

**YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**AKILLI BİNALARDA GÜVENLİK SİSTEMLERİNİN
KONTROLÜ**

937-18

Elek.Müh. Tahsin Okan KOŞAR

**F.B.E.Elektrik Mühendisliği Anabilim Dalında
Hazırlanan**

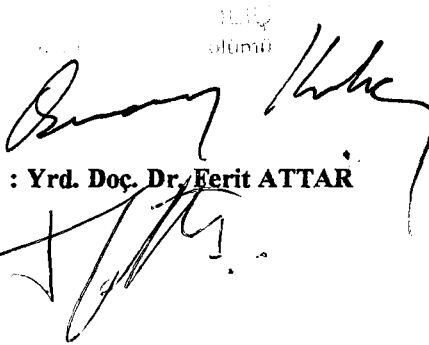
YÜKSEK LİSANS TEZİ

Yrd.Doc.Dr. Tuncay UZUN



Tez Danışmanı

Yrd. Doç. Dr. Ferit ATTAR



İSTANBUL, 2000

**T.C. YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ**

İÇİNDEKİLER

Sayfa

KISALTMA LİSTESİ	v
ŞEKİL LİSTESİ	vi
ÇİZELGE LİSTESİ	vii
ÖNSÖZ.....	viii
ÖZET	ix
ABSTRACT	x
1 GİRİŞ.....	1
1.1 Güvenlik Mühendisliği	1
1.1.1 Güvenlik mühendisliğinin amacı	1
1.1.2 Güvenlik mühendisliğinin temel kavramları	2
1.1.2.1 Risk değerlendirmesi	2
1.1.2.2 Fiziksel koruma	2
1.1.2.3 Algılama yöntemi	2
1.1.2.4 Alarm uygulaması.....	2
1.1.2.5 Alarm cevap uygulaması	2
1.1.2.6 Bakım-onarım ve sistemin periyodik gözden geçirilmesi	3
1.2 Risk Değerlendirmesi	3
1.2.1 Çizelge uygulaması.....	3
1.2.2 Risk değerlendirme çizelgeleri	4
1.2.2.1 Binanın yerleşim konumu ve çevresi (Çizelge 1.1).....	4
1.2.2.2 Binaya giriş kolaylığı ve yapısal kuvvet (Çizelge 1.2).....	5
1.2.2.3 Binadaki mal varlığı (Çizelge 1.3).....	6
1.2.2.4 Binaya yerleşim şekli (Çizelge 1.4).....	7
1.2.2.5 Kaybın doğuracağı sonuçlar (Çizelge 1.5)	7
1.2.2.6 Önceki kayıplar (Çizelge 1.6).....	9
1.2.2.7 Mevcut güvenlik önlemleri (Çizelge 1.7).....	9
1.2.2.8 Tavsiye edilen koruma seviyesi (Çizelge 1.8).....	9
1.2.2.9 Örnek hesaplama (Çizelge 1.9).....	10
2 GÜVENLİK SİSTEMLERİ.....	12
2.1 Alarm Sistemleri	12
2.1.1 Alarm sistemlerinin temel bileşenleri	13
2.1.2 Koruma yöntemleri	13
2.1.2.1 Çevre koruması	13
2.1.2.2 Alan koruması.....	14
2.1.2.3 Nesne koruması	15
2.2 Geçiş Kontrol Sistemleri.....	15
2.2.1 Kart okuyucular ve kartlar	15
2.2.1.1 Manyetik şerit	15

2.2.1.2	Baryum Ferit.....	16
2.2.1.3	Wiegand.....	16
2.2.1.4	Proximity	17
2.2.1.5	Biyometrik okuyucular	18
2.3	CCTV Sistemleri	19
2.3.1	CCTV sistemlerinin uygulama alanları	19
2.3.1.1	Güvenlik uygulamaları	19
2.3.1.2	Personel emniyeti uygulamaları	19
2.3.1.3	Yönetim uygulamaları	20
2.3.2	CCTV sistemlerine genel bakış	20
2.3.2.1	Aydınlatma	21
2.3.2.2	Kamera.....	21
2.3.2.3	Lensler	23
2.3.2.4	Video sinyallerini taşıma yöntemleri.....	24
2.3.2.5	Monitör	25
2.3.2.6	Zaman atlamalı video kayıt edici.....	26
2.3.2.7	Video seçici	26
2.3.2.8	Quad seçici.....	26
2.4	Sistemlerin Merkezi Entegrasyonu.....	26
2.4.1	XSM sistemi temel fonksiyonları ve özellikleri	27
2.4.1.1	Temel fonksiyonlar.....	27
2.4.1.2	Özellikler	27
2.4.1.3	İşletim sistemi.....	27
2.4.1.4	XSM server yazılım seçenekleri.....	27
2.4.1.5	XSM konfigürasyon yazılımı (Quickbuilder).....	28
2.4.1.6	XSM operatör yazılımı (Station)	28
2.4.1.7	XSM grafik yazılımı (Displaybuilder).....	28
2.4.2	XSM server.....	29
2.4.3	Yedek server	30
2.4.4	Operatör bilgisayarlar	30
2.4.5	Kontrolörler	30
2.4.6	Yazıcılar.....	31
2.4.7	XSM sisteminde geçiş kontrolü.....	31
2.4.7.1	Kart detayları	31
2.4.7.2	Geçiş noktaları	31
2.4.7.3	Geçiş bölgeleri.....	31
2.4.7.4	Zaman periyotları.....	31
2.4.7.5	Yetki seviyeleri.....	31
2.4.7.6	PGAP (Perimeter Global Anti-Passback).....	32
2.4.7.7	Arşivleme ve raporlama.....	32
3	UYGULAMA	33
3.1	Binaya Kurulacak Sistemlerin Sahip Olması Gereken Teknik Özellikler.....	33
3.1.1	Sistemlerin fonksiyon tanımları.....	33
3.1.1.1	Güvenlik yönetim sistemi ve kartlı geçiş sistemi	33
3.1.1.2	Alarm sistemi.....	34
3.1.1.3	CCTV sistemi	35
3.1.1.4	Güvenlik kontrol merkezi	36
3.1.1.5	Güvenlik resepsiyon bölgeleri	36
3.1.2	Cihazların tanımları ve teknik özellikleri	37
3.1.2.1	Güvenlik yönetim sistemi ve kartlı geçiş sistemi	37

3.1.2.2	Alarm sistemi.....	40
3.1.2.3	CCTV sistemi	40
3.1.2.4	Güvenlik kontrol merkezi.....	41
3.1.2.5	Güvenlik resepsiyon bölgeleri	42
3.1.2.6	Fiziksel güvenlik araçları	42
3.2	Gerekli Ekipman ve Yazılımlar	43
3.2.1	Güvenlik yönetim sistemi	43
3.2.2	Kartlı geçiş sistemi.....	44
3.2.3	Alarm sistemi.....	44
3.2.4	CCTV sistemi	44
3.3	Sistem Ekipmanlarının Yerleşim ve Bağlantı Diyagramları.....	45
3.4	Sistem Konfigürasyonu	50
3.4.1	Haberleşme kanalları	50
3.4.2	Kontrolörler	52
3.4.3	Operatör bilgisayarlar	53
3.4.4	Nokta tanımlamaları.....	54
3.4.4.1	Geçiş noktaları	54
3.4.4.2	Kapı durum noktaları	54
3.4.4.3	Kapı kontak noktaları.....	55
3.4.4.4	Alarm noktaları.....	56
3.4.4.5	Gizli alarm noktası.....	56
3.4.4.6	Monitör alarm noktası.....	58
3.5	Dinamik Ekranların Veritabanı Bağlantısı	59
3.6	Dinamik Ekranlar	60
3.6.1	Sistem ünitelerinin haberleşmelerinin ve alarmların izlenmesi.....	60
3.6.2	Kartlı geçiş sisteminin yönetilmesi ve geçişlerin izlenmesi.....	65
3.6.3	Kapı, turnike, buton ve kameraların izlenmesi ve kontrolü	71
3.6.4	Raporlamalar	77
4	SONUÇLAR.....	84
KAYNAKLAR.....		86
ÖZGEÇMİŞ.....		87

KISALTMA LİSTESİ

CCTV	Closed Circuit Television
LAN	Local Area Network
PAL	Phase Alternation by Line
PTZ	Pan Tilt Zoom
PGAP	Perimeter Global Anti-Passback
SE26	Sensor Engineering 26 bit Wiegand Format
SE34	Sensor Engineering 34 bit Wiegand Format
TCP/IP	Transmission Control Protocol/Internet Protocol
TVL	Television Line
WAN	Wide Area Network
XSM	Excel Security Manager



ŞEKİL LİSTESİ

Şekil 2.1 Temel XSM sistemi.....	29
Şekil 2.2 LAN kullanan tipik bir XSM sistemi.	29
Şekil 3.1 Güvenlik yönetim sistemi ile saha kontrol üniteleri arasındaki bağlantı diyagramı.	45
Şekil 3.2 Alarm sistemi ekipman yerleşimi.....	46
Şekil 3.3 CCTV sistemi ekipman yerleşimi.	48
Şekil 3.4 Kartlı geçiş sistemi kart okuyucu dağılımı.....	49
Şekil 3.5 Güvenlik yönetim sistemi server ve operatör bilgisayarları.....	50
Şekil 3.6 Haberleşme kanalının konfigürasyonu.	50
Şekil 3.7 Haberleşme kanalının port konfigürasyonu.	51
Şekil 3.8 Kontrolör konfigürasyonu.	52
Şekil 3.9 Operatör bilgisayar konfigürasyonu.....	53
Şekil 3.10 Geçiş noktası konfigürasyonu.	54
Şekil 3.11 Kapı durum noktası konfigürasyonu.	55
Şekil 3.12 Kapı kontak noktası konfigürasyonu.....	56
Şekil 3.13 Alarm noktası konfigürasyonu.	57
Şekil 3.14 Gizli alarm noktası konfigürasyonu.	57
Şekil 3.15 Monitör alarm noktası konfigürasyonu.....	58
Şekil 3.16 Bir kapı kontak noktasının veritabanı bağlantısı.....	59
Şekil 3.17 Kanalların haberleşme durumlarının izlendiği dinamik ekran.....	61
Şekil 3.18 Kontrolörlerin haberleşme durumlarını gösteren dinamik ekran..	62
Şekil 3.19 Operatör bilgisayarların server’a bağlantı durumlarını gösteren dinamik ekran. ...	63
Şekil 3.20 Sistemde meydana gelen alarmları gösteren dinamik ekran..	64
Şekil 3.21 Sistemde varolan yetki seviyelerine ulaşımı sağlayan dinamik ekran.	66
Şekil 3.22 “2.Kat Haftaiçi” yetki seviyesinin işlevinin tanımlandığı dinamik ekran.....	67
Şekil 3.23 Kart sahibi personelin kişisel bilgilerini gösteren dinamik ekran.	69
Şekil 3.24 Kartlara yetki seviyesi atanması için kullanılan dinamik ekran.....	70
Şekil 3.25 Kartlı geçiş olaylarını gösteren dinamik ekran.....	71
Şekil 3.26 Otopark kat ekipmanları izlemek ve kontrol etmek için kullanılan dinamik ekran.....	72
Şekil 3.27 Zemin kat ekipmanlarını izlemek ve kontrol etmek için kullanılan dinamik ekran.....	73
Şekil 3.28 1.kattaki ekipmanları izlemek ve kontrol etmek için kullanılan dinamik ekran.	74
Şekil 3.29 2.kattaki ekipmanları izlemek ve kontrol etmek için kullanılan dinamik ekran.	75
Şekil 3.30 5.kattaki ekipmanları izlemek ve kontrol etmek için kullanılan dinamik ekran.	76
Şekil 3.31 CCTV sistemini izlemek ve kontrol etmek için kullanılan dinamik ekran.	78
Şekil 3.32 Rapor istemek için kullanılan dinamik ekran.....	79
Şekil 3.33 Olay ve alarm raporu için yardımcı dinamik ekran.....	80
Şekil 3.34 Kapı ve turnike takip raporu için yardımcı dinamik ekran.	82
Şekil 3.35 Kart takip raporu için yardımcı dinamik ekran.	83

ÇİZELGE LİSTESİ

Çizelge 1.1 Binanın yerleşim konumu ve çevresi	5
Çizelge 1.2 Binaya giriş kolaylığı ve yapısal kuvvet	6
Çizelge 1.3 Binadaki mal varlığı	7
Çizelge 1.4 Binaya yerleşim şekli	8
Çizelge 1.5 Kaybın doğuracağı sonuçlar	8
Çizelge 1.6 Önceki kayıplar	9
Çizelge 1.7 Mevcut güvenlik önlemleri	10
Çizelge 1.8 Tavsiye edilen koruma seviyesi	10
Çizelge 1.9 Örnek hesaplama	11
Çizelge 3.1 Kartlı geçiş sistemi	34
Çizelge 3.2 Alarm sistemi	34
Çizelge 3.3 CCTV sistemi	35
Çizelge 3.4 Güvenlik yönetim sistemi.....	37



ÖNSÖZ

Yüksek lisans tezi olarak hazırladığım bu çalışmada güvenlik sistemlerinin kontrolü üç bölümde incelenmiştir. İlk bölümde güvenlik mühendisliğinin temel kavramlarına değinilmiş ve ikinci bölümde de güvenlik sistemleri incelenmiştir. Üçüncü bölümde ise, bir binanın güvenlik uygulamasına yer verilmiştir.

Tezimin hazırlanmasında benden bilgi ve yardımlarını esirgemeyen değerli hocam Y.Doç.Dr.Ferit ATTAR'a teşekkürlerimi sunarım.



ÖZET

Günümüzde; artan hırsızlık ve saldırı olaylarına karşı güvenlik sistemleri teknolojisinin gelişimi devam etmektedir. Kalabalık personel ve ziyaretçi sayısına sahip binalarda, güvenliğin üst düzeyde sağlanabilmesi için üç farklı güvenlik sisteminin bir arada kullanılmasına ihtiyaç duyulmaktadır: Alarm sistemi, geçiş kontrol sistemi, CCTV (Closed Circuit Television) sistemi. Bu sistemlerin birbirleriyle uyumlu çalışabilmeleri için, tek bir merkezden izlenmeleri ve kontrol edilmeleri gerekmektedir. Güvenlik firmaları, çalışmalarını bu yöne doğrultmuşlar ve sistemleri entegre edecek merkezi yazılımlar geliştirmişlerdir.

Çalışmanın giriş bölümünde, güvenlik mühendisliğinin temel kavramları irdelenmiş ve risk değerlendirmesi için kullanılan çizelge uygulamasına yer verilmiştir. İkinci bölümde, güvenlik sistemleri hakkında temel bilgiler yer almaktadır. Bu sistemlerin bir merkezden kontrolünü sağlayan ve Honeywell tarafından geliştirilen XSM (Excel Security Manager) yazılımının fonksiyonları açıklanmıştır. Uygulama bölümünde, yedi katlı bir binanın güvenlik ihtiyaçları belirtilmiş ve bu ihtiyaçları karşılayacak sistemler için gerekli ekipman ve yazılımlar seçilmiştir. Son aşamada; sistemler, XSM yazılımı ile tek bir merkezden yönetilecek şekilde konfigüre edilip, operatörlerin kullanacağı dinamik ekranlar oluşturulmuştur.

Merkezi yazılım kullanılarak gerçekleştirilen güvenlik uygulamaları, sistemlerin birbirlerine uyumlu çalışmasını sağlamak ve dinamik ekranlar aracılığıyla operatörlere kolay kullanım imkanı vermektedir.

ABSTRACT

Nowadays, the security systems technology continues to develop against increasing burglary and attacks. For high-level security in the buildings which have crowded personnel and visitors, it is mostly required to use three different security systems together: Alarm system, access control system, CCTV (Closed Circuit Television) system. These systems must be monitored and controlled from one center in order to operate efficiently and harmoniously with each other. Security companies use advanced supervisory control and data acquisition software to integrate their security systems.

In the introduction part of this study, it is explained that security engineering and the charts, which are used for risk assessment. In the second part, it is overviewed that the fundamentals of the security systems and the functions of XSM software, which is central software being developed by Honeywell Company. In the last part, a sample application is explained for a seven-story building security requirements and it is chosen equipment and software tools to meet necessary security requirements. Systems are configured by means of XSM software and dynamic displays which will be used by operators are made.

Using central software provides harmonious operation of the implemented systems and easy-to-use for operators.



1 GİRİŞ

Modern güvenlik çağı; 110 yıl önceye, elektrikle çalışan alarmların ortaya çıkışına dayanmaktadır. İlk zamanlar kullanılan basit hırsız alarmlarının uygulama alanı, finansal kurumlar ve mücevher dükkanlarının korunmasıyla sınırlı kalmıştır.

Bu sistemlerin büyümesi, her ne kadar sürekli olduysa da ağır ağır ve kademeli olarak gerçekleşmiştir. Sistemlerin etkinlikleri 1. Dünya savaşı günlerine kadar çok az gelişmiştir. Milli savunma ihtiyaçları, sistemlerin çok hızlı bir şekilde gelişmesine öncülük etmiştir.

2. Dünya savaşına doğru güvenlik sistem endüstrisi en hızlı büyüme dönemini geçirmiştir. Savaş sırasında; eğitilmiş düşman ajan ve sabotajcılarının tehditleri, ileri teknoloji ürünü sistemlerin icat edilmesine neden olmuştur.

Bu sistemler; 2. Dünya savaşından günümüze kadar, davetsiz misafirlerin becerilerinin gelişmesine karşılık olarak sürekli yenilenmiş ve mükemmelleşmiştir.

Günümüzde, iş dünyası ve halk; işyerlerini ve evlerini tehdit eden hırsızlık, vandalizm, endüstriyel casusluk, sabotaj gibi olaylardaki hızlı bir artışla karşı karşıya kalmıştır. Bu nedenle insanlar, uygun bir maliyetle gerekli korunma ihtiyaçlarını sağlamaya çalışmaktadırlar.

Kayıplar artarken, işadamları bu kayıpları kontrol etmek için bir şeyler yapmaları gerektiğinin hızla farkına varmaktadırlar. Çoğu modern işadamı etkin bir güvenlik yönetimi ile kayıpları önlemenin iş karına katkısının, diğer herhangi bir aktiviteden daha fazla olacağını düşünmektedir.

Güvenlik alanındaki birçok uzman; bir sistem ile korunmakta olan yerlerde kayıp önleme programlarının daha etkin bir şekilde çalışacağını ifade etmektedirler.

1.1 Güvenlik Mühendisliği

1.1.1 Güvenlik mühendisliğinin amacı

Bir bina projesinin her aşamasında suç işlenmesine karşı alınacak tüm önlemler değerlendirilmelidir. İleriyi görerek zamanında alınmış bir önlem, daha sonra oluşabilecek bir çok problemi ortadan kaldıracaktır.

Yapılacak tasarım; binanın yapımı ve kullanımı süresince hırsızlık, vandalizm, saldırı ve

sabotaj olasılıklarını bina içinde ve çevresinde en aza indirmeyi hedef almalıdır.

Bu hedefe ulaşırken fiziksel koruma yöntemleri kullanılabilir, fakat unutulmaması gereken bir nokta vardır: “Bina içindeki personele gerekli eğitimler verilmeli ve güvenlik prosedürüne uymaları sağlanmalıdır.”

1.1.2 Güvenlik mühendisliğinin temel kavramları

1.1.2.1 Risk değerlendirmesi

Yangın, su baskını, vandalizm, hırsızlık ve hatta terörizm ile meydana gelebilecek hasarlara yol açacak tüm riskler gözönüne alınmalıdır.

1.1.2.2 Fiziksel koruma

Fiziksel koruma; izinsiz giriş çıkışları engelleyecek veya geciktirecek şekilde, korunacak alan çit ile çevrilerek ve/veya bina unsurları (örneğin; duvarlar, bölme duvarları, kapılar, pencereler, bariyerler, sürgüler, kilitler, kasalar vb.) kullanılarak sağlanan koruma biçimidir.

1.1.2.3 Algılama yöntemi

Algılama yöntemi, değerlendirilen riskleri ve sağlanacak fiziksel koruma şeklini destekleyecek şekilde seçilmelidir. Fiziksel korumayı geçerek korunan alana sızmak için gerekli olan süre ve suçun başarıyla tamamlanmasını önlemek için gerekli olan cevap hızı dikkate alınmalıdır. Bir algılama sisteminin mutlaka caydırıcı olması gerekmektedir.

1.1.2.4 Alarm uygulaması

Alarm cihazlarının ve uygulama şekillerinin (elle, otomatik, sesli, görsel vb.) ortam koşullarına göre belirlenmesi gerekmektedir. Alarm, suç işleyen kişiyi rahatsız edecek düzeyde olmalı ve izinsiz eylemin başlamış yada başlamakta olduğunu güvenlikten sorumlu personele bildirmelidir.

1.1.2.5 Alarm cevap uygulaması

Bir alarm verilecek cevap, alarm algılandığında güvenlikten sorumlu personel tarafından yapılacak işlemleri kapsamaktadır. Eğer suç işleyen kişinin yakalanması önemliyse, alarm suçlu tarafından hissedilmemeli ve mümkün olduğunca çabuk, organize bir cevap uygulanmalıdır.

1.1.2.6 Bakım-onarım ve sistemin periyodik gözden geçirilmesi

Sık sık yapılacak testler ve yeterli bakım-onarım, sistemin başarısızlık olasılığını en aza indireyecektir. Binanın yapısındaki, kullanımındaki veya personelindeki değişiklikler incelenip güvenlik sistemlerinin yeterliliği periyodik olarak gözden geçirilmelidir.

1.2 Risk Değerlendirmesi

Bir güvenlik sistemi tasarlarırken en zor işlerden biri tehditlerin büyüklüğünü, önlemlerin kapsamını ve şartlara uygun finansal yatırımı tespit etmektir. Risklerini azaltmak isteyen sigorta şirketleri, pazar fırsatları arayan üretici firmalar ve işgücü firmaları, kurulum-bakım ve onarımdan sorumlu müteahhit firmalar doğal olarak koruma ve algılama sisteminin faydalarını ön plana çıkaracaklardır.

Eğer güvenlik önlemlerine finansal kaynaklar ayrılmışsa, tehdit unsurlarının rasyonel ve analitik olarak incelenmesi gerekmektedir. Güvenlik mühendisini ilgilendiren temel tehdit hırsızlıktır. Hırsızlık sık sık ve farklı yollarla işlenen bir suçtur, bundan dolayı tavsiyeler ve talimatlar basit bir değerlendirme yöntemi olarak kısıtlı kalacaktır.

Güvenlik önlemlerini değerlendirmekle sorumlu kişi;

- Binanın kullanım tarzını araştırmak için bina sahibiyle görüşmeler yaparak çalışmalıdır.
- Binayı ve binanın çevresini, komşu arazi ve binaları dikkate alarak incelemelidir.
- Bu detaylarla beraber Çizelge 1.1 ile Çizelge 1.7 arasındaki tüm çizelgelerde listelenmiş olan unsurların değerlendirmesini yapmalıdır.

Çizelge 1.8 ile riski azaltmak için gerekli olan güvenlik önlemlerinin ve hırsızlık riskinin seviyesini belirleyen genel bir değerlendirme yapılabilmektedir. Bu çizelgeler kullanılarak yapılan örnek değerlendirme, bu bölümün sonunda görülmektedir.

Hırsızlığın karşısında alınacak önlemler belirlenirken, hırsızlık olasılığının meydana gelecek zararın sonuçlarıyla birlikte değerlendirilmesi gerekmektedir. Zararın sonuçları sadece zararın mali değeri ile ilgili değildir. Birçok başka faktör vardır ve bunların önem dereceleri bina sahibiyle yapılacak detaylı görüşmeler sonucunda tam anlamıyla ortaya çıkacaktır.

1.2.1 Çizelge uygulaması

Hırsızlık riskini etkileyen temel kategoriler çizelgelerde formülüze edilmiştir. Her kategoride risk seviyesine göre sayısal derecelendirme yapılmıştır. Negatif sayılar, güvenlik önlemlerine yardımcı olan faktörleri göstermektedir.

Tüm unsurlar hesaba katıldıktan sonra, elde edilen toplam sonuç gereken koruma seviyesini gösterecek olan sonuç çizelgesinde değerlendirilir. Toplam sonucun değeri arttıkça hırsızlık riskinin seviyesi de artacaktır.

Bu çizelgeler, tanımlanmış yüksek riske sahip binalarda (örneğin; bankalar, askeri kuruluşlar gibi) veya adam kaçırmaya, terörizm ve gasp riski olan mekanlarda uygulanamaz.

Çizelgelerde listelenmemiş bölgesel koşullar ve diğer faktörler, listelenmiş faktörlerden daha büyük öneme sahiptir. Bina sahibinin binayı kullanımı ve binanın konfigürasyonu dikkate alınacağı için çizelgeler yalnızca riski ilgilendiren en yaygın unsurları açığa çıkaracaktır.

İlgili tüm unsurların değerlendirmeye katılması, riski değerlendiren kişinin sorumluluğundadır ve bu da yeni faktörler için yeni çizelgeler üretilmesini gerektirebilir. Bu faktörlerin belirlenmesi ve uygulanmasında sigorta müfettişlerinin, müşterinin sigorta şirketinin ve bölgesel polis teşkilatının tavsiyelerinin dikkate alınması gerekir.

Güvenlik önlemlerine sahip bir bina için yapılan hesaplamalar çok yüksek bir risk seviyesi ortaya çıkarıyorsa, koruma ve caydırma unsurlarının nasıl geliştirileceğini saptayacak tecrübeli bir güvenlik sorumlusu görevlendirilmelidir.

1.2.2 Risk değerlendirme çizelgeleri

1.2.2.1 Binanın yerleşim konumu ve çevresi (Çizelge 1.1)

Binanın genel konumu : Suçun işlenme oranı istatistiksel olarak kasaba veya şehrin büyüklüğüne bağlıdır. Suçlular daha küçük topluluklarda yabancı olarak tanınacaklarını hissederler ve daha az ihtimalle şüpheli hareketlere başvururlar.

Binaya komşu alanların karakteri : En çok suç işlenme oranı, harabe alanlarda ve şehir içi alanlarda görülmektedir.

Risk periyotları süresince komşu alanların yerleşim durumu : Bu faktör; binada yerleşim olmadığı yüksek riskli saatlerde komşu alanlardaki yerleşim durumunu dikkate alır.

Yoldan geçenlere sunulan görünüm : Suçlular, suç işlerken saklanmayı tercih ederler. Bu faktör binanın önündeki yoldan geçenlerin sıklığını hesaba katar.

Aydınlatma seviyesi : Suçlular, suç işlemek için karanlık alanları tercih eder. Gece aydınlatması sağlanmasının suçlardaki azalma oranına doğrudan etkisi kanıtlanmıştır. Bu faktörle; binanın ve komşu alanların aydınlatma durumları incelenir.

Çizelge 1.1 Binanın yerleşim konumu ve çevresi

Riski Etkileyen Koşullar	Faktör
<i>Binanın genel konumu</i>	
Uzak ücra yerler	0,75
Köy	1,0
Kırsal topluluk	1,5
Küçük kasaba	2,0
Büyük kasaba veya şehrin kenarı	5,0
Şehrin içi	6,0
<i>Binaya komşu alanların karakteri</i>	
İyi donanımlı	0,5
Vasat	1,0
Harap, yıkık	2,0
<i>Risk periyotları süresince komşu alanların yerleşim durumu</i>	
Tam yerleşim	-0,5
Kısmen yerleşim	1,0
Yerleşim yok	2,0
<i>Yoldan geçenlere sunulan görünüm</i>	
Tüm katlar tam görünüme açık	-1,0
Kolay zarar görecekt katlar tam görünüme açık	-0,5
Kolay zarar görecekt katların bir veya daha fazlası görünüme kapalı	1,0
Uzak görünüm veya az sayıda yoldan geçen kişinin olması	1,5
Bina görünüme kapalı	2,0
<i>Aydınlatma seviyesi</i>	
Bina ve komşu alanlar iyi aydınlatılmış	-1,0
Bina iyi aydınlatılmış, fakat komşu alanların aydınlatması zayıf	0,5
Binanın ve komşu alanların aydınlatması zayıf	1,5

1.2.2.2 Binaya giriş kolaylığı ve yapısal kuvvet (Çizelge 1.2)

Giriş ve hareket kolaylığı : Binadaki eşyaların dışarıya çıkartılmasının kolaylığı ve binaya dışardan girişin rahatlığıyla ilgilidir. Bu çizelge, yaya veya araç girişine uygulanabilir. Çizelge, binaya ait eşyaların dışarıya çıkartılmasındaki kolaylığı inceler.

Binanın yapısı : Binanın yapısal kuvveti saldırılara karşı binanın hassasiyetini etkiler.

Kapı ve pencere çerçevelerinin tipi : Kapı ve pencere çerçevelerinin fiziksel kuvveti binaya zorla girişi etkiler.

Kapı ve pencere güvenlik tesisatlarının kalitesi : Kapı ve pencere güvenlik tesisatlarının kalitesi, binaya zorla girişi doğrudan etkileyen bir faktördür.

Çizelge 1.2 Binaya giriş kolaylığı ve yapısal kuvvet

Riski Etkileyen Koşullar	Faktör
<i>Giriş ve hareket kolaylığı</i>	
Zor	-1,0
Orta derecede zorluk	0
Kolay	2,0
<i>Binanın yapısı</i>	
Taş, tuğla veya beton	0,5
Ahşap	1,0
Geçici, prefabrik, hareketli	1,5
Hiçbiri (örneğin; açık avlu)	2,0
<i>Kapı ve pencere çerçevelerinin tipi</i>	
Kuvvetli metal	0,5
Sert tahta	1,0
Tahta veya alüminyum	1,5
Plastik	2,0
<i>Kapı ve pencere güvenlik tesisatlarının kalitesi</i>	
Kuvvetli, yüksek kalite	-1,0
Vasat, orta kalite	0
Vasat, düşük kalite	1,5
Zayıf, düşük kalite	2,0

1.2.2.3 Binadaki mal varlığı (Çizelge 1.3)

Binadaki mülkün değeri : Binanın içindeki mülkün değeri riskin seviyesini doğrudan etkileyen bir faktördür. Binada depolanan malların bir bütün olarak (monte edilmiş) saklandığı yerler, parça parça saklandığı yerlerden daha büyük bir risk altındadır.

