3G İLE ENDÜSTRİYEL OTOMASYON SİSTEMLERİNİN İZLENMESİ

2012
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

Uğur ÖZDEMİR

3G İLE ENDÜSTRİYEL OTOMASYON SİSTEMLERİNİN İZLENMESİ

Uğur ÖZDEMİR

Karabük Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalında

Yüksek Lisans Tezi

Olarak Hazırlanmıştır

KARABÜK

Nisan 2012

Uğur ÖZDEMİR tarafından hazırlanan "3G İLE ENDÜSTRİYEL OTOMASYON SİSTEMLERİNİN İZLENMESİ" başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. İlhami Muharrem ORAK .....

Tez Danışmanı, Bilgisayar Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 18/04/ 2012

Ünvanı, Adı SOYADI (Kurumu) İmzası

Başkan : Yrd. Doç. Dr. Baha ŞEN (KBÜ) .....

Üye : Yrd. Doç. Dr. İlhami Muharrem ORAK (KBÜ) .....

Üye : Yrd. Doç. Dr. Hüseyin DEMİREL (KBÜ) .....

..../..../2012

KBÜ Fen Bilimleri Enstitüsü Yönetim Kurulu, bu tez ile Yüksek Lisans derecesini onamıştır.

Prof. Dr. Nizamettin KAHRAMAN .....

Fen Bilimleri Enstitüsü Müdürü

"Bu tezdeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim."

Uğur ÖZDEMİR

ÖZET

Yüksek Lisans Tezi

3G İLE ENDÜSTRİYEL OTOMASYON SİSTEMLERİNİN İZLENMESİ

Uğur ÖZDEMİR

Karabük Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı:
Yrd. Doç. Dr. İlhami Muharrem ORAK
Nisan 2012, 79 sayfa

Bu çalışmada, günümüzün ileri mobil iletişim teknolojisi 3G ile endüstriyel otomasyon sistemlerinin izlenmesine yönelik çalışma gerçekleştirilmiştir. 3G'nin sunmuş olduğu yüksek veri transfer hızı ile birlikte mekândan bağımsız internet erişim imkânı sunması; otomasyon sisteminde tercih edilmesinde rol oynamıştır. Otomasyon sisteminin çalışmasına ve üretime yönelik veriler OPC sunucu yardımıyla PLC'den alınmış ve 3G internet bağlantısı üzerinden farklı lokasyonda bulunan veri tabanı sunucusuna gönderilmiştir. Bu veriler kullanılarak oluşturulan yazılım yardımıyla sistem ve üretim bilgileri gerçek zamanlı olarak izlenebilmiş, geriye dönük üretim raporu alınabilmiştir. Uyarı sistemiyle sistemde oluşan anormal durumlardan anında haberdar olunması sağlanmıştır. Ayrıca uzak yardım ve uzak yardım sonuç sistemiyle otomasyon sisteminde oluşan problemlerin çözülmesi kolaylaştırılmış, bir araya getirilen problem çözümleri sayesinde daha sonra oluşabilecek aynı tür problemlerin çözümü için kaynak oluşturulmuştur. Sahadan

uzakta bulunan personelin bu sistemleri kullanabilmesi 3G telefon, 3G taşınabilir bilgisayar vb. cihazlarla sağlanmıştır.

İnternet tabanlı uygulamaların endüstriyel otomasyon sistemlerinde kullanılmasında sistem ve network güvenliğinin sağlanması için gerekli araştırma yapılmış ve çalışmada uygulanmıştır.

Çalışma sonucunda 3G'nin endüstriyel otomasyon sistemlerine etkin çözümler sunduğu görülmüştür.

Anahtar Sözcükler **:** 3G, endüstriyel otomasyon sistemleri, PLC, uzak yardım, veri entegrasyonu.

Bilim Kodu **:** 902.1.063

ABSTRACT

M.Sc. Thesis

THE MONITORING OF INDUSTRIAL AUTOMATION SYSTEMS VIA THE 3G

Uğur ÖZDEMİR

Karabük University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Thesis Advisor:
Asst. Prof. Dr. İlhami Muharrem ORAK
April 2012, 79 pages

In this study, a work has been conducted in order to monitor industrial automation systems by using 3G, today's advanced mobile communication technology. It has played an important role in choosing 3G, which has high data transfer speed and providing the opportunity to access independent internet, for automation system. The data related to the production and automation system are received from PLC with the help of OPC server and it was sent to the database server located in different location via 3G internet connection. System and production information could be monitored, backward production report could be taken with the help of software which was created by considering these data. With warning system developed, It was enabled to notify instantly the abnormal situations occurred in system. In addition to that, solving of the problems occurred in automation system was made easy with remote help and remote support result system, resource was created by combining the solutions of the problems occurred in the system which can lead solving the similar

problems that may occur in later. This system is enabled for the staff who is away from the field by utilizing the equipments such as 3G phones, 3G mobile computing etc.

Necessary research was carried out and applied in the study to provide system and network security in using internet-based applications in industrial automation systems.

As a result of the study it was seen that 3G provides effective solutions for industrial automation systems.

Key Words **:** 3G, industrial automation systems, PLC, remote support, data integration.

Science Code **:** 902.1.063

TEŞEKKÜR

Bu tez çalışmasının planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmamı bilimsel temeller ışığında şekillendiren sayın hocam Yrd. Doç. Dr. İlhami Muharrem ORAK'a sonsuz teşekkürlerimi sunarım.

Destek ve dualarını üzerimden hiç eksik etmeyen sevgili aileme teşekkür ederim.

Yazılım konusunda yardımlarını eksik etmeyen arkadaşım Alperen KETHUDAOĞLU'na, tez yazımında yardımlarını esirgemeyen arkadaşım Adem BARUT'a ve desteklerini esirgemeyen tüm arkadaşlarıma teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

KISALTMALAR

1G	: Birinci Nesil
2G	: İkinci Nesil
3G	: Üçüncü Nesil
4G	: Dördüncü Nesil
3GPP	: Third Generation Partnership Project (3G Ortaklık Projesi)
8-PSK	: 8-Phase Shift Keying (8 Faz Kaydırmalı Kipleme)
AMPS	: Advanced Mobile Phone Service
ATM	: Asynchronous Transfer Mode
BTS	: Base Transceiver Station (Baz İstasyonu)
BSS	: Base Station Subsystem (Baz İstasyonu Alt Sistemi)
CA	: Carrier Aggregation (Taşıyıcı Birleştirme)
CDMA	: Code Division Multiple Access
CDMA2000	: Code Division Multiple Access 2000
CN	: Core Network (Çekirdek Şebeke)
COM	: Component Object Model
DMZ	: De-Militarized Zone
DSS	: Karar Destek Sistemleri
DCOM	: Distributed COM
DNP3	: Distributed Networking Protocol3
DECT	: Digital Enhanced Cordless Telecommunications
DCS	: Distributed Control System
DS	: Direct Sequence (Doğrudan Sıralı)
DOS	: Denial of Service
ETSI	: European Telecommunications and Standars Institute
EDGE	: Enhanced Data Rates For Global Evolution
ERP	: Kaynak Planlama Sistemi

FDD : Frequency Division Duplex

FM : Frekans Modülasyonu

FPLMTS : Future Public Land Mobile Telecommunication System

GSM : Global System for Mobile Communication

HLR : Home Location Register (Ev Konum Kütüğü)

HSCSD : High-Speed Circuit-Switched Data

HSUPA : High Speed Uplink Packet Access

HSPA : High Speed Packet Access

HMI: : Human-Machine Interface

HTTP : Hypertext Transfer Protocol

HTTPS : Secure Hypertext Transfer Protocol

IMT-2000 : International Mobile Telecommunications-2000

ITU : International Telecommunication Union

IMSI : International Mobile Subscriber Identity

IPS : Intrusion Prevention System

LAN : Local Area Network

LNS : Lucent, Nortel, Samsung

MSC : Mobile Switching Center (Mobil Anahtarlama Merkezi)

MS : Mobil İstasyon

MES : Üretim Kontrol Sistemi

NMT : Nordic Mobile Telephone

OSI : Open Systems Interconnection

OPC : OLE for Process Control

OFDMA : Orthogonal Frequency Division Multiple Access

PS : Packet Switched

PSTN : Public Switched Telephone Network

PDC : Pacific Digital Cellular

PLC : Programmable Logic Controller

RNS : Radio Network System

SSL : Secure Sockets Layer

SCADA : Supervisory Control and Data Acquisition

SC : Single Carrier (Tek Taşıyıcı)

SMS : Short Message Service

SIM	: Subscriber Identity Module
SS7	: Signalling System No7
TACS	: Total Access Communication System
TDMA	: Time Division Multiple Access
TCP/IP	: Transmission Control Protocol/Internet Protocol
TD-SCDMA	: Time Division-Synchronous Code Division Multiple Access
TDD	: Time Division Duplex
UMTS	: Universal Mobile Telecommunication System
UE	: User Equipment
UWCC	: Universal Wireless Communications Consortium
USIM	: UMTS Subscriber Identity Module
UTRAN	: UMTS Terrestrial Radio Access Network
VLR	: Visitor Location Register
VLAN	: Virtual LAN
VPN	: Virtual Private Network
QAM	: Quadrature Amplitude Modulation
QPSK	: Quadrature Phase Shift Keying (İki Kanallı Faz Kaydırmalı)
WCDMA	: Wideband Code Division Multiple Access
WAP	: Wireless Application Protocol
WRC	: World Radiocommunication Conference
WAN	: Wide Area Network
WARC	: World Administrative Radio Conference

BÖLÜM 1

GİRİŞ

Veri iletişimi gerek uygulamalar gerekse altyapı boyutlarında sürekli bir gelişme göstermektedir. Dijital veri iletimi teknolojisi hızla yaygınlaşırken buna bağlı olarak da faklı sektörlerin de beraberinde bu ağın içerisine girmesini sağlamaktadır. Bu alanlardan bir tanesi olan mobil iletişim sistemlerindeki gözle görülür gelişmeler hayatımızın birçok bölümünde yenilikler sunmaktadır. Görüntülü görüşme, mobil TV ve e-ticaret uygulamaları 3G mobil iletişim sistemlerinin getirdiği hizmetlerden bazılarıdır. Yüksek veri transfer hızı ile birlikte mekândan bağımsız olarak sürekli internet erişimi sağlaması birçok sektörde 3G'yi kullanmayı cazip hale getirmektedir. 3G; tıp sektöründe doktorların acil durumlarda hasta film (röntgen vb.) sonuçlarına bakabilmesi, gitme imkânının mümkün olmadığı yerlerdeki (köy vb.) hastaları uzaktan görüntülü görüşme imkânı ile muayene edip teşhis koyabilmesi gibi önemli faydalar sağlamaktadır. Ayrıca haber kanallarının canlı yayınları yapmasında ve servis edilecek haber bilgilerinin merkeze aktarılmasında da 3G önemli çözümler sunmaktadır.

Veri entegrasyonu ve iletişim yapısı ele alındığında çok katmanlı bir yapıya sahip olan endüstriyel otomasyon sistemlerinde de veri iletişimi önemli bir yere sahiptir. Otomasyon sisteminin izlenmesinden karar destek sistemlerinin çalışmasına kadar bütün sistem sürekli veri alışverişi içerisindedir. Gelişen ve değişen dünya pazarında rekabet edebilmek için hızlı çözümler sunabilmek ve karar destek bilgilerini oluşturabilmek gerekmektedir. Bunların gerçekleştirilmesi de veriye anında erişim sağlanarak olmaktadır. Veriye anında erişim günümüzde internet sayesinde yapılmaktadır. Fakat internetin sunduğu veriye anında erişim ve uzaktan yönetim imkânlarının yanında bazı risklerde ortaya çıkabilmektedir. İnternet üzerinden yapılan sistem ve network saldırıları sonucu üretimin aksaması, durması ve

oluşabilecek iş kazaları bunların başında gelmektedir. Bu sebeple gerekli önlemler alınarak endüstriyel otomasyon sistemlerinin güvenliği sağlanmalıdır.

Farklı lokasyonlarla veri alışverişi ve sahadan uzakta bulunan personelin internet erişim imkânı gibi gereksinimler düşünüldüğünde 3G'nin; endüstriyel otomasyon sistemin çalışmasına ve üretime yönelik verilerin farklı lokasyonlara transfer edilmesi, sahadan uzakta bulunan personelin (mühendis, yönetici vb.) otomasyon sistemini gerçek zamanlı olarak izlemesi, uyarı sistemi yardımıyla sistemden haberdar olabilmesi ve uzaktan yardım edebilmesi gibi çözümler sunması öngörülmüştür.

Çalışmada ilk olarak mobil iletişim sistemlerinin tarihsel gelişim süreci, standartları, teknik özellikleri vb. konular ele alınmıştır. Sonraki bölümde endüstriyel otomasyon sistemlerinin bölümleri, çalışma yapısı, endüstriyel iletişim, endüstriyel otomasyon sistemlerinde sistem ve network güvenliği vb. konular anlatılmıştır. 3G ile endüstriyel otomasyon sistemlerinin birlikte kullanılabilmesi için öngörülen alt yapının irdelenmesine ve buna yönelik örnek bir uygulamanın gerçekleştirilmesine sonraki bölümlerde yer verilmiştir. Son olarak çalışmada elde edilen sonuçların değerlendirilmesi gerçekleştirilmiştir.

BÖLÜM 2

MOBİL İLETİŞİM SİSTEMLERİ

Günümüzde gözle görülür ilerlemeler kaydederek gelişimine devam eden mobil iletişim sistemlerinin temeli Guglielmo Marconi'nin telsiz iletişimi ile ilgili yaptığı deneylerle başlamış[1] ve ilk adımları da 1920'li yıllarda Amerika'da bazı polis karakollarında telsiz telefonların deneme amaçlı olarak kullanılmaya başlanması ile atılmıştır. Telsiz telefonlar deniz araçlarındaki iletişime faydalar sağlamasına rağmen karasal iletişime çok fazla uygun değildi. Bu iletişim araçları büyük binalar ve diğer engel olabilecek yapıların bulunduğu şehirlerde ağır ve ihtiyaçlara yetersiz kalıyordu. Bu sebeplerden ötürü kullanımı deneme aşamasında kaldı [2].

Daha sonra 1930'lu yıllarda Frekans Modülasyonu (FM) geliştirildi. FM sistemleri İkinci Dünya Savaşı Boyunca savaş alanlarında iletişimi sağlamada kullanıldı. Bu gelişmeler barış zamanına kadar taşındı ve 1940'lı yıllarda sınırlı mobil telefon hizmetleri ile bazı büyük şehirlerde mobil telefonlar kullanılmaya başlandı. Fakat mobil telefonların günümüzdeki ticari ürünler haline gelebilmesi uzun yıllar aldı [2].

2.1. BİRİNCİ NESİL (1G) MOBİL İLETİŞİM SİSTEMLERİ

2.1.1. 1G Tarihi

Bugünkü anlamıyla bildiğimiz mobil iletişim sistemlerinin birincisi 1G (Birinci Nesil) hücresel sistemler 1978 yılında Chicago'da denenen bir sistemle başladı. Bu sistem AMPS (Advanced Mobile Phone Service) olarak bilinen 800-Mhz frekans bandına sahip bir teknoloji kullanıyordu. 1979 yılında Japonya'da, 1983 yılında da Amerika'da AMPS kullanımına başlandı. Avrupa ülkelerinde (İsveç, Danimarka, Norveç, Finlandiya) 1981 yılında NMT (Nordic Mobile Telephone) olarak bilinen ve ilk başlarda 450 MHz frekans bandına sahip daha sonraki süreçte 900 MHz frekans

bandına çıkan mobil iletişim sistemi kullanılmaya başlandı [3]. 1985 yılında ise İngilizler TACS (Total Access Communication System) olarak bilinen ve 900 MHz frekans bandında çalışan sistemleri kullanmaya başladılar. Türkiye de ise bu sistemler 1986 yılında NMT standartlarında kullanılmaya başladı. 1G'nin kullanılmaya başlanmasıyla birlikte mobil iletişim pazarı yıllık %30-50 değerinde büyüme hızı ile 1990 yılında 20 milyonluk bir kullanıcı sayısına ulaştı.

