulunur.

**Resim 4.3:** Gelişmiş X-Işını cihazı içerisinde şüpheli nesneleri işaretlenmiş çanta görüntüsü.

**SIRA SİZDE 1** **Günlük yaşamda X-Işını cihazlarını nerelerde görüyorsunuz?**

**SIRA SİZDE 2** **X-Işını cihazlarının güvenilirliği hakkında ne düşünüyorsunuz?**

# X-IŞINI GÜVENLİK SİSTEMİ ÇEŞİTLERİ

Günümüzde çok farklı alanlarda kullanılan X-Işını güvenlik sistemleri taramanın yapıldığı nesnelere göre farklı sınıflara ayrılmıştır. Bunlar:

- İnsan Tarama Sistemleri
- Bagaj ve Paket Kontrolü Sistemleri
- Kargo ve Araç Kontrol Sistemleri
- El Bagajı Tarama Sistemleri

olarak dört farklı grubta değerlendirilebilir.

## İnsan Tarama Sistemleri

İnsan tarama sistemleri, hava limanları, alışveriş merkezleri, adliyeler, gümrükler, hapishaneler, deniz limanları, kamu binaları gibi çok farklı yerlerde kullanılmaktadır. Bu X-Işını tarama sistemlerine "geri-yansıma (backscatter)" sistemi denilmektedir. Çoğunlukla karşılıklı iki panel şeklinde olan bu sistemler insan üzerinde bulunan şüpheli cisimleri elle arama yapılmadan tespiti için kullanılmaktadır. Geri-yansıma cihazında taraması yapılan kişinin üzerinde gizlenmiş şüpheli bir cisme rastlanıldığında, sesli ve görüntülü olarak uyarı yapılmaktadır.

**Resim 4.4:** Geri-yansıma (backscatter) cihazı üzerinde insan vücudunun taranması işlemi.

Ayrıca bu sistemlerin, tıpkı bagaj taraması yapan cihazlarda olduğu gibi insan vücudunu monitörleyen çeşitleri de mevcuttur. Bu sistemlerde gizlenmiş nesneler yer olarak kolaylıkla tespit edilmektedir. Böylelikle tarama sonrası gizlenmiş olan nesnenin yerinin tespiti daha kolay olmaktadır. Geri-yansıma sistemleri, metal dedektör sistemlerine göre iyonlaştırıcı radyasyon kullandığından sağlık açısından daha az risk taşımakta ve tehdit algılamada daha güvenilir olmaktadırlar.

## Bagaj ve Paket Kontrolü Sistemleri

Günümüzde güvenlik sistemlerinde yoğunluklu olarak kullanılan X-Işını sistemleri ilk kullanılmaya başlandığı yıllarda insanlar tarafından tepkiyle karşılanmıştır. Özellikle 11 Eylül 2001'de A.B.D.'ye yapılan terör saldırıları ve ülkemizde yapılan terörist saldırılar neticesinde insanlar tarafından daha anlayışlı karşılanmaktadır. Aşağıdaki gazete haberi kişiler tarafından anlayışla karşılanmasına örnek olarak verilebilir:

> "*Sinagogların ardından İngiliz Konsolosluğu ve HSBC'ye yapılan bombalı saldırılar, şehrin her yerindeki güvenlik önlemlerini gözle görülür şekilde arttırdı.*
>
> *Özellikle Türkiye'nin dünyaya açılan kapısı olan Atatürk Hava Limanı'nın giriş alanlarındaki güvenlik önlemleri ve üst aramalar da daha titizlikle yapılmaya başlandı. Güvenlik görevlileri, daha patlamalar olmadan önce yolcuların özellikle üst aramalarına tepki gösterdiğini; ancak bugünlerde aramaları çok daha sıkı şekilde yapmalarına rağmen tepki bir yana destek gördüklerini söyledi.*
>
> *Sinagoglardaki patlamaların hemen ardından güvenlik önlemlerinin artırıldığı ilk yerlerden birisi Atatürk Hava Limanı oldu. Resmi ve özel yaklaşık iki bin 500 güvenlik görevlisinin görev yaptığı hava limanında, Levent ve Beyoğlu'ndaki son saldırılardan sonra önlemler daha da artırıldı. Bu arada, Çevik Kuvvet'e bağlı ekipler de özellikle Dış Hatlar Terminali girişlerinde görev almaya başladı.*
>
> *Görevli sayısı artırılırken, İç ve Dış Hatlar terminallerine girişler ve gümrüksüz sahalardaki aramalar da yoğunlaştırıldı. Daha önce yolcuların sıkı aramalara gösterdiği tepkilere alışkın olan güvenlik görevlileri ve polis, önlemlerin artırılmasıyla tepkinin de artacağını tahmin ederken, yolcuların tam tersi tavrı görevlileri hem şaşırttı hem de memnun etti. Yolcuların çantalarını X-Işını cihazından geçiren polis, bazı yolcuları daha yakın takibe alarak üzerindeki kıyafetleri, hatta ayakkabılarını bile çıkartmalarını istiyor. Güvenlik yetkilileri, eskiden bu tip uygulamalara tepki gösteren yolcuların, son saldırılardan sonra bu uygulamayı bile anlayışla karşıladığını, hatta aramaları daha da yoğunlaştırmalarını teşvik ettiğini belirtiyorlar.*" (Zaman, 30 Kasım 2003)

Yukarıdaki haberde de görüldüğü üzere, günümüzde artan tehditler karşısında X-Işını cihazlarının kullanımı son derece önem kazanmıştır. Hava alanları, bankalar ve önemli kamu binalarının girişlerinde yapılan paket ve bagaj aramaları güvenliğin vazgeçilmez bir unsuru haline gelmiştir. Bagaj ve paket kontrolü yapan sistemler mekânın niteliğine ve kullanım şekline göre imal edilirler.

Bu cihazlar genellikle, X-Işınlarının gönderildiği, algılandığı ve eşyaların konulduğu taşıyıcı bandın bulunduğu X-Işını ünitesi, aygıttan geçen paket veya bagajların içinin görüldüğü ekran ve aygıtı kontrol eden düğmelerin yer aldığı kontrol paneli olmak üzere üç ana bölümden oluşur.

Hareketli bir bant yardımıyla paket veya bagajlar X-Işını kaynağından geçirilir. Belirli bir hızla hareket eden bant, paket ya da bagajların içeriğinin monitörde görüntülenmesine olanak verir. Gerektiğinde güvenlik görevlisi tarafından sistem içerisinde paketler durdurularak yeniden bir tarama yapılabilir ve görüntünün netleştirilmesi sağlanabilir. Bant üzerinde paketlerin takılmasını engellemek için çoğunlukla tabanı düz plastik tepsiler kullanılır. Paketler bu tepsilerin içerisine yerleştirilerek, hareketli bantın üzerine konulmaktadır.

## Kargo ve Araç Kontrol Sistemleri

Güvenlik gerektiren havaalanları, gümrük kapıları, limanlar v.b. gibi nizamiyelerde kamyonların, deniz taşıtlarının, trenlerin ve konteynerlerin içlerinin açılmaksızın yabancı madde, kaçak yolcu, uyuşturucu, patlayıcı düzenek tespitinde kullanılan X-Işını cihazlarıdır.

Bu sistemlerin hareketli olanları da mevcuttur. Otoyollarda hareketli durumdaki araçların herhangi bir anda aranmasına olanak sağlayan bu cihazlar mobil cihazlara bütünleşmiş halde bulunabilmektedir. Araç ve kargo kontrol sistemleri düşük ve yüksek güçteki X-Işını jeneratörlü olmak üzere iki farklı türdedir:

Düşük güçlü X-Işını jeneratörü olan tarama cihazları ile küçük araçlar, binek araba, minibüs ve otobüs gibi araçlar taranmaktadır. Bu cihazların gönderdikleri X-Işınları 10 santimetreye kadar kalınlığı olan çeliği delebilmekte ve aranan araçların içeriği hakkında bilgi vermektedirler.

Yüksek güçlü X-Işını jeneratörlü cihazlarla konteyner, tır, vagon gibi araçlar taranabilmektedir. Bu cihazların gönderdikleri X-Işınları ise 50 santimetrelik kalınlığa sahip çeliğin içerisindeki madde ya da varlıklar hakkında bilgi vermektedir.

Özellikle ticari hareketliliğin yoğun olduğu gümrüklerde X-Işını cihazlarının kullanımı araçların ve gemilerin bekleme sürelerini azaltmaktadır. Bununla birlikte kaçakçılıkla mücadelede önemli başarılara elde edilmektedir. Aşağıdaki haber bu durumu özetleyen güzel bir örnektir.

**“*Limanlara Güvenlik Sistemi (Haber Ekspres, www.virahaber.com)***

*AB Katılım Öncesi Mali Yardım 2004 yılı programında başlayan Türk Gümrük İdaresi'nin Modernizasyonu - 2 Projesi kapsamında yatırımı tamamlanan İzmir, İstanbul Ambarlı, Mersin ve Samsun limanları ve Gürbulak Sınır Kapısı'ndaki Arama Hangarları ve Araç Konteyner Tarama (X-Işını) Sistemlerinin açılış töreni İzmir Limanı'nda yapıldı.*

*Devlet Bakanı ve Başbakan Yardımcısı Hayati Yazıcı, törende yaptığı konuşmada, Gümrük Birliği ile başlayan süreçte Türkiye'nin geçen yıl ihracatta Cumhuriyet tarihinin en yüksek rakamlarına ulaştığını, küresel pazarda söz sahibi olunması konusunda önemli bir kapının aralandığını söyledi. Hükümet olarak güven ve istikrarı tesis ederek Türkiye'yi uluslararası sermayenin cazibe merkezi haline getirdiklerini ifade eden Bakan Yazıcı, dünya ticaret hacminin de baş döndürücü hızla geliştiğine dikkati çekti. Küreselleşen olguların sadece ekonomi ve ticareti değil organize suçlar ve bundan beslenen uluslararası terörizm gibi konuları da gündeme getirdiğini anlatan Yazıcı, Gümrük İdaresi'nde yapılan modernizasyon projeleriyle kurumun, gümrükte bekleme süresi bakımından dünya ortalamalarının altında hizmet verir hale geldiğini kaydetti. Gümrüklerin idari kapasitelerinin artırılması konusunda AB ve Dünya Bankası başta olmak üzere uluslararası mali işbirliği projelerine büyük önem verdiklerini belirten Devlet Bakanı ve Başbakan Yardımcısı Yazıcı, şöyle konuştu: "Bu kapsamda kaçakçılıkla mücadele kapasitesinin geliştirilmesine yönelik modern teknolojiye dayanan X-Işını tarama sistemleri, nükleer madde detektörleri, uzaydan araç takip sistemleri, yüksek hızlı deniz botları gibi birçok güvenlik sistemi kullanımı artırılarak kaçak yakalama oranlarında Cumhuriyet tarihinin rekorları kırılmıştır. Bu hususların dünyanın hızlı değişen dinamiklerine tümüyle karşılık verdiğini söylemek tabii ki zordur. Bunun farkında olan Gümrük teşkilatımız başlattığı modernizasyon hamlesini sürdürecektir. Hükümetimiz ise bu hızlı değişim sürecini desteklemek amacıyla bu sene içinde AB müktesebatının bugün geldiği aşamadan hareketle hazırlanmış Gümrük Kanunu değişikliklerinin ve Gümrük Müsteşarlığı Teşkilatı Kanunu'nun yasalaşmasını sağlama konusunda kararlılık içindedir. Biz Türkiye'nin ufkunu açıyoruz, ülkeyi kısır çekişmelere çekecek tüm sabotajlara inat, Türkiye'yi dünyaya açıyoruz. Çünkü biz, içeride istikrar sağlandıkça dışarıda saygı görüyoruz. Hükümet olarak bunu görüyoruz ve önemsiyoruz." AB'ye giriş süreci Bakan Yazıcı, Avrupa Birliği'ni de bu açıdan son derece önemsediklerini belirterek, "Bizim insanımız bu standartlarda zenginlik ve özgürlüğü çoktan hak etmiş durumdadır. Gelinen bu noktada artık belki 'Türkiyesiz bir AB'nin anlamı nedir" sorusunun sorulması gerekiyor. Türkiye Maastricht ve Kopenhag kriterleri bağlamında önemli*

*açılımları gerçekleştirmiş, bu doğrultuda emin adımlarla yürümektedir" dedi. AB'nin bu açıdan Türkiye'yi değerlendirmesi gerektiğini, ilerde tam üye olunmasıyla Türkiye'nin doğu sınırının aynı zamanda AB'nin doğu sınırı olacağını kaydeden Bakan Yazıcı, "Biz bu vizyona göre adım atmaktayız. AB'nin de bu vizyonu bizimle paylaştığını projelerimize verdiği önemli katkılardan anlıyor ve teşekkür ediyoruz" diye konuştu.*

*Törene katılan Avrupa Komisyonu Türkiye Delegasyonu Başkanı Marc Pierini ise Gümrük Birliği sayesinde 12 yılda Türkiye ve AB arasındaki ticaret hacminin hızla arttığını ve Türkiye'nin tüm dünya ile olan ticaret hacminin yarısını oluşturduğunu ifade etti. Türkiye'nin AB ile ticaretindeki açığın ise toplam açığın yüzde 13'üne tekabül ettiğini kaydeden Pierini, bunun karşılıklı dengeli bir ticaretin olduğu anlamına geldiğini ifade etti. Gümrük Birliği sayesinde AB müktesebatı ile uyumun diğer alanlara göre çok daha yüksek olduğunu söyleyen Pierini, bunun giriş müzakereleri açısından önemli olduğunu belirterek, şöyle konuştu: "Tüm müzakereler yolunda gitmektedir. Tarama raporlarının çoğu tamamlanarak Türk yetkililere sunulmuştur. 6 fasıl açılmıştır. Slovenya'nın başkanlığı altında 2 tane daha açılması gerekiyor. En azından 2 tanesi de sonbaharda Fransa'nın başkanlığında açılacaktır. AB'ye giriş uzun ve zor bir süreçtir. Bu çok uzun bir yol, ancak biz müzakereleri başlatmak için oy birliğiyle bir karar verdik. AB ve Türkiye'deki politik sözler her iki taraftaki algılamaların istikrarını bozabilir. Çok aktif bir müzakere sürecimiz var. Müzakereler hiçbir şekilde askıya alınmamıştır. Türkiye veto edilmemiştir. Çok büyük bir heyecan yok ama müzakereler sürüyor. 35 faslın müzakere edilmesi, Kopenhag kriterlerinin yerine getirilmesi gerekiyor. Bu aynı zamanda ulusal politik tartışmayı da yansıtmaktadır. Son derece zor bir süreç bunu biliyoruz. Gittikçe uzamış, acı verici gibi görünüyor ama sürüyor." Türkiye'de üyelik öncesi programlar kapsamında 1.4 milyar avroluk aktif projelerin uygulandığını, buna bu yıl 540 milyon avronun ekleneceğini kaydeden Pierini, parasal konuların dışında Türkiye ve AB kardeş kuruluşları arası eşleştirme programlarının da aktif şekilde devam ettiğini kaydetti. Pierini, kendisinin bir liman kenti olan Marsilyalı olduğunu, limanları iyi tanıdığını ve uzun bir süredir İzmir Limanı gibi temiz ve düzgün bir liman görmediğini de sözlerine ekledi.*

*Gümrük Müsteşarı Emin Zararsız ise tamamlanan projeyle İzmir ile birlikte İstanbul Ambarlı, Mersin ve Samsun limanları ve Gürbulak Sınır Kapısı'na 5 adet araç ve konteyner tarama sistemi, İzmir ve Mersin limanlarına da arama hangarları yapıldığını, bugün hepsinin hizmete gireceğini ifade etti. Yatırımın yüzde 75'inin AB'nin sağladığı hibe kaynaklardan yararlanılarak yapıldığını kaydeden Zararsız, uygulanacak projelerin toplam bedelinin 76 milyon 449 bin avroya ulaştığını belirtti. Törende yapılan sunumda ise gümrüklerin modernizasyonu sonrası, 2002'de 343 kilogram olan eroin yakalama miktarının, 2007 yılında 2 bin 722 kiloya ulaştığı, bunun piyasa değerinin ise yaklaşık 155 milyon dolar olduğu belirtildi. Müsteşarlığın, çalışmalar kapsamında uzun vadede tüm kara ve deniz sınırlarının tarama sistemleriyle donatılması, hava limanlarının bagaj X-Işını sistemiyle donatılması ve büyük antrepolara koli ve paket tarama sistemlerinin konulmasını hedeflediği kaydedildi*."

Yine Karayolu ve Demiryolu ticari taşımacılığında duyulan güvenlik ihtiyacına karşılık vermek için Gümrük Müsteşarlığı Gümrükler Muhafaza Genel Müdürlüğü tarafından yürütülen bir çalışma ile ilgili aşağıdaki örnek dikkat çekicidir.

**"*Gümrüklerde Trenlere X-Işını Tarama (hürriyet.com.tr)***

*Gümrük Müsteşarlığının hazırladığı tren tarama sistemi projesi, Avrupa Birliği Komisyonu'nca kabul edildi. Van Kapıköy Sınır Kapısı'na kurulacak. Türkiye'nin ilk tren tarama sistemi, 5 milyon euroya mal olacak. Proje bedelinin % 75'ini AB karşılayacak. Hareket halindeki treni radyografi ışınlarıyla (X-Işını) tarayacak sistem, kaçak eşyaları tespit edecek.*

*Hareket halindeki treni radyografi ışınlarıyla tarayacak olan sistem, vagonlar ve yolcu bagajları içindeki kaçak eşyaların tespit edilmesini sağlayacak.*

*Gümrük Müsteşarlığı Gümrükler Muhafaza Genel Müdürlüğü tarafından 2000 yılında başlatılan ve Gümrük Güvenlik Sistemleri (GÜMSİS) olarak adlandırılan modernizasyon sürecinin bir devamı olarak 2008 AB Mali İşbirliği Programı kapsamında hazırlanan, "Türk Gümrük İdaresinin Modernizasyonu Projesi" AB Komisyonu tarafından kabul edildi. Proje kapsamında İran sınırındaki Van Kapıköy Sınır Kapısı'na Türkiye'nin ve bölgenin ilk tren tarama sistemi (X-Işını) kurulacak. AB ihale kurallarına uygun olarak satın alınacak tren X-Işını sistemi, yaklaşık 5 milyon avroya mal olacak. Proje bedelinin yüzde 75'i AB tarafından karşılanacak. Yetkililer, bu yılın sonuna doğru sistemin satın alınması için ihaleye çıkılacağını, önümüzdeki yılın başından itibaren ise kurulum çalışmalarına başlanacağını bildirdi.*

*Tren tarama sisteminin dünyada ABD, Finlandiya ve Çin'in de aralarında bulunduğu sayılı ülkede olduğunu belirten yetkililer, sistem sayesinde trenlerin sabit bir hızda giderken radyografi ışınlarıyla taranacağını, böylelikle vagonlar ve yolcu bagajları içindeki kaçak eşyaların tespit edilebileceğini kaydetti. Yetkililer, bagaj, kargo, araç ve konteyner tarama sistemlerine benzeyen tren tarama sistemlerinin, entegre edilen dedektörler vasıtasıyla aynı zamanda radyoaktif ve nükleer maddeleri de tespit edebileceğini vurguladı.*

*GÜMSİS Projesi çerçevesinde 2003 yılında üç adet X-Işını tarama sistemi alımı ile başlayan modernizasyon çalışmalarının sürdürüldüğünü ifade eden yetkililer, kara kapılarında ve limanlarda kurulan X-Işını sistemlerinin sayısının 2008 yılı sonu itibariyle 13'e ulaştığını bildirdi.*

*Cihazın gönderdiği radyografi ışınları, saatte 20-30 kilometre hızla hareket eden tren ve üzerindeki büyük hacimli kargolara nüfuz ederek, içeride bulunan her türlü eşyayı sistem odasındaki monitörlere yansıtacak. Bu sistem sayesinde yolcular da çok fazla bekletilmeyecek. Kapıköy Sınır Kapısı'na kurulacak sistem sayesinde başta uyuşturucu olmak üzere her türlü kaçak eşyanın Türkiye'ye sokulması önlenecek.*"

## El Bagajı Tarama Sistemleri

El bagajı tarama sistemleri hafif olması ve kompakt boyutlu olması nedeniyle tercih edilmektedir. Yüksek frekanslı anahtarlama teknolojisi ile taşınabilir X-Işını tarama sistemlerinden, taraması yapılacak olan cisimlerin kısa pozlama süreleri ile güvenilir sonuçlar alınabilmektedir. Bu tip sistemler genellikle; ışın üreten bir mekanizma, ışının yansıdığı bir panel ve içeriğin görüntülendiği bir ekrandan oluşmaktadır.

İçerisinde çoğunlukla bomba ya da patlayıcı madde olduğundan şüphelenilen çöp kutusu, çanta, zarf, kutu, uçak gövdesi ve kanatları ya da araç lastiği gibi diğer birçok cismin içeriğinin tespiti için kullanılan mobil tarama sistemleri günümüzde sıklıkla tercih edilmektedir. Sistemin sabit bir noktada değilde, güvenliği sorgulanacak her yere taşınabilir olması sistemin hafifliğini ön plana çıkartmaktadır.

Mağaza, alışveriş merkezi gibi noktalardan çok, emniyet teşkilatı ve bomba imha ekipleri bu cihazları tercih etmektedirler. Bu tür cihazların en önemli avantajı, taradığı cismin içeriğini, dizüstü bilgisayarlar yardımıyla kablosuz olarak görüntüleyebilmesidir.

**Resim 4.5:** Mobil El Bagajı ve Paket Tarama Sistemi.

SIRA SİZDE 3 **Mobil X-Işını tarama cihazlarının görüntüleme ekranının cihaza bütünleşik olarak kullanılmasının olumsuz etkileri neler olabilir?**

# X-IŞINI CİHAZ KULLANIMINDA DİKKAT EDİLMESİ GEREKEN KONULAR

X-Işını cihazlarını kullanacak operator güvenlik görevlileri aşağıdaki durumlara dikkat etmelidirler:

- Işınımdan korunma ve kazalardan korunma yöntemlerinin operatör tarafından iyi bilinmesi gerekir.
- Her türlü X-Işını cihazı, kesinlikle bu cihazın eğitimini almış kişiler tarafından kullanılmalıdır.
- Hareketli taşıma bandı üzerine hiç bir canlı oturtulmamalı ve cihaz çalışır durumda iken içerisinin kontrol ya da bakımı yapılmamalıdır. Tünelin önünde ya da arkasında bulunulmamalı, cihazın üzerine yiyecek ya da içecek bırakılmamalıdır.
- Taşıma bantlı bagaj-paket kontrol sistemlerinin operatörleri hiç bir zaman bol giyecek giymemeli; sarkan kravat, şal, fular, sarkan kolye gibi banta sıkışarak oluşabilecek kazaları önlemek için bu tip aksesuarlar takılmamalıdır. Ayrıca uzun saçlı operatörler saçlarını mutlaka toplamalıdır.
- Kontrol edilecek olan paket ya da çantalar X-Işını cihazının bant genişliğine uygun bir biçimde yerleştirilmelidir. Bant genişlikleri farklı farklı olan cihazlarda bu duruma özellikle dikkat edilmeli ve banda sokulacak paket veya bagajların arasına en az 50 santimetre mesafe konulmalıdır.
- Kontrol edilecek nesne, paket ya da bagaj içerisinde değilse (kemer, saat, dizüstü bilgisayar v.b.) mutlaka plastik kaplar içerisinde banta yerleştirilmelidir. Bagaj ya da paketlerin incelenmesi konusunda acele edilmemelidir.
- Görüntünün nitelendirilmesi ve analizi konusunda güçlük çekildiği durumlarda bagajın pozisyonu değiştirilerek bagaj cihazdan tekrar geçirilmelidir.
- Bagajın içerisindeki nesneler hakkında yine de kesin fikir sahibi olunamıyorsa, bu durumda, bagajın sahibine açtırılması ve kontrol edilmesi gerekir.
- Cihaz operatörlerinin maruz kalacağı radyasyonu ölçmeye yarayan “dozimetre” denilen cihazlar kullanılmalıdır. Bu cihazlar kişiye özel olmalı ve kesinlikle operatörler arasında

değişilmemelidir. X-Işını cihazının ve dozimetrelerin ölçümü ve bunların radyasyon kontrolleri Türkiye Atom Enerjisi Kurumu (T.A.E.K.) tarafından yapılarak sertifikalandırılmaktadır.

- Banta konulacak olan bagajlar ve ekranda incelenerek analizi yapılacak nesnelerin sırası, önce büyük sonra küçükler olacak şekilde olmalıdır.
- Havaalanı kontrollerinde operatörler özellikle; kemer, cep telefonu, dizüstü bilgisayar, saat, ayakkabı gibi eşyalar X-Işını ile taranmalıdır. Dizüstü bilgisayarların sahibi tarafından çalıştırılması gerekli durumlarda istenebilmektedir.

## X-Işını cihazları ve Radyasyon

X-Işını cihazlarının sağlık açısından güvenilirliği için, cihazların kalibrasyonunun, kalite kontrollerinin ve bakımlarının eksiksiz ve zamanında yapılması gerekir. Bu tip cihazların kurulum aşamasında genellikle, gerekli güvenlik kabul testleri yapıldıktan sonra, düzenli aralıklarla kalite güvence ve kalite kontrol testleri yapılmaktadır.

Kabul testi diye bilinen işlem, cihazın aranan teknik özellikleri sağlayıp sağlamadığının test edilmesi işlemidir. X-Işını cihazlarının teknik şartnamelerinde ölçülebilecek tüm parametreleri belirtilmiş olmalıdır. Özellikle her ünitenin radyasyon güvenliği yönünden denetimi yapılmalıdır.

Bagaj aramak için kullanılan cihazlarda kullanılan X-Işını radyoaktif özelliktedir. Ancak cihazın bulunduğu kutu içerisi özel kurşun kaplı olarak imal edilmiştir. Bu cihazların her ay periyodik kontrolleri yapıldığından ve kurşun kaplı olduklarından operatörler ve bagajları taramadan geçen insanlar doğrudan zarar görmezler. İnsanların aramaları ise dedektör kapılardan geçirilerek yapılmaktadır. Dedektörlerin, bu tip cihazlarda radyasyon kullanılmadığı için sağlık açısından bir sakıncası bulunmamaktadır. Ancak X-Işını cihazlarından geçen bavullarda yiyecek-içecek bulunması durumunda, her ne kadar radyasyon miktarları az da olsa sıklıkla yapılan aramalar sonrasında bu besinlerdeki radyasyon miktarı artar ve risk ortaya çıkmaktadır.

Radyasyonun insan vücuduna hangi miktarlarda zarar verebileceğini anlayabilmek için, öncelikle bir insanın yıllık radyasyon dozunun ne olabileceğini tespit etmek doğru olacaktır. Bunun için, doğal ve insanların meydana getirdiği radyasyon kaynaklarını incelemek gereklidir:

- **Kozmik Radyasyon**: Bu tip radyasyonlar dünyanın atmosferi tarafından büyük bir kısmı bloke edilen güneş ve diğer yıldızlardan dünyamıza gelen radyasyonlardır. Oksijen miktarının daha az olduğu yüksek irtifalarda bu radyasyon oranı deniz seviyesine göre daha fazladır. Deniz seviyesinde yılda 25 mikro rem radyasyon alınırken, yerden 1500 metre yüksekliklerde bu oran 50 mikro reme, yerden 3000 metre yükseklikte ise 100 mikro reme çıkmaktadır. Bu nedenden dolayı uçak ile yapılan uçuşlarda insanlar bir miktar radyasyon almaktadır. Ancak bu miktar havada kalınan her saat için 0,5 mikro rem radyasyon olduğu için göz ardı edilebilir.
- **Karasal Radyasyon**: Toprakta doğal olarak bulunan toryum, uranyum ve diğer radyoaktif elementlerin neden olduğu radyasyon türüdür. Yılda karasal radyasyon alımını ise yıllık 30 mikro rem olarak ölçülmüştür. Bu miktar sahillerdeki yerleşim yerlerinde daha da düşüktür. Ancak bazı yerleşim yerlerinde, özellikle radyoaktif madenlerin bulunduğu yerlerde bu miktar 2 katına çıkmaktadır. Radon elementinin bulunduğu bir ortamın solunması yoluyla yılda yaklaşık 200 mikro rem radyasyon alınmaktadır. Dünya'da Hindistan'da Kerela'da, Brezilya'da Minas Gerais bölgesinde ve Türkiye'de Eskişehir Sivrihisar ilçesin yakınlarında Toryum elementi yüksek oranlarda bulunmaktadır. Buralarda yaşayan insanların ortalama olarak yıllık 1000 mikro rem radyasyona maruz kaldıkları saptanmıştır.
- **Yiyeceklerde bulunan Radyasyon**: Yiyeceklerde çok az olarak radyasyon Karbon-14 radyoaktifi içeren potasyum doğal olarak bulunmaktadır. Yıllık olarak ortalama 20 mikro rem civarı bir radyasyon dozu içeren yiyeceler dış kaynaklardan gelen yayılımla çok daha fazla dozlara maruz kalmaktadırlar.

- **İnsanlardan kaynaklanan Radyasyon**: İnsanlarda tıpkı bitki ve hayvanlarda olduğu gibi doğal olarak potasyum bulunmaktadır. Bu da insanları radyoaktif yapmaktadır. Bir insanda ortalama olarak 40 mikro remlik bir doz bulunmakta ve bu miktarın diğer insanlara zararı hemen hemen yok gibidir.
- **Tıbbı cihazlardan kaynaklı Radyasyon**: Amerikan Nükleer Topluluğu'nun verilerine göre; kol bacak ve diş röntgeninde 1 mikro rem, göğüs röntgeninde 6 mikro rem, tiroid taramasında 14 mikro rem, boyun ve kafatası taramasında 20 mikro rem, Pelvis taramasında 65 mikro rem dozluk radyasyonlar alındığı tespit edilmiştir.

Bütün bunlar toplanıldığında bir insan yılda en az 300 mikro rem doz civarı bir radyasyona maruz kalmaktadır. Yapılan araştırmalara göre A.B.D.'de insanlarda alınan yıllık doz oranının 360 mikro rem civarı olduğu bilinmektedir. İnsan vücudunda toplamda 250.000 mikro rem doz birikmesi halinde kansere yakalanma şansı %10 artmaktadır. Bu dozda radyasyonun bir insanda toplanması, yılda 3000 mikro remden fazla radyasyonun 80 yıl boyunca alınması ile mümkündür. Burada alınan radyasyon miktarları ile kanser riski arasında doğrusal bir ilinti var gibi algılansa da miktarlar açısından bu riskin çok az olduğu öngörülmektedir.

## Dozimetre ve Dozimetre Kullanımı

Radyoaktif maddelerle veya radyasyon yayan cihazlarla (röntgen cihazı, X-Işını cihazı, v.b.) çalışan kişilerin maruz kaldığı radyasyon dozunu ölçmeye yarayan cihazlara kişisel dozimetre adı verilir. 24.03.2000 tarih ve 23999 sayılı Resmi Gazete'de yayımlanan TAEK Radyasyon Güvenliği Yönetmeliği'nin 21. Maddesi gereğince, "*yıllık dozun, izin verilen düzeyin 3/10'unu aşma olasılığı bulunan çalışma koşulu A durumunda görev yapan kişilerin, kişisel dozimetre kullanması zorunludur*". Bu hizmet ülkemizde, TAEK tarafından iki aylık periyotlarla kişinin tüm vücut dozunun tespiti için kullanılan film veya termolüminans (TLD) dozimetreler ve cilt dozunu tespit etmek amacıyla ikinci dozimetre olarak kullanılan yüzük dozimetreler ile verilmektedir.

Dozimetreler kullanıcıya özel olarak dağıtılmalı ve bilgileri de TAEK'e gönderilmelidir. Sonraki periyotlarda cihazları kullanacak olan kişilerin, yeni dozimetreleri kullanmaları ve bir önceki kullanılmış olan dozimetreleri kullanmamaları gerekmektedir. Dozimetreler kullanılmadığı zamanlarda, ölçüm bilgilerinin doğruluğu için radyasyon alanı dışında muhafaza edilmeli, ısı, nem ve basınca maruz bırakılmamalıdır.

Dozimetreler çalışma önlüğünün dışına takılmalı ve kartın önüne herhangi bir cisim (kalem, isimlik v.b.) konulmamalıdır. TLD'lerin değişimi taşıyıcıları ile birlikte yapıldığından, taşıyıcılar kesinlikle açılmamalıdır.

Dozimetre filmleri, taşıyıcı içerisine, filmin üzerindeki numara karşıdan bakıldığında okunacak şekilde yerleştirilmelidir. Gönderilen filmler mutlaka taşıyıcı içerisinde kullanılmalıdır. Aksi halde doz değerlendirilmesi sağlıklı olarak yapılamamaktadır.

Yüzük dozimetreler, cilt yıpranmasını engellemek amacıyla mutlaka eldivenin altına takılarak kullanılmalı ve yüzük, TLD kristalinin bulunduğu şeffaf kısım dışa bakacak şekilde takılmalıdır.

Çalışma sırasında kurşun önlük giyiliyorsa, tüm vücut dozunun ölçülebilmesi için dozimetre kurşun önlüğün altına takılmalıdır. Dozimetrenin önlük üzerinde taşınması durumunda ise kurşun önlük dışında kalan; troid, göz lensi, cilt gibi vücudun diğer kısımlarının maruz kaldığı radyasyon miktarı ölçülebilmektedir. Bu durumdaki operatörlere kurşun önlük altında ve üstünde olmak üzere iki dozimetre kullanması önerilmektedir.


**Resim 4.6:** TLD tipi dozimetre (sol) ve yakada kullanılan film tipi dozimetre (sağ).

İNTERNET **Ayrıntılı bilgi için: http://www.taek.gov.tr/belgeler-formlar/func-startdown/285/ adresinden yararlanabilirsiniz.**

SIRA SİZDE 4 **X-Işını cihazı operatörlerinde dozimetre bulunup bulunmadığını inceleyiniz.**

## Özet

X-Işını, 1895 yılında Alman bilim adamı Wilhelm Conrad Röntgen tarafından deneysel bir çalışma sırasında tesadüfen keşfedilmiş ve İngilizce' de bilinmeyen anlamına gelen X harfi ile kullanılarak X-Işını olarak isimlendirilmiştir.

X-Işını ile çalışan güvenlik cihazları X-Işını tüplerini kullanmaktadır. Temelde X-Işını tüpü vakum ortamına alınmış anot ve katot gerilimleri altında katot tarafında kaynak flaman ve anot tarafında hedef metalden oluşmaktadır. Bu metal atom numarası büyük olan ve erime sıcaklığı yüksek olan Tungsten elementinden imal edilmektedir.

X-Işını cihazları; insan, nesne ya da araçların sabit bir X-Işını kaynağından geçirilmesi sonucunda içeriği hakkında bilgi veren cihazlardır. X-Işınları; tıpta teşhis ve tedavi, fizikte maddenin kristal yapısı, teknolojide malzeme kontrollerinde, maddenin içeriğinin araştırılmasında, kimyasal maddelerin içerisindeki az miktarda bulunan maddelerin analizinde, güvenlik açısından kişilerin eşyaların ya da araçların içerisindeki uyuşturucu, silah, patlayıcı ve patlayıcı düzenekleri tespitinde sıklıkla kullanılmaktadır.

Güvenlik ekipmanları içerisinde kullanılan X-Işını cihazları, elde edilen görüntülerin çeşitli filtreleme işlemleri sonucunda bir takım görüntü işleme teknikleri yardımıyla nesnelerin içeriği hakkında bilgi verirler. Güvenlik taraması yapılan bagajların içerisindeki nesneler; organik, inorganik ve metal olması durumuna göre farklı renklerde monitörde gösterilmektedir. Cihaz üreticilerine göre bu nesnelerin renklendirilmesi konusunda farklı tercihler bulunsa da, organik olan nesneler için genelde turuncu tonları kullanılmaktadırlar.

X-Işını cihazı operatörleri, yalnızca silah, bıçak gibi nesnelerin yanı sıra, patlayıcı madde veya düzeneklerini de ayırt etmek ve tespit etmek için eğitilmektedirler. Patlayıcı maddeler, elle imal edildiği ve her biri farklı düzeneklerde olduğundan bu noktada cihaz operatörlerinin bilgi ve deneyimi son derece önemlidir.

X-Işını güvenlik sistemleri; insan tarama, bagaj ve paket kontrolü, kargo ve araç kontrolü, el bagajı tarama sistemleri olarak dört farklı gruba ayrılmaktadır. İnsan tarama sistemleri; hava limanları, alışveriş merkezleri, adliyeler, gümrükler, hapishaneler, limanlar, kamu binalarında ağırlıklı olarak kullanılmaktadır. Bagaj ve paket kontrol sistemleri; hava alanları, kamu binaları, alışveriş merkezleri gibi yerlerde vazgeçilmez güvenlik araçlarındandır. Kargo ve araç kontrol sistemleri; havaalanları, gümrük kapıları, limanlar gibi noktalarda büyük konteynerlerin içerisinin kısa sürede taranabilmesi nedeniyle tercih edilmektedirler. El bagajı tarama sistemleri ise, yukarıda sayılan bölgeler dışında, binaların dışında bırakılan paket veya bagajların içeriğinin görüntülenmesi ihtiyacında kullanılan mobil cihazlardır.

X-Işını cihazı operatörleri, ışınımdan ve kazalardan korunma yöntemleri konusunda bilgi sahibi olmalıdır. Ayrıca operatörler taraması yapılan bagajların ebat ve durumlarına göre hareketli banda uygun olarak sokulmasına dikkat etmelidir. Operatörler cihazı kullanırken, kılık kıyafetlerinin kişisel emniyetleri gereği bol olmamasına dikkat etmeli, kravat-şal-fular gibi sarkan aksesuarları kullanmamalı, saçları uzun ise bunlar kesinlikle toplanmalıdırlar. Ayrıca operatörler, Türkiye Atom Enerjisi Kurumu (T.A.E.K.) tarafından dağıtımı ve belirli periyotlarda denetimi yapılan dozimetre kullanımına önem verilmelidir. Cihazlardan kaynaklanan radyasyon konusunda, operatörlerin bilinçlendirilmesi ve bu cihazlardan geçirilen bagajlarda bulunan yiyecek, içecek gibi maddelerin radyasyona tabi tutulduğundan tüketilmemesi konusunda insanlar uyarılmalıdır.

Dozimetre; TLD ve yüzük olmak üzere iki çeşit olarak X-Işını cihazlarını kullanan bütün operatörler tarafından kullanılmalıdır. Operatörler bu cihazları kullanım sonrası, radyasyona maruz kalmayacak izole bir yerde saklamalı ve kendileri dışında kimsenin kullanmamasına dikkat etmelidirler. Ayrıca dozimetrenin önünde, kalem yaka kartı vb. gibi ölçümü etkileyecek yabancı cisimler bulundurulmamalıdır. Cihazların ölçüm periyotları ve kişisel takipleri T.A.E.K. tarafından internet üzerinden çevrimiçi olarak yapılabilmektedir.

## Kendimizi Sınayalım

**1.** X-Işınının varlığı, aşağıdaki bilim adamlarından hangisi tarafından bir deneyde tesadüfen keşfedilmiştir?

a. C. Hittrof

b. K. Crookes

c. W.C. Röntgen

d. S. Loewe

e. T. Edison

**2.** Aşağıdaki ışınlardan hangisinin frekansı diğerlerine göre daha büyüktür?

a. Kızılötesi

b. Mikrodalga

c. Morötesi

d. X-Işını

e. Gamma ışınları

**3.** Aşağıdaki ışınlardan hangisinin dalga boyu diğerlerine gore daha büyüktür?

a. Kızılötesi

b. Görülebilir ışıklar

c. Morötesi

d. X-Işını

e. Gamma ışınları

**4.** X-Işını cihazlarından geçen atom numarası 10'un altında olan organik maddeler, monitörde hangi renkte görünürler?

a. Yeşil

b. Turuncu

c. Mor

d. Mavi

e. Beyaz

**5.** Aşağıdakilerden hangisi X-Işını tarama sistemlerinden birisi değildir?

a. İnsan Tarama Sistemleri

b. Bagaj ve Paket Kontrolü Sistemleri

c. Manyetik Kapı Sistemleri

d. El Bagajı Tarama Sistemleri

e. Kargo ve Araç Kontrol Sistemleri

**6.** X-Işını cihazının ve dozimetrelerin ölçümü ve bunların radyasyon kontrolleri aşağıdakilerin hangisi tarafından yapılmaktadır?

a. X-Işını Denetleme Kurulu

b. Özel Güvenlik Şirketi

c. Emniyet Genel Müdürlüğü

d. Türkiye Atom Enerjisi Kurumu

e. Radyasyon Denetleme Kurulu

**7.** Güneş ve diğer yıldızlardan dünyamıza gelen, ancak dünyanın atmosferi tarafından büyük bir kısmı bloke edilen radyasyon çeşidi aşağıdakilerden hangisidir?

a. Zararsız Radyasyon

b. Havasal Radyasyon

c. Atmosferik Radyasyon

d. Karasal Radyasyon

e. Kozmik Radyasyon

**8.** Aşağıdakilerden hangisi yiyeceklerde doğal olarak bulunan radyoaktiftir?

a. Toryum

b. Karbon-14

c. Baryum

d. Demir

e. Aluminyum

**9.** Dozimetre kimler tarafından kullanılır?

a. Güvenlik Amirleri

b. X-Işını cihazı bakım-onarım teknisyenleri

c. Yıllık dozun, izin verilen düzeyin 3/10'unu aşma olasılığı bulunan yerlerdeki operatörler

d. Hamileler

e. Güvenlik mensupları

**10.** Taşıma bantlı bagaj ve paket kontrol sistemlerinin operatörleri aşağıdakilerden hangisine özellikle dikkat etmelidir?

a. Kravat takmaya

b. Fular takmaya

c. Bol kıyafetler giymeye

d. Kolye takmaya

e. Saçlarını toplamaya

## Kendimizi Sınayalım Yanıt Anahtarı

**1. c** Yanıtınız yanlış ise "Giriş" başlıklı konuyu yeniden gözden geçiriniz.

**2. e** Yanıtınız yanlış ise "Giriş" başlıklı konuyu yeniden gözden geçiriniz.

**3. a** Yanıtınız yanlış ise "Giriş" başlıklı konuyu yeniden gözden geçiriniz.

**4. b** Yanıtınız yanlış ise "X-Işını Cihazları ve X-Işını Cihazlarının Çalışma Şekli" başlıklı konuyu yeniden gözden geçiriniz.

**5. c** Yanıtınız yanlış ise "X-Işını Güvenlik Sistemi Çeşitleri" başlıklı konuyu yeniden gözden geçiriniz.

**6. d** Yanıtınız yanlış ise "X-Işını Cihaz Kullanımında Dikkat Edilmesi Gereken Konular" başlıklı konuyu yeniden gözden geçiriniz.

**7. e** Yanıtınız yanlış ise "X-Işını Cihazları ve Radyasyon" başlıklı konuyu yeniden gözden geçiriniz.

**8. b** Yanıtınız yanlış ise "X-Işını Cihazları ve Radyasyon" başlıklı konuyu yeniden gözden geçiriniz.

**9. c** Yanıtınız yanlış ise "Dozimetre ve dozimetre kullanımı" başlıklı konuyu yeniden gözden geçiriniz.

**10. e** Yanıtınız yanlış ise "X-Işını Cihaz Kullanımında Dikkat Edilmesi Gereken Konular" başlıklı konuyu yeniden gözden geçiriniz.

## Sıra Sizde Yanıt Anahtarı

### *Sıra Sizde 1*

Bu tip cihazlarla gülük yaşamda; hastanelerde alışveriş merkezi girişlerinde, havaalanları kontrollerinde, gümrük noktalarında, emniyet merkezleri girişlerindeki kontrol noktalarında, askeri birimlerin girişlerinde, kargo taşıma merkezlerinde ve gemi limanlarında sıklıkla karşılaşmaktayız.

### *Sıra Sizde 2*

X-Işını cihazları kullandığı teknoloji sayesinde aramalarda her türlü paket, çanta, valiz, koneyner, kamyon gibi aranılan cisimlerde olası şüpheli maddelerin tespitinde büyük yarar sağlamaktadır. El ve gözle yapılan aramalar çoğunlukla yetersiz ve güvensiz kalırken bu cihazlar kısa arama süreleriyle ve tespit başarı oranlarıyla son derece güvenilirdirler.

### *Sıra Sizde 3*

Cihazın hareketliliğinin sağladığı kolaylıklar nedeniyle mobil arama cihazları sıklıkla tercih edilmektedir. Mobil cihazlara tümleşik ekranlar, arama sırasında aranan cisime gizlenmiş patlayıcı maddenin olası bir durumda aktif hale geçmesi düşünüldüğünde, bir patlama sonucu, operatörüne zarar verebilir.

### *Sıra Sizde 4*

X-Işını cihazlarının kullanıldığı hastaneler, alışveriş merkezleri gibi yerlerde operatörlerin dozimetre kullanmadıklarını görmekteyiz.

## Yararlanılan Kaynaklar

Pearson, R.L. (2007). **Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions**, Butterworth-Heinemann, Elsevier.

Türkiye Atom Enerjisi Kurumu (TAEK) **Dozimetre Kullanım Talimatı**.

FDA U.S. Food And Drug Administration (2011). **Radiation-Emitting Products and Procedures**.

Arslan, T. (2010) **X Işınları ve Kullanım Alanları,** Gazi Üniversitesi Bitirme Tezi.

## Yararlanılan İnternet Kaynakları

http://www.rapiscansystems.com

http://www.howstuffworks.com/dictionary/physics-terms/xray-info4.htm.

# 5

## Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Kapalı devre görüntü ve kayıt sistemlerinin amaçlarını, avantajlarını ve eksik yönlerini açıklayabilecek,
- Değişik kapalı devre görüntü ve kayıt sistem mimarilerini tanımlayabilecek,
- Kapalı devre görüntü ve kayıt sistem bileşenleri ve görevlerini açıklayabilecek,
- Kapalı devre görüntü ve kayıt sistemlerinde kullanılan kamera çeşitlerini ve yapılarını örnekleyebilecek,
- Kapalı devre görüntü ve kayıt sistemlerinde kullanılan iletişim ve güç kablo çeşitlerini açıklayabilecek,

bilgi ve becerilere sahip olabilirsiniz.

## Anahtar Kavramlar

- Analog Kamera
- Sayısal IP Kamera
- Sayısal Web Kamerası
- Sayısal Video Kayıt Cihazı (DVR)
- Ağ Video Kayıt Cihazı (NVR)
- Görüntü Sensörü
- Mercek
- Odak Uzaklığı
- Koaksiyel Kablo
- UTP Kablo

## İçindekiler

# Kapalı Devre Görüntü ve Kayıt Sistemleri

## GİRİŞ

Kapalı Devre Görüntü ve Kayıt Sistemleri (Closed Circuit TV – CCTV) çeşitli sayıda kameralar kullanılarak belirli bir bölgenin gözetlenebilmesi, elde edilen görüntülerin kayıt altına alınması ve video ekranlarında görüntülenmesine olanak sağlayan sistemlerdir.

Teknolojideki hızlı ilerlemelerle birlikte teknik ekipmaların ucuzlaması ve herkes tarafından satın alınabilir hale gelmesi, terör, kundaklama ve hırsızlık olaylarının artması ve buna bağlı olarak güvenliğin daha fazla önem kazanması ile birlikte, CCTV sistemlerinin kurulum ve kullanılmalarında son yıllarda önemli artışlar meydana gelmiştir. Artık CCTV sistemleri sadece büyük firmalar, konsolosluklar, askeri birlikler ve devlet kurumları gibi bu tür sistemleri satın almaya gücü yeten kuruluşlar tarafından değil, çok küçük çaplı esnaf dükkânları tarafından bile kullanılabilir hale gelmiştir. Günümüzde CCTV sistemlerinin şehir merkezleri, dükkân ve alışveriş merkezleri, bankalar, park alanları, okullar, üniversiteler, hastaneler, tren istasyonları, otogarlar, havaalanları, apartman siteleri gibi çok çeşitli yaşam alanlarında caydırarak güvenliği sağlama, gözetleme ve denetleme amaçlı kullanıldığına şahit olmaktayız.