Binadaki mülkün elden çıkarılabilirlik durumu : Bir hırsız, çaldığı malları çabuk bir şekilde paraya dönüştürmek isteyecektir. Eşyanın elden çıkarılabilmesi, o eşya için hazır bir pazar olup olmadığına bağlıdır. Örneğin; alkol, sigaralar veya elektrikli eşyalar kolaylıkla satılabilir ve bunları takip etmek çok zordur. Böyle eşyalar hırsız için daha büyük bir çekiciliğe sahiptir ve daha büyük bir risk altındadır.

Binadaki mülkün taşınabilirlik durumu : Binadaki eşyaların büyüklüğü, ağırlığı ve konumu onları potansiyel hırsızlar için çekici yapabilir. Eşyayı kaldırmak için ekipmana ihtiyaç veya yardımcı ekiplere, ticari araçlara ihtiyaç hırsızlık riskini azaltıcı unsurlardır. Kolay taşınabilir yüksek değere sahip eşyalar daha büyük bir risk altındadır.

Çizelge 1.3 Binadaki mal varlığı

Riski Etkileyen Koşullar	Faktör
<i>Binadaki mülkün değeri</i>	
Düşük varsayılan değer	0,5
Düşük değer (örneğin; ucuz hammadde, önemsiz para vb.)	1,0
Kolay satılan değer (örneğin; para, alkol, elektrikli eşya)	1,5
Yüksek değer (örneğin; uyuşturucu)	2,0
<i>Binadaki mülkün elden çıkarılabilirlik durumu</i>	
Çok sınırlı Pazar	0,1
Sınırlı Pazar	0,5
Satılabilir	1,0
Kolayca ve çabuk bir şekilde satılabilir	2,0
Para (korunacak ilk madde)	3,0
<i>Binadaki mülkün taşınabilirlik durumu</i>	
Taşınması güç, mekanik kaldırma ekipmanı gerekli	-1,0
Yardımcı insan grubu ve ağır taşıma aracı gerekli	-0,5
Yüklemek için uzun zaman ve orta boy taşıma aracı gerekli	0
Taşınması kolay, fakat hafif taşıma aracı gerekli	1,0
Bir kişi tarafından taşınabilir	2,0

1.2.2.4 Binaya yerleşim şekli (Çizelge 1.4)

Yerleşim saatleri : Hırsızlar genellikle binalar boşken ortaya çıkarlar. Ev konutları için gündüz vakti, endüstriyel ve ticari alanlar için gece vakti riskli zamanlardır. Binada sürekli yerleşim olduğu zaman dilimindeki hırsızlık riski, bina boşaltılıp uzun periyotlarla yalnız bırakıldığı zaman diliminden çok daha azdır. Eğer hırsız, binanın boş olduğu zaman dilimlerini belirleyebiliyorsa risk artacaktır ve hırsız buna göre plan yapabilecektir.

Ziyaretçilerin denetlenmesi ve ziyaretçi sayısı : Ziyaretçilerin dürüst olduğu hiç bir zaman garanti edilemez. Bu çizelge ziyaretçilerin miktarına ve denetleme düzeyine göre riski değerlendirir. Ziyaretçi dolaşımının yüksek düzeyde olduğu yerlerde (örneğin; hastanelerde) kontrol hemen hemen imkansız hale gelir ve risk büyür.

1.2.2.5 Kaybın doğuracağı sonuçlar (Çizelge 1.5)

Hassasiyet : Zararın politik sonuçları da gözönüne alınmalıdır. Örneğin; bir güvenlik şirketinin kendi binası soyulursa, bu şirket komik duruma düşecek ve büyük ölçüde prestij kaybedecektir. Böyle durumlarda bina mülkünün mali değerine bakılmaksızın koruma hayati önem taşıyacaktır.

Kaybın vereceği rahatsızlık : Bu faktör, bina sahibinin binadaki mülke verdiği önemi dikkate alır. Örneğin; çok düşük mali değere sahip bir mülk, organizasyonun işlemesi için çok önemli olabilir ve bu kayıp gelir kaybıyla sonuçlanabilir.

Çizelge 1.4 Binaya yerleşim şekli

Riski Etkileyen Koşullar	Faktör
<i>Yerleşim saatleri</i>	
Sürekli yerleşim	-1,5
Kısa periyotlarda yerleşim yok	-0,5
Düzenli değil, çok uzun periyotlarda yerleşim yok	1,5
Düzenli, belirlenmiş periyotlarda yerleşim yok	1,75
Uzun, belirlenmiş periyotlarda yerleşim yok	2,0
<i>Ziyaretçilerin denetlenmesi ve ziyaretçi sayısı</i>	
Denetleme var, geçiş kontrol sistemi kurulu	-1,0
Az sayıda ziyaretçi, denetleme yok	0
Önemli sayıda ziyaretçi, denetleme yok	1,0
Çok fazla sayıda ziyaretçi, denetleme yok	1,5

Çizelge 1.5 Kaybın doğuracağı sonuçlar

Riski Etkileyen Koşullar	Faktör
<i>Hassasiyet</i>	
Düşük	0,5
Orta	1,0
Yüksek	2,0
Kabul edilemez	4,0
<i>Kaybın vereceği rahatsızlık</i>	
Düşük	0,5
Orta	1,0
Yüksek	2,0
Kritik	4,0

1.2.2.6 Önceki kayıplar (Çizelge 1.6)

Bina için önceki kayıpların düzeyi : Sigorta primlerinde, binada daha önce meydana gelmiş olaylar hesaba katılır. Kayıpla sonuçlanmış olaylar, geliştirici tedbirler alınmadıysa yeni kayıpların olabileceğini gösterir.

Çizelge 1.6 Önceki kayıplar

Riski Etkileyen Koşullar	Faktör
<i>Bina için önceki kayıpların düzeyi</i>	
Düşük	0,5
Orta	1,0
Yüksek	2,0
<i>Bina sahibi için önceki kayıpların düzeyi</i>	
Düşük	0,5
Orta	1,0
Yüksek	2,0

Bina sahibi için önceki kayıpların düzeyi : Bazı şirketler kayıp konusunda daha hassas olabilirler.

1.2.2.7 Mevcut güvenlik önlemleri (Çizelge 1.7)

Hırsız alarm sisteminin düzeyi : Hırsız alarm sisteminin varlığı işlenecek suçları önlemeyecektir, fakat caydırıcı bir güç olarak minimum düzeye indirecektir. Sistem ne kadar kapsamlı olursa, hırsızlığı algılama ve önleme olasılığı artacaktır.

Güvenlik görevlilerinin düzeyi : Güvenlik görevlilerinin sayısı ve düzenli çalışmaları uygunsuz aktiviteler için caydırıcı olacaktır. Güvenlik görevlilerinin çalışma saatleri çizelgede listelenmiş faktörleri etkilemektedir. Görevlilerin konuşlandırılması, eğitimi ve motivasyonu dikkate alınmalıdır.

Kapalı devre televizyon sisteminin düzeyi ve gözlem durumu : Kapalı devre televizyon sistemi suçu engellemeyecek, fakat caydırıcı bir güç olacaktır. Video kayıt edici kullanımı suçlunun tanınması ve yakalanması için verimli bir yöntemdir.

1.2.2.8 Tavsiye edilen koruma seviyesi (Çizelge 1.8)

Çok fazla sayıda faktörün olması nedeniyle güvenliğin risk değerlendirmesi oldukça güçtür. Bu yüzden Çizelge 1.8'deki tavsiyeler yalnızca yol göstericidir.

Çizelge 1.7 Mevcut güvenlik önlemleri

Riski Etkileyen Koşullar	Faktör
<i>Hırsız alarm sisteminin düzeyi</i>	
Kapsamlı ve yaygın, geçiş sistemi dahil	-2,0
Kapsamlı ve yaygın	-1,0
Basit	0
Yok	2,0
<i>Güvenlik görevlilerinin düzeyi</i>	
24 saat görevli var	-2,0
Gündüz görevli var, part-time gece devriyesi	-1,5
Tüm girişlerde gündüz görevli var	-0,5
Girişlerde sınırlı sayıda görevli var	0,5
Yok	2,0
<i>Kapalı devre televizyon sisteminin düzeyi ve gözlem durumu</i>	
Tüm katlar ve girişler, full-time gözlemci	-1,5
Tüm katlar ve girişler, part-time gözlemci	-1,0
Stratejik katlar ve girişler, full-time gözlemci	-0,5
Stratejik katlar ve girişler, part-time gözlemci	0,5
Yok	2,0

Çizelge 1.8 Tavsiye edilen koruma seviyesi

Toplam Faktör	Risk Seviyesi	Tavsiye Edilen Koruma
14'ten az	Çok düşük	Özel önleme gerek yok
14 – 19	Düşük	Fiziksel önlemler
19 – 23	Orta	Fiziksel ve sınırlı elektronik önlemler
23 – 27	Yüksek	Fiziksel ve orta derece elektronik önlemler
27 üstü	Çok yüksek	Fiziksel ve kapsamlı elektronik önlemler

1.2.2.9 Örnek hesaplama (Çizelge 1.9)

Büyük bir şehirde bir ofisin; metal pencere ve kapı çerçeveleri ile kuvvetli güvenlik tesisatı, 24 saat çalışan güvenlik görevlileri ve kartlı geçiş kontrol sistemi var.

Tüm girişleri kapalı devre televizyon sistemiyle gözetim altında ve hırsız alarm sistemi sürekli izleniyor. Binanın aydınlatma seviyesi iyi durumda, fakat komşu alanların aydınlatması yetersiz.

Binanın temel eşyaları hayati bilgiler içeren bilgisayarlar ve kaybın vereceği rahatsızlık kritik düzeyde.

Çizelge 1.9 Örnek hesaplama

Riski Etkileyen Koşullar	Faktör
Binanın genel konumu-Şehrin içi	6,0
Binaya komşu alanların karakteri-İyi donanımlı	0,5
Risk periyotlarında komşu alanların yerleşim durumu-Yerleşim yok	2,0
Yoldan geçenlere sunulan görünüm-Kolay zarar görecektir katların bir veya daha fazlası görünümüne kapalı	1,0
Aydınlatma seviyesi-Bina iyi aydınlatılmış, fakat komşu alanların aydınlatması zayıf	0,5
Giriş ve hareket kolaylığı-Orta derecede zorluk	0
Binanın yapısı-Taş, tuğla veya beton	0,5
Kapı ve pencere çerçevelerinin tipi-Kuvvetli metal	0,5
Kapı ve pencere güvenlik tesisatlarının kalitesi-Kuvvetli, yüksek kalite	-1,0
Binadaki mülkün değeri-Düşük değer	1,0
Binadaki mülkün elden çıkarılabilirlik durumu-Sınırlı Pazar	0,5
Binadaki mülkün taşınabilirlik durumu-Taşınması kolay, fakat hafif taşıma aracı gerekli	1,0
Yerleşim saatleri-Sürekli yerleşim	-1,5
Ziyaretçilerin denetlenmesi ve ziyaretçi sayısı-Denetleme var, geçiş kontrol sistemi kurulu	-1,0
Hassasiyet-Orta	1,0
Kaybın vereceği rahatsızlık-Kritik	4,0
Bina için önceki kayıpların düzeyi-Düşük	0,5
Bina sahibi için önceki kayıpların düzeyi-Düşük	0,5
Hırsız alarm sisteminin düzeyi-Kapsamlı ve yaygın, geçiş sistemi dahil	-2,0
Güvenlik görevlilerinin düzeyi-24 saat görevli var	-2,0
Kapalı devre televizyon sisteminin düzeyi ve gözlem durumu-Tüm katlar ve girişler, full-time gözlemci	-1,5
TOPLAM FAKTÖR	10,5

Tavsiyeler : Mevcut güvenlik önlemleri riski düşük seviyeye indirmiştir. Başka önleme gerek yoktur.

2 GÜVENLİK SİSTEMLERİ

Güvenlik sistemleri üç bölümde değerlendirilmektedir:

- Alarm sistemleri
- Geçiş kontrol sistemleri
- CCTV sistemleri

2.1 Alarm Sistemleri

Alarm sistemleri, aktif olduğunda alarm veren basit bir telli sistemden günümüzün yüksek teknoloji ürünü bilgisayar tabanlı sistemlerine büyük bir gelişim geçirmiştir.

Alarm sistemleri günümüzde, ileri teknoloji ürünü sensörleri ve bu sensörleri gözlemleyen alarm panelleri gibi ekipmanlara sahiptir. Alarm paneli; kendisine bağlı cihazları gözlemlediği gibi, bir müdahale yapılma olasılığına dayanarak kendisini de izlemektedir.

4 tip alarm sistemi mevcuttur:

- Yerel alarm sistemleri
- Merkezi izleme istasyonlu sistemler
- Mal sahibine ait sistemler
- Doğrudan bağlantı kuran sistemler

Yerel alarm sistemleri, korunan alanın çevresinde sesli bir alarm vermektedir. (Zil, korna, siren, vb.) Bu tip sistemler genel olarak, küçük dükkanlar gibi düşük risk altındaki yerleri korumak için kurulmaktadır. Yerel alarm sistemleri, uzak bir yerde bulunan bir izleme istasyonuna alarm işaretini ulaştırmanın mümkün yada ekonomik olmadığı durumlarda da tercih edilmektedir.

Merkezi izleme sisteminde; korunan alanda meydana gelen alarm işareti, bir güvenlik şirketi tarafından işletilen merkezi izleme istasyonuna ulaştırılmaktadır. Merkezi izleme istasyonundaki tüm ekipmanlar genellikle güvenlik şirketine ait olmakta ve korunan alanın sahibine kiralanmaktadır. Bu tür sistemler, çoğunlukla yoğun nüfuslu şehir merkezlerinde kurulmaktadır. Yüzlerce küçük işyeri sahibi, kendi koruma ekibini çalıştıracak ekonomik güce sahip olmadığından ve yerel alarm sisteminden daha güvenilir bir korunma istediğinden merkezi izleme sistemlerini tercih etmektedir. Bu sistem tarafından korunan yerler merkezi istasyona, kiralanmış telefon hatlarıyla bağlanmaktadır. Merkez, saldırılara karşı korunmakta ve içersinde 24 saat eğitimli personel bulunmaktadır. Bir alarm algılandığında, güvenlik görevlisi derhal polis merkezine haber ulaştırmaktadır.

Mal sahibine ait sistemlerde; korunan alanda meydana gelen alarm işareti, korunan alanın sahibine ait olan bir merkezi izleme istasyonuna ulaştırılmaktadır. Bu sistemler genel olarak; askeri üsler, büyük finansal kurumlar, büyük ofis binaları, hastaneler, üniversite kampüsleri gibi çok büyük işyerlerinde kurulmaktadır. Böyle sistemler çok büyük ve karmaşık oldukları için ihtiyaçları karşılayacak şekilde dizayn yapılması gerekmektedir.

Doğrudan bağlantı kuran sistemlerde, alarm işareti doğrudan polis merkezine ulaştırılmaktadır. Böyle sistemler genellikle, polis memurlarının alarmları izleyip, cevap verebilecekleri orta büyüklükteki şehirlerde kurulmaktadır.

2.1.1 Alarm sistemlerinin temel bileşenleri

Alarm sistemleri üç ana bileşene sahiptir: Alarm paneli, alarm algılama cihazları, alarm sinyal cihazları.

Alarm paneli; alarm algılama cihazlarından aldığı işaretleri, sesli alarm sinyal cihazlarına veya sürekli gözlenen bir uzak izleme istasyonuna iletmektedir.

Alarm algılama cihazları; elektromekanik algılayıcılar, fotoelektrik algılayıcılar, ses algılayıcılar, titreşim algılayıcılar, kapasitans algılayıcılar, pasif kızılötesi, ultrasonik ve mikrodalga detektörleri içeren hareket algılayıcılardır.

Alarm sinyal cihazları, korunan bölgenin çevresinde veya uzak bir izleme istasyonunda monte edilebilmektedir. Yerel sistemlerde kullanılan cihazlar genellikle, korunan alanların dış çevresine monte edilen büyük kornalardır. Uzak alarm sinyal cihazları, alarm alıcıları ve alarm kayıt edicileridir.

2.1.2 Koruma yöntemleri

Koruma yöntemleri 3 bölümde değerlendirilmektedir:

- Çevre koruması
- Alan koruması
- Nesne koruması

2.1.2.1 Çevre koruması

Dış çevre korumasını sağlayan etkin ve pratik yöntem, gergin tel algılama sistemidir. Bu tip sistemler, uzunluğu fazla alanların çevresini düşük bir maliyetle koruyabilmektedir. Bu sistem; bir çok endüstriyel komplekste, askeri tesislerde etkinliğini kanıtlamıştır.

Tipik bir gergin tel sisteminde, hemen hemen görünmez fakat çok kuvvetli bir tel, çit veya duvarın üstü boyunca çekilmektedir. Teldeki gerilme öyledir ki, sadece davetsiz bir misafirin teması sonucunda değil, dikkatli bir tırmanıcının sebep olduğu çitin hareketi sonucunda da alarm meydana getirmektedir.

Diğer dış çevre koruma sistemleri, elektronik çit sistemleri ve radyo frekans sistemleridir. Bazı üreticiler elektronik çit sistemleri üretmişler de, dış çevre koruma uygulamalarında çok büyük karışıklıklara neden olduğu için ürünlerini pazardan çekmişlerdir. Radyo frekans cihazları, günümüzde gelişim içindedir ama henüz ticari açıdan hazır değildir.

İç çevre korumasının uygulaması, çoğu aşılamayan iklim problemleri ortadan kalktığı için daha kolay olmaktadır. Kapıların ve pencerelerin korunması için yaygın olarak kontak cihazları kullanılmaktadır. Fotoelektrik sistemler, çoğu zaman kapıları otomatik açmak için kullanılmaktadır. Algılayıcı hücre, ışığı algıladığında hücrede bir elektrik akımı akmaktadır. Işık kesildiğinde alarm meydana gelecektir.

2.1.2.2 Alan koruması

Alan koruma sistemleri, binalardaki iç alanları korumak için kullanılmaktadır. 3 tip çok etkin alan koruma sistemi vardır :

- Ses algılama sistemleri
- Elektronik titreşim algılama sistemleri
- Hareket algılama sistemleri

Ses algılama sistemleri, alan içine göze çarpmayacak şekilde kurulmuş mikrofon-hoparlör ünitelerini kullanmaktadır. Bir vandal veya hırsız tarafından çıkarılan anormal gürültü algılanıp derhal izleme istasyonuna bildirilmektedir.

Bir elektronik titreşim detektörü, yaklaşık cep saati büyüklüğünde geliştirilmiş özel bir mikrofondur. Duvarlara, zemine veya tavana monte edilebilmekte ve bir kontrol ünitesine bağlanmaktadır. Bu sistem, korunan yüzeylere yapılan her türlü müdahaleyi algılamaktadır.

Hareket algılama sisteminde, korunacak alanda bir elektromanyetik dalga modeli oluşturulmaktadır. Böyle bir alana habersizce giren bir kişi hareketleri nedeniyle bu dalga modelini bozacaktır. Bu bozulma bir alarm devresini harekete geçirecek kontrol ünitesi tarafından algılanacaktır. Bazı sistemlerde, dalga modelini analiz etmek için ve insan hareketi ile zararsız küçük karışıklıkları ayırt edebilmek için özel fark devreleri kullanılmaktadır.

2.1.2.3 Nesne koruması

Nesne koruması, nesnelerin doğrudan korunmasıdır. Bu koruma, çeşitli koruma yöntemlerinin kullanıldığı bir sistemde en son basamaktır. Korunmasına en çok ihtiyaç duyulan nesneler; kasalar, çalışma masaları, dosyalama kabinleri ve pahalı ekipmanlardır.

Nesne koruması için bir çok tip detektör mevcut olsa da kapasitans koruması en çok kullanılan sistemdir. Bu sistemde nesnenin kendisi bir anten olmakta ve bir algılama kontrol ünitesine bağlanmaktadır. Bir insan bu nesneye yaklaştığında veya dokunduğunda, elektrostatik alanın dengesi bozulacaktır. Bu durum kontrol ünitesi tarafından analiz edilecek ve alarm devresi devreye girecektir. Bu tip koruma oldukça esnek ve çok ekonomiktir.

2.2 Geçiş Kontrol Sistemleri

Bir geçiş kontrol sisteminin en temel amacı; bir takım fiziksel araçlar kullanarak bir alan veya binaya girişi kontrol altına almaktır. Bu kontrol; bir düğmeye basılmasıyla elektrikli bir kilitin kapıyı serbest bırakması gibi basit bir sistem şeklinde olacağı gibi, biyometrik okuyucular kullanılan gelişmiş bir geçiş kontrol sistemi de olabilir.

Bir giriş noktasına uygulanacak geçiş kontrol için temel ihtiyaçlar :

- Giriş hakkının verilmesi için doğrulama (kart okuyucu)
- Kapıyı fiziksel olarak kilitlemek veya açmak için kullanılacak elektromekanik cihaz
- Kontrol paneli
- Kapının ve/veya kilidin durumunun gözlenmesi

2.2.1 Kart okuyucular ve kartlar

Basit manyetik şerit okuyuculardan biyometrik okuyuculara kadar, herbiri farklı güvenlik seviyeleri sunan birçok farklı kart okuyucu ve kart çeşidi vardır.

Kartlı geçişin en zayıf yanı giriş elde etmek için kullanılan kart ve bu kartın hakları arasındaki bağlantıdır. Kartlı geçişin çoğu durumda bir insana değil bir karta uygulandığını unutmamak gerekir.

2.2.1.1 Manyetik şerit

Plastik bir kartın arkasındaki manyetik şerit, kart numarası ve yer kodu gibi bilgileri saklar. Kart, okuyucuya sürtülür veya yerleştirilir ve bilgi manyetik şeritten okunur.

Manyetik şeritli kart, düşük maliyet ve manyetik şerit çözücü kullanarak programlama kolaylığı sağlar.

PCSC okuyucular, 12 rakamlı tek bir veri hattı ile veri çıkışı vermektedir. Okuyucunun konfigürasyonuna bağlı olarak veri, 2 yöntemle kullanılabilir.

1-Binary Mod : 12 rakam formatındaki 5 rakam yer kodu içindir, 2 rakam sıfırdır ve diğer 5 rakam da kart numarasıdır. Yer kodu ve kart numarası için maksimum sayı 65535'tir. Karttan okunan yer kodu, kontrol panelindeki yer koduyla kıyaslanır.

Örnek : 123450067890 verisine sahip bir kart, binary konfigürasyonlu bir okuyucuya okutulduğunda yer kodu 12345, kart numarası ise 67890'dır.

2-Desimal Mod : 12 rakam da kart numarası olarak kullanılır. Kart numarası için maksimum sayı 999999999999'dur. Kontrol panelindeki yer kodu bu kart okuyucu için ihmal edilir.

Örnek : 123450067890 verisine sahip bir kart, desimal konfigürasyonlu bir okuyucuya okutulduğunda kart numarası 123450067890'dır.

2.2.1.2 Baryum Ferit

Baryum Ferit kartta, PVC kartın iki kalıbı arasında kalıcı mıknatıs Baryum Ferit (BaFe) tabakası kullanılır.

Baryum Ferit şerit üzerindeki veri formatında kart numarası ve yer kodu gibi kart parametreleri saklanır. Bu kart da manyetik şeritli kart gibi iki yönlüdür.

Eski teknoloji Baryum Ferit kartlarda çok kuvvetli mıknatıslar kullanıldığından diğer tip kartlara olumsuz etkide bulunurlardı ve ayrı bir ortamda saklanmaları gerekirdi. Günümüzde mıknatısları o zamanki kadar güçlü değildir ve diğer tip kartlarla birarada bulunmalarının bir sakıncası yoktur.

Baryum Ferit kartlarda, manyetik şeritli kartlardaki gibi standartlar yoktur. Kart veri formatları, üreticiler arasında çeşitlenir.

2.2.1.3 Wiegand

Wiegand kart, kartı oluşturan iki plastik arasında bulunan iki tel grubu içerir. Bu kart sadece bir yönde okuyucuya okutulur. Veriler okuyucudan kontrol paneline iletilir.

Aktif kartlar içlerinde pile sahiptir ve bir dış kaynaktan enerji alırlar. Bu kartlar her zaman aktiftir ve genelde araç tanıma sistemlerinde kullanılırlar.

Proximity kart ve okuyucular daha çok tercih edilmektedir, çünkü kartı okuyucuya sürtmek yada yerleştirmek gerekmemektedir. Üretici firmalar okuyucuların estetik görünümüne de dikkat etmekte ve yeni modeller geliştirmektedirler.

Okuyucular, hava şartlarından ve vandalizmden korunmayı sağlayacak muhafazalar içine yerleştirilebilir. Fakat bu muhafazanın, okuma mesafesini doğrudan etkileyecek olan metal bir malzemeden imal edilmemesine dikkat edilmelidir.

2.2.1.5 Biyometrik okuyucular

Biyometrik okuyucular, geçiş kontrol sistemlerindeki başarısızlık olasılığını en aza indirmek hatta ortadan kaldırmak için dizayn edilmiştir.

Geçiş kontrol çoğu zaman bir karta uygulanmaktadır ve giriş hakları istenilen şekilde kısıtlanamayabilir. Çünkü kartla, giriş hakkı talep edildiği an karta sahip olan kişinin kim olduğu bilinemez. Kayıp, çalınmış diye rapor edilen kartların yetkilerinin iptal edilmesi de tam anlamıyla bir çözüm olmayacaktır. Kartı kullanan kişinin kartın gerçek sahibi olduğu garanti edilemez. Biyometrik okuyucular, bu güvenlik açığının üstesinden gelirler ve genellikle yüksek güvenlik gerektiren yerlerde kullanılmaktadırlar.

Biyometrik okuyucular; korunan bir alana giriş hakkı isteyen bir kişinin kimliğinin tespit edilmesi ve giriş izninin olup olmadığının kontrolü için kullanılmaktadır.

Biyometrik okuyucular; kişinin kimliğini, vücudunun bir parçasının (el, parmak izi, retina gibi) görüntüsünü okuyarak ve bu görüntüyü daha önce hafızasına kayıt edilmiş görüntüyle karşılaştırarak tespit eder. Eğer mevcut görüntü, önceden kaydedilmiş görüntüyle (belli bir toleransla) uyumluysa kimlik onaylanır ve giriş hakları incelenir. Okuma toleransı değiştirilebilir. Böylece yanlış okuma ve reddetme olasılığı azaltılabilir veya yükseltilebilir.

Farklı tiplerde biyometrik okuyucular mevcuttur:

- El okuyucular
- Parmak izi okuyucular
- Retina tarayıcılar
- Ses tanıyıcılar

2.3 CCTV Sistemleri

CCTV, kapalı çevrim çalışan bir televizyon sistemidir ve ilk olarak 50'li yıllarda kullanılmaya başlanmıştır. Günümüzde teknolojiye ilerlemeler sonucu kayıpların önlenmesi, video gözetimi, personel güvenliği konusunda en önemli araç haline gelmiştir.

Dükkan sahipleri, CCTV'yi hırsızları görüntülemek veya kilometrelerce uzaktaki dükkanlarını, ürünlerini kontrol etmek amacıyla kullanırlar. Üreticiler, hükümet kuruluşları, hastaneler ve üniversiteler, personeli ve ziyaretçileri tanımlamak, iş alanlarını kontrol etmek, hırsızlıkları engellemek, binanın ve otopark alanının güvenliğini sağlamak için CCTV sistemlerini kullanmaktadırlar.

CCTV sistemleri, kayıpların önlenmesi ve güvenliğin sağlanmasında teknolojik ilerlemeler sonucu şaşırtıcı ölçülere ulaşmıştır. Fakat CCTV sistemlerinin bu ölçüye kendi başına ulaşamayacağı unutulmamalıdır. Sistemi kullananların, sistemi yeterince bilmeleri, kameraların saptadığı görüntü ve olaylara anında gereken reaksiyonu göstermeleri gerekmektedir.

CCTV sistemlerinde gereken malzemenin seçimi, tamamen kullanıcının seçimine bağlıdır. Malzemenin seçiminden önce güvenlik personelinin ve yöneticilerin amaçlarını irdelemeleri gerekmektedir.

2.3.1 CCTV sistemlerinin uygulama alanları

2.3.1.1 Güvenlik uygulamaları

Geçiş kontrol sistemleri ile birlikte kullanılarak işletmeye yapılan giriş-çıkışların kontrolü ve videoya kayıt edilmesi sağlanmaktadır. Hareketli bir kameranın programlanması sonucu, pan tilt ve zoom işlemleriyle işletme kontrol edilmektedir.

Satış reyonlarının, büroların, depoların, otoparkların sürekli gözetimde tutularak hırsızlık veya saldırı olaylarının saptanması ve kayıt edilmesi için kullanılmaktadır. Önemli bölgeler (kasa vb.) monitörle gözlenebilmektedir.

2.3.1.2 Personel emniyeti uygulamaları

Sağlık açısından tehlikeli olan bölümler, olası kaza bölgeleri monitör ile izlenmekte ve güvenlik görevlileri, polis, itfaiye, acil sağlık personeli olay yerine zamanında çağırılabilir.

2.3.1.3 Yönetim uygulamaları

Stokların kontrolü için, satışların izlenmesi için ve üretim alanında iş akışının düzenli olarak gözlenmesi için kullanılmaktadır.

Bunların dışında CCTV sistemleri trafik akışının düzenli olarak sağlanmasında da polis görevlilerine büyük kolaylık sağlamaktadır.

2.3.2 CCTV sistemlerine genel bakış

CCTV sistemi, kamera ile okunan ayrı ayrı resimler (kare) dizisinin monitöre taşınması ve izleyiciye monitör aracılığıyla gösterilmesidir.