1G sistemler çok yaygın olarak kullanılmasına rağmen abone sayısının kısıtlı olması, artan taleplere cevap verememesi ve güvenlik tehditleri (dolandırıcılık vb.) gibi sebeplerden ötürü daha yeni sistemlerin aranması zorunlu hale gelmiştir.

2.1.2. 1G Sistemler

1G sistemlerin en yaygın kullanılanları aşağıda sıralanmaktadır.

1. AMPS (Advanced Mobile Phone Service)
2. NMT (Nordic Mobile Telephony)
3. TACS (Total Access Communication System)

2.1.3. 1G Sistemlerin Teknik Özellikleri

Temel analog ses iletim hizmetleri sunan 1G sistemlerde 9,6 Kbps iletim hızına sahip bir teknoloji kullanılmaktaydı. Çizelge 2.1'de 1G sistemlerin teknik özellikleri gösterilmektedir.

Çizelge 2.1. 1G sistemlerin teknik özellikleri.

Standartlar	Veri İletim Hızı	Açıklama
AMPS NMT TACS	9.6 Kbps	Analog Ses İletim Hizmeti

2.2. İKİNCİ NESİL (2G) MOBİL İLETİŞİM SİSTEMLERİ

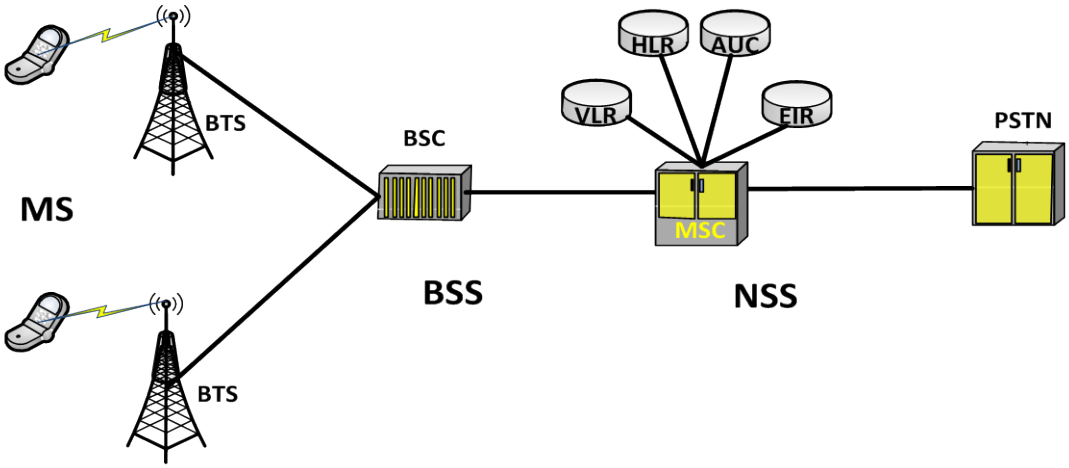
2.2.1. 2G Tarihi

2G sistemler 1990'lı yılların başlarında kullanılmaya başlanmış olup GSM (Global System for Mobile Communication), CDMA (Code Division Multiple Access) ve TDMA (Time Division Multiple Access) en yaygın kullanılan 2G sistemleridir. Türkiye de 1994 yılında ilk olarak GSM900 kullanarak bu sistemlerle tanışmıştır. 2G sistemlerin en önemli özelliği dijital olmalarıdır. Bu sebeple 1G analog sistemlerin aksine daha çok abone sayısı ve daha güvenli bir iletişim imkânı sunmaktadır. 2G sistemler kullanıcılarına günümüzde hala hizmet vermektedir. Fakat veri iletim hızının sınırlı olması ve internetin insan hayatındaki öneminin giderek artması araştırma çalışmalarını devam ettirmiştir.

2.2.2. 2G Sistemler

2.2.2.1. GSM (Global System for Mobile Communication)

Avrupa'da kullanmak amacıyla; ETSI tarafından 1990 yılında oluşturulan ve mobil haberleşme için küresel sistem anlamına gelen GSM kendi içerisinde GSM900, GSM1800, GSM1900 ve GSM400 gibi modellere sahiptir. GSM sistemler dünyanın birçok yerinde kullanılabilmektedir. Bu sistemlerde abonelerin sistem bilgilerinin bulunduğu SIM (Subscriber Identity Module) adı verilen Abone Kimlik Modül kartı cep telefonu gibi mobil istasyonların iletişim yapabilmesi için kullanılmaktadır. Şekil 2.1'de de Genel bir GSM şebekesinin bileşenleri gösterilmektedir.



Şekil 2.1. Genel GSM şebekesi.

GSM networkü SS7 (Signalling System No7) prensibine göre çalışır. Cep telefonu vb. mobil istasyonlar (MS), çağrıya uygun seviyeye sahip bir baz istasyonu (BTS-Base Transceiver Station) bulduğunda istek başlatır. Baz istasyonu alt sistemi (BSS-Base Station Subsystem), MS için iki yönlü bir işaretleşme kanalı tahsis eder ve aynı sırada mobil anahtarlama merkezi (MSC-Mobile Switching Center) ile bağlantı kurar. MSC, BSS vasıtasıyla gelen MS'ye ait Uluslararası Mobil Abone Kimliği Numara (IMSI -International Mobile Subscriber Identity) bilgisini kullanarak Ev Konum Kütüğünden(HLR-Home Location Register) bu aboneye ait bilgileri alır ve Misafir Konum Kütüğüne (VLR-Visitor Location Register) gönderir. Bu işlemden sonra MS aranan numarayı bildirir, BSS bir çağrı kanalı kurar ve MSC çağrıyı hedef abonenin bulunduğu diğer bir BSS'ye veya MSC'ye ya da arabağlantı üzerinden başka bir haberleşme şebekesine yönlendirir.

Haberleşme sırasında MS'nin bir başka hücreye geçmesi halinde aktarım (handover) işleminin gerçekleştirilmesi gerekir. Yeni hücre aynı BSC tarafından yönetiliyorsa, bu işlem BSC tarafından yapılır. MS'nin başka bir BSC tarafından hizmet verilen bir hücreye geçmesi durumunda geçiş işlemi MSC tarafından gerçekleştirilir.

Bir MS'ye çağrı gelmesi halinde ise BSC tarafından MS'nin bulunduğu hücre içerisinde işaretleşme kanalı üzerinden bir işaret gönderilir. MS'ler bu işaretleşme

kanalını sürekli olarak takip ederler. MS'nin çağrıyı kabul etmesi halinde BSC bir çağrı kanalı kurar ve haberleşme sağlanır [4].

2.2.2.2. CDMA (Code Division Multiple Access-Kod Bölmeli Çoklu Erişim)

Kod bölmeli çoklu erişim anlamına gelen CDMA'da; bir kapsama alanındaki birden fazla abone bir frekans kanalı üzerinden gönderilmektedir. Bir frekans kanalı üzerinden gönderilen sinyaller kodlama yöntemiyle bölünerek çoklu erişim sağlanmaktadır.

2.2.2.3. TDMA (Time Division Multiple Access-Zaman Bölmeli Çoklu Erişim)

Zaman bölmeli çoklu erişim anlamına gelen TDMA'da; sinyal farklı zaman aralıklarına (slot) bölünerek birden çok kullanıcının aynı frekans kanalı üzerinden iletişim kurması sağlanmaktadır. Kullanıcılar kendi zaman aralığında ardı ardına iletişim kurabilmektedirler. Böylelikle aynı kanalda birden çok istasyon kurulabilmektedir.

2.2.2.4. PDC (Pacific Digital Cellular)

PDC; Japonya'da geliştirilen bir 2G iletişim sistemidir. Temelinde zaman bölmeli çoklu erişim tekniği kullanmakta olan PDC'de birden çok kullanıcının aynı frekans kanalı üzerinden iletişim kurması sağlanmaktadır.

2.2.3. 2G Sistemlerin Teknik Özellikleri

2G sistemler sayısal ses iletim hizmeti ve devre anahtarlamalı veri iletimi özeliklerine sahiptir. Bu sistemlerde 14.4 Kbps veri iletim hızına çıkılabilmektedir ve 1G'den farklı olarak kullanıcılara SMS (Short Message Service) adı verilen kısa mesaj hizmeti sunulmaktadır. 2G sistemlerde devre anahtarlamalı veri iletim yöntemi kullanıldığından frekans kanalı dolu olduğu zaman başka kullanıcılar iletişim kuramamaktadır. İletişim kurulabilmesi için frekans kanalında yer açılması gerekmektedir. Çizelge 2.2'de 2G sistemlerin teknik özellikleri gösterilmektedir.

Çizelge 2.2. 2G sistemlerinin teknik özellikleri.

Sistem Adı	Veri İletim Hızı	Frekans Kanalı	Açıklama
GSM	9.6/14.4 Kbps	200 KHz	Dijital Ses İletim Hizmeti, Devre Anahtarlamalı veri İletimi, SMS
CDMA	9.6/14.4 Kbps	1.25 MHz	Dijital Ses İletim Hizmeti, Devre Anahtarlamalı veri İletimi, SMS
TDMA	9.6 Kbps	30 KHz	Dijital Ses İletim Hizmeti, Devre Anahtarlamalı veri İletimi, SMS
PDC	9.6 Kbps	25 KHz	Dijital Ses İletim Hizmeti, Devre Anahtarlamalı veri İletimi, SMS

2.3. 2.5G MOBİL İLETİŞİM SİSTEMLERİ

2.3.1. 2.5G Tarihi

2G sistemlerin eksikliklerini gidermek amacıyla yapılan çalışmalar neticesinde 1990'ların sonlarında 2G'ye göre daha hızlı veri iletimine imkân veren 2.5G olarak adlandırılan sistemler kullanılmaya başlandı. HSCSD (High-Speed Circuit-Switched Data), GPRS (General Packet Radio Services), EDGE (Enhanced Data Rates For Global Evolution) sistemleri bu gelişim sürecinde ortaya çıkan 2.5G sistemleridir. Türkiye'de 2000 yılında HSCSD sistemler ile bu sistemleri kullanmaya başlamıştır. 2.5G; 2G ile 3G (Üçüncü Nesil) sistemler arasında bir geçiş basamağı olarak kabul edilmektedir.

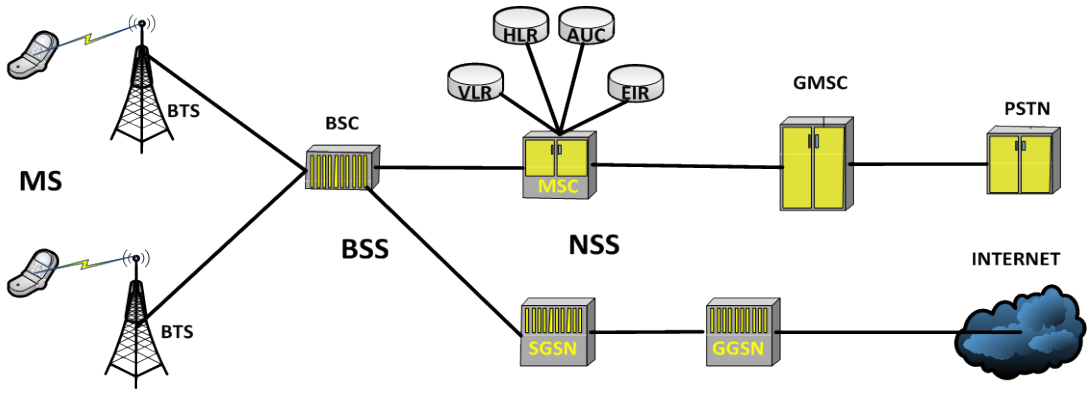
2.3.2. 2.5G Sistemler

2.3.2.1. HSCSD (High-Speed Circuit-Switched Data)

Yüksek hızlı devre anahtarlamalı veri anlamına gelen HSCSD kullanılan sistemlerde dört kanallı veri iletimi yapılabilmektedir. Veri iletiminde dört kanal kullanıldığından 2G sistemlerdeki devre anahtarlamalı sistemlere göre dört kat daha hızlı veri iletim (57.6 Kbps (4x14.4 Kbps)) hızına çıkılabilmektedir [3]. Bu sistemlerde devre anahtarlamalı olduğu için kanallar dolu olduğunda başka veriler bu işlem bitene kadar gönderilememektedir.

2.3.2.2. GPRS (General Packet Radio Services)

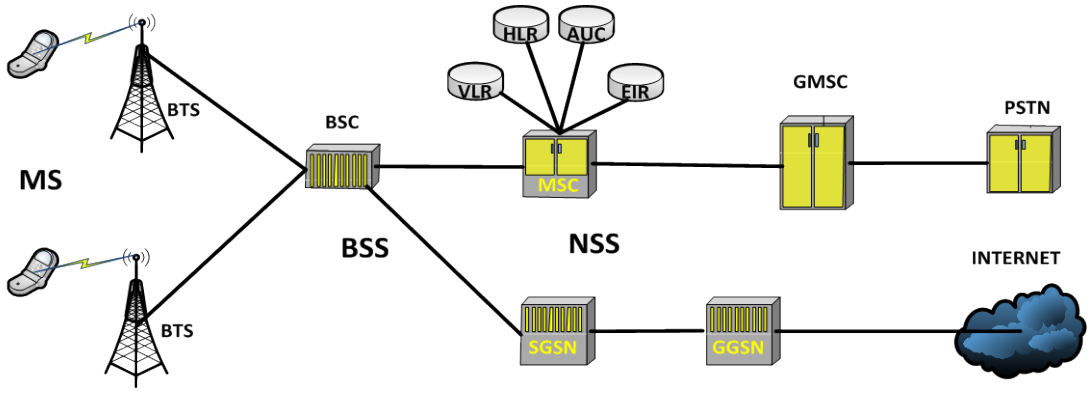
İnternet ve telsiz şebekelerinin birbirine erişimini sağlayan ve kullanıcılara noktadan noktaya veri iletişim imkânı sağlayan 2.5G sistemidir. Genel paket telsiz hizmetlerinde veri iletimi her biri 21.4 Kbps veri iletim hızına çıkabilen 8 kanalla toplam 171.2 Kbps veri iletim hızına teorik olarak çıkılabilmektedir. Paket anahtarlama yöntemi kullanan bu sistemlerde veriler parçalara ayrılarak gönderildiğinden aynı anda birden çok veri daha hızlı bir şekilde gönderilebilmektedir. Bu sistemlerde ücretlendirme kullanılan veri miktarına göre yapılmaktadır. Şekil 2.2.'de GPRS network mimarisi gösterilmektedir.



Şekil 2.2. GPRS network mimarisi.

2.3.2.3. EDGE (Enhanced Data Rates For Global Evolution)

Küresel evrim için geliştirilmiş veri hızları anlamına gelen EDGE sistemlerde her biri 48 Kbps veri iletim hızına çıkabilen 8 kanalla toplam 384 Kbps veri iletim hızına teorik olarak çıkılabilmektedir. EDGE sistemlerde; GSM sistemlerinde kullanılan Gauss Önsüzmeli Asgari Kaydırmalı Kipleme (GMSK-Gaussian Prefiltered Minimum Shift Keying) modülasyonundan daha büyük bant genişliği imkanı sunan bir modulasyon metodu olan 8 Faz Kaydırmalı Kipleme (8-Phase Shift Keying, 8-PSK) metodu kullanıldığından GPRS'ten daha hızlı bir veri iletim hızı sunulmaktadır. Baz istasyonlarında yapılacak bazı işlemler neticesinde GPRS ile aynı altyapıyı kullanmaları mümkün olmaktadır. Şekil 2.3.'de EDGE ve GPRS kullanan bir GSM şebekesi gösterilmektedir.



Şekil 2.3. EDGE ve GPRS kullanan bir GSM şebekesi.