CCTV sistemlerinin kullanılma amaçlarını üç ana sınıfta toplayabiliriz:

- **Güvenlik amaçlı:** CCTV sistemlerinin temel amaçlarından biri caydırıcılık sayesinde suç işlenmesine engel olmak, suç işlenmesi durumunda bunun çabucak fark edilerek olaya anında müdahale edilmesine olanak sağlamak ve elde edilen görüntüleri kayıt altına almaktır. Gözetlenen bölgenin muhtelif yerlerine uygun bir şekilde yerleştirilecek kameralar sayesinde bütün alan gözetim altında tutulacak, olası bir işgal ve suç teşebbüsü fark edilecek ve anında müdahale edilmesine olanak doğacaktır. Korunulan bölgenin tamamını kapsayacak şekilde yapılacak bir kurulum, bütün bölgenin sadece birkaç güvenlik elemanı ile gözetlenmesi ve korunmasına olanak sağlayacak, bu sayede koruma için gerekli güvenlik personeli sayısını büyük ölçüde azaltacaktır.
- **Gözetleme amaçlı:** Bu tür uygulamalar arasında ormanların yangınlara karşı gözetlenmesi, otoyol ve tünellerdeki trafik akışının gözetlenmesi, insan kullanımının zor ve sağlık açısından tehlikeli olduğu endüstriyel uygulamalarda kameraların kullanılması sayılabilir. Sistem sayesinde orman yangınları, trafik kazaları gibi acil durumlar anında fark edilerek kısa zamanda müdahale olanağı doğmaktadır. Ayrıca, ülkemizde son yıllarda hızla genişleyen ve polis teşkilatı tarafından kullanılan Mobil Elektronik Sistem Entegrasyonu (MOBESE) gözetleme ve güvenlik ağı sayesinde çalıntı ve trafik kuralı ihlali yapan araçlar plakalarıyla birlikte anında fark edilebilmektedir. Ayrıca, insan kullanılarak gözetleme yapmanın zor hatta imkansız olduğu, ve insan sağlığı için tehlike arz eden endüstriyel otomasyon uygulamalarında, nükleer santrallerde ve kanalizasyon ve diğer boru hatlarının gözetlenmesi ve görüntülenmesi uygulamarında kameraların kullanıldığı görülmektedir.
- **Denetleme amaçlı:** Bu tür uygulamalar daha çok fabrika ve servis veren işyerlerinde çalışanların performanlarının ve yaptıkları işlerin gözetlenmesi için kullanılmaktadır. Ayrıca çalışan anne ve babaların evde çoçuk bakıcıyı gözetleme ve denetlemesine olanak sağlayan Internet'e bağlı birkaç kameralı sistemler bu grup uygulamalar içinde sayılabilir. Bu tür sistemlerin kullanımında, denetleme ihtiyacı ve insanların özel hayatlarına müdahale ihtimali arasında çok ince bir çizgi olduğu gözden kaçırılmamalıdır.

**SIRA SİZDE 1 Kapalı Devre Görüntü ve Kayıt sistemleri ne işe yarar? Bu tür sistemlerin temel kullanım amaçları nelerdir?**

CCTV sistemleri yukarıda bahsedilen kullanım amaçlarının yanında aşağıdaki avantajları sağlarlar:

- Caydırıcılık sağlayarak, suç işlenmesinin önüne geçer. Potansiyel suçlular kameralar tarafından gözlenen bölgelerde suç işlemek yerine daha korumasız yerlere yönlenirler. Yapılan araştırmalar, CCTV ile korunan işletme ve bölgelerde suç işlenme oranlarının düştüğü sonucuna varmıştır.
- Çalışanların güvenliğini sağlar. Müşteri temsilcileri bazen sinirli müşteriler ile iletişime geçmek zorundadır. Sinirli müşteriler ile yüz-yüze iletişime geçmek çalışanları zor durumda bırakabilir. CCTV ile gözetlenen bir müşteri temsilcisine karşı müşterilerin daha kontrollü davranması ve temsilcinin bu sayede korunması beklenebilir.
- Güvenlik elemanlarının verimliliklerini artırır. CCTV sayesinde güvenlik elemanları kontrol ve kumanda merkezinden çok daha geniş bir alanı az sayıda bir personelle kontrol ve gözetim altında tutabilirler. Güvenlik elemanı sayısındaki azalma işverenin maliyetlerinin azalması için önemli bir faktördür.
- Güvenlik görevlileri tarafından kontrol edilmesi zor veya imkânsız olan veya insan sağlığı için tehlikeli olan bölgeler kolaylıkla gözetlenebilir. Bu tür alanlara örnek olarak kimyasal ve nükleer santraller, kanalizasyon ve petrol boru hatları verilebilir.
- Kayıt sistemi sayesinde işlenen bir suçun faillerinin hızlı bir şekilde belirlenmesine yardımcı olur. Ayrıca işyerlerinde çalışanlar arasında çıkması muhtemel kavga ve tartışmalarda, olayın kayıtlarına bakarak işverenin problemi çözümlenmesine yardımcı olur.

CCTV sistemlerinin yukarıda sayılan faydalarını www.dikkathaber.com sitesinde 21 Kasım 2011 tarihinde "*Emniyet Müdürü Ceren: Mobese, Halkın En Yakın Polisidir.*" başlığıyla yayımlanan aşağıdaki haber güzel bir şekilde özetlemektedir.

> "*Osmaniye İl Emniyet Müdürü Tayfur Erdal Ceren mobese kameralarının halkın huzur ve güvenliğini sağlayan en yakın polis olduğunu söyledi. Mobese merkezinin, kritik noktalardaki hareketli ve sabit birçok kamera ile 24 saat hizmet verdiğini kaydeden Ceren, sistemin, şehrin trafik ihlallerini tespiti ve suçları önleme ile takibi gibi konularında büyük faydaları olduğuna dikkat çekti.*
>
> *Mobese sisteminin, geçen yıl Mayıs ayında Osmaniye'de hizmete girdiğini belirten İl Emniyet Müdürü Ceren, açıklamasında, 'Suçların işlenmeden önce önlenebilmesi, işlenmiş suçların tespiti ve suç faillerinin yakalanmasına büyük katkılar sağlayan mobese sistemi, kent içerisinde olmuş veya olabilecek olaylar karşısında ekiplerin yönlendirilmesinde etkin bir rol oynamaktadır. Bunun yanı sıra mobese sisteminin trafik akışının düzenlenmesi ve kazaların en aza indirgenmesi, çalıntı ve aranan araçların en kısa sürede yakalanması, emniyet hizmetlerinin şeffaflaşması, vatandaşlarımızın kamu görevlilerine olan güveninin pekişmesi ve halkımızın güvenliğini maksimum düzeye çıkartmak gibi önemli faydalar sağlamaktadır.' dedi.*
>
> *Kural ihlali yapan sürücülerin mobese kameraları tarafından tespiti halinde ise gerekli fotoğraflamanın yapılmasının ardından, araç plakalarına cezai işlem uygulandığını belirten Osmaniye İl Emniyet Müdürü Tayfur Erdal Ceren, ceza tutanağı ve kural ihlali fotoğraf çıktısı sürücülerin adreslerine posta ile gönderildiğini sözlerine ekledi.*"

CCTV sistemlerinin avantajları yanında aşağıda listelenen eksik yanları ve dezavantajları da mevcuttur.

- Gözetlenen bölgenin büyük bir kısmı kameraların kapsama alanında olsa bile bölgenin bazı ücra köşeleri kapsama alanı dışında kalır. Kapsam alanı dışında kalan bu tür alanlarda işlenecek suçlar gözetlenemez ve kayıt altına alınamaz. Ayrıca kameraların üzerlerinin örtülmesi veya devre dışı bırakılmaları sonucunda suç mahalli belli bir süre kapsam alanı dışında kalabilir. Ayrıca sistemin işleyişini çok iyi bilen bazı çalışanların sistemin açıklarından faydalanarak suç işlemesinin önüne geçmek mümkün olmayabilir.
- Sistemde kullanılan kameralar doğru seçilmemişse ve elde edilen görüntülerin kaliteleri düşük ise, kayıt altına alınan görüntüler işlenen suçların aydınlatılmasında hiç bir işe yaramayabilirler. Ülkemizde kalitesiz görüntü kayıtlarından dolayı işe yaramayan olay yeri görüntüsü haberlerine sıkça rastlamaktayız.
- Kurulan sistemin 7/24 çalışmaması veya görüntü kayıtlarının güvenli bir şekilde saklanamamaları durumlarında, sistem kuruluş amacı olan güvenliğin sağlanması ve suçluların bulunmasına yardımcı olması amaçlarını gerçekleştiremeyecektir.
- Otogar, havaalanı, park vb. halka açık bölgelerindeki CCTV kurulumlarına karşı çıkan kesimler bu tür sistemlerin insanların özel hayatlarına müdahale ettiğini savunmakta ve halka açık yerlerde insanların özel hayatlarının kayıt altına alınmasına karşı çıkmaktadırlar. Ayrıca bazı çalışanlar işyerlerinin her bölgesinde yaşamlarının kayıt altına alınmasının insan haklarına aykırı olduğunu savunmaktadır.

CCTV sistemlerinin yukarıda sayılan eksik yanlarına www.haber365.com sitesinde 22 Ekim 2010 tarihinde "Apartmanlardan işyerlerine, okuldan alışveriş merkezlerine kadar her alanda güvenlik önlemi olarak kullanılan kameraların büyük bölümünü çalışmıyor." başlığı ile yayımlanan aşağıdaki haber güzel bir örnektir.

> "*Apartmanlardan işyerlerine, okuldan alışveriş merkezlerine kadar her alanda güvenlik önlemi olarak kullanılan kameraların büyük bölümünün eski teknoloji ve kalitesiz olmaları nedeniyle çalışmadığı, veri alınamadığı bildirildi.*
>
> *Genelde ucuz teknoloji olan güvenlik kamerası ve hırsız alarm sistemlerinin teknoloji çöplüğü oluşturduğu dile getiriliyor.*
>
> *Kayseri ve bölge illerde faaliyet gösteren İtimat Güvenlik Müdürü Zekeriya Daş, güvenlik sistemlerinde ucuzu aramanın, kaliteden taviz vermenin bedeli olarak apartmanlarda, işyerlerinde, okullarda, atıl, kullanılamayan yada verim alınamayan teknolojik çöplüklerin oluştuğunu dile getirdi.*
>
> *Güvenlik sistemlerinin artık hayatın vazgeçilmez bir parçası olduğuna işaret eden Zekeriya Daş, kalitesiz sistemlerin tercih edilmemesi konusunda vatandaşları uyardı.*
>
> *Son zamanlarda konutların bulunduğu binalarda güvenlik kamerası sistemlerinin arttığını dile getiren Daş, 'Binalarda güvenlik kamerası sistemi arttı. Geçen yıl kaçırılan çocuklarımız bunda etkili oldu. Eğer güvenlik kamerası olsaydı kaçırılan çocuklarla ilgili olay aydınlatılabilirdi. Alınan hizmetin kalitesi çok önemlidir.*
>
> *Çözünürlüğü düşük kamera alınıyor. Güvenlik kamerası var. Ama 2 metreden kişi tanınamıyor. Burada biz de zor durumda kalıyoruz. Vatandaş ekonomik çözüm istiyor. Ama olayların aydınlatılmasında sunulan ekonomik çözüm sıkıntı oluşturuyor. Bazı firmalar ekonomik olarak istenen ürünlerin sıkıntısını anlatıyor ve sorumluluk almıyor.*
>
> *Buna rağmen kişiler bu ürünleri kullanmak istiyor. Firmaların iş yükü artınca güvenlik sistemlerinin bakımı da ihmal edilebiliyor. Biz firma olarak her şeye rağmen 48 saat içerisinde güvenlik sistemindeki yaşanan sıkıntıya müdahale edeceğimiz söylüyor ve taahhüt ediyoruz.' diye konuştu.*

*Kalitesiz güvenlik sistemleri cihazları yüzünden teknoloji çöplüğü oluştuğunu anlatan Zekeriya Daş, şöyle konuştu: 'Teknoloji çöplüğü her geçen gün büyüyor. Apartmanlarda atıl bir teknolojik sistem var. Hiçbir ürün kaliteden taviz verilmeden ekonomik fiyatta sunulamaz. Cep telefonlarına bakalım. Çok sayıda telefon var. Kullanıcıların ihtiyacına nasıl cevap veriyor. Veya insanımız kullanmadığı özellikten dolayı bile cep telefonuna bin lira ödeme yapıyor. Bir çok özelliğini kullanmadığımız cep telefonu teknolojisi için çok rahat gereksiz harcama yaparken, hayatımızın güveni için önemli olan güvenlik sistemlerine aynı önemi göstermiyoruz.*

*Her gün televizyonlarda güvenlik kamerası görüntüleriyle çözülen olaylara şahit oluyoruz. Aydınlatılan olaylar var. O nedenle güvenlik kamera görüntülerinin hayatımızın bir parçası ve yaşanan olayların çözümünde önemli olduğunu bilmeliyiz. Güvenlik teknolojileri her gün yenilenen bir sektör. Uluslararası fuarlara katılarak teknolojiyi takip ediyoruz."*

# KAPALI DEVRE GÖRÜNTÜ VE KAYIT SİSTEMLERİNİN GENEL YAPILARI VE BİLEŞENLERİ

Bir kapalı devre görüntü ve kayıt sistemi temel olarak aşağıdaki dört bileşenden oluşur.

1. Kameralar
2. Güç ve iletişim kabloları
3. Video kayıt cihazları
4. Kontrol kumanda merkezi ve video görüntüleme cihazları

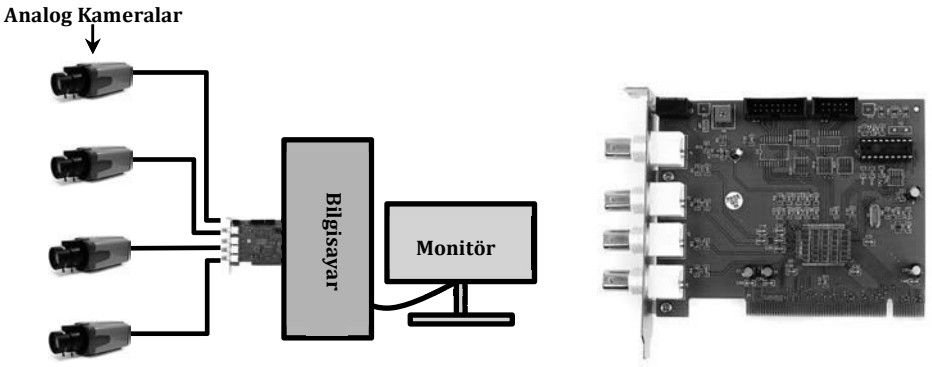
Yukarıdaki bileşenler piyasada çok değişik yapı ve görünümlerde karşımıza çıkmaktadır. Kurulacak olan CCTV sisteminin genel yapısının ana belirleyicisi kameralardır. Piyasada satışta olan değişik yapı ve görünüme sahip çok sayıda kamera mevcuttur. Bu da değişik CCTV mimarilerinin ortaya çıkmasına sebep olmaktadır. Bu bölümde, seçilecek kameralara bağlı olarak kurulması muhtemel CCTV mimarileri hakkında bilgiler verilmeye çalışılacaktır.

## Analog CCTV Mimarileri

Analog kelimesi bu başlıkta görüntünün kablolardan elektriksel bir sinyal olarak gönderilmesi amacı için kullanılmaktadır. Diğer görüntü aktarma şekli ise sayısal olarak adlandırılır ve görüntü belli aralıklarla gönderilen ikilik düzendeki veri bilgisi ile aktarılır. Bu terim günlük hayatta dijital kelimesi ile eşdeğerdir.

Ticari olarak ilk ortaya çıkan ve mevcut CCTV sistem kurulumlarının %80'ini teşkil eden analog CCTV mimarileri birkaç adet analog kamera, en az bir kayıt cihazı ve kameralar tarafından elde edilen görüntülerin gösterildiği en az bir monitörden oluşmaktadır. İki veya daha fazla kameranın olduğu durumlarda monitör ekranında her kameranın görüntüsünün gösterildiği ufak bir pencere açılır. Böylece bütün kameraların görüntülerini aynı mönitör ekranında görmek mümkündür.

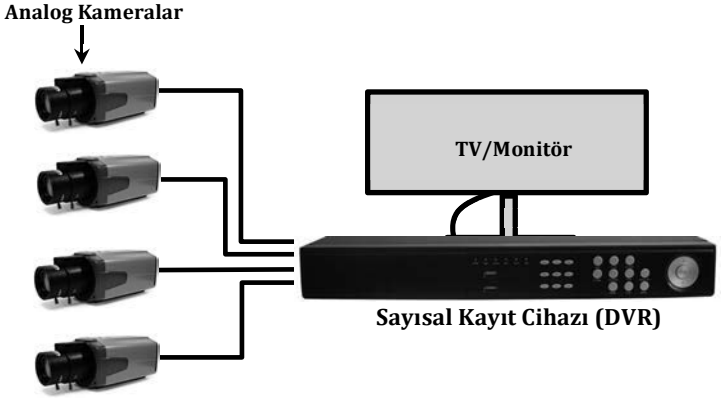
Bu tür sistemlerde kullanılan analog kameraların her biri ayrı bir kablo ile kayıt cihazına bağlanır. Kameralar tarafından elde edilen görüntüler analog elektronik sinyaller olarak kayıt cihazına aktarılır. Eğer kayıt cihazı çok eski sistemlerde olduğu gibi VCR teypleri kullanıyorsa, gelen görüntüler analog olarak teyplere kayıt edilir. Yeni sistemlerde ise, kayıt cihazı gelen görüntüleri elektronik bir kart vasıtasıyla sayısal hale getirir. Görüntüler az yer kaplamaları için önce sıkıştırmaya tabi tutulur, daha sonra sabit disklere kayıt edilir ve aynı anda kayıt cihazına bağlı monitör üzerinde gösterilir.




**Resim 5.1:** Örnek bir analog CCTV mimarisi: Analog kameralar bir masaüstü bilgisayara bağlanır. Masaüstü bilgisayar resimde gösterilen bir analog-sayısal çevirici kart kullanarak analog videoları sayısala çevirir ve sabit diske kayıt eder. Videolar aynı zamanda bilgisayar monitöründe gösterilir.

Bu mimaride kayıt cihazı bir masaüstü bilgisayar, görüntü ekranı bir bilgisayar monitörüdür. Kameralardan elde edilen görüntüler her biri ayrı kablo üzerinden bilgisayara aktarılır. Bilgisayara takılan bir elektronik analog-sayısal çevirici kart vasıtasıyla kameralardan gelen analog görüntüler sayısal hale getirilip sabit diskte saklanır ve aynı zamanda bilgisayar monitörü ekranında gösterilir.

Resim 5.1'de betimlenen analog CCTV sistemlerinin en iyi yanları ucuz olmalarıdır. Var olan bir masaüstü bilgisayar, birkaç kamera, bir analog-sayısal çevirici kart ve basit bir yazılım sayesinde bir CCTV sistemi oluşturulabilir. Piyasadaki analog-sayısal çevirici kartlar Resim 5.1'de de gösterildiği üzere genellikle 1-4 arası kamera girişine olanak sağladığından, kamera sayısı arttıkça masaüstü bilgisayara yeni analog-sayısal çevirici kartlar takmak gerekecektir.



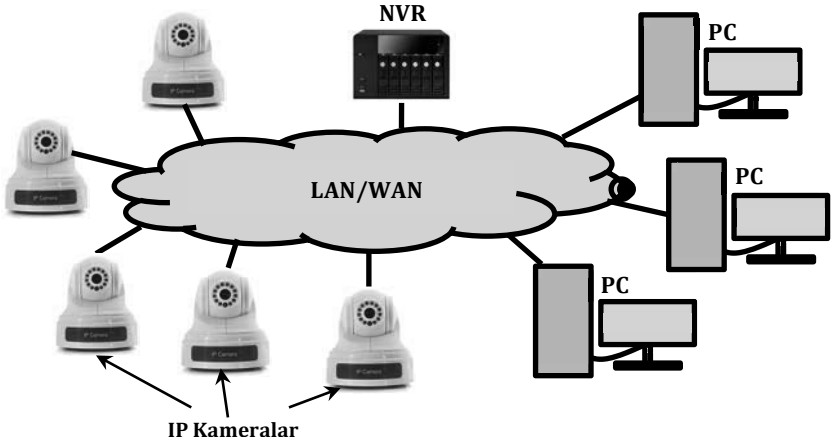

**Resim 5.2:** Örnek bir analog CCTV mimarisi: Analog kameralar ticari bir sayısal video kayıt cihazına (Digital Video Recorder – DVR) bağlanır. DVR analog videoları sayısala çevirir ve içindeki sabit disklere kayıt eder. Videolar aynı zamanda DVR'a bağlı televizyon veya monitörde gösterilir.

Resim 5.2'de analog CCTV mimariye başka bir örnek verilmiştir. Bu örnekte kayıt cihazı olarak masaüstü bir bilgisayar yerine, piyasada özel olarak satılan bir sayısal video kayıt cihazı (Digital Video Recorder – DVR) kullanılmıştır. DVR üzerinde her kameradan gelen kabloların bağlanacağı bir giriş ve mönitörün bağlanacağı bir giriş mevcuttur. DVR bir önceki örnekte masaüstü bilgisayarın yaptığı işi yapan özel bir donanımdır ve işlevi aynıdır. Genellikle uzun süreli kayıt yapabilmek için çok sayıda ve büyük kapasiteli sabit diskler içerir.

Analog **CCTV** mimarileri ucuz ve kurulması kolay olduğundan ufak çaplı kurulumlar için uygundur; fakat büyük çaplı kurulumlar için problemler arz etmektedir. Öncelikle, bu tür sistemlerde her analog kameradan DVR'a bir kablo gelmek zorundadır. Buna ek olarak, her kameranın elektrik alabilmesi için bir güç kablosu bağlanması gereklidir. Ayrıca, Çevir-Eğ-Odakla (Pan-Tilt-Zoom PTZ) denilen sağa sola, aşağı yukarı dönebilen ve görüntülediği objelere odaklanma özellikleri olan kameralar kullanıldığında, bu kameraların kontrol edilebilmesi için, kontrol merkezinden PTZ kameralara görüntü kablosu haricinde ayrı bir kontrol hattı çekilmesi gerekmektedir. Son olarak, DVR üzerindeki kamera giriş sayısı sınırlı olduğundan, çok kameralı sistemlerde birden fazla DVR kullanılması kaçınılmaz olmaktadır.

## Yeni Nesil Sayısal CCTV Mimarileri

Analog sistemlerin yukarıda bahsedilen eksiklikleri, CCTV üreticilerini bahsedilen problemlerin çözümünü kolaylaştıracak yeni kameralar üretmeye sevk etmiştir. Bilgisayar ağlarının ve İnternet'in yaygınlaşması ile birlikte CCTV üreticilerinin piyasaya Internet Protokolü (IP)'yi destekleyen sayısal kameralar sürdükleri görülmüştür.




**Resim 5.3:** Sayısal IP CCTV Mimarisi: IP kameralar doğrudan ağa bağlanırlar ve elde ettikleri görüntüleri sayısal hale getirerek ağ kayıt cihazına (NVR) göderirler. NVR gelen görüntüleri kaydeder ve ağdaki istemci bilgisayarlara talep etmeleri durumunda gönderebilir.

Resim 5.3'de yeni nesil sayısal IP CCTV sistem mimarisi örneği betimlenmiştir. Bu mimaride bütün kameralar, kayıt ve görüntüleme cihazları bir yerel veya Internet gibi geniş çaplı bir Internet Protokolü (IP) ağına bağlanırlar. Sayısal IP kameraların görüntüyü elde etme şekilleri ileride anlatılacağı üzere analog kameralar ile aynıdır. Fakat, analog kameralar elde ettikleri görüntüyü bağlı oldukları DVR'a genellikle bir koaksiyel kablo üzerinden analog olarak aktarırken, IP kameraları görüntüleri sayısal hale çevirirler, ve iletişimde oldukları Ağ Kayıt Cihazına (Network Video Recorder – NVR) ağ üzerinden Internet Prokolü (IP) paketleri olarak aktarırlar. Sistem üzerindeki NVR bütün kamerlardan gelen sayısal görüntüleri içindeki sabit disklere kayıt etmek ve eğer bir mönitöre bağlı ise görüntüleri monitör üzerinde göstermekle yükümlüdür. Sistemin bütün bileşenleri bir ağa bağlı olduğu için ağa bağlı istemci bilgisayarlardan NVR'ye veya direkt olarak kameralara bağlanmak ve elde edilen görüntüleri istemci bilgisayarlara yönlendirmek ve görüntülemek de mümkün olabilmektedir.

IP kamera kullanan sayısal CCTV sistemlerinin analog CCTV sistemlerine göre avantajları şu şekilde sıralanabilir:

- Kameralar için ayrı bir iletişim hattı çekilmesine gerek olmayabilir. Bütün kameralar ve kayıt ekipmanları zaten işyerinde mevcut bulunan yerel IP ağına (Local Area Network – LAN) bağlanabilirler. Kameralar için ayrı kablo hattı çekilmeyecek olması kurulumu kolaylaştırır ve masrafları düşürür.

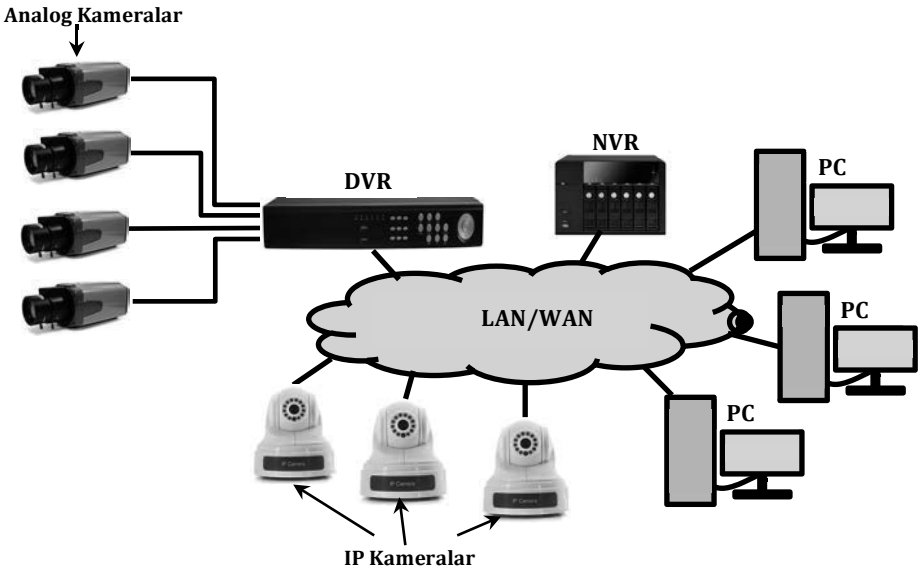
- Bazı IP kameraları çalışmaları için gerekli gücü direkt olarak ethernet kablosu üzerinden alırlar. Bu tür kameralar için ayrı bir güç hattı çekilmesine de gerek kalmaz.
- Sistemin yeni kameralar ile genişletilmesi genellikle kolaydır. Yeni alınan kameralar ağa bağlandıktan ve NVR üzerinde gerekli ayarlar yapıldıktan sonra kameralar hemen kullanılabilir. NVR'ın kapasitesinin yetersiz kalması durumunda yeni NVR'lar satın alınarak kayıt cihazları kapasitesi rahatlıkla artırılabilir.
- IP kameralar üzerinde bir işlemci mevcut olduğundan, kameradan NVR'a gönderilecek görüntü üzerinde işlemler yapmak mümkündür. Mesela, ağ kapasitesini az kullanmak için görüntünün önce sıkıştırmaya tabi tutulması çok kullanılan bir yöntemdir. Ağ güvenliğinin problemli olduğu durumlarda, mesela görüntüler genel kullanıma açık Internet üzerinden aktarılıyorsa, IP kameranın görüntüleri şifreleyerek NVR'a göndermesi de mümkün olmaktadır. Ayrıca, plaka tanıma, yüz tanıma, kaçak giriş yapılmasını belirleme, insan takibi yapma gibi görüntü analizi uygulamalarının direkt olarak kamera üzerinde çalıştırılması mümkün olmaktadır ki, belki de IP kameraların analog kameralara göre sağladığı en önemli üstünlük bu olarak karşımıza çıkmaktadır. Zira analog kamera kullanan sistemlerde bu tür yazılıma dayalı görüntü işleme uygulamaları görüntünün aktarıldığı merkezi bir bilgisayarda yapılmak zorundadır.
- IP kameralar ağa bağlanarak çalıştıklarından, sadece ethernet gibi kablolu değil aynı zamanda kablosuz ethernet (WLAN) veya 3G gibi kablosuz ağlara bağlanarak da kullanılabilirler. Bu sayede IP kameralar ile çok uzak bölgelerden güvenli bir şekilde görüntü elde etmek mümkün olabilmektedir.

Yukarıda sayılan avantajları yanından IP kamera kullanan sayısal CCTV sistemlerinin bazı dezavantajları da mevcuttur. Bunları şu şekilde özetlemek mümkündür.

- IP kameralar daha geniş özelliklere sahip olduklarından, analog kameralara göre çok daha pahalıdırlar.
- IP kamera kullanan CCTV sistemlerinin kurulum ve işletilmesi analog CCTV sistemlere göre zordur. Bu iş için ağ kurulum ve yönetimi konularında bilgili servis elemanlarına ihtiyaç duyulmaktadır.
- Bu tür sistemlerin kabul edilmiş bir standartı yoktur. Üretici her firma sistemin çalışması için kendi standartını geliştirmektedir. Bu sebeple satın alınacak bütün IP kameralar, NVR ve istemci yazılımlarının tamamı bir şirketten temin edilmek zorundadır. Farklı firmaların ürünlerinin bir arada çalışması hemen hemen imkânsızdır. Ürün temininde tek firmaya bağımlı kalmak bu tür sistemlerin en büyük dezavantajı olarak karşımıza çıkmaktadır.

## Karma CCTV Mimarileri

Halihazırda mevcut CCTV kurulumlarının çoğu eski nesil analog kameralar kullandığı için yeni nesil sayısal IP kamera kullanan CCTV sistemlerine bir anda geçiş mümkün değildir. Eski nesil analog sistemlere çok büyük yatırım yapmış firmalar, yeni nesil sayısal CCTV sistemlerine geçişleri sırasında eski analog kameralarını kullanmak istemektedirler. Bunu mümkün kılmak ve geçişi kolaylaştırmak için karma CCTV mimarileri önerilmiştir.




**Resim 5.4:** Karma CCTV Mimarisi. Yeni nesil IP kameralar ağa doğrudan bağlanırken, eski nesil analog kameralar bir sayısal video kayıt cihazı DVR vasıtası ile ağa bağlanır. DVR analog kameralardan gelen görüntüleri kayıt eder ve ağdaki istemcilere gönderebilir. Ağ kayıt cihazı NVR ise ağa bağlı IP kameralardan gelen videoları kayıt eder ve ağdaki istemcilere gönderebilir.

Resim 5.4'de bir karma CCTV mimarisi örneği betimlenmiştir. Analog kameralar eski nesil analog CCTV sistemlerinde olduğu gibi ayrı kablolar vasıtasıyla DVR'ye bağlanırlar ve elde ettikleri analog videoları DVR'ye gönderirler. DVR gelen analog görüntüleri sayısala çevirip, sıkıştırmaya tabi tuttuktan sonra kendi içindeki sabit disklere kayıt eder. DVR aynı zamanda ağa bağlı olduğu için, ağa bağlı istemcilerden gelen istekler doğrultusunda kaydettiği görüntüleri istemcilere gönderebilir. Yeni nesil IP kameraları ise direkt ağa bağlıdır ve elde ettikleri görüntüleri ağ kayıt cihazı NVR'ye gönderirler. Ağa bağlı istemciler NVR ile de iletişime geçerek kayıt edilen görüntüleri ekranlarında görebilirler.

Karma CCTV sistemleri eski nesil analog kameraların kullanımına olanak sağlayarak, tümüyle IP kameralardan oluşan yeni nesil sayısal CCTV sistemlerine geçisi kolaylaştırmaktadır. Fakat yukarıda yeni nesil sayısal CCTV sistemleri için saydığımız dezavantajların tamamı karma CCTV sistemleri için de geçerlidir. IP kameraların ve NVR'lerin kabul edilmiş bir standartının olmayışı bu sistemlere geçişin önündeki en büyük engel olarak görülmektedir. Buna rağmen yukarıda bahsettiğimiz avantajları göz önüne alındığında gelecekte orta ve büyük çaplı CCTV kurulumlarının IP kameralar kullanacaklarını söyleyebiliriz. 1-5 kameralı ufak kurulumlar için ise analog kameralı eski tip sistemlerin yeterli olacağı öngörülebilir. Hatta ucuz USB Web kameraları ve bir masaüstü bilgisayardan oluşan çok ucuz CCTV kurulumlarına da rastlamak her zaman mümkündür.

SIRA SİZDE 2 **CCTV sistem mimarileri nelerdir?**

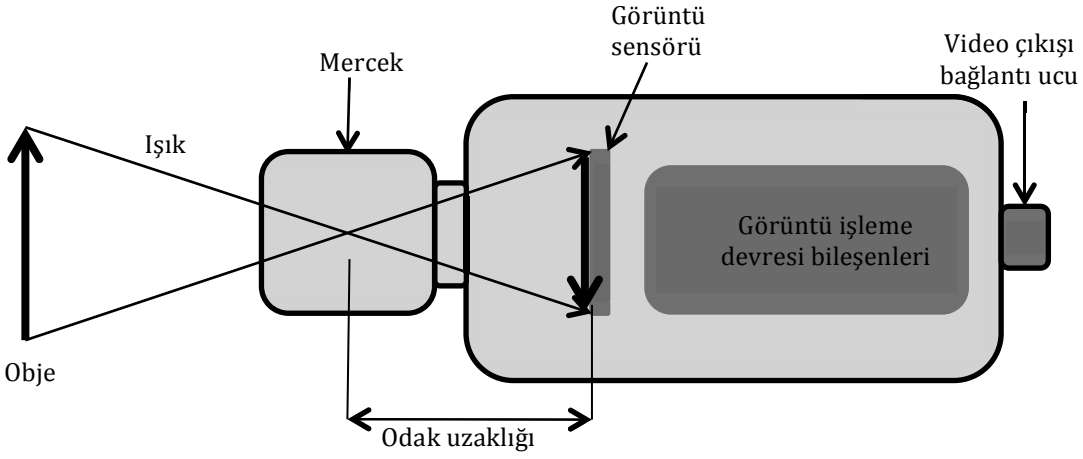
# KAMERALAR

Kameralar bir CCTV sisteminin en önemli bileşenleridir, ve sistemin diğer bileşenlerinin yapısı kameraların yapılarına göre şekillenir. Kameralar genel olarak analog ve sayısal olarak ikiye ayrılsalar da her iki tip kameranın da görüntüyü elde etme şekilleri aynıdır. Farklılık sadece elde edilen görüntülerin kameradan alıcıya aktarımı sırasında ortaya çıkmaktadır. Bu bölümde önce kameraların iç yapılarından ve görüntüyü nasıl elde ettiklerinden bahsedilecek, daha sonra CCTV sistemlerinde kullanılan değişik şekil ve tipteki kameralar tarif edilecektir.

## Kameraların İç Yapıları ve Bileşenleri

Bir kamera temel olarak üç bileşenden oluşur:

1. **Görüntü sensörü**: Kameranın içine giren ışığı elektronik sinyallere çeviren ve görüntüyü elde eden bileşendir.
2. **Mercek (Lens)**: Ortamdaki cisimlerden yansıyan ışıkları görüntü sensörüne yönlendiren bileşendir.
3. **Görüntü işleme devresi**: Görüntü sensörü tarafından ısığın elektronik sinyallere çevrilmesiyle elde edilen görüntüyü organize ve en uygun hale getiren (optimize eden), gerekirse sayısala çeviren ve alıcıya doğru yönlendiren elektronik devredir.




**Resim 5.5:** Tipik bir kameranın bileşenleri ve bir objenin görüntü sensörü üzerinde görüntüsünün oluşması.

Resim 5.5 tipik bir kameranın bileşenlerini ve bir objenin görüntü sensörü üzerinde görüntüsünün nasıl oluştuğunu betimlemeye çalışmaktadır. Objeden yansıyan ışık kameranın merceğinden geçerek görüntü sensörü üzerine düşer ve burada objenin görüntüsü oluşur. Objenin oluşacak görüntü üzerindeki büyüklüğü; objenin büyüklüğü, kameraya olan uzaklığı, görüntü sensörünün büyüklüğü ve merceğin odak uzaklığı gibi parameterler ile ilişkilidir.

Görüntü sensörü üzerine düşen ışık, elektronik sinyallere çevrildikten sonra kameranın görüntü işleme devresine aktarılır. Görüntü işleme devresi elde edilen görüntüyü değişik işlemlere tabi tuttuktan sonra kameranın video çıkışı üzerinden alıcıya yönlendirir. Çıkışa yönlendirilen görüntü analog veya sayısal olabilir.

Bir kamera renkli görüntü üretebileceği gibi, siyah-beyaz (monochrome) görüntü de üretebilir. CCTV sistemleri için genellikle renkli kameralar tercih edilirler, zira renkli görüntü ile ortam hakkında daha fazla bilgi sahibi olunur ve görüntü içindeki objeler daha iyi belirlenebilir. Siyah-beyaz kameralar ise daha ucuzdur ve görüntü elde edebilmeleri için renkli kameralara göre daha az ışığa ihtiyaç duyarlar. Son yıllarda ortaya çıkan gündüz/gece kameraları ise hem renkli hem siyah-beyaz kameraların en iyi özelliklerini barındırmaktadırlar. Bu sebeple gündüz/gece kameraları yeni nesil CCTV uygulamarında sıklıkla tercih edilmektedirler.

## Görüntü Sensörü

Görüntü sensörü kameranın kalbidir ve içine giren ışığı elektronik sinyallere çeviren bileşendir. Bir görüntü sensörü iki boyutlu ve dikdörtgensel bir yapıya sahiptir, ve çok sayıda ışığa duyarlı elektronik devreden oluşur. Bu küçük elektronik devrelerin her birine bir "piksel" denir. Her piksel üzerine düşen ışık miktarına bağlı olarak bir voltaj üretir. Örneğin, hiç ışık olmaması sıfır voltaja yani siyah renge

karşılık gelir. Maksimum ışık ise maksimum voltaja yani beyaz renge karşılık gelir. Diğer ışık seviyeleri sıfır ile maksimum arasında voltajları üretirler ve her voltaj seviyesi değişik gri tonlarda renkleri üretir. Piksellerin ürettiği voltaj, kameradaki elektronik devreler tarafından işlenerek bir çerçeve görüntüye çevrilirler. Bir sensör üzerindeki piksel sayısı ne kadar çoksa, üretilen görüntünün çözünürlüğü de o kadar yüksek olacaktır.

Saniyede 25 (PAL) veya 30 (SECAM) görüntü çerçevesinin arka arkaya gösterilmesi ile video görüntüsü meydana gelir. İnsan gözü arka arkaya gösterilen sabit görüntü çerçevelerini sürekli hareket eden bir video gibi algılar.

Ticari olarak satılan CCTV kameralarda çoğunlukla iki çeşit görüntü sensörü kullanılmaktadır:

1. CMOS (Complimentary Metal-Oxide Semiconductor) sensörleri ucuzdur, az enerji tüketir, fakat ürettiği görüntülerin kalitesi yeni tip sensörlere göre genellikle daha kötüdür.
2. CCD (Charge Coupled Device) sensörleri CMOS sensörlere göre daha pahalı olmakla birlikte, genellikle daha kaliteli görüntü üretir. Bu sebeple görüntü kalitesinin çok önemli olduğu uygulamalarda kullanılmalıdır. CCD sensörleri CMOS'a göre 100 kata kadar daha fazla güç kullanırlar.

Bir görüntü sensörü tarafından üretilen görüntünün kalitesi sensörün fiziksel büyüklüğü ile doğrudan ilişkilidir. Sensör ne kadar büyük bir alana sahipse, ürettiği görüntünün kalitesi de o kadar iyi olur. Fakat sensör büyüdükçe maliyeti de artar. Bu da kameranın fiyatının artması demektir. Özetle, satın alınacak kameranın sensörünün büyüklüğü, uygulamanıza ve bütçenize bağlı olarak belirlenmektedir.

Kamera görüntü sensörü büyüklükleri standartlara uygun olmayan bir biçimde "inç" cinsinden listelenir. Piyada mevcut kameraların tipik sensör büyüklükleri 1/4 inç, 1/3 inç, 1/2 inç, 2/3 inç, 1 inç olarak gözümüze çarpmaktadır. Bu rakam sensörün köşegensel büyüklüğüne karşılık gelir. Sensörün genişlik ve yüksekliği genellikle 4x3'lük orandadır. Yani genişlik 4 birim ise, yükseklik 3 birim olacak şekilde oranlanmıştır. Aşağıdaki tabloda değişik sensör büyüklüklerine karşılık gelen sensör genişlik ve yükseklikleri milimetre cinsinden listelenmiştir.

**Tablo 5.1:** Çeşitli görüntü sensör büyüklükleri ve bunlara karşılık gelen sensör genişlik ve yükseklik bilgileri.

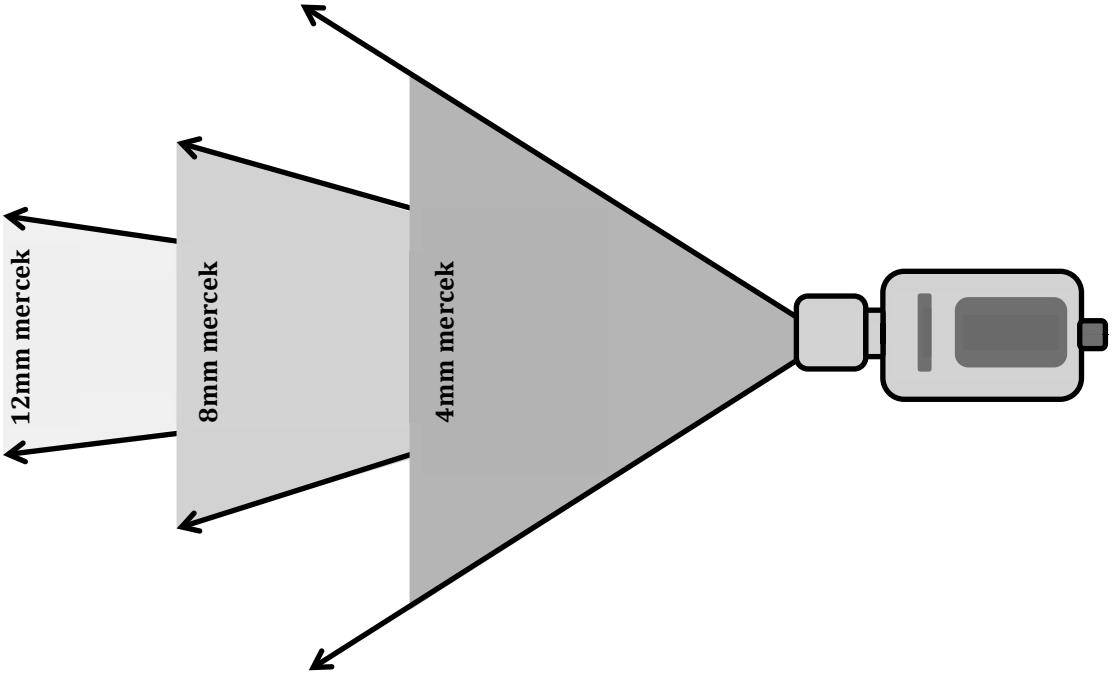
| Görüntü sensörü büyüklüğü (inç) | Genişlik (mm) | Yükseklik (mm) |
|---|---|---|
| 1/4 | 3.2 | 2.4 |
| 1/3 | 4.8 | 3.6 |
| 1/2 | 6.4 | 4.8 |
| 2/3 | 8.8 | 6.6 |
| 1 | 12.7 | 9.525 |

## Mercek (Lens)

Mercek kameranın gözüdür. Çoğunlukla camdan veya saydam plastikten imal edilen mercekler temel olarak iki ana fonksiyonu yerine getirir:

1. Odak uzaklığı sayesinde görüş alanı içinde olacak bölgenin büyüklüğünü belirler.
2. Diyafram açıklığı sayesinde görüntü sensörüne ulaşacak ışık miktarını belirler.

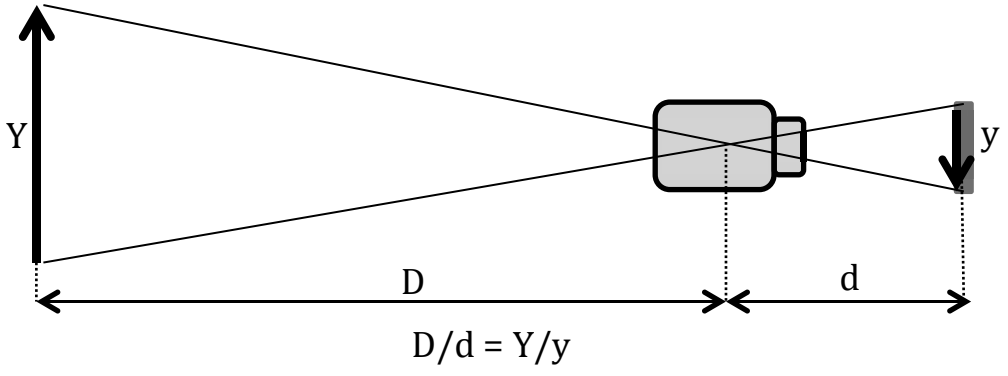
Merceğin odak uzaklığı, kameranın görüş alanı içinde olacak bölgenin genişliğini ve görüş alanı içindeki objelerin oluşacak görüntü üzerindeki büyüklüklerini belirler.




**Resim 5.6:** Mercek odak uzaklığına bağlı olarak kameranın görüş alanı.

Resim 5.6'da bir kameranın görüş alanı, kullanılan merceğin odak uzaklığına bağlı olarak betimlenmeye çalışılmıştır. Genel kural şöyle özetlenebilir: Odak uzaklığı büyüdükçe kameranın görüş alanı daralır, fakat görüş alanı içindeki objelerin görüntü üzerindeki büyüklükleri ve detayları artar. Tersinden ifade ile; odak uzaklığı küçüldükçe kameranın görüş alanı genişler, fakat görüş alanı içindeki objelerin görüntü üzerindeki büyüklükleri ve detayları azalır. Diğer bir deyişle, objeler kameradan daha uzakta görünürler.

Yakın ortam görüntülerinin arzu edileceği uygulamalarda 8mm veya 12mm gibi büyük odak uzaklığına sahip mercekler kullanılmalıdır. Kameranın geniş bir alanın görüntüsünü elde etmesi arzu ediliyorsa, 4mm gibi küçük odak uzaklığına sahip mercekler kullanmak daha uygun olacaktır.