Bütün CCTV sistemlerinde aşağıdaki temel elemanlar bulunur.

- Aydınlatma
- Kamera ve lensler
- Video sinyallerinin taşınması
- Monitörler
- Çevre Birimleri

Kameranın okuyacağı resmin kaliteli olması için, çekim yerinde; doğal, suni veya her ikisinden oluşan yeterli aydınlatma sağlanmalıdır. Resmin okunabilmesi için çevre koşullarına, kullanım amacına ve fiyata bağlı olarak uygun kamera ve lensin seçilmesi gerekmektedir. Video sinyallerinin kameradan monitöre taşınması zorunludur. Çevre koşullarına, fiyata ve istenen görüntü kalitesine bağlı olarak bir taşıma yöntemi seçilecektir.

CCTV sistemleri eskiden, herbiri güvenlik personeli tarafından izlenen monitörlere sinyaller gönderen kameralardan oluşurdu. Teknolojideki ilerlemeler yeni tasarım kavramları getirdi. Son yıllarda mikroişlemciler, video sinyallerini taşıma yöntemleri ve matris değiştiriciler konusundaki ilerlemeler, eski geleneksel sistemin bütün kısıtlamalarını ortadan kaldırdı. Ulaşılması çok zor olan işletmelere düşük maliyetli telefon kabloları ile ulaşma imkanı, hareket algılanan bölgeye kameraları çevirebilme imkanı ve bir tek video kayıt cihazına 16 ayrı kameranın görüntüsünü kayıt edebilme imkanı yaratılmıştır.

Bir kuruluş, CCTV sisteminde işlem parametrelerini (görüntüler, dome uyarıları vs.) ve yönetim parametrelerini (işlemler, yedek kayıtlar vb.) belirleyecek bir sistem yöneticisi ile amacına ulaşabilir. Önemli olan; sistem yöneticisinin, kuruluşun yönetim kadrosu ile birlikte çalışarak CCTV sistemi amaçlarının işletme politikasına uygun biçimde saptanmasıdır.

Sonuçta; CCTV sistemi kurmak isteyen kuruluş, personeli hedeflerine uygun biçimde eğitmelidir. Yönetim; amaçlarının, kuruluşun mallarını korumak, personeli korumak ve güvenilir bir çalışma ortamı yaratmak olduğunu belirtmelidir.

2.3.2.1 Aydınlatma

CCTV için en önemli faktörlerden biri çekim yerine yansıyan ışığın miktarı, kalitesi ve türüdür. Çünkü kamera nesnelere çarpıp yansıyan ışığı görür.

Bir çekim yeri; değişik miktarda ışık yansıtan farklı renkler, alanlar ve nesnelerden meydana gelir. Kullanılacak uygun malzemenin seçilebilmesi için gece ve gündüz çekim yerinden kameraya ulaşacak minimum aydınlatma seviyesinin saptanması gereklidir. Bu aydınlatma seviyesi resmin kalitesinden netliğine kadar her şeyi etkiler. Çekim yeri, doğal veya suni ışık kaynakları ile aydınlatılabilir.

Renkli kameralar, siyah/beyaz kameralara oranla daha fazla ışık gerektirirler. Nesnelerin saptanması renkli görüntüde daha kolaydır. Örneğin; renkli sistemde izleyici kırmızı ve yeşil otomobili birbirinden kolayca ayırt edebilirken, siyah/beyaz sistemde ikisi de birbirine çok yakın gri tonlarda görünecektir. Renkli sistem, satış dükkanlarında hırsızları giysilerinin renkleri ile çok daha kolay ortaya çıkarabilir.

Siyah/beyaz kameralar ise renklilere oranla daha ucuzdur ve çok düşük aydınlatma seviyelerinde çalışabilirler. Siyah/beyaz kamera görüntülerinin uzun mesafelere taşınma süresi renklilere oranla daha kısadır.

Düşük aydınlatma seviyelerinde kaliteli görüntü verebilecek siyah/beyaz ve renkli kameraların maliyetleri hayli yüksektir. Kamera seçilmeden önce kuruluş, aydınlatma maliyeti ile kamera maliyetini karşılaştırmalıdır.

2.3.2.2 Kamera

Kameralar, lensin algıladığı resimleri elektronik bir sinyale dönüştürür ve bu sinyalleri görüntü vermek üzere monitöre gönderirler.

Yıllarca tüp kameralar güvenlik sisteminde kullanılan tek tür kameralar olmuştur. Günümüzde, kameralar görüntü almak için entegre devre/çip kullanmaktadır. Bu entegre algılayıcılar lensin aldığı ışığı resme dönüştürürler.

Bir CCTV için uygun kamera-lens kombinasyonunu seçerken dikkate alınması gereken çeşitli faktörler vardır.

- CCTV sisteminin amacı
- Çekim yerindeki ışık seviyesi ve ışık seviyesi değişimi
- İstenen görüş alanı
- Maliyet
- Kameranın çalışacağı ortam (iç mekan/dış mekan)

Bütün kameraların performansı, büyük ölçüde çekim yerinden yansıyan ışığa ve kamera algılayıcısının kalitesine bağlıdır. Yansıyan ışık, algılayıcıyı aktif hale getirebilecek yeterlilikte olmalıdır.

Çekim yerindeki ışık seviyesinin değişikliğe uğradığı yerlerde otomatik diyafram kontrollü bir kamera, görüntü kalitesini koruyabilir. Otomatik diyafram kontrolü, diyaframı açıp kapatarak lensten geçen ışık yoğunluğunu ayarlayabilir. Örneğin; güneşli bir günde kamera, diyaframı kapatarak algılayıcıya fazla ışık gelmesini engelleyecektir. Geceleri kamera, diyaframı açarak algılayıcıya daha fazla ışık girmesini sağlayacaktır. Otomatik diyafram kontrolü olmayan kameralar fazla ışık değişikliği olmayan iç mekanlarda ve suni aydınlatma altında kullanılmalıdır.

CCTV kameraları sabit yada hareketli (yani pan tilt zoom özelliklerine sahip) olabilir. Sabit kameralar, sabit bir yuvaya oturtulur ve hareket etmez. Hareketli (pan tilt) kameralar ise bir motorla sağa sola (pan), aşağı yukarı (tilt) hareket ettirilebilir ve zoom özelliklerine sahiptir.

Kamera koruma kutusu, kamera ve lensi saldırılardan ve çevre koşullarından korur. Kameranın görüntüsünü güzelleştirir, montajını kolaylaştırır ve içindeki malzemelerin görünmesini engeller. Dış mekanlarda kullanılacak bütün kameraların bir koruma kutusuna ihtiyacı vardır. Kameraların en yüksek performansı gösterebilmeleri ve ömürlerinin uzaması için soğuk, sıcak, toz, kir ve diğer etkenlerden sürekli olarak korunması gerekir.

PTZ kameraların büyük bir bölümü günümüzde dome adı verilen koyu renkli bir yuva ile gizlenmektedir. Büyük marketlerde, alış veriş merkezlerinde, birçok endüstriyel/ticari işletmede, hastanelerde, okullarda ve hükümet kuruluşlarında dome kameralar kullanılmaktadır. Açıkta olan bir kamera; lens, pan tilt motoru ve kabloları ile kötü bir görünüme sahiptir. Dome kamera kutusu bütün bunları içinde toplayarak estetik bir görünüm sağlar. Dome kamera gibi gözükecek içi boş dome'lar kullanılarak görünen kamera sayısı yükseltilebilir. Sonuçta; düşük bir maliyet artışı ile görünen kamera sayısı artırılabilir.

2.3.2.3 Lensler

Lenslerin CCTV sistemi tasarımındaki yeri çok önemlidir. Lensler, çekim yerinden yansıyan ışığı toplayarak kameranın görüntüleyecisine net bir görüntü yollamaktadırlar. Lensten geçen ışık ne kadar fazla ise resim kalitesi o kadar iyi olur.

Lens seçimi kritik bir konudur ve görüntüleyiciye aktarılan resmin boyutunu, biçimini ve niteliğini doğrudan etkiler.

Uygun görüntüleyici boyutu ve mesafe kombinasyonunun istenilen görüş açısını vermesi için hesaplama tabloları vardır. Kamera lensleri iki ana bölüme ayrılabilir: Sabit odaklı ve değişken odaklı (zoom). Sabit odaklı lenslerin odak uzunluğu değişmez. Odak uzunluğu, mercek merkezinden lensin arkasındaki odak noktası arasında kalan mesafedir. Bu uzunluk lens üzerinde yazılıdır ve lensin görüş açısını belirtir.

Sabit odaklı lensler; geniş, orta ve dar görüş alanı için ayrı ayrı tasarlanmıştır. Belirli bir görüş alanı için sabit odaklı bir lens seçildiğinde, görüş alanını değiştirmek istediğinizde lensi de değiştirmeniz gerekmektedir.

Hem uzak, hem de yakın görüntüler isteniyorsa değişken odaklı (zoom) lens kullanılmalıdır. Böylelikle tek bir lensle görüş açısını dar, orta ve geniş açığa çevirmek mümkündür.

Bir lensin ışık toplama yeteneği, merceğin açılması ile odak uzunluğu arasındaki ilişkiye bağlıdır. Bu ilişkinin simgesi “f” harfidir ve genelde f-stop değeri lenslerin üzerinde yazılıdır. f-stop değeri ne kadar küçükse maksimum mercek açılışı o kadar büyüktür ve lensin kamera görüntüleyicisine ışık geçirme yeteneği o kadar fazladır. Örneğin; f-stop değeri 1.2 olan lens, f-stop değeri 4 olan bir lensten çok daha fazla ışık toplayabilir.

Lensler C-montaj veya CS-montaj olarak üretilirler. İki tip lens arasındaki fark; mercek ile kamera görüntüleyicisi arasındaki mesafedir. C-montaj lensin görüntüleyiciye uzaklığı 17.5 mm iken, CS-montaj lensin görüntüleyiciye uzaklığı 12.5 mm’dir. C-montaj lens, ancak 5 mm’lik bir ara parça takılarak CS-montaj lens isteyen bir kamerada kullanılabilir. CS-montaj lensler ise hiçbir şekilde C-montaj lens gerektiren bir kamerada kullanılamaz.

Kameralar lensin algıladığı resimleri elektronik bir sinyale dönüştürür ve bu sinyalleri görüntü vermek üzere monitöre gönderirler.

2.3.2.4 Video sinyallerini taşıma yöntemleri

Taşımanın amacı; kameranın gönderdiği video sinyallerinin monitöre ulaşmasını sağlamaktır. Günümüzde bir çok taşıma yöntemi kullanılmaktadır. Bütün bu teknolojilerin kendilerine özgü avantaj ve dezavantajları vardır.

CCTV video sinyalleri 30 Hz ile 10 MHz arasında geniş bir aralıkta yer almaktadır. Sinyal kalitesi düşünüldüğünde, bu geniş bantta çalışmak için özel devreler gerekmektedir. CCTV video sinyallerinin zaman zaman uzun mesafeler kat etmesi gerektiği için değişik durumlara göre özel taşıma yolları bulunmaktadır. Taşıma yönteminin seçilmesi sırasında mesafe, maliyet ve işletme planı gibi faktörlerin dikkate alınması gerekir. Bu yöntemlerin hemen hemen hepsi belli ölçülerde parazit ve kayba neden olur.

Koaksiyel kablo, kamera ve monitör arasında sürekli fiziki temas sağlayan bir taşıyıcıdır. Kablo yakınındaki elektronik aygıtların karışımını engellemek için izole edilmiştir. Gerek geleneksel CCTV sistemlerinde ve gerekse günümüzde kullanılan bir çok uygulamada kısa mesafeler arasında video sinyali taşınması için bu yöntem en yaygın ve maliyeti en düşük olanıdır. Koaksiyel kablolar genellikle 75 ohm empedanslı yüksek kaliteli kablolardır. Kablo en içte bakır iletken ve bunu saran sert yalıtıkana (örn; polythene) sahiptir. Daha dışta örgü şeklinde bakır yer alır. En dışta ise dış etkilere korunmak için PVC yer alır.

Bükülmüş çift telli kablo 75 ohm empedans ve 1 volt sinyali kabul eder ve bu sinyali kullanırken kablosuna göre 2 volt, 50 ile 150 ohm arasında empedanslı sinyale çevirir. Bu uygulama ucuzdur ve koaksiyel kablo yönteminden daha uzun mesafelere sinyallerin taşınmasını sağlar. En büyük dezavantajı, her sinyal kaynağı için ayrı bir gönderme ve alma ünitesi gerektirmesidir. Çünkü monitörler doğrudan bükülmüş çift telli kablo ile taşınan sinyali kabul etmezler.

Fiber optik teknolojisi, elektronik video sinyallerini lazer ışını şekline dönüştürmekte ve cam telin diğer tarafına vermektedir. Kopan bir fiber optik kablodan kıvılcım çıkma olasılığı yoktur. Böylece yangın tehlikesinin en yüksek olduğu ortamlarda bile güvenle kullanılabilir. Fiber optik ile video sinyallerinin taşınması günümüzde artarak kullanılmaktadır. Optik fiberler, optik geçirgenliği çok fazla olan çok ince cam tellerdir. Kablolarla oranla çok düşük kayba yol açarlar ve elektriksel karışımlara maruz kalmazlar. Laser teknolojisindeki gelişmeler fiber optiğin video sinyali taşınmasında kullanılmasını arttırmıştır. Laser demetine dönüştürülen video sinyali fiber boyunca 50 km'den uzak mesafelere bile taşınabilmekte ve görüntü kalitesi mükemmel kalmaktadır.

Mikrodalga, siyah/beyaz ve renkli video sinyallerinin taşınması için çok etkili ve düşük maliyetli bir yöntemdir. Mikrodalga, video sinyallerini yüksek frekanslı radyo sinyallerine dönüştürerek bir noktadan diğerine herhangi bir kablo kullanmaksızın havadan taşır. Bu sistemde mikrodalga kaynakları, binaların veya kulelerin üstüne birbirini görecektir şekilde yerleştirilmelidir. Bu sistem kablo çekmenin zor olduğu şehir mekanlarında, nehir kıyılarında ve benzer yerlerde kullanılmaktadır.

Radyo frekansı teknolojisi, kısa mesafelerdeki görüş doğrultusunda güvenilir bir yöntemdir. Kablolu yöntemlerin olanaksız veya maliyetinin çok yüksek olduğu durumlarda, kullanılması giderek artmaktadır. Çevresel ortamdan ve diğer radyo frekanslarından etkilenirler. Bant genişliği, monitör tarafından alınan video görüntülerinin kalitesini etkileyecektir. Dar bantlarda taşınan görüntüler bütün karelerin taşınamaması nedeniyle çok net olarak görünmeyecektir.

2.3.2.5 Monitör

Monitör, kameradan gelen elektronik video sinyallerini alarak, görüntüyü yaratmak için katot ışın tüpüne aktarır. Bir televizyon sistemine çok benzemesine karşın daha yüksek bir çözünürlük sağlar.

Çözünürlük çizgileri, kamera yada monitörün gösterebileceği toplam yatay çizgiler anlamında kullanılmaktadır. Ekranda ne kadar fazla yatay çizgi olursa resim kalitesi o kadar iyi demektir. Televizyonlarda ortalama 300 çizgi varken, CCTV monitörlerinde bu rakam 700-800 çizgilik bir çözünürlüğe ulaşmaktadır.

Monitörlerin sayısı ve operatörlerin çalışmasına göre yerleri, tasarımın ilk aşamalarında dikkatle incelenmelidir. Monitör seçimini çeşitli faktörler etkileyebilir: Monitörün ekran ölçüsü (9", 14" vb.), izleyicinin oturduğu yere göre monitör pozisyonunun açısı, monitör adedi ve çözünürlük oranı. Sistem genişledikçe monitörlerin bir konsol tasarımına dönüştürülmesi gerekir. Monitörlerin yayacağı ısı da unutulmamalıdır. Masanın üzerinde yada bir konsol içinde de olsa hava almasına ve soğutulmasına özen gösterilmelidir.

CCTV sistemlerinin büyük bir çoğunluğunda; hem tahsis edilmiş monitörler, hem de istenilen görüntünün çağrılabilmesi yada iki veya daha fazla kamera görüntüsünün izlenebileceği monitörler kullanılır. Tahsis edilmiş monitör sadece bir kameranın görüntüsünü ekrana getirir. İstenilen görüntülerin çağrıldığı yada iki veya daha fazla kamera görüntüsünün izlenebileceği monitörler için bir tür seçici sistemi gerekmektedir.

2.3.2.6 Zaman atlamalı video kayıt edici

CCTV sistemlerinde kullanılan videolar, normal video cihazlarından farklı olarak zaman atlamalı kayıt yapma yeteneğine sahiptirler.

Zaman atlamalı video (Time Lapse Video) olarak bilinen bu videolar üç saatlik standart bir video kasete markasına ve özelliklerine bağlı olarak 24 saatlik, 72 saatlik, 168 saatlik veya 960 saatlik kayıt yapabilmektedirler. CCTV sisteminde kullanılacak video seçilirken dikkate alınması gereken en önemli faktör kayıt süresidir.

2.3.2.7 Video seçici

CCTV sistemlerinde bir monitörden birden fazla kamera takip edilmek isteniyorsa bir video seçici kullanılması gerekmektedir.

Video seçiciler 2, 4, 6, 8 veya 12 kanallı olabilmektedir. Örneğin; 6 kanal bir video seçici vasıtasıyla 6 kamera görüntüsünden hangisi görülmek isteniyorsa monitöre getirilebilir.

2.3.2.8 Quad seçici

Quad seçiciler, video seçicilerden farklı olarak ekranı dörde bölebilir ve dört kamera görüntüsü de aynı anda monitörden gösterebilir. Bir quad seçiciye en fazla 4 kamera bağlanabilir. Bu kameraların görüntüleri, monitörden dördü bir arada izlenebildiği gibi tek tek tam ekran olarak da izlenebilir. Quad seçiciler siyah/beyaz ve renkli olmak üzere iki gruba ayrılırlar. Renkli sistemlerde renkli quad, siyah/beyaz sistemlerde siyah/beyaz quad kullanılmalıdır.

2.4 Sistemlerin Merkezi Entegrasyonu

Günümüz binalarında güvenliği sağlamak amacıyla; alarm, kartlı geçiş ve CCTV sistemlerinin bir arada kurulması, bu sistemlerin bir merkezden gözlenebilme ve kontrol edilebilme zorunluluğunu ortaya çıkarmıştır.

Çeşitli firmalar tarafından bu sistemleri tek bir merkezden izleyebilen ve kontrol edebilen yazılımlar geliştirilmiştir. Honeywell tarafından geliştirilen Excel Security Manager yazılımı ile böyle bir entegrasyonu sağlamak mümkün olmaktadır.

XSM yazılımı ile; kartlı geçiş sistemine ait saha kontrol ünitelerinin, kart okuyucularının, kapıların ve turnikelerin durumları izlenebilmekte, istenen karta istenen geçiş hakkı

verilebilmekte, kapı ve turnikeler dinamik ekranlardan açılıp kapatılabilmektedir. Alarm sistemindeki alarm noktalarının durumları gözlenebilmekte, CCTV kameralarının görüntüleri izlenebilmekte, istenen kamera görüntüsü istenen monitöre aktarılabilmektedir. Bu yazılım ile yangın sistemi de izlenip kontrol edilebilmektedir. Detektör ve yangın alarm butonlarından gelecek alarmlar görülebilmekte ve flaşörlerle kornalar isteğe bağlı olarak da kontrol edilebilmektedirler.

2.4.1 XSM sistemi temel fonksiyonları ve özellikleri

2.4.1.1 Temel fonksiyonlar

- Kapıların izlenmesi
- Kart konfigürasyonu ile kartlı geçiş kontrolü
- Yangın izlemesi
- Kritik olayların takibi
- Sistem saha cihazları ve operatörler tarafından yapılan işlemlerin kaydedilmesi
- İstenilen zamanda çeşitli raporlar alınabilmesi
- Asansör kartlı geçiş kontrolü
- CCTV kamera seçme kontrolü

2.4.1.2 Özellikler

- Zaman programlamalı kontrol
- Alarm yönetimi
- Güvenlik, kartlı geçiş, CCTV ve yangın cihazlarının entegrasyonu
- Yerel veya uzak bağlantı
- Detaylı sistem takibi için ekranlar oluşturma
- Operatör bilgisayarlar
- Olay arşivi
- Aydınlatma kontrolü
- Operatör güvenlik ve kontrol seviyeleri

2.4.1.3 İşletim sistemi

XSM Server yazılımı, MS Windows NT 4.0 üzerinde çalışacak şekilde dizayn edilmiştir. Operatör yazılımı ise MS Windows NT 4.0, MS Windows 95 veya MS Windows 98 sistemleri üzerinde çalışabilmektedir.

2.4.1.4 XSM server yazılım seçenekleri

Kontrolör arabirimleri : Farklı tip kontrolörlerle haberleşmeyi sağlayan yazılımlardır.

Yedek server : İkinci bir server bilgisayarının yedek olarak kullanılabilmesini sağlayan yazılımdır.

Aydınlatma kontrolü : Bir kartın, programlanmış okuyucuya gösterilmesi durumunda cevap olarak aydınlatmanın devreye girmesini sağlayacak yazılımdır.

CCTV kamera kontrolü : Operatörlere kameraları kontrol etme ve izleme imkanı sağlayan yazılımdır.

Bölge raporlaması : Seçilen bölgede, o anda bulunan kart sahiplerinin raporunu almayı sağlayan yazılımdır.

Kart kullanım raporlaması : Bir kartın kaç defa kullanıldığı hakkında rapor almayı sağlayan yazılımdır.

2.4.1.5 XSM konfigürasyon yazılımı (Quickbuilder)

Quickbuilder, server bilgisayarda yer alacak, donanım bağlantılarını ve nokta bilgilerini konfigüre etmek veya değiştirmek için kullanılan yazılımdır. Bu yazılım yardımıyla bir proje dosyası hazırlanıp server bilgisayara yüklenir. Var olan bir konfigürasyondaki bilgiler de bu yazılım aracılığıyla öğrenilebilmekte ve değişiklikler yapıp tekrar server bilgisayarına yüklenebilmektedir.

2.4.1.6 XSM operatör yazılımı (Station)

Sistem bu yazılım yardımıyla server dışındaki operatör bilgisayarlar aracılığıyla izlenebilmekte ve kontrol edilebilmektedir.

Operatör bilgisayar ile server bilgisayarda depolanan veriler farklı ekranlar kullanılarak görülebilmektedir. Örneğin; bir ekran yardımıyla yetki seviyeleri görülebilirken, bir diğer ekran yardımıyla aktif durumdaki alamlar izlenebilmektedir.

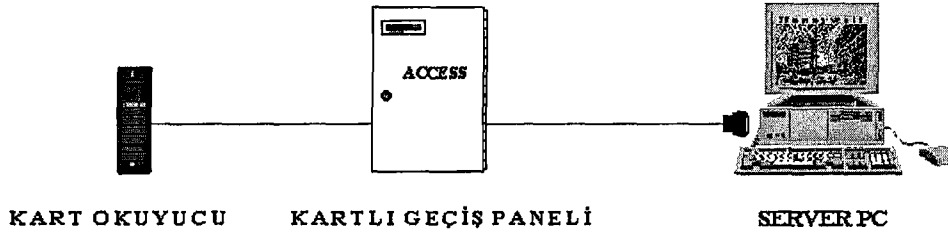
2.4.1.7 XSM grafik yazılımı (Displaybuilder)

Bu grafik yazılımı ile operatör bilgisayarlarda görülecek ekranların dizaynları yapılabilir. Bu yazılım yardımıyla istenen tarzda veriye sahip ekranlar oluşturulabilmekte ve bu ekranlar operatör bilgisayarlar tarafından izlenebilmektedir.

Ekranlar oluşturulurken genel olarak, alarmların nerelerden geldiğini detaylı olarak gösterecek bina planları kullanılmaktadır.

2.4.2 XSM server

Şekil 2.1’de görülen basit bir sistemde MS Windows işletim sistemiyle çalışan XSM server bilgisayarı vardır. Bu bilgisayarda; server veritabanını içeren server yazılımı, sistemi çalıştırmaya ve konfigüre etmeye yarayan operatör, konfigürasyon ve grafik yazılımları yer almaktadır.

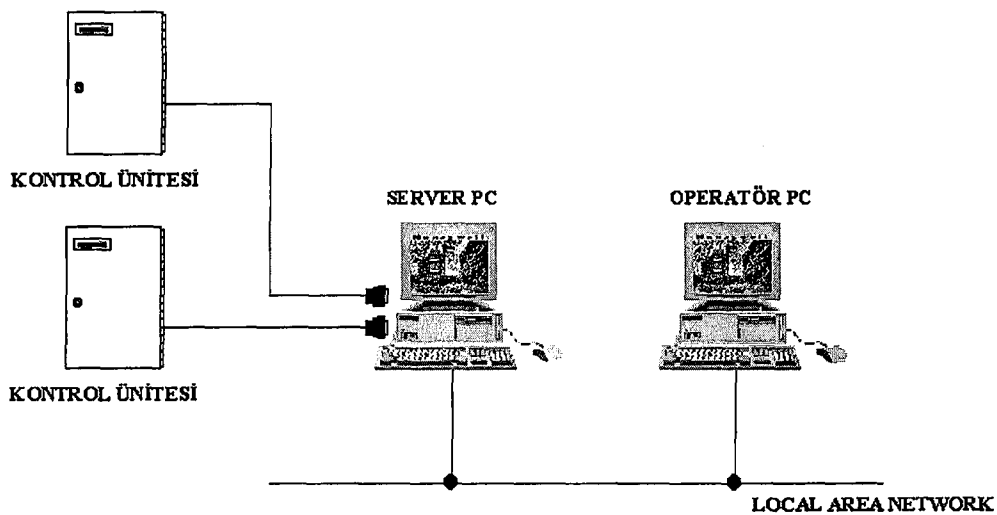


Şekil 2.1 Temel XSM sistemi.

Server, seri bir bağlantıyla yada bir terminal server bağlantısı ile kontrolörlere bağlanabilmektedir.

Rapor almak ve alarmları takip etmek için, server bilgisayara bir yazıcı bağlanabilmektedir.

Daha büyük sistemlerde, server bilgisayar diğer operatör bilgisayarlara ve kontrolörlere bir network aracılığıyla bağlanabilmektedir. Şekil 2.2’de LAN kullanan tipik bir sistem konfigürasyonu görülmektedir.



Şekil 2.2 LAN kullanan tipik bir XSM sistemi.

XSM, network haberleşmesi için TCP/IP kullanmaktadır. Sistem, modemle bağlanmış birimlerle haberleşebilecek WAN konfigürasyonlarına da imkan sağlamaktadır.

2.4.3 Yedek server

Yedek server seçeneği, daha yüksek güvenilirliğe sahip bir konfigürasyonun oluşturulabilmesine olanak sağlamaktadır. Yedek server bilgisayar, ana server bilgisayarın herhangi bir nedenle devre dışı kalması durumunda devreye girerek sistemin düzgün bir şekilde çalışmaya devam etmesini sağlamaktadır.

2.4.4 Operatör bilgisayarlar

Operatör bilgisayarlar, MS Windows NT 4.0, MS Windows 95 veya MS Windows 98 işletim sistemlerinden biriyle çalışabilen operatör yazılımına sahip bilgisayarlardır.

Operatörler, bu bilgisayarlar yardımıyla sistemi izleyebilmekte ve kontrol edebilmektedirler.

Operatör bilgisayarlar, server bilgisayara;

- Doğrudan seri bağlantı ile (Operatör PC'deki seri port, server PC'deki seri porta bağlanır.)
- TCP/IP network bağlantısı ile
- Modem aracılığıyla çevirmeli seri bağlantı ile bağlantı kurabilmektedir.

2.4.5 Kontrolörler

Kontrolörler (Alarm panelleri, kartlı geçiş panelleri, CCTV seçicileri); kart okuyucularla, kameralarla, infrared dedektörlerle ve XSM server bilgisayarla bağlantılara sahiptir. Kontrolörler, saha cihazlarından verileri toplayıp server bilgisayara iletirler.

Tiplerine bağlı olarak kontrolörler, server bilgisayara;

- Doğrudan seri bağlantı ile (genellikle RS232)
- Terminal server aracılığıyla (Seri haberleşen cihazları network'e bağlar.)

bağlanabilmektedir.

Kontrolörleri server bilgisayara bağlamak için kullanılan haberleşme bağlantılarına kanal adı verilmektedir. Genellikle her bir kontrolör tipi farklı bir haberleşme protokolü kullanır, bu yüzden de kendine ait bir kanala sahiptir.

2.4.6 Yazıcılar

Yazıcı; basit bir sistemde paralel veya seri port aracılığıyla doğrudan server bilgisayara

bağlanmaktadır. Daha büyük sistemlerde; network'e bağlı yazıcılardan raporlar alınabilmektedir.

2.4.7 XSM sisteminde geçiş kontrolü

2.4.7.1 Kart detayları

Bir kart sahibi için iki tür bilgi server veritabanında yer almaktadır; kişisel bilgiler ve geçiş bilgileri.

Kişisel bilgiler; kart sahibinin ismi, kart numarası ve diğer bilgileri (şirketi, telefon numarası vb.) içermektedir.

Geçiş bilgisi; kart sahibinin girebileceği bina bölümlerini belirleyen yetki seviyelerini, kartın kullanım süresini ve durum bilgisini (aktif, kayıp, çalınmış veya kapalı) içermektedir.

2.4.7.2 Geçiş noktaları

Geçiş noktaları; bir bölgeye girişi veya çıkışı, yani bir kart okuyucuyu temsil eden noktalardır. Bu noktalar XSM konfigürasyon yazılımı ile konfigüre edilip server bilgisayara yüklenirler.

2.4.7.3 Geçiş bölgeleri

Geçiş bölgeleri, kart okuyucular ile giriş çıkışı kontrol edilen bölgelerdir. Sisteme yüklenmiş olan geçiş noktaları, geçiş bölgelerini oluşturmaktadır.