2.3.3. 2.5G Sistemlerin Teknik Özellikleri

2.5G sistemlerin teknik özellikleri Çizelge 2.3'te gösterilmektedir.

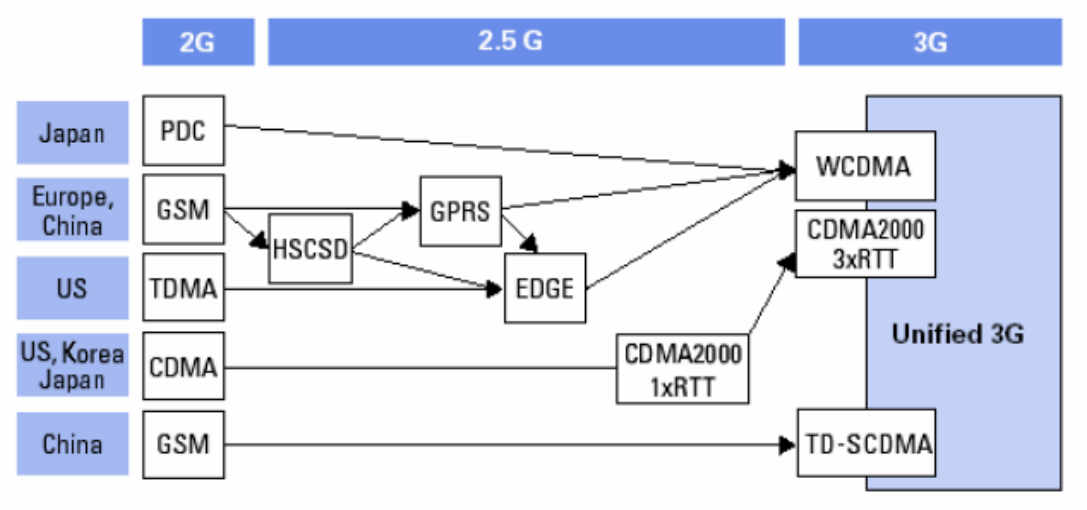
Çizelge 2.3. 2.5G sistemlerin teknik özellikleri.

Sistem Adı	Veri İletim Hızı (Teorik)	Frekans Kanalı	Açıklama
HSCSD	57.6 Kbps	200 KHz	Dijital Ses İletim Hizmeti, Devre Anahtarlamalı veri İletimi, SMS
GPRS	171,2 Kbps	200 KHz	Dijital Ses İletim Hizmeti, Devre/Paket Anahtarlamalı veri İletimi, SMS
EDGE	384 Kbps	200 KHz	Dijital Ses İletim Hizmeti, Devre/Paket Anahtarlamalı veri İletimi

2.4. ÜÇÜNCÜ NESİL (3G) MOBİL İLETİŞİM SİSTEMLERİ

2.4.1. 3G Tarihi

İlk olarak ITU (Internetional Telecomunication Union) tarafından 1986 yılında çalışmaları başlatıldı. 1992 yılında WARC (World Administrative Radio Conference-Dünya Yönetimsel Telsiz Konferansı) 3G mobil sistemleri için ilk 3G spektrumunu belirledi. Bu spektruma göre 1885-2025 MHz ile 2110-2200 MHz frekans bantları 3G mobil sistemler için ayrıldı. İlk olarak Japonya'da 2001 yılında kullanılmaya başlandı. 2002 yılında Amerika'da, 2003 yılında da Avrupa'da yayılmaya başladı. Türkiye'de ise 2008 yılında yapılan Üçüncü nesil (3G) mobil iletişim sistemi kurulmasına ilişkin ihale sonucunda 3 tip lisans (A, B, C lisansları servis sağlayıcılarına sırasıyla 45MHz, 35MHz ve 30MHz frekans bandı kullanma izni veriyordu.) sırasıyla Turkcell, Vodafone, Avea şirketlerine verildi. 2009 yılında hazırlıkları tamamlanan WCDMA standardında kullanılmaya başlandı. Dünya'da 3G'ye geçişteki süreç Şekil 2.4'te gösterilmektedir.



Şekil 2.4. Dünyada 3G'ye geçişteki süreç [5].

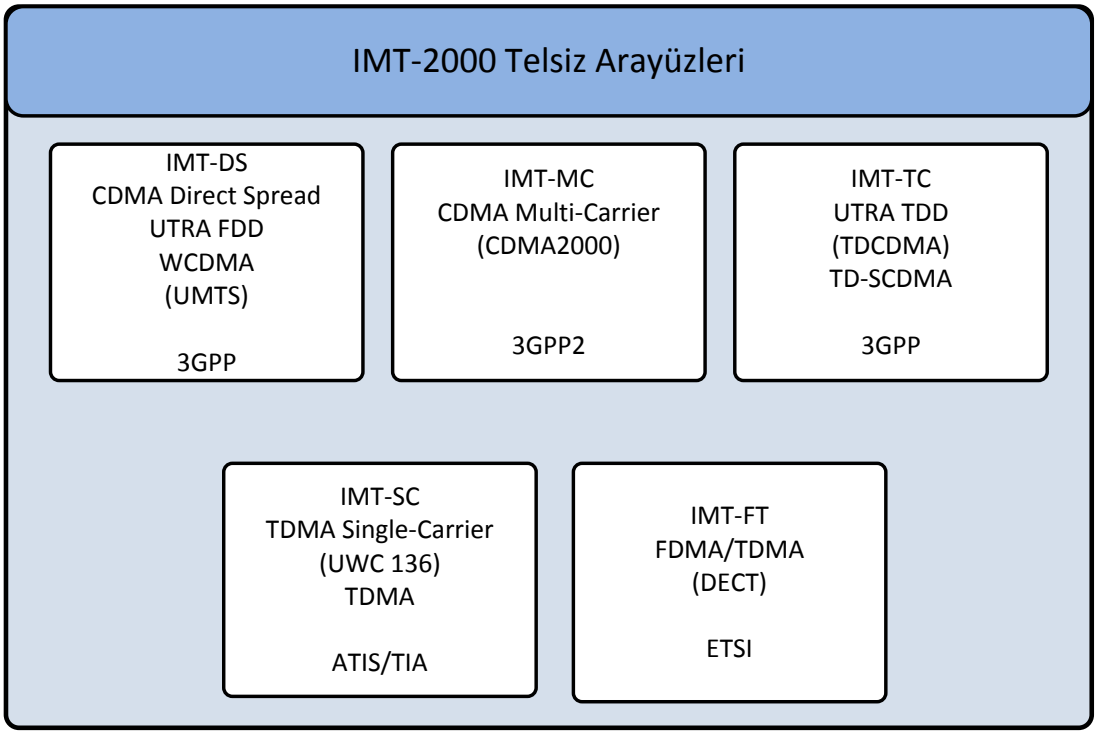
2.4.2. 3G Sistemler

Daha iyi ses kalitesi, daha yüksek kapasite, internet erişimi ve yüksek hızlı data paketleri, multimedya uygulamalar gibi özellikleri içeren uluslar arası 3G standartları ITU tarafından Uluslararası Mobil Haberleşme (International Mobile Telecommunications, IMT2000) adı altında kabul edildi. Bu uluslararası 3G standartlarının amacı kullanıcılara dünya çapında kapsama alanı ve birden çok hücresel networkte konuşma imkânı sağlamaktı. IMT2000; yüksek hızda multimedya dataları ve aynı zamanda ses hizmetlerinin tüm dünyada teslim edilmesini hedefleyen 3G kablosuz telefon standartlarının çerçevesidir. ITU IMT2000'de bir dizi standardı sağlamayı gerekli kılmıştır. Bunlar; sistem kapasitesi ve spektrumun etkinliğini geliştirmek, mobil (hareketli) durumlarda minimum veri hızı oranı 144 Kbps (tercih edilen 384 Kbps) sağlamak ve sabit mekânlarda minimum 2048 Kbps veri hızlarını sağlamaktı [4]. Önceleri Gelecek Kamu Karasal Mobil Haberleşme Sistemi (Future Public Land Mobile Telecommunication System, FPLMTS) olarak bilinen IMT-2000; WCDMA ve CDMA2000 gibi data hızlarını arttıran çeşitli standartlara sahiptir.

IMT2000 içerisindeki bu standartlar 3G Ortaklık Projesi (3rd Generation Partnership Project, 3GGP) ve 3GPP2 tarafından geliştirildi. 1998 yılında, ETSI (Avrupa), TTC (Japonya), ARIB (Japonya), TTA (Güney Kore), ATIS (ABD) standart geliştirme

kuruluşları GSM sistemlerinin teknik özelliklerini geliştirmek amacıyla 3GGP'yi başlattı. Bu projeye 1999 yılında CCSA (Çin)'da katıldı [3]. 3GPP'nin IMT2000 için teklif ettiği standartlardan ilki UTRA FDD'dir. UTRA FDD; WCDMA ya da Doğrudan Sıralı (Direct Sequence, DS) CDMA olarak da tanımlanmaktadır. 3GPP'nin ikinci teklifi de UTRA TDD'dir.

3GPP'ye paralel olarak 1999'da GSM olmayan sistemlerin geliştirilmesi için başka bir partnerlik projesi daha oluşturuldu. 3GPP2 adı verilen bu partnerlik projesinin amacı CDMA2000 3G sistemlerinin teknik özelliklerini geliştirmekti. CDMA2000 IS-95 standartlarının temelini oluşturan 2G CDMA sistemlerinden geliştirilmiş 3G sistemlerdir. Bu projenin partnerleri TIA (ABD), ARIB (Japonya), CCSA (Çin), TTA (Güney Kore), TTC (Japonya), standart geliştirme kuruluşlarıydı [1]. Şekil 2.5'te IMT2000 Telsiz Ara yüzleri ve bu ara yüzleri geliştiren kuruluşlar gösterilmektedir.



Şekil 2.5. IMT2000 telsiz ara yüzleri ve geliştiren kuruluşlar.

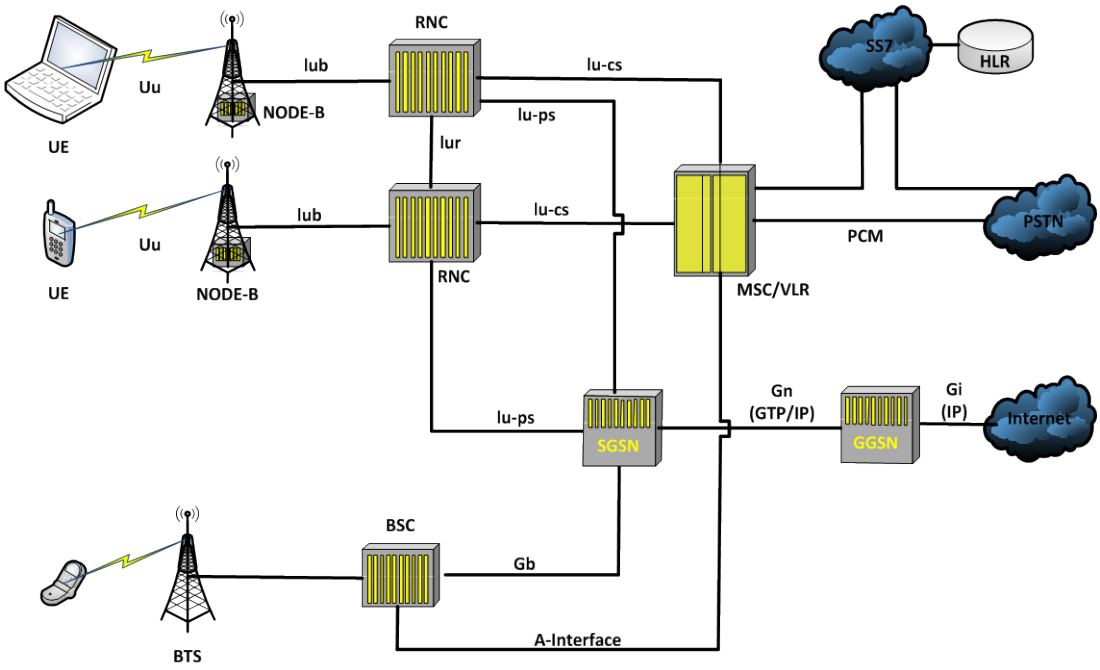
2.4.2.1. UMTS (Universal Mobile Telecommunication System-Evrensel Gezgin İletişim Sistemi)

UMTS; kullanıcı terminali (UE-User Equipment), telsiz erişim şebekesi (UTRAN) ve çekirdek şebeke (CN-Core Network) olmak üzere üç temel öğeden oluşmaktadır. UMTS'de UE; GSM, GPRS ve EDGE sistemlerinde kullanılan SIM kartla çalışan terminal cihazlarından farklıdır. UE; USIM (UMTS Subscriber Identity Module) adı verilen kartla çalışır.

UTRAN, bir veya daha fazla RNS'ten (Radio Network System) oluşmaktadır. Her bir RNS ise bir adet RNC (GSM'deki BSC (Base Station Controller)'e eşdeğer) ve bu RNC'ye bağlı Node-B'lerden (baz istasyonlarına (GSM'deki Base Transceiver Station)'e eşdeğer)) oluşmaktadır. UTRAN telsiz arayüzünü diğer şebekelerden farklı kılan taraf, 2 adet farklı, fakat birbirini tamamlayan telsiz erişim modu içermesidir [6]. Bunlar; UTRA FDD, UTRA TDD'dir. FDD (Frequency Division Duplex) modu tamamen WCDMA tabanlıdır. TDD (Time Division Duplex) modunda ise ilave olarak bir TDMA kısmı mevcuttur. UTRA FDD'de, aboneye doğru ve baz istasyonuna doğru olmak üzere iki ayrı frekans bandı kullanılmaktadır. Telsiz erişim tekniği 3,84 Mc/s yonga hızında ve 5 MHz bant genişliğinde veri iletimine sahip doğrudan sıralı CDMA niteliğindedir. Modülasyon tekniği, iki kanallı Faz Kaydırmalı (Quadrature Phase Shift Keying, QPSK)'dır. UTRA TDD'nin Zaman Kodlu IMT (International Mobile Telecommunications Time Code, IMT-TC) ve doğrudan sıralı CDMA olmak üzere iki sürümü bulunmaktadır. IMT-TC 3,84 Mc/s yonga hızına ve 5 MHz bant genişliğine sahiptir. Doğrudan sıralı CDMA'da ise 1.28 Mc/s yonga hızı ve 1.6 MHz bant genişliğine sahiptir ve Zaman Bölmeli Eşzamanlı CDMA (Time Division Synchronous CDMA, TDSCDMA) olarakta bilinmektedir. TDD sistemleri tekli spektrum bölümleri üzerinden çalışabilmektedir. Evrensel Telsiz Haberleşme Konsorsiyumu (Universal Wireless Communications Consortium, UWCC)'nin tek taşıyıcılı (Single Carrier, SC) UWC-136 arayüzü, TIA/EIA-136 ve GSM GPRS teknolojilerinin birbirlerine yaklaştırılması ve TIA/EIA-136 teknolojisinin 3G yeteneklerine yükseltilebilmesi amacıyla TIA'nın öncülüğünde geliştirilmiştir. Bu amaçla 30 kHz kanallarının ses ve veri kapasiteleri

artırılmış, yüksek gezginlik uygulamalarında 384 Kbps için 200 kHz taşıyıcı, düşük gezginlik uygulamalarında ise 2 Mbps için 1,6 MHz taşıyıcı eklenmiştir [4].