**Resim 5.7:** En iyi görüntü için odak uzaklığının hesaplanması.

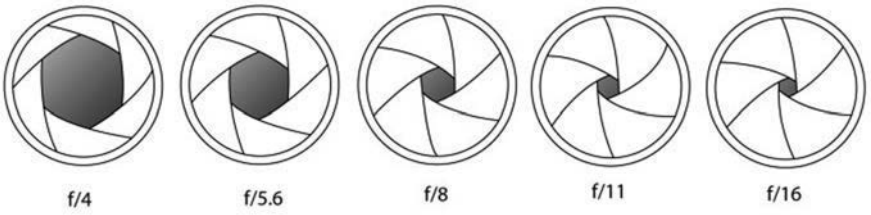
Belli bir bölgeyi gözlemlemesi için yerleştirilen bir kameranın merceği için en uygun odak uzaklığı, görüş alanındaki bir objenin görüntü üzerinde elde edilmek istenen büyüklüğü göz önüne alınarak hesaplanabilir. Resim 5.7'de kameraya D uzaklığında olan Y yüksekliğindeki bir objenin kamerada oluşacak görüntü üzerinde bütünüyle ve "y" büyüklüğünde görünmesi için gerekli olan "d" odak uzaklığı

betimlenmeye çalışılmıştır. Örnek olarak, Y=4.8m olan bir obje, D=12m uzaklıkta bulunsun. Eğer kamera 1/2 inç, yani 4.8mm, büyüklüğünde bir görüntü sensörü kullanıyorsa, o zaman merceğin odak uzaklığı "d" resimdeki formül kullanılarak d = D*(y/Y) = 12000*(4.8/4800) = 12mm olarak hesaplanır. Daha ufak odaklı bir lens kullanıldığında objenin tamamı yine görüntü içinde olacak, fakat daha küçük olacaktır. Daha büyük odaklı (mesela 16mm) bir mercek kullanıldığında ise objenin sadece bir kısmı görüntü içine girebilecektir.

CCTV sistemlerinde kullanlan kamera mercekleri odak uzaklık yapılarına göre üç kategori altında sınıflandırılabilirler:

1. **Sabit odaklı mercekler**: En basit mercek tipidir, bu sebeple en ucuz olan merceklerdir. Odak baştan sabitlendiği için, gözetlenecek bölgedeki arzu edilen görüntü alanı çok iyi hesaplanmalı ve odak uzaklığı hesaba uygun bir mercek seçilmelidir. Tipik sabit mercekler 30 veya 60 derecelik görüntü alanı sunarlar. 30 derecelik görüntü alanı dar olmakla birlikte belirli bir uzaklıktaki objelerin daha fazla detayını elde etmeye yarar. 60 derecelik görüntü alanı ise daha geniş bir alanın görüntü içine girmesini sağlar, fakat elde edilen görüntülerdeki detaylar daha az belirgindir.
2. **Değişken odaklı mercekler**: Odak uzaklıkları elle ayarlanabilen ve kullanıcıya kamera görüş alanı genişliğini belirleme imkanı sunan merceklerdir. Sabit odaklı merceklere göre daha pahalı olmakla birlikte daha ince görüntü ve görüş alanı ayarı yapılmasına olanak sağladıkları için daha popülerdirler. Bu tür mercekler sistem spesifikasyonlarının belirlenme aşamasını da kolaylaştırırlar; zira bu tür kameralar ile değişik görüş alanları elde etmek mümkün olduğu için, sistemdeki bütün kameralar için tek bir değişken odaklı mercek tipi seçilebilir. Sistem kurulumu sırasında merceğin odağı arzu edilen görüş alanını sağlayacak şekilde elle ayarlanır. Sabitlenen odak uzaklığını otomatik olarak değiştirmek mümkün değildir. Bunun için kullanıcının merceğe elle müdahale etmesi gerekecektir.
3. **Motorla odak uzaklığı değiştirilebilen mercekler**: En karmaşık mercek tipidir, fakat en esnek fonksiyonu sunarlar. Bu tür merceklerin odak uzaklıkları kurulumdan sonra bir uzaktan kumanda cihazı ile değiştirilebilir. Odak uzaklığı değişimi sırasında görüntü alanındaki objelere odaklanabilir. Bu sayede çok geniş bir alan tek bir kamera sayesinde gözetlenebilir. Korunan bölgeye bir sızma fark edilecek olursa, kontrol ve kumanda odasındaki güvenlik görevlisi kamera kontrol cihazını kullanarak failler üzerine kamerayı döndürebilir, kameranın odağını değiştirerek (yani zum yaparak) faillerin daha yakından görüntülerini elde edebilir. Bu tür mercekler genellikle kameranın da hareket ettirilebildiği çevir-eğ-odakla (PTZ) tipi kameralarda kullanılır.

Merceğin ortasında yer alan ve ışığın kamera içine girdiği deliğe diyafram denir. Diyafram kamera için insan gözündeki gözbebeğinin fonksiyonunu görür ve kamera içine girip görüntü sensörü üzerine düşecek ışık miktarını belirler. En uygun performans için görüntü sensörü üzerine ne çok az, ne de çok fazla ışık düşmelidir. Eğer diyafram çok açıksa ve gerektiğinden fazla ışık kamera içine girerse, üretilecek görüntünün bazı bölgeleri yıkanmış gibi bembeyaz olacaktır. Böyle bir durumu düzeltmek için diyaframı biraz kapatmak gerekecektir. Diğer taraftan, eğer diyafram çok kapalı ise ve gerektiğinden az ışık kamera içine girerse, üretilecek görüntünün büyük bölümleri simsiyah olacaktır ve sadece çok beyaz objeler görünür olacaktır. Böyle bir durumu düzeltmek için diyaframı biraz açmak gerekecektir.




**Resim 5.8:** Değişik f-dur değerleri için diyaframa açıklıkları.

**Diyafram** açıklığının büyüklüğü f-dur (f-stop) cinsinden ifade edilir. Resim 5.8'de değişik f-dur değerleri için diyafram açıklıkları gösterilmiştir. Görüleceği üzere, küçük f-dur değerleri daha açık diyaframlara, büyük f-dur değerleri daha kapalı diyaframlara karşılık gelir. Diğer bir deyişle, küçük f-dur değerlerinde kamera içine daha fazla ışık girer; büyük f-dur değerlerinde ise kamera içine daha az ışık girer.

CCTV sistemlerinde kullanılan kamera mercekleri diyaframlarının çalışma yapılarına göre 3 kategori altında sınıflandırılabilirler:

1. **Sabit diyaframlı mercekler**: Bu tür merceklerde diyafram açıklığı sabittir ve değiştirilemez. Bu tür merceklerin sabit ışık koşullarında kullanılması mümkün olmakla birlikte, değişik ışık şartları altında kullanılması mümkün değildir. Zira, kaliteli bir görüntü elde etmek için ortamdaki ışık miktarı değiştikçe, diyafram genişliği de değişmek zorundadır.
2. **Elle ayarlanan diyaframlı mercekler**: Bu tür merceklerde diyafram açıklığı sabit değildir ve elle değiştirilebilir. Daha çok sayısal fotoğraf makinalarında tercih edilirler. CCTV kameralarında diyafram genişliğini elle değiştirmek çok zahmetli bir iş olduğundan CCTV sistemlerinde kullanılan kameralarda pek tercih edilmezler. Eğer mevcutsa, bu tür diyaframa sahip mercekler çoğunlukla ışık miktarının sabit olduğu iç alan uygulamalarında kullanılabilir.
3. **Elektronik diyaframlı mercekler**: Bu tür merceklerde kameranın elektronik devresi görüntü sensörü üzerine düşen ışık miktarını sürekli örnekler ve ışık miktarına bağlı olarak diyafram genişliğini otomatik olarak açar veya daraltır. Işığın çok olduğu durumlarda diyafram genişliği otomatik olarak azaltılacak, ışığın az olduğu durumlarda diyafram genişliği otomatik olarak artırılacaktır. Bu tür diyaframa sahip mercekler değişken ışık koşullarında en iyi sonucu verir. Dolayısıyla, çoğu ticari CCTV kamerada bu tür mercekler kullanılmaktadır.

**Bir kameranın iç bileşenleri nelerdir?**

## Kamera Seçiminde Dikkat Edilecek Hususlar

Bir CCTV sisteminin amacına uygun olarak işlevini görebilmesi için uygun kamera seçimi çok önemlidir. Ticari olarak çok değişik özelliklere sahip kameralar olduğundan, doğru seçimi yapmak maliyetleri azaltmaya büyük katkı yapar. Bunun için kameraların nerede ve hangi koşullar altında kullanılacağını önceden belirlemek çok önemlidir. Baştan yapılacak yanlış tercihler ya gereğinden daha ucuz ve kötü kameraların alınmasına sebep verecektir. Böyle bir durumda kameralardan elde edilen görüntüler çoğunlukla faydasız olacaktır. Ya da gereğinden daha pahalı ve kaliteli kameraların alınmasına sebep verecektir ki böyle bir durumda gereksiz yere fazladan para ödenmiş olacaktır.

Bir CCTV sistemi için kamera seçiminde dikkat edilmesi gereken çok çeşitli unsurlar olmakla birlikte, aşağıda listelenen 3 unsur çok büyük önem arz eder:

1. Duyarlık (sensitivity)
2. Aydınlatma (illumination)
3. Çözünürlük (resolution)

Duyarlık; bir kameranın kullanılabilir ve anlaşılabilir bir görüntü üretmesi için gerekli olan minimum ışık seviyesini ifade eden bir kavramdır. Bir kameranın duyarlığı ne kadar yüksekse, kameranın kullanılabilir ve anlaşılabilir seviyede bir görüntü üretmesi için o kadar az ışığa ihtiyaç var demektir. Duyarlığı düşük bir kamera ise kullanılabilir bir görüntü için çok daha fazla ışığa ihtiyaç duyacaktır.

Kamera duyarlık değerleri kamera özelliklerinde "lux" cinsinden belirtilir. Dolayısıyla, bir kamera satın alırken kameranın hangi ışık koşulları altında çalıştırılacağı ve satın alınacak kameranın bu koşullarda kullanılabilir bir görüntü üretip üretemeyeği kamera duyarlık değerlerine bakılarak belirlenmelidir. Genel kural şöyle özetlenebilir: Ortam ışık seviyesinin belli bir değerin altına

düşmeyeceği iç ortam uygulamalarında kullanılacak bir kamera düşük duyarlıklı olabilir, yani duyarlık değeri yüksek olabilir. Fakat, ortam ışık seviyesinin değişken olduğu ve düşük ışık seviyelerinin mümkün olduğu dış ortam uygulamarında yüksek duyarlıklı bir kamera kullanılmalıdır. Örnek olarak, kızıl-ötesi ışıklara duyarlı bir gündüz/gece kamerası yıldız ışığı altında bile kullanılabilir görüntüler üretebilir. Fakat düşük duyarlıklı bir iç ortam kamerası böyle bir ortamda kullanılması ve anlaşılması imkânsız, hemen hemen simsiyah bir görüntü üretecektir.

Aydınlatma; görüntülenen alana düşüp yansıyan ışık miktarını ifade etmek için kullanılan bir kavramdır. Aydınlatma bir kamera fonksiyonu değildir, fakat gözetlenecek bölge için kullanılacak kamera seçiminde önemli rol oynar. Bildiğimiz gibi, ışık bir obje üzerine çarptıktan sonra yansır. Yansıyan ışık hüzmeleri kameranın merceğinden içeri girip görüntü sensörü üzerine düşer ve bu sayede görüntü oluşur. Gözetlenen ortamdaki ışık miktarı aynı olmakla birlikte yansıyacak ışık görüntülenen objenin yapısına göre farklı olacaktır. Mesela, görüntülenen objeler yansıtma özelliği yüksek olan kar gibi beyaz malzemeler ise kameraya çok ışık ulaşacak, objeler yansıtma özelliği az olan asfalt gibi siyah malzemeler ise kameraya az ışık ulaşacaktır. Dolayısıyla, belli bir duyarlık seviyesine sahip bir kamera, aynı seviye ışığının bulunduğu bir ortamda, görüntülenen objelerin yapısına göre farklı görüntüler üretecektir. Az yansıma yapan objeler daha karanlık, çok yansıma yapan objeler daha beyaz görünecektir. Az yansıma yapan objelerin görüntülendiği durumlarda tavsiye edilen şudur: Ortamı gözetleyecek kameranın duyarlık seviyesinin ortamdan yansıyan aydınlatma değerinin en az 10 katı daha fazla olması, kameranın kullanılabilir görüntü üretmesini sağlayacaktır.

Çözünürlük; bir kameranın ürettiği görüntünün detay miktarını ifade etmek için kullanılan bir kavramdır. Analog sistemler için bu değer televizyon satırları (Television lines - TVL) olarak ifade edilir. Sayısal sistemler için ise megapiksel olarak ifade edilir. CCTV sistemlerinde kullanılan kameralar genellikle 380 ila 540 TVL aralığında çözünürlüğe sahip görüntüler üretirler. Çözünürlük ne kadar yüksekse, elde edilen görüntünün detayları da o kadar belirgin olacaktır. Düşük çözünürlüklü kameraların ürettiği görüntülerin detayları daha az belirgin olacaktır. Bir kameranın çözünürlük değeri kamera özellikleri üzerinde açıkça yazılı olarak görülebilir. Uygulamanıza uygun çözünürlükte bir kamera seçimi önemlidir. Çünkü çok düşük çözünürlüğe sahip bir kamera kullanıldığı durumda elde edilen görüntü içinde hiç bir detay seçilemeyebilir. Bu da sisteminizi kullanışsız hale getirecektir.

## CCTV Sistemlerinde Kullanılan Kamera Çeşitleri

CCTV sistemlerinde kullanılan kameralar değişik şekil, büyüklük ve görünümlerde ortaya çıkmaktadır. Sistemde kullanılacak kameraların şekil bakımından seçiminde görünüm, estetik, kozmetik, kurulum kolaylığı ve yerleşim yeri gibi faktörler ön plana çıkmaktadır. Yoksa, hangi tip kamera kullanılırsa kullanılsın, kameradan elde edilecek görüntünün kalitesi sadece kameranın iç yapısı ve bileşenleri ile ilişkilidir. Aynı iç mimari ve bileşenlere sahip iki değişik tip kamera aynı kalitede görüntü üretecektir. Bu bölümde piyasada bulunan değişik tipdeki kameralar hakkında kısa bilgiler verilecektir.

### *Tavan Kameraları*

Tavan kameraları genellikle yarım küre şeklinde plastik bir koruyucu kapak içine yerleştirilerek bir tavana asılan kameralardır. Resim 5.9'da bir tavan kamerası örneği gösterilmiştir.

**Resim 5.9:** Bir tavan kamera örneği.

Bina dışındaki uygulamalarda kullanılmaları mümkün olmakla birlikte, özellikle bina içi kurulumları için en ideal kamera şekli olan tavan kameraları hakkında şunlar söylenebilir:

- Kurulumları en kolay olan kameralardır. Kurulumu gerçekleştirmek için kamerayı tavana 2-3 vida ile sabitlemek yeterli olacaktır.
- Tavan kameralarının üzerleri koruyucu bir kapak ile örtüldükleri için, kameranın bakış yönü dışarıdan bakan biri tarafından kolaylıkla belirlenemez. Bu da kameranın caydırıcılığını artırır.
- Kamera insanların erişimine yakın bir yerde dahi olsa, üzerindeki koruyucu kapak sayesinde çok kolay bir şekilde manipule ve tahrip edilemez. Koruyucu kapağın sert bir cisimden yapılmış olduğu durumlarda tahrip edilmesi daha da güçleşir.
- Tavan kameraları gece görüşü sağlayan kızıl-ötesi (infra-red) kameraları da saklayabilir.

## *Kutu Kameralar*

Kutu kameralar adından da anlaşılacağı gibi, kutu şeklinde bir kapak içine yerleştirilen ve bir askı aparatı ile birlikte bir duvara, çatıya veya direğe sabitlenen kameralardır. Resim 5.10'da bir tavan kamerası ve tavan kameralarının içine yerleştirildiği bir askı ve koruma aparatı örneği gösterilmiştir.

**Resim 5.10:** Bir kutu kamera ve kutu kamera askı ve koruyucu aparatı örneği.

Genellikle bina dışı uygulamalarda kullanılan kutu kameralar, güneş ışıkları, aşırı soğuk, yağmur, kar gibi kameraya zarar vermesi muhtemel olumsuz hava koşullarına karşı çoğunlukla koruyucu bir aparat içine konularak takılırlar. Resim 5.10'da bir kutu kameranın içine koyulabileceği örnek bir koruyucu aparat resmi verilmiştir. Piyasada çok değişik görünüm ve özelliklerde koruyucu aparatlar bulmak mümkündür. Kutu kameraların kullanımları hakkında şunlar söylenebilir:

- Duvara, çatıya, direğe veya bunlara benzer dikey bir yüzeye kurulum gerektiğinde kullanılmalıdır.
- Çok uzak mesafelerin görüntülenmesi gerektiğinde, büyük odak uzaklığına sahip mercekler kullanılması gerekmektedir. Büyük mercekler bir tavan kamerası kutusu içine genellikle sığmaz. Kutu kameraların koruma aparatları da kutu şeklinde olduğundan kullanılan mercek ne kadar büyük olursa olsun, koruma aparatı içine rahatlıkla sığar. Böyle durumlarda kutu kameralar kullanılması daha uygundur.

## *Kızıl-Ötesi Kameralar*

Çok az ışığın bulunduğu ortamlarda görüntü elde edebilmek için kutu kameraların ön kısımlarına, genellikle koruyucu aparat üzerine, çeşitli sayıda kızıl-ötesi led ışıkları yerleştirilerek elde edilen kameralardır. Kızıl-ötesi led ışıklardan faydalanabilmek için, kullanılacak kameranın kızıl ötesi ışınlara duyarlı olmasına dikkat edilmelidir. Aksi takdirde kızıl-ötesi led ışıklar bir işe yaramayacaktır. Resim 5.11'de örnek bir kızıl-ötesi kamera resmi gösterilmiştir.

**Resim 5.11:** Bir kızıl-ötesi kamera örneği.

Kızıl-ötesi kameraların görüş mesafeleri mevcut led ışıkların aydınlatma kapasiteleri ile doğru orantılıdır. Kesin olmamakla beraber, genel kural her led ışığın yaklaşık 33 cm uzaklığındaki görüntüsünün elde edilmesine olanak sağladığıdır. Buna göre, 30 tane led ışığı olan bir kamera ile yaklaşık 10 metre uzaklıktaki objelerin görüntüleri elde edilebilir. Kızıl-ötesi led ışıkların zaman içerisinde yandıkları ve değiştirilmeleri gerektiği akıldan çıkarılmamalıdır. Piyasada çok değişik türde ve kalitede kızıl-ötesi led ışıkları mevcuttur. Satın alınacak bir kameraya takılı led-ışıkların tür ve özelliklerini ayırt edebilmek maalesef çok zor bir iştir. Çoğunlukla kamera üreticisinin kutu üzerine yazdığı özelliklere güvenilmesi gerekecektir.

## *Çubuk Kameralar*

CCTV sisteminde kullanılacak kameraların ufak ve görünmesi zor olması istendiğinde tercih edilecek kamera tipidir. Resim 5.12'de bir çubuk kamerası örneği gösterilmiştir.

Resim 5.12: Bir çubuk kamera örneği.

Çubuk kameraların kullanımındaki asıl amaç insanlar tarafından fark edilmelerinin önlenmesi ve gizli kalmaları olduğundan genellikle kolayca fark edilmeyecek ve insanların kolayca ulaşmasının zor olduğu yerlere monte edilirler. Kızıl-ötesi led ışıklar kullanmaları mümkün olmadığından düşük ışık olan bölgelerde kullanılamazlar. Ayrıca küçük, genellikle silindir tipindeki kutular içine yerleştirildiklerinden kullanılan mercekler ve görüntü devreleri ufak ve kalitesizdir. Bu nedenle elde edilecek görüntü tavan ve kutu kameralara göre kalitesiz olacaktır.

## *Çevir-Eğ-Odakla (Pan-Tilt-Zoom PTZ) Kameraları*

CCTV sistemlerinin bazı uygulamalarında bir kameranın sadece sabit bir oryantasyonda durması ve baştan belirlenen belli bir alanın görüntüsünü vermesi yeterli değildir. Bazen kontrol odasındaki güvenlik görevlilerinin bir kontrol ve kumanda cihazı sayesinde kameralara müdahale ederek sağa-sola, aşağı-yukarı çevirmesi veya belli bir uzaklığa odaklanarak uzaktaki objelerin detaylarını görmesi istenebilir. Bazen de kameranın otomatik olarak, belli bir peryotla korunan bölgenin tamamını dolaşan hareketler yapması, tek bir kamera ile çok geniş bir alanın görüntünün elde edilmesine olanak verir ve caydırıcılık açısından daha etkili olabilir. Böyle durumlarda kameranın kurulumdan sonra hareket etmesi gerecektir.

Bu tür özellikleri bulunan kameralara piyasada Çevir-Eğ-Odakla (**Pan-Tilt-Zoom PTZ)** kameraları denilmektedir. Resim 5.13'de bir PTZ kamerası ve kamera kontrol-kumanda cihazı örneği gösterilmiştir.

**Resim 5.13:** Bir PTZ kamera ve PTZ kamera kontrol-kumanda cihazı örneği.

Resimden de görüleceği üzere kamera motorize bir düzeneğin üzerine yerleştirilmiştir. Bu motorize düzenek güvenlik görevlileri odasına yerleştirilen ve resimde gösterilen bir kontrol-kumanda cihazı sayesinde elle kontrol edilir. Bu sayede kontrol edilen bölge içinde bir alana doğru kameranın döndürülmesi, odaklanması ve detaylı görüntü elde edilmesi mümkün olacaktır.

PTZ kameraları kullanıcıya daha fazla kontrol vermekle birlikte, sabit kameralara göre 5 ila 10 kat daha pahalıdırlar. Sayısal IP PTZ kameraların kontrol mesajları kameranın bağlı bulunduğu ağ üzerinden gönderilebilirken, analog PTZ kameralarının güvenlik görevlileri tarafından kontrol edilebilmeleri için kontrol odasından kameraya kadar ayrı bir kontrol veri hattının çekilmesi gerektiği unutulmamalıdır. Bu da her analog PTZ kamera için ayrı bir kablo kurulması anlamına gelir. Bütün bunlar göz önüne alındığında, tipik bir CCTV sistemi kurulumunda kameraların büyük bir bölümü sabit kameralardan seçilmeli, sadece önemli bazı noktalardaki kameralar PTZ olarak belirlenmelidir.

## *Ethernet ve Kablosuz Sayısal IP Kameraları*

Ünitenin başında bahsettiğimiz gibi, yeni nesil sayısal CCTV sistemlerinde sayısal IP kameraları kullanılmaktadır. IP kameralar direkt olarak IP ağlarına bağlanmakta ve elde edilen görüntüleri sayısal olarak ağ kayıt cihazına aktarmaktadır.

Resim 5.14'de önü ve arkasıyla bir adet ethernet kamerası ve bir adet kablosuz IP kamerası resmi gösterilmektedir. Ortadaki resimden görüleceği gibi, Ethernet kamerası yerel IP ağına bir masaüstü bilgisayar gibi RJ-45 kablosu ile bağlanır ve ağ kayıt cihazı NVR'ye videoları bu arayüzden aktarır.


**Resim 5.14:** Bir kablolu IP kamerası ön ve arka yüzü, bir kablosuz IP kamerası örneği.

Ethernet kameralar çalışmaları için gerekli gücü ethernet kablosundan alabileceği gibi (buna Power over Ethernet – PoE denir), direkt olarak 12V veya 24V'luk bir elektrik adaptörü bağlanması ile de güç elde edebilirler. Örneğin, resimdeki ethernet kamerası bahsedilen her iki yöntemle güç alabilen bir kameradır. Resimdeki kablosuz IP kamerası ise kablosuz ethernet (WLAN) ağına bağlanabilen bir kameradır. Kablosuz kameranın ağa bağlanması dizüstü bir bilgisayarın kablosuz bir DSL modeme bağlanması ile aynı yöntemle çalışır. Ayrıca çok uzak mesafelerden görüntü elde edilmesi gerektiğinde kablosuz ethernet yerine videolu cep telefonu şebekesi 3G arayüzü kullanılabilir. Bu sayede, teorik olarak dünyanın herhangi bir yerindeki kablosuz bir kameradan görüntü elde etmek mümkündür.

Kablosuz IP kameraları genellikle pahalıdır. Fakat kameraya kadar kablo çekmenin zor veya imkansız olduğu durumlarda tercih edilebilirler. Örnek olarak, orman yangınlarını gözetlemek için orman bölgelerine yerleştirilecek kameralar bu tip kameralardan seçilebilir. Yalnız kameranın çalışması için bir güç kaynağına mutlaka ihtiyaç duyulduğu unutulmamalıdır. Güç problemini kablosuz olarak çözmek için bazı kablosuz IP kameraların pille çalıştıkları bilinmektedir. Fakat pil ömrünün çok uzun olmayacağı aşikardır. Pil ömrünün uzatılması için kameranın sadece korunan bölgede bir hareket olduğu zaman devreye sokulması veya saniyede 25/30 görüntü çerçevesi göndermek yerine 1-2 görüntü çerçevesi göndermesi tercih edilebilir.

### *USB Web Kameraları*

Çok ucuz bir CCTV sistemi kurulumu istendiği durumlarda, Web kameralarının kullanılması düşünülebilir. Resim 5.15'de ticari bir Web kamerası örneği gösterilmiştir.

**Resim 5.15:** Bir USB Web kamerası örneği.

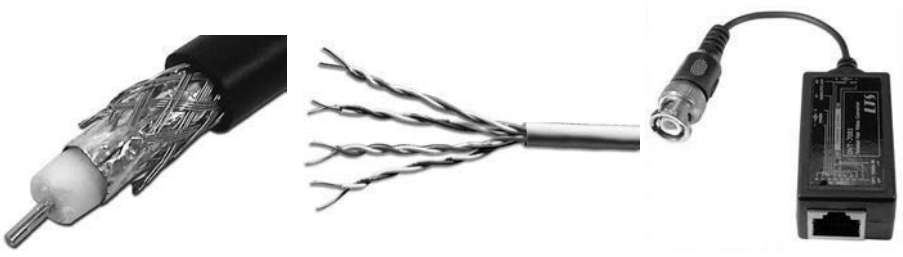
Web kameraları sayısal görüntü üretirler ve bir USB kablosu üzerinden video kayıt cihazlarına bağlanırlar. Web kamerası kullanan sistemlerde video kayıt cihazı olarak özel CCTV yazılımı kurulu bir masaüstü bilgisayar veya USB girişi olan bir DVR kullanılmak zorundadır. Web kameraları kullanarak çok ucuza 1-5 kameralı küçük CCTV sistemleri kurmak mümkündür.


**CCTV sistemlerinde kullanılan değişik kamera tipleri nelerdir?**

## İLETİŞİM VE GÜÇ KABLOLARI

CCTV sistemlerinde kameraların çalışması için gerekli enerjiyi kameraya iletmek için güç kabloları ve kameraların elde ettikleri analog veya sayısal görüntüleri sistemdeki video kayıt cihazlarına veya görüntü monitörlerine aktarmak için iletişim kabloları kullanılmak zorundadır. Kablosuz IP kameralardan sisteme görüntü aktarımı WLAN veya 3G gibi kablosuz ağlar üzerinden yapılmakla birlikte, CCTV sistemlerinde çoğunlukla kablolu iletişim kullanılmaktadır. Kablosuz IP kameraları pahalı olmaları sebebiyle sadece kamerayı kablo ile bağlamanın zor veya imkânsız olduğu durumlarda tercih edilirler.

Bir kamerayı CCTV sistemine bağlamak için kullanılacak kablolar kameranın tipi ile doğrudan ilişkilidir. Diğer bir deyişle, analog kameralar için farklı, sayısal IP kameraları için farklı, USB Web kameraları için farklı kablolar kullanılması kaçınılmazdır. Aşağıda, öncelikle CCTV sistemlerinde video iletişimi için kullanılan kablo çesitlerinden bahsedilecek, daha sonra kameralara güç iletimi yöntemleri üzerinde durulacaktır.



**Resim 5.16:** (soldan sağa) Koaksiyel kablo, UTP ağ kablosu, balun cihazı örneği.

Analog kameraların elde ettikleri görüntüleri sayısal video kayıt cihazlarına (DVR) aktarılabilmesi için her bir kameradan DVR'ye kadar uzanan bir kablo çekilmesi gerektiğinden bahsetmiştik. Bu tür kameraların bağlantısı için en çok kullanılan kablo çeşiti Resim 5.16'da gösterilen koaksiyel kablodur. Bir koaksiyel kablo, ortasından geçen bir iletken bakır kablo, onu yalıtan bir yalıtım ortamı ve en dışta bir kalkan malzemeden oluşur. İletimi sağlayan bakır kablo ile dıştaki kalkan malzeme aynı eksen üzerine yerleştirildiklerinden ve aynı elektriksel özelliklere sahip olduklarından bu kablo tipine dengeli (balanced) kablo da denir. Kamera bağlantıları için çoğunlukla RG-59 ve RG-6 ismi verilen iki çeşit koaksiyel kablo kullanılmaktadır. RG-59 için tavsiye edilen azami uzaklık 200 metredir. Daha pahalı olan RG-6 kullanılarak 100-150 metre daha uzun mesafelere bağlantı yapmak mümkündür. Kabloların uçlarına kameraya veya DVR'ye bağlanabilmeleri için BNC (Bayonet Neill Colcelman, British Naval Connector veya Bayonet Nut Connector) denilen bağlantı uçları takılır.

Son dönemde analog kameraların bağlantıları için koaksiyel kablo yanında Cat-5, Cat-5e veya Cat-6 denilen ve bilgisayarları ethernet ağlarına bağlamak için kullanılan ağ kabloları (Unshielded Twisted Pair - UTP) da kullanılmaktadır. Resim 5.16'da gösterildiği gibi, bir UTP ağ kablosu birbirine dolanmış 4 kablo ikilisinden oluşur. UTP kabloları koaksiyel kablolara göre hem daha hafifdir hem de çalışılması daha kolaydır. UTP kabloları ile tavsiye edilen azami kamera bağlantı uzaklığı 300 metredir. Bu tür kabloların uçlarına ethernet bağlantısı olarak bilinen RJ-45 takılır. Kameraların veya DVR'nin bağlantı uçlarının BNC olduğu göz önüne alıntığında, bir UTP kabloyu analog bir kamera veya DVR'ye bağlamak için "video balun" (BALanced UNbalanced) denilen bir cihaz kullanılması gerekmektedir. Resim 5.16'da bir video balun örneği gösterilmiştir. Görüleceği üzere video balunun bir ucu BNC, diğer ucu RJ-45 bağlantı ucu içermektedir. BNC ile DVR veya kameraya, RJ-45 ile UTP kabloya bağlantı gerçekleştirilir. Aktif video balunlar ve UTP kablolar sayesinde analog kameralar için 1000 metre uzaklığa kadar bağlantı gerçekleştirilebilir.

Sayısal IP kameraları ethernet ağlarına direkt bağlandıklarından, yukarıda anlatılan UTP tipi kablo ve RJ-45 bağlantı ucu kullanmaktadır. Bu tür kameralardan görüntü verisi sayısal olarak IP paketleri üzerinden sisteme aktarılır. Bu aktarım sırasında kullanılan TCP/IP protokolleri konumuz dışında olduğu için burada bahsedilmeyecektir. Daha fazla bilgi için bir bilgisayar ağları kitabına bakılabilir.


**Bilgisayar Ağlarının ve TCP/IP protokollerinin çalışma prensipleri hakkında daha fazla bilgi sahibi olmak için Alper Özbilen'in Pusula Yayıncılık tarafından basılmış "Bilgisayar Ağları ve Güvenliği" (2006) adlı kitabını okuyabilirsiniz.**

Son olarak, USB Web kameralarının veri iletimi bir USB (Universal Serial Bus) kablosu üzerinden olmaktadır. Bu tür kameralar IP kameraları gibi sayısal görüntü üretirler, fakat veri iletimini bir Cat-5

ethernet kablosu yerine USB kablosu üzerinden gerçekleştirirler. Bir USB kablo ile ulaşılabilecek azami uzaklık 5 metredir. Fakat USB çoklayıcılar kullanılarak bu mesafeyi 25 metreye kadar çıkarmak mümkündür.

Bir CCTV sisteminde kullanılan kameralar hangi tipte olursa olsun, çalışmaları için güce ihtiyaç duymaktadırlar ve gücün bir şekilde kameraya ulaştırılması gerekmektedir. Kameraya güç iletimi ayrı bir güç kablosu kurulması ile olabileceği gibi, bazı kameraların gerekli gücü direkt olarak veri kablosundan almaları, pil vasıtasıyla çalışmaları veya güneş enerjisi panelleri ile güç elde etmeleri mümkündür. Aşağıda, değişik kamera çeşitleri için güç iletiminin nasıl yapılabileceği hakkında bilgiler verilecektir.

Analog kamera kullanıldığı durumlarda veri iletimi için kullanılacak bir kablo yanında elektrik iletimini sağlayacak bir güç kablosu da kurulması gerekmektedir. Bu da her analog kamera için iki adet kablo kurulumu anlamına gelmektedir. Fakat, piyasada "Siamese" ismiyle bilinen ve hem güç hem de video kablosunu aynı örtü içinde taşıyan bir kablo çeşiti olduğu da bilinmelidir. Bu kablo sayesinde kameradan DVR'ye sadece bir kablo kurmak yeterli olacaktır.

Sayısal IP kameralarını bir güç kablosu ile çalıştırmak mümkün olduğu gibi, bazı IP kameraları çalışmaları için gerekli gücü direkt olarak Eternet ağından alırlar. Buna literatürde PoE (Power over Ethernet) denir. Bu tip kameralara ayrı bir güç hattı çekilmesine gerek yoktur. USB Web kameraları da çalışmaları için gerekli gücü çoğunlukla USB kablosu üzerinden alırlar. Fakat çok sayıda kızıl-ötesi led ışık kullanan IP veya USB kameraların ağdan aldıkları güç, led-ışıkların çalışması için yeterli olmayabilir. Bu durumlarda kameraların ayrı bir güç kablosu ile çalıştırılmaları gerekecektir.

Kablosuz IP kameraları çoğunlukla ayrı döşenen bir güç hattı ile çalışırlar. Çok az da olsa, bazı kablosuz IP kameraların uzun ömürlü piller veya güneş ışığı panelleri ile çalıştırıldıkları bilinmektedir.

# VİDEO KAYIT CİHAZLARI

Bir CCTV sisteminin en önemli bileşenlerinden biri video kayıt cihazıdır. Bir video kayıt cihazının görevi sistemdeki kameralardan gelen görüntü verilerini gün-saat-dakika-saniye-salise bilgisi ile işaretleyerek kayıt etmektir.

İlk CCTV sistemleri kayıt ortamı olarak video-teypler kullanmakta ve görüntüleri analog olarak kayıt etmekte idi. Tahmin edileceği üzere, elde edilen gerçek zamanlı görüntüleri saklayabilmek için çok sayıda video kaset gerekmekte idi. Bu sebeple kaydedilen görüntüler kısa bir zaman saklantıktan sonra silinmekte ve kasetler tekrar kullanılmakta idi. Kasetler sürekli olarak kullanılmaları sebebiyle bir süre sonra yıpranmakta ve bu da görüntü kalitesini çok büyük ölçüde düşürmekte idi.

Teknolojideki gelişmeler ile birlikte sayısal görüntü elde etmek kolay ve ucuz hale geldi. Bu sayede teyp kullanan analog kayıt sistemleri yerine sabit disklere kayıt yapan sayısal kayıt sistemleri ortaya çıktı. Bu tür sistemlerin en basitleri bir analog-sayısal çevirme kartı, geniş kapasiteli bir sabit disk ve özel CCTV yazılımı içeren bir masaüstü bilgisayarı video kayıt cihazı olarak kullanan sistemlerdir. Bilgisayardaki CCTV yazılımı analog kameralardan gelen görüntüleri analog-sayısal çevirme kartı sayesinde sayısal hale çevirir. Gerekirse az yer tutması için sıkıştırmaya tabi tutar ve sabit diske kayıt eder. Bütün kameralardan gelen görüntüler aynı zamanda bilgisayar ekranında ufak bir pencere içinde gösterilirler. USB Web kameralarının kullanıldığı durumlarda, kameradan USB arayüzü aracılığıyla gelen sayısal görüntüler direkt olarak sabit diske kayıt edilir ve ekranda gösterilir.


**Resim 5.17:** Sekiz kamera/ses girişi olan bir DVR cihazı ön ve arka yüzü.

CCTV piyasasının genişlemesi ile birlikte üreticilerin masaüstü bilgisayarın işlevini gören ve Sayısal Video Kayıt Cihazı (Digital Video Recorder - DVR) denilen özel kayıt cihazları ürettikleri görüldü. Resim 5.17'de ticari bir DVR'nin ön ve arka yüzü görülmektedir. Resimden de görüleceği üzere bir DVR üzerinde kamera ve ses bağlantıları için çok sayıda BNC giriş uçları bulunmaktadır. Verilen örnek DVR üzerinde 9 adet BNC ucu mevcuttur. Bunlardan 8 tanesi video/ses girişi, 1 tanesi video/ses çıkışı için ayrılmıştır.

VGA video çıkışına bir adet bilgisayar monitorü bağlanarak kayıt altına alınan videolar monitörde görüntülenebilir. Alternatif olarak, HDMI video çıkışına bir televizyon bağlanarak, kaydedilen görüntüler televizyonda da görüntülenebilir. DVR kayıt için bir veya birkaç adet sabit disk içermektedir. Toplam sabit disk kapasitesi genellikle 1000 GB veya daha büyüktür. DVR üzerinde ayrıca bir adet ethernet girişi vardır. Bu sayede DVR yerel ağa bağlanabilmekte ve ağa bağlı istemciler ile iletişime geçebilmektedir. DVR'ın ön panelinde bulunan düğmeler sayesinde değişik video kanalları seçilebilmekte, kayıt edilen videolar üzerinde ileri-geri gidilerek video analizleri yapılabilmektedir.

**Resim 5.18:** Yirmi IP kamerası ile iletişim kurabilen bir ağ kayıt cihazı (NVR) örneği.

Yeni nesil sayısal IP kamerası kullanan CCTV sistemlerinde video kayıt cihazı direkt olarak ağa bağlı olmak zorundadır. Bu tip kayıt cihazlarına Ağ Kayıt Cihazı (Network Video Recorder – NVR) denir. Resim 5.18'de ticari bir NVR örneği verilmiştir. Bu NVR Resim 5.3'de gösterildiği gibi direkt olarak ağa bağlanmakta ve IP kameralardan gelen sayısal videoları kayıt altına alabilmektedir.

Videolar H.264, M-JPEG, MPEG-4 gibi değişik video kayıt formatlarında saklanabilmektedir. Yukarıda gösterilen NVR azami 20 adet IP kamerası ile iletişime geçebilmektedir ve kayıt için 8000 GB kapasitesi olan sabit diskler içermektedir. Piyasada ticari ularak satılan ve azami 32 IP kameradan gelen video verilerini saklama kapasitesine sahip NVR'ler satılmaktadır. NVR'nin kapasitesi arttıkça fiyatı da doğal olarak artmaktadır.

# KONTROL KUMANDA MERKEZİ VE VİDEO GÖRÜNTÜLEME CİHAZLARI

Bütün CCTV kurulumlarında kameralardan gelen videoların görüntülendiği ekranlar bulunmaktadır. Bu ekranlar genellikle herkesin göreceği yerlere yerleştirilir. Bunun amacı hem sistemdeki kameraların çalışıp çalışmadığını gözlemlemek, hem de bölgenin kameralar ile izlendiğini göstererek muhtemel suçlulara karşı caydırılığı sağlamaktır. Büyük ölçekli kurulumlarda ise görüntülerin güvenlik görevlileri tarafından gerçek zamanlı izlendiği ve kameraların uzaktan kumanda edildiği bir kontrol kumanda merkezi mevcuttur.


**Resim 5.19:** Dört kameralı bir CCTV sisteminde kameralardan gelen videoların gösterildiği bir ekran.

Birkaç kameralı küçük ölçekli kurulumlarda genellike tek bir televizyon veya bilgisayar monitörü bütün kameralardan gelen videoları görüntülemek için yeterlidir. Çoğunlukla, ekran belli büyüklükte kare şeklinde kutucuklar olarak bölünür ve her kameradan gelen görüntü küçültülerek ekranda kendisi için ayrılan bölge gösterilir. Resim 5.19'da dört kameralı bir CCTV sisteminde kameralardan gelen videoların gösterildiği bir ekranın resmi örnek olarak gösterilmektedir.

Çok kameradan oluşan büyük ölçekli CCTV kurulumlarında ise, kameralardan gelen videoların çok sayıda ekranda görüntülendiği ve çeşitli sayıda güvenlik görevlisi tarafından gerçek zamanlı olarak izlendiği bir kontrol ve kumanda merkezi mevcuttur. Genellikle büyük holding merkezlerini korumak için yapılan kurulumlarda veya ülkemizde son yıllarda polis teşkilatları tarafından kullanılan mobese sistemlerinin kontrol, kumanda ve görüntüleme merkezleri bunlara örnek olaraka verilebilir.

**Resim 5.20:** Adana emniyet müdürlüğü mobese kontrol, kumanda ve görüntüleme merkezi. http://www.adana.pol.tr

Resim 5.20'de Adana emniyet müdürlüğü bünyesinde kurulmuş olan mobese kontrol, kumanda ve görüntüleme merkezinin "*www.adana.pol.tr/mobese-web.index.html*" sayfasından alınmış bir resim verilmiştir. Teşkilatın web sitesinde verilen bilgilere göre, sistem kentin stratejik öneme sahip değişik noktalarında kurulmuş olan, hareketli ve uzaktan kumanda edilebilen 51 adet kameradan oluşmaktadır. Resimden görüleceği üzere kameralardan gelen görüntüler sistem kontrol ve kumanda odasında çok sayıda bilgisayar ve televizyon ekranında anında gösterilmekte ve çok sayıda güvenlik görevlisi tarafından izlenmekte ve değerlendirilmektedir. Ayrıca, sistemde kullanılan bazı kameralar uzaktan kumanda edilebilen PTZ kameraları olduğundan, kontrol merkezindeki güvenlik görevlileri tarafından kumanda cihazları ile kontrol edilebilmektedir.

## Özet

Kapalı Devre Görüntü ve Kayıt Sistemleri (Closed Circuit TV – CCTV) çeşitli sayıda kameralar kullanılarak belirli bir bölgenin gözetlenebilmesi, elde edilen görüntülerin kayıt altına alınması ve video ekranlarında görüntülenmesine olanak sağlayan sistemlerdir. CCTV sistemlerinin kullanılma amaçlarını güvenlik, gözetleme ve denetleme olarak üç sınıfta toplayabiliriz. Güvenlik amaçlı uygulamalarda temel hedef caydırıcılık sağlayarak suç işlenmesine engel olmak ve kayıt altına alınan görüntülerin olay sonrası analizleri ile faillerin bulunmasına yardımcı olmaktır. Gözetleme amaçlı uygulamalar arasında otoyol ve tünellerdeki trafik akışının gözetlenmesi, insan kullanımının zor ve sağlık açısından tehlikeli olduğu endüstriyel uygulamalarda kameraların kullanılması sayılabilir. Denetleme amaçlı uygulamalara örnek olarak fabrika ve servis veren işyerlerinde çalışanların performanlarının ve yaptıkları işlerin gözetlenmesi sayılabilir.

Mimarilerine göre CCTV sistemlerini üç ana sınıfa ayırmak mümkündür. Analog sistemler en yaygın ve en uzun süredir kullanılan sistemlerdir. Bu tür sistemlerde çeşitli sayıda analog kamera koaksiyel veya UTP kablolar ile bir video kayıt cihazına bağlanırlar. Video kayıt cihazı olarak ya bir masaüstü bilgisayar yada sayısal video kayıt cihazı (DVR) denen özel bir cihaz kullanılır. Yeni nesil sayısal IP kamera CCTV sistemlerinde kameralar direkt olarak IP tabanlı bir yerel ağa bağlanırlar ve elde ettikleri görüntüleri sayısal olarak ağ üzerinden ağ kayıt cihazına (NVR) gönderirler. Bu tür sistemlerin analog sistemlere göre en önemli avantajı sistemin genişletilebilmesinin kolay olmasıdır. En büyük dejavantajı ise bu tür sistemlerin bir standartının bulunmaması, bu sebeple tek bir üretici firmaya bağımlı kalınmasıdır. Analog ve sayısal IP kameraların beraber bulunduğu karma CCTV sistemleri de mevcuttur. Bu tür sistemler eski nesil kameraların yeni nesil sistemlere entegrasyonunu kolaylaştırmaktadır.

Bir CCTV sistemi, kameralar, güç ve iletişim kabloları, video kayıt cihazları ve kontrol kumanda merkezi ve görüntüleme cihazları olmak üzere dört temel bileşenden oluşur.

Kameralar sistemin kalbidir ve doğru kamera seçimi kurulacak CCTV sisteminin amacına uygun olarak işlevini yerine getirebilmesi için son derece önemlidir. Kamera seçiminde sistemin kurulacağı bölgenin yapısal özellikleri, ışıklandırma durumu gibi çevresel özellikler dikkate alınmalıdır. Gerçekleştirilecek uygulama için gereğinden düşük özelliklere sahip kameraların seçilmesi, sistemden elde edilecek görüntülerin kullanılamaz ve anlaşılamaz olmasına sebep verecektir. Bu ise sistem için boşuna yatırım yapılmış olması anlamına gelecektir. Diğer taraftan, gereğinden fazla özelliklere sahip kameralar alınması, sistem için fazla para harcanmasına sebep olur. Bu ise maliyetlerin artması demektir.

Bir kamera temelde üç bileşenden meydana gelir. Mercek ortamdaki ışığın kamera içine girdiği bileşendir. *Odak uzaklığı* ayarı ile kameranın görüş alanını belirler. *Diyafram açıklık* ayarı ile kamera içine girecek ışık miktarını belirler. Kamera içine giren ışıklar, görüntü sensörü üzerine düşerler ve burada elektronik sinyallere çevrilirler. Elektronik sinyallere çevrilen görüntü kamera içinde elektronik devreler vasıtasıyla çeşitli işlemlerden geçirilir ve en kaliteli görüntü üretilmeye çalışılır. Üretilen görüntü video bağlantı ucu üzerinden alıcıya iletilir.

Kameralar analog ve sayısal olarak iki sınıfa ayrılırlar. *Analog kameralar* görüntüleri koaksiyel veya UTP ağ kabloları üzerinden video kayıt cihazına aktarırlar. Video kayıt cihazı gelen analog görüntüyü *analog-sayısal çevirme kartı* vasıtasıyla sayısal hale getirir; azla yer kaplaması için sıkıştırmaya tabi tutar, ve sabit-disk içinde saklar. *Sayısal kameralar* ise görüntüyü sayısal olarak alıcıya aktarırlar. *USB Web kameraları* görüntüyü USB kablosu üzerinden, *sayısal IP kameraları* ise görüntüyü UTP ağ kablosu üzerinden gönderir. Sayısal görüntüyü alan kayıt cihazı görüntüyü sıkıştırmaya tabi tutar veya direkt olarak sabit-diske kayıt eder.

CCTV sistemlerinde kullanılan değişik şekillerde kameralar mevcuttur. En çok kullanılan kameralar *tavan kameraları*, *kutu kameralar*, *çubuk kameralar*, *çevir-eğ-odakla kameraları*, *kablolu ve kablosuz IP kameraları* ve *USB Web kameraları* olarak sayılabilir. Bir CCTV sisteminde hangi tip kamera kullanılacağı sistemin kurulacağı bölge ile doğrudan irtibatlıdır. Genel olarak, iç bölge uygulamalarında tavan kameralar, çatı ve direk kurulumlarında kutu kameralar, uzak mesafeli kurulumlarda kablosuz kameralar kullanılır.

## Kendimizi Sınayalım

**1.** CCTV sistemlerinin kullanım alanları ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır**?

a. Belirli bir bölgenin güvenliğinin sağlanması için kullanılırlar.

b. Otoyol ve tünellerde trafik akışını gözetlemek için kullanılırlar.

c. Orman yangınlarını gözetlemek için kullanılırlar.

d. İnsanlar tarafından gözetimin zor veya imkansız olduğu bölgelerde kullanılırlar.

e. Sadece kalabalık insan topluluklarının olduğu bölgelerde kullanılırlar.