2.4.7.4 Zaman periyotları

Kart sahiplerinin yetkilerini belirli saatler arasında sınırlayabilmek için zaman periyotları oluşturulmaktadır.

2.4.7.5 Yetki seviyeleri

Yetki seviyeleri, bir kart sahibinin bir bölgeye geçiş hakkını kontrol etmek için kullanılmaktadır. Yetki seviyeleri; geçiş bölgeleri ve zaman bilgilerinin birleştirilmesi ile oluşturulmaktadır.

Bir karta en fazla sekiz adet yetki seviyesi atanabilmektedir.

Bir kart, kart okuyucuya gösterildiği zaman giriş veya çıkışa izin verilmesi için, karta verilmiş yetki seviyesi; kart okuyucuya atanmış bölge ve zaman parametreleri ile uyuşmalıdır.

2.4.7.6 PGAP (Perimeter Global Anti-Passback)

PGAP; binaya giriş yapıldıktan sonra, çıkış yapılmadan tekrar giriş yapılmasını ve çıkış yapıldıktan sonra, giriş yapılmadan tekrar çıkış yapılmasını engellemek amacıyla kullanılmaktadır.

Bu özellik, binadışı olarak konfigüre edilen bölgelere giriş çıkışlarda aktif olmaktadır.

2.4.7.7 Arşivleme ve raporlama

XSM sistemi, sistemde meydana gelen tüm olayları hafızasında depolar. Olay hafızası belli sayıda olaya ulaştığında dolmaktadır. Bu olaylar harddiske ve kasete kayıt edilebilmektedir.

Olay hafızası dolduğunda bu olaylar arşive kopyalanır ve sistem, arşivi kasete kaydetmesi için operatörü uyaran bir alarm mesajı verir.

Kasete kaydedilmiş olaylar istenilen zamanda tekrar kurulup raporlama için kullanılabilir.

3 UYGULAMA

Bir firmaya ait yönetim binasının güvenlik uygulaması yapılacaktır. Bu bina, büyük bir şehrin içersinde inşa edilmiş, 7 kata sahip bir binadır ve hırsızlık, saldırı gibi olaylara karşı kapsamlı elektronik önlemlerle korunacaktır.

Bu binaya kurulacak sistemlerin sahip olması gereken özellikler ve sistemde kullanılacak ekipmanlar hakkında teknik bilgiler, bina sahibi tarafından yapılacak bir çalışma sonucunda belirlenecektir.

İlk aşamada; belirlenmiş özellikleri sağlayan sistemler tasarlanacak ve uygulamada kullanılacak yazılımlar ile ekipmanlar seçilecektir.

Sonraki aşamada; her bir sistem için, ekipmanların yerleşim ve bağlantı diyagramları dizayn edilecektir.

En son aşamada ise; sistemleri tek bir merkezden yönetmek için kullanılacak yazılımda yer alan noktalar ve dinamik ekranlar konfigüre edilecektir. Sistemde tanımlanan noktalar ile dinamik ekranlar arasındaki veritabanı bağlantıları yapılacaktır.

3.1 Binaya Kurulacak Sistemlerin Sahip Olması Gereken Teknik Özellikler

3.1.1 Sistemlerin fonksiyon tanımları

3.1.1.1 Güvenlik yönetim sistemi ve kartlı geçiş sistemi

Sistem; insanların binaya otomatik giriş çıkışına imkan tanıyacak elektronik araçlarla, binaya serbest girişi engelleyecek fiziksel elemanlar içerecektir.

Kartlı geçiş sistemi aşağıdaki 3 farklı gruba göre çalışacaktır:

- Geniş yetkili kart sahipleri
- Bina personeli
- Geçici kart sahipleri (ziyaretçiler)

Kartlı geçiş sistemi, Çizelge 3.1’de belirtilen bölgelerde kurulacaktır.

Bazı önemli kısımlara giriş, kartlı geçiş sistemiyle kontrol edilecek ve kısıtlı sayıda insana bu kısımlara giriş yetkisi verilecektir.

Alarm sistemiyle, seçilen kapıların açık veya kapalı durumlarının izlemesi yapılabilecektir.

Çizelge 3.1 Kartlı geçiş sistemi

Yer	Kart okuyucular
5. Kat Giriş Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu
5. Kat Genel Müdür Odası Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu
4. Kat Giriş Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu
3. Kat Giriş Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu
2. Kat Giriş Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu
1. Kat Giriş Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu
1. Kat Güvenlik Merkezi Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu
1. Kat Güvenlik Müdürü Odası Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu
Zemin Kat Giriş Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu
Zemin Kat Bina Giriş Turnikesi 1	Giriş kart okuyucu+Çıkış kart okuyucu
Zemin Kat Bina Giriş Turnikesi 2	Giriş kart okuyucu+Çıkış kart okuyucu
Otopark Bina Giriş Kapısı	Giriş kart okuyucu+Çıkış kart okuyucu

Bazı önemli kısımlara giriş, kartlı geçiş sistemiyle kontrol edilecek ve kısıtlı sayıda insana bu kısımlara giriş yetkisi verilecektir.

Alarm sistemiyle, seçilen kapıların açık veya kapalı durumlarının izlemesi yapılabilecektir.

3.1.1.2 Alarm sistemi

Sistem, alarm butonları ve keypad aracılığıyla bir saldırı durumunu saldırganlara belli etmeden güvenlik merkezine bildirecektir.

Monte edilecek alarm sistemi cihazları Çizelge 3.2’de gösterilmiştir.

Çizelge 3.2 Alarm sistemi

Yer	Cihazlar
5. Kat Genel Müdür Odası	Panik butonu
Zemin Kat Banka Şubesi Vezne 1	Panik butonu
Zemin Kat Banka Şubesi Vezne 2	Panik butonu
Zemin Kat Kasa Dairesi Kapısı	Keypad

3.1.1.3 CCTV sistemi

CCTV sistemi, binada belirlenmiş hassas yerlerde gözetim yapılmasına imkan tanıyarak caydırıcı rol oynayacak ve binaya yada içindeki insanlara yapılabilecek saldırıları önceden tespit etmek amacıyla kullanılacaktır.

CCTV kameraları özellikle kapı girişlerinde monte edilecek ve gözetimle beraber görüntü kaydı yapılacaktır.

Görüntüler sistem tarafından kayıt edilecek ve daha sonra analiz edilebilmesi için arşivde saklanacaktır.

CCTV kameralarının monte edileceği yerler Çizelge 3.3'te gösterilmiştir.

Çizelge 3.3 CCTV sistemi

Yer	Cihazlar	
5. Kat Girişi	1/3" CCD Renkli kamera	4 mm lens
4. Kat Girişi	1/3" CCD Renkli kamera	4 mm lens
3. Kat Girişi	1/3" CCD Renkli kamera	4 mm lens
2. Kat Girişi	1/3" CCD Renkli kamera	4 mm lens
1. Kat Girişi	1/3" CCD Renkli kamera	4 mm lens
Zemin Kat Girişi	1/3" CCD Renkli kamera	4 mm lens
Zemin Kat Bina Girişi	1/3" CCD Renkli kamera	4 mm lens
Zemin Kat Banka Şubesi	1/3" CCD Renkli kamera	4 mm lens
Otopark Bina Girişi	1/3" CCD Siyah/beyaz kamera	8 mm lens
Güvenlik Merkezi	17" Renkli monitor	
Güvenlik Merkezi	17" Renkli monitör	
Güvenlik Müdürü Odası	15" Renkli monitor	
Güvenlik Merkezi	9 girişli video multiplexer	
Güvenlik Merkezi	Zaman atlamalı video kayıt edici	

3.1.1.4 Güvenlik kontrol merkezi

Merkez, binanın 1. katında yer alacaktır ve 24 saat personel bulunacaktır. Merkeze kullanılan sistemlerin kontrol araçları kurulacaktır.

Merkezden aşağıdaki sistemlerin gözlem ve kontrolü yapılabilecektir:

- Güvenlik yönetim sistemi ve kartlı geçiş sistemi
- Alarm sistemi
- CCTV sistemi

Tüm güvenlik sistemi kontrol cihazları, merkezde bir konsola yerleştirilecektir. Sürekli kullanımı gerektirmeyen ikincil cihazlar, merkezin başka bir bölümünde kabin içine yerleştirilecektir.

Güvenlik merkezinde bulunacak cihazlar şunlardır:

- Güvenlik yönetim sistemi
- Gerekli software ve hardware ile kurulu olan server bilgisayar
- Gerekli software ve hardware ile kurulu olan operatör bilgisayar
- Renkli raporlar ve grafikler basmak için A4 formatında renkli lazer yazıcı
- Tüm kontrolörler (Kartlı geçiş ve alarm sistemleri)
- CCTV sistemi
- 3 adet monitör
- 1 adet zaman atlamalı video kayıt edici

Güvenlik sistemi konsol ve kabinleri, paslanmaz çelik veya alüminyumdan imal edilecektir. Tüm cihazlar konsolun yüzeyiyle aynı hizada monte edilecektir. Konsoldaki tüm güvenlik cihazları, güvenli bir alana yerleştirilmiş kesintisiz güç kaynağından beslenecektir.

3.1.1.5 Güvenlik resepsiyon bölgeleri

Resepsiyon bölgelerinde, ziyaretçilerin ve personelin binaya rahat giriş çıkışı için gerekli ekipmanlar yerleştirilecektir.

Kurulması gereken ekipmanlar şunlardır:

- Ziyaretçiler için operatör bilgisayar (güvenlik yönetim sistemi uzak terminal)
- X-Ray ünitesi
- Metal dedektörü

Resepsiyon bölgeleri, binanın 1. bodrum katında otoparktan binaya girişte ve zemin katta yer alacaktır.

3.1.2 Cihazların tanımları ve teknik özellikleri

3.1.2.1 Güvenlik yönetim sistemi ve kartlı geçiş sistemi

Güvenlik yönetim sistemi bir LAN (Local Area Network) üzerinde çalışacaktır. Sistem ve network, en az bir server ve 3 operatör bilgisayarı destekleyecek kapasitede olmalıdır. Sistem, network'e bağlı tüm kullanıcıların durumlarını gösterecektir.

Sistemde kurulacak server ve operatör bilgisayarların yerleri Çizelge 3.4'te gösterilmiştir.

Çizelge 3.4 Güvenlik yönetim sistemi

Yer	Bilgisayar
Güvenlik Merkezi	Server bilgisayar
Güvenlik Müdürü Odası	Operatör bilgisayar
Zemin Kat Resepsiyon	Operatör bilgisayar
Otopark Resepsiyon	Operatör bilgisayar
Güvenlik Merkezi	Renkli laser yazıcı

Tüm menülere ve ekranlara giriş, fonksiyonların kullanımı, şifre yetki seviyeleri ile kontrol edilecektir. Güvenlik müdürü, güvenlik operatörünün belirli ekranlara ve fonksiyonlara erişimini sınırlandırabilecektir. En az 15 operatör tanımlanabilecektir. Operatörler, mouse aracılığıyla menü ve ikon seçimi yapabilecektir ve minimum eğitim ile sistem fonksiyonlarını kolayca kullanabileceklerdir. Komut hatırlamaya ihtiyaç olmayacaktır. Operatörler tarafından sistemde yapılan değişiklikler ve değişikliklerin yapıldığı tarihler kayıt edilecektir.

Alarm ekranları renkli olacaktır. Sistem, farklı alarm seviyelerine farklı renkler atayabilecektir. Sistem, alarm noktalarını gösteren renkli grafik haritalarına sahip olacaktır ve sistemdeki olaylar gerçek zamanda izlenebilecektir.

Sistemi yönetmek için, tüm sistem yönetim fonksiyonlarının global kontrolü, güvenlik kontrol merkezindeki güvenlik yönetim sistemi bilgisayarından yapılabilecektir. Yönetim, aşağıdaki fonksiyonları içerecektir:

- Sistem operatörleri eklemek ve çıkarmak
- Veritabanı yedeklerini almak
- Program güvenlik seviyeleri tanımlamak
- Uzak cihazlara bilgi transferi yapabilmek

Güvenlik yönetim sisteminde aşağıdaki tanımlamaları yapmak mümkün olacaktır:

- Kart sahibi bilgisi
- Zaman periyotları
- Geçiş bölgeleri
- Geçiş hakları

Kart sahipleri, sistemde geçiş hakları olan kullanıcılardır. Bir kart sahibine birden fazla yetki seviyesi verilebilmeli ve sisteme kart sahibi bilgileri girilebilmelidir. Bu bilgiler şunlar olacaktır: Kart numarası, personel numarası, adı soyadı, çalıştığı bölüm, kart son kullanım tarihi, adres, telefon numarası.

Sistemdeki kullanıcılar iki gruba ait olacaktır:

- Sürekli kart sahipleri : bina personeli, geniş yetkili kart sahipleri
- Geçici kart sahipleri : ziyaretçiler

Kart okuyucuya sahip kapı veya turnikelerdeki geçiş olayları kayıt edilecektir. Kayıt edilen bilgi; geçiş yapılan kapı veya turnikenin ismini, geçiş yapan kart numarasını, kart sahibinin ismini ve geçiş zamanını içerecektir.

Sistem, kart sahibinin kartını kaybettiğini veya çaldırdığını bildirmesi durumunda yeniden kullanılmasını engellemek için bu kartı geçersiz hale getirebilecektir.

Kartlı geçiş sistemi, güvenlik yönetim sisteminin içinde yer alacaktır. Sistem, saha kontrol ünitelerinin eklenmesi sonucu en az %50 genişletilebilir şekilde modüler yapıya sahip olacaktır.

Güvenlik yönetim sisteminin server bilgisayarını, saha kontrol ünitesinde meydana gelen tüm olayları kayıt edecektir. Başarılı geçişler, sistem tarafından yalnızca olay olarak kayıt edilecektir. Diğer tüm olaylar bir alarm sebeptir ve alarm olarak kayıt edilecektir. Bu olaylar güvenlik merkezindeki ve güvenlik müdürünün odasındaki operatör bilgisayarlar tarafından gözlenebilecektir.

Güvenlik yönetim sistemi ve saha kontrol üniteleri arasında meydana gelecek haberleşme kayıpları sistemde alarm yaratacaktır. Her kartlı geçiş ve alarm cihazı bir saha kontrol ünitesine bağlı olacaktır. Ünitenin hafızası en az 2000 yetkili kullanıcıyı içerebilecek kapasitede olmalıdır. Her bir üniteye en az 2 kart okuyucu bağlanabilmelidir. Her ünite, kendi içerisinde tarihi de takip eden bir dahili saat içerecek ve enerji kesintisi durumunda en az 30 dakika çalışmasına imkan tanıyacak bataryalara sahip olacaktır. Üniteler, kilitlenebilir metal muhafazaları içinde kurulacaktır.

Kart okuyucular; mimari dizayna uyumlu bir yapıya sahip olmalıdır. (küçük boyutlar, renk uyumu, vb.) Okuma mesafesi 5 ile 10 cm arasında olacaktır. Her okuyucu yeşil ve kırmızı ışık yayabilen bir LED içerecektir. Bir geçiş onaylandığı zaman LED yeşil yanacaktır. Kırmızı ışık sürekli yanacaktır ve okuyucunun çalıştığını gösterecektir.

Sürekli kart sahiplerinin bilgileri, kartların üzerinde yer alacaktır. Kart, boyuna asılabilmesi için bir zincire yada elbiseye tutturulabilmesi için bir klipse sahip olacaktır.

Ziyaretçi kartlarında “ZİYARETÇİ” yazısı bulunacaktır. Bu kart diğer kartlardan farklı bir renge sahip olacaktır.

Sistemden aşağıdaki raporlar alınabilecektir :

- Kartlı geçiş raporu: Bu raporla, seçilecek zaman aralığı içinde yapılan geçişlerin listesi alınacaktır.
- Alarm raporu : Bu raporla, seçilecek zaman aralığı içinde meydana gelen alarm olaylarının listesi alınacaktır.
- Kart raporu : Bu raporla, çeşitli kriterler kullanılarak kartların içerdiği bilgiler listelenecektir. (Kart sahibinin ismi, çalıştığı bölüm, yetki seviyesi, vb.)
- Olay raporu : Bu raporla, seçilecek zaman aralığı içinde meydana gelen olayların listesi alınacaktır.
- Ziyaretçi raporu : Bu raporla ziyaretçi kartlarının seçilecek zaman aralığı içinde yaptıkları geçişlerin listesi alınacaktır.
- Bölge raporu : Bu raporla, binanın seçilecek bölgesinde o anda mevcut olan personel listelenecektir.

Sistem, server bilgisayardaki olay dosyalarının dolması durumunda bir kasete yedek alınmasını sağlayacaktır. Sistem, disk hafızası maksimum kapasiteye ulaştığında otomatik olarak bir uyarı mesajı verecektir.

Daha önce tanımlanan bir alarm olayı gerçekleştiğinde güvenlik yönetim merkezindeki operatör bilgisayarında sesli bir uyarı meydana gelecektir. Bu sesli uyarı bir komutla susturulabilecektir, fakat bu alarm sistemden silinip resetlenemeyecektir. Sistem, alarm durumu normale dönmeden alarmın silinmesine izin vermeyecektir.

Güvenlik yönetim sistemi, bir seri haberleşme portu aracılığıyla CCTV sistemiyle haberleşme yeteneğine sahip olacaktır.

Sistem en az 45 kameralı ve 15 monitörlü bir CCTV sistemini destekleyebilecektir.

Sistemde istenilen kamera görüntüsü istenilen monitöre aktarılabilir. Kamera görüntüleri sistemdeki bilgisayarlar tarafından görüntülenebilir.

3.1.2.2 Alarm sistemi

Alarm sistemi, güvenlik yönetim sistemine entegre edilecektir. Sistemde tanımlı olan panik butonlarına basılması durumunda, güvenlik kontrol sistemindeki ve güvenlik müdürünün odasındaki güvenlik yönetim bilgisayarlarına sesli ve görsel alarm gelecektir.

Sisteme bağlı bir keypad ile zemin katta bulunan banka şubesinin kasa dairesine giriş kontrol altında tutulacaktır. Keypad aracılığıyla duress şifresi girildiğinde kapı açılacak ama aynı anda güvenlik kontrol sistemindeki ve güvenlik müdürünün odasındaki güvenlik yönetim bilgisayarlarına sesli ve görsel alarm gelecektir.

3.1.2.3 CCTV sistemi

CCTV sistemi, güvenlik yönetim sistemine entegre edilecektir. Kartlı geçiş ve alarm sistemlerindeki olaylara cevap olarak, önceden tanımlanmış bir alarm durumunda istenen kamera görüntüsü istenen monitöre atanabilecektir.

CCTV sistemi, monitördeki kamera görüntülerine isim verilebilmesini sağlayacaktır. Kamera isimleri yer, tarih ve saat içerecektir. Bu isimler kayıt yapılmış video kasetlerde de görülecektir.

Tüm video sinyalleri PAL formatında olacaktır ve tüm video ekipmanı PAL uyumlu olacaktır.

Aşağıda CCTV ekipman seçimi için temel özellikler verilmiştir:

Renkli Kameralar:

- CCD 1/3" görüntü formatı
- Yatay çözünürlük : En az 330 TVL
- Hassasiyet : Aydınlatma en az 1,5 lux
- Gürültü oranı : En az 46 db
- Video çıkışı : 1.0 ± 0.1 Vp-p, 75 ohms
- Sabit kapama hızları : PAL B: 1/120 ile 1/4000

Siyah Beyaz Kameralar:

- CCD 1/3" görüntü formatı
- Yatay çözünürlük : En az 500 TVL
- Hassasiyet : Aydınlatma en az 0,2 lux
- Gürültü oranı : En az 54 db
- Video çıkışı : 1.0 ± 0.1 Vp-p, 75 ohms
- Kapama kontrol : PAL B: 1/50 ile 1/10,000

Lensler:

- 1/3" CCD kameralara monte edilecek tüm lensler autoiris olacaktır.
- Lensler, kameraya uygun olacak şekilde C veya CS montaj olacaktır.
- Tavsiye edilen lens odak mesafeleri Çizelge 3.3'te belirtilmiştir.

Kamera Koruma Kutusu:

- 1/3" CCD kameranın montajı için uygun koruma kutusu kullanılacaktır.
- Koruma kutusu ısıtıcıya sahip olacaktır.

Video Multiplexer:

- 9 kamera girişi
- Minimum 1 video çıkışı ve 1 monitör çıkışı
- Multiplexer'dan video kasete kodlama formatı
- Kodlama formatıyla uyumlu çözücü, istenilen kameranın görüntülerini kayıtlardan çözerek gösterecek.
- Tüm girişler multiplexer tarafından izlenecek, bir sesli ve görsel video sinyali kaybı alarmı mevcut olacak.

Renkli Monitörler (17" ve 15"):

- Yatay çözünürlük : en az 500 lines

Video Kayıt Edici:

- Yüksek çözünürlüklü zaman atlamalı kayıt edici
- Renkli ve siyah/beyaz kayıta en az 400 TVL çözünürlük
- En az 24 saatlik zaman atlamalı kayıt
- Alarm girişi
- Arıza alarm çıkışı

3.1.2.4 Güvenlik kontrol merkezi

Güvenlik kontrol merkezi, güvenlik sistemlerinin verimli çalışmasına imkan verecek şekilde dizayn edilecektir.

Merkezdeki aydınlatma, CCTV monitörlerindeki parlaklıklar ve kamaşmalar nedeniyle operatörlerde oluşacak göz ağrılarını azaltacak şekilde yapılmalıdır. Tercihen dolaylı floresan aydınlatma kullanılmalıdır.

Güvenlik kontrol merkezinde bir kontrol konsolu kurulacaktır. Güvenlik yönetim sisteminin monitörü ve CCTV monitörleri konsolda yer alacaktır. Konsol boyutları, oda boyutları ile uyumlu olmalıdır. Konsol, paslanmaz çelik veya alüminyum modüllerden oluşacaktır.

Ekipman kabinleri, konsol ile aynı yapıda olacaktır. Sürekli kullanılmayan ekipmanlar bu kabinlere monte edilecektir. (multiplexer, video kayıt edici, kontrolörler, vb.)

Konsola ve kurulu ekipmanlara gerekli enerji, güvenlik kontrol merkezinde kurulmuş olan kesintisiz güç kaynağından sağlanacaktır.

Güvenlik müdürünün ofisinde aşağıdaki ekipman kullanılacaktır:

- 15” renkli monitör
- Gerekli yazılım ve donanım ile kurulu olan operatör bilgisayar

Güvenlik müdürü, operatör bilgisayarı ve CCTV monitörünü kullanarak tüm kameraların görüntülerini izleyebilecektir.

3.1.2.5 Güvenlik resepsiyon bölgeleri

Resepsiyon bölgeleri, binanın 1. bodrum katında otoparktan binaya girişte ve zemin katta yer alacaktır.

Ziyaretçiler için operatör bilgisayar kurulacaktır. Bu bilgisayar, güvenlik merkezindeki merkez bilgisayar ile bir network aracılığıyla haberleşecektir. Bu bilgisayar ile sadece ziyaretçi kontrolü işlemleri yapılacaktır. Ziyaretçilerin detaylı bilgileri güvenlik yönetim sisteminin veritabanına girilecektir. Ziyaretçiye bir kart verilecek ve bu kartın içereceği gerekli yetki seviyesi ve kart geçerlilik süresi operatör bilgisayar aracılığıyla sisteme girilecektir.

3.1.2.6 Fiziksel güvenlik araçları

3 kollu tip turnikeler, binanın zemin kattaki girişine monte edilecektir. Turnikelerin giriş ve çıkış yanlarında geçiş göstergeleri olacaktır. Turnike, geçiş için bir defada bir insana izin verecektir. Yetkili kartın giriş tarafındaki kart okuyucuya gösterilmesi durumunda, turnike kolları giriş yönünde serbest kalacaktır. Yetkili kartın çıkış tarafındaki kart okuyucuya gösterilmesi durumunda, turnike kolları çıkış yönünde serbest kalacaktır. Enerji kesintisi durumunda, turnikeler her iki yönde de serbest kalacak ve kollarını düşürecektir.

Kartlı geçiş sistemi tarafından kontrol edilen kapılar, Çizelge 3.1’de belirtilmiştir. Kapının durumunu kontrol etmek için bir elektrikli kilit monte edilecektir. Kilit, enerji kesintisi durumunda açılacaktır. Ek olarak bir mekanik kilit, bir sistem arızası durumunda kapının elle kilitlenebilmesi için monte edilecektir. Kapıya mekanik bir kapı kapayıcı eklenecek ve kapının açık kalması engellenecektir.

3.2 Gerekli Ekipman ve Yazılımlar

3.2.1 Güvenlik yönetim sistemi

Güvenlik yönetim sistemi için kullanılacak ekipman ve yazılımlar şunlardır:

a) Server bilgisayar donanımı:

- 17” monitör
- Pentium III 500 Mhz mikroişlemci
- 128 MB RAM
- 10 GB SCSI Harddisk
- Network kartı
- Grafik kartı
- Multiport

b) Server bilgisayar yazılımı:

- Microsoft Windows NT 4.0 Workstation işletim sistemi
- Excel Security Manager 630.2 server yazılımı
- MicroLPM arabirimi
- Intelliguard 9000 arabirimi
- CCTV arabirimi
- Bölge raporu
- 4 operatör bilgisayar kapasitesi

c) Operatör bilgisayar donanımı:

- 15” monitör
- Pentium II 400 Mhz mikroişlemci
- 64 MB RAM
- 4 GB SCSI Harddisk
- Network kartı
- Grafik kartı

d) Operatör bilgisayar yazılımı:

- Microsoft Windows NT 4.0 Workstation işletim sistemi
- Excel Security Manager 630.2 station yazılımı

e) A4 Laser yazıcı

f) 1 adet RS232/485 dönüştürücü

3.2.2 Kartlı geiş sistemi

Kartlı geiş sistemi iin kullanılacak ekipmanlar řunlardır:

- a) 2 adet MicroLPM saha kontrol ünitesi
 - 12 adet okuyucu baėlantısı
 - 2000 kart hafızası
 - 12 V 6.5 Ah akü
- b) 2 adet 3 kollu tip paslanmaz elik turnike
- c) 24 adet 10 cm okuma mesafesine sahip kart okuyucu
- d) 2000 adet proximity kart

3.2.3 Alarm sistemi

Alarm sistemi iin kullanılacak ekipmanlar řunlardır:

- a) 1 adet Intelliguard 9000 saha kontrol ünitesi ve RS-232 haberleşme arabirimi
- b) 2 adet 6 girişli saha adres modülü
- c) 2 adet saha güç kaynaėı
- d) 1 adet keypad
- e) 3 adet panik butonu

3.2.4 CCTV sistemi

CCTV sistemi iin kullanılacak ekipmanlar řunlardır:

- a) 8 adet 1/3" CCD renkli kamera
 - 330 TVL yatay özünürlük
 - 1,5 lx hassasiyet
- b) 1 adet 1/3" CCD siyah/beyaz kamera
 - 570 TVL yatay özünürlük
 - 0,08 lx hassasiyet
- c) 2 adet 500 TVL yatay özünürlüėe sahip 17" renkli monitör
- d) 1 adet 500 TVL yatay özünürlüėe sahip 15" renkli monitör

e) 1 adet video multiplexer

- 9 kamera girişi
- 1 video çıkışı, 2 monitör çıkışı

f) 1 adet 24 saat zaman atlamalı video kayıt edici

g) 8 adet CS montaj, 4 mm 1/3" CCD auto iris lens

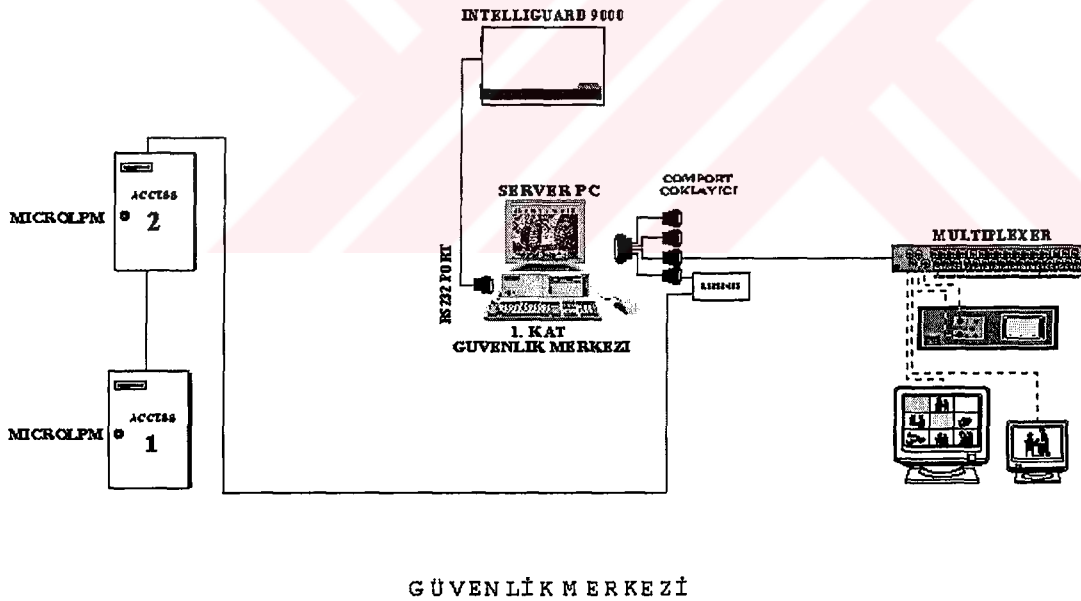
h) 1 adet CS montaj, 8 mm 1/3" CCD auto iris lens

ı) 1 adet ısıtıcı koruma kutusu

3.3 Sistem Ekipmanlarının Yerleşim ve Bağlantı Diyagramları

Saha kontrol ünitelerinin, güvenlik yönetim sistemiyle olan bağlantıları Şekil 3.1'de görülmektedir.