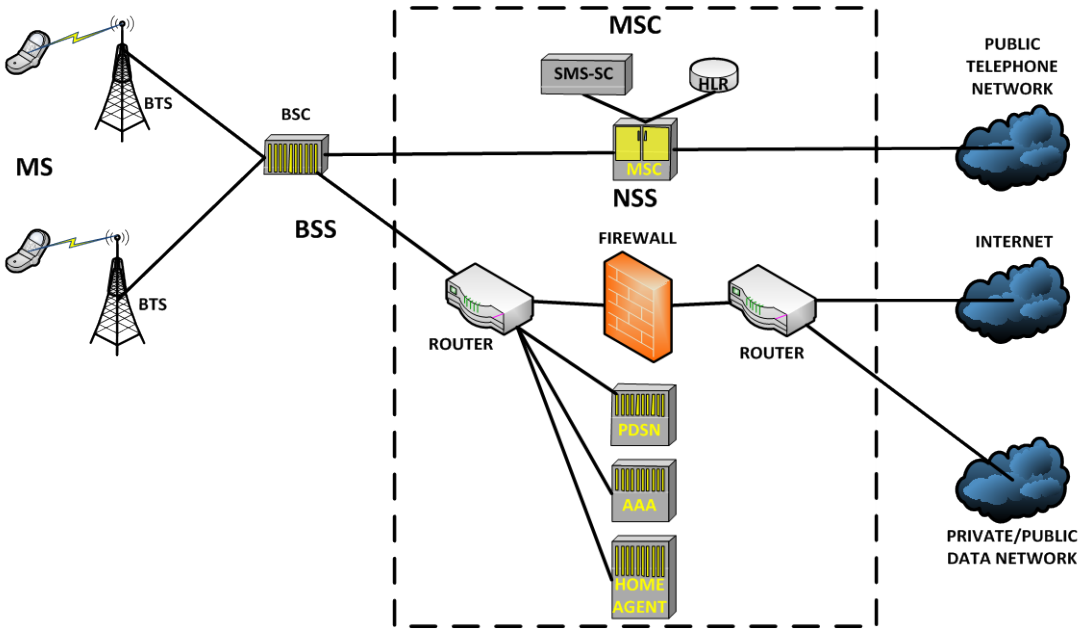
UMTS'de, 2G sistemlerden farklı olarak "Uu","Iub", "Iur" ve "Iu" isimli dört yeni arabirim tanımlamaktadır. "Uu" arabirimi kullanıcı terminaliyle Node-B arasında bağlantıyı sağlamaktadır. "Iub" arabirimi Node-B ile RNC arasındaki bağlantıyı sağlamaktadır. "lub" arabirimi tamamen standartlaştırılmış olduğundan bir Node-B'den farklı satıcının RNC'sine bağlanmak mümkün olmaktadır. "Iur" arayüzü farklı RNC'lerdeki Node-B'ler arasında yumuşak bir geçiş sağlamak amacıyla RNC'ler arasında kullanılmaktadır. Diğer arayüzlerin aksine "Iur" arayüzünün GSM'de benzer bir karşılığı yoktur. "Iu" arayüzü telsiz erişim şebekesi (UTRAN) ile Çekirdek şebeke (CN) arasındaki bağlantıyı sağlamaktadır. RNC ile MSC arasını bağlayana "lu-cs" (devre anahtarlamalı), RNC ile SGSN arasını bağlayana ise "lu-ps" (paket anahtarlamalı) denilmektedir. "Iub", "Iur" ve "Iu" arayüzlerinde veri hızı oranları birbirinden değişken olan paket anahtarlamalı ve devre anahtarlamalı sistemler arasında uyumlu olarak çalışabilen ATM (Asynchronous Transfer Mode) kullanılmaktadır. UMTS Release1999 şebeke mimarisi Şekil 2.6'da gösterilmektedir.



Şekil 2.6. UMTS release1999 şebeke mimarisi.

2.4.2.2. CDMA2000 (Kod Bölmeli Çoklu Erişim-2000)

CDMA2000 IS-95A/B ve J-STD-008 standartlarını kullanan CDMAone kablosuz telefon sistemlerinin genişletilmiş halidir. WCDMA'da olduğu gibi aynı ortamda eş zamanlı iletişim (duplexing) için FDD kullanılır. Farklı olarak CDMA2000'de 3.75 MHz band genişliği kullanılıp, chip hızı da 3,6864 Mcps dır. Cdma2000 ve W-CDMA birbiriyle uyumsuz sistemlerdir. CDMA2000 taşıyıcısı, daha hızlı chip hızına sahip tek bir 3.75 MHz taşıyıcısı gibi kullanılmak üzere bir araya getirilmiş üç standart 1,25 MHz taşıyıcıların toplamından oluşur. Üç taşıyıcının kullanılma nedeni, toplamlarından oluşan band genişliğinin IMT-2000 için istenen 2 Mbps hız ihtiyacını karşılıyor olmasıdır. Bununla birlikte, kullanıcılardan gelen talepler doğrultusunda 1'den 12'ye kadar sayısı artırılabilen 1,25 MHz'lik kanalların kullanımı ile kanal genişliğini 15 MHz'e kadar çıkarmak mümkündür [6]. CDMA2000 şebeke mimarisi Şekil 2.7'de gösterilmektedir.



Şekil 2.7. CDMA2000 şebeke mimarisi.

2.4.2.3. TD-SCDMA (Time Division-Synchronous Code Division Multiple Access-Zaman bölmeli-Eş Zamanlı Kod Bölmeli Çoklu Erişim)

3GPP çalışmalarının başında Çin tarafından geliştirilen 3G temelli TD-SCDMA; ilerleyen zamanlarda 3GPP Release4 içerisine ilave bir TDD mode olarak koyuldu.

2.4.2.4. DECT (Digital Enhanced Cordless Telecommunications-Sayısal Gelişmiş Kablosuz Telekomünikasyon)

Sayısal Geliştirilmiş Kablosuz Telekomünikasyon olarak bilinen DECT sistemler ETSI standartlarındaki bileşik FDMA/TDMA tekniğini kullanmaktadır.

2.4.3. 3G Sistemlerin Teknik Özellikleri

3G sistemlerin teknik özellikleri Çizelge 2.4'te gösterilmektedir.

Çizelge 2.4. 3G sistemlerin teknik özellikleri.

Sistem	Veri İletim Hızı	Açıklama
UMTS/CDMA2000	144Kbps (Hareketli Minimum) 384Kbps (Hareketli Maksimum) 2Mbps (Az Hareketli)	Paket Anahtarlamalı Veri Yüksek Hızda Görüntü Aktarımı IP Tabanlı Uygulamalar

2.5. 3.5G/4G MOBİL İLETİŞİM SİSTEMLERİ

2.5.1. 3.5G/4G Tarihi

3G sistemler günümüzde yaygın olarak kullanılmaktadır. Fakat 3GPP, 3GPP2 ve IEEE kuruluşları mobil iletişim sistemleri üzerindeki çalışmalarına hız kesmeden

devam etmektedir. Bu kuruluşların geliştirdiği HSDPA, HSPA, HSPA+, LTE, IEEE 802.20, WiMAX (IEEE802.16e), EV-DO vb. teknolojiler 3G'den 4G'ye geçişte ara basamak olarak kabul edilmektedir ve 3.5G olarak adlandırılmaktadır. 2002 yılında HSDPA ile gelişimi başlayan 3.5G sistemler 2005 yılında hedefleri tanımlanan LTE sistemler ile 4G öncesi son adım olarak kabul edilmektedir. 2008 yılında çalışmaları başlayan LTE-Advanced (Release 10 ve sonrası) teknolojisi ve yeni nesil WiMAX teknolojileride 4G sistemler olarak günümüzde yerini almaktadır. 3.5G sistemler yaygın bir şekilde kullanılmasına rağmen dünyada şu anda 4G hizmeti sunan 49 tane ticari şebeke ve 4G testlerini yapan 285 tane şebeke bulunmaktadır. 4G ile şu anda 150-300 megabit arasındaki hızlar şebeke teknolojileri için hazır durumda bulunmaktadır. 2015'ten sonra LTE teknolojisiyle 600 Mbps ve 1 Gbps'e ulaşılması beklenmektedir [7].

2.5.2. 3.5G/4G Sistemler

2.5.2.1. HSDPA (High Speed Downlink Packet Access)

3GPP Release 5'te HSDPA adı verilen şebekeden kullanıcıya doğru yüksek hızda paket erişimi sağlayan bir sistemdir. Bu sistemde kullanılan QAM (Quadrature Amplitude Modulation) modülasyon tekniği ile 10Mbps veri iletim hızlarına çıkılabilmektedir.

2.5.2.2. HSUPA (High Speed Uplink Packet Access)

3GPP Release 6'da ise HSUPA adı verilen kullanıcıdan şebekeye doğru yüksek hızda paket gönderebilen bir sistem sunulmaktadır.

2.5.2.3. HSPA (High Speed Packet Access)

3GPP Release 7'de HSDPA ve HSUPA'nın özelliklerinin bir araya getirildiği ve 14.4 Mbps veri hızına kadar çıkabilen bir sistemdir.

2.5.2.4. HSPA+

HSPA'dan sonra eklenen özelliklerin oluşturduğu sistemdir. 42.0 Mbps download hızı ve 5.8 Mbps upload hızına 3G sistemleri üzerinden erişilebilmektedir. Günümüzde çoklu taşıyıcılı sistemler kullanılarak birden çok frekans kanalı üzerinden veriler taşınıp download ve upload hızları daha yüksek hızlara çıkarılabilmektedir.

2.5.2.5. 3G-LTE (Long-Term Evolution)

2005 yılında 3GPP LTE hedeflerini tanımladı. Bu hedefler aşağıdaki gibidir:

1. 1.25-20 MHz arasındaki Frekans bandı
2. 20Mhz frekans değerinde 100Mbps download hızı ve 50Mbps upload hızı
3. 3G ve LTE arasında iletişim
4. Mevcut UMTS sistemler ile uyumluluk
5. Bir hücrede bulunan minimum 200 aktif kullanıcı için 5MHz'lik bant genişliği
6. 350 km/h hızlara kadar sorunsuz çalışma
7. Bazı yerlerde 20ms kadar küçük bir gecikme süresi

LTE (Release 8)'de OFDMA (Orthogonal Frequency Division Multiple Access) erişim yöntemi kullanılmaktadır. 1.4, 3, 5, 10, 15 ve 20 MHz kadar frekans bantları üzerinden çoklu iletimi desteklemektedir. SU-MIMO (Single User MIMO) Multiplexing özelliği downlink tarafında 4 katmanlı bir çoklama yapılabilmektedir. Uplink tarafında MIMO Multiplexing desteklenmemektedir [8].

2.5.2.6. EV-DO Revision C

CDMA2000 standardını geliştirmek amaçlı bir araya gelen Nokia, Qualcomm ve LNS (Lucent, Nortel, Samsung) şirketlerinin üzerinde çalıştığı sistemdir. TDD veya FDD modda 1.25 MHz-20MHz aralığında bant genişliği kullanmayı hedefler. 20 MHz frekans bandı için 75 Mbps veri hızı ve 150-200 Mbps tepe değerdeki veri hızına çıkmayı hedefler.

2.5.2.7. IEEE 802.20

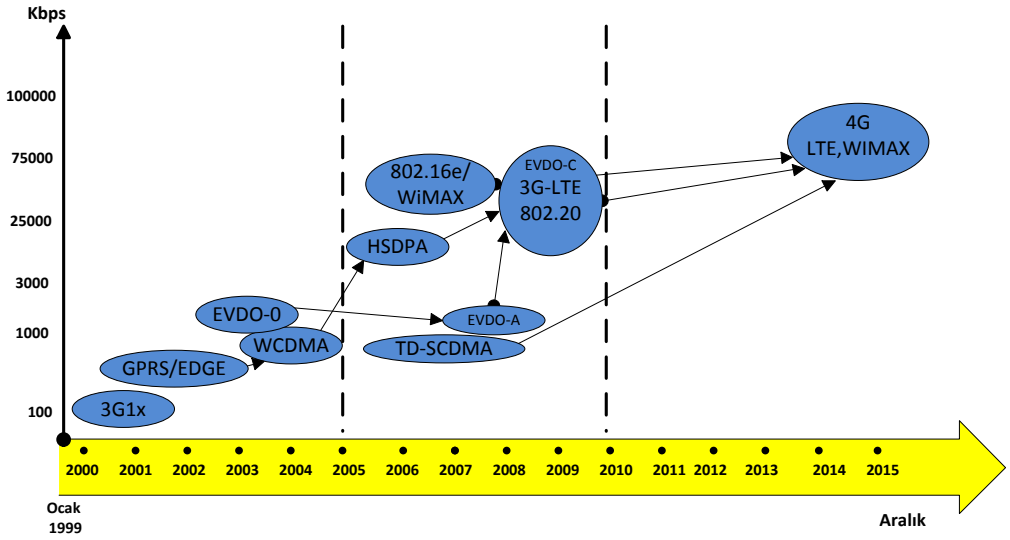
IEEE 802.16e sistemi ile EV-DO sistemini bir araya getiren bir sistemdir. Frekans bandı 5-20 MHz arasında değişebilmektedir. 20MHz frekans bandında tepe değeri olarak 130 Mbps veri hızı değerinin üzerine çıkabilmektedir.

2.5.2.8. Wimax (IEEE 802.16e)

Worldwide Interoperability for Microwave Access kelimelerinin kısaltması olan WiMAX teknolojisi sabit, taşınabilir ve mobil erişimleri destekleyen bir geniş bant kablosuz erişim teknolojisidir. Görüş hattında olan veya olmayan, noktadan noktaya, noktadan çok noktaya ve çok noktadan çok noktaya uygulamaları desteklemektedir. İdeal şartlarda 50 km'lik kapsama alanı içerisinde 75 Mbps hızlarda ses, veri ve görüntüyü hizmet kalitesi ve güvenlik gerekliliklerinde taşıyıp dağıtabilmektedir. 2.5GHz ve 3.5GHz frekansının lisanslı kullanıma; 5.8GHz frekansının ise lisanssız kullanıma tahsis edildiği söylenebilir [9].

2.5.2.9. 4G-LTE (Advanced)

2008 yılında 3GPP tarafından çalışmaları başlatılan LTE (Advanced) sistemler daha önceki LTE sistemlerin (Release 8,9) özelliklerine sahip olmakla beraber taşıyıcı birleştirme (carrier aggregation-CA) ve geliştirilmiş anten desteği gibi önemli yeni özelliklere de sahiptir. OFDMA erişim tekniği kullanan bu sistemler 1.4 MHz'den 20 MHz'e kadar frekans bantlarını kullanabilmektedirler. 5'li taşıyıcıya kadar çıkabilen bu sistemlerde CA özelliği ile 100 MHz'e kadar taşıma bant genişliğini arttırabilmektedir. Bu özellik ile 1Gbps download hızı ve 500Gbps upload tepe hızlarına çıkılması beklenmektedir. LTE (Advanced) MIMO (multiple-input multiple-output) iletim özelliği de geliştirilmiştir. SU-MIMO Multiplexing özelliğinde downlink tarafında 8 katmanlı, uplink tarafında 4 katmanlı bir çoklama yapılabilmektedir [8]. Şekil 2.8'de 4G'ye giden yolda sistemler ve veri iletim hızları arasındaki ilişki gösterilmektedir.



Şekil 2.8. 4G'ye giden yolda sistemler ve veri iletim hızları arasındaki ilişki.

2.5.3. 3.5G/4G Sistemlerin Teknik Özellikleri

3.5G/4G sistemlerin teknik özellikleri Çizelge 2.5'te gösterilmektedir.

Çizelge 2.5. 3.5G/4G teknik özellikleri.