**2.** Aşağıdakilerden hangisi CCTV sistemlerinin avantajlarından biri **değildir**?

a. Gözetlenen bölgede suç işlenmesini engeller.

b. Daha az güvenlik personeli ile daha geniş bir bölgenin denetlenmesine olanak sağlar.

c. Kaydedilen görüntüler sayesinde suçluların bulunmasına yardımcı olur.

d. İnsan kullanmanın zor veya imkansız olduğu bölgelerin gözetlemesine olanak sağlar.

e. Potansiyel suçlulara karşı caydırıcılık teşkil eder.

**3.** Analog CCTV sistemleri için aşağıdaki ifadelerden hangisi doğrudur?

a. Analog CCTV sistemleri kurulduktan sonra hiç bakım gerektirmez.

b. Analog CCTV sistemleri sayısal IP CCTV sistemlerine göre daha ucuzdur.

c. Analog CCTV sistemleri uzun süre bozulmaz.

d. Analog CCTV sistemleri daha kaliteli görüntü üretir.

e. Analog sistemleri videoları analog olarak kayıt eder.

**4.** Karma CCTV sistemleri için aşağıdaki ifadelerden hangisi doğrudur?

a. Karma CCTV sistemleri en ucuz CCTV sistemleridir.

b. Karma CCTV sistemleri sadece analog kameralardan kurulur.

c. Karma CCTV sistemleri sadece sayısal IP kameralardan oluşur.

d. Karma CCTV sistemlerinde hem analog hem sayısal kameralar beraber kullanılabilir.

e. Karma CCTV sistemleri en kaliteli görüntü üreten sitemlerdir.

**5.** Aşağıdakilerden hangisi bir görüntü sensörü çeşididir?

a. CIS

b. ICD

c. CCD

d. VCD

e. IMD

**6.** Aşağıdaki kamera bileşenlerinden hangisi kamera içine giren ışık miktarını ayarlamak için kullanılır?

a. Odak uzaklığı

b. Diyafram açıklığı

c. Görüntü sensörü

d. Görüntü işleme devreleri

e. Video bağlantı ucu

**7.** Aşağıdaki kamera bileşenlerinden hangisi bir kameranın görüş alanını belirlemek için kullanılır?

a. Odak uzaklığı

b. Diyafram açıklığı

c. Görüntü sensörü

d. Görüntü işleme devreleri

e. Video bağlantı ucu

**8.** Aşağıdakilerden hangisi bir kamera tipi **değildir**?

a. Tavan kamerası

b. Kutu kamera

c. Çubuk kamera

d. Çevir-Eğ-Odakla kameraları

e. VP kameraları

**9.** Analog kameraları video kayıt cihazlarına bağlamak için hangi kablo tipi kullanılır?

a. Telefon kablosu

b. Video kablosu

c. Balun

d. Koaksiyel kablo

e. Görüntü kablosu

**10.** Kablolu IP kameraları yerel ağa bağlamak için aşağıdaki kablo tiplerinden hangisi kullanılır?

a. UTP

b. Koaksiyel kablo

c. Video kablosu

d. Fiber optik kablo

e. Balun

## Kendimizi Sınayalım Yanıt Anahtarı

**1. e** Yanıtınız yanlış ise "Giriş" başlıklı konuyu yeniden gözden geçiriniz.

**2. a** Yanıtınız yanlış ise "Giriş" başlıklı konuyu yeniden gözden geçiriniz.

**3. b** Yanıtınız yanlış ise "Kapalı Devre Görüntü ve Kayıt Sistemlerinin Genel Yapıları ve Bileşenleri" başlıklı konuyu yeniden gözden geçiriniz.

**4. d** Yanıtınız yanlış ise "Kapalı Devre Görüntü ve Kayıt Sistemlerinin Genel Yapıları ve Bileşenleri" başlıklı konuyu yeniden gözden geçiriniz.

**5. c** Yanıtınız yanlış ise "Kameralar" başlıklı konuyu yeniden gözden geçiriniz.

**6. b** Yanıtınız yanlış ise "Kameralar" başlıklı konuyu yeniden gözden geçiriniz.

**7. a** Yanıtınız yanlış ise "Kameralar" başlıklı konuyu yeniden gözden geçiriniz.

**8. e** Yanıtınız yanlış ise "Kameralar" başlıklı konuyu yeniden gözden geçiriniz.

**9. d** Yanıtınız yanlış ise "İletişim ve Güç Kabloları" başlıklı konuyu yeniden gözden geçiriniz.

**10. a** Yanıtınız yanlış ise "İletişim ve Güç Kabloları" başlıklı konuyu yeniden gözden geçiriniz.

## Sıra Sizde Yanıt Anahtarı

### *Sıra Sizde 1*

Kapalı devre görüntü ve kayıt sistemleri (CCTV) çeşitli sayıda kameralar kullanılarak belirli bir bölgenin gözetlenebilmesi, elde edilen görüntülerin kayıt altına alınması ve video ekranlarında görüntülenmesine olanak sağlayan sistemlerdir. Bu sistemler temel olarak güvenlik, gözetleme ve denetleme amaçlı kullanılırlar.

### *Sıra Sizde 2*

Temel olarak üç çeşit CCTV mimarisi mevcuttur: Analog sistemler, sayısal IP kamerası kullanan sistemler ve karma sistemler.

### *Sıra Sizde 3*

Bir kamera temel olarak üç bileşenden oluşur: Mercek ışığın kamera içine girdiği bileşendir. Odak noktası ayarı ile kameranın görüş alanını, diyafram açıklık ayarı ile kamera içine giren ışık miktarını belirler. Görüntü sensörü kamera içine giren ışığın elektronik sinyallere çevrildiği ve görüntünün oluştuğu bileşendir. Elektronik devreler ise görüntü sensöründe oluşan görüntünün çeşitli işlemlerden geçirilerek optimize edildiği bileşendir.

### *Sıra Sizde 4*

CCTV sistemlerinde çoğunlukla kullanılan kamera tipleri şunlardır: Tavan kameraları, kutu kameralar, çubuk kameralar, çevir-eğ-odakla kameraları, kablolu ve kablosuz IP kameraları, USB web kameraları.

## Yararlanılan Kaynaklar

Pearson, R.L. (2007). **Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions**, Butterworth-Heinemann, Elsevier.

## Yararlanılan İnternet Kaynakları

en.wikipedia.org/wiki/Closed-circuit_television (2011), Closed-circuit television.

www.popcenter.org (2011), A Review of CCTV Evaluations: Crime Reduction Effects and Attitudes Towards its Use.

www.dipolnet.com (2011), Architecture of video surveillance systems based on IP networks.

www.boshsecurity.us (2011), Selecting the Right CCTV Camera.

www.aventuracctv.com (2011), Camera Tutorial.

www.aventuracctv.com (2011), Analog vs. IP Cameras.

# 6

## Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Elektronik çevre güvenlik sistemlerini anlatabilecek,
- İç ve dış ortamdaki dedektörlerini özetleyebilecek,
- İnsansız hava araçlarının fonksiyonlarını açıklayabilecek

bilgi ve becerilere sahip olabilirsiniz.

## Anahtar Kavramlar

- Elektronik
- Güvenlik Sistemleri
- Algılayıcılar
- Kapı Dedektörleri
- Sesüstü Dedektörler
- Kızılötesi Dedektörler
- Foto Elektrik Dedektörler
- İnsansız Hava Araçları

## İçindekiler

# Elektronik Çevre Güvenlik Sistemleri

## GİRİŞ

Elektronik çevre güvenlik sistemi, güvenliği yapılacak yerin veya bölgenin çevre korumasını elektronik cihazlarla sağlayan sistemdir. Çevre güvenlik sisteminin kurulması, iç ve dış dedektörler, davetsiz misafir girişi algılama yeteneğine sahip özel kablo döşeli tel örgüler, toprak altı elektronik algılama, mikrodalga, kızılötesi, sesüstü, foto elektrik, lazer, kapı, cam kırılma dedektörlerinden biri veya bir kaçının kullanımı şeklinde olabilmektedir.

Güvenlik sistemlerinin kalitesi, uygun dedektör seçimi ile başlar. Dedektörlerin seçimi, onların gücüne ve uygulama alanlarına göre seçilmelidir. Çoğunlukla dedektörler çalışmak zorunda oldukları çevre için daha az dikkatle kurulur. Sonuç olarak güvenlik sistemi sürekli sıkıntılı alarmlardan muzdarip olacaktır ve daha da kötüsü aradığını bulamayacaktır. Herhangi bir güvenlik dedektöründen beklenen amaçlar; fiyatının uygun olması, yüksek güvenilirlikli çalışması, sızma girişimlerini bulabilme başarısının yüksekliği, düşük yanlış alarmları şeklinde sıralanabilir. Bütün dedektörler bu amacın tamamını karşılayamazlar. Fakat dedektörlerin güçlü oldukları taraflarını anlayarak, dedektörleri doğru ortamlarda kullanarak, mantıklı beklentiler ile istenen sonuçlar alınabilir. Bu bölümde iç ve dış güvenlik dedektörleri incelenecektir. Güçlü ve zayıf, çevre konuları ve gerçek hayat problemleri açıklanacaktır.

Elektronik sistemlere ek olarak bu ünitede, son günlerde sıkça sınır bölgelerinde kullanım haberleri verilen insansız hava araçlarından (İHA) bahsedilecektir. İnsansız hava araçları, kendi kendine veya yer istasyonundan komut ve rota bilgilerini alarak uçabilen, taşıdıkları dedektörler ve kameralar ile davetsiz misafirleri tarayabilen sistemlerdir. Algıladıkları veriler yer istasyonunda veya kendileri tarafından işlenmektedir. Davetsiz misafir tarandığı anda alarm üretebilmektedir.


**Dikkat çevrenizde hangi elektronik güvenlik sistemleri var?**

## DIŞ ÇEVRE DEDEKTÖRLERİ

Bir binanın verilen bir alanının bütününün taranması için güvenlik sistemi tasarlanması istenebilir. Bu tasarım probleminin en önemli sorunu, bütün davetsiz misafirler için böyle bir tasarım yapmanın neredeyse imkânsız olmasıdır. Ortalama maliyet ile kurulan bir güvenlik sistemi, istenmeyen misafirlerin sıradan sızma girişimlerini %90 bulabilmektedir. Tam başarı elde edilmek istenildiğinde, daha büyük kurulum maliyeti gerekir. Bunun için, belirlenen bölgenin taramasının gerçekçilik olasılığını (PD) belirlemek gerekir. Bu da bazı testler ile öznelliğin katılmasıyla mümkündür. Yani gereken test tipinin oluşturulmasında biraz öznellik ve sayısallaştırmaya ihtiyaç vardır. Örneğin, amacımız iki katlı binanın ikinci katındaki bilgisayar odasındaki davetsiz misafirlerin bulunma olasılığını bulmak olsun. Tavandaki kızılötesi hareket tarayıcısı ile tarama gerçekleştirilsin. İlk adım, davetsiz misafirlerin taranacak alana girmesinin yolları tanımlanır. Örneğin, korunan alanda davetsiz misafirlerin yürüyebildiklerini veya koşabildiklerini kabul edelim. Tabii ki davetsiz misafirler tavandan aşağıya doğru, yuvarlanarak, sürünerek veya benzeri başka yollarla bilgisayar odasına gelebilir. Her bir faaliyet, davetsiz misafirin gerçekte bu faaliyetle fiziksel olarak bilgisayar odasına ulaşma olasılığı olarak ağırlıklandırılır. Örneğimizde, yürüme ve koşma muhtemel faaliyettir. Bu faaliyetler %45 olasılıkla davetsiz misafir

tarafından kullanılabilir. Davetsiz misafirin %90 olasılıkla yürüyerek veya koşarak bilgisayar odasına erişebildiği kabul edilmektedir. Özetle, diğer faaliyetler Tablo 6.1 deki gibi ağırlıklandırılmalıdır.

Her faaliyet verilen sayı kadar test edilmelidir. Sonuçlar % olarak tabloya eklenmelidir. Her faaliyetin 10 defa test edildiğini kabul edelim. Yürüme test sonuçları zamanın %95'inde davetsiz misafiri tarıyorsa, tabloda testin bulunduğu sütüna eklenecektir. Her faaliyet test edilmeli ve sonuçlar test sütününa yazılmalıdır. Gerçek PD değerini bulmak için, her faaliyet yatayda çarpılmalı ve PD sütununa yazılmalıdır, PD sütunundaki değerler toplanmalıdır. Yürüme örneğimize geri dönersek, sızma girişimlerinin %45'inde davetsiz misafirin yürüyerek bölgeye geleceği beklenmektedir. Test sonuçlarındaki %95 tarama yürüme faaliyeti ile çarpılarak tablodaki PD sonucu 0.43 bulunur. Her faaliyet bu şekilde çarpılarak PD değerleri tabloda hesaplanır. Sonuçta PD sütunundaki değerler toplanır. PD sütunundaki %91 PD değeri davetsiz misafirin bizim kabullenmelerimiz altında bilgisayar odasına girmeye çalışırken taranabileceğini, hareket tarayıcısının ve yerinin seçilebileceğini göstermektedir.

**Tablo 6.1:** PD Tablosu

| Faaliyet | Olasılık | Test | PD |
|---|---|---|---|
| Yürüme | 0.45 | 0.95 | 0.43 |
| Koşma | 0.45 | 0.95 | 0.43 |
| Sürünme | 0.05 | 0.05 | 0.03 |
| Çatıdan giriş | 0.05 | 0.04 | 0.02 |
| | | | **0.91** |


**Tarama alanını %100 yapmak için ne yapılabilir?**

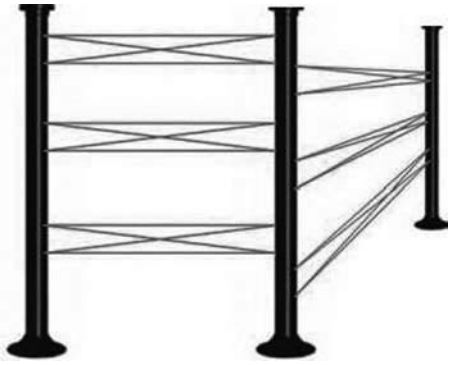
Tarama % 100 PD değerine ulaşmadığı için, "PD değeri nasıl iyileştirilebilir" sorusu akla gelmektedir. PD'yi iyileştirebilmenin birçok yolu vardır. Aynı tip dedektörlerden birden fazla ekleme, farklı dedektör teknolojilerini birlikte kullanma veya bazı giriş faaliyetlerini sınırlandırma bu yollardan bir kaçıdır. Bilgisayar odasının girişine kapı anahtarı ilave edilebilir. Tavandan veya çatıdan yapılacak sızma girişimlerini önlemek için tedbirler alınabilir. Amaç PD'yi en ekonomik şekilde %100'e yakınlaştırmaktır. Belli bir güvenlik tasarımı sonunda, PD'yi % 100 yapmanın ekonomik olmadığı ya da ne yaparsak yapalın PD'yi % 100 yapmanın mümkün olmadığı anlaşılabilir. Verilen bir bölge için PD'nin %100 olamayacağı beklentisi mantıklı olabilir. Toplam taramaya yaklaşmak mümkün olabilir, fakat maliyet % 100 taramaya değer mi, değmez mi buna kuruluş yöneticileri karar verecektir.

Alarm tarayıcılarının seçimine binanın dışı ile başlanacaktır. Yaygın dış tarama teknolojilerinden birisi mikrodalgadır. Aktif cihazlar olan mikrodalga tarayıcılar iki sınıfta değerlendirilirler. İlk tip **mono statik** mikro dalga sistemlerinde gönderici ve alıcı aynı kutunun içindedir. Mikrodalga cihaz kutusundan yayılacak şekilde alan üretir. Bu alan bozulduğunda, alarm çıkış rölesi aktifleşir. İkinci tip, **çiftli statik** cihazda ise gönderici ve alıcı ayrıdır. Alıcı gönderici tarafından üretilen alanı gözetler. Bu alan bozulduğunda, alarm rölesi aktifleşir. Resim 6.1'de çiftli statik gönderici görülmektedir. Desen veya alan, futbol topunun şekline benzeyen bu mikrodalgalar tarafından üretilmektedir. Elektronik alan, büyük ölçüde dikeyde ve yatayda yayılmaktadır.

**Resim 6.1:** Mikrodalga Tarayıcı

Bu cihazların en önemli avantajı, taranmaksızın içinden veya üzerinden geçmek zordur. Arazi düzgün değilse bu cihazlar atlatılabilir. Davetsiz misafir aşağı seviyeden sürünerek ve elektronik alanın altından saptanmadan başarılı bir şekilde geçebilir. Ayrıca karlı havalarda, karın altından saptanmadan geçmek mümkündür.

Kızılötesi ışınlar diğer aktif dış tarayıcı tipidir. Bu cihazlarda gönderici ve alıcı ayrı ayrıdır. Gönderici alıcıya kızılötesi ışın gönderir. Alıcı tarafında engellenen veya engellenmeyen bir ışın varsa, alarm çıkış rölesi etkin olur. Bu cihazlar normalde birçok gönderici ve alıcıyı kullanmak için, Resim 6.2'deki gibi üst üste konur. Bu yaklaşım kızılötesi tel örgü olarak düşünülebilir. Kızılötesi tarayıcılar, birçok casus veya hareketli resimlerde bulunmaktadırlar. Fakat genellikle bina içi uygulamalarda görülmektedirler. Kızılötesi ışınlar, gönderici ve alıcıları bağlayan görünmeyen kablolara benzemektedir. Bu üst üste konmuş cihazlar çok verimlidir. Fakat mikrodalga gibi tarayıcı olarak kulanılmak istenildiğinde, aynı amaç için uygun düzenleme isterler. Yağmur ve sis bu tarayıcı tipini etkiler. Kızılötesi lensinin içindeki yoğunlaşma yanlış alarmlara neden olur.



**Resim 6.2:** Kızılötesi Dedektör

Açık alan dedektörlerinin diğer bir grubu da gömülü düzende çalışan dedektörlerdir. Bu dedektörlerin depremsel, depremsel/manyetik, koaksiyel bağlantılı ve fiber optik çeşitleri vardır. Her biri kendisi ile ilgili teknolojiyi kullanır. Örneğin, gömülü fiber optik kablo ile sürekli gönderilen sinyal, fiber optik teknolojisini kullanır. İstenmeyen misafir gömülü kabloya adım attığı zaman, kablo yavaşça fiber içinde kırılıcak ve üzerindeki elektrik akımı kesilecektir. İstenmeyen misafiri gösteren bu kesinti ile fibere gönderilen sinyal etkilenecektir. Gönderen cihaz optik zaman alan yansıması ölçme (ODTR) temeliyle sinyal gönderir. ODTR, gönderilen sinyal ile fiber optik kablodan yansıyarak gelen sinyali karşılaştırır, kesintiyi algılar, kesintinin olduğu yerin mesafesini bulur. Güvenlik kontrol merkezi sadece zorla içeriye girildiğini değil, aynı zamandan nereden zorla girildiğini de operatöre söyler. Bu cihazların tipik alan

büyüklüğü diğer dedektör tiplerine ve kapalı devre televizyonun (CCTV) kapsadığı alana bağlı olarak 100 metredir. Bu cihazların alan büyüklüğü büyük veya küçük olabilir.

Diğer bir gömülü dedektör de istenmeyen misafirin yürüyerek veya koşarak gömülü dedektörden geçerken sismik etkisine göre çalışır. Mekanik olarak gerildiğinden elektrik akımı üreten basınç dedektörünün kullanımı ile yapılabilir. İstenmeyen misafir gömülü dedektöre doğru yürüdüğünde veya yaklaştığında gerilim üretilir. Diğer gömülü cihazlar gibi istenmeyen misafir bölgeden geçerken elektriksel alan üretirler. Sızıntı kablo olarak adlandırılan birçok farklı kablo tipi, bu sistemde vardır. Kablolar; merkezinde iletken, etrafında yalıtkan, koruma ve koruyucu yelekten oluşan standart koaksiyel kablolardan yapılmaktadır. Bu tip kablolar ile benzer konfigürasyonlu diğer kablolar arasındaki fark, koruma iletkenin merkezinden geçen akımın neden olduğu, kaçan veya yayılan manyetik alana izin verecek boşluğu olan bir tasarım ile yapılmaktadırlar. Sonuçta oluşan elektronik alan istenmeyen misafir gömülü kabloya yürürken veya üzerinden geçerken bozulacaktır.

Sismik harekete göre sızma girişimini belirleyen diğer bir tasarım

da gömülü dengeli basınç detektörleridir. Bunlar, iki bölgenin ortasında algılama cihazı olarak vardır. Gömülü hatlara istenmeyen misafir yaklaşıncaya kadar her bölgedeki basınç aynıdır. Hatların birindeki basınç arttığında, istenmeyen misafir algılanmış olur. Kablolar arasındaki alanı ve iki kabloyu kullanan gömülü kablo da vardır. Gömülü kablo Resim 6.3 de görülmektedir.

Gömülü dedektörlerin avantajı görünmezler ve bölgeyi çok iyi takip ederler. Görmek güçtür ve çok doğal görünen bölgenin korunmasına izin verirler. Bu cihazlar genellikle yüksek güvenlik uygulamaları veya görünümün kritik olduğu uygulamalarda kullanılır. Örneğin, bir uygulama olarak herhangi bir kuruluşun faaliyet bölgesinde, güvenliğin görünmeden sağlanması amacı için kullanılabilir. Bu cihazlar farklı toprak ortamlarında farklı davranırlar. Bu yüzden testleri kritiktir. Hendek tabanı, dolgusu ve derinliğinin belirlenmesi hendek inşaası için gereklidir. Cihazlar verilen bir alanda uygun çalışma için test edilmelidir. Üreticisi veya temsilcisi yeni kurulumla ilgilenmelidir. Birçok defa gömme derinliği toprak şartlarına göre değişmektedir. Hendekte kayaların veya diğer atıkların olmadığı belirlenmelidir. Bu dedektörler tak ve kullan cihazları değildir. Bu dedektörlerin kurulumu, çalışma alanının hazırlanması ve sıkıntı oluşturabilecek muhtemel durumların azaltılması için özen gerektirir. Mikrodalga, kızılötesi ve gömülü dedektörler genellikle boş veya kontrol edilebilen bitkilerin bulunduğu açık alanlarda kullanılır.

**Resim 6.3:** Gömülü kablo sistemi

Çift tel örgünün kullanıldığı yüksek güvenlik uygulamaları da ilave dedektör teknolojileri ile PD'nin arttırılması için kullanılmaktadır. İç tel örgü; gergin tel, elektrik alanı, sığa, basınç, coğrafi haberleşme dedektörleri gibi montaj edilebilen olası birçok dedektör tipinden oluşabilir. Tel örgü dedektörlerinin sabit bir tel örgü üzerinde olması istenmektedir. Tel örgü üreticilerinden üretim ve sonrasında bu şartları sağlamaları ve bu sayede yanlış alarmların azaltması beklenmektedir. Tel örgü üretimi test edilmeli ve yanlış alarm problemlerini azaltacak her durum için tekrar gerilmelidir. Bu dış dedektörler bir defa kurulup unutulmazlar. Bunlar devamlı bakım gerektirirler. Tel örgü direği kalıcı olması için betonla montajı yapılır. Eğer tel örgünün hareketine izin veriliyorsa veya üretimden kaynaklanan esnekliği fazla

ise, yanlış alarmların oranı istenilmeyecek kadar yüksek olacaktır. Dış dedektörlerin çalışma ortamı çok görülü olamayacaktır.

Bu bölümde, tel örgü dedektör teknolojilerinin ve uygulama yollarının örneklerine elekrik alanı (X-alan) dedektör örneği ile başlanacaktır. Bu dedektörde üç veya daha fazla ayrı kablo kullanılır ve ayrı veya ay şeklinde güneşlenen tel örgüde paralel çalıştırılır. Üç kablo sisteminde, bir kablo tel örgünün üstünde, bir tanesi ortada, bir tanesi de aşağıya yakın bir yerdedir. Orta kabloda, kendisi ile üst ve alt kablo arasında elektrik alanı üretecek şekilde sinyal vardır. Davetsiz misafir kablolara yaklaşırken elektrik alanı engellenir ve bu engelleme alarmın üretilmesine neden olur. X-alan dedektörü Resim 6.4'te görülebilir.

Sığa tel örgü dedektör sistemleri, elektronik alan sistemlerine benzer şekilde sadece dedektör teknolojisi olarak kablolar arasındaki sığayı kullanarak çalışırlar. Davetsiz misafir tel örgüye yaklaşınca sığa değişir ve alarma neden olur. Gergin tel üstteki her anahtardan geçen gergin telden oluşan anahtarlar dizisini kullanır. Davetsiz misafir tel örgüyü keser veya tel örgüye tırmanırsa, gergin tel yönünü değiştirecek ve anahtarları aktif yapacaktır. Teknolojik olarak diğer farklı bir tel örgü sisteminde elektrik, bobinin içinden geçen mıknatıstan oluşmaktadır. Mıknatıs hareket ettiğinde elektrik akımı üretilir ve alarma neden olur.

**Resim 6.4:** X-alan Dedektörü

Bahsedilen dış dedektörler genellikle davetsiz misafirler için "dinleme" veya geliştirilen sinyallerin elektronik kontrolleri şeklinde uygulanmaktadır. Davetsiz misafirin dedektörü çalıştırması bir nevi ilk anahtar açma-kapama olarak düşünülebilir. Gerçek alarm genelde davetsiz misafir içteki elektronik devrelerce belirlendiğinde olur. Buna rağmen birçok kuruluş gömülü dedektörler kullanarak davetsiz misafirin sızma girişiminde bulunduğunu yeri ile birlikte gösteren sistemleri kullanmaktadırlar. Açık alan dedektörleri yüksek güvenlik uygulamaları için tel örgü dedektörlerinin birleşimi ile yaygın olarak kullanılır. Verilen alanda değişik teknolojilerin beraber kullanılması, davetsiz misafiri doğru bir alarmla fark edeceği ve alarmın geçerliliğini arttıracağı için bu yaklaşım daha olumlu taramaya izin verir

Dış alarm sistemleri ile beraber düşünülen bazı temel tedbirler de vardır. Dış dedektör kullanıldığında alarm alanını görebilmek için kapalı devre televizyon (CCTV) sistemi ilave edilmesi önemlidir. Dış ortamda muhtemel birçok yanlış alarmlar olacaktır. Alanı görebilme ile davetsiz misafirin alarma neden olduğu ihtimali değerlendirilir. CCTV olmadan, her alarm güvenlik açısından değerlendirilmesi gereken ciddi bir durum olarak ele alınacak ve müdahele yapılacaktır. Bu yüzden gelen alarmın doğruluğunu CCTV ile kontrol etmek, yanlış alarmlardan kaynaklanan gereksiz iş yükünü azaltacaktır.

Diğer bir tedbir de aydınlatmanın iyileştirilmesidir. Kablolar toprağın altına gömülse bile, aydınlatma ile kablolara verilen yüzlerce hattaki elektrik birbirini etkileyecek ve elektromagnetik etkileşim (EMI) olacaktır. Bu da birçok elektronik bileşenin zarar görmesine neden olacaktır. Bu zararın önlenebilmesi ve elektronik bileşenler ile dedektörlerin sorunsuz çalışması için, elektronik alan paneline veya düzgün güç sağlayıcılara gerek olacaktır. Genel kural olarak, aydınlatma koruması ile bir kablonun dışarıdan binanın içerisine getirilmesi önerilir. Bunun yanında aydınlatma ve farklı alternatif akımlar (AC) için kaçak akım röleleri kullanılmaktadır.

Çevreyi kontrol etmek için diğer bir önlem ise yanlış alarmları en aza indirmek için alınacak ilave tedbirlerdir. Bu tedbirler şunlardır:

- Hayvanların detektörlere ulaşmaması ve yanlış alarma sebep olmaması için tel örgüler sıklaştırılmalıdır. Fakat bu kuruluşlara ek masraf getirecektir.
- Suyun toplanmayacağı veya göl olmayacağı uygun kazım teknikleri kullanılmalıdır. Mikrodalga sinyalleri suyun göl olması ile farklı yönlere enerjinin yayılmasına ve sinyal dizisinin değişimine neden olacaktır.
- Gömülü dedektörlerin yakınındaki büyük ağaçlar şiddetli rüzgâr ile sallandığında yanlış alarmlara neden olacaktır. Sallanma ağaç köklerine baskı yapacaktır. Bu da birçok gömülü dedektör teknolojilerinde davetsiz misafir olarak görülecektir. Bunun için dedektörlerin ağaçlardan uzak bölgelere yerleştirilmesi gerekir.

Her dedektör tipinin yanlış alarmları en aza indirebilecek ve en yüksek PD'yi sağlayacak güçlü ve zayıf tarafları vardır. Teknoloji ne kadar gelişmiş olursa olsun, kurulan dış çevre sistemlerinin yanlış alarm vermesi mümkündür. Bunun önlenmesi için dikkatli planlama yapılmalıdır. CCTV ile dış dedektör uygulamalarının birlikte kullanılması gerekir ve koordinasyonun iyi sağlanması başarılı bir güvenlik sisteminin oluşturulması için çok önemlidir.

# İÇ ÇEVRE DEDEKTÖRLERİ

İç çevre dedektörleri deyince aklımıza bina çevresini kuşatan tel örgü ya da duvarların hemen iç kısmında yer alan dedektörler aklımıza gelmelidir. Çevre güvenlik sistemlerinin başarılı olabilmesi için, diğer bir deyişle yüksek PD değerine sahip olabilmeleri için iç çevre dedektörlerle uyum içerisinde çalışmaları gerekir. 2. Ünite'de iç çevre dedektörleri, elektronik alarm sistemleri olarak ayrıntılı bir şekilde anlatılmıştı. Fakat bu bölümde dış çevre birimleri ile uyumlu bir şekilde kullanılmaları açısından, gerekli bilgilerin verilmesi gerektiğinden tekrar ele alınmıştır. Burada anlatılacak iç dedektörler üç temel grupta ele alınacaktır:

1. Kapı dedektörleri
2. Hareket dedektörleri
3. Cam kırılma dedektörleridir

Her dedektör grubunun avantajları, kullanım kısıtları ve nasıl çalıştıkları tek tek incelenecektir.

## Kapı Dedektörleri

En basit şekilde kapı anahtarı iki parçadan oluşmaktadır: dokunan röle ve mıknatıs. Mıknatıs hareket eden kapının üstüne takılır. Dokunan röle sabit kapı çerçevesine takılır. Mıknatıs dokunan röleye yaklaşınca, dokunan rölenin yaklaşmasına ve elektrik akımının akmasına neden olur. Mıknatıs düşeyde ve yatayda dokunan röle ile aynı hizada olmalıdır. Mıknatısın dokunan röleye ilk teması ile fiziksel mesafe arası, kapı anahtar aralığı olarak tanımlanır. Kapı dedektörleri farklı aralıklar için satın alınabilir. Geniş aralık kullanmanın nedeni kapının kendi kendine daralma ve şişmesine ve bunun yanında kapı çerçevesi için de kapının doğal hareketine izin vermektir. Kapı kapalı iken anahtar bu hareket tiplerinde kapalıdır. Garaj veya çekilen kapılar, büyük kapı dedektör aralığı ile bilinir. Garaj kapılarındaki dokunan role, genellikle ağır alüminyum kutu içinde garajın tabanında veya üzerinden geçildiğinde zarar görmeyecek bir yerdedir.

Daha karmaşık ve güvenli kapı anahtarı dengeli mıknatıs anahtarı (DMA) olarak bahsedilir. DMA birkaç dokunan röle ve mıknatıstan oluşur. Mıknatıslar, dokunan röleleri kapalı olacak şekilde uygun hizada yerleştirilmiştir. Mıknatısların kutuplarının ve mıknatıs paketinin DMA için yapıldığı düşünülmüştür. Gerçekte mıknatıs paketi ve dokunan röle bileşenleri uygun çiftler olarak satılır. Bir mıknatıs parçası farklı diğer bir mıknatıs parçası ile yer değiştirilirse güvenilir çalışmayabilir. Bu cihazlar yüksek güvenlik gereksinimi olan kapılarla birlikte kullanılır. Veri merkezlerinde, kritik, yüksek para depolama alanlarında veya erişime kapalı devlet alanlarında sıklıkla kullanılır. Dört adet montaj deliği

vardır ve iki parça vida ile birleştirilir. Yüksek güvenlik bölgelerinde DMA'yı montaj etmek için kullanılan vidalar özeldir ve takılmaları için özel araç gerekir. Özel güvenli vida, özel güvenli tornavida olmadan çıkarılamaz. Bu özel tornavida toplam güvenliğe kurulumda ilave katkı sağlar.

## Hareket Dedektörleri

### *Kızılötesi Hareket Dedektörleri*

Bu gruptaki iyi bilinen dedektör kızılötesi hareket dedektörüdür. İç kızılötesi hareket dedektörleri pasif cihazlardır. Pasif kızılötesi dedektörler enerji üretmezler. Onlar gördükleri alanda bulunan kızılötesi enerjiyi saptarlar. Kızılötesi enerji ısıdır ve insanlar ısı üretirler. İnsan derisinin dış sıcaklığı yaklaşık 32 ºC ve oda sıcaklığı ise 22 ºC'dır. Aradaki fark fazla olduğu için hareketli bir kişi sıcak nokta olarak çabucak bulunabilir. Ayrıca odada 22 ºC olan bir kişi saptanmayabilir. Bu durumda başka bir hareket dedektörü kullanılabilir. Sıcaklık kontrolu olmayan bölgeler veya depolarda bu çözüm gereklidir. Bu dedektör hem ısıya hem de harekete bakmaktadır.

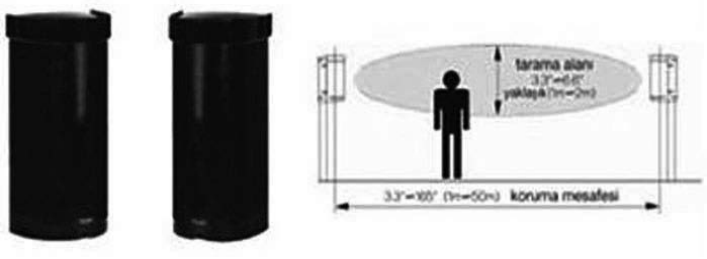
Kızılötesi dedektörler, ısının frekansına duyarlı kızılötesi enerjiye odaklanan Freznel mercek kullanırlar. Mercek korunan alanı elinizdeki parmaklar gibi birkaç bölgeye ayırır. Her bölge daha hassas dedektör sağlamak için çeyreklere bölünmüştür. Davetsiz misafir bir bölgeyi geçmek zorundadır. Bölgedeki belirli sayıdaki çeyrekler algılamayı temin edecektir. Bu yaklaşım hayvanların neden olduğu yanlış alarmları azaltmaya yardım edecektir. Kızılötesi dedektörler dikey dar duvar taramasını da desteklemektedir. Bu kapsama, sıklıkla perde olarak adlandırılır. Birçok üretici kendi dedektörlerini Freznel mercekleri ile değiştirerek parmak düzeninden perde düzenine veya tam tersine geçmişlerdir.

Bölgenin büyüklüğü, 6 ayak uzunluktaki bir kişiyi, en uzak noktadan algılayacak kadar olmalıdır. Örneğin tarama düzeni 30'a 30 ayak bir alan için yapılacaksa, 6 ayak uzunluktaki bir kişi, detektörden 30 ayak uzaktaki bir mesafeden taranabilir. Dedektör 30 ayaktan daha uzakta bulunan davetsiz misafiri hala tarayacaktır. Fakat davetsiz misafir 6 ayaktan daha büyük olmalıdır. Bu fare ve fil hikâyesidir. Fil 30 ayaktan çok uzakta olsa bile taranacaktır ve fare dedektörden 1 ayak uzakta olsa taranabilecektir. Bu hedef bilgisi kızılötesi, hareket dedektörü kullanıldığında dikkate alınmalıdır.

Diğer bir konu da kızılötesi enerji malzeme içine işlemeyecektir. Örneğin, kızılötesi dedektör cam pencerenin diğer tarafındaki davetsiz misafiri taramayacaktır. Bir parça kâğıt dedektörün önüne yerleştirildiğinde davetsiz misafir taranmadan herhangi bir yere gidecektir. Birçok üretici dedektörlerine bu yolla yanlış sinyalleri güvenlik komuta merkezi operatörüne ileten elektronik kabiliyet eklemiştir. Bu elektronik kabiliyet dedektöre yakın küçük kızılötesi düzeni ile sıklıkla gerçekleşebilmektedir. Parlak ışıklar ve hayvana bağışıklık gibi diğer ilaveler yapılarak cihazlar daha güvenilir yapılabilmektedir.

### *Mikrodalga Hareket Dedektörü*

Mikrodalga iç hareket dedektörünün diğer bir çeşitidir. Mono statik dış mikrodalga gibi aynı şekilde çalışır. Bu cihazlar düşük seviyede mikrodalga enerji ürettikleri için aktiftir. Kızılötesi ve mikrodalga dedektör arasındaki önemli farklardan bir tanesi mikrodalga dedektör nesnelerin içinden yayılır. Resim 6.5'te mikrodalga dedektörü görülmektedir.




**Resim 6.5:** Mikrodalga Hareket Dedektörü

Bu dedektörlerin sorunsuz kullanılmasında yerleştirileceği yer çok önemlidir. Örneğin, şirket yöneticisine ait iç büro mikrodalga hareket dedektörü kullanılarak korunuyorsa, koridordan yürüyerek yandaki büroya gelen biri alarma neden olacaktır. Duvardaki PVC atık su borusundan geçen su alarm verebilir. Mikrodalga dedektörler mükemmel hacimsel cihazlardır. Diğer teknolojiler gibi sınırları vardır.

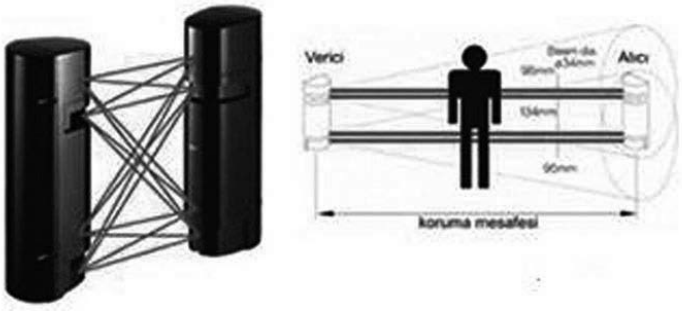
## *Sesüstü Hareket Dedektörleri*

Sesüstü hareket dedektörleri Doppler kaymaya bakan aktif cihazlardır. Doopler kayma gözleyici veya sisteme ulaşan dalganın frekansındaki değişimdir. Genel örnek tren ıslığının duyulabilen frekans değişimidir. Tren size yaklaşınca frekansı azalır. Sesüstü hareket dedektöründe, frekansı gönderme ve davetsiz misafiri gösteren frekans kaymasını kontrol eden birim birlikte bulunmaktadır. Frekans insan kulağının duyabileceğinden daha büyük fakat mikrodalga dedektörlerde kullanılan frekanstan çok daha azdır.

Frekans üreten birimler de yanlış alarmlar üretebilirler. Örneğin havada asılı duran gıcırdayan bir kemer yanlış alarma sebep olabilir. Bir insan havada asılı duran gıcırdayan kemerin ürettiği tüm frekansları değil, bazı frekansları duyabilir. Bu örnekte üretilen frekanslar sadece bizim duyabileceğimiz frekanslar değil, onların harmonik ve alt harmonik frekansları da vardır. Bunları duyamayız, fakat bunlar sesüstü hareket dedektörünü etkileyecektir. Harmonik ve alt harmonik frekanslar temel frekans bileşeninin katlarından oluşmaktadır. Üretilirken her harmoniğin yarısının sinyal büyüklüğünde azalma vardır.

## *Foto Elektrik Dedektörler*

Foto elektrik dedektörler daha önce anlatılan dış kızılötesi ışın dedektörlerine benzerler. Genellikle bir gönderici ve bir alıcıdan oluşan aktif çift statik cihazlardır. Gönderici alıcı tarafından taranan kızılötesi bir ışın üretir. Davetsiz misafir korunan alana geldiğinde, göndericinin ışını kırılır ve alarm üretilir. Resim 6.6 görüleceği gibi ışın yeterince dardır. Bu yüzden davetsiz misafir ışının üzerinden sıçrayabilir veya ışının altından sürünebilir. Davetsiz misafir dedektörün yerleştirildiğinin farkına varmadığı için çoğu zaman ışın dedektörleri diz seviyesinde montaj edilir. Tipik foto elektrik dedektörün ışını görünmez ve dedektörler yeterince aşağıya montaj edilir. Bununla beraber çoklu gönderici ve alıcı üniteleri dış dedektörlerdekine benzer üst üste konacak şekilde satın alınabilir. Ayrı çoklu üniteler benzer şekilde aynı sonuçları elde etmek için kullanılabilir.




**Resim 6.6:** Foto elektrik dedektör

## *Lazer Alan Dedektörleri*

Lazer alan dedektörleri, korunan bölgeyi kapsamak için çok ince görünmeyen lazer duvarı veya perdesi üreten aktif cihazlardır. Bu cihazlar farklı birçok uygulamada kullanılır. Fakat ortak uygulama alanı bir müze olabilir. Duvarda pahalı bir tablo olduğunu ve korunması gerektiğini kabul edelim. Lazer alan dedektörü duvardaki tablonun önünde pahalı sanat eserinden birkaç cm uzakta tarama sağlayabilir. Fakat tablonun toplam kapsama alanına destek veremez. Birisinin tabloyu alması, tabloya dokunması veya

yakıp yıkmayı denemesi lazer duvar tarafından engellenmek zorundadır. Bu yüzden güvenlik kontrol merkezindeki sunucuya veya bilgisayara ya da elektronik alan paneline hemen alarm gönderebilmektedir.

### *Çift Teknoloji Dedektörü*

Hareket dedektör tiplerinin varyasyonu çift teknoloji dedektörüdür. Cihaz alarm durumuna geçmeden önce, iki teknolojinin de birbirini tamamlaması hedeflenmektedir. Bu yaklaşımın avantajı, her iki teknoloji de davetsiz misafiri taramak zorunda olduğu için, yanlış alarmları mümkün olduğu kadar azaltmaktır. Genelde çift teknoloji hareket dedektöründe kızılötesi ve mikrodalga kullanır. Önceki örneği tekrar ele alacak olursak, duvardaki atık su borusundan su akıyorsa mikrodalga dedektörü hareketi tarayacak ve davetsiz misafir olarak düşünecektir. Fakat kızılötesi hiç bir şey görmeyecektir. Kızılötesi enerjinin olmama sebebi, duvarda alçıpan tarafından tutulmasıdır. Bu durumda, her iki teknoloji de davetsiz misafiri taramadığı için yanlış alarm yoktur.

## Cam Kırılma Dedektörü

Cam kırılma dedektörü, kırılan camın frekansını taradığı için farklı tarama yaklaşımıdır. Camın kırılma frekansı genellikle 4 ile 6 kilohertz (kHz) arasındadır. Cama vurulduğunda, oluşan kırık camın frekansının süresi, frekansı ve aniden olması taranır. Cam kırıldığında, belirgin bir ses veya kırılan camın frekans aralığına ayarlanmış, frekans filtreleri olan tarayıcı ile kontrol edilebilecek frekanslar üretir. Cam kırılma dedektörleri genlik, süre ve 4 ile 6 kHz frekansları arasındaki aniden olmayı ölçer ve bütün bileşenler hazır olduğu zaman alarmı aktive eder. Bu dedektörler, korunacak pencerenin üstündeki tavana monte edilir. Pencereye olan mesafe duruma gore değişebilir. Fakat cam kırılma dedektörü 10 metre mesafede olan kırılmayı algılar. Dedektör cam ile dik açı yaptığında güvenilirlik değişecektir. Bu dedektörlerdeki sıkıntılı alarmların ana kaynağı aydınlatma veya daha doğrusu aydınlatma ile birlikte gök gürültüsüdür. Gök gürültüsünün vurgusu camı tıkırdatacaktır ve hem ses dalgası hem de bu dedektörleri tetikleyecek frekanslara neden olacaktır.

Aynı tip cam örneğinin gerçekten kırılması veya elektronik cam kırılma benzetimi ile cam kırılma dedektörleri test edilebilir. Farklı cam tiplerinin ürettiği frekanslar değişiktir. Üç temel cam çeşidi vardır. Evlerde veya eski binalarda kullanılan düz camdır. Kalınlığı camın kapladığı alana göre değişebilir. Düz cam kalınlığı tipik olarak 6.35 milimetredir. İkinci çeşit sertleştirilmiş veya katılaştırılmış camdır. Sertleştirilmiş cam kırıldığında büyük parçalar halinde kırılır. Sertleştirilmiş cam binlerce parçaya kırılamaz, kesilemez veya delik açılamaz. Cama yapılacak herhangi bir işlem sertleştirilmeden önce yapılmalıdır. Yukarıda belirtildiği gibi, binlerce küçük parçaya ayrılarak cam kırıldığında düz cam plakadan farklı frekans cevapları üretir. Sertleştirilmiş cam güvenli iki cam tipinden biridir. Modern arabalarda camın çoğu sertleştirilmiş camdır. Cam çok etkili dayanıklıdır ve çok küçük parçalar halinde kırılırsa, aracın içindeki kişilere daha az zararlıdır. Birisi arabaya kırarak girerse, kenar pencerenin ortasını delerek yapacaktır. Pencerenin ortasını delme bu cam tipinin en zayıf noktasına (aşırı küçük noktaya) var olan kuvveti üretir. Üçüncü cam tipi kat kat yapılan (laminat) güvenli camdır. Laminat camda iki veya daha fazla sıradan cam tabakası kullanır. Cam tabakaları plastiğe benzeyen polimer ile ayrılmıştır. Cam kırılacaktır. Fakat cam parçacıkları polimere yapışık halde kalacaktır. Araba ön camları bu cam tipinden yapılmaktadır. Eski arabalarda ön camın yanı sıra bütün camlarda, bu cam tipi kullanılırdı. Eski arabalarda bu eski camların kenarlarında küçük balonlar görebilirsiniz. Bu hava balonları, bu iki parça camın arasındaki laminatın zamanla bozulmasından kaynaklanmaktadır. Üç farklı cam tipinin karakteristikleri ve farklı tekniklerine bağlı olarak, cam parça parça kırıldığında frekanslarının farklı olacağı açıktır. Bu nedenle cam dedektörünün test edilmesi ve gerekiyorsa ayarlanması gereklidir.

Diğer bir cam kırılma dededektör tipi camın fiziksel olarak üstüne montaj edilen tipidir. Bu dedektörler etki tip dedektörlerdir. Kullanılan farklı teknikler vardır. Çoğunlukla basınç kullanılır. Fakat hepsi kırıldığı zaman camın sallanmasına dayanmaktadır. Bu cihazlar, kullanılan camın tipine göre test edilmelidir. Yanlış alarmların sayısı, cihazın camın neresine montaj edildiğine (Camın köşeleri en iyi yerlerdir.) ve camı destekleyen çerçeve tipine bağlıdır. Bu cihazların diğer cam kırılma dedektör tipleri gibi genellikle hassas ayarları vardır. Bu dedektörlerin, diğerlerinden farklı olarak, camın üstüne montajı yapılmak zorundadır. Elektronik alan paneli üzerindeki bölgeye kablo ile bağlandığı zaman pencereye

erişim uygun olmak zorundadır. Genelde yeni yapılarda kullanılmaktadırlar. Cihazlar kablosuz olabilir. Cam kırılma dedektörü var olan yapıda kullanılıyorsa, çoğu zaman tavana monte edilir.