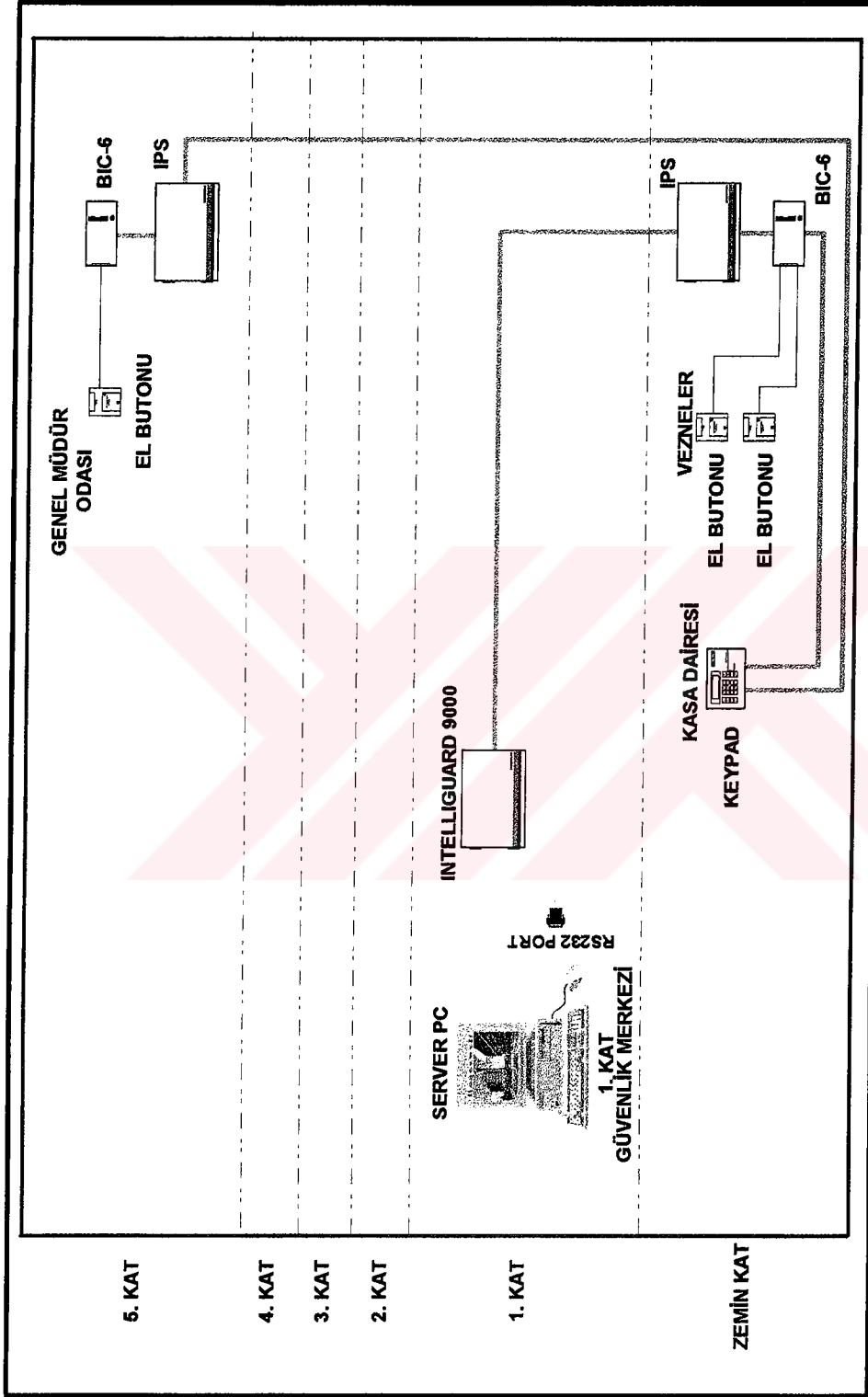
2 adet MicroLPM kartlı geçiş paneli; bir haberleşme kanalı kullanılarak güvenlik yönetim sistemi server bilgisayarına seri port üzerinden bağlanmaktadır.



Şekil 3.1 Güvenlik yönetim sistemi ile saha kontrol üniteleri arasındaki bağlantı diyagramı.

İkinci haberleşme kanalı aracılığıyla CCTV multiplexer ünitesi, multiport kartı kullanılarak çoklanmış seri portlardan biri üzerinden server bilgisayara bağlanmaktadır.

Üçüncü haberleşme kanalı aracılığıyla da, Intelliguard alarm panelinin server bilgisayar üzerindeki seri porttan haberleşmesi sağlanmaktadır.



Şekil 3.2 Alarm sistemi ekipman yerleşimi.

Alarm sistemine ait saha kontrol ünitesinin ve saha ekipmanlarının yerleşim ve bağlantıları Şekil 3.2’de görülmektedir.

Güvenlik yönetim merkezindeki Intelliguard 9000 saha kontrol ünitesi; 5. kattaki IPS güç kaynağı ve BIC saha adres modülüyle, zemin kattaki IPS güç kaynağı ve BIC saha adres modülüyle ve kasa dairesi girişindeki keypad ile haberleşme sağlamaktadır.

Intelliguard 9000 saha kontrol ünitesi ile güvenlik yönetim sistemi arasındaki haberleşme, server bilgisayar üzerindeki seri port aracılığıyla sağlanmaktadır.

IPS güç kaynakları, bağlı oldukları BIC adres modüllerine gerekli enerjiyi vermektedir. BIC adres modülleri aracılığıyla da 5. kattaki genel müdür odasındaki panik butonundan, zemin kat banka şubesindeki veznelerde bulunan panik butonlarından gelen bilgi izlenmekte ve saha kontrol ünitesine ulaştırılmaktadır.

Keypad ile banka kasa dairesine giriş-çıkış için kullanılan kapı kontrol edilmektedir. Alarm şifresi girildiğinde kasa dairesinin kapısı açılacak fakat saha kontrol ünitesine gizli alarm bilgisi ulaşacaktır.

CCTV sistemine ait kontrolör ve saha ekipmanlarının yerleşim ve bağlantıları Şekil 3.3’te görülmektedir.

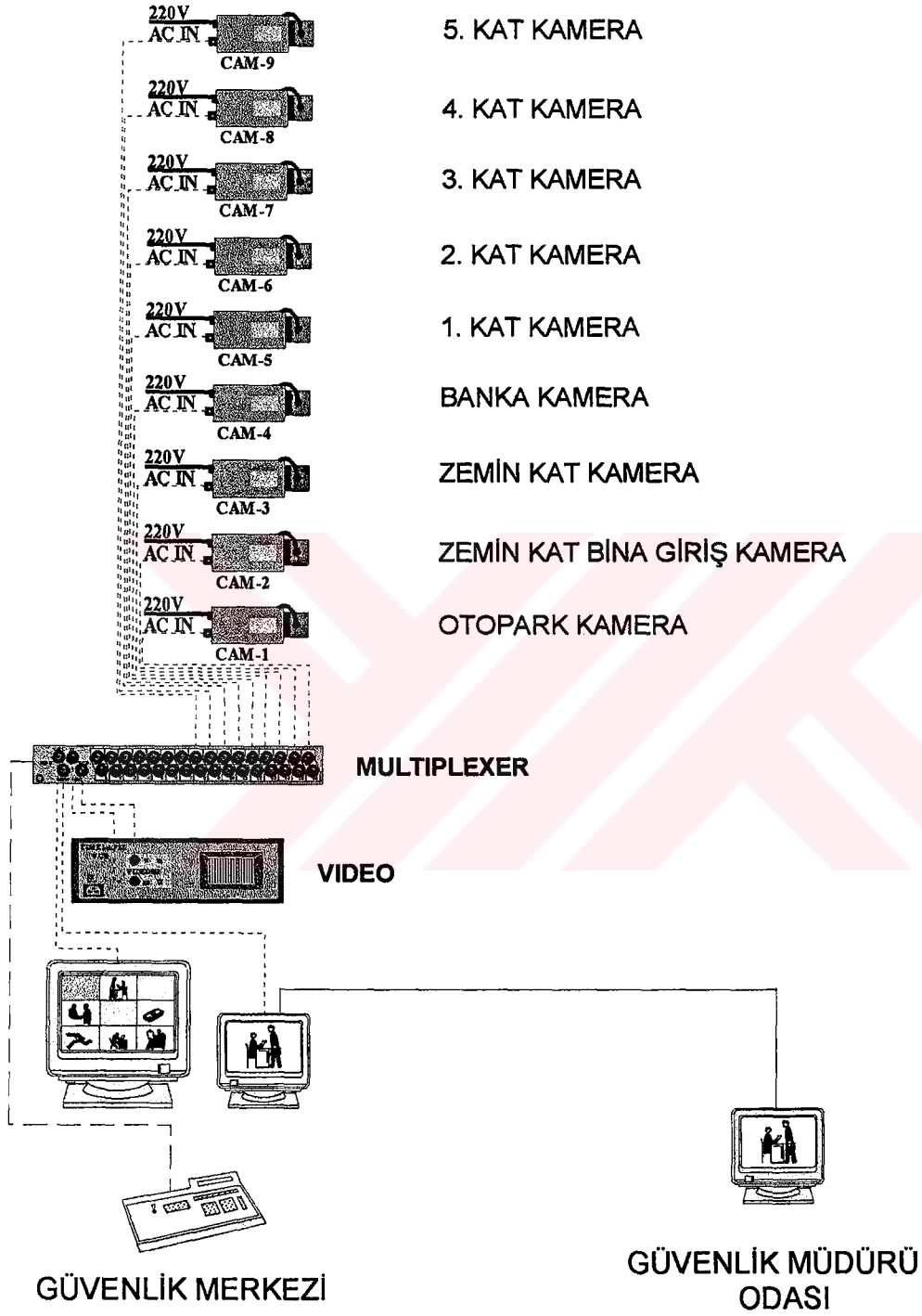
Güvenlik yönetim merkezinde bulunan multiplexer ünitesine bir zaman atlamalı video kayıt edici, 2 adet monitör ve 9 adet kamera bağlanmaktadır.

Ana monitör aracılığıyla, multiplexer tarafından çoklanmış görüntü yani 9 kameranın görüntüleri aynı anda gözlenmektedir. Spot monitör aracılığıyla, seçilen bir kameranın görüntüsü tam ekran izlenmektedir. Güvenlik müdürünün odasında bulunan monitör yardımıyla, güvenlik müdürü kameraların görüntülerini takip edebilmektedir.

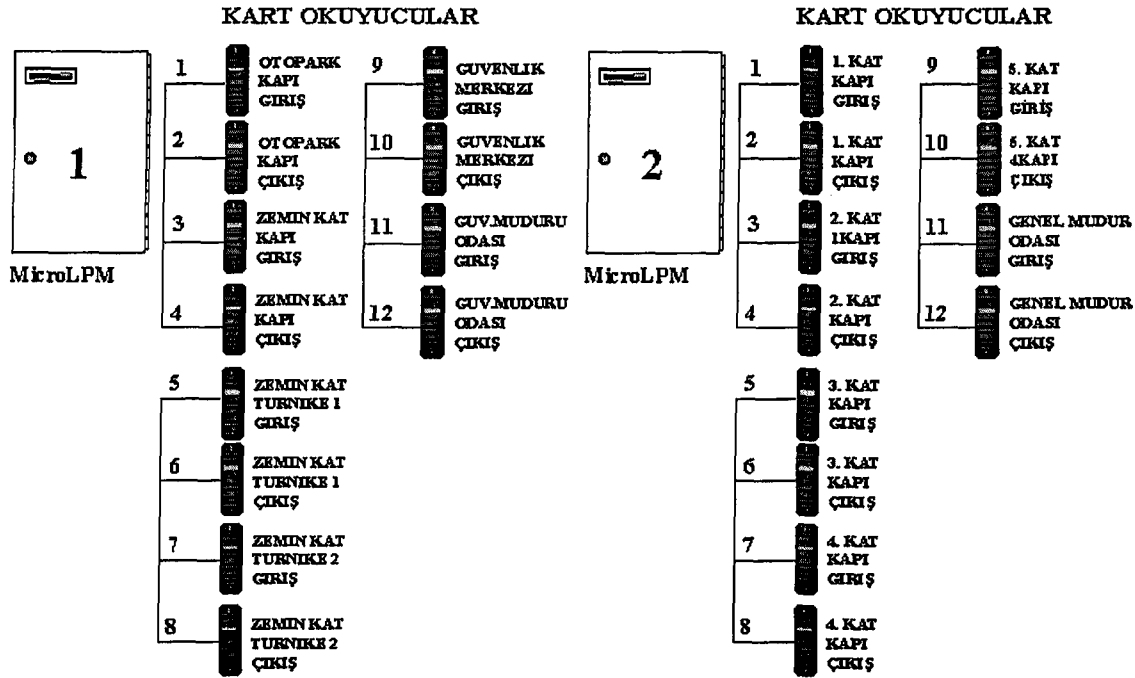
Kartlı geçiş sistemine ait saha kontrol ünitelerinin ve kart okuyucuların fonksiyonlarının yer aldığı diyagram Şekil 3.4’te görülmektedir.

1 numaralı MicroLPM saha kontrol ünitesi; zemin kata, otopark katına ve güvenlik merkezine ait olan 12 adet kart okuyucuyu, 2 numaralı MicroLPM saha kontrol ünitesi ise; 1.kat ile 5. kat arasında bulunan 12 adet kart okuyucuyu içermektedir.

İki saha kontrol ünitesi de tek bir haberleşme kanalı kullanarak güvenlik yönetim sistemine bağlanmaktadır. Server bilgisayarla haberleşme, multiport kartıyla çoklanmış seri portlardan birine bağlı bulunan RS232/485 konverter aracılığıyla sağlanmaktadır.



Şekil 3.3 CCTV sistemi ekipman yerleşimi.



Şekil 3.4 Kartlı geçiş sistemi kart okuyucu dağılımı.

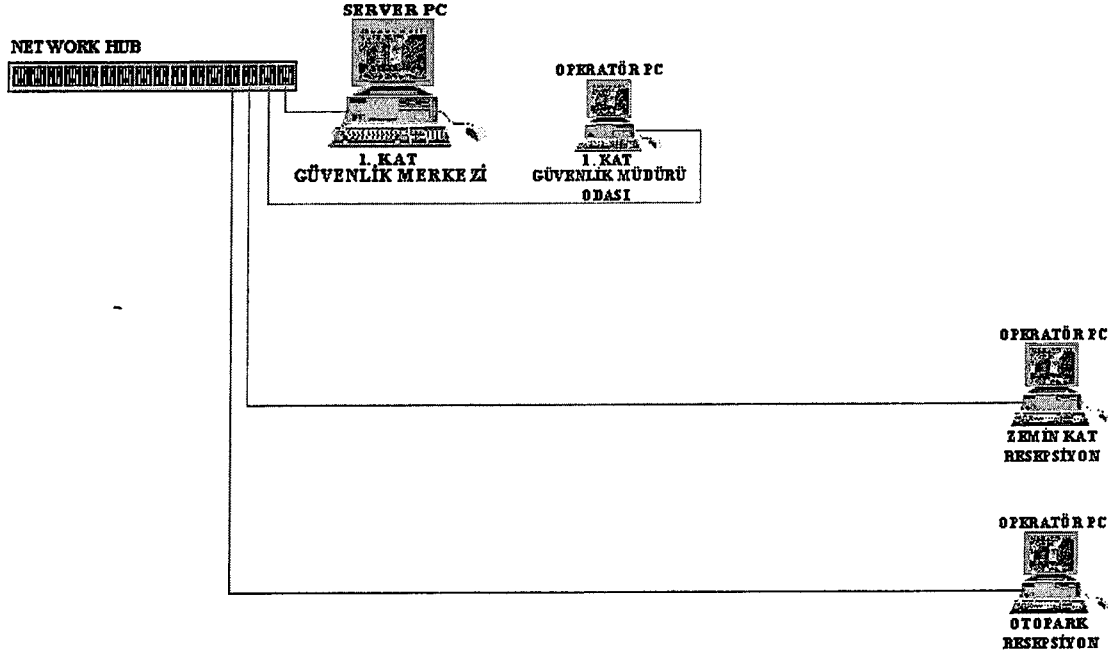
Kart okuyuculardan birine kart okutulması durumunda bilgi; önce saha kontrol ünitesine, ardından da güvenlik yönetim sistemine ulaşmaktadır.

Güvenlik yönetim sisteminde yer alan server ve operatör bilgisayarların yerleşimi ve bağlantıları Şekil 3.5’de görülmektedir.

Server bilgisayar, güvenlik müdürünün odasındaki operatör bilgisayar, zemin kat resepsiyondaki operatör bilgisayar ve otopark bina girişindeki operatör bilgisayar arasındaki LAN (Local Area Network) bağlantıları; bir hub yardımıyla sağlanmakta ve haberleşme protokolü olarak TCP/IP kullanılmaktadır.

Güvenlik müdürü; odasındaki operatör bilgisayar yardımıyla sistemdeki her türlü olay ve alarmı izleyebilmekte ve gerektiğinde sisteme müdahale edebilmektedir.

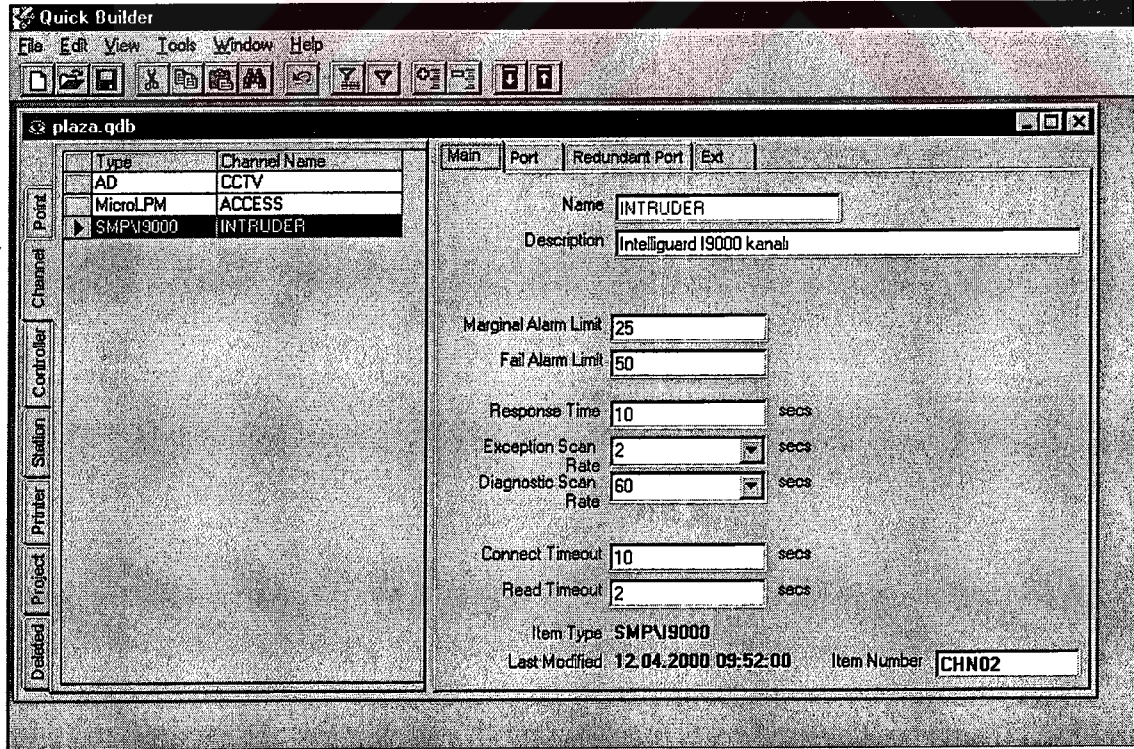
Resepsiyonlarda bulunan operatör bilgisayarlar yardımıyla, binaya giriş-çıkış yapan ziyaretçiler kontrol edilecektir. Gelen ziyaretçilere ziyaretçi kartları verilecek ve bu kartlara gerekli geçiş hakları atanabilecektir. Ziyaretçiler binadan çıkış yaparken kartlar geri alınacak ve geçiş hakları iptal edilecektir.



Şekil 3.5 Güvenlik yönetim sistemi server ve operatör bilgisayarları.

3.4 Sistem Konfigürasyonu

3.4.1 Haberleşme kanalları



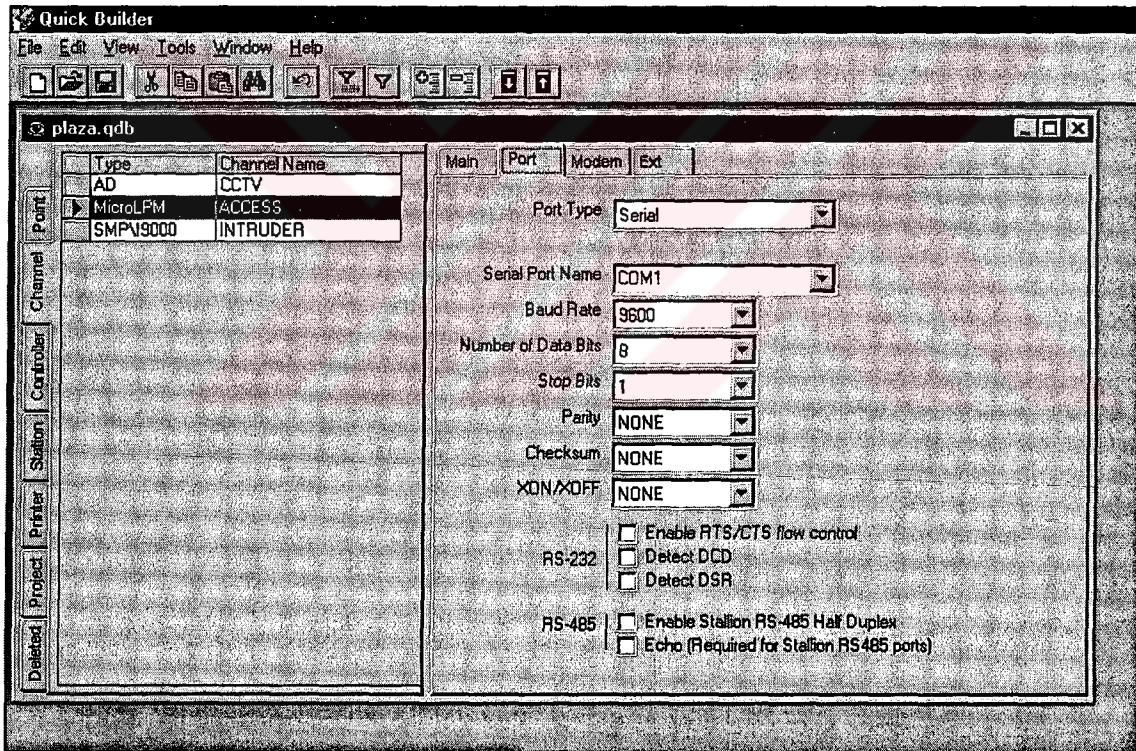
Şekil 3.6 Haberleşme kanalının konfigürasyonu.

Sistemle haberleşecek olan Intelliguard9000 alarm sisteminin kanal konfigürasyonu Şekil 3.6’da görülmektedir.

Haberleşme kanalını sistemde temsil edecek isim, “Name” bölümünde belirtilmektedir. Haberleşme kanalı hakkındaki açıklamalar “Description” bölümünde yer almaktadır.

Kanalda oluşacak haberleşme hataları sonucunda artan hata değeri, “Marginal Alarm Limit” bölümündeki değeri aştığında sistem alarm vererek operatörleri uyarmaktadır. Haberleşmenin düzelmemesi veya kesilmesi durumunda hata değeri “Fail Alarm Limit” bölümündeki değeri de aşacak ve sistem birinci derecede acil alarm verecektir.

Server bilgisayarın, bu kanaldan haberleşmeyi sağlaması gereken süre “Connect Timeout” bölümündeki değerle saptanmaktadır. Server bilgisayarın, bu kanala bağlı kontrolörlerden cevap alması gereken minimum süre “Read Timeout” bölümündeki değerle saptanmaktadır.



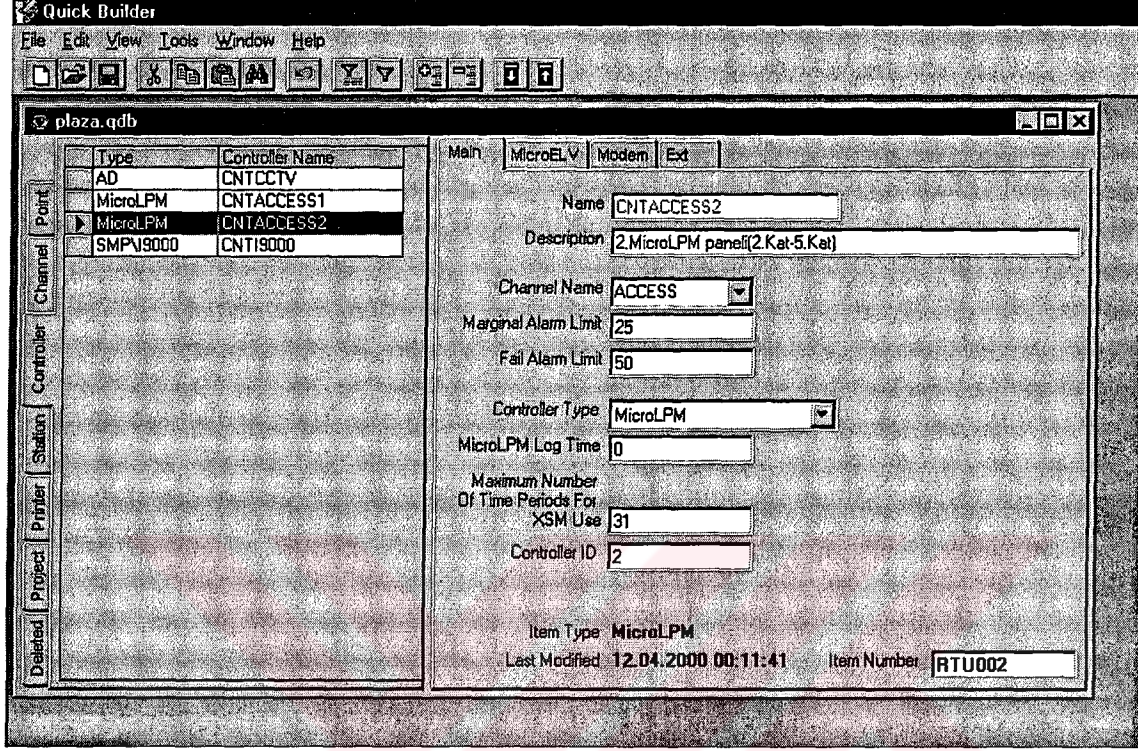
Şekil 3.7 Haberleşme kanalının port konfigürasyonu.

Sistemle haberleşecek olan MicroLPM kartlı geçiş sisteminin kanal port konfigürasyonu Şekil 3.7’de görülmektedir.

Bu kanaldan haberleşme sağlanması için kullanılacak portun tipi “Port Type” bölümünde ve kullanılacak portun numarası da “Serial Port Name” bölümünde yer almaktadır.

Seçilen port tipine ait “Baud Rate” ve diğer port özellikleri de Şekil 3.7’deki port konfigürasyonu ekranında görülmektedir.

3.4.2 Kontrolörler



Şekil 3.8 Kontrolör konfigürasyonu.

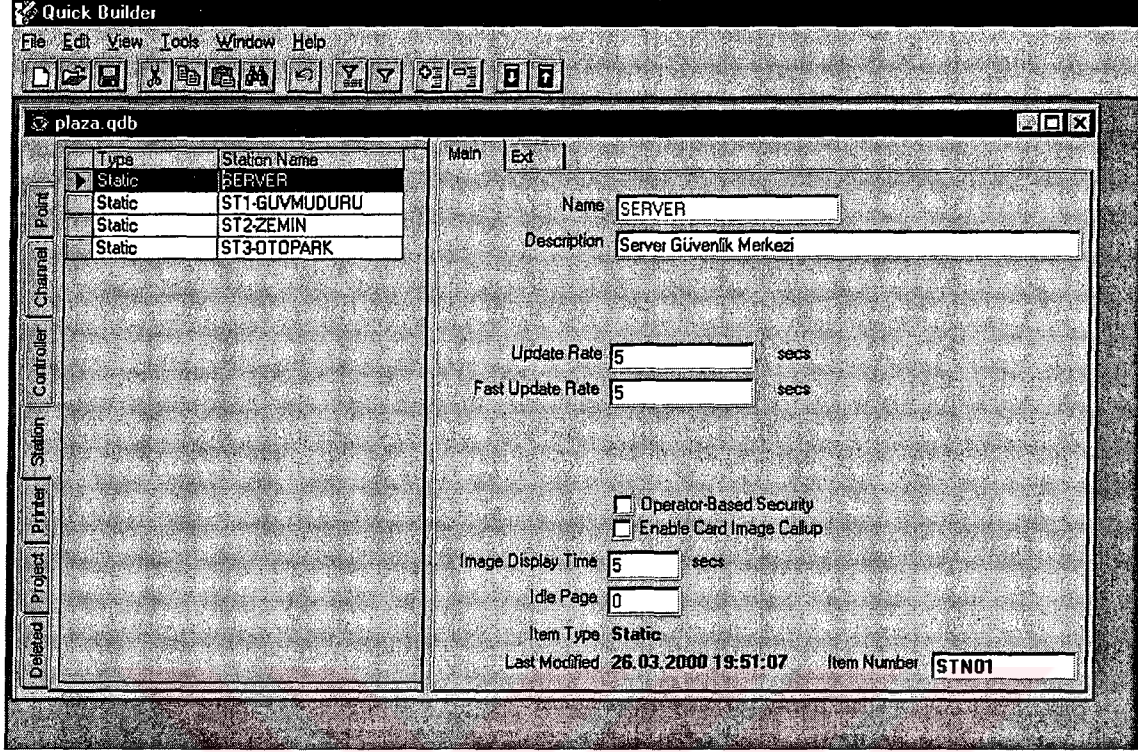
Sistemle haberleşecek olan MicroLPM kartlı geçiş sisteminin saha kontrol ünitesinin konfigürasyonu Şekil 3.8’de görülmektedir.