Sistem Adı	Kuruluş Adı/Nesil Adı	Veri İletim Hızı (Teorik)	Açıklama
HSPA	3GPP/3.5G	14.4Mbps (Download) 5.8Mbps (Upload)	Yüksek Hızda Görüntü Aktarımı, IP Tabanlı Uygulamalar, Paket Anahtarlamalı Veri
HSPA+	3GPP/3.5G	42Mbps (Download) 5.8Mbps (Upload)	
3G-LTE	3GPP/3.5G	100Mbps (Download) 50Mbps (Upload)	
EVDO Revision-B	3GPP2/3.5G	75Mbps (Download)	
IEEE 802.20	IEEE/3.5G	130Mbps (Download)	
WiMAX (IEEE 802.16e)	IEEE/3.5G	75Mbps (Download)	
4G-LTE (Advanced)	3GPP/4G	1Gbps (Download) 500Mbps (Upload)	

BÖLÜM 3

ENDÜSTRİYEL OTOMASYON SİSTEMLERİ

3.1. GENEL BİR BAKIŞ

Endüstriyel sistemler gerçekleştirilen işlemlere göre yatayda ve fonksiyonel işlevler konusunda da dikeyde olmak üzere iki farklı sınıflandırma ile değerlendirilebilir. Tek bir sitemi ele aldığımızda geleneksel yaklaşımda endüstriyel otomasyon kavramının dar bir çerçevede ele alındığını görmekteyiz. Bu çerçeve sadece mekanik sistemin kumandası ile sınırlı kalmaktadır.

Günümüzdeki teknolojik gelişmeler ışığında dijital fabrika kavramı endüstriyel sistemlerde etkin bir alan oluşturmuştur. Sistemlerin sadece bir kısmının değerlendirilmesi ile yetinmeyip bütünün iletişim içerisinde olduğu bir çerçevede algılanması gerektiği ortaya konulmuştur.

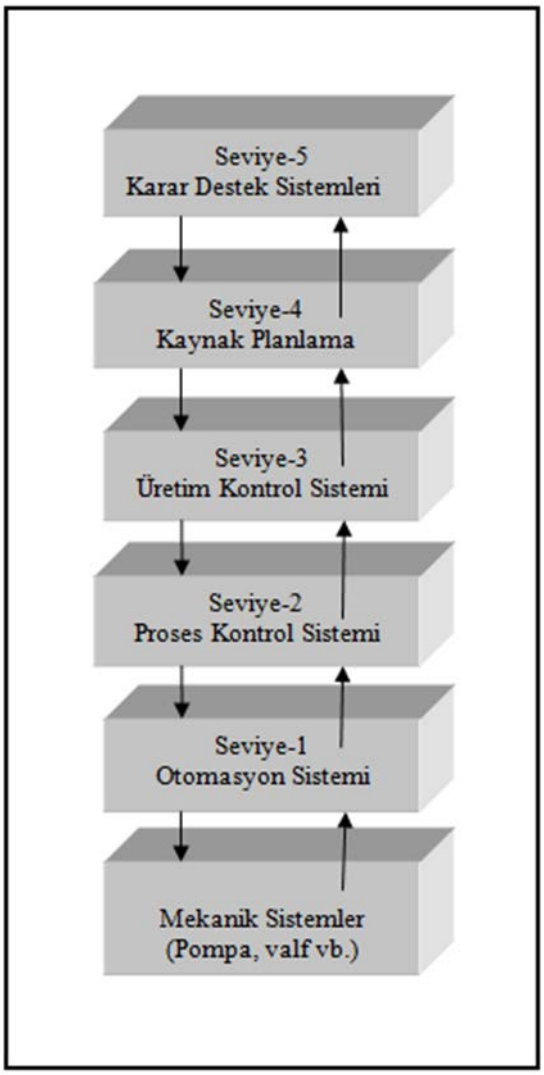
Veri entegrasyonunu ve iletişim yapısını referans alarak değişik katmanlarda endüstriyel sistemlerin sınıflandırılması mümkün olmaktadır.

3.2. BÖLÜMLERİ VE GENEL ÇALIŞMASI

Endüstriyel otomasyon sistemleri genel olarak altı katmanda sınıflandırılabilir. Şekil 3.1'de endüstriyel otomasyon sistemlerinin katmanları gösterilmektedir.

1. Seviye-0: Mekanik ve Elektrik Sistemler
2. Seviye-1: Otomasyon Sistemleri
3. Seviye-2: Proses Kontrol Sistemleri
4. Seviye-3: Üretim Kontrol Sistemleri
5. Seviye-4: Kaynak Planlama Sistemleri

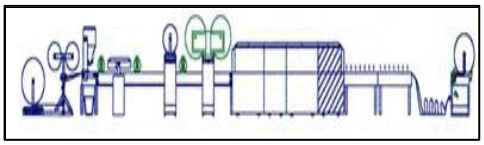
6. Seviye-5: Karar Destek Sistemleri



Şekil 3.1. Endüstriyel otomasyon sistemlerinin katmanları.

3.2.1. Seviye-0: Mekanik ve Elektrik Sistemler

Üretimin yapılabilmesi için gerekli makinelerin ve mekanik elemanların (Motor, valf, pompa, yürüyen bant vb.) bulunduğu bölümdür. Sistemin çekirdeğini oluşturur. Bütün sistem bu yapıya göre şekillendirilir. Kontrol edilecek sistemler bu katmanda yer almaktadır. Bu kısımda elde edilen elektriksel veriler alınarak üst katmanlarda değerlendirilir. Şekil 3.2'de örnek bir mekanik sistem gösterilmektedir.



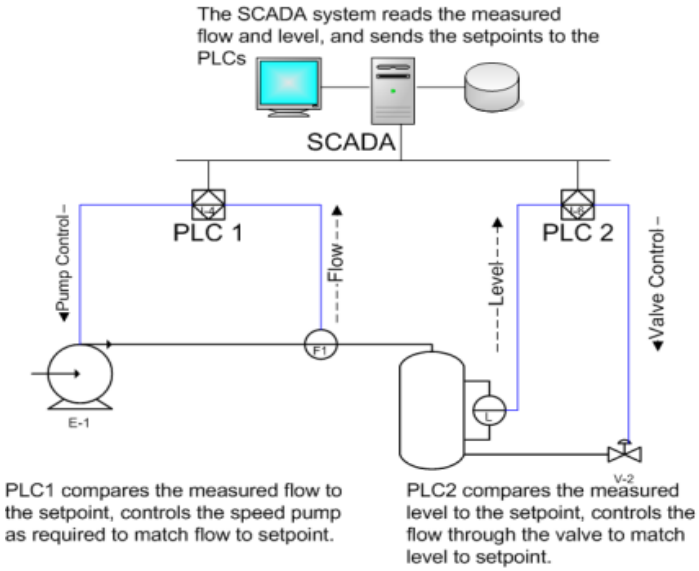
Şekil 3.2. Örnek bir mekanik sistem.

3.2.2. Seviye-1: Otomasyon Sistemleri

Mekanik sistemlerin kontrol ve kumandası için otomasyon sistemi olarak adlandırılan PLC (Programmable Logic Controller), DCS (Distributed Control System) ve SCADA (Supervisory Control and Data Acquisition) sistemleri kullanılırlar. Sistemin uzaktan izlenmesini ve sistem parametrelerinin kontrolünü mümkün kılan Scada sisteminin temelleri 1932 yılında Automatic Electric Company'nin uzaktan kontrol ürünlerinden yola çıkarak atıldı. 1960'ların sonlarında bilgisayar tabanlı sistemlerin kullanılmaya başlanması ve 1971 yılında Intel 4004 serisi mikroişlemcilerin çıkmasıyla birlikte bilgisayar tabanlı Scada sistemlerinin gelişimi devam etmiş günümüzde de hala devam etmektedir [10]. Günümüz otomasyon sistemlerinde yönetim, kontrol, veri entegrasyonu vb. görevleri yerine getirmede kullanılan Scada, PLC, OPC sistemlerinden aşağıda bahsedilmektedir.

3.2.2.1. SCADA (Supervisory Control and Data Acquisition)

Bir fabrikada veya işletmede kullanılan tüm ekipmanların otomatik kontrolü ve gözlenmesini sağlayan sistemdir. SCADA, mekanik sistemlerden sensörler, transducerlar vb. elektronik devre elemanları yardımıyla bilgi toplar ve bu bilgiler ışığında kontrol programları yardımıyla merkezi birime geri aktarır mekanik sistemlerin hedeflendiği gibi çalışmasını sağlar. Örnek bir scada sistemi Şekil 3.3'te gösterilmektedir. HMI (Human-Machine Interface) adı verilen kullanıcı ara yüzleri yardımıyla sistem sürekli olarak uzaktan izlenir ve gerektiği yerde müdahale edilir. Bölüm 4.3.'te anlatılan örnek uygulamadaki otomasyon sisteminin kontrolü ve gözlenmesi HMI operatör ekranıyla yapılmaktadır.



Şekil 3.3. Örnek bir scada sistemi.

3.2.2.2. PLC (Programmable Logic Controller)

PLC sensörlerden, doğrulayıcılardan ve diğer PLC'lerde işlenen giriş ve çıkış sinyallarini kontrol eden otomatik kontrol cihazıdır. Kontrol algoritması Merdiven Diyagramı (Ladder Diagram-LD), Yapısal Metin (Structured Text-ST) ve Komut Listesi (Instruction List-IL) gibi standart dillerde yazılabilir [11]. Uzak terminal birimi (Remote Terminal Unit-RTU) olarakta bilinirler. PLC'ler kontrol algoritmaları vasıtasıyla kumanda edilen sistemlerin ilgili hedef değerlere ulaşmasını sağlar. Bu kumanda edilen sistemin yapısına bağlı olarak mantıksal işlemler, ileri beslemeli, geri beslemeli kontrol algoritmaları ile gerçekleştirilmektedir. Kontrol algoritmaları giriş sinyallerinin değerlendirilip uygun çıkış sinyallerinin elde edilerek sisteme gönderilmesini sağlar.

PLC üç ana birimden oluşur.

1. CPU: Kontrol programının yönergeleri doğrultusunda giriş değerlerini alma çıkış değerlerini gönderme gibi görevleri yerine getirir.
2. Bellek: Üreticinin yüklediği yönetim yazılımı, kontrol programı, veri tabloları ve işlem alanlarının bulunduğu belleklerdir (ROM, RAM).

3. Giriş-Çıkış Modülleri: Analog giriş/çıkış modülleri ve dijital giriş/çıkış modülleri olmak üzere ikiye ayrılırlar. Analog giriş/çıkış modülleri 4,8,16,32'li giriş veya çıkışlı olurlar. Analog girişi alıp CPU'ya gönderir, dijital değeri alır sensörler veya doğrulayıcılara gönderirler. Dijital giriş/çıkış modülleri ise akım, gerilim vb. değerlerin durum ve alarm sinyallerini göstermek için kullanılırlar.

PLC sistemleri kendi içerisinde gerçek zamanlı iletişimi destekleyen Profibus, Canbus gibi ağ yapısına sahiptir. Bu yapı kumanda edilecek sisteme belirlenen zaman diliminde kumanda edebilmeyi garanti etmektedir.

PLC sistemlerinin üst katman olan Seviye-2 ile haberleşmesi daha az zaman sınırlı işlemleri kapsamaktadır. Bu açıdan çoğunlukla Ethernet tabanlı haberleşme kullanılmaktadır. İki sistem arasındaki haberleşmeler TCP/IP bazlı programlar ile gerçekleştirilerek iki yönlü veri aktarımı sağlanabilmektedir. Bu amaçla özel olarak yazılan haberleşme programlarının yanında günümüzde standart hale gelen OPC üzerinden haberleşme Seviye-1 içerisinde olduğu gibi Seviye-2 ile de haberleşmede kullanılmaktadır.

Bölüm 3.3'te anlatılan örnek uygulamada Siemens S7-300 PLC kullanılmaktadır. Bu PLC Profibus ağ yapısı üzerinden iletişim sağlamaktadır.

3.2.2.3. OPC (OLE for Process Control)

OPC, endüstriyel otomasyon sistemlerinde kullanılan farklı üreticilerin ürettiği ürünleri yönetmeyi ve veri alışverişini mümkün kılan ortak iletişim standardıdır. 1990'lı yıllarda her üreticinin kendi ürünleri için özel iletişim standardı kullanması yüzünden ortaya çıkan problemleri ortadan kaldırmak için geliştirilmiştir [12].

Temelini Microsoft'un OLE, COM (Component Object Model) ve Distributed COM (DCOM) teknolojileri oluşturur. Bir bilgisayardaki süreçler arasındaki iletişim COM, farklı bilgisayarlardaki süreçler arasındaki iletişim için DCOM kullanır. Bundan dolayı OPC; kullanıcılar tarafından oluşturulan istemcilerin sunucudan veri alabildiği sunucu/istemci çözümüdür. Sunucu aynı bilgisayardaki bir istemci (COM) olabilir

veya başka bir bilgisayardaki istemci (DCOM) olabilir. Böylelikle sunucu otomasyondaki bütün cihazlarla iletişim sorununu aşabilir. Sunucu/istemci modelinin en önemli faydası bir sunucunun birden fazla istemciye destek verebilmesidir [13].

OPC'nin günümüzde sahip olduğu birçok özellik vardır. Bu özellikler aşağıda maddeler halinde yazılıdır [14].

1. Alarms and Events
2. Batch
3. Commands
4. Common
5. Complex Data
6. Data Access
7. Data Access Automation
8. Data eXchange
9. Historical Data Access
10. OPC.NET 3.0 (WCF)
11. Security
12. Unified Architecture
13. XML Data Access

Bölüm 3.3'te anlatılan örnek uygulamada Kepware OPC sunucusu kullanılmaktadır. Bu OPC sunucusunun veri loglayıcı (Data Logger) özelliği kullanılarak otomasyon sisteminde bulunan Siemens S7-300 PLC'den alınan veriler farklı lokasyondaki veri tabanı sunucusuna gönderilmektedir.

3.2.3. Seviye-2: Proses Kontrol Sistemleri

Bu katman kumanda edilen sisteme özgü olan ancak üst seviyede yapılması gereken bazı fonksiyonların gerçekleştirilmesini sağlar. Bu seviyede sahip olunan yazılım ve donanım imkânları otomasyon sisteminde gerçekleştirilme imkânı olmayan işlemlere fırsat vermektedir. Ürünlerin kimlik bazlı takip edilmesi, belirli süreli verilerin saklanması ve raporlama işlemleri gerçekleştirilmektedir. Seviye-1 sisteminin ihtiyaç

duyduğu hedef değerlerde yine bu katmanda modellerle veya benzeri yöntemlerle oluşturulmaktadır. Bu işlem veri tabanından ilgili verilerin sorgulanıp oluşturulması ile gerçekleştirilebileceği gibi modeller vasıtasıyla da elde edilebilmektedir. Sistemin ve üretimle ilgili bilgilerin takibi HMI ekranından gerçekleştirilmektedir.

3.2.4. Seviye-3: Üretim Kontrol Sistemleri (MES)

Üretimle ve sistemle ilgili bilgilerin uzun süreli saklanması değişik amaçları barındırmaktadır. Bu işlem entegre endüstriyel sistemlerde veri koordinasyonunu sağlanması açısından önemlidir. Ayrıca geriye dönük verilerin analizi için de gereklidir. Özellikle kalite kontrol incelemelerinde, müşteri şikâyetlerinde vazgeçilmez bir gerekliliktir. Bu katmanda veri tabanı uygulamaları kullanılarak üretime yönelik raporlar alınır, üretim planlaması yapılır ve sistemin optimizasyonu sağlanır. Burada da yine HMI ekranından sistem sürekli kontrol edilir.

3.2.5. Seviye-4: Kaynak Planlama Sistemleri (ERP)

Kümelenmiş sistemlerin ve veri tabanı uygulamalarının kullanıldığı ve üretim aşamasına doğrudan müdahale edilmeyen ancak üretim öncesi ve sonrası işlemlerle yardımcı bilgilerin yönetiminin yapıldığı kısımları kapsamaktadır. Satın alma, satış, stok kontrol, sipariş, finans, insan kaynakları, müşteri yönetimi gibi süreçlerin gerçekleştirildiği kısımdır. Uzun vadede çıkarımlar yapılabilmesi için destekleyici verilerin oluşturulması açısından önemli bir katmandır.

3.2.6. Seviye-5: Karar Destek Sistemleri (DSS)

Bilgilerin hızlı bir şekilde tüm sistem içerisinden aktarıldığı ve verilerin analiz edilip karar vericinin sistem üzerindeki kararlarına destek olması için kullanılan sistemlerdir. Şekil 3.1.'de Endüstriyel otomasyon sistemlerinin bölümleri gösterilmiştir.