# İNSANSIZ HAVA ARAÇLARI

Türkiye, coğrafi konumu ve stratejik önemi nedeniyle geçmişten beri çeşitli tehditler altındadır. Bunlara son dönemlerde sınır ülkelerde olan olumsuz gelişmelerin de eklenmesiyle, buralarda eğitilen teröristlerin gerçekleştirdiği terörizm faaliyetleri en belirgin sorun olarak ortaya çıkmaktadır. Türkiye'de terör faaliyetlerinin sürmesinin temelinde sınır geçişlerinin kontrol zayıflığı ve buna bağlı faaliyetler yatmaktadır. Doğrudan terör amaçlı gerçekleşen sınır ihlallerinin yanı sıra, terörün finansmanı için yasak maddelerin kaçakçılığı ve insan kaçakçılığı da bu yolla yapılmaktadır. Sınırların kontrolünün güç olmasının en belirgin iki nedeni coğrafik zorluklar ve bölgenin genişliğidir. Sınırdaki bu istenmeyen faaliyetlerin azaltılması, terör olaylarının azaltılmasında önemli bir etkendir.

Son yıllarda sınır karakollarına düzenlenen saldırıların önüne geçilmesi ve daha az riskle sınırların güvenliğinin sağlanması için insan gücünün dışında teknolojik imkânlardan da yararlanmak önemli hale gelmiştir. Bu teknolojilerden beklenen, sınır bölgelerine giriş ve çıkışların gözetim altında tutulabilmesi, bir ileriki adımda etkili müdahale ile bu bölgelerde kontrol sağlanmasıdır. Bu bağlamda sınır devriyesinin etkili bir biçimde yapılması önem kazanmaktadır. Bölge şartları itibariyle bu devriye görevi en etkin şekilde havadan yapılabilir. Yapılacak gözlem uçuşları ile sınırdaki değişiklikler görsel olarak veya ısı değişikliklerinin tespiti ile takip edilebilir. Uydu kullanımına göre daha esnek ve geniş kullanım kabiliyeti olan uçaklarla bu görevin gerçekleştrilmesi daha etkili olacaktır. Yapılacak devriye uçuşlarının, sürekli olması gerektiğinden, daha az riskli ve daha az masraflı insansız hava aracı (İHA) teknolojisiyle yapılmasının daha etkin olacağı açıktır. Bu sistem insansız hava aracı ve yer sisteminden oluşmaktadır. İnsansız hava aracı ve yer ünitesi arasında haberleşme ile aracın kontrolü yapılabilmekte ve araç üzerindeki faydalı yükler olarak adlandırılan dedektörler yardımıyla veriler alınmaktadır. Bu veriler işlenerek alarm üretilmekte, yeni rota verilebilmektedir.

İnsansız hava aracı kullanımı dört bölümde incelenebilir; mini, taktik, stratejik ve deneysel sistemler. Mini sistemler sırtta taşınabilir özellikte olup hızlı ve kısa menzilde etkin bir kullanıma sahip ve ucuz insansız hava araçlarıdır. Taktik sistemler kısmen taşınabilir olup en çok ve etkin kullanılan sistemlerdir. Stratejik sistemler uzun süre yüksek irtifada görev yapabilme özellikleri ile en fonksiyonel ve bu yüzden de edinilmesi en maliyetli sistemlerdir. Bugün haberlerde sıkça duyduğumuz İsrail'den alınan Heronlar bu sınıfta insansız hava araçlarıdır. Bir de askeri tatbikatlarda yüksek hızda hedef olarak kullanılan deneysel İHA sistemleri mevcuttur.


**Türkiye'de insansız hava araçlarında yapılan çalışmalar var mı?**

Türkiye'de de insansız hava araçları ile ilgili çalışmalar son yıllarda artmaktadır. Bu konudaki öncü kuruluşlardan birisi TUSAŞ'dır. Bu kuruluşun taktik amaçlı geliştirdiği ANKA projesi ile ilgili şu haber 3 Kasım 2011 tarihinde Milliyet Gazetesi'nde yer almıştır:

"*İsrail, yerli ANKA'yı gökte görünce...*

*Yerli insansız hava aracı ANKA test uçuşunu başarıyla tamamlayınca panik yapan İsrail elinde tuttuğu 6 Heron'dan 4'ünü anında geri gönderdi. ...*

*Heronlar konusunda sürekli sorun çıkaran İsrail, yerli insansız hava aracı ANKA test uçuşunu başarıyla tamamlayınca panik yaptı. İsrail elinde tuttuğu 6 Heron'dan 4'ünü anında geri gönderdi.*
*Yerli İnsansız Hava Aracı ANKA'nın 10 bin feet testini başarıyla geçmesi ve aktif görev için 2012'de Hava Kuvvetleri'ne tahsis edileceğinin açıklanması üzerine, İsrail elinde tuttuğu 6 Heron'dan 4'ünü acele geri gönderdi.*

*Başbakan Recep Tayyip Erdoğan, İsrail'in sözleşme gereği bakımını yapması gereken Heronları aylardır vermediğini açıklamıştı. Dışişleri kaynakları İsrail'in Heronları acil olarak*

*vermesinin, ANKA Projesinin hızlı ilerlemesinde rehavete yolaçma çabasıyla ilişkili olabileceğini belirtirken, ASELSAN yetkilileri yavaşlama olmaması konusunda uyarıldı. Ayrıca özel firmalarca yürütülen İHA projelerinin askıya alınmaması için de gerekli uyarıların yapıldığı ifade ediliyor. İsrail, Heron sürecini sürekli yeni gerekçelerle uzatmış ve Milli Projeler yaklaşık 10 yıl sekteye uğramıştı.*

*Üçüncü ülke gerilimi*

*Heron sisteminin bütünüyle İsrail tarafından yapılmış olması ciddi endişeler oluşturuyor. Elde edilen görüntülerin anlık ve canlı olarak İsrail'e de gittiği, TSK'nın iç emir komuta sistemi içerisinde görüntülerdeki PKK'lıları vurma talimatı çıkmadan Irak'ın Kuzeyine haber verildiğinden şüpheleniliyor. Heronların yoğun olarak kullanıldığı bazı operasyonların öncesinde belirlenen PKK'lılardan bazılarının aniden bölgeyi terk etmeye başlamasının bu şüpheyi desteklediği belirtiliyor.*

*Pazarlığın kilit noktası*

*Bu bilgiler ışığında Türkiye, Predatör sözleşmesinde "Görüntülerin 3. ülkeye verilemeyeceği" maddesinin konulmasını ABD tarafına bildirdi. Amerikan tarafı 'Üçüncü ülkelere görüntü zaten vermiyoruz' gerekçesiyle karşı çıktı. Heron görüntülerinden hareketle planlanan operasyonlar öncesi PKK unsurlarındaki hareketlenmeler, elde edilen görüntülerin bir uçla İsrail'e gittiği şüphesini doğurdu.*

*Heron ağı güçlendirildi*

*Kandil ve Kazan Vadisi operasyonunda başarı elde edilen İHA öncelikli saldırı yöntemi, İsrail'den gelen 4 Heron'la birlikte iyice güçlendi. Aynı anda havada tutulan birkaç Heron'un dışında, hareketlilik, telsiz trafiği ve insan istihbaratına dayalı olarak yerdeki İHA'lar da anında kaldırılıyor.*

*ANKA DAHA ÜSTÜN*

*Heronda personel sorunu yaşanıyor*

*İsrail Heronlarının sık motor bakımı gerektiren türden olması nedeniyle de bakım süresi hızla dolmasın diye araçların tamamı aynı anda havada tutulmayıp ihtiyaca göre hareket ediliyor. Yerli ANKA ise seri üretim imkânı, geliştirme imkânın elde olması ve uzun bakım ömrü nedeniyle bu sorunu ortadan kaldırabilecek nitelikte. Kara Kuvvetleri'nin elinde 3 İHA bulunuyor. KK'nın kullanım konusunda eğitilmiş personeli bulunmaması nedeniyle bu İHA'ları, İsrailli pilotlar uçuruyordu. İki ülke arasındaki gerilim nedeniyle İsrail personellerini çekince uçamaz duruma geldiler. Yetkililer, Heronları kullanan teknik elemanların hedefi lazerleyip, F-16 pilotuna tarif edecek veya harekâtı havadan yönlendirecek, pilotla sürekli irtibat halinde olacak personelin sadece Hava Kuvvetleri'nde olduğunu ifade ediyor. Kara Kuvvetleri'nin elindeki İHA'ların Hava Kuvvetleri'ne devredilmesinin uygun olacağı belirtiliyor.*

*PREDATÖR SORUNU*

*Gördüğünü vuran silahlılar gelmiyor*

*Amerika Birleşik Devletleri'nin İncirlik Üssü'ne getireceği ve Türkiye'ye kullanım tahsisi yapacağı Predatörlerle ilgili diğer konu da görüntülerin canlı ve direkt değil bir süre sonra verilecek olması. Uydu kontrollü Predatörler, Türk subayları tarafından yönetilemeyecek.*

*Radarda görülememesi nedeniyle Türkiye, tam olarak nerenin görüntülendiğini tespit edemeyeceği için, "Görüntülerin 3. ülkeye verilemeyeceği" konusunda endişeler devam ediyor. Predatörler konusunda diğer bir sorunda Türkiye'nin kullanımına verileceklerin "görünce vuran" türden silahlı olmaması. Bu da aşılmaya çalışılan konulardan diğeri. 31 Aralık'ta Irak'tan çekileceğini açıklayan ABD yönetimi için Irak'ın Kuzeyi'ndeki Özerk bölgenin güvenliği önemli. İncirlik Üssü bu nedenle kritik önemde.Türkiye iki ülke için de önemli olan pazarlık konusunu Predatörler üzerinden maksimum verimle çözmeye çalışıyor.*"

İNTERNET http://www.tai.com.tr

Günlük hayatımızda yakın zamanda mini İHA'lar yerini alacaktır. Çünkü şehirler büyüdükçe sorunları da artmaktadır. Belediyeler için yerleşim birimlerinin gelişim kontrolü, orman yangınlarının tespiti, kaçak yapıların tespiti gibi sivil amaçlı kullanımlara uyarlanabilecek birtakım avantajları olan bu sistemler, belki de her güvenlik görevlisi ya da kolluk kuvvetlerinin sırtında taşıyacakları temel ekipmanlardan birisi olacaktır. Ayrıca birçok büyük işletmenin, örneğin doğal gaz şirketlerinin boru hatları kontrolü amaçlı bu sistemleri kullanması sıradan hale gelecektir.

**Resim 6.7:** İnsansız Hava Aracı ANKA

İnsansız hava araçları, havada kendileri hareket edebilen veya yerden komut ve rota bilgileri alabilen sistemlerdir. Bulundurdukları faydalı yükler olarak adlandırılan dedektörler ve kameralar ile davetsiz misafirleri belirleyebilmekte ve alarm verebilmektedirler.

Bütün dedektörlerin amacı ister dış, ister iç olsun davetsiz misafiri taramak ve yanlış alarmlar vermemektir. Bu ideal duruma ulaşılması mümkün değildir. Bununla beraber yanlış alarmları taranacak bölge için en uygun dedektör teknolojisi kurularak, büyük ölçüde azaltmak mümkündür. Dış ortam iç ortamdan daha zor olduğundan dedektör teknolojisi seçimi dış dedektörler için aşırı önemlidir.

## Özet

Bir binanın verilen bir alanının bütününün taranması için güvenlik sistemi tasarlanması istenebilir. Bu tasarım probleminin en önemli sorunu, bütün davetsiz misafirler için böyle bir tasarımı yapmak neredeyse imkânsız olmasıdır. Ortalama maliyet ile kurulan bir güvenlik sistemi, istenmeyen misafirlerin sıradan sızma girişimlerini %90 bulabilmektedir. Tam başarı elde edilmek istenildiğinde, daha büyük kurulum maliyeti gerekir. Bunun için, belirlenen bölgenin taramasının gerçekçilik olasılığını (PD) belirlemek gerekir. Bu da bazı testler ile öznelliğin katılmasıyla mümkündür. PD'yi iyileştirebilmenin birçok yolu vardır. Aynı tip dedektörlerden birden fazla ekleme, farklı dedektör teknolojilerini birlikte kullanma veya bazı giriş faaliyetlerini sınırlandırma bu yollardan bir kaçıdır. Bilgisayar odasının girişine kapı anahtarı ilave edilebilir. Tavandan veya çatıdan yapılacak sızma girişimlerini önlemek için tedbirler alınabilir. Amaç PD'yi en ekonomik şekilde %100'e yakınlaştırmaktır.

Yaygın dış tarama teknolojilerinden birisi mikrodalgadır. Aktif cihazlar olan mikrodalga tarayıcılar iki sınıfta değerlendirilirler. İlk tip mono statik mikro dalga sistemlerinde gönderici ve alıcı aynı kutunun içindedir. Mikrodalga cihaz kutusundan yayılacak şekilde alan üretir. Bu alan bozulduğunda, alarm çıkış rölesi aktifleşir. İkinci tip, çiftli statik cihazda ise gönderici ve alıcı ayrıdır. Alıcı gönderici tarafından üretilen alanı gözetler. Bu alan bozulduğunda, alarm rölesi aktifleşir.

Kızılötesi ışınlar diğer aktif dış tarayıcı tipidir. Bu cihazlarda gönderici ve alıcı ayrı ayrıdır. Gönderici alıcıya kızılötesi ışın gönderir. Alıcı tarafında engellenen veya engellenmeyen bir ışın varsa, alarm çıkış rölesi etkin olur. Kızılötesi ışınlar, gönderici ve alıcıları bağlayan görünmeyen kablolara benzemektedir. Bu üst üste konmuş cihazlar çok verimlidir. Fakat mikrodalga gibi tarayıcı olarak kulanılmak istenildiğinde, aynı amaç için uygun düzenleme isterler. Yağmur ve sis bu tarayıcı tipini etkiler. Kızılötesi lensinin içindeki yoğunlaşma yanlış alarmlara neden olur..

Açık alan dedektörlerinin diğer bir grubu da gömülü düzende çalışan detektörlerdir. Bu dedektörlerin depremsel, depremsel/manyetik, koaksiyel bağlantılı ve fiber optik çeşitleri vardır. Her biri kendisi ile ilgili teknolojiyi kullanır. Örneğin, gömülü fiber optik kablo ile sürekli gönderilen sinyal, fiber optik teknolojisini kullanır. İstenmeyen misafir gömülü kabloya adım attığı zaman, kablo yavaşça fiber içinde kırılıcak ve üzerindeki elektrik akımı kesilecektir. Kablolara sinyal gönderen cihaz optik zaman alan yansıması ölçme (ODTR) temeliyle sinyal gönderir. ODTR, gönderilen sinyal ile fiber optik kablodan yansıyarak gelen sinyali karşılaştırır, kesintiyi algılar, kesintinin olduğu yerin mesafesini bulur.

Diğer bir gömülü dedektör de istenmeyen misafirin yürüyerek veya koşarak gömülü dedektörden geçerken sismik etkisine göre çalışır. Mekanik olarak gerildiğinden elektrik akımı üreten basınç dedektörünün kullanımı ile yapılabilir. İstenmeyen misafir gömülü dedektöre doğru yürüdüğünde veya yaklaştığında gerilim üretilir. Diğer gömülü cihazlar gibi istenmeyen misafir bölgeden geçerken elektriksel alan üretirler.

Hareket dedektörleri grubunda en iyi bilinen dedektör kızılötesi hareket dedektörüdür. İç kızılötesi hareket dedektörleri pasif cihazlardır. Pasif kızılötesi dedektörler enerji üretmezler. Onlar gördükleri alanda bulunan kızılötesi enerjiyi saptarlar. Kızılötesi enerji ısıdır ve insanlar ısı üretirler. İnsan derisinin dış sıcaklığı yaklaşık 32 ºC ve oda sıcaklığı ise 22 ºC'dır. Aradaki fark fazla olduğu için hareketli bir kişi sıcak nokta olarak çabucak bulunabilir.

Sesüstü hareket dedektörleri Doppler kaymaya bakan aktif cihazlardır. Doopler kayma gözleyici veya sisteme ulaşan dalganın frekansındaki değişimdir. Genel örnek tren ıslığının duyulabilen frekans değişimidir. Tren size yaklaşınca frekansı azalır.

İnsansız hava aracı kullanımı dört bölümde incelenebilir; mini, taktik, stratejik ve deneysel sistemler. Mini sistemler sırtta taşınabilir özellikte olup hızlı ve kısa menzilde etkin bir kullanıma sahip ve ucuz insansız hava araçlarıdır. Taktik sistemler kısmen taşınabilir olup en çok ve etkin kullanılan sistemlerdir. Stratejik sistemler uzun süre yüksek irtifada görev yapabilme özellikleri ile en fonksiyonel ve bu yüzden de edinilmesi en maliyetli sistemlerdir. Bir de askeri tatbikatlarda yüksek hızda hedef olarak kullanılan deneysel İHA sistemleri mevcuttur.

## Kendimizi Sınayalım

**1.** Dedektör nedir?

a. Güvenlik sistemlerinde kullanılan elektronik algılayıcı

b. Teknoloji

c. Güvenlik katsayısı

d. Bilgisayar

e. Hiçbiri

**2.** Aşağıdakilerden hangisi dış detektörlerden **değildir**?

a. Mikrodalga dedektörü

b. Sesüstü dedektörler

c. Açık alan dedektörleri

d. Kızılötesi ışınlar

e. Hepsi

**3.** Aşağıdakilerden hangisi gömülü dedek-törlerin dezavantajlarındandır?

a. Görünmezler.

b. Bölgeyi çok iyi takip ederler.

c. Toprak altında aynı çalışırlar.

d. Doğal görünen bölgeyi takip ederler.

e. Hepsi

**4.** Tel örgü dedektörlerde hangi teknoloji **kullanılmaz**?

a. Alan

b. Sığa

c. Basınç

d. Ses

e. Gerginlik

**5.** Aşağıdakilerden hangisi iç dedektörlerden **değildir**?

a. Kapı dedektörleri

b. Hareket dedektörleri

c. Cam kırılma dedektörleri

d. Gömülü dedektörler

e. Hepsi

**6.** Kapı dedektörleri aşağıdakilerden hangi-sinden oluşmaktadır?

a. Dokunan röle - Mıknatıs

b. Kızıl ötesi ışın - Mercek

c. Sesüstü - Hoparlör

d. Mikrodalga - Osiloskop

e. Lazer - Ayna

**7.** Aşağıdakilerden hangisi hareket dedektör-lerinden **değildir**?

a. Kızılötesi

b. Mikrodalga

c. Sesüstü

d. Lazer alan

e. CCTV

**8.** Camın kırılma frekansı nedir?

a. 2-4 Khz

b. 4-6 KHz

c. 4-20 KHz

d. 4-6 MHz

e. 4-20 MHz

**9.** İnsansız hava araçlarının kontrolü nasıl yapılır?

a. Otonom kontrol yapılır.

b. Uzaktan kontrol yapılır.

c. Otonom kontrol ve yer istasyonundan kontrol yapılabilir.

d. Dedektör ile kontrol yapılır.

e. Hepsi

**10.** Aşağıdakilerden hangisi insansız hava aracıdır?

a. CCTV

b. Kamera

c. Ses üstü

d. Kızılötesi

e. ANKA

## Kendimizi Sınayalım Yanıt Anahtarı

**1. a** Yanıtınız yanlış ise "Giriş" başlıklı konuyu yeniden gözden geçiriniz.

**2. b** Yanıtınız yanlış ise "Dış Çevre Dedektörleri" başlıklı konuyu yeniden gözden geçiriniz.

**3. c** Yanıtınız yanlış ise "Dış Çevre Dedektörleri" başlıklı konuyu yeniden gözden geçiriniz.

**4. d** Yanıtınız yanlış ise "Dış Çevre Dedektörleri" başlıklı konuyu yeniden gözden geçiriniz.

**5. d** Yanıtınız yanlış ise "İç Çevre Dedektörleri" başlıklı konuyu yeniden gözden geçiriniz.

**6. a** Yanıtınız yanlış ise "Kapı Dedektörleri" başlıklı konuyu yeniden gözden geçiriniz.

**7. e** Yanıtınız yanlış ise "Hareket Dedektörleri" başlıklı konuyu yeniden gözden geçiriniz.

**8. b** Yanıtınız yanlış ise "Cam Kırılma Dedektörü" başlıklı konuyu yeniden gözden geçiriniz.

**9. c** Yanıtınız yanlış ise "İnsansız Hava Araçları" başlıklı konuyu yeniden gözden geçiriniz.

**10. e** Yanıtınız yanlış ise "İnsansız Hava Araçları" başlıklı konuyu yeniden gözden geçiriniz.

## Sıra Sizde Yanıt Anahtarı

### *Sıra Sizde 1*

Aynı çeşit dedektörlerden birden daha fazla kulanılabilir, farklı dedektör teknolojileri birlikte kullanılabilir veya bazı giriş faaliyetleri sınırlandırılabilir.

### *Sıra Sizde 2*

Türkiye'de insansız hava araçları konusunda Vestel Savunma Sanayi A.Ş., TAİ ve Baykar Makine A.Ş. ve birçok firmanın ürettiği insansız hava araçları vardır.

## Yararlanılan Kaynaklar

Pearson, R.L. (2007). **Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions**, Butterworth-Heinemann, Elsevier.

## Yararlanılan Internet Kaynakları

http://www.oyaksgs.com.tr

http://www.gozlemguvenliksistemleri.com

http://yuzdeyuz.wordpress.com/2011/03/06/cevre-guvenlik-sistemleri

http://www.genetlab.com

http://www.essed.com.tr/cevreguvenlik.php

http://www.sibertek.com.tr/urunler/2-cevre-guvenlik-sistemleri.html

# 7

## Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Biyometrik verinin özelliklerini tanımlayabilecek,
- Biyometrik güvenlik sistemi bileşenlerini açıklayabilecek,
- Kimlik doğrulama yöntemlerini karşılaştırabilecek,
- Biyometrik eşleştirme ilkelerini listeleyebilecek,
- Fiziksel özellik temelli biyometrik güvenlik sistemlerinin çalışma şeklini özetleyebilecek,
- Davranışsal özellik temelli biyometrik güvenlik sistemlerinin çalışma şeklini özetleyebilecek,

bilgi ve becerilere sahip olabilirsiniz.

## Anahtar Kavramlar

- Biyometrik Veri
- Güvenlik Sistemi
- Kimlik Doğrulama
- Parmak İzi
- Yüz
- El Geometrisi
- İris
- Retina
- DNA
- Ses
- İmza
- Yürüyüş Şekli

## İçindekiler

# Biyometrik Temelli Güvenlik Sistemleri

## GİRİŞ

Gizlilik arz eden bir mekâna, bir cihaza veya bir bilgiye yalnızca belirli kişi veya kişilerce erişim sağlanmasının öngörüldüğü durumlarda, güvenlik sistemlerinin kimlik doğrulama bileşeni öne çıkmaktadır. Örneğin, ATM cihazından hesap bilgilerine ulaşmak için, bir bilgisayara giriş yapabilmek için veya gizlilik derecesi yüksek bir mekâna erişim sağlayabilmek için kimlik doğrulaması yapılmaktadır. Böylelikle, yetkisiz kişi veya kişilerin gizlilik arz eden bilgiye, mekana veya cihaza erişmesi engellenmektedir.

Kimlik doğrulaması denildiğinde akla ilk gelen yöntemlerin başında şifre uygulaması yer alır. Yukarıda verilen örnekler tekrar göz önüne alındığında, gerek ATM cihazına, gerek bilgisayara, gerek gizli bir mekana erişim sırasında kimlik doğrulama için önceden belirlenmiş şifre bilgisi kullanılabilir. Güvenliği sağlanan ortama erişim için şifrenin dışında, uygun bir anahtardan veya manyetik bir karttan da faydalanılabilmektedir. Ancak, bu yöntemler için unutulma, kaybolma, kopyalanma veya çalınma gibi tehlikeler mevcuttur.

Günümüzde, teknolojideki gelişmelere paralel olarak güvenlik sistemlerinde de önemli ilerlemeler kaydedilmiş ve yukarıda bahsedilen yöntemlerden farklı olarak, biyometrik verilerden faydalanan biyometrik güvenlik sistemleri de geliştirilmeye başlamıştır. Biyometri, kişilerin fiziksel ve davranışsal özelliklerini kullanarak otomatik kimlik doğrulama veya tanımlama yapmayı hedefleyen bir disiplindir. Dolayısıyla biyometrik veri, kişilerin fiziksel ve davranışsal özelliklerini temsil eder. İdeal olarak, bir biyometrik veri şu özelliklere sahip olmalıdır:

- Evrensel olmalı, yani her insan bu özelliği taşımalıdır.
- Kalıcı olmalı, zaman içerisinde değişmemelidir.
- Ayırt edicilik sağlamalı, yani kişiye özgün olmalıdır.
- Erişilebilir olmalı, yani veriye kolaylıkla ulaşılabilmelidir.
- Kopyalanması zor olmalıdır.

Kişilerin fiziksel ve davranışsal özelliklerini temsil eden, aynı zamanda yukarıda belirtilen özelliklere sahip başlıca biyometrik veriler şunlardır:

1. Fiziksel Özellikler
    - Parmak izi
    - Yüz
    - El geometrisi
    - İris
    - Retina
    - DNA

2. Davranışsal Özellikler
    - Ses
    - İmza
    - Tuş vuruş dinamiği
    - Yürüyüş şekli


**Önceden tanıdığınız birisiyle karşılaştığınızda, o kişiyi hatırlamanızı sağlayan en temel biyometrik veri nedir?**

Biyometrik güvenlik sistemlerinde, bu özellikler tek tek kullanılabildiği gibi bazı durumlarda birden fazla özellikten de faydalanılabilmektedir.

Geçmişten günümüze kadar biyometri alanındaki çalışmalar incelendiğinde, teknolojideki gelişmelere paralel olarak, pek çok farklı biyometrik güvenlik sisteminin geliştirildiği ve bu sistemlerin yine pek çok alanda kullanıldığı görülmektedir. Biyometrik güvenlik sistemlerinin kullanıldığı alanlardan bazı örnekler şöyle sıralanabilir:

- Mobil telefonlar
- Bilgisayarlar
- İnternet bankacılığı
- Çağrı merkezleri
- Yüksek güvenlikli tesisler
- Havaalanları
- İş yerleri
- ATM cihazları

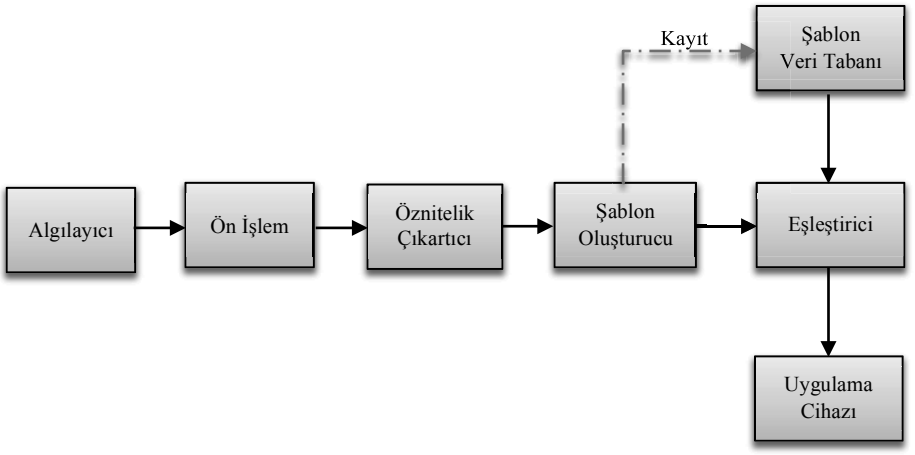

**Birden fazla biyometrik verinin birlikte kullanıldığı biyometrik güvenlik sistemleri hangi durumlarda yararlı olabilir?**

# BİYOMETRİK GÜVENLİK SİSTEMİ BİLEŞENLERİ

Biyometrik güvenlik sistemlerinin temel yapısı, Resim 7.1'de görülmektedir. Biyometrik sistem, genel yapı itibariyle girişinde algılayıcı bir cihaz bulundurur. Ayrıca kayıt ve tanımanın gerçekleştirildiği bir sistem ile kayıtlı verilerin tutulduğu bir veri tabanına sahiptir. Hangi biyometrik bilgi kullanılacaksa, ona özgü bir algılayıcı kullanılır. Algılayıcıdan gelen ham veri, çeşitli algoritmik ve matematiksel ön işlemlerden geçirilerek özniteliklerden oluşan bir şablon çıkarılır.

İlgili kişiye ait şablon, sistem tarafından ilk defa oluşturulacaksa, bu aşama kayıt aşamasını oluşturur. Bu aşamada, kullanıcının biyometrik bilgisi veri tabanına kaydedilir. Sisteme sonraki erişimlerde ise, algılayıcı ile taranan biyometrik veri, yine benzer ön işlemlerden geçirilerek bir şablon oluşturulup daha önceden veri tabanına kaydedilen şablon veya şablonlar ile eşleştirilir. Bu aşama ise tanıma ve doğrulama aşamasıdır. Tanıma işlemi olumlu sonuçlanır ise doğrulama gerçekleşmiş olur. Bunun sonucunda, kullanıcının sahip olduğu yetkiler aktif hale getirilerek bilgi, cihaz ya da mekâna erişime izin verilir. Böylece, diğer kimlik doğrulama sistemlerinin aksine, kullanıcılar yanlarında kart benzeri nesneler taşımak veya şifrelerini akıllarında tutmak zorunda kalmazlar. Çok nadir durumlar dışında, biyometrik veriler kişiye özgü olduğundan taklit edilemezler. Biyometrik verinin çalınma, unutulma, bir başkasına

aktarılma ya da kaybolma tehlikesi yoktur. Bu sebeplerden ötürü, biyometrik veri, kişiye veya kişilere özgü güvenlik sistemleri oluşturulmasına da olanak tanımaktadır.




**Resim 7.1:** Biyometrik güvenlik sistemlerinin genel yapısı.


**Biyometrik tanımada kullanılan temel modeller hakkında daha ayrıntılı bilgi edinmek için Leyla Keser Berber ve Murat Lostar'ın Yetkin Yayınevinden basılmış olan "Bilişimde Biyometrik Yöntemler (2006)" adlı kitabını okuyabilirsiniz.**

# KİMLİK DOĞRULAMA

Güvenlik sistemlerinde kimlik doğrulama yöntemleri başlıca üç gruba ayrılır:

- Bilgi temelli
- Nesne temelli
- Biyometrik temelli

Biyometrik güvenlik sistemlerinin çeşitlerinden bahsetmeden önce, kimlik doğrulama yaklaşımlarının açıklanması, aralarındaki farkların daha iyi anlaşılmasını sağlayacaktır.

## Bilgi Temelli Kimlik Doğrulama

Bilgi temelli kimlik doğrulamada, sisteme kayıtlı kullanıcılar kullanıcı adı, şifre veya PIN gibi bilgilere sahiptir. Kullanıcı sisteme erişmek istediğinde gerekli gizli bilgileri girer. Böylece daha önce sistem veri tabanında kayıtlı olan bilgilerle eşleşme sağlandığında, sistem yöneticisi doğru kişinin giriş yaptığını varsayarak yetkilendirmeyi onaylar. Ancak bu tür sistemlerde, kullanıcı adı, şifre veya PIN bilgisinin başka kişilerin eline geçebilmesi ya da bu bilgilerin unutulması gibi dezavantajlar söz konusudur.

## Nesne Temelli Kimlik Doğrulama

Nesne temelli kimlik doğrulamada, sistem kullanıcıya anahtar veya manyetik bir kart vererek erişimi bu nesne ile yaptırır. Nesne içerisinde doğrulama bilgileri bulunmaktadır. Ancak bu nesnelerin de unutulma ya da başkaları tarafından çalınma riski bulunmaktadır.

## Biyometrik Temelli Kimlik Doğrulama

Biyometrik temelli kimlik doğrulamada, kişiler bilgi ve nesne temelli sistemlerin aksine herhangi bir şifreye ya da anahtara ihtiyaç duymadan, yalnızca kendi fiziksel veya davranışsal özelliklerinden faydalanırlar. Fiziksel veya davranışsal özelliklerin kaybolma, çalınma ya da unutulma tehlikesi yoktur.

Örneğin bir işyerinde çalışanların giriş çıkışlarını kontrol eden ve kayıt altında tutan bir kartlı geçiş sisteminde, kişinin ne kadar süre iş yerinde olduğu net bir şekilde belirlenemeyebilir. Çünkü bir başkası o kişinin kartını sisteme okutmuş olabilir. Ancak biyometrik temelli sistemlerde böyle bir durum yaşanması söz konusu değildir. Biyometrik temelli kimlik doğrulama için, INCITS (International Committee for Information Technology Standarts - Uluslararası Bilgi Teknolojileri Standartları Komitesi) tarafından oluşturulmuş standartlara uygun biyometrik ölçüler kullanılmaktadır.

Kullanılan kimlik doğrulama yöntemi veya yöntemlerine göre güvenlik seviyeleri düşükten yükseğe doğru şu şekilde sıralanabilir:

- Seviye 1: Sahip olduğunuz bir bilgi (şifre, PIN, vb.)
- Seviye 2: Sahip olduğunuz bir nesne (anahtar, manyetik kart, vb.)
- Seviye 3: Sahip olduğunuz bir nesne ile birlikte sahip olduğunuz bir bilgi (ATM kartı ve şifre)
- Seviye 4: Sahip olduğunuz bir özellik (biyometrik bilgi)
- Seviye 5: Sahip olduğunuz bir bilgi ile birlikte sahip olduğunuz bir özellik
- Seviye 6: Sahip olduğunuz bir nesne ile birlikte sahip olduğunuz bir özellik
- Seviye 7: Sahip olduğunuz bir bilgi ile birlikte sahip olduğunuz bir nesne ve sahip olduğunuz bir özellik


**Biyometrik verilerle ilgili standartlara www.incits.org adresinden ulaşabilirsiniz.**

# BİYOMETRİK EŞLEŞTİRME TEMELLERİ

Biyometrik bir güvenlik sistemine kayıt işlemi esnasında, kullanıcı biyometrik verisini sisteme tanıtmak için sistem yöneticisinden onay ister. Erişim izni aldıktan sonra hangi biyometrik veri kullanılacaksa uygun tanıma algoritması, ilgili verinin sisteme nasıl tanıtılacağı bilgisine gereksinim duyar. Sisteme bir ya da birkaç kez bu verinin tanıtımı yapıldıktan sonra sistem, tanımada kullanacağı ayırt edici tüm detayları ilgili biyometrik veriden elde eder. Örnek olarak, bu veri parmak izi ise, daha sonra aynı parmakla sisteme giriş yapılmaya çalışıldığı her durumda parmağa ait ayırt edici detayları içeren bu şablon kullanılacaktır. Böylece kayıt işleminin ardından, sistemde biyometrik bilgileri kayıtlı olan kullanıcılar **yetkili kullanıcı**, bu kullanıcıların dışındaki herkes ise **yetkisiz kullanıcı** olarak sınıflandırılacaktır**.**

Yetkili kullanıcının güvenlik sistemine her girişinde, biyometrik verisi sistem tarafından tekrar alınır ve daha önceden veri tabanına kaydetmiş olduğu biyometrik şablon bilgisi ile eşleştirilip bir eşleşme skoru hesaplanır. Benzeşmeyi ölçen bu sayısal değer, belli bir eşik değerinden büyük ise kullanıcının yetkileri aktifleştirilecektir. Yetkisiz kullanıcı sisteme giriş yapmaya çalıştığında ise, eşleşme işlemi sonucu çıkan sayısal değer, eşik değerinden oldukça küçük olacaktır. Böylece sistem kullanıma açılmayacaktır. Ancak, karşılaştırma yapılan sayısal değerin algoritmada nasıl belirlendiği önemlidir. Bu nedenle algoritma birçok testten geçirildikten sonra gerçek sistemde kullanılmaktadır. Test işlemleri esnasında biyometrik bilgi girişinin, hangi yetkili ya da yetkisiz kullanıcı değerlerine karşılık geldiği ve buna karşılık hangi skoru ürettiği bilgisi etiketlenerek kayıt altına alınır. Test aşamasında elde edilen tanıma işlemlerinin örnek değerleri çeşitli matematiksel fonksiyonlardan geçirilerek karşılaştırma grafikleri elde edilir. Biyometrik güvenlik sisteminde, tanıma aşamasında kullanılacak karşılaştırma sayısal değeri, bu testler ve grafiklerden elde edilen performans sonuçlarına göre belirlenir.


**Biyometrik güvenlik sistemlerinin performans karşılaştırmalarında hangi tür grafikler kullanılmaktadır?**

## Performans Ölçütleri

Bir biyometrik güvenlik sistemi, çalışma esnasında iki tür hata yapabilir. Bu hatalardan birincisi, yetkili bir kullanıcıya erişim izni verilmemesidir. İkinci tür hata ise yetkisiz bir kullanıcıya erişim izni verilmesidir. Bu hataları ölçmek için **yanlış ret oranı** (false reject ratio) ve **yanlış kabul oranı** (false accept ratio) değerleri hesaplanır. Yanlış ret oranı, belirli sayıda yetkili kullanıcı erişiminden kaç tanesinin reddedildiğini belirtir. Yanlış kabul oranı ise belirli sayıda yetkisiz kullanıcı erişiminden kaç tanesinin kabul edildiğini ifade eder.

Örneğin, yanlış ret oranı çok yüksek olan bir biyometrik güvenlik sisteminde, yetkili kullanıcı erişimleri çoğunlukla reddedilecektir. Bu durumun, sistemin verimliliğini düşüreceği oldukça açıktır. Yanlış kabul oranı çok yüksek olan bir biyometrik güvenlik sisteminde ise yetkisiz kullanıcı erişimleri çoğunlukla kabul edilecektir. Bu durum önemli bir güvenlik açığına yol açacağı için sistemin verimliliği yine olumsuz etkilenecektir. Dolayısıyla, bir biyometrik güvenlik sisteminden beklenen hem yanlış ret oranının hem de yanlış kabul oranının minimum olmasıdır.

Yanlış ret oranı ve yanlış kabul oranı, birbirleriyle çelişen ölçütlerdir. Biyometrik güvenlik sistemi hassaslaştıkça yanlış kabul oranı düşerken yanlış ret oranı ise yükselir. Dolayısıyla, bir biyometrik güvenlik sistemini yalnızca yanlış ret oranına veya yalnızca yanlış kabul oranına göre değerlendirmek çok sağlıklı değildir. Genellikle, bu değerlendirme için yanlış ret oranı ve yanlış kabul oranı bilgisini birleştiren **çapraz hata oranı** (crossover error rate) kullanılır. Çapraz hata oranı, yanlış ret oranı ile yanlış kabul oranının eşit olduğu değeri belirtir. Düşük çapraz hata oranı, hem yanlış ret oranının hem de yanlış kabul oranının düşük olduğu anlamına gelir.


**Farklı biyometrik güvenlik sistemlerinin performansını karşılaştırmak için çapraz hata oranlarını karşılaştırmak doğru bir yaklaşım olacaktır. Örneğin, çapraz hata oranı "2" olan bir biyometrik güvenlik sisteminin performansı, çapraz hata oranı "3" olan bir sisteme kıyasla daha yüksektir.**

# FİZİKSEL ÖZELLİK TEMELLİ BİYOMETRİK GÜVENLİK SİSTEMLERİ

Biyolojik olarak her kişiye özgü ve ayırt edici fiziksel özellikler bulunmaktadır. Bu özellikler, kişiyi diğer insanlardan ayıran özelliklerdir. Fiziksel biyometrik veri temelli güvenlik sistemleri, daha önce de bahsedildiği üzere, değişmez özellikler yardımıyla kişi tanıma işlemini gerçekleştirerek, güvenliği sağlanmak istenen ortamlarda kullanılmaktadır. Bunlardan başlıcaları; parmak izi, yüz, el geometrisi, iris, retina ve DNA tanıma temelli sistemler şeklinde sıralanabilir.

## Parmak İzi

Parmak izi verisi günümüzde en yaygın olarak kullanılan biyometrik bilgilerden biridir. Çünkü bir kişinin parmak izi bu bölgedeki tahribatlar dışında hayatı boyunca değişmeden kalan bir biyometrik özelliğidir. İkiz olan kişilerin parmak izleri bile birbirinden farklıdır. Parmak izi biyometrik okuyucusu kullanılan yerlerde, tek ihtiyaç olunan nesne parmağınızdır. Parmağın, anahtar benzeri nesnelerin aksine kaybolma veya unutulma riski yoktur. Resmi işlemlerde okuma yazma bilmeyen insanlar için imza yerine parmak izi istenmesi aslında oldukça yaygın bir uygulamadır. Son yıllardaki kullanımının artmasıyla birlikte, biyometrik temelli güvenlik sistemlerinde kullanılan yöntemlerden biri olan parmak izi, emniyet hizmetleri, pasaport işlemleri, bilgisayarlar gibi pek çok alanda kullanılmaktadır. Resim 7.2'de parmak izi okuyuculu örnek bir güvenlik sistemi görülmektedir.

Sabah Gazetesi'nde 22 Ağustos 2011 tarihinde yayımlanmış olan aşağıdaki haberden de anlaşılacağı üzere, artık bazı bankaların ATM cihazlarında kimlik doğrulaması için kartın yanında biyometrik verilerden de faydalanmaya başladığını görebiliriz:

"*Ziraat Bankası ATM'den parmak iziyle para çektirecek*

*Otomatik para çekme makinelerinden (ATM) artık parmak izi ile para çekme dönemi başlıyor. Yeni kurulan sistemle yanınızda bankamatik ya da kredi kartı taşımadan, kart kaybetme endişesi taşımadan bankamatikten tüm banka işlemlerini yapabilmek mümkün olacak. Ziraat Bankası'nın faaliyete geçireceği biyometrik bankacılık hizmetiyle bankamatiklerde özel olarak hazırlanan bölüme parmağını koyan müşteri doğrudan banka işlemlerini yapacak. Bunun için, önce parmak izleri sisteme kaydettirilecek.*"

Parmak izi uygulamalarının kullanılmaya başlandığı ilk günlerden itibaren günümüze kadar birçok ilerlemeler kaydedilmiştir. Günümüzde parmak izi tanıma işlemi otomatik parmak izi tanıma sistemleri ile yapılmaktadır. Parmak izi aslında parmaklarda var olan çizgilerin karakteristiğidir. Bu karakteristik çizgiler her kişide farklı yapıda, kapalı, açık veya sarmal eğri şeklinde bulunabilirler. Parmak izindeki farklılık çizgilerin birbirleri ile başlangıç, bitiş ve kesişme noktalarındaki referans noktalarda oluşmaktadır. Bu referans noktalar yatay ve dikey eksene yerleştirilerek analiz edilir. Kişiye ait parmak izi şablonu ile sisteme giriş yapılan parmak izi bilgisi, bu referans noktalarında parametrik olarak karşılaştırılır. Belirlenen skor değerinden daha fazla sayıda referans noktası aynı koordinatta çıkarsa kişinin kimliği doğrulanır. Günümüzde artık bu cihazlar oldukça uygun fiyatlarda ve değişik yapılandırmalarda esnek kullanım alanlarına sahiplerdir. Örneğin, pek çok dizüstü bilgisayar modelinde kimlik doğrulaması için parmak izi okuyucular bulunmaktadır.

**Resim 7.2:** Parmak izi okuyuculu bir güvenlik sistemi.

Otomatik parmak izi tanıma sistemlerinde temel olarak aşağıdaki işlemler gerçekleştirilir:

- Parmak izi görüntüsü alınarak sayısal formata çevrilir.
- Parmak izinde bilgi taşıyan, üzerinde işlem yapılacak kısım arka plandan ayrılır.
- Referans noktaları elde edilir.
- Parmak izi görüntüsü temizlenip iyileştirilir.
- Resim ikili formata dönüştürülür.
- İkili formattaki resim inceltilir.
- Özellik noktaları ve bu noktalara ait parametreler bulunur.
- Yalancı özellik noktaları iptal edilir.
- Karşılaştırma işlemi gerçekleştirilir.
- Sistemin başarısı değerlendirilir.

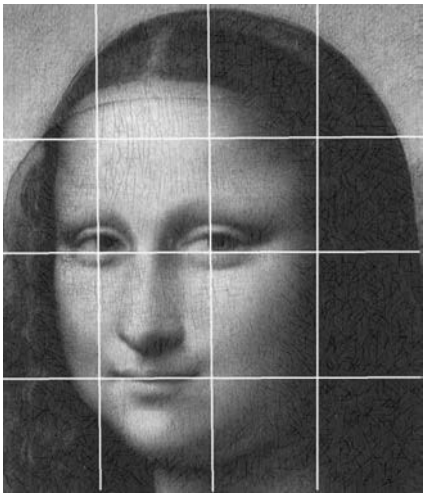
Parmak izi tanıma sistemlerinde, kullanıcıların parmak izlerinin kaydedilmesi, gizlilik ihlali endişelerine yol açmaktadır. Ancak parmak izinin kendisi yerine, özel algoritmalar yardımıyla elde edilen

ve parmak izi verisini temsil eden öznitelik değerlerinin kaydedilmesi bu duruma çözüm olarak kullanılmaktadır. Parmak izi kullanılan güvenlik sistemlerinde parmak izi taklit edildiğinde sistem yanılabilmektedir. Bu duruma engel olabilmek için parmağın canlılığını test edecek algılayıcılar kullanılmaktadır. Ayrıca değişik deri hastalıkları ya da bir kaza sonucu parmak izi kaybolmuş olabilir. Bir diğer olumsuz durum ise kullanıcının parmak izinin net olmaması halinde ortaya çıkmaktadır. Bu gibi durumlarda sisteme kayıt işlemi gerçekleştirilememektedir. Ancak, sistemde birden fazla parmağa ait parmak izi görüntüsünün kullanılıyor olması bu probleme çözüm getirebilmektedir.

SIRA SİZDE 4 **Parmak izi tanımada hangi çeşit parmak izi algılayıcıları kullanılmaktadır?**

## Yüz

Herhangi bir yere girişte, geçmişten beri kullanılmakta olan fotoğraflı kimlik belgesinin yetkili görevliye gösterilmesi günümüzde oldukça sıradan ve basit hale gelmiş bulunmaktadır. Bazı durumda kimlik belgesindeki fotoğraf, kişinin mevcut haline hiç benzememekte ve kontrol işlemi görevlinin takdirine bırakılmaktadır. Oysaki yüz tanıma sistemleri bu işlemi daha hassas bir şekilde gerçekleştirebilmektedirler. Biyometrik cihaz, görevlinin gözleri ve beyni ile algıladığı işlemi, bir kamera ve yazılım aracılığıyla gerçekleştirmektedir. Kamera iyi aydınlatılmış bir ortama gereksinim duymaktadır.



**Resim 7.3:** Bir yüz örneği.

Yazılım, kullanılan fotoğrafın türü, gözlük, eşarp vb. aksesuarlar, bıyık ve sakal gibi faktörlerden etkilenmemelidir. Yüzün görülebilir alanı belli bir seviyenin altına düşerse tanıma işlemi güçleşebilmektedir. Yüzle ilgili hesaplama yöntemi, karmaşıklık ve veri saklama gereksinimlerine göre değişebilmektedir. En temel yöntem, yüzün görüntüsünü 2-boyutlu olarak ele alıp, yüz üzerinde belirlenen burun, ağız, gözler gibi öznitelikler arasındaki uzaklıkları kullanarak yüzün geometrik özelliklerini hesaplamaya dayalıdır. Daha karmaşık olan bir diğer yöntemde ise yüzün dokusu ve ten rengini analiz işlemine dâhil eder. Ayrıca 2-boyutlu yüz görüntülerini kullanılarak 3-boyutta çalışan sistemler de son zamanlarda geliştirilmiş yeni yöntemlerden birisidir.

DİKKAT **Yüz görüntüsünün alındığı yerdeki aydınlatma farklılıkları, bıyık, sakal, makyaj, arka plan görüntüsü vb. faktörler yüz tanıma işlemini güçleştirebilmektedir.**

## El Geometrisi

Özellikle havaalanı, nükleer güç istasyonları gibi yerlerde tercih edilen bir yöntem olan el geometrisi tanımada, kullanılan sisteme göre kişilerin elinin ya da iki parmağının geometrik yapısı incelenir. Bu inceleme işleminde parmakların uzunlukları, genişlikleri, eklem yerlerindeki noktalarda ayırt edici özellikler elde edilir. Sağ ve sol el modelleri mevcuttur.