Saha kontrol ünitesini sistemde temsil edecek isim, “Name” bölümünde belirtilmektedir. Saha kontrol ünitesi hakkındaki açıklamalar “Description” bölümünde yer almaktadır.

Saha kontrol ünitesi ile server bilgisayar arasında oluşacak haberleşme hataları sonucunda artan hata değeri, “Marginal Alarm Limit” bölümündeki değeri aştığında sistem alarm vererek operatörleri uyarmaktadır. Haberleşmenin düzelmemesi veya kesilmesi durumunda hata değeri “Fail Alarm Limit” bölümündeki değeri de aşacak ve sistem birinci derecede acil alarm verecektir.

Kullanılan saha kontrol cihazının tipi “Controller Type” bölümünde görülmektedir. Aynı haberleşme kanalından haberleşen kontrol ünitelerinin her biri diğerlerinden farklı olarak kendine ait bir numaraya sahip olacaktır. Bu numara “Controller ID” bölümünde görülmektedir.

3.4.3 Operatör bilgisayarlar



Şekil 3.9 Operatör bilgisayar konfigürasyonu.

Server bilgisayarın üzerindeki operatör yazılımının konfigürasyonu Şekil 3.9’da görülmektedir.

Operatör bilgisayarı sistemde temsil edecek isim, “Name” bölümünde belirtilmektedir. Operatör bilgisayar hakkındaki açıklamalar “Description” bölümünde yer almaktadır.

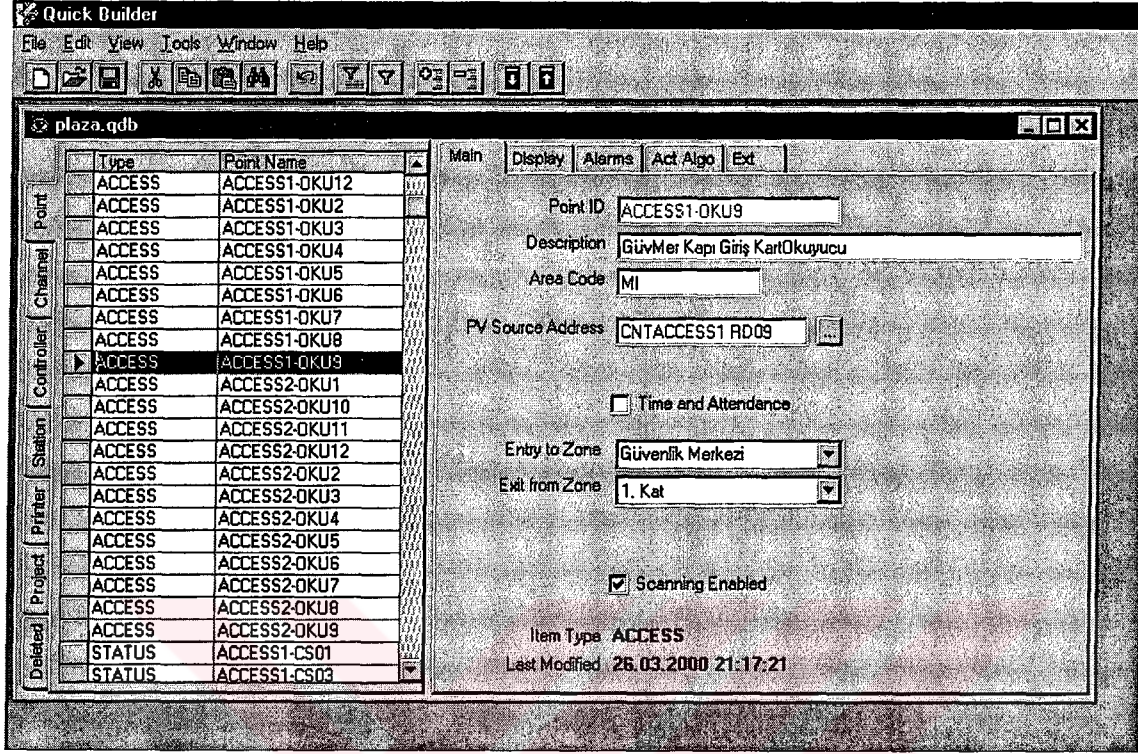
Ekrandaki dinamik değerlerin güncellenme süresi “Update Rate” bölümünde, aktif edilmesi durumunda kullanılabilecek hızlı güncelleme süresi de “Fast Update Rate” bölümünde yer almaktadır.

Operatör tabanlı güvenlik yöntemi seçilmesi durumunda, sistem devreye alındığında operatör bilgisayardaki yazılımı çalıştırmak için operatörün seviyesini gösterecek şifrelerin girilmesi gerekmektedir. Operatör yazılım çalıştırıldığında ilk olarak açılacak ekran “Idle Page” bölümündeki ekran numarasıyla saptanmaktadır.

“Card Image Callup” seçeneğinin aktif olması durumunda operatör bilgisayarlar tarafından kart sahiplerinin resimlerinin görülmesi mümkün olmaktadır. Ekrana gelen bir resmin, minimum ekranda kalma süresi “Image Display Time” bölümünde yer almaktadır.

3.4.4 Nokta tanımlamaları

3.4.4.1 Geçiş noktaları



Şekil 3.10 Geçiş noktası konfigürasyonu.

Kartlı geçiş sistemine ait güvenlik merkezi kapısındaki giriş kart okuyucusuna ait geçiş noktasının konfigürasyonu Şekil 3.10’da görülmektedir.

Geçiş noktasını sistem veritabanında temsil edecek isim, “PointID” bölümünde belirtilmektedir. Geçiş noktası hakkındaki açıklamalar “Description” bölümünde yer almaktadır.

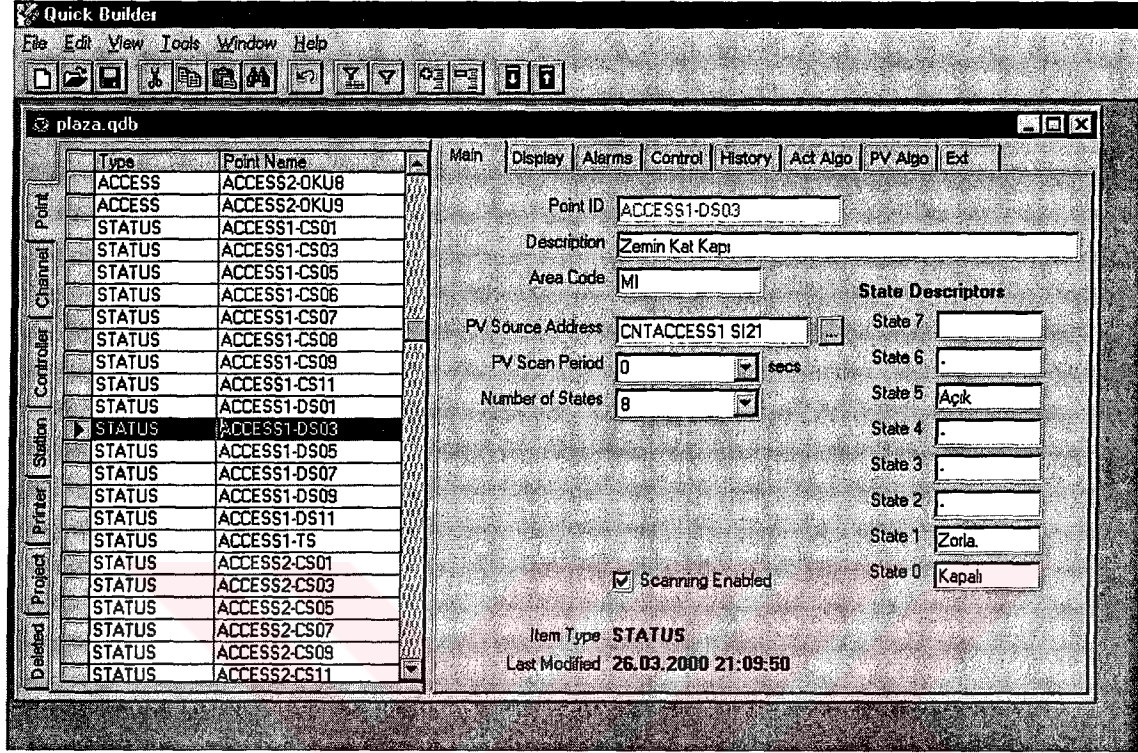
Geçiş noktasının bağlı bulunduğu saha kontrol ünitesi ve noktanın bu kontrolördeki adresi “PV Source Address” bölümünde görülmektedir.

Geçiş noktasından geçildiğinde içine girilen bölge “Entry To Zone” bölümünde, çıkış yapılan bölge “Exit From Zone” bölümünde belirtilmektedir.

3.4.4.2 Kapı durum noktaları

Kartlı geçiş sisteminde bulunan zemin kat kapısına ait durum noktasının konfigürasyonu Şekil 3.11’de görülmektedir.

Kapı durum noktasını sistem veritabanında temsil edecek isim, “PointID” bölümünde belirtilmektedir. Kapı durum noktası hakkındaki açıklamalar “Description” bölümünde yer almaktadır.



Şekil 3.11 Kapı durum noktası konfigürasyonu.

Kapı durum noktasının bağlı bulunduğu saha kontrol ünitesi ve noktanın bu kontrolördeki adresi “PV Source Address” bölümünde görülmektedir.

Kapının durumunu gösteren tanımlamalar “State Descriptors” bölümünde yer almaktadır. (Kapalı, Zorlama var, Açık)

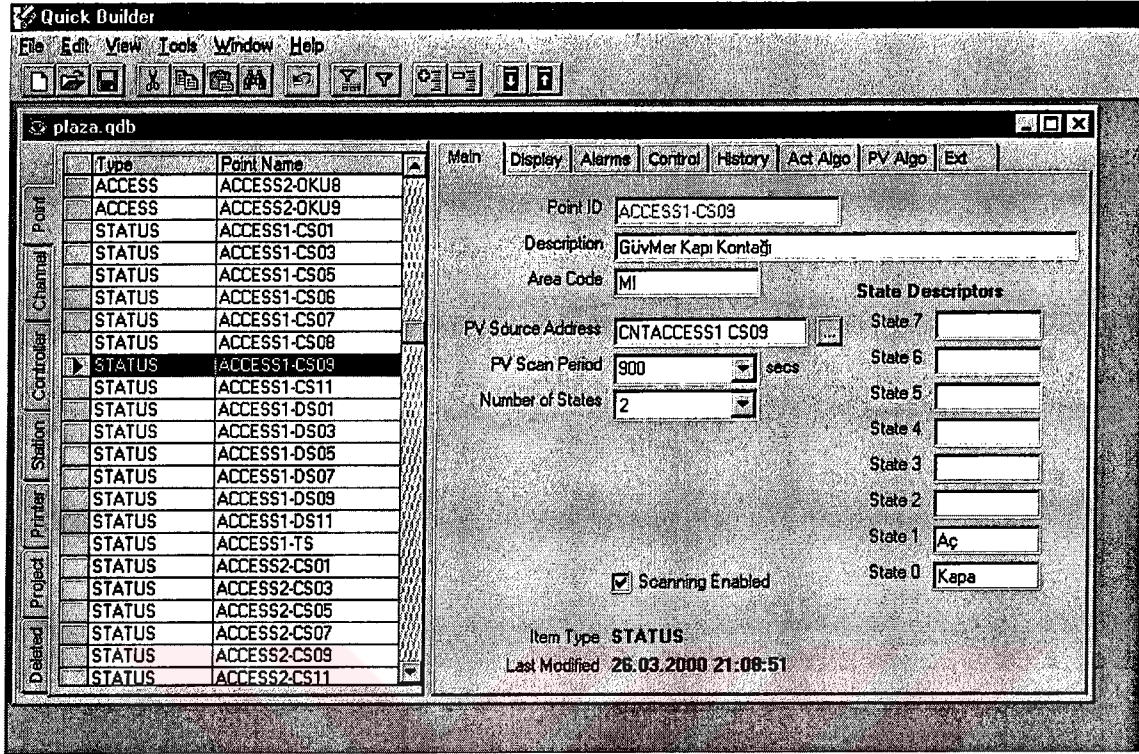
3.4.4.3 Kapı kontak noktaları

Kartlı geçiş sisteminde bulunan güvenlik merkezi kapısına ait kontak noktasının konfigürasyonu Şekil 3.12’de görülmektedir.

Kapı kontak noktasını sistem veritabanında temsil edecek isim, “PointID” bölümünde belirtilmektedir. Kapı kontak noktası hakkındaki açıklamalar “Description” bölümünde yer almaktadır.

Kapı kontak noktasının bağlı bulunduğu saha kontrol ünitesi ve noktanın bu kontrolördeki adresi “PV Source Address” bölümünde görülmektedir.

Kapı kontağını kontrol etmek için kullanılacak komut tanımlamaları “State Descriptors” bölümünde yer almaktadır. (Kapa, Aç)



Şekil 3.12 Kapı kontak noktası konfigürasyonu.

3.4.4.4 Alarm noktaları

Alarm sisteminde bulunan 5.kattaki genel müdür odasındaki butona ait alarm noktasının konfigürasyonu Şekil 3.13'te görülmektedir.

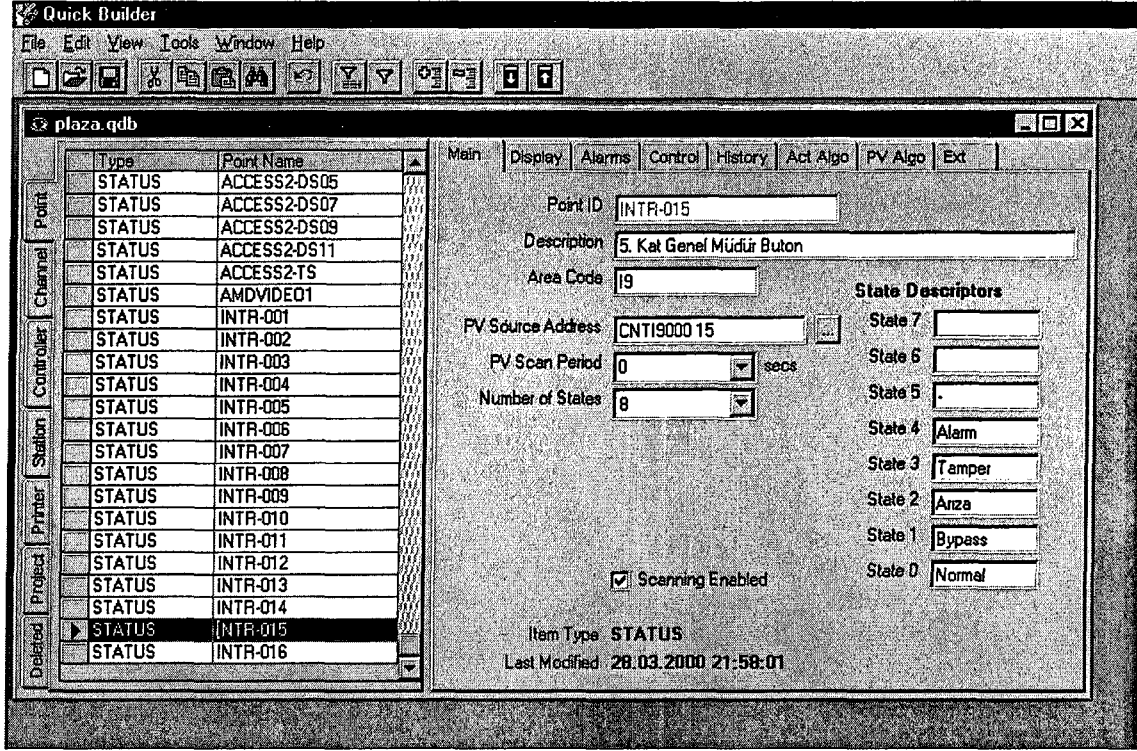
Alarm noktasını sistem veritabanında temsil edecek isim, “PointID” bölümünde belirtilmektedir. Alarm noktası hakkındaki açıklamalar “Description” bölümünde yer almaktadır.

Alarm noktasının bağlı bulunduğu saha kontrol ünitesi ve noktanın bu kontrolördeki adresi “PV Source Address” bölümünde görülmektedir.

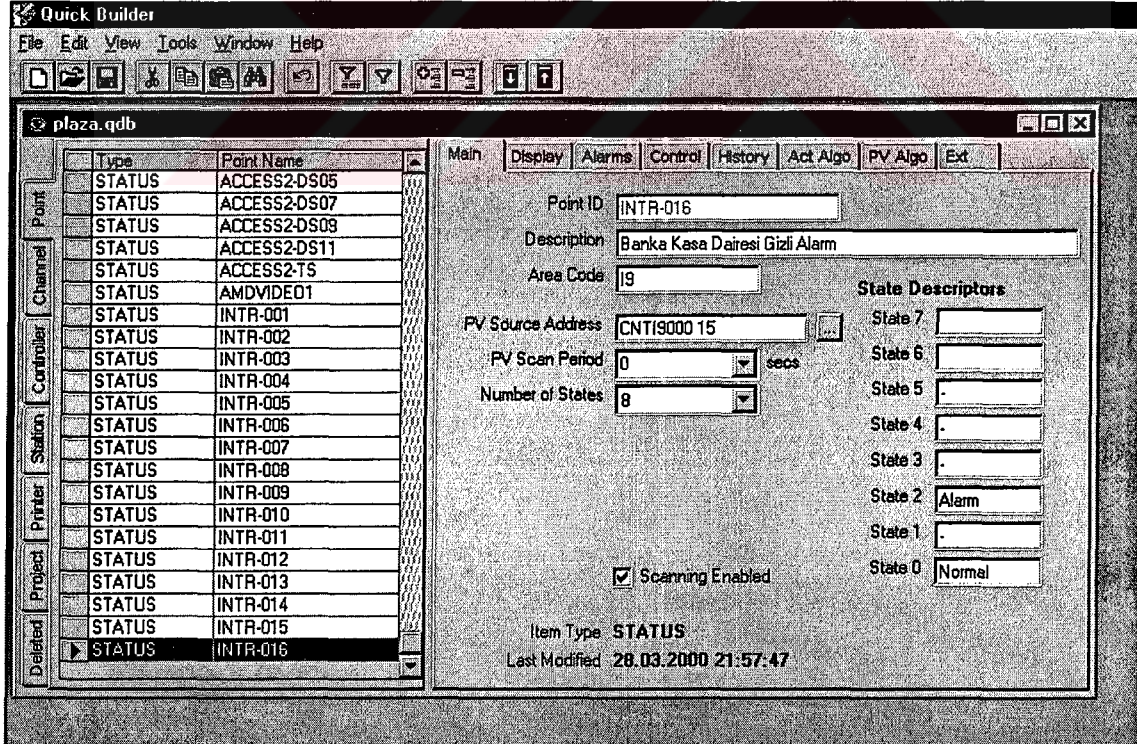
Butonun durumunu gösteren tanımlamalar “State Descriptors” bölümünde yer almaktadır. (Normal, Bypass, Arıza, Tamper, Alarm)

3.4.4.5 Gizli alarm noktası

Alarm sisteminde bulunan banka kasa dairesi girişindeki keypad'e ait gizli alarm noktasının konfigürasyonu Şekil 3.14'te görülmektedir.



Şekil 3.13 Alarm noktası konfigürasyonu.



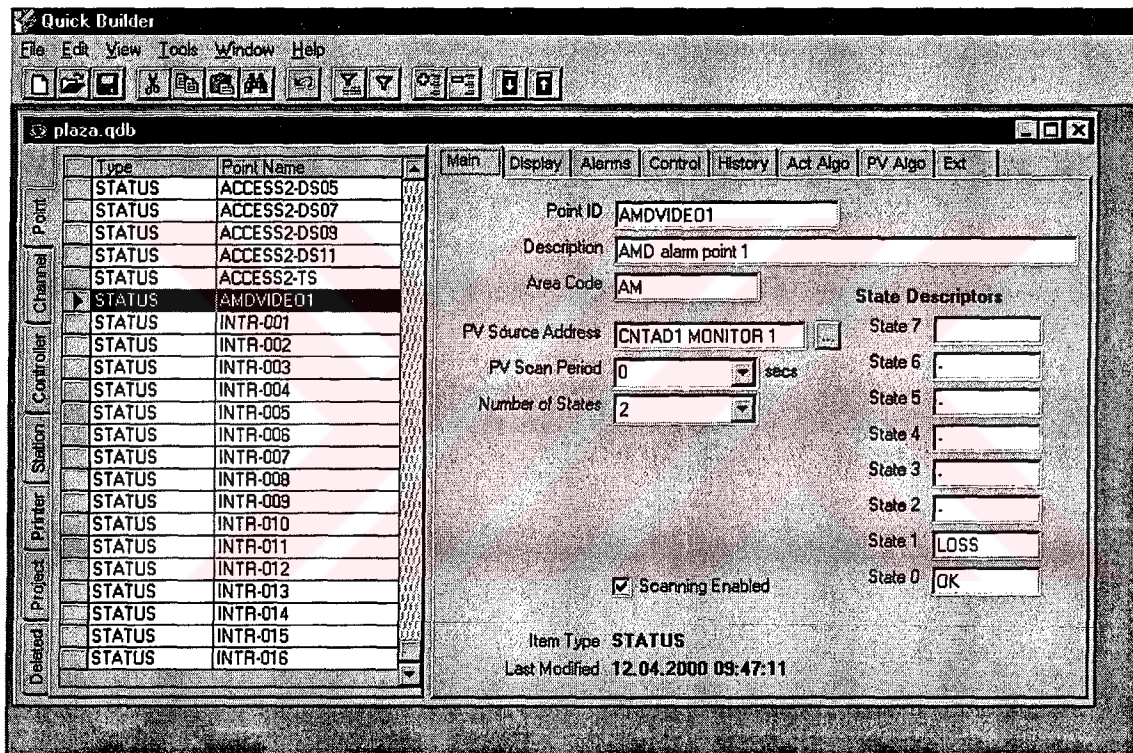
Şekil 3.14 Gizli alarm noktası konfigürasyonu.

Gizli alarm noktasını sistem veritabanında temsil edecek isim, “PointID” bölümünde belirtilmektedir. Gizli alarm noktası hakkındaki açıklamalar “Description” bölümünde yer almaktadır.

Gizli alarm noktasının bağlı bulunduğu saha kontrol ünitesi ve noktanın bu kontrolördeki adresi “PV Source Address” bölümünde görülmektedir.

Keypad’den girilen şifre durumunu gösteren tanımlamalar “State Descriptors” bölümünde yer almaktadır. (Normal, Alarm)

3.4.4.6 Monitör alarm noktası



Şekil 3.15 Monitör alarm noktası konfigürasyonu.

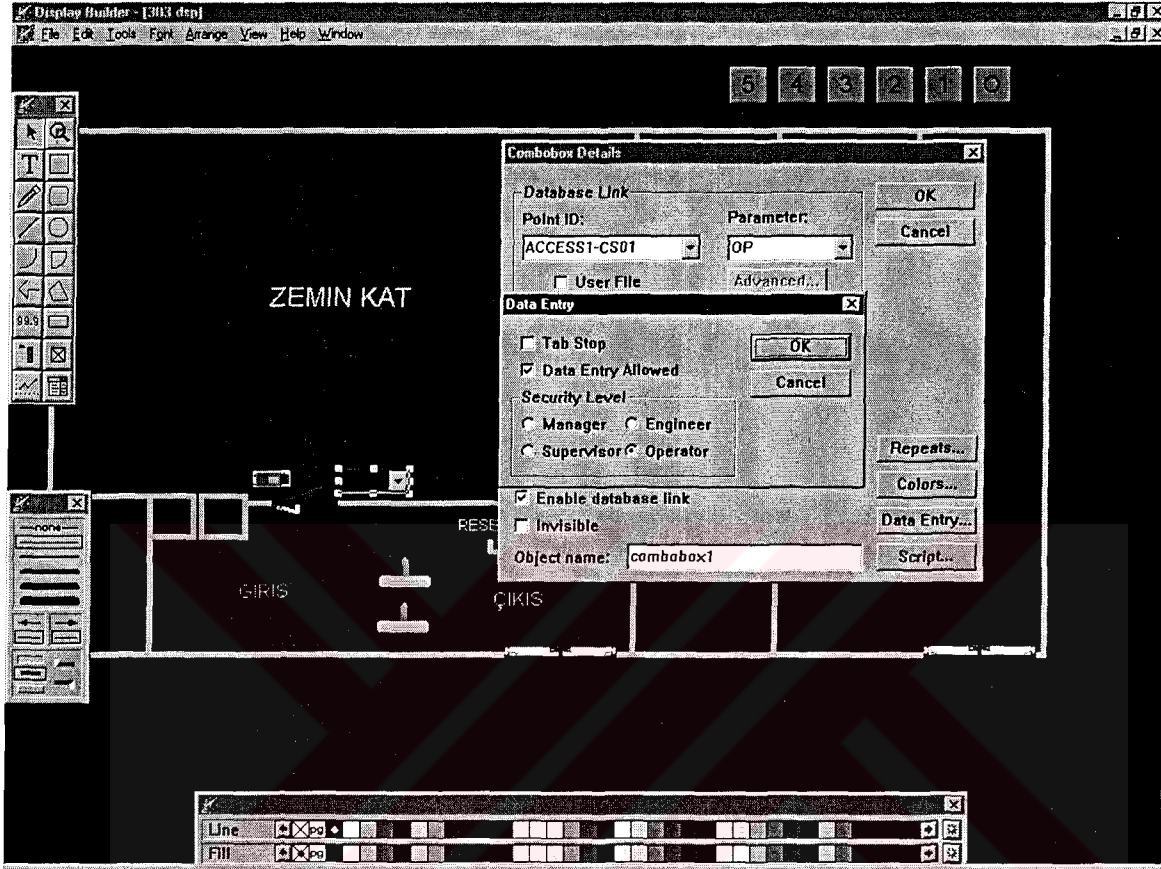
CCTV sisteminde bulunan güvenlik odasındaki ana monitöre ait alarm noktasının konfigürasyonu Şekil 3.15’te görülmektedir.

Monitör alarm noktasını sistem veritabanında temsil edecek isim, “PointID” bölümünde belirtilmektedir. Monitör alarm noktası hakkındaki açıklamalar “Description” bölümünde yer almaktadır.

Monitör alarm noktasının bağlı bulunduğu CCTV seçicisi ve noktanın bu kontrolördeki adresi “PV Source Address” bölümünde görülmektedir.

Monitörün durumunu gösteren tanımlamalar “State Descriptors” bölümünde yer almaktadır. (OK, LOSS)

3.5 Dinamik Ekranların Veritabanı Bağlantısı



Şekil 3.16 Bir kapı kontak noktasının veritabanı bağlantısı.

Grafik yazılımı ile hazırlanan ekranlarda yer alan kapı, turnike, kamera gibi şekillerle; bu şekillerin sistem veritabanında temsil ettikleri noktalar arasında bağlantılar kurulmaktadır.

Şekil 3.16’da; kartlı geçiş sistemine dahil olan zemin kat kapısına aç veya kapa komutu gönderebilecek olan kontak noktasının veritabanı bağlantısı görülmektedir. Kapı kontak noktalarıyla veritabanı bağlantıları yapılmış nesneler kullanılarak kapılara aç veya kapa komutları gönderilebilmektedir.

Grafiklerde veritabanı bağlantısı yapılmış dinamik nesneler, veritabanında temsil ettikleri noktanın durumuna göre ekranda renk ve şekil değiştirmektedirler. Örneğin bir kapı durum noktasından kapalı bilgisi geliyorsa, ekrandaki kapı nesnesi kapalı ve yeşil renkte görülecek veya açık bilgisi geliyorsa, ekrandaki kapı nesnesi açık ve yanıp sönen kırmızı renkte görülecektir.

Ekranlara yerleştirilmiş, sisteme komut gönderebilen her bir nesnenin güvenlik seviyesi bulunmaktadır. Nesneyi kullanarak komut verebilecek operatörlerin seviyesi “Data Entry” bölümünde belirtilmektedir. Böylece, yetkisi olmayan operatörlerin ekranlardaki nesneleri kullanarak sisteme komut göndermesi engellenmiş olmaktadır.