Endüstriyel otomasyon sistemlerinde katmanlar arası haberleşmede katmanın yerine ve fonksiyonuna göre değişik iletişim protokolleri kullanılmaktadır. Bu iletişim protokollerinden Bölüm 3.3.'te bahsedilmektedir.

3.3. ENDÜSTRİYEL OTOMASYON SİSTEMLERİNDE İLETİŞİM

Endüstriyel otomasyon sistemleri; kaliteli ve hızlı bir üretim için proseslerin sistematik ve kontrollü olarak gerçekleştirildiği, insan gücü kullanımının en aza indirgendiği sistemlerdir. Bu sistemlerin işleyişinde iletişimin önemli bir yeri vardır. Çünkü sistemin başlangıç noktası olan mekanik sistemlerin kontrolünden en üst seviyedeki karar destek sistemlerinin çalışmasına kadar bütün katmanlar birbiriyle sürekli iletişim halinde bulunurlar. Bu iletişim sağlamak için otomasyon sistemlerinin gereksinimleri doğrultusunda değişik iletişim protokolleri geliştirilmiştir. ModBus, Profibus, CAN ve DNP3 gibi endüstriyel network iletişim protokolleri bu protokollere örnek gösterilebilir. İnternet tabanlı uygulamaların endüstriyel otomasyon sistemlerinde kullanılmaya başlanmasıyla da TCP/IP internet protokolü de bu endüstriyel iletişim protokolleriyle birlikte ele alınabilir.

3.3.1. Modbus

Endüstriyel otomasyon sistemlerinde kullanılan standartlaşmış seri iletişim protokollerinden biridir. Sadeliği, kolay uygulanması ve yüksek performansı bu sistemlerde kullanılmasında büyük rol oynamıştır. OSI modelinin 7. seviyesindeki uygulama katmanıdır ve network üzerindeki çeşitli cihazlar arasındaki client/server haberleşmeyi sağlamaktadır. Modbus sistemde genellikle bir sahip (master) cihaz ve birde köle (slave) cihaz bulunmaktadır. Sahip cihaz broadcast yayın yapıp "0" göndererek köle cihazla iletişim kurmaktadır. Bu broadcast işlemi standart modbus RS-232C seri ara yüzünü kullanarak yapılmaktadır. ASC II ve RTU olmak üzere iki çeşit iletişim modu bulunmaktadır [15]. Genellikle 1.2Kbps veya 19.2 Kbps veri hızı kullanılmaktadır.

3.3.2. Profibus

Yüksek hızlarda iletişim imkânı sunan endüstriyel iletişim protokolüdür. Profibus-DP, Profibus-PA, Profibus-FMS olmak üzere üçe ayrılmaktadır. RS-485, Fiber optik ara yüzleri kullanarak iletişim kurulabilmektedir. Fiber optik veya koaksiyel kablo kullanıldığında iletişim hızları Profibus-DP'de 1 Mbps seviyesine çıkabilmektedir.

3.3.3. Can

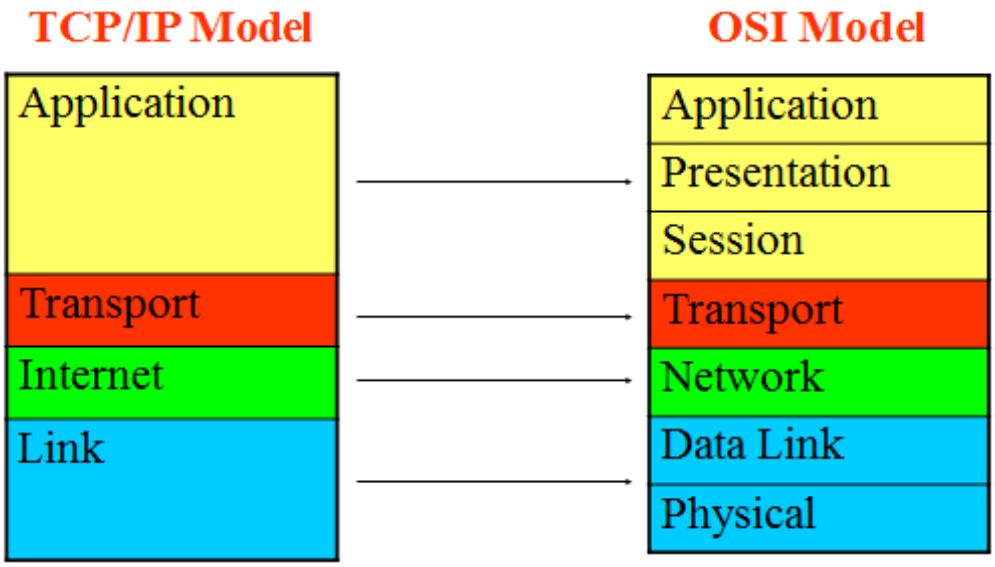
1980'lerin başlarında Alman Bosch Şirketi tarafından bulunan ve otomobillerde kullanılan birçok kontrolör ve ölçülecek değer arasındaki iletişimi sağlamak amacıyla kullanılan seri iletişim protokolüdür. Bu protokolde de fiber optik kablo veya koaksiyel kablo kullanıldığında iletişim hızı 1Mbps veri hızına kadar çıkabilmektedir.

3.3.4. DNP3 (Distributed Network Protocol)

1990 yılında Westronic şirketi tarafından geliştirilen endüstriyel iletişim protokolüdür. Öncelikli hedefi elektrik endüstrisi olan DNP3 protokolü aynı zamanda enerji ve su dağıtım endüstrilerinde de kullanılmaktadır.

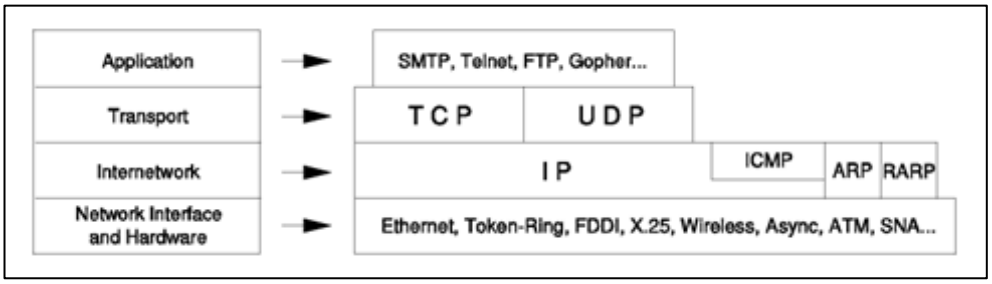
3.3.5. TCP/IP (Transmission Control Protocol/Internet Protocol)

1960'lı yılların sonlarında bilgisayarlar arasında veri iletişimi sağlamak amacıyla yapılan çalışmalar ile temelleri atılmış ve bu çalışmaların sonucunda TCP/IP internet protokolü olarak hayatımızda yerini almıştır. OSI (Open Systems Interconnection) modelinin oluşturulmasında TCP/IP modelinin yapısı referans olarak kabul edilmiştir. OSI referans modelindekinin aksine TCP/IP'de 4 temel katman (Link, Internet, Transport, Application) vardır. Şekil 3.4'te TCP/IP ile OSI katmanları arasındaki ilişki gösterilmektedir.



Şekil 3.4. TCP/IP ile OSI katmanları arasındaki ilişki.

TCP/IP protokolünde bulunan link katmanı adından da anlaşılacağı gibi bağlantı katmanıdır. Bağlantı katmanından sonra internet katmanı gelmektedir. Burada IP çözümlemeleri yapılmaktadır. IP tabanlı çözümlemeden sonra transport katmanı adı verilen port bilgilerinin değerlendirildiği katman gelmektedir. Son katman olan uygulama katmanında ise SMTP, Telnet vb. uygulamaların yapılabildiği OSI modelindeki oturum (Session), sunum (Presentation) ve uygulama (Aplication) katmanlarının hepsinin bir arada olduğu uygulama katmanı yer almaktadır. Şekil 3.5'te TCP/IP katman yapısı gösterilmektedir.



Şekil 3.5. TCP/IP katman yapısı.

Farklı fonksiyon ve görevleri olan endüstriyel otomasyon sistemlerinin katmanlarının birbirleri ile haberleşmesinde TCP/IP protokolü etkin bir şekilde kullanılmaktadır. Farklı lokasyonlarda bulunan bu katmanlardaki haberleşmede TCP/IP internet

protokolünün kullanılması bazı sorumlulukları da beraberinde getirmektedir. Bu sorumluluklardan en önemliside haberleşmenin internet üzerinden sağlandığı ve sistemin dış dünya ile sürekli ilişkili olduğu otomasyon sistemlerine yapılabilecek network saldırılarını ve bilgisayar sistemlerine sızabilecek zararlı yazılımları engellemektir.

Endüstriyel otomasyon sistemlerinde güvenliğini sağlamak için göz önünde bulundurulması gerekenler Bölüm 3.3'te network saldırıları ve zararlı yazılımlar alt bölümlerinde anlatılmaktadır. Ayrıca meydana gelen kazalar, saldırılar ve sonuçlarından da bahsedilmektedir.

3.4. ENDÜSTRİYEL OTOMASYON SİSTEMLERİNDE GÜVENLİK

Endüstriyel otomasyon sistemlerine yapılacak saldırılar büyük problemlere sebep olabilir. Bu protokollerin TCP/IP protokolü ile birlikte kullanılmasının da sisteme bir saldırgan tarafından kolay bir şekilde zarar verme fırsatı sunduğu söylenmektedir. [16]. Endüstriyel protokollerde güvenlik bakımından bazı eksikliklerin var olduğu bilinmektedir. DNP3 ve Profibus protokollerinin herhangi bir yetkilendirme veya güvenlik sorgusuna bakmaksızın uzaktaki aygıtların kontrolüne imkân sunması da buna örnek gösterilebilir. Honeywell (USA), Emerson (USA) ve Siemens (German) gibi Scada sistem üreticileri bu eksiklikleri kendi ürünlerinde ortadan kaldırmak için güvenlik çözümleri geliştirmeye ve aynı zamanda geleneksel IT şirketleride (CISIO, IBM, Symantec vb.) bu kritik güvenlik altyapısını sağlayabilecek ürünler sunmak için kendi güvenlik duvarı, sunucu ve güvenlik yazılımlarında yoğun çalışmalar başlatmıştır [17]. Bu alanda yapılmış olan çalışmalar neticesinde ortaya çıkarılan ürünlere Siemens şirketinin piyasaya çıkardığı; Firewall, NAT/NAPT router, DHCP server, Network Syslog, IPsec tunnel (VPN, Virtual Private Network) gibi network güvenliğinde göz önünde bulundurulacak hizmetleri sunan network güvenlik donanımı (Scalance S613-V2) ve bu donanımla birlikte çalışabilen SOFTNET Security Client güvenlik yazılımı örnek gösterebilir. Bu yazılım ve donanım network saldırıları kısmında anlatılan birçok saldırıyı engelleme imkânı sunmaktadır. Ayrıca diğer networklerde kullanılan güvenlik yazılımları ve donanımlarının TCP/IP temelli

saldırılara çözüm sunması da endüstriyel otomasyon sistemlerinde alternatif olarak kullanılmasını mümkün kılmaktadır.

3.4.1. Network Saldırıları ve Güvenlik Yapılandırılması

Bu bölümde anlatılan saldırılar genel anlamda networklerde karşılaşılan saldırı yöntemleri anlatılmaktadır. Fakat bu yöntemler üretimi yavaşlatma, durdurma, kazaya sebebiyet verme gibi kötü amaçlar için endüstriyel otomasyon sistemlerinde de kullanılmaktadır. Bu sistemlerde meydana gelen kazalar, saldırılar ve sonuçları Bölüm 3.4.3'te anlatılmaktadır.

3.4.1.1. Man-in-the-Middle Saldırıları

Bu tür saldırılarda saldırgan hedef bilgisayar ile hedef bilgisayarın gitmek istediği varış noktası arasına girerek bütün iletişimi istediği gibi kontrol etmektedir. Bu saldırılar birçok değişik şekilde (ARP Zehirlenmesi, DNS Ön Bellek Zehirlenmesi vb.) ortaya çıkmaktadır.

3.4.1.2. ARP Zehirlenmesi

ARP saldırısı yerel ağlarda gerçekleştirilebilen bir saldırıdır. Bu saldırı, üç şekilde gerçekleştirilmektedir. Birincisi; hedef bilgisayarın ARP tablosunun yanlış bilgilerle dolmasını sağlayarak hedef bilgisayarın göndereceği paketlerin saldırganın istediği adreslere gitmesini sağlamak. İkincisi; hedef bilgisayarın göndereceği tüm paketlerin, saldırganın bilgisayarı üzerinden geçmesini sağlamak (Man in the Middle). Üçüncüsü de; hedef bilgisayarın, paketlerini bir başka bilgisayara göndermesini sağlayarak bu bilgisayara servis dışı bırakma (Denial of Service) saldırısı yapmak şeklindedir. IP-MAC eşleştirmelerini switchler üzerinde port bazlı tutarak ve statik arp tabloları kullanarak bu saldırı engellenebilmektedir [18].

3.4.1.3. DNS Ön Bellek Zehirlenmesi

Bu saldırılar, bir DNS sunucusuna yetkisiz bir kaynaktan veri yüklenmesi ile kullanıcıların istediği alan adlarına gittiğini zannedip önemli bilgilerini elde etmeye çalışmak veya mağdur etmek için kullanılmaktadır. Açıklığın kapatılması için yaygın yazılım üreticileri tarafından çıkartılan yamaların uygulanması tavsiye edilmektedir. Yamalar uygulanamıyorsa veya yama mevcut değilse bu sunuculara erişimin kısıtlanması, yerel (internetten doğrudan ulaşılamayan) DNS önbelleğinin kullanılması, DNS sunucuları önüne saldırıyı engelleyebilecek Linux Iptables, OpenBSD PF vb. yerleştirilmesi veya tüm trafiğin yamanmış, açıklığı olmayan bir sunucuya yönlendirilmesi ile engellenmesi tavsiye edilmektedir [19].

3.4.1.4. DHCP Snooping

Bu saldırı yönteminde saldırı yapan bilgisayar ağ üzerindeki DHCP sunucusunun yerine geçiyor ve IP bilgilerini isteyen istemcilere kendi istediği bilgileri veriyor. Bu bilgilerden en önemlisi DNS sunucusu ve varsayılan ağ geçidinin IP adresidir. Saldırgan bu bilgileri değiştirerek istemcilerin bağlanmak istedikleri web sitelerinin yerine kendi istediği web sitesine hedeflemektedir. Sonuçta internet bankacılığı gibi uygulamalarda kullanıcı farkına varmadan sahte bir siteye yönlendirilip şifresi çalınabilmektedir [20]. Güvenilen DHCP sunucusu tanımlarının switchlere girilmesiyle bu saldırılar engellenebilmektedir.

3.4.1.5. DOS (Denial of Service) Saldırıları

Bu tür saldırılarda amaç değişik hizmetler veren ağ cihazlarını (e-posta sunucusu, web sunucusu vb.) servis dışı bırakarak kullanıcıları mağdur etmektir. Bu saldırıda sunuculara eş zamanlı olarak çok fazla istek gönderilerek sunucular servis dışı bırakılmaktadır. IPS (Intrusion Prevention System) çözümleri kullanılarak bu saldırılar engellenebilmektedir. Fakat zombi bilgisayarlar aracılığıyla yapılan saldırıların saptanmasında IPS cihazları yetersiz kalmaktadır. Çünkü farklı yerlerden ve farklı IP bloklarından yapılan bu tür saldırılar IPS cihazları için normal istekler gibi görülmektedir.