El geometrisi yönteminde Resim 7.4'deki gibi cihazlar yardımıyla, öncelikle kişinin elinin görüntüsünün alınacağı yerde parmakları yerleştirmek için çivili bir platform bulunmaktadır. Şablon oluşturmak ve sayısallaştırma amaçlı üç boyutlu görüntü elde edebilmek için bir kamera kullanılır. Bu platform üzerine yerleştirilen elden, üç boyutlu monokrom görüntü alınır. 25 ile 90 arasında değişik referans noktalarından değerler okunur. Alınan referans noktalarının karşılaştırılmasında değişik matematiksel ölçüm yöntemleri ve algoritmalar kullanılır. Alınan veri sıkıştırılıp, boyutu indirgenerek sistemin hafızasına yüklenir. Sisteme erişim esnasında tekrar kullanılacağı zaman, o kişiye ait veri, özel bir algoritma kullanılarak, yeniden sıkıştırılmamış haline geri döndürülerek karşılaştırma işlemi yapılır. El geometrisi elin yalnızca bir yönünün görüntüsünü almasından dolayı çok sayıda yüzük takan kişilerde yanlış tanımaya sebep olabilir.

Başarı oranı yüksek bir yöntem olsa da parmak izi tanıma yönteminde olduğu gibi eldeki tahribatlar, parmakların kaybedilmesi, gut, kireçlenme gibi hastalıklar sistemin başarısını düşürebilmektedir. Ayrıca okuma cihazlarında resmin alınma aşamasında ve ön işlemlerden dolayı çalışma hızı yavaştır. Ellerinin büyüklüğünün zamanla değişmesinden dolayı çocuklarda kullanılamamaktadır. Ayrıca görüntünün alındığı platforma el ile dokunulması gerektiğinden sağlığa uygunluk açısından problem yaratmaktadır.

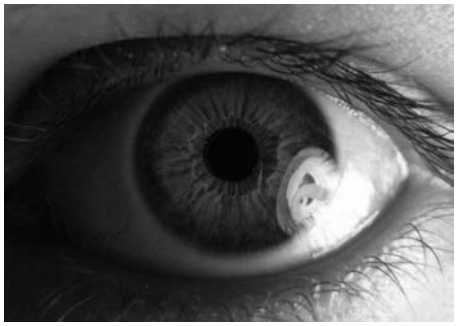
**Resim 7.4:** El geometrisi temelli bir güvenlik sistemi (Kaynak: Pearson, R.L. (2007). Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions, Butterworth-Heinemann, Elsevier).

## İris

İnsan vücudunda, gözün içinde bulunan iris yapısı ömür boyu değişmemektedir. Ayrıca göz dış etkenlerden daha az etkilenen bir yapıya sahiptir. İris tarama en basit biyometrik işlemlerden birisidir. Basit bir CCD kamera ile tarama yapılan yöntemde, fiziksel bir temasa gerek bulunmamaktadır. Genellikle havaalanları gibi kalabalık giriş çıkışların yaşandığı kimlik doğrulama gerektiren giriş çıkış kontrol noktalarında kullanılmaktadır.

Çok sayıda referans noktası kullanılarak tanıma işlemi gerçekleştirilmektedir. Genellikle ışıklı kamera kullanılarak elde edilen monokrom resimlerden faydalanılır. Yöntem, iris resmi alınırken gözlerin durumu, göz kapaklarının ve kirpiklerin görüntülerinin irise yansıması gibi tanımayı engelleyici detayları sadeleştirebilecek bir yönteme ihtiyaç duyar. İris tanıma işlemindeki aşamalar aşağıda sıralanmıştır:

- Gözün resmi alınır.
- Resimde irisin konumu bulunur.
- İrisin iç ve dış sınırları belirlenir.
- Analizde kullanılacak yapı süzgeçlenir.
- Yapının vektörleri elde edilir.
- İris kodu hesaplanır.
- İris kodu, önceden kayıtlı kod ile karşılaştırılır.



**Resim 7.5:** Bir iris örneği.

Her ne kadar uykusuzluk, gözyaşı ve bazı hastalıklar irisi etkilese de diğer bazı biyometrik yöntemlerde olduğu kadar fazla etkilenme yaşanmamaktadır. Elbette ki göz titreme hastalığına sahip ya da gözleri görmeyen insanlarda kullanılamasa da kimlik doğrulamanın önemli olduğu yerlerde yüksek başarı göstermektedir.

## Retina

Retina, gözümüzün arka iç duvarında, ışığa ve renge duyarlı hücrelerin bulunduğu katmandır. Baktığımız nesnelerden yansıyan ışık, retina üzerine düşer. Sinir sistemi tarafından beyne iletilen bu yansıma, beyinde işlenerek görme işlemi gerçekleşir. Retinal bölgede bulunan kan damarlarının yapısı kişiden kişiye farklılık göstermektedir. Bu sebeple, kişinin retinal özelliği de biyometrik güvenlik sistemlerinde kullanılabilmektedir. Ancak, retinal bölgedeki damarların diyabet gibi damar hastalıklarından etkilenmesi, zaman içerisinde kişinin damar yapısını değiştirebilmekte; dolayısıyla, kimlik doğrulama işlemini zorlaştırmaktadır. Resim 7.6'da, retina ve retinal kan damarlarının göz içerisindeki konumları gösterilmiştir.

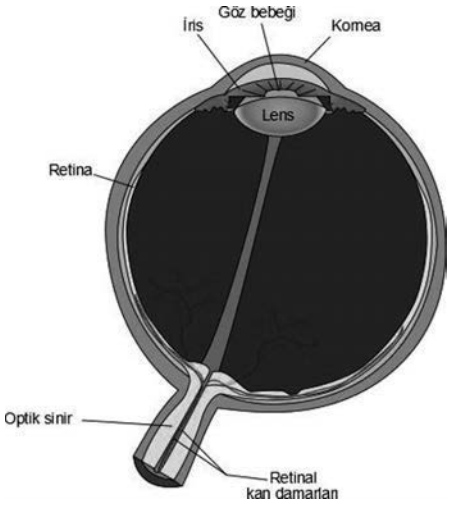
Retina tanıma temelli biyometrik güvenlik sistemlerinde, genellikle kullanıcı küçük bir delikten sabit bir noktaya bakarken, gözüne yansıtılan kızılötesi ışık ile retina görüntüsü alınır. Sayısallaştırılan şablon üzerinde 300'den fazla sayıda nokta sayısallaştırılır ve karşılaştırma için saklanır. Daha sonra, çeşitli görüntü işleme yöntemleri yardımıyla damar yapısı elde edilir. Son olarak, kullanıcının damar yapısı, veri tabanında bulunan örnekler ile karşılaştırılarak kimlik doğrulama işlemi tamamlanır.


**Geçmişte damarsal yapıyı belirlemek için kullanılan kızılötesi tarama cihazlarının, göze hasar verebileceği konusunda kaygılar bulunmaktaydı. Ancak son yıllarda bu ışınların düşük güçte kullanılmasıyla ve biyometrik cihaza doğrudan göz ile bakmaya gerek kalmadan damarsal yapının taranabilmesi ile bu konudaki endişeler giderilmiştir.**

Milliyet Gazetesi'nin 13 Mayıs 2011 tarihli aşağıdaki haberi, retina tanıma temelli biyometrik güvenlik sistemlerine dair güzel bir örneğe yer vermektedir:

"*İnternetteki tüm hesaplara şifre yerine göz kırparak girmek, portatif bir retina tarayıcı sayesinde mümkün olacak.*

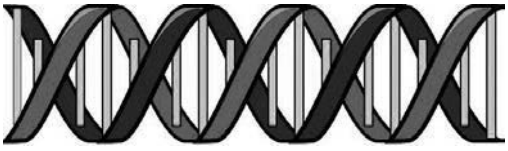
*New York merkezli biyometrik güvenlik şirketi Hoyos Group'un geliştirdiği dünyanın ilk ve tek portatif retina tarayıcısı "EyeLock" güvenli kilit sistemiyle internet üzerinden hesapların ele geçirilmesine karşı kullanıcının kendi gözüyle garanti sağlıyor. Bilgisayara yüklenen bir programla, hangi program ve sayfalar için cihazın kullanılacağına karar verdikten sonra facebook, e-posta, internet bankacılığı gibi hesaplara retina okutularak giriliyor. Her defasında, okuduğu retinayı farklı bir seri numara olarak kaydederek sayfaları açan EyeLock, böylece hesapların ele geçirilmesine karşı otomatik bir önlem sunuyor.*"




**Resim 7.6:** Retina ve retinal kan damarlarının göz içerisindeki konumu.

## DNA

Günümüzde güvenlik sistemlerinde, özellikle de adli olaylarda oldukça önemli delil olarak kullanılabilen DNA tanımada saç, kan, tırnak, deri parçası, sperm ve diğer biyolojik materyaller kullanılmaktadır. İnsanların hücrelerindeki kromozomlarda bulunan DNA moleküllerinin dizilimlerinin eşleştirme prensibine göre çalışmaktadır. Resim 7.7'de DNA'nın yapısı görülmektedir.



**Resim 7.7:** DNA yapısı.

Her bir DNA molekülünde Adenin (A), Guanin (G), Sitozin (C) ve Timin (T) olmak üzere dört kimyasal birim bulunmaktadır. Bu yapılar pozisyon ve dizilişleri açısından kişiye özgü bir çatı yapısı oluştururlar. Tandem tekrarlaması olarak adlandırılan bu yapı tekrar yapısı, sayısı ve miktar değişimlerine göre ayırt edici bir bilgi oluşturur. DNA tanıma aşamaları şu şekilde sıralanabilir:

- DNA örneği alınır.
- DNA izole edilir.
- Polimeraz zincir tepkimesi (PCR) kullanılarak enzimatik sınırlama ve yükseltme gerçekleştirilir.

- Parçalar ayrılır.
- Tekrar yapıları vb. bulunur.
- Elde edilen sonuçlar analiz edilir.

DNA analizi, maliyeti fazla olmakla birlikte doğruluğu oldukça yüksek olan bir yöntemdir. Ancak doğruluk değerini örnek kalitesi belirler. Bu sebeple örneklerin karışmaması, kirletilmemesi büyük önem taşımaktadır. Fakat bu yöntem, işlem süresinin 24 saati bulabilmesi açısından gerçek zamanlı kimlik kontrolünde elverişli değildir. Ancak son yıllarda gelişmekte olan DNA yongalar ve mikro diziler gerçek zamanlı uygulamalara da olanak sağlayacaktır.

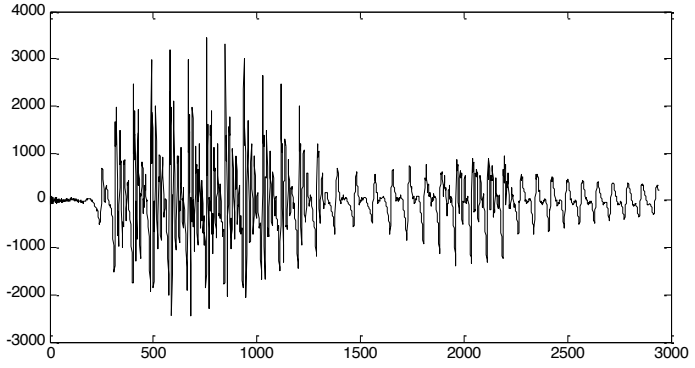
**Kemik iliği nakli yapılmış kişilerde DNA yapısı değişebilmekte ve kimlik doğrulama işlemi zorlaşabilmektedir.**

# DAVRANIŞSAL ÖZELLİK TEMELLİ BİYOMETRİK GÜVENLİK SİSTEMLERİ

Davranışsal özellik temelli biyometrik güvenlik sistemleri, kişilerin davranışsal biyometrik verilerinden faydalanır. Başlıca davranışsal verilerin arasında ses, imza, tuş vuruş dinamiği ve yürüyüş şekli bulunmaktadır.

## Ses

İnsan vücudunda, diyafram, gırtlak, ses telleri, burun, ağız boşluğu, geniz, damak, dil, diş ve dudak gibi organlar ses yolunu oluşturur. Akciğerlerden gelen hava, gırtlakta bulunan ses tellerine çarpar. Ses tellerinin titreşimiyle oluşan ses dalgası, geniz, burun, ağız boşluğu, damak, dil, dişler ve dudakların yapısına göre biçimlenerek konuşmamızı sağlayan sesleri oluşturur. Her insanda, ses yolunun yapısı kendine özgüdür. Dolayısıyla, her insanın konuşması esnasında çıkardığı sesler farklıdır. Bu sebeple, konuşma sonucu oluşan ses verisi, güvenlik sistemlerinde kimlik doğrulama için kullanılabilmektedir. Resim 7.8'de bir ses sinyali örneği görülmektedir.




**Resim 7.8:** Bir ses sinyali örneği.

Ses tanıma temelli biyometrik güvenlik sistemlerinde sırasıyla şu işlemler yürütülmektedir:

- Kullanıcı ilk olarak önceden belirlenmiş bir cümleyi telaffuz eder.
- Telaffuz edilen cümle sonucu ortaya çıkan ses sinyali sayısallaştırılır.
- Sayısal ses sinyali, belirli ön-işlemlerden geçirilir.
- Spektral analiz sonucunda, sinyali temsil eden öznitelikler çıkarılır.

- Özel sınıflandırma yöntemleri kullanılarak, kişinin ses verisi veri tabanında kayıtlı verilerle karşılaştırılır.
- Karşılaştırma sonucunda çıkan değere göre kimlik doğrulama işlemi tamamlanır.

Bu tarz biyometrik güvenlik sistemleri, günümüzde çağrı merkezlerinde yaygın olarak kullanılmaya başlamıştır. Böylece, kullanıcıların bir operatöre bağlanarak "Doğum tarihiniz?", "Doğum yeriniz?" ve "Annenizin kızlık soyadı?" gibi çok sayıda kişisel güvenlik sorusuna cevap vermesine gerek kalmadan, sadece belirli bir cümleyi telaffuz etmesiyle kimlik doğrulaması yapılabilmektedir.


**Kamuya açık alanlarda veya yankılı telefon hatları gibi gürültülü ortamlarda, ses verisi kullanan biyometrik güvenlik sistemleri sağlıklı çalışamayabilir. Ayrıca, kişinin sağlık ve psikolojik durumuna göre sesinin farklılık göstermesi de bu sistemlerin işini zorlaştırmaktadır.**

## İmza

İmza sosyal hayatta kimlik belirleme işlemlerinde sıklıkla kullanılan bir belirteçtir. Herhangi bir belgedeki yazının altında bulunan imza, ilgili yazının o kişi tarafından yazıldığını, okunduğunu ve onaylandığını gösterir. Bu nedenle hukuki açıdan önemi büyüktür. Kişinin imzası her zaman aynı şekilde yazılan isim veya işaretlerden oluşmalıdır. İlgili kişiye ait ve geçerli olabilmesi için her durumda aynı şekilde oluşturulmalıdır. Resmi işlemlerde kimlik doğrulamada oldukça önemli bir yöntem olduğundan ve taklit edilmesi hukuki açıdan imza sahibi kişiyi çok zor durumlarda bırakabilmektedir. Bu nedenle imzanın gerçek sahibine ait olup olmadığını belirleme işlemi oldukça önemlidir. Resim 7.9'da bir imza örneği görülmektedir.


**Resim 7.9:** Bir imza örneği.

İmza tanıma sistemlerinde tanıma işlemi iki farklı açıdan değerlendirilir. Bunlardan ilki davranışsal özellikler, diğeri ise bir desen olarak şeklinin değerlendirilmesidir. Çünkü imza bazı durumlarda desen olarak taklit edilebilir. Ancak imzalama süresi, hızı, ivmesi, kalemin basım şiddeti gibi imzanın atış şeklini belirleyen davranışsal özellikler kişiye özgüdür. Bu davranışsal özelliklerin analizinde gerçek zamanlı imza tanıma yöntemi kullanılmalıdır. Gerçek zamanlı tanıma için matematiksel ya da algoritmik yaklaşımlar kullanılmaktadır. Gerçek zamanlı olmayan sistemler imzayı yalnızca desen olarak inceler. Akıllı bir imza tanıma sisteminin başarısını uygun sayıdaki imza örneği belirler. Ayrıca kullanıcının o anki ruh haline, sağlığına, acelesi olup olmadığına bağlı olarak değişebilmesi de başarımı etkiler.

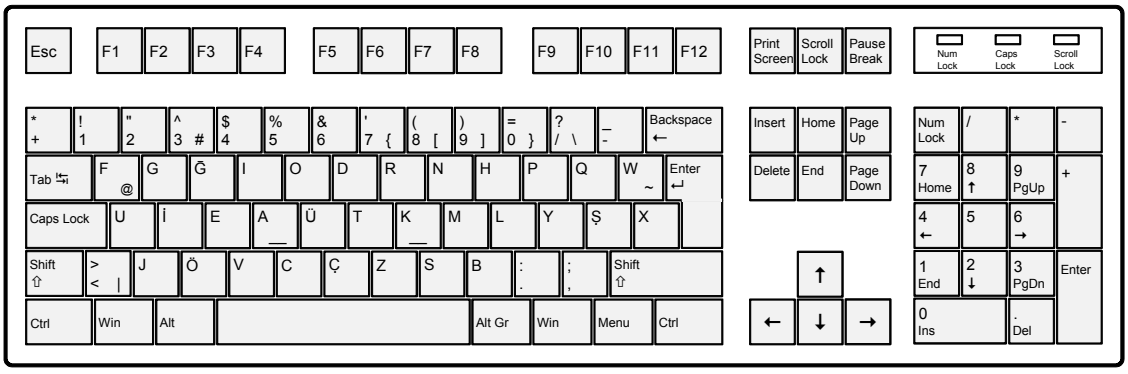
## Tuş Vuruş Dinamiği

Davranışsal biyometrik temelli verilerden biri olan tuş vuruş dinamiği, kişinin klavye kullanarak yazımı esnasında ritmindeki karakteristik bilgilerden kim olduğunu belirlemeye yarayan bir yöntemdir. En basit örneği, ikinci dünya savaşı sırasında, "Göndericinin Vuruşu" (The Fist of the Sender) olarak bilinen ritme bağlı olarak mors alfabesi ile gönderilen mesajın müttefikler veya düşmanlar tarafından gönderilip gönderilmediğini anlamada askeri istihbarat tarafından kullanılmaktaydı. Günümüzde, klavyenin yaygınlaşmasıyla birlikte biyometri alanında kullanımı da yaygınlaşmaya başlamıştır.

Tuş vuruşu dinamiğinde, harflerin, karakterlerin veya rakamların yazımı esnasındaki ritim ve klavye kullanım hızlarını analiz ederek, karşılaştırma yapılacak biyometrik şablon kişiye özgü bir şekilde oluşturulur. Ham veri, tuş basım süresi ve tuş geçiş süresi gibi ölçümlerle oluşturulur. **Tuş basış süresi** bir tuşun ne kadar süre basılı kaldığını gösterir. **Tuş geçiş süresi** ise bir tuştan diğerine geçişin ne kadar zaman aldığını gösterir. Çünkü klavye kullanarak herhangi bir metni yazarken tuş basış süresi ve tuş geçiş

süresi genel yazım hızından bağımsızdır. Metin ne kadar hızlı yazılırsa yazılsın tuş basış karakteristikleri kişiye özgüdür. Kişinin kullandığı dile bağlı olarak aşina olduğu kelimeleri daha hızlı yazabilir. Ayrıca, örneğin kişi solak ise soldaki tuşları daha kolay bulabildiği ve sağdakileri bulmada ise gecikme yaşadığı belirlenmiştir. Bazı durumlarda, herhangi bir işyerinde yönetici belli işlemlerde yardımcı olması için asistanına bilgisayara giriş şifresini vermiş olabilir. Fakat her ikisi de aynı şifre ile giriş yaptığından dolayı bilgisayarın kullanımı esnasında kullanan kişinin yönetici mi yoksa asistan mı olduğu anlaşılamazken, klavye kullanım karakteristiği kimin bilgisayar başında olduğunu ayırt etmeye yarar. Ayrıca son zamanlarda geliştirilen yazılımlarla, fare benzeri bilgisayar bileşenlerinin kullanımında ivmelenme ya da tıklanma frekansı gibi bilgileri tuş vuruşu dinamiği ile birleştirerek değişik karşılaştırma şablonları oluşturabilmektedir. Ancak kişinin yazım stilinin farklı zamanlarda değişiklik gösterebilmesinden dolayı, şablon oluşturulması esnasında çok sayıda örnek alınması gerekmektedir. Uzaktan sohbet programlarındaki yazım esnasında değerlendirmeyi yapacak sistem, başka bir bilgisayarda ise iletimdeki gecikmeler tanıma işlemini güçleştirir. Kişiye bağlı olarak, klavyenin çeşidi ve nerede kullanıldığı da önemlidir. Örneğin hareketli bir araç içerisinde yazım şekli etkilenecektir. Ayrıca, bu biyometrik veri ancak klavye bilgisi olan kişilerde kullanılabilir.

Klavye kullanım stili kişinin yorgun, uykusuz olduğunda ya da bilgisayar, klavye şekli değiştiğinde değişkenlik gösterebilir. Böyle durumlarda fiziksel biyometrik özellikler kadar yüksek ayırt edici özelliğe sahip olmayabilir. Doğrudan birebir aynı olmasa da birbirine benzer tuş vuruş dinamiğine sahip kişiler olabilir. Bu yüzden şifreli kimlik doğrulama yöntemi ile birlikte kullanımı daha yüksek performans sağlayacaktır. Bu açıdan tuş vuruş dinamiği biyometrik veri olarak kullanımda dezavantajlara sahiptir. Ancak diğer biyometrik cihazlarla karşılaştırıldığında özel bir donanıma ihtiyaç duyulmaz. Her bilgisayarda bulunabilen bir klavye yeterlidir.




**Resim 7.10:** Bir klavye örneği.

## Yürüyüş Şekli

Yapılan son araştırmalar, yürüyüş şeklinin kişiden kişiye farklılık gösteren ayırt edici bir özellik olduğunu ortaya koymuştur. Bu sebeple, yürüyüş şeklini biyometrik güvenlik sistemlerinde kimlik doğrulama için kullanmak mümkündür.

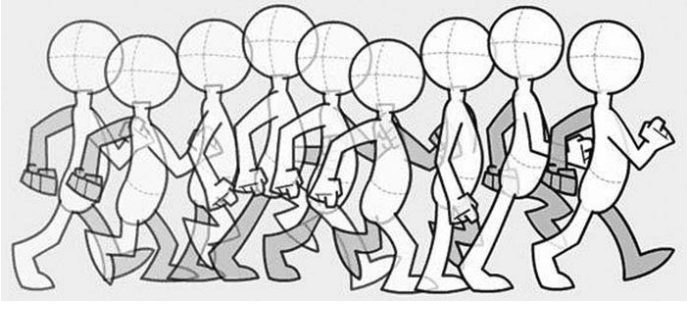
Bu güvenlik sistemlerinde, genellikle tünel veya koridor gibi uzun bir alana görüntü almak için kameralar yerleştirilir. Kişinin bu mekândan yürüyerek geçişi esnasındaki hareketleri kameralar vasıtasıyla kaydedilir. Kaydedilen video üzerinde bilgisayarlı görü yöntemleri kullanarak, kişinin hareketleri tespit edilerek yürüyüş karakteristiğine ait özellikler elde edilir. Son olarak bu özellikler, veri tabanına önceden eklenmiş yürüyüş şekli bilgileri ile karşılaştırılarak kimlik doğrulaması sağlanır.

Yürüyüş şekli verisini kullanan biyometrik güvenlik sistemleri, kişilerin belirli bir mesafe boyunca yürürken görüntüsünün alınmasına ihtiyaç duyduğu için, küçük mekânlarda kullanılamamaktadır. Ancak, havaalanı gibi büyük tesislerde faydalı olabilmektedir. 14 Eylül 2010 tarihli Sabah Gazetesi'nde

yayımlanmış olan bir haber, yürüyüş şeklini kimlik doğrulama için kullanan güvenlik sistemlerine dair güzel bir örneği sunmaktadır:

"*Suçluyu yürüyüşünden tanımak mümkün mü?*

*İngiltere'de yapılan yeni bir araştırmaya göre suçluları yürüyüşünden tanımak mümkün. Southampton Üniversitesi'ndeki araştırmacılar, insanların yürüme şeklinin parmak izi gibi kimlik tespitinde kullanılabilecek kadar birbirinden farklı olduğunu ortaya çıkardılar. BBC'nin haberine göre, içine 12 kamera yerleştirilmiş bir biyometrik gözlem tüneli kullanılan araştırmada, buradan geçen 25 kişinin benzersiz üç boyutlu görüntüleri elde edildi. Bu tekniğin, havaalanlarında güvenliği sağlamak da dahil olmak üzere, farklı amaçlara yönelik kullanılması düşünülüyor. Araştırmayı yöneten Darko Matovski, yürüme şeklinin güvenilir bir biyometrik veri olarak kullanılabileceğinin ilk kez ortaya çıkarıldığını söylüyor. Araştırma ekibi, bu tekniğin havaalanlarındaki pasaport kontrol salonlarında içine kameralar yerleştirilen basit bir koridorla, bir anda çok sayıda kişinin kimliğini tespit etmekte kullanılabileceğini söylüyor. Üniversitenin elektronik ve bilgisayar bilimi fakültesinden olan Matovski, "bir banka soyguncusu yüzünü saklamak için maske takabilir, parmak izi bırakmamak için eldiven giyebilir, saç kılından DNA tespit edilmemesi için şapka kullanabilir, ama ne yaparsa yapsın, bankaya yürüyerek girmek zorunda ve yürüyüşüyle kendini ele verebilir" diyor. Veri tabanına 2000 ayrı yürüme şeklini kaydeden Matovski, kimlik tespitindeki başarı oranının yüzde 95 olduğunu belirtiyor. Yürüme şeklini tespit eden teknik uzaktan da yapılabildiği için, diğer biyometrik tanımlama yöntemlerine göre avantajlı. Ancak araştırmacılar, insanların giyimlerini aşırı bir şekilde değiştirmeleri halinde, doğru tanımlama oranında azalma olabildiğini kaydediyorlar.*"



**Resim 7.11:** Yürüyüş şekli (Kaynak: www.idleworm.com).

## Özet

Gizliliğe dikkat edilen bir mekâna (yüksek güvenlikli tesisler, havaalanları, işyerleri gibi), cihaza (mobil telefonlar, bilgisayar, ATM cihazları gibi) veya bilgiye (internet bankacılığı, çağrı merkezleri gibi) erişim için kimlik doğrulama yöntemleri kullanılır. Bu yöntemler klasik tarzda, şifre ya da kart okutma temelli olabilir. Ancak bu tür sistemlerin kaybolma, çalınma, unutulma risklerinden dolayı, zaman içinde, kişilerin fiziksel ve davranışsal özelliklerini kullanarak otomatik kimlik doğrulama veya tanımlama yapmayı sağlayan biyometrik temelli çalışan güvenlik sistemleri daha avantajlı hale gelmiştir. Kişilerin fiziksel veya davranışsal özelliklerinden elde edilen biyometrik veriler, evrensellik, kalıcılık, ayırt edicilik, erişilebilirlik ve zor kopyalanma gibi niteliklere sahip olmalıdır.

Biyometrik güvenlik sistemleri, algılama, ön işlem, öznitelik çıkarma, şablon oluşturma, eşleştirme ve uygulama gerçekleştirme aşamalarından oluşur. Ayrıca verilerin kayıtlı olduğu bir veri tabanına sahiptir.

Bütün güvenlik sistemlerinde bir kimlik doğrulama yöntemi bulunmaktadır. Biyometrik güvenlik sistemlerinde biyometrik veriye bağlı bir kimlik doğrulama yöntemi kullanılırken, diğer sistemlerde kullanıcı adı, şifre veya PIN gibi bilgilere dayalı olan bilgi temelli ya da anahtar veya manyetik bir kartla çalışan nesne temelli kimlik doğrulama yöntemleri kullanılabilmektedir. Bu kimlik doğrulama yöntemlerinin tek tek kullanımı ya da bir kaçının birlikte kullanımı güvenlik sisteminin seviyesini belirler.

Biyometrik güvenlik sistemi ile herhangi bir yere erişim esnasında tanıtım ve tanıma işlemleri sonucunda kullanıcının yetkili veya yetkisiz olduğu belirlenir. Bu sınıflandırma işlemi değişik matematiksel algoritma, işlem ve karşılaştırmalar kullanılarak gerçekleştirilir. Sistemin performansı ise gerçek uygulamalardaki kullanımı öncesindeki test işlemlerinde elde edilen yanlış ret oranı, yanlış kabul oranı ve çapraz hata oranı ile ölçülür.

İnsanlardaki hayatları boyunca değişmez özelliklere sahip verileri kullanan fiziksel temelli biyometrik güvenlik sistemlerinden başlıcaları; parmak izi, yüz, el geometrisi, iris, retina ve DNA tanımadır. Bu veriler arasında DNA tanıma haricindeki diğer yöntemler anlık olarak yürütülebilen yöntemler olmasına karşılık, bu verilerin elde edildiği organlardaki bir tahribat, eksiklik olması dezavantaj oluşturmaktadır. DNA tanıma ise doğruluk oranı çok yüksek olan bir yöntem olmasına karşılık sonuçlanması 24 saati bulabilmektedir.

Biyometrik güvenlik sisteminin türü, maliyet, kullanım kolaylığı, performans, tanıma süresi gibi faktörlerin önem sırasına göre belirlenir. Davranışsal özellik temelli biyometrik güvenlik sistemleri ise daha karmaşık işlem ve analizler gerektiren, kişiye özgü ardışık bazı hareketlerden elde edilir. Tanıma işlem süresi fiziksel özellik kullanan sistemlere göre daha uzun sürer.

Biyometrik güvenlik sistemleri teknolojinin gelişmesine paralel olarak son zamanlarda donanımsal açıdan büyük gelişme kaydetmiştir. Ayrıca bilimsel alanda da tanıma işlemlerini gerçekleştiren algoritmalar ve yöntemler üzerindeki çalışmalar devam etmektedir. Her geçen gün tanıma oranını yükselten, işlemleri daha hızlı gerçekleştiren tanıma yöntemleri önerilmektedir.

Bu alandaki bir diğer önemli çalışma konusu da biyometrik verileri ham veri halinde depolamak yerine şifreleyerek saklanması le ilgili yapılan çalışmalardır. Tüm bu gelişmeler ve devam eden çalışmalar göz önüne alındığında biyometrik güvenlik sistemleri, önümüzdeki yıllarda daha da gelişmiş halleriyle yaygın kullanıma sahip olacak ve geçmişte belki de sadece bazı bilim kurgu filmlerinde görülen sahneler günlük hayatta çok sıradan hale gelecektir.

## Kendimizi Sınayalım

**1.** Aşağıdakilerden hangisi biyometrik güvenlik sistemlerinde kullanılan fiziksel özelliklerden birisi değildir?

a. Parmak izi

b. Yüz

c. Yürüyüş şekli

d. El geometrisi

e. İris

**2.** _____ doğrulama sistemlerinde, sistem kullanıcıya anahtar veya manyetik bir kart vererek erişimi bu nesne ile yaptırır. Nesne içerisinde doğrulama bilgileri bulunmaktadır.

a. Kaynak kod temelli

b. Nesne temelli

c. Biyometrik temelli

d. Eşleştirme temelli

e. Bilgi temelli

**3.** Retina tanıma temelli güvenlik sistemlerinde hangi ışık kullanılır?

a. Mor ötesi

b. Kızıl ötesi

c. Sarı

d. Mavi

e. Floresan

**4.** Aşağıdakilerden hangisi biyometrik güvenlik sistemlerinin yapısı içerisinde yer almamaktadır?

a. Güvenlik görevlisi

b. Algılayıcı

c. Doğrulama

d. Kayıt

e. Eşleştirme

**5.** Resmi işlemlerde, okuma yazma bilmeyen insanlar için imza yerine _____ kullanılır.

a. parmak izi

b. DNA

c. ses

d. yüz resmi

e. el resmi

**6.** Biyometrik güvenlik sistemlerinde, DNA tanıma işlemini hangi durum güçleştirebilir?

a. Grip olmak

b**.** Ameliyat geçirmek

c. İlik nakli yapılması

d. Makyaj yapmak

e. Peruk takmak

**7.** Kimlik doğrulamada, davranışsal ve desen olarak değerlendirmeye alınan biyometrik veri hangisidir?

a. Ses

b. Yüz

c. Yürüyüş şekli

d. İmza

e. Parmak izi

**8.** Biyometrik güvenlik sistemlerinin performansını karşılaştırmak için ____ kullanılır.

a. yanlış kabul oranı

b. yanlış ret oranı

c. çapraz hata oranı

d. biyometrik oran

e. doğrulama oranı

**9.** Tuş vuruşu dinamiği tanımada, _____ süresi bir tuşun ne kadar zaman basılı kaldığını ölçer.

a. tuş basış

b. tuş geçiş

c. tuşlama

d. giriş

e. çıkış

**10.** Bir soyguncu yüzünü saklamak için maske, parmak izi bırakmamak için eldiven, saç kılından DNA tespit edilmemesi için şapka kullanabilir. Bu durumda, soyguncunun tespiti için hangi biyometrik veri kullanılmalıdır?

a. Yüz

b. Parmak izi

c. El geometrisi

d. DNA

e. Yürüyüş şekli

## Kendimizi Sınayalım Yanıt Anahtarı

**1. c** Yanıtınız yanlış ise "Giriş" başlıklı konuyu yeniden gözden geçiriniz.

**2. b** Yanıtınız yanlış ise "Kimlik Doğrulama" başlıklı konuyu yeniden gözden geçiriniz.

**3. b** Yanıtınız yanlış ise "Retina" başlıklı konuyu yeniden gözden geçiriniz.

**4. a** Yanıtınız yanlış ise "Biyometrik Güvenlik Sistemi Bileşenleri" başlıklı konuyu yeniden gözden geçiriniz.

**5. a** Yanıtınız yanlış ise "Parmak İzi" başlıklı konuyu yeniden gözden geçiriniz.

**6. c** Yanıtınız yanlış ise "DNA" başlıklı konuyu yeniden gözden geçiriniz.

**7. d** Yanıtınız yanlış ise "İmza" başlıklı konuyu yeniden gözden geçiriniz.

**8. c** Yanıtınız yanlış ise "Performans Ölçütleri" başlıklı konuyu yeniden gözden geçiriniz.

**9. a** Yanıtınız yanlış ise "Tuş Vuruş Dinamiği" başlıklı konuyu yeniden gözden geçiriniz.

**10. e** Yanıtınız yanlış ise "Yürüyüş Şekli" başlıklı konuyu yeniden gözden geçiriniz.

## Sıra Sizde Yanıt Anahtarı

### *Sıra Sizde 1*

Daha önceden karşılaştığımız ya da tanıştığımız bir kişi ile sonraki karşılaşmamızda kendisini hatırlamamızı sağlayan en temel biyometrik veri o kişinin yüzüdür.

### *Sıra Sizde 2*

Birden fazla biyometrik verinin birlikte kullanıldığı biyometrik güvenlik sistemleri, sistemin bileşenlerinden herhangi bir biyometrik veri ile ilgili sorunu veya eksikliği olma durumunda yararlı olabilir. Örneğin, parmak izi kullanan bir güvenlik sisteminde, kayıtlı bir kullanıcının bir süre sonra elinde bir tahribat oluşmasından dolayı tanıma işlemi yapılamayabilir. Bu tür durumlarda, aynı sistem örneğin ses verisini de kullanıyorsa, o bilgiyi kullanarak erişim izni alabilir. Böylece mağduriyet giderilmiş olur. Bazı durumlarda ise hepsinin bir arada kullanılması güvenliği daha çok arttıracaktır.

### *Sıra Sizde 3*

Skor histogram grafiği, ROC (Receiver Operating Characteristic) eğrisi, CMC (Cumulative Match Characteristic) eğrisi, alarm grafiği, zoo grafiği, box plot grafiği.

### *Sıra Sizde 4*

Tanıma prensibi ve teknolojilerine göre optik, kapasitif, termal, basınç ve RF temelli sensörler kullanılabilmektedir.

## Yararlanılan Kaynaklar


Daon (2003). **Biometrics and PKI based Digital Signatures**, A short white paper.

Dunstone, T. and Yager, N. (2009). **Biometric System and Data Analysis Design, Evaluation, and Data Mining**, Eveleigh, NSW, Australia.

Özkaya, N. ve Sağıroğlu, Ş. (2006). **Açık Anahtar Altyapısı ve Biyometrik Teknikler**, Ulusal Elektronik İmza Sempozyumu, Ankara, Türkiye.

Pearson, R.L. (2007). **Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions**, Butterworth-Heinemann, Elsevier.

Perronnin, F., Junqua, J.-C., Dugelay, J.-L. (2005). **Biometrics Person Authentication: From Theory to Practice**, EURASIP Newsletter, Volume 16, Number 1.

Sönmez, E.B., Özbek, N.Ö., Özbek, Ö. (2008). **Avuç İzi ve Parmak İzine Dayalı Bir Biyometrik Tanıma Sistemi**, Akademik Bilişim'08, Çanakkale, Türkiye.

Şamlı, R. ve Yüksel, M.E. (2009). **Biyometrik Güvenlik Sistemleri**, Akademik Bilişim'09, Şanlıurfa, Türkiye.


## Yararlanılan İnternet Kaynakları


http://www.biometric-solutions.com

http://www.guvenliksistemleri.gen.tr

http://www.wikipedia.org

# 8

## Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Bilgisayar ve bilişim sistemlerine karşı olası güvenlik tehditlerini tanımlayabilecek,
- Olası tehditlere karşı kullanılabilecek kontrol mekanizmalarını açıklayabilecek,
- Gizlilik, kimlik doğrulama, veri bütünlüğü ve erişilebilirlik kavramlarını tanımlayabilecek,
- Bilişim sistemini meydana getiren bileşenleri ve her bir bileşene karşı yapılabilecek atakları sıralayabilecek,
- Olası tehditleri sınıflandırabilecek,

bilgi ve becerilere sahip olabilirsiniz.

## Anahtar Kavramlar

- Bilişim Sistemi
- Gizlilik
- Veri Bütünlüğü
- Kimlik Doğrulama
- Erişilebilirlik
- Kötü Niyetli Kişi
- Tehdit
- Kontrol
- Kötücül Yazılımlar
- Şifre
- Şifreleme
- Güvenlik Açığı

## İçindekiler

# Bilgisayar ve Bilişim Güvenliği

## GİRİŞ

Canlı ve cansız değerli varlıkları koruma ihtiyacı insanlık tarihi boyunca süregelmiştir. İlk çağlarda insanlar korunmak için mağaralarda yaşamış ve kendilerini her türlü tehlikelerden korumaya çalışmıştır. Orta çağda toplumlar korunmak amacıyla şehirlerin etrafını kalelerle çevirmişlerdir. Kendilerini ve değerli eşyalarını korumak amacıyla değişik surlar inşa edip, belli noktalara okçular yerleştirmişlerdir. Güvenliği artırmak amacıyla kale duvarlarını mümkün olduğunca kalın yapmaya çalışmışlardır. Korunması kolay olması için kaleleri yüksek tepelere yapmışlardır. Kalelere giriş ve çıkışların gerçekleştirilmesi için dayanıklı kapılar inşa etmişlerdir. Bunlara ilave olarak, eğer mümkünse, kalenin etrafına su kanalları açarak güvenliği artırmayı amaçlamışlardır. Kale girişlerine açılır kapanır ahşap köprüler yerleştirerek giriş-çıkışları mümkün olduğunca kontrol altına almaya çalışmışlardır. Kendilerini korumak amacıyla her topluluk güçlü askerlerden oluşan donanımlı ordular oluşturmuşlardır. Bütün bu yapılanlarda tek amaç her türlü tehlikeye karşı insanların hem kendilerini hem de değerli eşyalarını korumaktır.

Günümüzde de durum çok farklı değildir. Sadece gelişen teknoloji ile beraber korunma teknikleri değişmiştir. Her millet korunmayı sağlayacak güçlü ordular oluşturmuştur. Çok değişik teknolojik silahlarla bu ordular donatılmıştır. Kara kuvvetlerine ek olarak, hava ve deniz kuvvetleri oluşturulmuştur. Tehditlere karşı ortak güçler ve birlikler oluşturup değişik antlaşmalarla ortak hareket etmek amaçlanmıştır.

Orta çağ ile karşılaştırıldığında günümüzdeki ataklar (saldırılar) ve bunlara karşı alınan tedbirler çok gelişmiş ve değişmiştir. Teknolojinin gelişmesi ve özellikle haberleşme ve ulaşım alanında olan gelişmeler hem atakları hem de savunma tekniklerini yakından etkilemiştir. Her ne kadar bu gelişmeler tehditleri ve tedbirleri değiştirmiş olsa da orta çağda kullanılan ataklar ve bunlara karşı geliştirilen tedbirler günümüzde gerçekleşen saldırı ve savunma mekanizmalarına örnek teşkil etmiştir.

Her devletin kendi milleti ve toprağını korumayı amaçladığı gibi, her kurum ve kişi de sahip olduğu değerli varlıkları (bu varlıklar canlı veya cansız olabilir) korumak için değişik yöntemler kullanmaktadır. Herhangi bir kurum için ticari değer taşıyan her türlü bilgi, belge, ürün, eşya ve varlık değerli sıfatı taşıdığından bunları korumak ihtiyacı hisseder. Benzer şekilde her aile reisi ailesini ve sahip oldukları değerli varlıkları korumayı amaçlarlar. Kişiler yine kendileri için değerli sayılacak her türlü varlığı korumak isterler.

Gelişen teknoloji ile beraber güvenlik sistemleri de gelişmiştir. Bilgisayarlar, hayatımızın her alanında kullanılıyor olması, farklı alanlarda değişik kolaylıklar sağlaması ve çok popüler olmaları dolayısıyla güvenlik sistemlerinin bir parçası olmuşlardır. Bilişim sistemi bilgi ve verinin bilgisayar desteği ile yönetilmesi demektir. Bilgisayar herhangi bir güvenlik sistemi için basit bir ekran görevi göreceği gibi bir sunucu olarak da kullanılabilir. Ayrıca merkezi bir birimden değişik güvenlik sistemlerinin beraber çalışmasını sağlayan ve bu sistemleri takip eden mekanizma olarak da kullanılabilir. Bu nedenle hem bilgisayar hem de bilişim sistemleri hayatın her alanında olduğu gibi güvenlik sistemleri alanında da kullanılmaktadır.

Bu ünitede genel olarak, bilgisayarların güvenlik sistemlerinin bir parçası olduğu düşünülerek, bilgisayarların ve dolayısıyla bilişim sistemleri güvenliği konusu anlatılacaktır. Temel olarak bilişim

sistemlerinde üç ana bileşenden bahsedebiliriz. Bu temel bileşenler donanım, yazılım ve veri veya bilgidir. Bu ana bileşenlere ek olarak üç yardımcı parça daha vardır. Bu ek parçalar kişiler, ağ ve depolama üniteleridir. Herhangi bir bilişim sistemini bu altı bileşene ayırmanın temel amacı, her bir parçaya karşı yapılabilecek atakları ve bunlara karşı alınabilecek tedbirleri gruplandırmaktır. Her bir bileşenin kendine özgü özellikleri vardır. Mesela, donanım ve donanım sınıfına girebilecek her türlü nesne somut nesne olarak adlandırılabilir. Fakat yazılım grubuna girecek nesneler soyut olarak adlandırılır. Somut ve soyut nesnelerin bir çok özelliği birbirinden çok farklıdır. Bu farklı özelliklerinden dolayı bunlara yapılacak her türlü saldırı da farklı olacaktır. Dolayısıyla bu saldırılara karşı alınacak veya alınması gereken savunma teknikleri de farklı olacaktır. Bu nedenden dolayı herhangi bir bilişim sisteminin güvenliğinden bahsederken sıraladığımız bu parçaları ayrı ayrı ele alarak açıklamak daha doğru olacaktır.

# TEMEL KAVRAMLAR

Güvenlik denince akla ilk gelen fiziksel güvenliktir. Herhangi bir varlığın fiziksel olarak her türlü tehlikeye karşı korunmasına fiziksel güvenlik denir. Bir çocuğun dışarıdan gelebilecek her türlü saldırıya ve tehlikeye karşı ebeveynleri tarafından korunması fiziksel güvenliğe bir örnektir. Herhangi bir kişinin otomobilini her türlü saldırıdan ve oluşabilecek tehditlerden korumak için garaj kullanması da yine fiziksel güvenliğin sağlanmak istenmesindendir. Fiziksel güvenliğe bir diğer örnek ise bir öğrencinin diz üstü bilgisayarını korumak için özel bir çantada taşıması verilebilir.

Bilişim sistemleri güvenliği dediğimizde, genel olarak bilgisayar güvenliğinden bahsedilmektedir. Bilgisayar güvenliği veya bilişim sistem güvenliği demek çok önemli üç özellik olan gizlilik, bütünlük ve erişilebilirlik özelliklerinin sağlanmasıdır. Herhangi bir bilişim sistemine karşı planlanan her türlü saldırı bu üç özelliğin birini, ikisini veya üçünü ortadan kaldırmayı amaçlamaktadır. Bu nedenle ortaya konacak savunma teknikleri de bu üç özelliği sağlayacak ve bunlara karşı yapılabilecek atakları ortadan kaldıracak şekilde geliştirilmelidir.

Gizlilik herhangi bir mesajı veya bilgiyi yetkili kişi veya kişilerin görmesi demektir. Mesela, Leyla arkadaşı Mecnun'a bir mektup göndermek istiyor. Bu mektup ikisi arasında gizli bir mesajı içerdiğinden Leyla göndermiş olduğu bu mektubu Mecnun'dan başka hiç kimsenin okumasını istemez. Leyla'nın gönderdiği bu mektubu ve dolayısıyla mesajı sadece Mecnun'un görmesini ve okumasını sağlamak demek, gizlilik özelliğinin gerçekleşmesi demektir. Çünkü, mesajı gönderen kişi olan Leyla bu mesajın sadece Mecnun tarafından okunmasını istedeğinden ilgili kişi Mecnun'dur. Eğer mesajı Mecnun'dan başka kişi veya kişiler de okursa bu durumda gizlilik ihlal edilmiş olur. Bir diğer örnek şöyle verilebilir. Bir firmada o firmanın müşterilerine ait adres bilgileri olsun. Bu adres bilgileri bu firma için değerli ürün niteliğindedir. Ayrıca bu bilgiler firma için gizli bilgidir. Bu bilgilerin sadece o firmada bu bilgilere erişim yetkisi olan çalışan veya çalışanlarca okunabilmesi gizliliktir. Bu bilgilerin başka firma çalışanlarınca elde edilmesi, okunması ve değişik amaçlarla kullanılması yine gizlilik ihlali olmaktadır. Gizliliği başka bir örnekle şöyle açıklayabiliriz. Mesela, bir firmanın güvenlik sistemlerinin takip edildiği merkezi bir oda olsun. Bu odada güvenlik kameralarının takip edildiği ekranlar olsun. Bu kameraların kayıtlarının da bu odada saklandığını varsayalım. Bu odaya sadece bu odaya girme yetkisi olan kişilerin girebilmesi ve kamera kayıtlarını görebilmesi gizliliktir. Bu odaya giriş yetkisi olan kişiler dışında başka kişi veya kişilerin girmesi yine gizlilik ihlali demektir. Burada gizliliğin sağlanması demek, sadece yetkili kişilerin bu odaya girebilmesidir. Bu odaya sadece bu kameraların görüntülerini ekrandan takip eden güvenlik görevlileri, bu görevlilerin amirleri ve firmanın üst düzey yöneticilerinin giriş yapabilmeleri demek, gizliliğin sağlanmış olması demektir. Çünkü bu kişilerin bu odaya girme yetkileri vardır.