3.6 Dinamik Ekranlar

3.6.1 Sistem ünitelerinin haberleşmelerinin ve alarmların izlenmesi

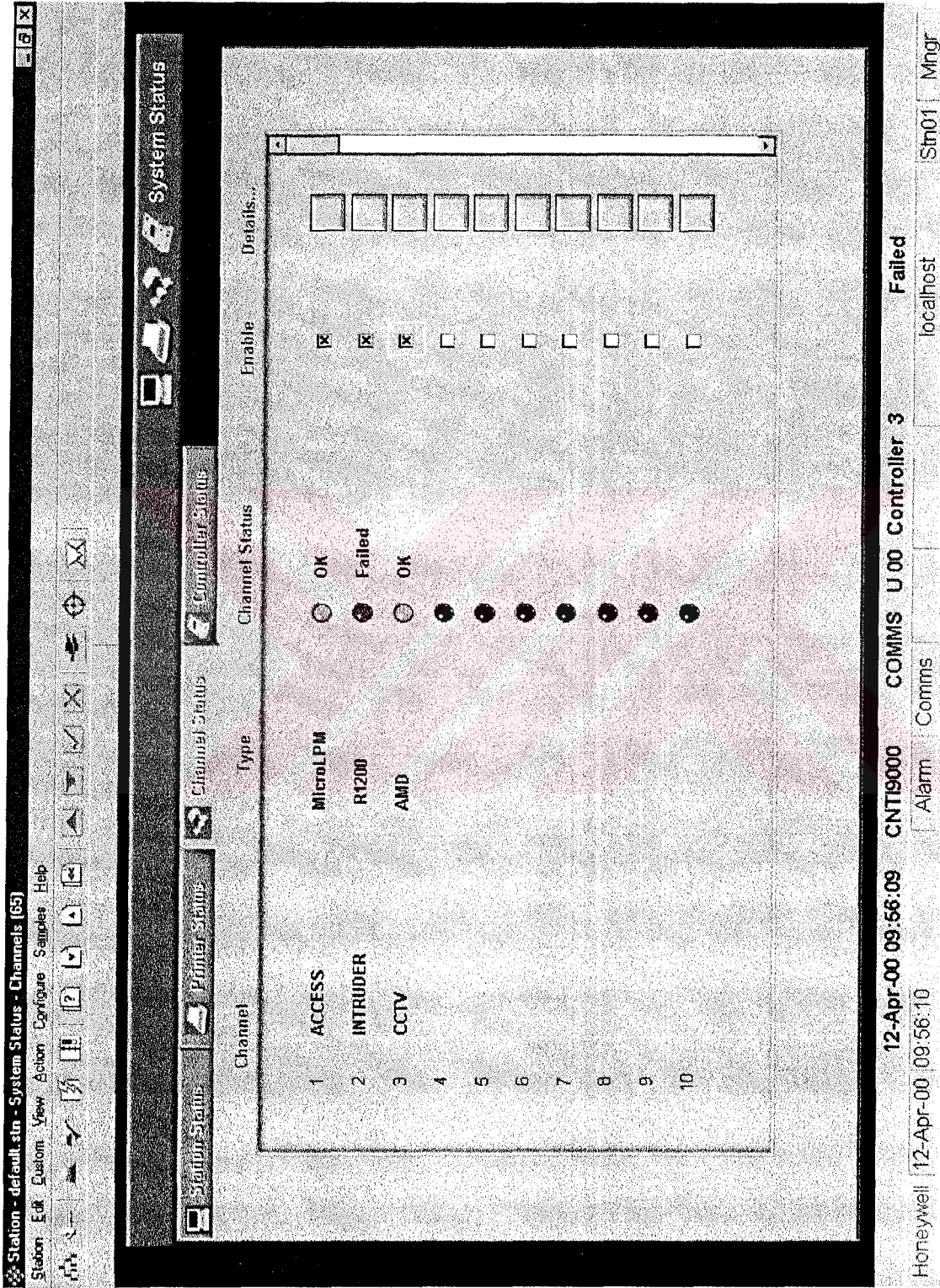
Haberleşmeyi sağlayan kanal ve kontrolörlerin izlenmesi; Şekil 3.17, 3.18 ve 3.19’da görülen ekranlar aracılığıyla yapılmaktadır. Şekil 3.20 yardımıyla da alarmlar gözlenmektedir.

Şekil 3.17, sistemde yer alan Access, Intruder ve CCTV kanallarının haberleşme durumlarını, kanal isimlerinin hemen sağ tarafındaki birer LED ile göstermektedir. LED yeşil yandığında, haberleşmenin hatasız bir biçimde devam ettiği, sarı yandığında haberleşme hatalarının çok arttığı, kırmızı yandığında da haberleşmenin kesildiği anlaşılmaktadır.

Şekil 3.18, sistemde yer alan Access saha kontrol ünitelerinin, I9000 alarm panelinin ve CCTV seçicisinin haberleşme durumlarını, kontrolör isimlerinin hemen sağ tarafındaki birer LED ile göstermektedir. LED yeşil yandığında, haberleşmenin hatasız bir biçimde devam ettiği, sarı yandığında haberleşme hatalarının çok arttığı, kırmızı yandığında da haberleşmenin kesildiği anlaşılmaktadır.

Şekil 3.19, güvenlik merkezinde ve resepsiyonlarda bulunan operatör bilgisayarların server bilgisayara bağlantı durumlarını, bilgisayar isimlerinin hemen sağ tarafındaki birer LED ile göstermektedir. LED yeşil yandığında, operatör bilgisayarın server bilgisayara bağlı olduğu, kırmızı yandığında da server bilgisayar ile bağlantı olmadığı anlaşılmaktadır.

Şekil 3.20, sistemde meydana gelen alarmların, tarih ve saat sırasına göre özetini vermektedir. Operatör bu ekran yardımıyla alarmları izleyecek, onaylayacak ve gerekirse müdahale edecektir.



Şekil 3.17 Kanalların haberleşme durumlarının izlendiği dinamik ekran.

Station - default.sln - Controller Status Summary [67]
 Station Edit Custom View Action Configure Samples Help

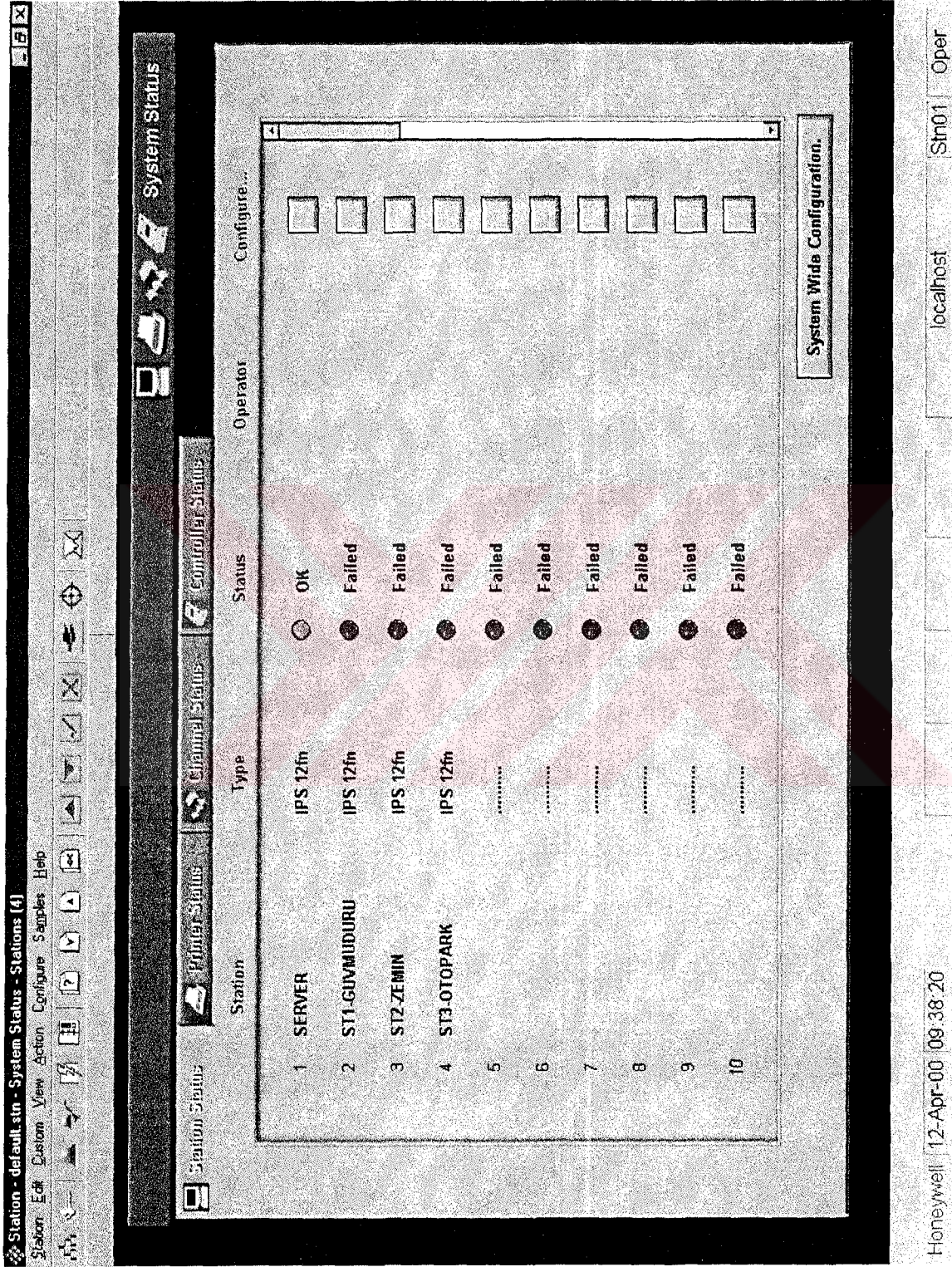
System Status

Station Status Printer Status Element Status Controller Status

Controller	Channel	Controller ID	Status	Enable	Details...
1	1	1	OK	☒	
2	1	2	OK	☒	
3	2	1	OK	☒	
4	3	1	OK	☒	
5	0	0		☐	
6	0	0		☐	
7	0	0		☐	
8	0	0		☐	
9	0	0		☐	
10	0	0		☐	

Honeywell 12-Apr-00 11:10:05 localhost Str01 Oper

Şekil 3.18 Kontrolörlerin haberleşme durumlarını gösteren dinamik ekran.



Şekil 3.19 Operatör bilgisayarların server'a bağlantı durumlarını gösteren dinamik ekran.

Station - default.stn - Alarm Summary - All Priorities (9)

Station Edit Custom View Action Configure Samples Help

The alarm has not returned to normal.

Page Alarm Summary

Unack only All Areas Urgent High All

Date	Time	Point ID	Alarm	Priority	Point Description	Value
* 12-Apr-00	21:38:04	CNTACCESS2	COMMS	H 00	Controller 2	Marg
* 12-Apr-00	21:38:03	CNTACCESS1	COMMS	U 00	Controller 1	Failed
* 12-Apr-00	21:38:02	ACCESS	COMMS	H 00	Channel 1	Marg
* 12-Apr-00	21:37:59	CNTACCESS1	COMMS	H 00	Controller 1	Marg

Total unacknowledged alarms: 0

Total acknowledged & still in alarm: 4

Unacknowledged & returned to normal
 * Unacknowledged & in alarm
 * Acknowledged & still in alarm

Acknowledged & waiting for response
 * Responded & in alarm
 * Responded & returned to normal

Honeywell 12-Apr-00 21:38:50

Alarm Comms localhost Stn01 Mngr

Şekil 3.20 Sistemde meydana gelen alarmları gösteren dinamik ekran.

3.6.2 Kartlı geiş sisteminin yönetilmesi ve geişlerin izlenmesi

Şekil 3.21, 3.22, 3.23 ve 3.24’te kartlı geiş sistemini yönetmek için kullanılan dinamik ekranlar, Şekil 3.25’te ise geiş olaylarının izlendiği dinamik ekran görölmektedir.

Sistemde 12 adet bölge bulunmaktadır :

- Giriş bölgesi (Turnikelerden veya otopark kapısından binaya giriş yapıldığında içinde bulunulan bölgedir. PGAP aktiftir.)
- Çıkış bölgesi (Turnikelerden geçilerek binadan çıkış yapıldığında bina dışı olarak varsayılan bölgedir. PGAP aktiftir.)
- Otopark bölgesi (Otopark kapısından geçilerek binadan çıkış yapıldığında bina dışı olarak varsayılan bölgedir. PGAP aktiftir.)
- Zemin kat bölgesi (Zemin kat kapısından giriş yapıldığında içinde bulunulan bölgedir.)
- 1. kat bölgesi (1. kat kapısından giriş yapıldığında içinde bulunulan bölgedir.)
- Güvenlik merkezi bölgesi (Güvenlik merkezi kapısından giriş yapıldığında içinde bulunulan bölgedir.)
- Güvenlik müdürü bölgesi (Güvenlik müdürü odasının kapısından giriş yapıldığında içinde bulunulan bölgedir.)
- 2. kat bölgesi (2. kat kapısından giriş yapıldığında içinde bulunulan bölgedir.)
- 3. kat bölgesi (3. kat kapısından giriş yapıldığında içinde bulunulan bölgedir.)
- 4. kat bölgesi (4. kat kapısından giriş yapıldığında içinde bulunulan bölgedir.)
- 5. kat bölgesi (5. kat kapısından giriş yapıldığında içinde bulunulan bölgedir.)
- Genel müdür bölgesi (Genel müdür odasının kapısından giriş yapıldığında içinde bulunulan bölgedir.)

Bu bölgeler arasındaki geişler kart okuyucular ile kontrol edilmektedir.

Yetki seviyelerini oluşturmak ve kart kullanım sürelerini sınırlamak için sistemde 3 adet zaman periyodu bulunmaktadır :

- TP1 zaman periyodu (Beraber kullanıldığı bölgeye, 7 gün 24 saat sürekli geiş izni vermektedir.)
- Haftaiçi zaman periyodu (Beraber kullanıldığı bölgeye, pazartesi ve cuma günleri arasında 07:00-22:00 saatleri içersinde geiş izni vermektedir.)
- Ziyaret zaman periyodu (Beraber kullanıldığı bölgeye, haftanın 7 günü 08:00-20:00 saatleri içersinde geiş izni vermektedir.)

Bölgelerin ve zaman periyotlarının eşleştirilmesi sonucu yetki seviyeleri oluşturulmaktadır.

Şekil 3.21’de sistemde varolan yetki seviyelerini gösteren dinamik ekran, Şekil 3.22’de ise “2.Kat Haftaiçi” yetki seviyesinin işlevinin tanımlandığı dinamik ekran yer almaktadır.

Her kat için bir hafta içi yetkisi, ziyaret yetkisi ve tam yetki tanımlanmıştır. “2.Kat Haftaiçi” yetki seviyesine sahip kart; “Giriş”, “Çıkış” ve “2.kat” bölgelerine “Haftaiçi” zaman periyodu içersinde geiş yapma hakkına sahip olacaktır.

Station - default.stn - Access Configuration - Access Levels [215]

Station Edit Custom View Action Configure Samples Help

Access Levels Zone Time Profiles Life Access

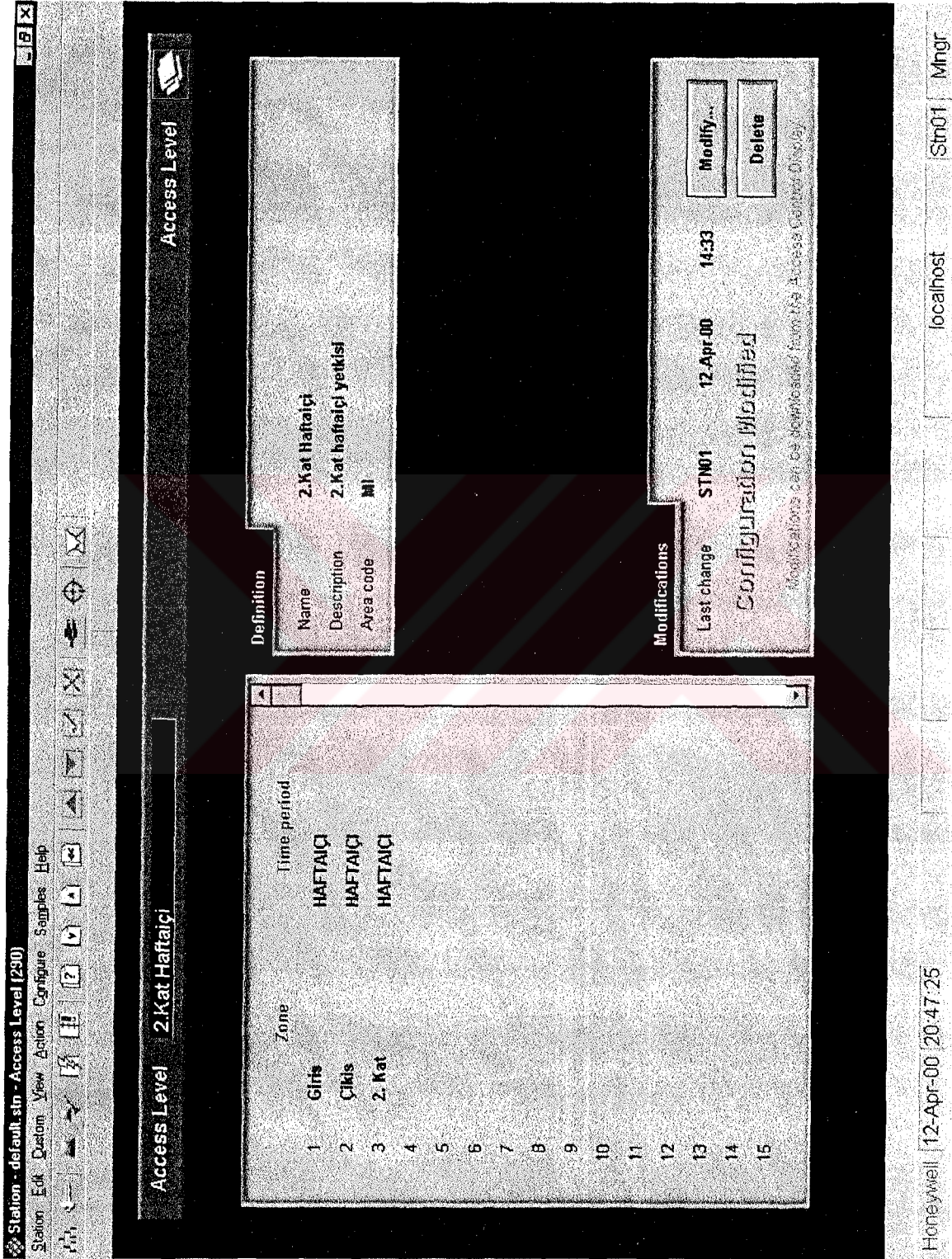
Access Configuration

Access Level	Description	Area Code	Details...
1	Supenuser	MI	
2	Genel Müdür	MI	
3	Güvenlik Müdürü	MI	
4	Zem.Kat Tam	MI	
5	Zem.Kat Haftaıçı	MI	
6	Zem.Kat Ziyaret	MI	
7	1.Kat Tam	MI	
8	1.Kat Haftaıçı	MI	
9	1.Kat Ziyaret	MI	
10	Otopark	MI	
11	Güvenlik Merkezi	MI	
12	2.Kat Tam	MI	
13	2.Kat Haftaıçı	MI	
14	2.Kat Ziyaret	MI	
15	3.Kat Tam	MI	
16	3.Kat Haftaıçı	MI	
17	3.Kat Ziyaret	MI	
18	4.Kat Tam	MI	
19	4.Kat Haftaıçı	MI	
20	4.Kat Ziyaret	MI	

Honeywell 12-Apr-00 20:43:28

localhost Str01 Mngr

Şekil 3.21 Sistemde varolan yetki seviyelerine ulaşımı sağlayan dinamik ekran.



Şekil 3.22 “2.Kat Haftaici” yetki seviyesinin işlevinin tanımlandığı dinamik ekran.

“2. Kat Tam” yetki seviyesine sahip kart; “Giriş”, “Çıkış” ve “2.kat” bölgelerine “TP1” zaman periyodu (7 gün 24 saat) içerisinde geçiş yapma hakkına sahip olacaktır.

“2.Kat Ziyaret” yetki seviyesine sahip kart; “Giriş”, “Çıkış” ve “2.kat” bölgelerine “Ziyaret” zaman periyodu içerisinde geçiş yapma hakkına sahiptir.

“Otopark” yetki seviyesine sahip kart; “Otopark” bölgesine “TP1” zaman periyodu içerisinde geçiş yapma hakkına sahiptir.

“Genel Müdür” yetki seviyesine sahip kart; “Genel müdür” bölgesine “TP1” zaman periyodu içerisinde geçiş yapma hakkına sahiptir.

“Güvenlik Müdürü” yetki seviyesine sahip kart; “Güvenlik müdürü” bölgesine “TP1” zaman periyodu içerisinde geçiş yapma hakkına sahiptir.

“Güvenlik Merkezi” yetki seviyesine sahip kart; “Güvenlik merkezi” bölgesine “TP1” zaman periyodu içerisinde geçiş yapma hakkına sahiptir.

Kart sahibi personelin kişisel bilgileri ve fotoğrafı, Şekil 3.23’teki dinamik ekran yardımıyla operatörler tarafından görülebilmektedir. Bilgiler, gerektiğinde yeterli güvenlik seviyesine sahip operatörler tarafından bu ekran yardımıyla değiştirilebilmektedir.

Bu ekranda; kart sahibinin çalıştığı bölüm, görevi, personel numarası, dahili telefonu, doğum tarihi, doğum yeri, öğrenim durumu, sahip olduğu araç ve plakası gibi bilgilerin yanısıra en son geçiş yaptığı bölge, geçişi yaptığı tarih ve saat bilgisi de yer almaktadır.

Şekil 3.24’te kartlara yetki seviyelerinin atanması için kullanılan dinamik ekran görülmektedir. Bir karta “Access levels” bölümünden 8 adet yetki seviyesi verilebilmektedir. 5 numaralı kart; “Otopark”, “1.Kat Tam” ve “Güvenlik Merkezi” olmak üzere 3 adet yetki seviyesine sahiptir.

“Commencement date” bölümünde kartın sahibi tarafından kullanılmaya başlandığı tarih, “Expiry date” bölümünde ise sahibinin kartı en son kullanabileceği tarih görülmektedir. Yetki seviyeleri ve tarih sınırlaması, gerektiğinde yeterli güvenlik seviyesine sahip operatörler tarafından bu ekran yardımıyla değiştirilebilmektedir.

“Card state” bölümünde kartın bulunduğu durum tanımlanmaktadır. Kart sadece Active durumdayken çalışmaktadır. Bu bölümde kartın çalınmış veya kaybolmuş olduğu tanımlanmışsa, kart çalışmayacaktır.

Station - default.stn - Card Detail - Overview (235)

Station Edit Custom View Action Configure Samples Help

Station Edit Custom View Action Configure Samples Help

Card 5 Zafer Karabacak Area MI Card Detail

Overview Personal Details Access Details

Personal Profile

Eğitimi	Teknik Müdürlük
Görevi	Tekniker
Personel No	98000005
Dahili Tel	2444
D.Yeni	Trabzon
D.Tanhi	1973
Öğrenim D.	Yüksek Okul
Araç Model	Ford Escort
Araç Plaka	34 UP 2345

Card Access

Card State	Active
Last zone accessed	Giris
Last door accessed	at 0:00:00 on
Last access message	Granted

Associated page 0

Zafer Karabacak

Configuration Modified

STN01 23-Apr-00 13:42:09 Download Modify localhost Stn01 Mngr

Honeywell 23-Apr-00 13:50:45

Şekil 3.23 Kart sahibi personelin kişisel bilgilerini gösteren dinamik ekran.

Station - default.stn - Card Detail - MicroLPM Access Details (2003)

Station Edit Custom View Action Configure Samples Help

MicroLPM Access Details (2003)

Card 5 Zafer Karabacak Area MI Card Detail

Overview Personal Details Access Details

Access Levels

1	Otopark
2	1.Kat Tam
3	Güvenlik Merkezi
4	
5	
6	
7	
8	

Card

Card technology	MicroLPM
Card state	Active
Commencement date	12-Feb-98
Expiry date	31-Dec-03
☐	
☐	

MicroLPM

Secondary expiry date	0
Affiliation code	0
Class H counter	
☐	
☐	
☐	
☐	
☐	

FS90 AMIC

FS90 AMC Card Type	Employee
☐	Allow access on communications loss

Lighting Control

Light zone	
------------	--

Access Point Alarm Override

Instruction page	0
☐	
Alarm priority	Journal
Subpriority	0

Last change STN01 12-Apr-00 21:05:01

Honeywell 12-Apr-00 21:05:05

localhost Str01 Mngr

Modify Download

Şekil 3.24 Kartlara yetki seviyesi atanması için kullanılan dinamik ekran.

Access Event Summary

All Events

Time	Point ID	Event	Level	Door Name/Card Holder	Card Number	Field Time/Reason
					# 293	Authorized
10-Apr-00 11:21:26	MICROLPM-RD03	GRANTED		6. Kat Giriş Kart Okuyucu	# 259	10-Apr-00 11:22:00
				Zafer Karabacak	# 259	Authorized
10-Apr-00 11:19:54	MICROLPM-RD04	GRANTED		6. Kat Çıkış Kart Okuyucu	# 259	10-Apr-00 11:20:00
				Zafer Karabacak	# 259	Authorized
10-Apr-00 11:19:04	MICROLPM-RD03	DENIED	L 00	6. Kat Giriş Kart Okuyucu	# 130	10-Apr-00 11:19:00
					# 130	Undefined card

Şekil 3.25 Kartlı geçiş olaylarını gösteren dinamik ekran.

Operatörler , kapılardan ve turnikelerden yapılan geçişleri izlemek için Şekil 3.25'teki dinamik ekranı kullanacaktır.

“Time” bölümünde; geçişin yapıldığı tarih ve saat, “Point ID” bölümünde; geçiş yapılan noktanın veritabanındaki ismi, “Event” bölümünde; geçişe izin verilip verilmediği, “Door Name/Card Holder” bölümünde; geçiş yapılan okuyucunun tanımı ve geçiş yapan kişinin ismi, “Card Number” bölümünde; kullanılan kartın numarası, “Field Time/Reason” bölümünde ise saha ünitesinden bu geçiş hakkında alınan bilgi görülmektedir.

“Event” bölümünde; “GRANTED” ifadesinin görülmesi geçiş izninin verildiği, “DENIED” ifadesinin görülmesi ise geçişe izin verilmediği anlamına gelmektedir.

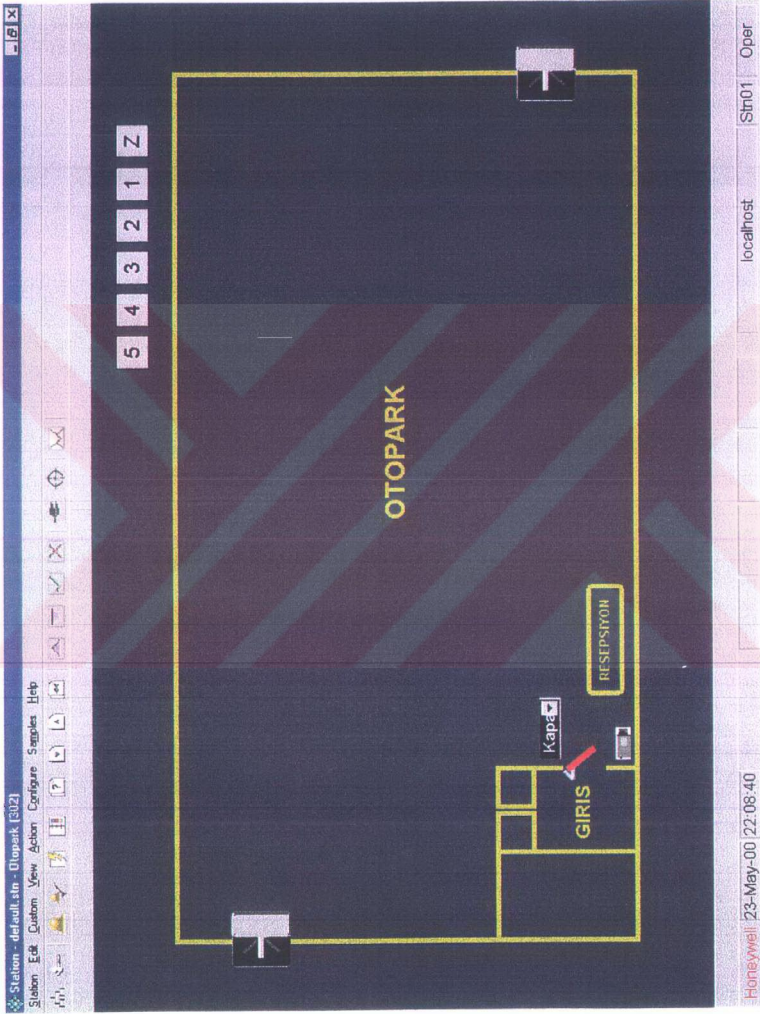
Eğer geçişe izin verilmemişse, “Reason” bölümünde bunun nedeni görülecektir. PGAP ihlali durumunda, kartın yetkisi olmadığı, çalınmış veya kayıp olarak tanımlandığı yada sistemde tanımlı olmadığı durumlarda ayrı ayrı uyarı ifadeleri görülecektir.

3.6.3 Kapı, turnike, buton ve kameraların izlenmesi ve kontrolü

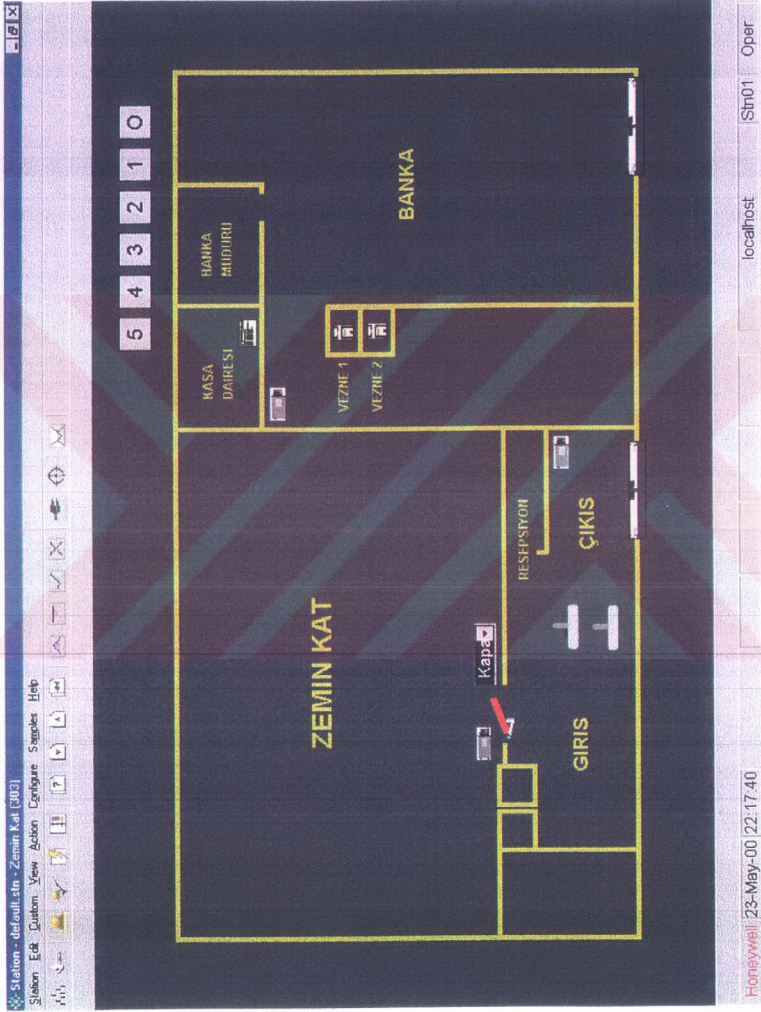
Şekil 3.26, 3.27, 3.28, 3.29 ve 3.30'da görülmekte olan dinamik ekranlar vasıtasıyla, binanın her bir katındaki kapı, turnike, buton ve kameraları temsil eden dinamik elemanlara ulaşmak mümkün olmaktadır. 3. ve 4. katların dinamik ekranları, 2. katın dinamik ekranıyla aynı elemanlara sahip olduğundan bu şekiller arasında yeralmamaktadır.