3.4.1.6. Ping of Death Saldırısı

ICMP protokolünün içerisinde bulunan ping işlemi kullanılarak varsayılan aralıktan çok daha büyük veri gönderip almaya çalışıldığında hedef bilgisayar bu duruma cevap veremeyip hizmet dışı kalmaktadır. Güvenlik duvarı üzerinden ping portunu kapatarak saldırı engellenebilmektedir.

3.4.1.7. Ping Flooding

Bu saldırı hedef bilgisayara çok fazla ping paketi gönderilerek gerçekleştirilmektedir. Bilgisayar bir süre sonra bu isteklere cevap veremeyip hizmet dışı kalmaktadır. Bu saldırıda güvenlik duvarından ping portunu kapatılarak engellenebilmektedir.

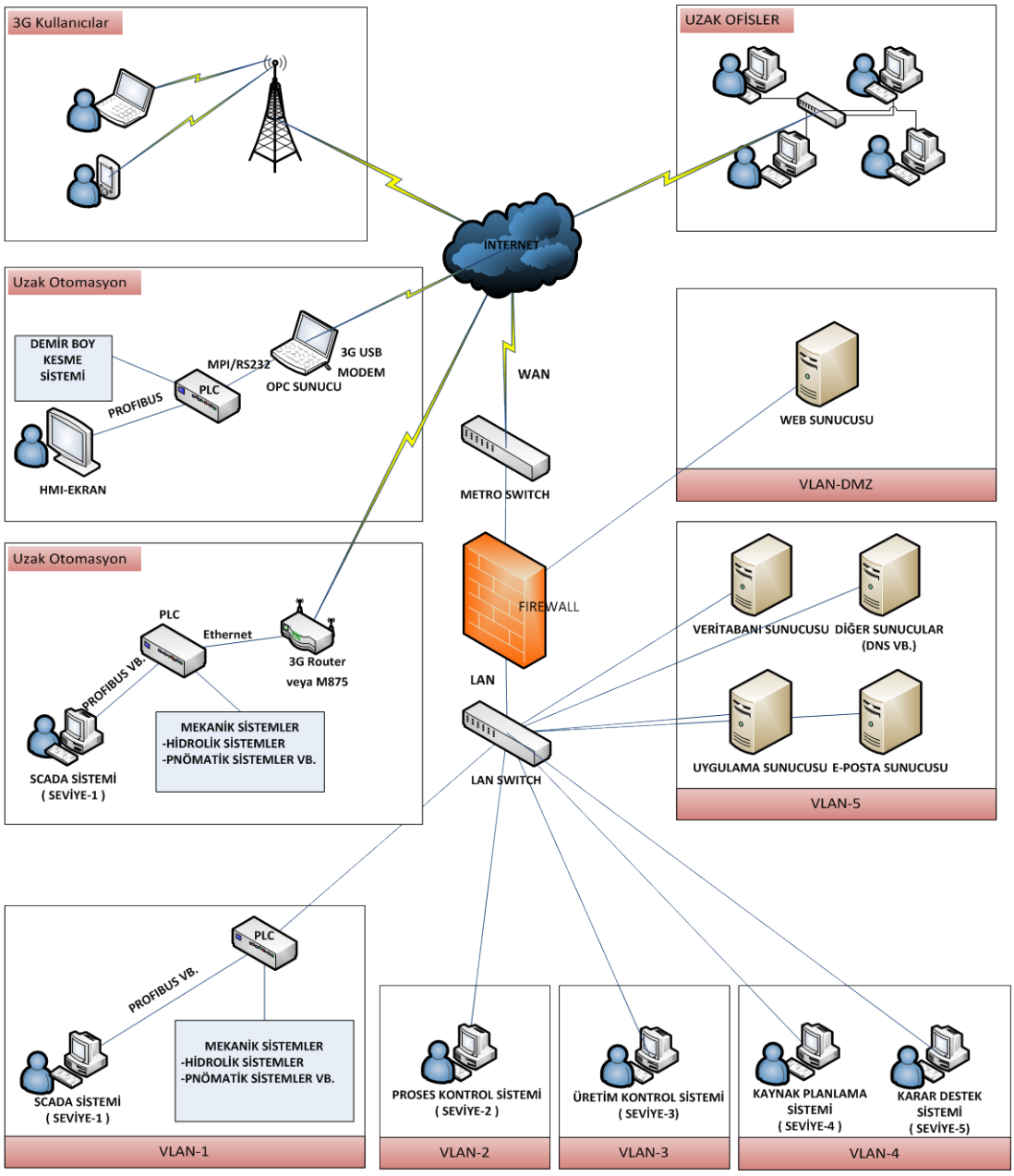
3.4.1.8. SYN Flooding

Bu saldırıda saldırgan kullanılmayan IP adreslerini aldatma amaçlı kaynak adresi olarak kullanarak birçok SYN paketini kurbanın bilgisayarına yollamaktadır. Alınan her SYN paketi için hedef bilgisayar kaynak ayırmakta ve onay paketini SYN paketinin yollandığı kaynak ip adresine göndermektedir. Hedef bilgisayar saldırgandan yanıt alamayacağından, SYN-ACK paketini 5 kez daha göndermeye çalışmaktadır. Bu işlemler her SYN paketi için gerçekleşeceğinden belirli bir süre sonra kaynaklar tükenip sistem cevap veremez hale gelmektedir. Bu saldırı güvenlik duvarından SYN paketleri daha çabuk zaman aşımına uğratılarak engellenebilmektedir.

3.4.1.9. Güvenlik Yapılandırılması

Endüstriyel otomasyon sistemlerinin genel network mimarisi şekil 3.6‘da gösterilmektedir. Bu network mimarisinde LAN (Local Area Network), WAN (Wide Area Network) ve DMZ (De-Militarized Zone) olmak üzere üç ana bölge bulunmaktadır. LAN; üretim ve diğer işlerin yapıldığı bölgedir. LAN içerisinde güvenlik, broadcast kontrol ve esneklik gibi avantajlar sağlayan VLAN (Virtual LAN)’lar kullanılmaktadır. WAN; İnternete ve diğer LAN ile bağlantının sağlantığı

bölgedir. DMZ; web sunucusunun bulunduğu bölgedir. Genellikle internet üzerinden yapılan saldırılar öncelikle web sunucularına olmaktadır. Bu yüzden web sunucularının özellikle üretim sistemlerinden farklı bir bölgede tutulması gerekmektedir. Şekil 3.6.'da endüstriyel otomasyon sistemlerinin genel network mimarisi gösterilmektedir.



Şekil 3.6. Endüstriyel otomasyon sistemlerinin genel network mimarisi.

LAN'ın Yapılandırılması

Güvenlik tedbirleri olarak LAN'da aşağıda belirtilen önlemler alınarak sistemde oluşabilecek problemlerin engellenmesi hedeflenmiştir.

1. Network veri hattı ve cihazlarının fiziksel güvenliği sağlanmalıdır.
2. Veri kaybını engellemek için veri kablo boyları standartlara uygun yapılandırılmalıdır.
3. Networkte kullanılacak bütün cihazlar kayıt altına alınmalıdır.
4. Cihazlar switchlerin hangi portuna bağlanacaklarsa port bazlı MAC güvenliği sağlanmalıdır.
5. Switchlerin kullanılmayan portları yönetimsel olarak kapatılmalıdır.
6. Cihazlara sabit IP-MAC eşleştirmesi yapılarak IP dağıtılmalıdır.
7. Switchlerde DHCP snooping saldırılarına karşı güvenilir DHCP portu tanımlanmalıdır.
8. Switchlerde ARP zehirlenmesine karşı IP-MAC listeleri oluşturulmalıdır.

Güvenlik Duvarı Yapılandırılması

1. Dışarıdan içeriye doğru tüm portlar öncelikle kapalı olmalıdır. İhtiyaçlar doğrultusunda içeriye doğru (uzak ofislere ve uzak kullanıcılara) ilgili portlar açılmalı, dışarıdan gelebilecek yetkisiz isteklerin filtrelenmesi sağlanmalıdır.
2. Sistemde her yerden erişimin olacağı sunucuların ilgili portları açılmalıdır.
   Web Sunucusu: TCP Port 80
   E-Posta Sunucusu: POP3 TCP Port 110, SMTP TCP Port 25
   DNS Sunucusu: UDP Port 53
3. OPC sunucusunun veri tabanı sunucusuna veri gönderebilmesi ve Web sunucusunun veri tabanı sunucusundan gerekli verileri alabilmesi için veri tabanı portu açılmalıdır.
   Veri Tabanı Sunucusu: TCP Port 1433
4. Uzak yardım yapılacak sunuların uzak masaüstü bağlantı portu kullanıcılara tanımlı sabit IP adreslerine açılmalıdır.
   Uzak Masaüstü Bağlantısı: TCP Port 3389

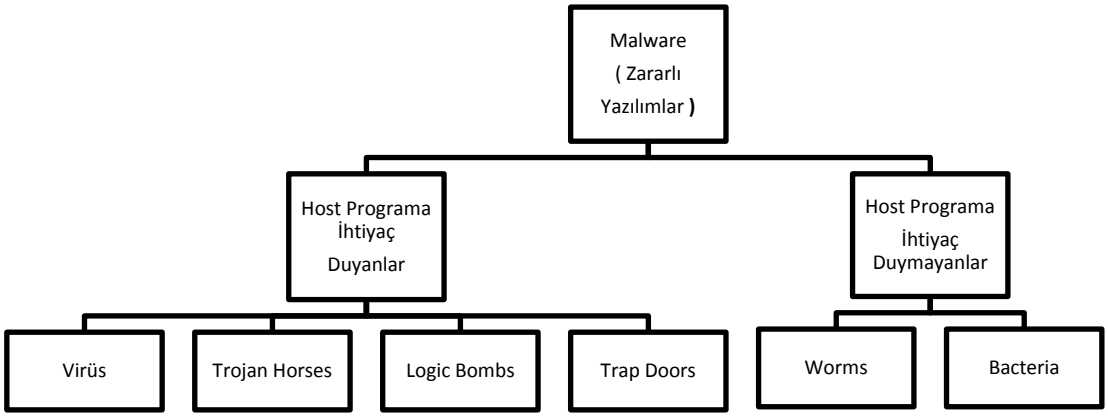
3.4.2. Zararlı Yazılımlar (Malware)

Günümüzde birçok alanda zorunlu ihtiyaç olarak kullanılan bilgisayar ve bilgisayar sistemleri endüstriyel otomasyon sistemlerinde de önemli bir yer teşkil etmektedir. Bu sistemler iş akışını engelleyebilecek veya durdurabilecek birçok zararlı yazılımın tehlikesi altında bulunmaktadır. Ayrıca mobil telefonlarda 3G mobil internetin kullanımının yaygınlaşmasıyla hem mobil telefonlar hem de bu telefonların dâhil olduğu sistemler zararlı yazılımların tehlikesi altına girmektedir.

Bu bölümde bilgisayar sistemlerinde görülen zararlı yazılımlar anlatılmaktadır. Fakat bu zararlı yazılımlar üretimi yavaşlatma, durdurma gibi kötü amaçlar için endüstriyel otomasyon sistemlerinde de kullanılmaktadır. Bu sistemlerde görülen zararlı yazılımlarla ilgili örnekler Bölüm 3.4.3'te bulunmaktadır.

Malware (Malicious software-Zararlı Yazılım); Kullanıcıların izni olmadan bilgisayar sistemlerine sızmak veya zarar vermek amacıyla geliştirilen yazılımların genel adıdır. Malwareler; Spywareler, virüsler, wormlar vb. diğer zararlı yazılımları içermektedirler [21].

Bu yazılımlar genel olarak ikiye ayrılmaktadır. Şekil 3.7'de zararlı yazılımların sınıflandırması gösterilmektedir.



Şekil 3.7. Zararlı yazılımların sınıflandırması.

3.4.2.1. Host Programlara İhtiyaç Duyan Zararlı Yazılımlar

Virüs

Bilgisayar virüsleri, bilgisayarlara internet, network veya medya cihazları aracılığıyla bulaşmaktadır. Bilgisayarın çalışmasını yavaşlatmak hatta durdurmak ya da kullanıcının çalışmasına engel olmak amacıyla yazılmış programlardır. Bu programlar genellikle bilgisayarda bulunan başka bir programın içine yerleşerek çalışmaktadır. Virüslü yazılım, bir kere çalıştırılınca başka dosyalara da bulaşmaya çalışmaktadır. Bu programlar işletim sistemleri tarafından otomatik olarak çalışan bir programa bulaşırsa bilgisayarın her açılışında otomatik çalıştırılmaktadır ve başka dosyalara, flash disklere, ağ paylaşımlı klasörlere vb. yerlere bulaşabilmektedir. Şekil 3.8'de Dünya'da 24 saat içerisinde bilgisayarlara bulaşan virüsler hakkında örnekler gösterilmektedir.

Spyware

Adından da anlaşılacağı üzere, casus yazılımı bir veri sensörü olarak hareket edip, son kullanıcıların bilgilerini toplar ve üçüncü şahıslara gönderir. Spywareler hatta diğer bilgisayarlara saldırarak servis dışı bırakabilmektedirler. Kullanıcıların internetteki aktivite bilgileri ve kredi kartı numarası gibi alışveriş bilgileri de spywarelerin hedefinde bulunmaktadır. Bu zararlı yazılımları saptamak ve ortadan kaldırmak için anti-spyware yazılımları kullanılmaktadır [21].

Adware

Bilgisayar kullanıcılarına reklam yapmak amacıyla bilgisayarlarına yüklenen yazılımlardır. Bu yazılımlar aynı zamanda kullanıcının ilgisini çekebilecek reklamları göstermek için; kullanıcının sörf yaptığı siteleri veya tercihleri gibi özel bilgilerini izlerler. Bu yazılımların gelişmiş olanları ise sistemi savunmasız bırakıp lokal dosyalardaki verileri okurlar, sörf ve görüşme bilgilerini toplarlar ve hatta gelecekte yazılım transfer etmek ve yüklemek için uzak bağlantı oluştururlar. Adwarelerin diğer zararlı yazılımlardan farkı kullanıcıların onayı ile veya onayı

olmadan yüklenebilmeleridir. Kullanıcılar adware'in varlığını bilmeden ücretsiz yazılımları bilgisayarlarına yükledikleri zaman EULA (End-User License Agreement-Son Kullanıcı Lisans Anlaşması) içerisinde kabul edebilir veya arka tarafta hiç kullanıcıya sorulmadan yüklenebilir [22].

Dialer

Bilgisayarın internet bağlantı ayarlarını değiştirerek tarifesi yüksek bir telefon hattına yönlendiren programlardır. Bu yönlendirme işleminden sonra İnternete bağlantı yapıldığında kullanıcılara gelen faturaların çok fazla gelmesine sebep olan yazılımlardır.

Macro virüsü

Bilgisayarda kullanılan bazı paket programların, eksiklerini tamamlamak veya birlikte çalışarak katkıda bulunmak için yardımcı olarak geliştirilen, ana programla aynı kodlama diliyle yazılan programlar vardır. Programların bu özelliğini kullanarak yazılan virüsler aynı kodlama ile yazılmış diğer dosyalara da bulaşıp bozmaya çalışmaktadır. Böylece tüm dosyaları ele geçirip bozabilmektedir.

Exploit (Sömürmek)

İşletim Sistemleri ve bazı programların açıklarını bulup bu açıkları kötüye kullanma zararlı yazılımlardır. Genellikle sisteme yetkisiz erişim için kullanılmaktadır. Kazanılan yönetici yetkileri ile de bu sistemi ele geçirirler ve başka sistemlere de bu bilgisayarları kullanarak bulaşmaktadır. Bu tip virüslerin birçok kullanıcıya hitap eden sunuculara bulaştığını varsayılırsa, sunucuya bağlanan her bilgisayara bu tip virüslerin bulaşması ile bir anda birçok bilgisayarın zarar görmesi kaçınılmaz olmaktadır. Hemen hemen her işletim sistemi için (Linux, Windows, FreeBSD, MacOS) exploit yazılmıştır.