Gizliliği sağlamak için kullanılan geleneksel yöntemlere en güzel örnek mesajların veya mektupların kapalı bir zarf içinde gönderilmesidir. Kapalı bir zarfla gönderilen mesajın veya bilginin anlamı bu zarf içerisinde ne varsa bunun sadece zarfın üzerinde alıcı kısmında ismi yazılan kişi tarafından okunması veya görünmesidir. Eğer bu zarfı, alıcı kısmında adı ve soyadı yazan kişiden başka biri açar ve içindeki mesajı veya bilgiyi okursa, bu durumda gizlilik sağlanmış olmaz. Bu nedenle kurumlarda ve firmalarda gizli diye tabir ettiğimiz her türlü belge kapalı zarflar içinde gönderilir. Alıcı dışında yetkisi olmayan herhangi bir kişinin bu zarfı açması doğru olmaz.

**SIRA SİZDE 1** **Günlük hayatınızdan gizlilik ihlaline neden olabilecek bir örnek veriniz.**

Bütünlük özelliğini iki kısma ayırarak tanımlamak uygun olacaktır. Bunlardan biri kimlik doğrulama dediğimiz orijin veya kaynak bütünlüğüdür. Kimlik doğrulama demek, herhangi bir kişinin iddia ettiği kişi olduğunun kanıtlanması demektir. Mesela, güvenlik kameralarının takip edildiği odaya girecek kişinin gerçekten o odaya girmesi yasak olmayan kişi olduğunu kanıtlamasına kimlik doğrulama denir. Diyelimki Leyla bu odaya girmeye yetkili bir güvenlik görevlisi olsun. Leyla bu odaya girmek istediği zaman kendisinin Leyla olduğunu kanıtlamak zorundadır. Bunun için Leyla'nın yapması gereken kimliğini kanıtlayacak bir belgeyi göstermesidir. Bu belge nüfus kimliği, sürücü belgesi, pasaport veya firmanın kendisine verdiği kimlik kartı olabilir. Bu saydığımız belgeler genel olarak kimlik doğrulama için kullanılan belgelerdir. Bunlara ek olarak kişilerin tam adı, adres bilgileri, anne kızlık soyadları, doğum tarihleri, kendilerine verilmiş herhangi bir numara ve buna benzer kişilerin kimliğini doğrulayabilecek her türlü bilgi ve belge bu amaç için kullanılabilir. Bir başka örnek şu şekilde verilebilir. Herhangi bir firmada çalışan kişiler isimlerinin ve resimlerinin olduğu kimlik kartlarını göstererek veya kendileri için hazırlanmış olan akıllı kartları turnikelere okutarak binaya giriş yaparlar. Bu çalışanların binaya giriş yapabilmek için kendilerinin firmanın bir çalışanı olduklarını, bu kimlik kartları veya akıllı kartlarla kanıtlamaları da kimlik doğrulama demektir. Firma çalışanı olmayan herhangi bir kişinin elinde bu kartlardan olmayacağından ve firmada çalışanlar listesinde ismi olmayacağından, bu kişinin kimliğini doğrulaması mümkün olamayacağından binaya girişi de mümkün olmayacaktır.

Bir diğer bütünlük ise veri veya bilgi bütünlüğüdür. Bu noktada veri veya bilgi bütünlüğünü tanımlamadan önce veri ve bilgi tanımını ve ayrımını yapmakta fayda vardır. Bazı kaynaklarda veri ve bilgi aynı manada kullanılmaktadır. Fakat bu iki kavram arasında fark vardır. Bu farkı bir kaç örnekle açıklayıp daha sonra bu terimleri tanımlamaya çalışalım. Mesela, Güvenlik Sistemleri dersinde son üç yılda öğrencilerin sınavlardan aldıkları notlar veri sınıfına girer. Bu notların incelenerek ve işlenerek, son üç yılda öğrencilerin Güvenlik Sistemleri dersindeki başarı ortalamalarının hesap edildiğini varsayalım. Bu durumda elde edilen başarı ortalamaları bilgidir. Bir diğer örnek şöyle verilebilir. Bir firmanın son 10 yılda güvenlik sistemleri için harcadığı toplam bütçe veri sınıfına girer. Bu toplam bütçe içinde güvenlik personeli için harcadığı bütçenin toplam bütçeye oranını hesap edersek, bu oran da bilgi sınıfına girer. Bu iki örnekden sonra veri ve bilgi kavramları şöyle tanımlanabilir. Veri; üzerinde herhangi bir işlem yapılmamış gerçekler kümesidir. Bilgi ise veri kümesi üzerinde değişik hesaplamalarla elde edilen işlenmiş gerçeklere denir.

Bu tanımlamalardan sonra veri bütünlüğünü açıklamaya çalışalım. Herhangi bir veri veya bilginin yetkisi olmayan kişilerce değiştirilememesine veri veya bilgi bütünlüğü denir. Bundan sona veri bütünlüğü terimini hem veri hem de bilgi bütünlüğü için kullanacağız. Mesela, güvenlik kameralarının günlük kayıtlarının firmanın güvenlik odasında saklandığını düşünelim. Bu kayıtların yetkisi olmayan kişilerce değiştirilememesine veri bütünlüğü denir. Bunların içeriği herhangi bir şekilde yetkisi olmayan herhangi bir kişi tarafından, herhangi bir zamanda, değiştirilmişse bu durumda, veri bütünlüğü ihlal edilmiş demektir. Bir diğer örnek şöyle verilebilir. Güvenlik odasına girme yetkisi olan kişilerin kimlik bilgilerinin saklandığı bir dosya düşünelim. Bu listede ismi olan kişiler, bu odaya girme yetkisi olan kişilerdir. Yetkisi olmayan kişi veya kişilerce bu listenin içeriğinin değiştirilememesi veri bütünlüğüdür. Bunun tersi ise veri bütünlüğü ihlalidir. Bir başka ifadeyle, bu listeye herhangi bir çalışanın isminin yetkisiz kişilerce eklenmesi veya listede adı olan kişi veya kişilerin isimlerinin bu listeden silinmesi veya değiştirilmesi veri bütünlüğü ihlali olur. Veri bütünlüğünü sağlamak için kullanılan geleneksel yöntemlere logo kullanılması, belgelerin mühürlenmesi ve imzalanması gösterilebilir.

**SIRA SİZDE 2** **Kimlik doğrulama ve veri bütünlüğü arasındaki fark nedir? Açıklayınız.**

Erişilebilirlik; herhangi bir sisteminin bileşenlerine yetkisi olan kişilerin belli zamanlarda ulaşabilmeleridir. Mesela, güvenlik personelinden güvenlik odasına girme yetkisi olanların, bu odaya girmeleri gerektiği zaman girebilmeleri erişilebilirliğe bir örnektir. Bir başka örneği şöyle verebiliriz. Firmanın güvenlik kamerası kayıtlarını yetkisi olan kişilerin istedikleri zaman inceleyebilmeleri erişilebilirliğe örnektir. Bazen bilgisayarların ve bilişim sistemlerinin yetkili kişilere servis sağlamasını engellemek için saldırganlar sahte servis istekleri göndererek bilgisayarları ve bilişim sistemlerini bu sahte isteklerle meşgul ederler. Bu durumda sistem servis bekleyen yetkili kullanıcılara servis üretemez olur. Bu durumda erişilebilirlik özelliği ihlal edilmiş olur.


**Erişilebilirlik özelliğini ihlal etmek için gerçekleştirilen atakların genel adı nedir?**

Her türlü maddi ve manevi zarara yol açabilecek veya zarar verme potansiyeli olan her türlü eyleme tehdit denir. Yetkisiz kişilerin turnikelerden geçmeye çalışması, firmanın müşterilerinin bilgilerinin olduğu dosyayı rakip firmaların elde etmeye çalışması ve güvenlik kameralarına zarar verilmek istenmesi tehdit olarak adlandırılır. Bu nedenle zarar verme potansiyeli olan her türlü olayın, metodun, saldırının ve buna benzer her türlü olayın tehdit olarak algılanarak ona göre hareket edilmesi gerekir. Güvenlik sistemlerindeki zaafiyetlere ve açıklıklara zayıf nokta denir. Eğer güvenlik sistemindeki zayıf nokta veya noktaları tespit edebilirsek savunma tekniklerimizi bu zayıflıkları ortadan kaldıracak şekilde geliştirebiliriz. Herhangi bir sistemin güvenliği en zayıf noktasından daha güvenli olamaz. Bir başka ifade ile güvenlik sisteminin güvenlik derecesini, bu sistemdeki en zayıf nokta belirler. Saldırganlar güvenlik sisteminin en zayıf noktasını tespit ederek o noktadan saldırmayı amaçlarlar. Bu zayıflıkları ve olası tehditleri tamamen ortadan kaldıracak veya etkilerini azaltacak her türlü yöntem, teknik, kural ve mekanizmaya kontrol veya savunma denir.


**Herhangi bir bilişim sistemi için tehdit olabilecek bir duruma örnek veriniz. Bu tehdite karşı alınabilecek tedbir olarak bir kontrol mekanizması öneriniz.**

Herhangi bir bilişim sistemine zarar vermek için değişik yollar deneyerek bu sistemelere saldırı yapan kişilere kötü niyetli kişiler denir. Bu kişileri özelliklerine göre aşağıdaki gruplara ayırabiliriz.

- **Amatörler:** Bunlar genelde saldırıları eğlence için yapan kişilerdir. Sisteme zarar vermek amacı gütmeyen bu saldırganların tek amacı, sistemdeki açıklıkları tespit ederek, bu açıklıklardan faydalanmak isterler. Bu gruba giren kötü niyetli kişiler genellikle lise veya üniversite öğrencileridir. Sistemlerdeki açıklıklardan faydalanarak arkadaş grupları arasında eğlenmek isterler. Çoğu zaman yaptıkları saldırıların nasıl sonuçlar doğuracağını bilmezler. Aşağıdaki haber amatörlerin gerçekleştirdiği ataklara güzel bir örnektir:

  *Çikolata Manyağı Bilgisayar Korsanı Tarifleri Değiştirdi (www.tknlj.com, 7 Ağustos 2011)*

  "*Çikolata üreticisi şirket Hershey's'in web sitesine düzenlenen saldırı sonrası, şirket resmi web sitesinden tüketicilerini uyarmaya yönelik bilgilendirme e-postaları yolladı. Yalnız bu hackleme durumunda garip olan şey ise hackerın yalnızca bir çikolatanın tarifini değiştirmekten başka bir şey yapmamış olması. Firma, herhangi bir kredi kartı ya da banka bilgisinin, tarifler ile aynı sunucuda olmasından endişelendi. Ancak burada yalnızca siteye üye olmuş olan kullanıcıların şifreleri, e-posta adresleri, açık adres ve doğum tarihi gibi bilgiler bulunuyordu.*

  *Hershey's'in hackerının yemek takıntısı olan amatör bir tatlı şefi olma olasılığının yanı sıra, şirketin sunucularındaki sistemin açıklarını test etmek ve yaptığı değişikliğin şirket tarafından fark edilip edilmeyeceğini görmek istemesi daha büyük bir olasılık taşıyor. Saldırı sonrası atılan toplu e-postada çikolata üreticisi şirket güçlü şifre oluşturma, şifreleri sıklıkla değiştirme ve şüpheli e-postaların açılması ile ilgili uyarıda bulundu. Şirket aynı zamanda güvenlik sistemlerindeki bu açığı kapatacağına dair söz verdi.*"

- **Hackerlar:** Bunlar kötü amaçlarla bir bilişim sistemine girmeye çalışan kişilerdir. Amaçları sisteme zarar verip, değerli bilgi ve belge elde etmektir. Bu grup saldırganların en çok yaptıkları atak türleri gizli şifreleri ele geçirmek için yaptıkları saldırılardır. Amatörlere göre daha bilinçli hareket ederler. Belli bir amaç doğrultusunda saldırılarını gerçekleştirirler. Bu kişiler ataklarının nasıl sonuçlar doğuracağını bilir ve ona göre hareket ederler. Çoğu zaman amaçları para elde etmek olsa da daha çok şifre kırmayı başardıklarını ve bir bilişim sistemine saldırı gerçekleştirebildiklerini göstermek isterler. Aşağıdaki haber hackerların gerçekleştirdiği ataklara güzel bir örnektir:

  *Sony'ye Yeni Hacker Saldırısı (Milliyet, 7 Haziran 2011)*
  "*Bir grup bilgisayar korsanı, Sony Computer Entertainment'ın kaynak kodlarının bulunduğu bir dosyayı internette yayınlayarak Japon elektronik devi Sony'ye yeni bir saldırı düzenlediğini bildirdi. Daha önce SonyPictures.com'dan geçen hafta bir milyondan fazla kullanıcının şifre, elektronik adres ve diğer bilgileri elde ettiğini açıklayan "Lulz Security" adlı bilgisayar korsanı grup, twitter'daki "@Lulzsec" hesabından, Playstation ve PSP oyun konsolları için yazılım geliştiren şirket Sony Computer Network'un kaynak kodlarını yayınladığını belirtti. Bu kaynak kodlarının ayrıca Sony BMG müzik şirketinin iç yazışma şebekesiyle bağlantılı olduğunu da kaydeden bilgisayar korsanları, Sony'nin online ağlarına son haftalarda düzenlenen siber saldırıların sayısını göstermek için, "Hackerlar:16-Sony:0. Oyuna devam!" ifadesini kullandı.*"
- **Kariyer Suçluları:** Amatör ve hackerlardan farklı olarak kariyer suçluları belli bir hedefe odaklanmış kötü niyetli kişilerdir. Amaçları ne eğlence ne de paradır. Asıl amaçları idealleri doğrultusunda terör ortamı oluşturmak, kargaşa yaratmak, siyasi kriz ve benzeri ciddi sonuçlar doğuracak ortamlar oluşturmaktır. Bu nedenle hem amatörlere hem de hackerlara göre çok tehlikelidirler. Tek başlarına karar alıp uygulamazlar. Tek hareket etmezler. Belli bir siyasi, terör veya dini örgüte üyedirler. Örgüt hedefleri doğrultusunda hareket ederler. Yaptıkları saldırılar çok önemli sonuçlar doğurabilir. Aşağıdaki haber atakların nasıl büyük hedefler amaçladıklarına güzel bir örnektir.

  *Fransa Hükümeti'nin 150 Bilgisaayrı Hack Edildi (www.infoworld.com)*

  "*Fransız ulusal BT sistemleri güvenlik ajansı geçtiğimiz günlerde Fransız hükümeti bilgisayarlarına yapılan saldırılar hakkında detaylı bilgi verdi ve siber-casuslar tarafından hedeflendiklerini söyledi. Fransa maliye bakanlığına yapılan saldırının etkilerini düzeltmek için 150 BT çalışanı hafta sonu büyük bir temizleme operasyonuna girişti. Saldırıda bakanlıkların 170 bin bilgisayarından 150'sine sızılmış.*

  *Saldırı gerçekleştirildiği sırada bilinmeyen veya güvenlik ürünleri tarafından korunmayan güvenlik açıklarını hedefleyen e-posta dalgası ile başlamış. Mesajlar tüm seviyelerdeki bakanlık personelini hedeflemiş ve meslektaşlarından geliyor gibi görünüyor ve ek dosyalar işleri ile ilgili gibi görünüyormuş.*

  *Ek dosyalar açıldığında bilgisayara bir Trojan kuruluyor. Kimliği bilinmeyen saldırganların kontrolündeki bu yazılımlar daha sonra bilgisayarlara sızmada, bakanlığa ait bilgilerin dışarıya gönderilmesinde ve son olarak kendi izlerini gizlemede kullanılmış. Saldırganlar e-posta kutularına ve sunuculara haftalarca erişmişler. Trojan'ın ne yaptığı ve ne kadar yayıldığı ancak geçen hafta farkedilmiş.*

  *Maliye bakanlığına yapılan saldırıların koordinasyonu ve teknik seviyesi bilgisayar korsanlarının kararlı ve organize profesyoneller olduğunu gösteriyor. Bakanlığın internet trafiği kapatıldıktan sonra 150 BT çalışanı hafta sonu temizlik yaparak güvenlik sistemlerini güçlendirdikten sonra Pazartesi günü İnternet bağlantısını tekrar açmışlar.*

  *Bakanlık sözcüsü Pailloux saldırının arkasında kimler olduğu konusunda yorum yapmadı fakat geçen ay Kanada hükümetinin BT sistemlerine yapılanla benzerlik gösterdiğini söyledi. O*

*saldırıda Çin suçlanmıştı ve Çin hükümeti bu iddiaların asılsız olduğunu, kendileri ile bir alakası olmadığını söylemişti. Maliye bakanlığından François Baroin pazartesi günü bir radyo röportajında saldırıların muhtemelen Fransa dışından yapıldığını, bu konuda bazı ipuçları olduğunu fakat doğrulayamadıklarını söyledi.*

*Saldırının G20 organizasyonu sırasında yapıldığı ve hedefin de G20 olduğu düşünülüyor. G20, veya 20 grubu, 19 ülke ve Avrupa Birliğinin maliye bakanlarını ve merkez bankası yöneticilerinin biraraya geldiği bir buluşma. Avrupa Birliğine ek olarak G20 üyeleri Arjantin, Avustralya, Brezilya, Kanada, Çin, Fransa, Almanya, Hindistan, Endonezya, İtalya, Japonya, Meksika, Rusya, Suudi Arabistan, Güney Afrika, Güney Kore, Türkiye, İngiltere ve Amerika var. Ekim ayında da Seul'daki G20 konferansı kuzey koreli bilgisayar korsanları tarafından hedeflenmişti.*

*Son olay mali casuslukta artık sadece firmaların değil hükümetlerin de hedeflendiğini gösteriyor. Hükümet BT sistemlerinin iyi korunması gerektiğini gösteren bir olay daha.*"

# TEHDİT ÇEŞİTLERİ

Bu bölümde bilişim sistemlerine karşı gerçekleştirilebilecek atakları değişik parametrelere göre sınıflandırıp açıklamaya çalışacağız. Tehditleri genel özelliklerine göre aşağıdaki gibi dört ana gruba ayırabiliriz.

1. **Ele geçirme**: Kötü niyetli kişilerin veya yetkisiz kişilerin erişim yetkisi hakkı olmadıkları her türlü bilgi, belge ve varlığı değişik yöntemler kullanarak elde etmeleridir. Bu tür ataklara örnekler şöyle sıralanabilir. Herhangi bir firmanın müşterilerinin bilgilerini içeren bir belgenin kötü niyetli kişilerce kopyalanması bu tür bir ataktır. Telefon veya elektronik posta yoluyla haberleşen iki çalışanın konuşmalarının dinlenmesi yine bu tür saldırılara örnektir. Bu tür ataklarda ele geçirilmek istenen bilgi, belge veya nesnenin görülmesi veya kopyalanması amaçlanır.
2. **Sekteye uğratma**: Bu tür ataklarda kötü niyetli kişiler bilişim sistemine ait herhangi bir parçayı sekteye uğratırlar. Mesela, haberleşen iki kişi arasındaki haberleşmenin kesilmesi, buna en güzel örnektir. Bir başka ifade ile Leyla'nın Mecnun'a gönderdiği mektubu kötü niyetli bir kişinin elde edip Mecnun'a ulaşmasını engellemesidir. Herhangi bir firmanın müşteri listesinin çalınması yine bu tür ataklara örnektir. Ele geçirme ataklarında belgelerin kopyası yapılır veya haberleşme dinlenir. Ama sekteye uğratma ataklarında belgenin aslı çalınır veya haberleşme kesilir. Belge veya mesajın karşı tarafa ulaşması engellenir.
3. **Değişiklik**: Herhangi bir değerli varlığın içeriğinin değiştirilmesidir. Örneğin elektronik posta yoluyla haberleşen iki kişi arasındaki mesajın içeriğinin değiştirilerek karşı tarafa gönderilmesi bu tür bir ataktır. Herhangi bir firmanın güvenlik odasına girme yetkisi olan kişilerin kayıtlı olduğu belgenin içeriğinin değiştirilmesi (yeni bir kişi eklenmesi, mevcut kişi veya kişilerin listeden silinmesi veya mevcut isimlerin değiştirilmesi) de bu ataklara verilebilecek bir örnektir. Çok yaygın olarak kullanılan bir atak çeşitidir. Özellikle yazılım parçalarının içeriğinin değiştirilmesi için yapılan ataklar bu gruba dahildir.
4. **Fabrikasyon**: Sahte nesnelerin yapılmasıdır. Günlük hayatımızda fabrikasyon çok sık rastlanan bir durumdur. Belli nesnelerin sahtelerinin yapılarak satılması, kullanılması ve buna benzer durumlara çok sık rastlarız. Güvenlik odalarına girerken yetkili kişilerin kimlik doğrulama için kullandıkları kimlik kartlarının sahtelerinin yapılması bu tür ataktır. Buradaki amaç sahte kimliklerle kimlik doğrulamayı sağlayarak erişim hakkı olmayan yerlere yetkisiz kişilerin girmesini sağlamaktır.

**Ele geçirme ve sekteye uğratma saldırıları arasındaki fark nedir? Bir örnek vererek açıklayınız.**

Atakları bu dört ana gruba yukarıda bahsedilen özelliklere göre sınıflandırabiliriz. Bu sınıflandırmaya ek olarak saldırı çeşitlerini somut ve soyut nesnelere karşı yapılmış ataklar olarak da iki ana gruba bölebiliriz. Somut nesneler elle tutulur nesnelerdir. Bilişim sisteminin parçaları olan bilgisayar donanımı, ağ kabloları, depolama üniteleri ve buna benzer nesneler somut nesneler sınıfına girer. Somut nesnelerin tersi olan ve elle tutulmayan nesnelere soyut nesneler denir. Bilişim sistemindeki bilgisayarımızdaki yazılımlar, bilgi ve veriler bu gruba girer. Somut ve soyut nesnelerin farklı özellikler göstermesinden dolayı bunlara karşı yapılabilecek ataklar da farklı olacaktır. Bu atakların farklı olmasını kılan bu özellikleri aşağıdaki gibi dört ana başlıkta toplayabiliriz.

Birincisi, fiziksel temastır. Somut nesnelere yapılacak ataklarda fiziksel temas gereklidir. Fiziksel temas olmadan somut nesnelere karşı herhangi bir atak mümkün değildir. Garaja park edilmiş bir arabayı çalmak, bir öğrencinin dizüstü bilgisayarına tekme atmak, herhangi bir güvenlik sistemi parçasının prize bağlı elektrik kablosunu keserek devre dışı bırakmak ve bir bankanın çelik kasasındaki altınları çalmak için fiziksel temas şarttır. Görüldüğü gibi fiziksel temas olmadan yukarıda bahsettiğimiz saldırıları, bu somut nesnelere karşı gerçekleştirmek mümkün değildir. Fakat bir bilgisayara kayıtlı bilgileri internet üzerinden ve uzaktan yapılacak bir atak ile ele geçirmek mümkündür. Bu bilgileri çalmak için bunların kayıtlı olduğu bilgisayara fiziksel temas yapmaya gerek yoktur. Burada bir noktaya dikkat çekmek gerekir. Eğer bilgisayarda kayıtlı bu bilgiler yazıcıdan çıkarılarak bir dökümana basılırsa, soyut nesne sınıfına giren bu bilgiler artık somut nesne olmuştur. Kağıda basılı bu bilgileri çalmak için artık fiziksel temas şart olmuştur. Başka bir örneği şu şekilde verebiliriz. Herhangi bir kişinin banka hesabındaki paranın kötü niyetli kişilerce internet üzerinden başka bir hesaba aktarılması, yine soyut nesnelere karşı yapılmış bir ataktır. Ama aynı kişinin bankadaki kasada korunan altınlarını çalmak için bankadaki kasaya ulaşmak ve fiziksel temasda bulunmak gerekir.

İkincisi ise hacim veya büyüklüktür. Hacim farklılığından kaynaklanan ataklar birbirinden farklıdır. Somut nesnelerin hacmi çok küçük ve çok büyük değerler arasında değişmektedir. Mesela, bir otomobil ile dizüstü bilgisayarın hacimleri birbirinden çok farklıdır. Pahalı bir otomobili güvenli şekilde saklamak istediğimizde, otomobilin büyüklüğüne göre bir garaja ihtiyaç vardır. Dizüstü bilgisayarın güvenli korunması için bilgisayarın içine sığabileceği bir çanta yeterli olmaktadır. Çok değerli olan bir alyans yüzüğü saklamak için çok büyük alanlara ihtiyaç olmaz. Kısacası, somut nesnelerin saklanması için ihtiyaç duyulan saklama alanları, bu nesnelerin hacimleri ile ilişkilidir ve bu alanların büyüklüğü, somut nesnenin hacmine göre çok büyük değişiklikler göstermektedir. Soyut nesnelerde ise durum çok farklıdır. Çok değerli olan bir bilgiyi ikili değerler (0 ve 1) cinsinden sayısal olarak bilgisayarımızda saklayabiliriz. Bunun için somut nesnelerin saklanması için gerekli büyük hacimlere gerek yoktur. İnternetten takip ettiğimiz hesaplarımızda büyük miktarlarda parayı sakladığımızı söyleyebiliriz. Kötü niyetli kişiler somut nesneleri çaldıklarında onları saklayabilecekleri alanlar ile soyut nesneleri ele geçirdiklerinde ihtiyaç duyacakları alanlar birbirinden çok farklı olacaktır. Bu nedenle somut ve soyut nesnelere karşı yapılacak ataklar ve bu saldırılara karşı alınacak tedbirler bu nesnelerin hacimlerine göre değişiklik gösterecektir.

Üçüncüsü ise saldırı yapılacak nesnelerin hareket kabiliyetidir. Somut nesnelerin hareket kabiliyeti soyut nesnelerin hareket yeteneğine göre çok azdır. Mesela, bir firmaya ait otomobili çalıp başka bir yere götürmek çok zahmetlidir. Ama aynı firmaya ait bilgisayarda kayıtlı değerli bir bilgiyi, internet üzerinden çok uzak mesafelere zahmetsizce göndermek çok kolaydır. Genellikle küçük somut nesnelerin çalınarak uzak mesafelere taşınması, büyük somut nesnelere göre daha kolaydır. Soyut nesnelerin ise her türlü somut nesneye göre çalınıp hareket ettirilmesi çok daha kolaydır. Kısacası, somut ve soyut nesnelerin farklı hareket kabiliyetleri, onlara karşı olacak saldırıları ve bu saldırılara karşı alınacak önlemleri etkilemektedir.

Sonuncusu ise nesnelere biçilen değerdir. Nesneler değerli oldukları sürece koruma altına alınır. Buna ek olarak kontrol mekanizmaları için harcanan paralar, işçilik ve her türlü gider nesnelerin değerlerine göre belirlenir. Genel olarak, somut nesnelerin fiyatı bellidir ve zaman içinde hangi değere sahip olacakları tahmin edilmektedir. Mesela, bilişim sistemlerinde donanımın değeri zaman geçtikçe düşmektedir. Herhangi bir somut nesnenin beş veya on yıl sonra ne değer alacağı tahmin edilebilir. Fakat çoğu soyut nesnenin değerinin zamanla nasıl değişeceğini önceden tahmin etmek çok zordur. Mesela, soyut nesne grubuna giren bir bilginin değeri çok farklı değerler alabilir. Bugün çok değersiz olan bir

bilgi beş yıl sonra çok değerli olabilir. Benzer şekilde bugün için çok değerli olan bilgi on yıl sonra çok değersiz olabilir. Bir örnekle bunu şöyle açıklayabiliriz. Diyelimki iki ülke arasında devam eden bir savaş var. Her iki ülkenin askeri bilgilerini savaş sürdüğü sürece bilmek ve ele geçirmek çok önemlidir. Böyle bir bilgi savaş sürdüğü sürece değerlidir. Fakat bu iki ülke arasındaki savaş sona erdiğinde bu bilginin herhangi bir değeri yoktur.

# BİLİŞİM SİSTEMİ KONTROL MEKANİZMASI ADIMLARI

Herhangi bir bilişim sistemi, bina, firma veya kurumun güvenliğini sağlayan her türlü güvenlik sistemine karşı gerçekleştirilecek atakların temel amaçları benzerdir. Aynı şekilde belli özelliklere göre değişiklikler gösterseler bile, yapılacak ataklar da birbirine benzer. Saldırıların amaçları ve atak türleri benzer olduğu gibi, bu saldırılara karşı alınması gereken tedbirler ve yapılması gerekenler de benzerlik gösterir. Bilişim sistemlerine ve genel olarak güvenlik sistemlerine karşı yapıbilecek saldırılara karşı alınması gereken tedbirleri, yapılması gerekenleri veya kontrol mekanizması basamaklarını üç ana başlıkta toplamak mümkündür.

## Engelleme

Engelleme adımında yapılması gerekenleri de kendi içinde üç alt basamağa ayırabiliriz. Bunlar tamamen engelle, saldırıyı zorlaştır ve hedef saptır. Bu alt adımları sırasıyla açıklamaya çalışalım. Engelleme adımında ilk önce yapılması gereken şey, oluşabilecek her türlü saldırıyı tamamen engellemektir. Ama gerçek hayatta bu amacı gerçekleştirmek mümkün olmamaktadır. Bir saldırının gerçekleşmesini tamamen engellemek imkansız bir amaç olarak değerlendirilmektedir. Atakları tamamen engellemek çok zor olduğundan bu atakların gerçekleştirilmesini zorlaştırmak gerekmektedir. Eğer tamamen engellenemiyorsa, bu saldırıların gerçekleştirilmesi mümkün olduğunca zorlaştırılmalıdır. Eğer bu da mümkün olmuyorsa, bu durumda, hedef saptırma yöntemi kullanılarak saldırıları asıl hedeften sahte hedeflere yönlendirmek gerekir. Politikacılar, sanatçılar ve iş adamlarının gazetecilerden kurtulmak için kullandıkları yöntemler hedef saptırma olarak adlandırılabilir. Ana çıkış kapısından otomobil ile çıkış yapıyormuş gibi göstererek gazetecileri o yöne yönlendirmek mümkündür. Daha sonra bu kişi arka kapıdan başka bir araçla uzaklaşarak gazetecilerden kurtulmayı başarabilir. Firmaya ait çok gizli bilgilerin olduğu dosyalara olacak saldırılarda, hedef saptırmak için kötü niyetli kişilerin dikkatini çekecek şekilde sahte dosyalar oluşturarak bu saldırganları bu dosyalara yönlendirmek mümkündür. Bu da yine hedef saptırma olarak kullanılacak bir yöntemdir. Bilişim sistemlerinde hedef saptırmak için kullanılan yöntemlerin genel adına bal kavanozu adı verilir. Nasıl ki yaban arılarını belli bir noktaya toplayarak onları sahte bir hedefe yönlendirmek istediğimizde bal kavanozları kullanılıyorsa, benzer şekilde kötü niyetli kişileri sahte hedeflere yönlendirerek asıl hedeften saptırabiliriz. Hedef saptırma hem günlük hayatta hem de bilişim sistemleri güvenliğinde yaygın olarak kullanılan bir yöntemdir.

## Tespit Etme

Eğer saldırılara tamamen engel olamıyorsak, bu durumda saldırıların olması kaçınılmazdır. Çoğu zaman saldırılar birinci adımı geçerler. Bir saldırı olduğunda ikinci aşamada yapılması gereken bu saldırıların tespit edilmesidir. Herhangi bir atak olduğunda, bu atağı tespit edebiliyor olmamız lazım. Bunun için sürekli korumaya çalıştığımız sistemi, binayı, firmayı ve buna benzerleri gözlem altında tutmalıyız. Gözlem yapmaya ek olarak saldırı tespit araçlarından yararlanabiliriz. Yapılması gereken en önemli şey gözlemdir. Bir binanın güvenliğinden sorumlu isek yapmamız gereken en önemli şeylerden biri 24 saat süreyle bu binayı gözetlemektir. İkinci kullanılan yöntem ise saldırı tespit sistemleridir. Bu sistemler, bilişim sistemlerini kötü niyetli kişilerin her türlü saldırısından korumak için sistemi sürekli izleyen kontrol mekanizmalarıdır.

## Kurtarma veya Geri Alma

Saldırıları tespit ettikten sonra bu saldırıların sistemimize verdiği zararları belirlemek gerekir. Sistemin hangi parçalarında ne kadar ve nasıl zararlar oluştuğunu tespit ettikten sonra, bu zararların telafi edilmesi sağlanmalıdır. Mesela, güvenlik odasına erişim hakkı olan yetkili kişilerin bilgilerinin yazılı olduğu

belgeyi bilgisayarımızda saklamış olalım. Eğer yetkisiz kişiler bu dosyaya ulaşır ve bu dosyanın içeriğini değiştirir veya tamamen yok ederlerse, kaybolan veri veya bilgiyi yeniden elde etmemiz gerekir. Bu nedenle bu dosyanın bir kopyası da başka bir güvenli yerde saklanır. Herhangi birinin kaybolması veya içeriğinin değişmesi durumunda diğer kopyadan yararlanarak orijinal veriye yeniden ulaşmamız sağlanır. Bunun yanında saldırıyı gerçekleştiren kötü niyetli kişilerin tespit edilmesi ve gerekli hukuki sürecin de başlatılması gerekir.

# SALDIRILAR

Daha önce bahsedildiği gibi bilişim sistemini oluşturan üç temel unsur vardır. Bunlar donanım, yazılım ve veridir. Bu bölümde öncelikle bu üç temel bileşene karşı yapılabilecek atakları ve bu bileşenlerin ana özelliklerinden bahsedeceğiz. Daha sonra bilişim sisteminin ek bileşenleri olan kişiler, ağ ve depolama ünitelerine karşı yapılabilecek saldırılardan bahsedeceğiz.

## Donanıma Yapılan Saldırılar

Bilişim sistemlerinde donanım olarak adlandırdığımız parçalar bilgisayar kasası, ekran, klavye, fare, ağ kabloları, bilgisayar kasası içerisindeki ana kart, işlemci, hafıza ve buna benzer somut nesnelerdir. Donanım ve parçaları somut nesne sınıfına girdiğinden, yazılım ve yazılım bileşenlerine göre daha gözle görülür ve elle tutulur nesnelerdir. Donanım fiziksel veya somut parçalardan oluşur. Bu nedenle hem güvenlik görevlileri hem de kötü niyetli kişiler sisteme bağlı olan donanım parçalarını kolaylıkla görebilir. Donanıma karşı yapılabilecek saldırıları şöyle sıralayabiliriz:

- Yeni parça eklenebilir veya parça çıkarılabilir.
- Donanım parçaları üzerine işlevlerini engelleyecek şekilde su ve değişik içecekler dökülebilir.
- Ağ kabloları kesilebilir.
- Donanım bileşenleri çalınabilir.
- Elle veya değişik kesici aletlerle donanımlara zarar verilebilir.


**Yukarıda listelenen saldırılardan başka bilişim sistemlerinde donanımlara karşı yapılabilecek saldırılara bir örnek veriniz.**

## Yazılımlara Yapılan Saldırılar

Bilgisayar sistemlerinde yazılımlar iki ana gruptan oluşur. Bunlar sistem yazılımları ve uygulama yazılımlarıdır. Sistem yazılımlarına örnek işletim sistemidir. Uygulama yazılımlarına örnek ise ofis programlarıdır. Bunlar kelime işlemci, işlem tabloları, elektronik posta yazılımları ve buna benzer programlardır. Yazılımlara karşı yapılabilecek saldırılar şunlardır:

- Yazılımlar başka bir yazılımla yer değiştirilebilir.
- Yazılımların içeriği değiştirilebilir.
- Yazılımlar tamamen yok edilebilir.
- Yazılımlar olması gereken yerden başka yerlere yüklenebilir.
- Yazılımlar çalınabilir.
- Başkalarına ait olan yazılımlar izinsiz kopyalanabilir.

Yazılımlara karşı yapılabilecek ataklar bazen gözle görülebilecek şekilde çok açıktan olabilir. Mesela, saldırıya uğramış bir yazılım artık çalışmıyor olabilir. Bu durumda, bu yazılımın saldırıya uğradığı kanaatine varılabilir. Fakat yazılımlara karşı yapılan çoğu atak farkedilemeyecek değişikliklere yol açar. Görünüşte yazılım normal olarak çalışıyor görünür. Fakat ön tarafta normal çalışıyor görünen program arka tarafta başka işler yapıyor olabilir. Donanıma karşı yapılacak saldırılara göre yazılımlara karşı olan atakları tespit etmek daha zordur.

Yazılımlara karşı yapılacak saldırılarda ana amaç yazılımların değiştirilmesidir. Bu amaca yönelik saldırılara kötücül yazılım denir. Bu bölümde bu tür kötücül yazılımlardan en bilinenleri kısaca özetlenecektir.

## Virüsler

Virüs yazılımlar kötü etkilerini bir bilgisayardan diğerine bulaştırırlar. Kendini çalıştırmalı ve kendini çoğaltmalı olarak iki gruba ayrılabilirler. Bunlar geliş kaynağı belli olmayan elektronik postalara eklenmiş dosyalardan bulaşabilir. Yine güvenilirliğini bilmediğimiz internet sayfalarında değişik programları bilgisayarımıza yüklemeye çalışırken bulaşabilir. Bu tür virüslere karşı korunmak için virüsleri engelleyen programları bilgisayara kurmanız gerekir. Aşağıdaki haber kötü niyetli kişilerin virüsleri tespit eden ve onları silen anti virüs programlarını atlatabilen virüs yazılımlar ortaya koyabildiklerine güzel bir örnektir.

*Anti Virüsü Atlatan Tehlike! (Milliyet, 19 Eylül 2011)*

*"Anti virüs yazılımları kullanmak işletim sisteminizi zararlı yazılımlardan korumak için en güvenilir yöntemlerden biri. Fakat her geçen gün gelişen güvenlik yazılımları tarafından fark edilmemeyi hedefleyen virüsler de sürekli yeni yöntemler deniyorlar. Son ortaya çıkan virüslerden biri kendini korumak adına, benzerleri gibi işletim sisteminin içerisinde değil bilgisayarın BIOS'un da saklanmayı tercih ediyor.*

*BIOS ROM'da saklanan **Trojan.Mebromi** adı verilen bu yeni nesil virüs bilgisayar açıldığı anda, henüz işletim sistemi yüklenmeye başlamadan önce çalışmaya başlıyor. İşletim sistemi çalışmadığı için anti virüs yazılımları devreye girmeden önce zararlı kod parçasını bilgisayarın sabit diskine kopyalayan bu virüs son derece sofistike bir çalışma yöntemine sahip.*

*Anti virüs firması bu zararlı yazılım parçasını bulup temizlese bile bilgisayar yeniden başlatıldığında tekrar çalışan virüs işlemi tekrarladığı için bu kesin bir çözüm olmaktan uzak. Daha da büyük sorun anti virüs firmaları için BIOS ROM içerisindeki bir virüsü temizlemeyi denemek son derece riskli bir işlem çünkü en ufak hata bilgisayarın bir daha açılamayacak hale gelmesine neden olabilir.*

*Şu anda pek çok anti virüs yazılımı **Mebromi**'nin işletim sistemine bulaştırdığı zararlı yazılımları temizleyecek şekilde güncellendi. Bu nedenle anti virüs yazılımınızı sürekli açık ve güncel tutmaya özen göstermeniz ve emin olmadığınız kaynaklardan gelen dosyalar konusunda dikkatli olmanızda fayda var.*"

## Truva Atları

Bu tür kötücül yazılımlar görünüşte normal bir iş yapıyor görünür ama saklanarak arka planda başka işler yaparlar. Bunların çalışması Truva atı olayına benzer. Bilindiği gibi Truva atı, kral Odysseus'un çok güvenli ve güçlü olan Truva surlarını aşmak ve şehre gizlice girmek için yaptırdığı tahtadan at maketidir. Maket atın içine saklanan askerler gecenin sessizliğinde maketten çıkarak kaleyi içten fethetmeyi başarmışlardır. Benzer olarak Truva atı saldırılarında, bilgisayarımıza kurduğumuz herhangi bir program görünüşte istediğimiz işi yapar. Fakat arkadan bilgisayarımıza ve belgelerimize zarar verecek kötü işleri yapar. Görünüşte çok masum görünen program aslında kötücül işler yapmaktadır. Aşağıdaki haber Truva atlarının nasıl zararlı olabileceklerine güzel bir örnektir.

*Banka Hesabına Truva Atı Tehditi (Milliyet, 14 Ağustos 2011)*

*"Bilgisayar korsanlarının tüm dünyadaki bir numaralı hedefi bankalar. Bank of America, Wells Fargo, Citibank ve HSBC gibi küresel bankalar dışında rotasını Türkiye gibi gelişmekte olan ülkelerin bankalarına çeviren bilgisayar korsanları, mevduat sahiplerinin hesabını truva atı yöntemiyle boşaltıyor.*

*Korsanlar, müşterinin anlayamayacağı kadar küçük kesintilerle hesaplardan para çekiyor veya aylarca bilgi toplayıp bir gecede milyonlarca liralık vurgun yapabiliyor.*

*Özellikle Bank of America, HSBC, Wells Fargo, JP Morgan Chase, US Bank, Citibank gibi küresel finans kuruluşları ve bankalar bilgisayar korsanlarının sürekli tehdit ettiği kurumlar listesinde ilk sırayı oluşturuyor. Bankaların güvenlik önlemlerine büyük yatırım yapmalarına rağmen tehdit devam ediyor.*

*Ancak bilgisayar korsanları, daha az güvenlik önlemi alan gelişmekte olan ülkelerin bankalarını da seçiyor. Türkiye, hızla artan alternatif bankacılık uygulamaları yüzünden bu tür korsanların açık hedeflerinden biri haline geldi. İHS Telekom Genel Müdürü Emre Sayın, Türkiye'nin de hem uluslararası bankaların yatırımları hem de korsanların savunmasız banka arayışı ile hedef ülkeler arasında olduğunu söylüyor. İnternet bankacılığında en önemli tehlikenin kullanıcı bilgisayarına yerleşen truva atı yazılımları olduğunu belirten Sayın, "Bunlar virüs programlarıyla belirlenemiyor, özel bir yazılım gerekiyor. Trusteer bu tür yazılımları belirliyor. Bankalara şimdiye kadar bilinen çok büyük bir atak olmadı. Ancak bu yazılımlar aylarca hesap bilgilerini toplayıp, bir gecede milyonlarca dolarlık vurgunlar yapılabiliyor. Bu örgütler daha çok yasa dışı kuruluşlara destek verme motivasyonuyla bunu yapıyor" diye konuştu.*

*Truva atları vasıtasıyla saldırılar düzenleyen bilgisayar korsanları uzun süre kullanıcıyı takip ederek çok küçük miktarda parayı hesaptan çekiyor. Bazen de aylarca uykuda kalarak sadece bilgi topluyor. En uygun zamanı yakalayıp milyonlarca lirayı hesaptan boşaltıyor. Cep telefonuna uyarı gelecek kadar büyük dilimlerde para çekilmiyor. Hesap sahibi uzun yolculuklara çıktığında cep telefonu kapalıyken de harekete geçiliyor.*"

## *Tuzak Kapanı*

Kullandığımız herhangi bir programda gizli bir giriş noktasının olmasıdır. Mesela orta çağda korunmak amacıyla inşa edilen bir kale düşünelim. Bu kaleyi yapan kişilerin gizli bir giriş kapısı inşa etmeleri bu tuzak kapanına örnektir. Bu kişiler daha sonra bu gizli kapıyı kullanarak kaleyi koruyan askerlere görünmeden kalenin içine rahatlıkla girip istediklerini yapabilirler. Tuzak kapanı atakları yazılımlarda benzer şekilde çalışır. Aşağıdaki haber tuzak kapanları ve virüsler vasıtasıyla neler yapılabileceğine güzel bir örnektir.

*İsrail, Suriye'nin Radarlarındaki Görüntüyü Durdurdu (Milliyet, 3 Temmuz 2010)*

*"İsrail uçakları, 6 Eylül 2007'de, Türkiye'nin Suriye sınırından 120 kilometre içerde bir inşaatı bombaladı. Kuzey Koreliler'in yardımıyla inşa edilen bir nükleer tesis olduğu zannedilen bina gece içinde yerle bir edildi. Suriyeliler'in ise, olaydan ancak sabah uyandıklarında haberleri oldu. Oysa Rusya'dan satın aldıkları güçlü radarların İsrail uçaklarının hava sahasına girişini görüntülemiş olması gerekirdi. Soruşturmanın ardından İsrail'in Suriye savunma ağına yerleştirdiği bir virüsle radarlardaki görüntüyü dondurduğu ortaya çıktı. Yani İsrail uçaklarının ülke sınırları içinde olduğu anlarda Suriyeli askeri yetkililer tertemiz bir radar görüntüsü izliyorlardı ve dolayısıyla olaysız bir gece yaşadıklarını zannediyorlardı.*

*"Sanal Savaş" kitabının yazarı ve ABD Savunma Bakanlığı (Pentagon) danışmanı Richard Clarke'ye göre, İsrailliler bu sanal saldırıyı yapmak için üç yöntem kullanmış olabilir:*

*- Saldırıdan önce Suriye hava savunmasına sahasına gizlice sokulan insansız hava aracı (UAV) kendine doğru gelen radar sinyallerini durdurdu. Uçaklar, geriye bozuk sinyal göndererek arızaya neden oldu ve radarda her şeyin sorunsuz gözükmesini sağladı.*

*- İsrailliler, Suriye hava sahasını denetleyen bilgisayar koduna "trapdoor" (tuzak kapanı) yerleştirildi. Ağ sisteminin kontrolünü ele geçirmek için kullanılan sistem radardaki görüntüyü İsrailliler'in istediği gibi değiştirildi.*

*- İsrailli bir ajan, Suriye sınırları içinde internet bağlantısı sağlayan fiber optik kabloyu buldu. Ajan, yakalanma riskini göze alarak virüslü kodu sisteme buradan "enjekte" etti ve radardaki görüntünün kontrolünün İsrailliler'e geçmesini sağladı.*"

Virüsler, Truva atları ve tuzak kapanına ek olarak bilgisayar solucanı, casus yazılım, mesaj sağnağı ve klavye dinleme sistemi gibi daha başka kötücül yazılımlar da mevcuttur. Solucanlar kendilerini bir bilgisayardan diğer bilgisayara otomatik olarak kopyalayan kötücül yazılımlardır. Virüsler kendilerini otomatik kopyalayamazken solucanlar bu işi otomatik yapacak şekilde yazılırlar. Virüsler gibi kaynağı belli olmayan elektronik posta, bu postalara eklenmiş dosya, kaynağı bilinmeyen internet sitelerinden indirilen dosyalar ve program dosyaları vasıtasıyla bilgisayara bulaşırlar.

Casus yazılımlar da yaygın olarak kullanılan kötücül yazılımlardır. Casus yazılımlar adından anlaşıldığı gibi bilgisayar kullanıcılarının bilgilerini bu kişilerin bilgisi olmadan toplayan ve kötü niyetli kişilere gönderebilen kötücül yazılımlardır. Herhangi bir kullanıcının bilgisayarındaki gizli bilgilere ulaşmak için kullanılan yöntemdir. Virüsler ve solucanlar gibi kendini kopyalamaz. Bilgisayar kullanan kişinin gizli bilgilerini bu kişinin bilgisi olmadan gizlice elde etmeyi amaçlar. Bu tür kötücül yazılımlara karşı anti casus yazlımlar geliştirilmiştir.

Mesaj sağnağı elektronik posta kullananlar tarafından sıkça dile getirilen bir tehdit türüdür**.** Spam posta diye de adlandırılır. Elektronik posta kullanan kişilere gereksiz ve uygunsuz elektronik postaların gönderilmesidir. Mesaj sağnağında yaygın olarak kullanılan elektronik postalar genellikle, ürün tanıtımları ve kişileri kandırmaya yönelik bir takım ilgi çekici tekliflerin sunulduğu postalardır. Elektronik posta yazılımlarının bu spam mesajları tespit edebilecek programları mevcuttur. Spam mesajlar veya postalar istenmeyen elektronik mesajlardır. Bu tür mesajlarda dikkat edilmesi gereken bir husus ise, bunların içeriğinin yalan ve yanıltıcı olmasıdır. Değişik vaatler içeren mesajlarla kişilerin banka bilgileri, şifreleri, adres bilgileri ve buna benzer gizli bilgiler elde edilmeye çalışılmaktadır.