Katlardaki kapıların durumları, kapı sembolleri yardımıyla gözlenmektedir. Sembol; kapalı durumda ve yeşil renkte görüldüğü zaman kapının kapalı konumda olduğu, açık durumda ve kırmızı renkte yanıp söndüğü zaman kapının açık konumda olduğu anlaşılmaktadır.

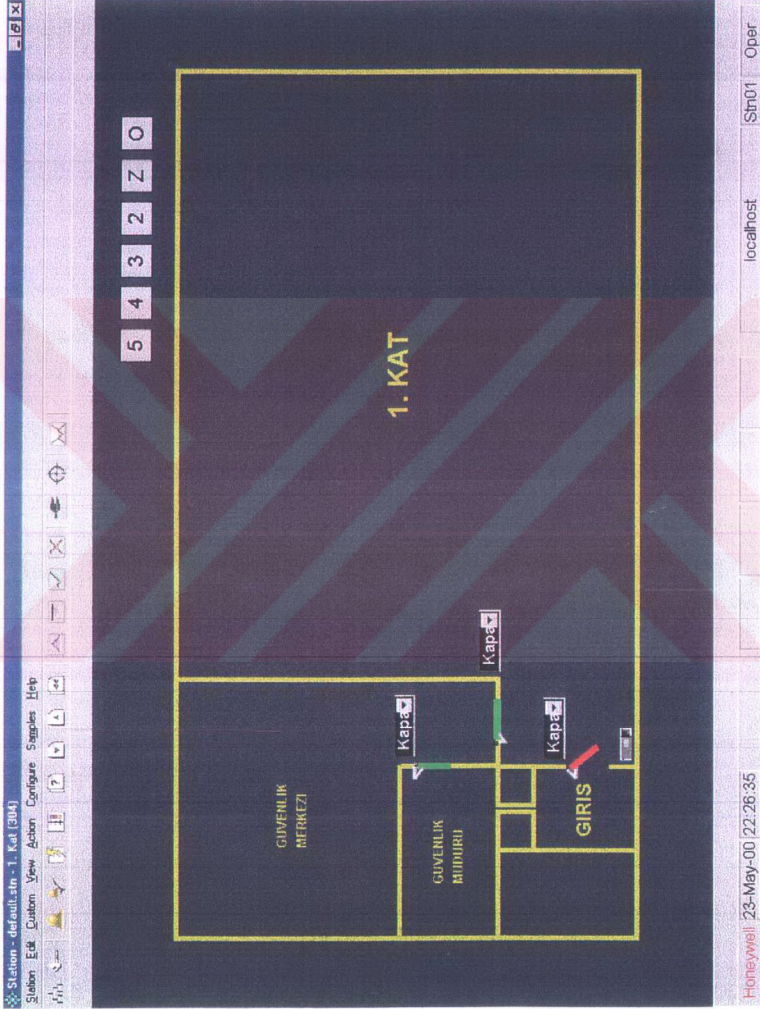
Dinamik ekranlardaki kapı sembolünün yanında yeralan kutucuk yardımıyla kapıya operatör bilgisayarlardan aç veya kapa komutu gönderilebilmektedir.



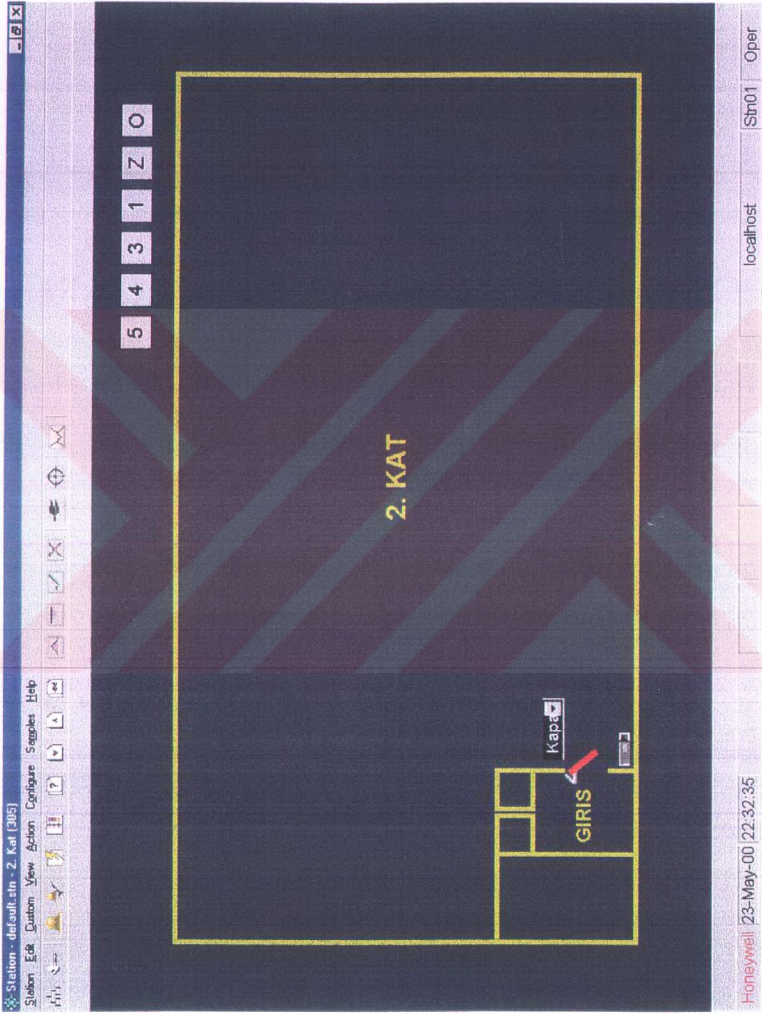
Şekil 3.26 Otopark kartı ekipmanları izlemek ve kontrol etmek için kullanılan dinamik ekran.



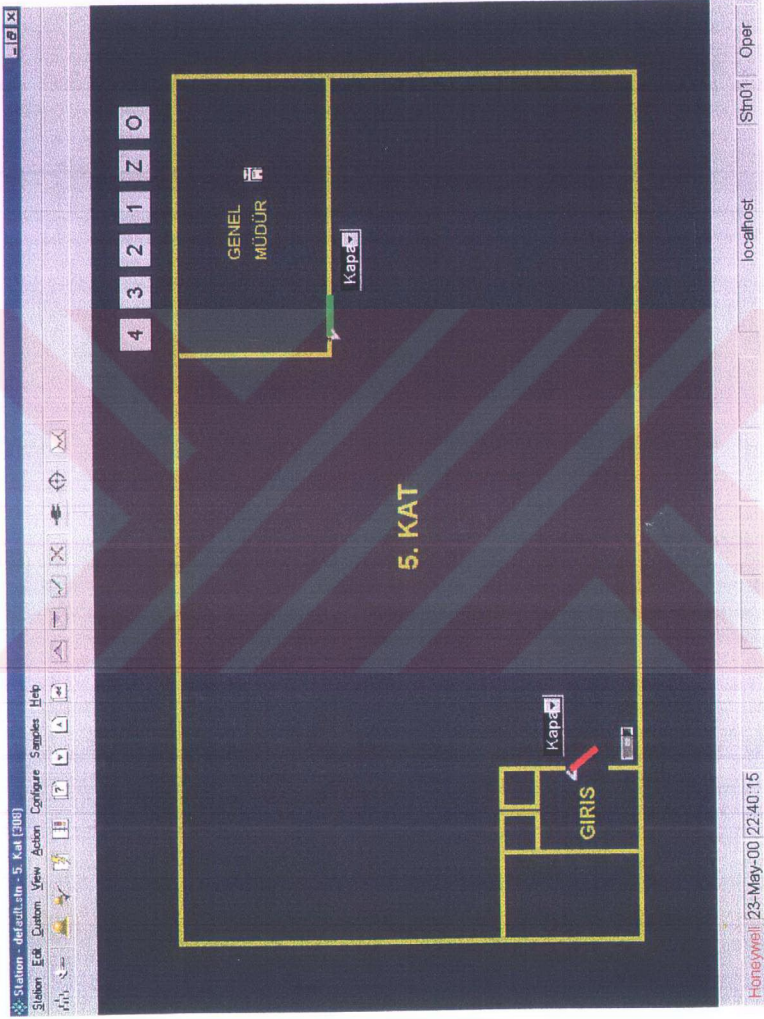
Şekil 3.27 Zemin kattaki ekipmanları izlemek ve kontrol etmek için kullanılan dinamik ekran.



Şekil 3.28 1. kattaki ekipmanları izlemek ve kontrol etmek için kullanılan dinamik ekran.



Şekil 3.29 2.kattaki ekipmanları izlemek ve kontrol etmek için kullanılan dinamik ekran.



Şekil 3.30 5.kattaki ekipmanları izlemek ve kontrol etmek için kullanılan dinamik ekran.

Turnikelerin durumu da turnike sembolü yardımıyla gözlenmektedir (Şekil 3.27). Sembol; turnike, normal konumunda çalışırken gri renkte, uygunsuz bir geçiş sonucu alarm verdiği zaman kırmızı renkte yanıp sönerken görülecektir.

5.katta ve zemin katta yer alan butonlar ve keypad (Şekil 3.27 ve Şekil 3.30), o katlara ait dinamik ekranlardan izlenmektedir. Normal konumlarındayken sembolleri sarı renkte gözükülecektir. Butonlardan birine basıldığı zaman veya keypad'den alarm sinyali alındığı zaman, ait oldukları kat operatör bilgisayarın ekranına otomatik olarak gelecek ve sembol kırmızı renkte yanıp sönecektir.

Dinamik ekranlardaki kamera sembolüne basıldığı zaman Şekil 3.31'deki CCTV kontrol dinamik ekranı ortaya çıkacaktır. "View" bölümündeki ayarlar kullanılarak istenen kamera görüntüsü istenen monitöre aktarılabilir. Operatör, gerektiğinde kamera görüntüsünü dondurulabilecek veya kopyalayabilecektir. Şekilde; 2. kat kamerasının görüntüsünün ana monitöre atandığı görülmektedir.

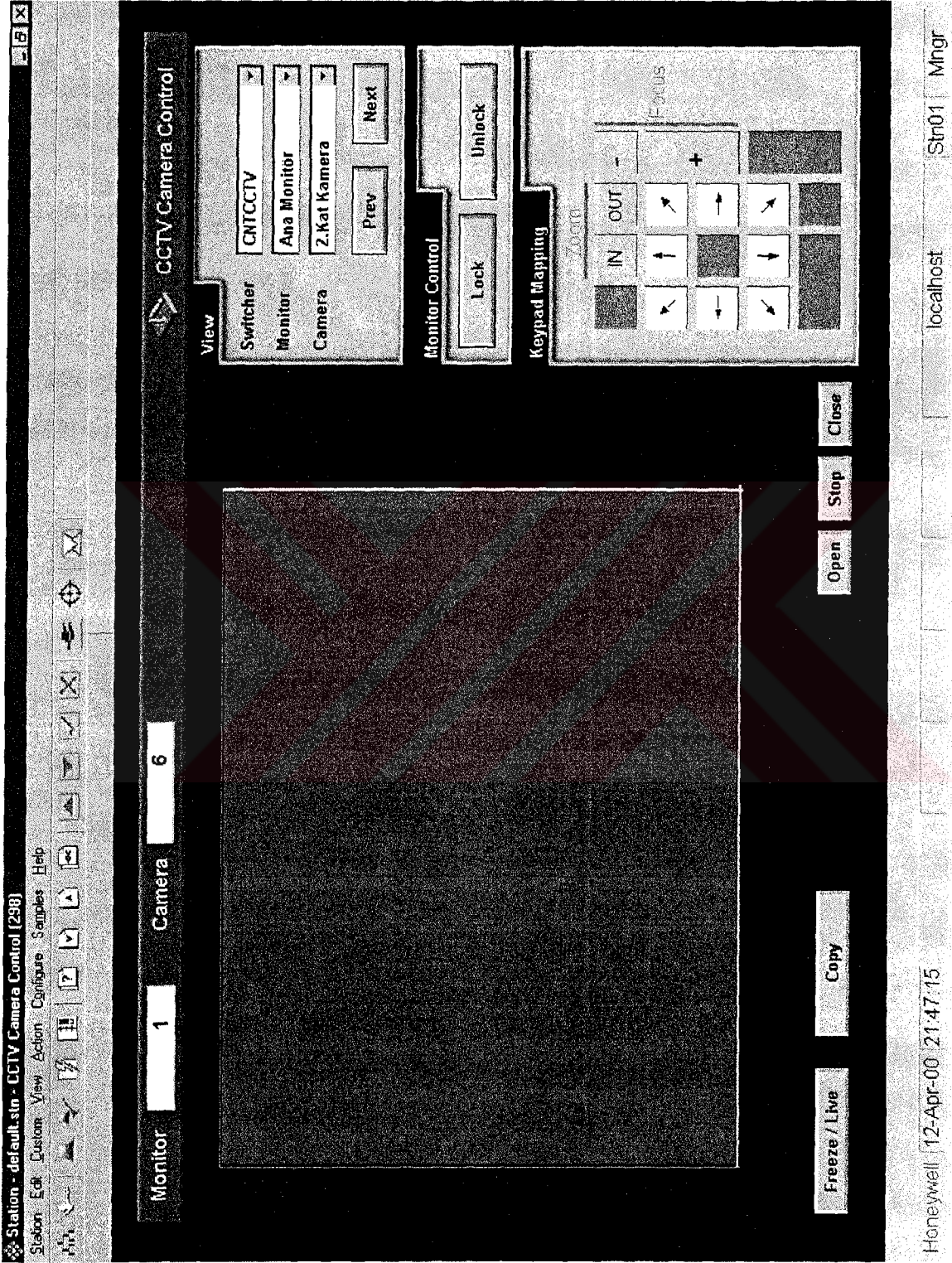
3.6.4 Raporlamalar

Şekil 3.32'de sistemde tanımlı olan raporlara erişimi sağlayan dinamik ekran görülmektedir. Burada görülen 13 adet rapordan bazılarında, kriterler belirlemek amacıyla yardımcı ekranlar kullanılması gerekmektedir.

Olay ve alarm raporu ile; seçilecek zaman aralığı içinde meydana gelen olayların ve alarmların listesi alınacaktır. Bu rapor için kullanılacak yardımcı ekran Şekil 3.33'te görülmektedir. Operatör, bu ekrandaki "Point ID" bölümüne raporu alınacak noktanın veritabanındaki ismini yazacak ve "Time Span" bölümüne de rapora alınacak olayların tarih-saat aralığını belirtecektir.

Kart raporu ile, çeşitli kriterler kullanılarak kartların içerdiği bilgiler listelenecektir. (Kart sahibinin ismi, çalıştığı bölüm, yetki seviyesi, vb.) Operatör, yardımcı ekrana kriterlerini girecek ve sonra raporu isteyecektir.

Operatör; bina içi personel raporunu istediğinde, o anda binanın içersinde mevcut olan personel listelenecektir. Bina harici personel raporu istendiğinde o anda bina dışında bulunan personel, zemin kat personel raporu istendiğinde o anda zemin katta bulunan personel, 1.kat personel raporu istendiğinde o anda 1.katta bulunan personel listelenecektir. 2.kat personel, 3.kat personel, 4.kat personel ve 5.kat personel raporları da aynı şekilde kullanılacaktır.



Şekil 3.31 CCTV sistemini izlemek ve kontrol etmek için kullanılan dinamik ekran.

Station - default.stn - Report & History Archive Summary [134]
 Station Edit Custom View Action Configure Samples Help

Report and History Archive Summary

Report/Archive	Title	Configuration	Request..
1 Olay Alarm	Olay ve Alarm Raporu	Alarm and Event (Old Style)	
2 Kart Liste	Kart Raporu	Card List	
3 Binalıç	Bina içi personel raporu	Occupancy (Old Style)	
4 Binaharici	Bina harici personel raporu	Occupancy (Old Style)	
5 ZeminKat	Zemin Kat personel raporu	Occupancy (Old Style)	
6 1.Kat	1.Kat personel raporu	Occupancy (Old Style)	
7 2.Kat	2.Kat personel raporu	Occupancy (Old Style)	
8 3.Kat	3.kat personel raporu	Occupancy (Old Style)	
9 4.Kat	4.Kat personel raporu	Occupancy (Old Style)	
10 5.Kat	5.Kat personel raporu	Occupancy (Old Style)	
11 Kapi Turn	Kapi ve Turnike takip raporu	Door History (Old Style)	
12 Kart Takip	Kart Takip Raporu	Card Trail	
13 Ziyaretçi	Ziyaretçi Takip Raporu	Group Card Trail (Old Style)	
14		None	
15		None	

Changing the Report Type will clear ALL report configuration settings

Honeywell 12-Apr-00 21:09:05 Str01 Mng

Şekil 3.32 Rapor istemek için kullanılan dinamik ekran.

Station - default.stn - Alarm & Event Report (87)

Station Edit Custom View Action Configure Samples Help

Alarm & Event Report

Report 1 Olay ve Alarm Raporu Area Alarm & Event Report

Title Olay ve Alarm Raporu Request program LRN 0

Name Olay Alarm

This report will show all alarms and events matching the search criteria, which occurred during the specified time span

Search Criteria

Event location Online

Area

Point ID(s) ACCESS1-DS1

Event description

Event type All

Sub priority

Leave Subpriority blank for all subpriorities or operators

Time Span

Start time 05-Apr-00 6:00

End time 10-Apr-00 21:00

Time span up to current time set start and end dates to a blank field

Controller offline time 0:00

Controller offline time is added on to the time span to allow for the controller field times being different from XSM system time

Next report 0:00

Interval None

Destination

Request

Honeywell 12-Apr-00 21:13:25 localhost Str01 Mngr

Şekil 3.33 Olay ve alarm raporu için yardımcı dinamik ekran.

Kapı ve turnike takip raporu ile; seçilen zaman aralığı içinde, seçilen kart okuyucudan yapılan geçişlerin listesi alınacaktır. Bu rapor için kullanılacak yardımcı ekran Şekil 3.34'te görülmektedir. Operatör, bu ekrandaki “Door Name” bölümüne raporu alınacak kart okuyucunun veritabanındaki ismini yazacak ve “Time Span” bölümüne de rapora alınacak geçişlerin tarih-saat aralığını belirtecektir.

Kart takip raporu ile; seçilen zaman aralığı içinde, seçilen kartın yaptığı geçişlerin listesi alınacaktır. Bu rapor için kullanılacak yardımcı ekran Şekil 3.35'te görülmektedir. Operatör, bu ekrandaki “Card number” bölümüne raporu alınacak kartın numarasını yazacak ve “Time Span” bölümüne de rapora alınacak geçişlerin tarih-saat aralığını belirtecektir.

Ziyaretçi raporu ile; ziyaretçi kartlarının seçilecek zaman aralığı içinde yaptıkları geçişlerin listesi alınacaktır. Operatör; yardımcı ekrana, rapora alınacak geçişlerin tarih-saat aralığını girecek ve sonra raporu isteyecektir.



Station - default.stn - Door History Report (92)

Station Edit Custom View Action Configure Samples Help

Report 11 Kapi ve Turnike takip raporu

Area Door History Report

Title Kapi ve Turnike takip raporu

Name Kapi Turn Request program LRN 0

This report will show all alarms and events matching the search criteria, which occurred during the specified time span

Search Criteria

Event location Online

Sorting key Time

Area code

Door Name ACCESS1-OKU1

Event type All

Sub priority

Leave sub priority blank for all sub priorities.

Next report

Interval None

Destination

Time Span

Start time 01-Apr-00 7:00

End time 02-Apr-00 12:30

Time span up to current time set start and end dates to a blank field

Controller offline time

Controller offline time is added on to the time span to allow for field times being different from XSM system time

Honeywell 12-Apr-00 21:17:56

localhost Str01 Mngr

Şekil 3.34 Kapi ve turnike takip raporu için yardımcı dinamik ekran.

Station - default.stn - Card Trail Report (90)

Station Edit Custom View Action Configure Samples Help

Report 12 Kart Takip Raporu

Area

Card Trail Report

Title: Kart Takip Raporu

Name: Kart Takip Request program LRN: 0

This report will show all alarms and events matching the search criteria, which occurred during the specified time span

Search Criteria

Event location: Online

Sorting key: Time

Card number: 5

Event type: All

Sub priority: Subpriority (00-15)

Leave sub priority blank for all sub priorities

Request

DD-MM-YY: 01-Mar-00 HH-MM: 00:00

Next report: None

Interval: 0:00

Destination: 0:00

Time Span

Start time: 01-Mar-00 05:00

End time: 31-Mar-00 23:00

Time span up to current time set start and end dates to a blank field

Controller offline time

Controller offline time is added on to the time span to allow for field times being different from XSM system time

Honeywell 12-Apr-00 21:19:15

localhost

Str01

Mngr

Şekil 3.35 Kart takip raporu için yardımcı dinamik ekran.

4 SONUÇLAR

Günümüzde; insanlar, işyerlerini ve evlerini tehdit eden, hırsızlık, vandalizm, endüstriyel casusluk, sabotaj gibi olaylardaki hızlı bir artışla karşı karşıya kalmıştır. Bu olaylardaki artışa karşılık olarak, güvenlik sistemleri teknolojisi gelişimini sürdürmektedir. İnsanlar, uygun bir maliyetle gerekli korunma ihtiyaçlarını sağlamaya çalışmaktadır.

İş gücü kayıplarının artması, hırsızlık sonucu malzeme kayıplarının meydana gelmesi, saldırıların can ve mal kayıplarına neden olması, işyeri sahiplerine bu kayıpları kontrol etmek için bir şeyler yapmaları gerektiğini göstermektedir. Bir çok işadamı etkin bir güvenlik yönetimi ile kayıpları önlemenin iş karına katkısının, diğer herhangi bir aktiviteden daha fazla olacağını düşünmeye başlamıştır.

Kayıpları önleyecek bir güvenlik sistemi tasarımı yapılırken; binanın yapımı ve kullanımı süresince, hırsızlık, vandalizm, saldırı ve sabotaj olasılıklarının bina içinde ve çevresinde ortadan kaldırılması hedef alınmalıdır. İleriye görerek zamanında alınacak bir önlem, daha sonra oluşabilecek bir çok problemi ortadan kaldıracaktır.

Güvenliğin tam anlamıyla sağlanabilmesi için, risk değerlendirmesi yapılarak binanın risk seviyesi saptanmalı ve belirlenen risk seviyesine uygun önlemler alınmalıdır.

Kalabalık personel ve ziyaretçi sayısına sahip binalarda, güvenliğin üst düzeyde sağlanabilmesi için üç farklı güvenlik sisteminin bir arada kullanılmasına ihtiyaç duyulmaktadır: Alarm sistemi, geçiş kontrol sistemi, CCTV (Closed Circuit Television) sistemi. Geçiş kontrol sistemi ve CCTV sistemi birlikte kullanılarak binaya giriş-çıkışlar kontrol edilmektedir. Alarm sistemi, şüpheli durumlara ve hırsızlık olaylarına kısa sürede müdahale imkanı vermektedir. CCTV sistemi yardımıyla; satış reyonlarında, bürolarda, otoparkta hırsızlık olaylarına kısa sürede müdahale imkanı sağlanmakta, üretim alanında iş akışı düzenli olarak gözlenmekte ve iş gücü kayıpları engellenmektedir. Bu sistemlerin birbirleriyle uyumlu ve etkin çalışabilmeleri için, tek bir merkezden izlenmeleri ve kontrol edilmeleri gerekmektedir. Yazılım firmaları, çalışmalarını bu yöne doğrultmuşlar ve sistemleri entegre edecek merkezi yazılımlar geliştirmişlerdir.

Merkezi yazılım kullanılarak gerçekleştirilen güvenlik uygulamaları, sistemlerin birbirlerine uyumlu çalışmasını sağlamakta ve dinamik ekranlar aracılığıyla operatörlere kolay kullanım imkanı vermektedir.

Çalışmanın uygulama bölümünde, Excel Security Manager yazılımı ile sağlanan sistem entegrasyonu sonucunda bina sahibinin istekleri karşılanmıştır.

Kartlı geçiş sistemi ile binaya, katlara ve önemli odalara giriş-çıkışlar kısıtlanmıştır. Bu kapıların açık veya kapalı olup olmadıkları izlenebilmekte ve gerektiğinde aç veya kapa komutu gönderilerek, kapılar kontrol edilebilmektedir. İstenilen zamanda; bina içindeki, bina dışındaki yada herhangi bir kattaki personel belirlenebilmekte, kart sahiplerinin yaptıkları geçişler rapor halinde alınabilmektedir. Ziyaretçilere, sadece ziyaret zaman dilimi içinde kullanılabilecek ve kısıtlı geçiş haklarına sahip kartlar verilebilmektedir.

CCTV sistemi ile binadaki tüm giriş-çıkışlar gözlenmektedir. Gözlem yapılırken; aynı anda kamera görüntüleri, zaman atlamalı video kayıt edicisi aracılığıyla video kasete kayıt edilmektedir.

Veznedarlar ve genel müdür; şüpheli durumlarda, alarm sistemine bağlı olan panik butonları aracılığıyla güvenlik görevlilerini uyarabilmektedir. Panik butonuna basıldığında; o katın planı, güvenlik merkezinde bulunan operatör bilgisayarın ekranına otomatikman gelecek ve hem sesli olarak, hem de basılan butonun simgesi yanıp sönerek operatörü uyaracaktır. Aynı şekilde kasa dairesini zorla açmak zorunda kalan bir görevli; gizli şifreyi kullanarak, güvenlik merkezine sessiz bir şekilde alarm sinyali gönderebilmektedir. Bu durumda, kasa dairesinin kapısı açılacak ve hırsızların alarm sinyali gönderildiğinden haberi olmayacaktır.

Sistemde hazırlanmış olan kullanımı basit dinamik ekranlar sayesinde operatörlerin karmaşık komutlara ihtiyacı yoktur. Operatörler; görsel komutlarla alarm, cctv, kartlı geçiş sistemlerini tek bir merkezden kontrol edebilmektedir.

Geçmişte; merkez yazılımlarını geliştiren firmalar, kendilerine ait sistemlerin entegrasyonu üzerinde yoğunlaşmıştır. Ancak tüketicinin istekleri, güvenlik sektörünün değişen ihtiyaçları ve firmaların farklı sistemler üzerine uzmanlaşmaları üzerine, diğer firmaların sistemlerini de kontrol edebilecek yazılımlar için çalışmalar yapılmaya başlanmıştır.

Günümüzde artan güvenlik ihtiyaçları nedeniyle, güvenlik sektöründeki ve güvenlik yönetim sistemlerindeki gelişimin gelecekte de süreceği ve farklı firmalara ait farklı sistemlerin tek bir merkezden kontrolü üzerine yapılan çalışmalarda ilerlemeler kaydedileceği görülmektedir.

KAYNAKLAR

Charlett, A.J., (1985), Security of building sites, The Chartered Institution Of Building Services Engineers, London.

CIBSE, (1991), Security engineering, The Chartered Institution Of Building Services Engineers, London.

Clark, R. ve Mayhew P., (1980), Designing out crime, Home Office Research Unit/HMSO, London.

Cumming, N., (1987), Security: the comprehensive guide to equipment selection and installation, Architectural Press, London.

Fay, J., (1987), Butterworths security dictionary: terms and concepts, Butterworths, London.

Fennelly, L.J., (1989), Handbook of loss prevention and crime prevention, Butterworths, London.

Green G., (1987), Introduction to security , Butterworths, London.

Honeywell, (1998), Excel Security Manager Overview and Planning Guide, Honeywell Ltd. Australia.

Keynes, M., (1986), Code of practice for remote centres for intruder alarm systems, British Standards Institution.

Keynes, M., (1987), BS6804: Code of practice for social alarm systems, British Standards Institution.

Keynes, M., (1988), Specifications for high security intruder alarm systems in buildings, British Standards Institution.

Keynes, M., (1990), Guide for security of buildings against crime, British Standards Institution.

Öztürk, E., (1997), "CCTV", Yangın ve Güvenlik Dergisi, Sayı 33, Eylül-Ekim 1998, İstanbul.

Yangın ve Güvenlik Dergisi, (1998), "Kapalı Devre Televizyon Sistemlerinin ABC'si", Sayı 35, Ocak-Şubat 1998, İstanbul.

Yangın ve Güvenlik Dergisi, (1998), "Kapalı Devre TV Sisteminde Mercekler ve Mercek Seçimi", Sayı 36, Mart-Nisan 1998, İstanbul.

ÖZGEÇMİŞ

Doğum tarihi	26.07.1975	
Doğum yeri	Rize-Pazar	
Lise	1989-1992	İstanbul Şehremini Lisesi
Lisans	1992-1996	Yıldız Teknik Üniversitesi Elektrik-Elektronik Fak. Elektrik Mühendisliği Bölümü
Yüksek Lisans	1996-2000	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektrik Müh. Anabilim Dalı

Çalıştığı kurum(lar)

1997-1998	Elit CCTV Center Elektronik San.ve Tic. Ltd Şti.
1998-Devam ediyor	Honeywell Otomasyon ve Kontrol Sis. San.ve A.Ş.