Klavye dinleme sistemi ise bilgisayar kullananların bilgisi olmadan klavye üzerindeki tuşlamalarının gizlice takip edilmesidir. Böylece kullanıcıların yaptıkları işlemler takip edilmiş olur.

Aşağıdaki haber spam mesajların ne kadar yaygın olduğuna dair güzel bir örnektir.

*E-posta Trafiğine Spam Darbesi (Hürriyet, 24 Mayıs 2004)*

"*Online güvenlik firması MessageLabs, Nisan ayında spam e-postaların internette dolaşan bütün e-postaların üçte ikisini oluşturur hale geldiğini açıkladı. Spam'de başı çeken ABD'de ise her beş mesajdan dördü istenmeyen mesaj.*

*8 bin 500 müşterisinin e-posta trafiğini yakın takibe alan MessageLabs önümüzdeki yıl bu oranın çok daha artarak yüzde 90'lara ulaşabileceği tahmininde bulundu. Araştırma sonuçlarını değerlendiren MessageLabs'ın pazarlama başkan yardımcısı Biran Czarny "Hiç kimse çöp postaların artış hızını koruyabileceğini tahmin etmemişti, ancak arttılar" dedi.*

*Benzer bir teknoloji kullanarak günde yaklaşık 200 milyon e-postayı tarayan Postini Inc. firması da ABD Kongresi'nde verdiği birbrifingde benzer sonuçlar sundu. Firma, çoğu ABD'de bulunan müşterilerine gelen e-postaların yüzde 83'ünün spam olduğunu açıklarken, bu oranın ocak ayında yüzde 78 olduğunu kaydetti.*

*"Artış trendi devam ediyor" diyen Postini ürün pazarlama direktörü Andrew Lochart, "Spam mesajcılar yeni hileler ve teknikler geliştirmeyi sürdürüyor" şeklinde konuşuyor. Bu teknikler arasında başı spam filtrelerini aşabilen basit mesajlar ve Truva At'ları geliyor. Çöp posta konusunda beşte dörtlük oranıyla en kötü durumda olan ülkenin ABD olduğu kaydedilirken, İngiltere'de bu oranın yüzde 52, Almanya'da yüzde 41, Avusturya'da ise yüzde 32 olduğu ifade ediliyor.*"


**Truva atı ve tuzak kapanı saldırıları arasındaki farkı kısaca açıklayınız.**

## Verilere Yapılan Saldırılar

Donanım ve yazılımlara karşı yapılan saldırılarla karşılaştırdığımızda verilere karşı yapılan saldırıların daha yaygın olduğu görülür. Benzer şekilde donanım ve yazılımla karşılaştırıldığında verinin değerinin daha yüksek olduğu görülür. Donanım ve yazılımın değeri zaman ilerledikçe azalır. Fakat verinin değerinin zamanla nasıl değişeceği bilinemez. Ama genel olarak söylenecek olursa, kötü niyetli kişiler donanım veya yazılımlara saldırı düzenlemek yerine daha çok firmaların veya kişilerin sahip oldukları veri veya bilgileri elde etmeye çalışırlar.

Verilere karşı yapılacak atakları aşağıdaki şekilde açıklayabiliriz.

- Veri içeriğinin değiştirilmesi; bu tür ataklarda kötü niyetli kişilerin amacı veri bütünlüğünü ortadan kaldırmaktır. Bu amaca ulaşmak için içeriğini değiştirmek istedikleri veriye ulaşır ve eklemeler, çıkarmalar veya değişiklikler yaparlar. Mesela, bir şirkette güvenlik odasına girme yetkisi olan kişilerin bilgilerinin olduğu dosyanın içeriğinin değiştirilmesi veri bütünlüğüne karşı yapılmış bir atak çeşididir. Bu tür atakların sebep olabilecekleri zararlar çok farklı olabilir. İçeriği değiştirilmiş bir dosya insan hayatına mal olacak sonuçlar doğurabilir. Mesela, hasta bilgilerinin tutulduğu dosyanın içeriğinin değiştirilmesi bu hastalara yanlış tedavilerin uygulanmasına ve dolayısıyla ölümlere neden olabilir.
- Veri çalınması; herhangi bir kişiye, kuruma veya şirkete ait gizli bilgilerin kötü niyetli kişilerce çalınması olarak tanımlayabileceğimiz bu tür atakların zararları daha çok maddi kayıplar şeklinde olabilir. Örneğin bir şirketin müşteri bilgilerinin olduğu dosyanın saldırganlarca çalınması bu şirketin maddi olarak zarara uğramasına neden olur. Çalınan bu müşteri bilgileri rakip firmaların eline geçebileceğinden rakip firmalar bu bilgileri kendilerine maddi kazanç sağlamak için kullanabilirler. Bu müşterilere çeşitli promosyonlar göndererek kendi şirketlerinden alış veriş yapmalarını sağlayabilirler. Böylece verisi çalınmış firma müşteri kaybına ve dolayısıyla maddi kayba uğramış olur. Aşağıdaki haber veri hırsızlığına güzel bir örnektir.

  *Veri Hırsızlığının Boyutu Çok Büyük (Hürriyet, 4 Mayıs 2011)*

  "*Oyun konsollarının en güvenlisi olarak kabul edilen ve şifreleri kırılmamış olan tek sistem olan Playstation 3'ün hacker saldırısına maruz kalması, milyonlarca kullanıcıyı şok etti. Sony, Everquest, Star Wars: Galaxies gibi büyük ilgi gören çevrimiçi oyunların bulunduğu Sony Online Entertainment (SOE) hizmetinin sunucularını geçici olarak kapatması ardından bilgisayar korsanlarının, bilgilerine eriştiğini düşündükleri müşteri sayısının daha fazla olduğunu açıkladı. Sony'nin geçen hafta saldırıya uğrayan bilgisayar oyunları konsolunda 70 milyonu aşkın müşterinin kişisel bilgilerinin çalınmasından sonra eğlence hizmetlerine de saldırı düzenlenerek müşterilerin kişisel bilgileri çalındı.*

  *Japon elektronik devi Sony, Playstation oyun konsolu kullanıcılarından geçen hafta yaşananlar nedeniyle özür dilemiş, 20 Nisan'dan bu yana hizmet vermeyen Playstation'ı bu hafta içinde yeniden hizmete sokacaklarını bildirirken, kullanıcıları telefon ve e-posta ile dolandırıcılık girişimlerine karşı dikkatli olmaya çağırdı. Ancak şirket 24 saat geçmeden bir bölümde daha veri hırsızlığı olduğunu açıklamak zorunda kaldı. Japon elektronik devi Sony, bu rakamın daha büyük olduğunu, 25 milyon kullanıcısının daha bilgilerinin çalınmış olabileceğini duyurdu.*

  *Sony, büyük ilgi gören çevrimiçi oyunların bulunduğu Sony Online Entertainment (SOE) hizmetinin sunucularını geçici olarak kapatması ardından bilgisayar korsanlarının, bilgilerine eriştiğini düşündükleri müşteri sayısının daha fazla olduğunu açıkladı. Sony, önceleri SOE müşteri verilerinin şirkete yönelik saldırıda çalınmadığının düşünüldüğünü bildirirken, "1 Mayıs itibariyle SOE hesap bilgilerinin de çalınmış olabileceği sonucuna vardık" açıklaması yaptı. Sony, müşterilerin doğum tarihi, cinsiyet bilgileri, yaş, açık adres ve e-posta bilgileri ve banka hesapları bilgilerinin çalınmış olabileceğini kabul etti. Sony, SOE hizmetini kullanan, çoğu Avrupa'da 20 bini aşkın kişiye ait bilgi ve banka hesap ayrıntılarında da güvenlik ihlali olduğunu bildirdi. Çalınan kredi kartı numaraları ve son kullanma tarihlerinin 2007 yılına ait bir veri bankasına dayandığı kaydedildi.*"

## Kişilere Yapılan Saldırılar

Bilişim sisteminin üç temel bileşeni olan donanım, yazılım ve veriye karşı yapılacak saldırıları yukarıda açıkladık. Bu temel bileşenlerin yanında üç ek bileşen vardır. Bunlardan biri kişilerdir. Sistemin ek bileşeni olmasına rağmen kişiler sistemin en önemli parçası olarak düşünülebilir. Kişilere karşı yapılabilecek saldırıları *sosyal mühendislik* olarak adlandırıyoruz. Sosyal mühendislik; kötü niyetli kişilerin kilit konumda olan önemli kişileri değişik yöntemlerle kandırarak veya rüşvet vererek onlar vasıtasıyla gizli bilgileri elde etmelerine denir. Mesala, bir şirketin müşteri bilgilerinin saklandığı dosyayı

bu dosyaya erişim hakkı olan herhangi bir şirket çalışanının para karşılığında rakip firmaya vermesine ikna edilmesi bir sosyal mühendislik atağıdır. Benzer şekilde herhangi bir giriş kapısında duran güvenlik görevlisini değişik yöntemlerle ikna ederek, kapıdan giriş yetkisi olmayan birisinin içeri girmesinin sağlanması da yine sosyal mühendisliğe örnektir. Unutulmamalıdır ki kötü niyetli kişiler önemli kişileri veya kilit konumdaki çalışanları ikna etmek için her türlü yolu deneyebilirler. "Her insanın bir zayıf noktası vardır." sözünden hareketle bu kişiler hakkında gerekli araştırmalar yaparlar. Zayıf noktalarını tespit ettikten sonra bu zayıf noktalarını kullanarak önemli kişileri kandırıp gizli bilge ve belgelere ulaşmayı hedeflerler. Burada dikkat edeceğimiz bir noktayı açıklamakta fayda vardır. Ölümle tehdit ederek veya silah zoruyla belli bilgileri ele geçirmek sosyal mühendislik değildir. Sosyal mühendislikte tehdit ve zorlama yoktur. Kilit insanları değişik yöntemlerle, vaatlerle veya rüşvet vererek kandırmak ve ikna etmek vardır. Aşağıdaki haber sosyal mühendisliği açıklayan güzel bir örnektir.

*Bilgisayarınızı Tehlikelere Karşı Koruyun (Hürriyet, 5 Ocak 2011)*

"*Siber suçların, teknik yollarla çözülebilen teknik bir sorundan ibaret olduğunu düşünmeyin. Bir güvenlik duvarı ve anti virüs yazılımı bilgisayarınızı korusa bile kişisel bilgileriniz güvende değildir.*

*Hacker'lar, sosyal mühendislik olarak adlandırılan güven, cahillik, aç gözlülük, sevilme ihtiyacı, hayırseverlik ve hatta saflık gibi insani niteliklerimizi kullanarak bizi denetim altına alabilirler. En gelişmiş güvenlik yazılımı bile bizi kendimizden korumayı başaramaz.*

*Bu tür saldırılardan korunmak için, hacker'ların başvurduğu bu yöntemlere karşı dikkatli olmalı, kendinizi sosyal mühendislik konusunda bilgilendirmelisiniz.*"

## Ağlara Yapılan Saldırılar

Kişilerin yanında bir diğer ek bileşen ise bilgisayar ağlarıdır. Bilgisayar ağı birden çok bilgisayarın kablolu veya kablosuz birbirine bağlanması ile oluşan yapıya denir. Bina, ev ve buna benzer küçük ölçekli bir alandaki bütün bilgisayarların birbirine bağlanması ile oluşan ağa yerel ağ denir. Yerel ağların birbirine bağlanması ile daha büyük alanları kapsayan ağa ise geniş iletişim ağı adı verilir. Bu ders kapsamında önemli olan yerel ağdır.

Unutmayalım ki herhangi bir bina, kurum veya şirketin güvenliğinin sağlanması için kullanılan bütün güvenlik mekanizmaları (ekranlar, güvenlik kameraları, X-ray cihazları, turnikeler ve buna benzer), bu mekanizmaları kontrol eden bilgisayarlar ve diğer bilgisayarlar kablolu veya kablosuz olarak birbirine bağlanarak bir ağ oluşturur. Ağlara yapılacak ataklar, donanım ve yazılıma yapılabilecek atakların ağ üzerinden gerçekleştirilmesi yolu ile olur. Ağ üzerinde gerçekleştirilebilecek ataklara verilebilecek atak türü DoS veya servis dışı bırakma ataklarıdır. Bu tür ataklarda amaç sistemi çalışmaz hale getirmektir. Bu atakların temelinde sisteme fazla miktarda sahte istek göndererek sistemin gerçek isteklere cevap veremez hale getirilmesidir.

Diğer bileşenlerden farklı olarak ağın kendine özgü özelliklerinden dolayı oluşabilecek güvenlik açıkları da farklıdır. Birincisi, ortak kullanımdır. Bir başka ifadeyle ağlar vasıtasıyla çeşitli kaynaklar değişik kullanıcılar arasında ortak kullanılır. Ortak kullanılan bu kaynaklara erişim hakkı olan birçok kişi vardır. Mesela, bir bilgisayara kimin gireceği bellidir. Fakat ağ üzerinden giriş yapılan bir sunucuya birden fazla kişi giriş yapabilir. Bu nedenle kişi sayısı arttıkça tehdit oluşma potansiyeli de aynı derecede artar.

İkincisi, karmaşıklıktır. Tek bir bilgisayar veya güvenlik kamerası ile karşılaştırıldığında ağlarla birbirine bağlı bilişim sisteminin veya güvenlik kamerası sisteminin karmaşıklığı birbirinden çok farklıdır. Karmaşıklık artıkça sistemin güvenliğini sağlamak o kadar zorlaşır.

Üçüncüsü, nokta sayısıdır. Ağlar birden çok bilgisayar veya herhangi bir güvenlik mekanizma içerdiğinden atak yapılabilecek nokta sayısı fazladır. Kötü niyetli kişiler herhangi bir noktadan saldırı gerçekleştirebilir. Mesela, bir şirketin giriş ve çıkışlar için kullanılan sadece bir kapısı mevcut ise bir güvenlik görevlisi, bir X-ray cihazı veya bir turnike ile giriş ve çıkışlar kontrol edilebilir. Ama birden fazla kapıdan giriş ve çıkışlar yapılıyorsa, kapı sayısına göre kullanılacak kontrol mekanizmaları da

artacaktır. Bir kapı olduğunda, kötü niyetli kişiler bu kapıdan girmeye çalışacaktır. Ama kapı sayısı arttıkça atak yapabilecekleri nokta sayısı da artmış olur.

Dördüncüsü ise bilinmeyen yoldur. Herhangi bir atak gerçekleştirildiğinde, bu saldırı değişik noktaları takip ederek yapılabilir. Hangi makineden veya noktadan saldırının yapıldığını tespit etmek zorlaşır. Aşağıdaki haber servis dışı bırakma ataklarını açıklayan güzel bir örnektir.

*Bilgisayarlara DoS Saldırıları Tekrar Gündemde (Milliyet, 16 Ocak 2007)*

"*Bir tür bilgisayar ağı saldırısı olarak bilinen DoS saldırılarında bilgisayar korsanları, istedikleri Web sitesini çalışmaz hale getirebiliyor. Trend Micro'dan yapılan açıklamaya göre, korsanlar bu saldırıları, kişisel bilgisayarları kullanarak yapıyor. Özellikle büyük Web siteleri bu tür saldırılar nedeniyle büyük zararlar görebiliyor.*

*Bilgisayar korsanlarının eski taktiklerinden biri olan DoS saldırıları tekrar gündeme taşındı. Bir Web sitesinin hizmet verememesine neden olan DoS saldırısında korsanlar, bireysel ve kurumsal kullanıcılarının bilgisayarlarından yararlanıyor.*

*Sistem şöyle işliyor: Bilgisayar korsanı, hiçbir şeyden habersiz bilgisayar kullanıcılarına bir program yüklüyor. Bu şekilde binlerce kullanıcı avlanıyor. Bilgisayar korsanının belirlediği bir güne kadar bu programlar sessiz sedasız bir kenarda bekliyor. Bu programların yüklendiği makinelere zombi makineler deniyor. O gün geldiğinde, bütün bilgisayarlar aynı anda, önceden belirlenmiş bir Web sitesine, giriş talebi göndermeye başlıyor.*

*Bu tür talep gönderen bilgisayar sayısı on binleri bulduğunda, doğal olarak karşı tarafın sunucusu yanıt veremez duruma geliyor. Sonuçta da Web sitesi çöküyor, işlem yapamıyor ve site sahipleri maddi zarara uğruyor. Trend Micro Türkiye Ülke Müdürü Luc-Erol Alptuna, saldırıda kullanılan programcıkların yüklendiği bilgisayarlar ve kurumsal ağların, ciddi bir bantgenişliği darboğazı yaşadıklarını, çünkü bu saldırıların, büyük miktarda veri gönderimi yapılmasını gerektirdiğini kaydetti.*

*Alptuna, saldırılara karşı korunmanın yolunun, bilgisayar ve ağ güvenliği sağlayan çözümlerin kurulmasından ve doğru şekilde konfigüre edilmesinden geçtiğini dile getirdi.*"


**En büyük geniş iletişim ağına ne ad verilir?**

### Depolama Aygıtlarına Yapılan Saldırılar

Elektronik bilgi ve belgelerin saklandığı cihazlar sabit diskler, harici sabit diskler, flaş bellekler, CD'ler, DVD'ler ve bunlara benzer aygıtlardır. Bunlar donanım bileşenleri sınıfına giren somut nesnelerdir. Bu nedenle bunlara karşı yapılabilecek ataklar, donanıma karşı yapılan saldırılarla aynıdır. Depolama cihazlarında saklanan bilgi ve belgenin saldırılarda kaybolması, değiştirilmesi, tahrif edilmesi ve buna benzer zararlara karşı korunmak için yapılması gereken her türlü bilgi ve belgenin bir kopyasının da asıl kopyalara ek olarak saklanmasıdır.

## BİLİŞİM SİSTEMİ KONTROL MEKANİZMALARI

Bu bölümde bilişim sistemlerinin güvenliğini sağlamak için kullanılan yöntemlerden bahsedeceğiz. Hangi yöntem kullanılırsa kullanılsın %100 güvenli bir sistem elde etmek zordur. Değerli varlıklarımızı korumak için çeşitli kontrol teknikleri kullanırız. İnsanlar, korunmak için değişik barınaklar yaparak hayatlarını devam ettirirler. Otomobil ve benzeri araçların korunması için kapalı garajlar kullanılır. Altın, gümüş ve benzeri değerli takılar için özel kilitli kasalar kullanılır. Dizüstü bilgisayarların korunması için çantalar kullanılır. Sahip olduğumuz paraları korumak için banka gibi güvenli olduğunu düşündüğümüz servisleri kullanırız. Bu bölümde, bilgisayar ve bilişim sistemlerini korumak için ve her türlü tehdite karşı koymak için kullanılan en genel kontrol mekanizmaları anlatılacaktır.

## Fiziksel Koruma

Bilişim sistemlerinin fiziksel olarak kontrol edilmesine fiziksel koruma denir. Bu teknikler en tesirli ve kolay metotlardır. Ayrıca diğer yöntemlere göre uygulanmaları daha da ucuzdur. Bu nedenle çok yaygın olarak kullanılırlar. Bilişim sistemlerinin kapalı ve kilitli odalarda bulundurularak, buralara giriş çıkışın kontrollü yapılması fiziksel korumaya örnektir. Herhangi bir şirketin güvenlik sistemlerinin, bilgisayar ve ağlarla takip edildiği ve koordineli çalışmalarını sağlayan sistemler için bir oda kullanırlar. Bu odalar kilitli olur ve buralara girebilecek kişi sayısı kısıtlıdır. Yetkili kişiler dışında başkalarının buralara girmesi kısıtlanmıştır. Gizli bilgilerin yazılı olduğu belgelerin, kilitli özel kasalarda bulundurulması da fiziksel korumaya örnektir. Kurumlarda, şirketlerde, firmalarda ve buna benzer yerlerde görevlendirilen güvenlik görevlilerinin yaptıkları işler de fiziksel koruma olarak adlandırılabilir. Önemli belgeler ve dosyaların yedeklenerek, bu yedeklerinin de saklanması fiziksel kontrole örnektir. Değerli varlıkların güvenlik görevlilerince korunması da yine fiziksel kontrol metodudur.

## Şifreleme

Şifreleme uzun yıllardır kullanılan bir kontrol tekniğidir. Düz metnin karıştırılarak anlamsız hale getirilmesi işlemine şifreleme denir. Şifreleme sonucu elde edilen karıştırılmış metine şifrelenmiş metin denir. Şifreleme işleminin tersi şifre çözme işlemidir. Şifre çözme şifrelenmiş metnin tekrar düz metin haline getirilme işlemine denir. Geleneksel şifreleme algoritmalarına verilebilecek en güzel örnek Ceasar şifreleme algoritmasıdır. Basit bir mantıkla çalışan bu sistemde düz metnin her bir harfi alfabede bu harften sonra gelen üçüncü harfle yer değiştirilir. Düz mesaj içindeki bütün harfler bu şekilde başka harflerle yer değiştirilerek şifrelenmiş metin elde edilir. Mesela, şifrelemek istediğimiz düz metnin bir parçası “Merhaba” olsun. Bu mesajı Ceasar şifreleme algoritması ile şifrelemek istersek mesajdaki ilk harfimiz olan “m” harfinin yerine alfabede bu harften sonra gelen üçüncü harf olan “Ö” harfini yazarız. Benzer şekilde düz metnimizin ikinci harfi olan “e” harfinin yerine alfabede bu harften sonra gelen üçüncü harf olan “Ğ” harfini yazarız. Düz metindeki bütün harfler için aynı işlemi yaparsak şifrelenmiş metin olan “ÖĞTJÇDÇ” metnini elde ederiz.

Şifreleme en güçlü kontrol tekniğidir. Bu metodun güvenliği şifrelemede kullanılan anahtarın gizliliğine dayanır. Mesela, yukarıda örnek olarak verdiğimiz Ceasar şifreleme algoritmasında anahtar üç (3) rakamıdır. Bunun manası düz metindeki her harfin alfabede kendisinden sonra gelen üçüncü harfle yer değiştirilmesi demektir. Mesajı bu şekilde şifrelediğimizde düz metni elde etmek için yine bu anahtara ihtiyaç vardır. Sadece bu gizli anahtarı bilenler şifrelenmiş metni çözebilirler. Mesela, yukarıdaki şifrelenmiş metni alan kişi anahtarın üç olduğunu ve bu metnin Ceasar şifreleme algoritması ile karıştırıldığını bilirse düz metni şöyle elde eder. Şifrelenmiş metindeki harfleri tek tek ele alır. Her harfi alfabede o harfden önce gelen üçüncü harf ile değiştirir. Bu işlemi şifrelenmiş mesajdaki bütün harfler için yaparsa düz metne ulaşmış olur.

## Yazılım Kontrol Mekanizmaları

Yazılımlara karşı olan saldırıları önlemek için kulanılan tekniklerdir. Bunlardan en önemlisi virüs tarayıcılarıdır. Virüslere karşı geliştirilen bu programlar, virüslerin özelliklerine göre tarama yaparak virüs programlarını tespit etmeye çalışır. Bir diğer yazılım kontrol tekniği ise şifre kontrolü programlarıdır.

Şifreler çok yaygın olarak kullanılır. Elektronik posta adresimize girmek için kullanıcı adı ile beraber bizim ürettiğimiz gizli şifremizi gireriz. Herhangi bir kötü niyetli kişi bizim elektronik posta kullanıcı adımızı bilse bile, şifremizi bilmediği sürece elektronik posta heasabımıza giremez. Bazı binalarda veya girişi kısıtlı olan önemli belge ve nesnelerin saklandığı kapalı mekânlara, şifre tuşlayarak girmek gerekir. Bu tür mekânlara girmek için giriş şifresinin bilinmesi şarttır. Benzer şekilde adımıza ait herhangi bir şifreli hesaba girmek için sadece kendimizin bildiği şifreye ihtiyaç vardır. Eğer bu gizli şifreleri kötü niyetli kişiler ele geçirirse bu şifrelerle girilebilen her türlü hesaba girebilirler. Bu nedenle şifreleri seçerken güvenli şifreler seçmeliyiz.

Güvenli şifreler aşağıdaki özelliklere sahip olmalıdır.

- Şifre uzunluğu çok kısa olmamalıdır. Kısa şifreler kötü niyetli kişiler tarafından deneme yanılma yöntemi kullanılarak daha kısa sürede ele geçirilebilir.
- Sözlükte yer alan sözcükler şifre olarak seçilmemelidir. Şifrenizi ele geçirmek isteyen kişi öncelikle sözlükte yer alan sözcükleri deneyecektir. Eğer şifreniz sözlükte yer alan bir kelime ise kötü niyetli kişiler bu şifrenizi deneme yanılma yöntemi ile bulabilecektir.
- Mümkün olduğunca şifreler; harfler, rakamlar ve sembollerden oluşmalıdır. Bu şekilde şifrenin güvenliği artırılmış olur. Şifreyi ele geçirmek isteyenler bütün harf, rakam ve sembolleri denemek zorunda kalacaktır.
- Şifreler güvenliği sağlayacak kadar uzun ama hatırlanacak kadar da kısa olmalıdır. Uzun seçilen şifrelerin hatırlanması zor olacağından insanlar bu tür şifreleri bir yere kaydederler. Fakat şifremizin yazılı olduğu belge başkalarının eline geçerse şifremizi elde etmiş olurlar. Bu nedenle hafızamızda tutabileceğimiz şifreleri seçmek daha uygundur.
- Büyük ve küçük harflerden oluşmalıdır. Bu şekilde şifre harflerini küçük ve büyük harflerden seçersek şifremizi elde etmek isteyen kötü niyetli kişilerin işini zorlaştırmış oluruz. Bütün küçük ve büyük harfleri denemek zorunda kalırlar.
- Doğum tarihi, soyadımız, anne veya baba adı ve buna benzer bilgileri içermemelidir. Şunu unutmayalım ki şifremizi ele geçirmek isteyen kişiler, önce bizimle alakalı bilgilerin şifre seçilmiş olabileceğini düşünerek bu bilgileri denerler. Bu nedenle kendimizle yakından alakalı tarih, isim ve bilgileri şifre seçmekten sakınmalıyız.
- Şifre başka kişilere söylenmemelidir. Şifreler kendimize ait gizli bilgilerdir. Bu bilgileri diğer kişilerle paylaşmamalıyız.

Aşağıdaki haber şifrelerin ele geçirilebileceğine güzel bir örnektir.

*İşte Yaşanmış Gerçek Bir Olay! (Milliyet, 29 Ocak 2010)*

"*Şifrelerinizi akılda kalıcı ama güvenli tutmak istiyorsanız anlamlı kelimelerin baş harflerinden anlamsız bir şifre oluşturun.*

*Akılda tutması biraz daha zor olsa da buna değecektir. Bazı şifre kırıcıların, kullanıcıların özel hayatlarından yararlanmayı sevdiğini aktarırken dalga geçmiyorduk. Croll isimli bir hacker, Google Apps'ın şifre resetleme mekanizmasını kullanarak, bir Twitter çalışanının Gmail hesabını ele geçirdi.*

*Şifre resetleme işlemi, şifresini unutan kullanıcılara özel bir soru soruyor. Croll, Twitter çalışanı hakkında bilgi toplayarak hesabının sorusunu tahmin etmeyi ve ele geçirmeyi başardı. Sonra onun hesabıyla başka kişilerin kişisel bilgilerini öğrendi ve bunları kullanarak daha fazla insanın hesabını hackledi. Bunlar arasında Twitter CEO'su Evan Williams'ın eşi bile vardı.*

*Yani keskin bir zeka ve iyi gözlemcilik insana pek çok kapıyı açıyor.*"

## Donanım Kontrol Mekanizmaları

Donanıma karşı yapılacak saldırılardan korunmak için kullanılan en yaygın kontrol mekanizması fiziksel korunmadır. Bu nedenle bilgisayar ve bilişim sisteminin donanımı güvenli bir odada korunur. Bu odaya giriş ve çıkışlar kontrollüdür. Güvenlik odası dediğimiz bu oda sürekli kilitli tutulur. Bu nedenle her türlü kilit de bir diğer kontrol mekanizmasıdır. Bunlara ek olarak kişilerin kimliklerini doğrulamak için kullanılan her türlü cihaz da donanım kontrol mekanizmaları sınıfına girer.

## Kural ve Prosedürler

Genel olarak kişilerin uyması gerektiği şeylere kural denir. Neyi nasıl yapacağını açıklayan şeylere de prosedür denir. Bir bilişim sisteminin yöneticisi olan kişinin uyması gereken kurallar ve yapacağı işlerde takip edeceği prosedürler bellidir. Benzer şekilde herhangi bir binanın giriş ve çıkışlarını kontrol eden güvenlik görevlisinin de uyması gereken kurallar vardır. Giriş ve çıkışları kontrol ederken uygulayacağı prosedür bellidir.

Bilişim sistemleri güvenliğinde de uyulması gereken kurallar ve takip edilmesi gereken prosedürler vardır. Mesela, kullanıcıların uygulaması gereken prosedürlerden biri kullandıkları şifreleri belli aralıklarla değiştirmeleridir. Aynı şifreyi uzun süre kullanmak tavsiye edilmez. Bu nedenle ara sıra bu şifreleri değiştirmek güvenlik açısından önemlidir. İnternet bankacılığı hizmeti sunan bankalar genellikle üç ayda bir internet bankacılığı şifremizi değiştirmemizi isterler. Bir diğer prosedür ise şifre ile giriş yaptığımız farklı hesaplar için farklı şifreler kullanmaktır. Aynı şifre kullandığımız zaman eğer bir hesabımıza ait şifre kötü niyetli kişiler tarafından ele geçirilirse bu şifre ile diğer bütün hesaplarımıza girebilirler.

Prosedürler genellikle tavsiye niteliğinde olurlar. Herhangi bir zorlama söz konusu değildir. Diğer taraftan kurallara uymak zorunludur. Kurallara göre hareket etmek zorundayız. Şifre ile giriş yapılabilen bir güvenlik odasının giriş şifresi belli aralıklarla değiştirilmelidir diye bir kural konulmuşsa, belirtilen aralıklarla bu şifrenin değiştirilmesi zorunludur.

# GÜVENLİK İLKELERİ

Genel olarak ilke herhangi bir işte kişilere yol gösteren genel dayanak noktası olarak tanımlanabilir. Özellikle bilişim güvenliğinde ve genel olarak güvenlikte ortaya konacak uygulamalarda yol gösterecek dört temel ilke vardır. Bu ilkeleri kısaca şöyle açıklayabiliriz.

1. **En kolay nüfuz etme ilkesi**: Herhangi bir güvenlik sistemine saldırı gerçekleştirmek isteyen kötü niyetli kişi gerçekleştirilebilecek en kolay saldırıyı yapacaktır. Bu nedenle yapılabilecek ataklara karşı alınacak tedbirler planlanırken, saldırganların en kolay yolu deneyecekleri unutulmamalıdır.
2. **Yeterli süre koruma ilkesi**: İnsanlar değerli her türlü varlığı korumak isterler. Herhangi bir şey değerini kaybetmediği sürece korunur. Zamanla değerini yitirmiş hiç bir nesne korunmaz ve çöpe atılır. Yeterli süre koruma ilkesi değerli varlıkların değerlerini kaybetmedikleri sürece korunmalarını söyleyen ilkedir.
3. **Tesirlilik ilkesi**: Bu ilke güvenlik sistemlerinde kullandığımız kontrol tekniklerinin kullanılabilir ve beklenen amaçları gerçekleştirebilir olmalarını gerektiren ilkedir. Herhangi bir kontrol metodunun sağlaması gereken üç temel amaç yeterli güvenlik, kolay kullanılabilirlik ve performanstır. Ama bu üç amaç genellikle birbiriyle çelişen amaçlardır. Bir başka ifadeyle bu üç amaçtan herhangi birisini veya ikisini gerçekleştirmek istersek, diğer iki veya bir amacın belli miktarlarda fedakârlıkta bulunması gerekir. Eğer çok güvenli bir sistem oluşturmak istersek, ya sisteminin performansı düşecektir, ya kullanılabilirliği zorlaşacaktır ya da hem performans hem de kolay kullanılabilirlik kötüleşecektir. Bu nedenle bu üç amaç arasında bir denge oluşturacak şekilde kontrol mekanizmaları kullanmak gerekir. Burada dikkat etmemiz gereken bir başka nokta ise, güvenlik derecesinin, performansın ve kolay kullanılabilirlik derecesinin kişiden kişiye farklılık gösterebileceğidir. Bir kişi için performans en önemli iken başka bir kişi için güvenlik en önemli amaçtır. Bu nedenle istenen amaçlar ve bu amaçların hangi derecede başarılmak istenmesine göre güvenlik sistemi geliştirilir.
4. **En zayıf halka ilkesi**: Bir sistemin güvenliği bu sistemin en zayıf noktasından daha güvenli olamaz. Yani bir sistemin güvenlik derecesini o sistemin en zayıf noktası belirler. Çünkü kötü niyetli kişiler sistemdeki en zayıf noktayı tespit edip o noktadan saldırı gerçekleştirirler. Birinci ilkede bahsettiğimiz gibi saldırganlar en kolay atağı deneyecektir. En kolay saldırı da en zayıf noktadan gerçekleştirilebilir. Güvenlik sistemi tasarlarken zayıf noktaları tespit edip bütün noktaların mümkün olduğunca aynı seviyede güvenli olması sağlanmalıdır.


**Güvenlik ilkelerini sıralayınız.**

# TEHDİTLERE KARŞI YAKLAŞIMLAR

İnsanlık tarihininin ilk gününden günümüze kadar insanlar iyi niyetli kişiler ve kötü niyetli kişiler olarak iki gruba ayrılmıştır. Kötü niyetli kişiler her türlü sistemdeki açıkları ve zayıflıkları tespit edip bu noktalardan saldırılar gerçekleştirir. İyi niyetli kişiler ise yapılabilecek saldırıları tespit edip onları yok edecek savunma mekanizmaları geliştirirler. Bir grup kötü niyetli kişi virüs yazılımları geliştirirken, diğer yandan iyi niyetli kişiler virüs tarama programları geliştirir.

Güvenlik tedbirleri almadan önce sistemin güvenlik açısından incelenmesi çok önemlidir. Burada üç yaklaşım sergilenir. Birincisi, sisteme karşı herhangi bir saldırı olmaz yaklaşımıdır. Bu uç bir yaklaşımdır. Bu yaklaşımda son derece iyi niyetli bir yaklaşım sergilenir. Ama bu kesinlikle doğru değildir. Bu yaklaşımı sergileyenler hiç hırsızlık olayı olmaz deyip evinin kapısını kilitlemeden yatan kişilere benzer. Şirket binama kötü niyetli kimse girmez diyerek, şirket girişlerini kontrol etmek için herhangi bir güvenlik görevlisi veya kontrol mekanizması kullanmayan şirket sahibinin yaklaşımı da buna örnektir.

Diğer yaklaşım ise ilk yaklaşımın tam tersi olan diğer uç yaklaşımdır. Bu yaklaşım ise oluşabilecek saldırıları abartmaktır veya olabileceğinden daha şiddetli olabileceğini düşünerek alınacak tedbirleri ona göre gereksiz şekilde çoğaltmaktır. Eğer şirket binasının girişi bir güvenlik görevlisi ile kontrol edilebiliyorsa, burada iki veya daha çok güvenlik görevlisi çalıştırmak doğru değildir. Başka bir örnek verecek olursak, tek bir kilitle korunabilecek güvenlik odasının kapısını birden çok kilitle kilitleyip önüne bir kaç güvenlik görevlisi yerleştirmek de bu yaklaşıma örnektir.

Üçüncüsü ve uygulanması gereken yaklaşım ise atakların olabileceğini düşünerek, bu atakların olası etkilerini ve zararlarını makul şekilde hesaplayarak ona göre güvenlik tedbirleri almaktır. Korumak istediğimiz sistem ne ise incelenir. Olası zayıflıklar tespit edilir. Korunmak istenen varlıkların değeri belirlenir. Hangi seviyede koruma istendiği belirlenir. Bunlara göre güvenlik sistemi oluşturulur.

## Özet

Bir bilişim sistemini meydana getiren üç ana bileşen donanım, yazılım ve veridir. Bu ana bileşenlere ek olarak yardımcı bileşenler olarak ağ, kişiler ve depolama aygıtları da vardır. Bu bileşenlerin kendilerine özgü özellikleri vardır. Mesela, yazılım bileşeni sınıfına giren parçalar genel olarak soyut nesne grubuna girer. Bunun yanında donanım parçaları somut nesnelerdir. Bu farklı özelliklerden dolayı bu bileşenlere karşı yapılacak tehditler de farklı özelliklerde olacaktır. Tehditler farklı olduğundan bunlara karşı alınacak tedbirler ve kullanılacak kontrol mekanizmaları da yine farklı olacaktır. Donanıma karşı olacak saldırılar genelde fark edilebilir saldırılardır. Fakat yazılıma karşı gerçekleştirilen ataklar o kadar açık olmayabilir. Kişilere karşı olacak ataklar genelde sosyal mühendislik ataklarıdır.

Bilişim sistemlerine karşı oluşacak tehditler; ele geçirme, sekteye uğratma, değişiklik ve fabrikasyon şeklinde dört ana gruba ayrılabilir. Güvenlik sisteminize karşı kötü niyetli kişilerce yapılacak her türlü saldırı bu dört ana tehdit grubundan birinin içinde yer alır. Haberleşmeye çalışan iki kişinin mesajının kötü niyetli kişilerce kopyalanması veya okunması ele geçirmeye örnektir. Bir firmanın müşteri listesinin yetkisiz kişilerce okunması veya kopyalanması da yine ele geçirmeye örnektir. Mesajın ele geçirilerek karşı tarafa ulaşmasını engellemek sekteye uğratmaya örnektir. Ele geçirilen mesajın içeriğinin değiştirilerek karşı tarafa ulaşmasını sağlamak değişiklik atağına örnektir. Son olarak belli ürünlerin sahtelerinin yapılması ise, fabrikasyon olarak adlandırılır.

Güvenlik sistemlerine ve bilişim sistemlerine karşı tehditlerin olması kaçınılmazdır. Bu tehditlere karşı kullanılabilecek kontrol mekanizmaları engelleme, tespit etme ve kurtarma veya geri alma olarak üç ana grupta toplanır.

Tehditlerin oluşmasını tamamen engellemek engelleme olarak adlandırılır. Fakat bu çoğu zaman başarılması güç bir kontrol mekanizmasıdır. Bu nedenle tehditlerin oluşmasını zorlaştırmak veya hedef saptırmak için çeşitli yöntemler kullanılır.

Engelleme gerçekleştirilemiyorsa oluşan tehditleri tespit etmek önemlidir. Bu nedenle sürekli sistemi izlemek ve atakları tespit edecek metotlar kullanmak gerekir. Tehditlerden sonra olası kayıpları ve zararları tespit etmek ve kötü niyetli kişileri bulmak önemlidir.

Bilişim sistemi güvenliğinde başarılmak istenen hedefler gizlilik, kimlik doğrulama, veri bütünlüğü ve erişilebilirliktir. Gizlilik herhangi bir mesajı veya bilgiyi sadece yetkili kişi veya kişilerin görmesi demektir. Yetkili kişilerin dışındaki herhangi bir kişinin bu gizli bilgileri görmesi engellenmelidir.

Kimlik doğrulama herhangi bir kişinin iddia ettiği kişi olduğunun kanıtlanması demektir. Güvenlik sistemlerinde kimlik doğrulama çok önemlidir. Erişim hakkı olan kişilerin gerçekten erişim hakkı olan kişi olduklarını kanıtlamaları gerekir.

Veri bütünlüğü herhangi bir bilgi veya belgenin içeriğinin yetkisiz kişilerce değiştirilmesinin önüne geçilmesidir. Bu içerik sadece yetkili kişilerce değiştirilebilir. Erişilebilirlik ise herhangi bir sisteme yetkili kişilerin belli zamanlarda belli süreyle ulaşabilmeleridir.

Bilişim sistemlerine karşı yapılacak atakları ele geçirme, sekteye uğratma, değişiklik ve fabrikasyon olarak sınıflandırabiliriz. Bir başka sınıflandırma soyut nesnelere ve somut nesnelere karşı yapılan ataklar şeklinde olabilir. Saldırıları bilişim sistemini oluşturan altı ana ve yardımcı bileşene karşı olan ataklar olarak da altı sınıfa ayırmak mümkündür.

Donanımlar karşı olan saldırılar genelde donanım parçalarının çalınması, değiştirilmesi veya yeni parçaların eklenmesi şeklinde olur.

Yazılımlara karşı olan ataklar genelde kötücül yazılımlar olarak adlandırılır. Verilere karşı olan saldırılar verinin çalınması veya değiştirilmesi şeklinde meydana gelmektedir.

Kişilere karşı olan saldırılar ise sosyal mühendislik ataklarıdır. Ağ ve depolama aygıtlarına karşı olabilecek saldırılar ise donanıma yapılan ataklara benzerdir.

Bilişim güvenliğinde ve genel olarak güvenlikte ortaya konacak uygulamalarda yol gösterecek dört temel ilke vardır. Bunlar; en kolay nüfuz etme ilkesi, yeterli süre koruma ilkesi, tesirlilik ilkesi ve en zayıf halka ilkesidir.

## Kendimizi Sınayalım

**1.** Aşağıdakilerden hangisi herhangi bir bilişim sisteminin temel bileşenlerinden değildir?

a. Donanım

b. Yazılım

c. Veri

d. Depolama aygıtları

e. Virüs

**2.** Aşağıdakilerden hangisi bilişim güvenlik sistemlerinin sağlaması gereken özelliklerden biri değildir?

a. Veri bütünlüğü

b. Şifreleme

c. Gizlilik

d. Kimlik doğrulama

e. Erişilebilirlik

**3.** Herhangi bir bilgiyi, veriyi veya mesajı sadece yetkili kişilerin görebilmesi özelliğine ne ad verilir?

a. Kimlik doğrulama

b. Bütünlük

c. Gizlilik

d. Güvenlik

e. Erişilebilirlik

**4.** Aşağıdakilerden hangisi kimlik doğrulama için kullanılmaz?

a. Nüfus Cüzdanı

b. Pasaport

c. Sürücü Belgesi

d. İlk isim

e. Özel kimlik kartı

**5.** Aşağıdakilerden hangisi bir bilişim tehditi çeşiti değildir?

a. Fabrikasyon

b. Ele geçirme

c. Veri toplama

d. Değişiklik

e. Sekteye uğratma

**6.** Herhangi bir nesnenin sahtesini yapma tehditine ne ad verilir?

a. Değişiklik

b. Veri bütünlüğü

c. Zayıf nokta

d. Fabrikasyon

e. Ele geçirme

**7.** Aşağıdakilerden hangisi somut ve soyut nesnelere karşı yapılacak tehditleri etkileyen bir özelliktir?

a. Hareket kabiliyeti

b. Donanım

c. Yazılım

d. Veri

e. İçerik

**8.** Aşağıdakilerden hangisi kötücül yazılımlardan değildir?

a. Virüs

b. Bilgisayar solucanı

c. Tuzak kapanı

d. Açılır pencere

e. Truva atı

**9.** Kötü niyetli kişilerin kilit konumda olan önemli kişileri, değişik yöntemlerle kandırarak veya rüşvet vererek, onlar vasıtasıyla gizli bilgileri elde etmelerine ne denir?

a. Sekteye uğratma

b. Truva atı

c. Şifreleme

d. Zayıf nokta

e. Sosyal mühendislik

**10.** Aşağıdakilerden hangisi bilişim güvenliğinde kontrol mekanizmalarına bir örnek değildir?

a. Şifreleme

b. Fiziksel koruma

c. Virüs tarayıcılar

d. Kurallar

e. Bilgi güvenliği

## Kendimizi Sınayalım Yanıt Anahtarı

**1. e** Yanıtınız yanlış ise "Giriş" başlıklı konuyu yeniden gözden geçiriniz.

**2. b** Yanıtınız yanlış ise "Temel Kavramlar" başlıklı konuyu yeniden gözden geçiriniz.

**3. c** Yanıtınız yanlış ise "Temel Kavramlar" başlıklı konuyu yeniden gözden geçiriniz.

**4. d** Yanıtınız yanlış ise "Temel Kavramlar" başlıklı konuyu yeniden gözden geçiriniz.

**5. c** Yanıtınız yanlış ise "Tehdit Çeşitleri" başlıklı konuyu yeniden gözden geçiriniz.

**6. d** Yanıtınız yanlış ise "Tehdit Çeşitleri" başlıklı konuyu yeniden gözden geçiriniz.

**7. a** Yanıtınız yanlış ise "Tehdit Çeşitleri" başlıklı konuyu yeniden gözden geçiriniz.

**8. d** Yanıtınız yanlış ise "Saldırılar" başlıklı konuyu yeniden gözden geçiriniz.

**9. e** Yanıtınız yanlış ise "Saldırılar" başlıklı konuyu yeniden gözden geçiriniz.

**10. e** Yanıtınız yanlış ise "Bilişim Sistemi Kontrol Mekanizmaları" başlıklı konuyu yeniden gözden geçiriniz.

## Sıra Sizde Yanıt Anahtarı

### *Sıra Sizde 1*

Değişik örnekler verilebilir. Bir örnek verecek olursak şöyle verebiliriz. Adınıza gelen mektubu aile bireylerinden herhangi birinin açarak okuması gizlilik ihlalidir.

### *Sıra Sizde 2*

Kimlik doğrulama orijin bütünlüğü veya kaynak bütünlüğüdür. Veri bütünlüğü içerik bütünlüğüdür. Mesaj örneği üzerinde aralarındaki farkı şöyle açıklayabiliriz. Leyla Mecnun'a bir mektup göndermiş olsun. Mecnun'un bu mektubun Leyla'dan geldiğine %100 emin olmasına kimlik doğrulama, mektubun içeriğinin kötü niyetli kişilerce değiştirilememesi ise veri bütünlüğüdür.

### *Sıra Sizde 3*

Bu tür ataklara servis dışı bırakma atakları denir.

### *Sıra Sizde 4*

Değişik örnekler verilebilir. İnternet bankacılığı şifrelerinin elde edilmesi bir tehdittir. Bu tehdite karşı yapılabilecek kontrol mekanizmalarına şifrelerin şifrelenerek saklanması örnek gösterilebilir.

### *Sıra Sizde 5*

İki kişi arasında gönderilen mesajın içeriğinin yetkisi olmayan bir kişi tarafından görülmesi veya bu mesajlaşmanın dinlenmesi ele geçirmedir. Eğer mesaj elde edilip alıcının eline geçmesi engellenirse buna sekteye uğratma denir.

### *Sıra Sizde 6*

Değişik örnekler verilebilir. Donanım sınıfına girecek özel kimlik kartlarının veya akıllı kartların kopyalanması veya fabrikasyonla sahtelerinin yapılması saldırı örneği olarak verilebilir.

### *Sıra Sizde 7*

Truva atı görünüşte doğru çalışan fakat arkada kötücül işler yapan kötücül yazılımdır. Tuzak kapanı ise programlar içine gizlice yerleştirilmiş bir açık kapıdır.

## *Sıra Sizde 8*

İnternet denir.

## *Sıra Sizde 9*

1. En kolay nüfuz etme,
2. Yeterli süre koruma,
3. Tesirlilik ve
4. En zayıf halka ilkeleri.

## Yararlanılan Kaynaklar


Pfleeger, C. P. and Pfleeger, S. L. (2003). **Security in Computing**: USA, Prentice Hall.

Easttom, C. (2006). **Computer Security Fundamentals**: USA, Prentice Hall.

Pearson, R.L. (2007). **Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions**, Butterworth-Heinemann, Elsevier.