Trojan horses (Truva Atları)

Truva Atları kendilerini kullanıcıların yüklemesi ve çalıştırması için yararlı veya zararsız gösteren yazılımlardır. Aynı zamanda uzaktan erişim ve kontrol gibi özellikleri aktif hale getirerek bulaştığı sisteme kısmi veya tam erişim hakkı vermektedirler. Truva Atları birçok şekilde bulaşabilir ve temizlemesi hayli zordur. Saldırgan bağlantı yapana kadar kullanıcılar zararlı kodu fark etmemektedir. Kullanıcıdan bağımsız olarak çalıştırılabilmektedir. Uzak saldırgan bağlantı kurduğu zaman zararlı kodlar yönetilmektedir. Truva atlarının kullandığı dosya isimleri ve network adresleri gibi kaynaklar binary kodludur. Zararlı yazılımın kullandığı işletim sistemi kaynakları (Proses, memory) sistemin performansını azaltabilmektedir [23]. Bu gibi durumlara maruz kalınmaması için bilinmeyen yazılımlar, e-posta ile gelen ekler vb. çalıştırmamalıdır.

Trap doors (Tuzak Kapısı)

Tuzak kapısı ya da arka kapı olarak bilinen bu yazılımlar bir programı yazan kişi tarafından programın içerisine girebilmek için bırakılan bir açık kapıdır. Bu programın çalıştığı bilgisayara programı yazan kişinin, uzaktan erişim yöntemiyle sistem güvenlik yazılımlarını aşarak girmesine imkân sağlamaktadır.

Logic Bombs (Mantık Bombası)

Logic Bombs, herhangi bir programın içerisine yerleştirilen zararlı yazılımlardır. Bazı şartların sağlanması durumunda çalışmaya başlayarak dosyaların silinmesi, sistemin çökmesi gibi zararlar verebilmektedirler.

3.4.2.2. Host Programlara İhtiyaç Duymayan Zararlı Yazılımlar

Worm (Solucan)

Worm kendini ağ üzerinden direk erişim veya e-postalar ile kendisini başka bilgisayarlara kopyalayıp bulaştığı yeni bilgisayarda kendisini aktif eden

yazılımlardır. Kendisini başka sistemlere kopyalamasının yanı sıra wormlar yazılma amacına göre uzaktaki bir bilgisayardan emir alabilmekte veya bilgi sızdırabilmektedirler. Buradan da anlaşılacağı üzere bazı wormlar aynı zamanda trojen (Truva Atı) işlevini de taşıyabilmektedir. Trojen yazılımlar bir bilgisayarın ağ üzerindeki başka bir bilgisayar tarafından yönetilmesini sağlayan yazılımlardır. Trojenler, cd-rom cihazının kapağını açmak gibi masum işlemler yapabileceği gibi, online bankacılık şifrelerinin çalınmasına veya başka bir bilgisayara DoS atak yapmasına da sebep olabilmektedirler. Wormlar bulaştığı bilgisayara zarar vermesinin yanı sıra kendini bulaştırmak için yarattıkları trafik ile de bant genişliğinin israfına ve bütün ağ kullanıcılarının erişim kalitesinin düşmesine sebep olmaktadırlar. Ayrıca ağ cihazlarında gereksiz işlemci yüküne, daha da kötüsü toplu bir DoS atağı yapmaları durumunda bütün altyapıyı felç de edebilmektedirler [24].

Bacteria (Bakteri)

Bilgisayar üzerinde bulunan dosyalara kendini sürekli kopyalayarak çoğalırlar ve çoğaldıkça sistem kaynaklarından daha fazla tüketerek (disk alanı, cpu, memory vb.) bilgisayarın verimli çalışmasını engellerler.

#	Virus Name	# of Infected Computers	# of Scanned Computers	% Infected
1	Generic!atr	4288	96077	4.46
2	ZeroAccess	3630	96077	3.78
3	BackDoor-EZC!lnk	2855	96077	2.97
4	Adware-HotBar.d	2242	96077	2.33
5	W32/Conficker.worm!inf	2174	96077	2.26
6	JV/Exploit-Blacole.a	2162	96077	2.25
7	Generic.dx	1657	96077	1.72
8	Adware-HotBar.f	1537	96077	1.60
9	Exploit-CVE-2010-2568	1352	96077	1.41
10	W32/Sality.gen.z	1298	96077	1.35
11	Exploit-CVE2010-2568	1124	96077	1.17
12	New Autorun!inf.a	1111	96077	1.16
13	W32/YahLover.worm.gen	1107	96077	1.15
14	W32/Conficker.worm.gen.a	1033	96077	1.08
15	GameVance.gen.q	972	96077	1.01
16	W32/Autorun.worm!inf	851	96077	0.89
17	W32/Rontokbro.gen@MM	824	96077	0.86
18	Downloader-CJX!lnk	789	96077	0.82
19	W32/Ramnit.a!inf	780	96077	0.81
20	Generic PUP.x	773	96077	0.80

Şekil 3.8. Dünyada 24 saat içerisinde bilgisayarlara bulaşan virüsler [25].

3.4.2.3. Sistem Güvenliğinin Sağlanması

Zararlı yazılımların etkileri göz önüne alındığında bilgisayar ve sunucu sistemlerini bu etkilerden korunmak için bazı önlemler alınması gerekmektedir. Bu önlemler aşağıda maddeler halinde sıralanmaktadır.

1. Bilgisayar ve sunucularda lisanslı işletim sistemleri ve yazılımlar kullanılmalıdır.
2. Bilgisayar ve sunuculara virüs programı kurulmalı ve güncelleme işlemi belirli aralıklarla yapılmalıdır.
3. Bilgisayar ve sunucuların üzerinde bulunan işletim sistemlerinin güncellemeleri düzenli olarak yapılmalıdır.
4. Bilgisayar ve sunucuların üzerinde bulunan güvenlik duvarı etkin olmalıdır.
5. Sisteme güvenilmeyen ve bilinmeyen yazılımlar yüklenmemelidir.

6. USB bellek gibi depolama araçlarından bulaşabilecek virüs vb. tehlikelere karşı virüs programı ile tarattıktan sonra kullanılmalıdır. Sistemi direkt olarak ilgilendiren bilgisayar ve sunucular üzerinde yapılacak işlemler için ayrı bir USB bellek kullanılmalıdır.
7. Gelen E-postalar analiz edildikten sonra açılmalıdır.
8. Kullanıcılar sistemi direkt olarak ilgilendiren bilgisayar ve sunucular üzerinde şahsi işleri için kullanmamalıdır.

3.4.3. Meydana Gelen Kazalar, Saldırılar ve Sonuçları

1. 2010 yılında bir bilgisayar virüsünün İran'ın Buşehr nükleer santralindeki personelin bazılarının kişisel bilgisayarlarının etkilendiği saptandı. Stuxnet olarak adlandırılan virüs Symantec'in raporuna göre birçok ülkede belirlendi fakat en fazla İran'ı etkilediği bildirildi. Stuxnet saldırısı Siemens SCADA sistemleri ve bu sistemlerde kullanılan PLC'leri tekrar programlamayı hedeflemekteydi. Bu saldırıdan on binlerce bilgisayar etkilendi [26].
2. Amerika'da 2003 yılında nükleer düzenleme kurulu; Ohio DavisBesse nükleer santralinde operatörleri kazalar hakkında uyaran iki önemli monitör sisteminin saatler boyunca hizmet dışı kalmasına Slammer bilgisayar wormunun networke sızmasının sebep olduğunu resmi olarak duyurdu.
3. 2000 yılında Maroochy Shire'da iş başvurusu reddedilen Avustralyalı bir adam atık su kontrol sistemine dizüstü bilgisayar ve kablosuz bir radio kullanarak girip intikam aldı. Milyonlarca litre atık su yerel parklara, nehirlere ve Majör otelin arazisine boşaldı.

Scada sistemlerinde meydana gelebilecek kazaların sonuçları tahmin edilemeyecek kadar kötü olabilir. Yapılan araştırmalara göre:

1. 10 Haziran 1999'da Bellingham'daki bir scada system hatasında 230.000 galon benzin iki derenin içerisine boşaldı. Bu benzinde ateş alarak 3 kişinin ölümüne yol açtı ve 8 kişininde yaralanmasına sebep oldu. Ayrıca önemli çevresel zararlara yol açtı.

2. 7 Nisan 1992'de Texas Branham'daki gaz boru hattında scada kontrolörü yanlış bir şekilde işlemeye başladı. Scada izleme sistemide hayli uçucu olan sıvının anormal sızıntısını algılayamadı. Bunun sonucunda ateş alan madde 3 kişinin ölümüne, 21 kişinin yaralanmasına ve 9 milyon dolar zarara sebep oldu.
3. 22 Haziran 2009'da iki DC Metro treni çarpıştı. NTSB araştırması Scada tabanlı otomatik tren koruma sisteminin rölantide olan bir treni algılayamamasından kaynaklandığını saptadı. Bunun sonucunda 9 kişi öldü ve 52 kişi yaralandı [27].

Endüstriyel otomasyon sistemlerinde internet tabanlı uygulamaların kullanılmaya başlanması ile klasik network sistemlerinden daha farklı bir network yapısına sahip olan bu sistemlere eksiklikleri nedeniyle içeriden ve dışarıdan yapılabilecek network saldırı riski de artmıştır. Bu sistemlere yapılacak network saldırıları ve sisteme sızan zararlı yazılımlar üretimi yavaşlatabilir, durdurabilir ve hatta can ve mal kaybına yol açabilir. Bu sebeplerden ötürü sistem ve network güvenliğini sağlamak çok önemlidir. Bunu yaparken zararlı yazılımlara ve network saldırılarına karşı korunmak için gerekli önlemler alınmalı ve internet tabanlı uygulamalara kontrollü bir geçiş yapılmalıdır.

BÖLÜM 4

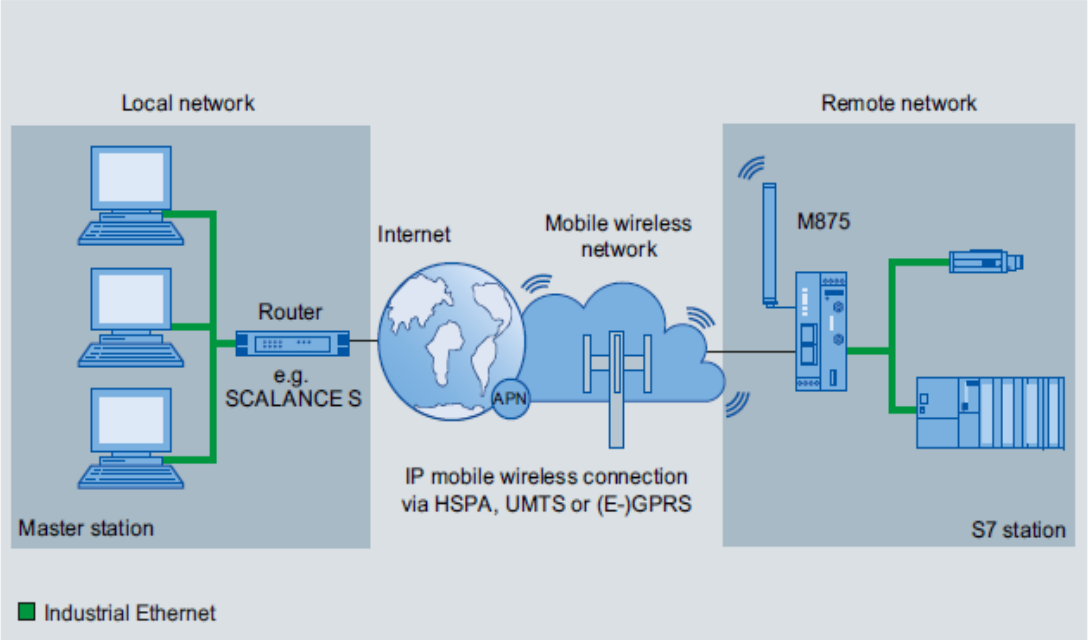
3G İLE ENDÜSTRİYEL OTOMASYON SİSTEMLERİNİN İZLENMESİ

4.1. 3G'NİN UYGULAMALARDA KULLANILMASI

3G mobil iletişim teknolojisi günümüzde yüksek hızda veri iletim imkânı sunmakta ve birçok iş kolunda (Tıp, Medya vb.) değişik uygulamalarla kendini göstermektedir. 3G mobil iletişim teknolojisinin uygulamalarda kullanılmasında donanımsal ve yazılımsal gelişmeler de önemli rol oynamaktadır.

4.1.1. Donanımsal Gelişmeler

Son kullanıcı tarafında 3G telefonlarla başlayıp 3G Usb Modem, 3G Netbook, 3G Tablet PC'ler ile internet hizmeti sağlamaya devam eden 3G donanımlar; farklı iş kollarında da üretici firmalar tarafından iş çözümleri sunmak için kullanılmaktadır. Endüstriyel çözümler sunan Siemens üretici firmasının çıkarmış olduğu 3G/UMTS router SCALANCE M875 ve network çözümleri sunan Cisco üretici firmasının çıkarmış olduğu Cisco EHWIC and 880G for 3.7G (HSPA+)/3.5G (HSPA) donanımları bu gelişmelere örnek gösterilebilir. Bu donanımsal gelişmeler aynı zamanda kablolu internet imkânının olmadığı tesislerde veya hareketli kullanıcılar internete erişmek istediklerinde çözüm sağlayabildiklerinden kablolu iletişime alternatif olmaya başlamıştır. Şekil 4.1'de 3G ile endüstriyel otomasyon sistemi üzerine örnek bir çözüm gösterilmektedir.



Şekil 4.1. 3G-Endüstriyel otomasyon sistemi üzerine örnek bir çözüm [28].

4.1.2. Yazılımsal Gelişmeler

Yazılım alanındaki gelişmeler genellikle 3G telefonlar üzerine olmaktadır. Yazılım üreten firmalar; e-ticaret uygulamaları, e-posta yönetim yazılımları, web tarayıcı programları, güvenlik yazılımları, GPS uygulamaları, ofis uygulamaları, uzak masaüstü programları vb. birçok uygulama alanında kullanıcılara önemli çözümler sunmaktadır.

4.1.3. Örnek Uygulamada 3G'nin Tercih Edilmesi

Örnek Uygulamada 3G'nin tercih edilmesindeki sebepler aşağıda maddeler halinde yazılıp açıklanmaktadır.

1. Uzak Yardım Sistemi: Otomasyon sistemlerinde çalışan mühendislerin genelde sahada bulunmaları sebebiyle ofise gelme imkânı çok fazla bulunmamaktadır. Sistemde bir problem olduğunda, sistemde güncelleme yapılacağında veya herhangi bir konuda destek verileceğinde sisteme uzak erişimle bağlanılmakta ve yardım edilmektedir. Uzak yardım için kablolu veya kablosuz internete ihtiyaç duyulmaktadır. 3G cihazlardaki gelişmeler, kolay taşınabilmesi,

mekândan bağımsız olarak internet erişimi sağlayabilmesi ve uzak yardım uygulamaları için yeterli bağlantı hızı sunması 3G'nin tercih edilmesinde rol oynamaktadır.

Bu kısmen yerel sayılabilecek uygulamalar yanında farklı firmadan satın alınmış sistemlerle ilgili yapılan anlaşmalar kapsamında teknik destek alınmaktadır. İlgili teknik destek ekiplerinden hızlı bir şekilde yardım alabilmek ancak bulundukları yerdeki internet imkânlarına bağlı kalmaksızın sunabilecekleri hizmetlerle sağlanabilecektir. Bu açıdan da 3G imkânlarını kullanmak bu hizmetin yaygınlaşmasına katkı sağlayacaktır.

2. Otomasyondan Veri Alma: Fabrikalarda genellikle üretimin yapıldığı kısım yani mekanik sistemlerin ve scada sisteminin bulunduğu kısımdır. Proses kontrol sistemi, üretim kontrol sistemi gibi sistemler farklı lokasyonlarda bulunur. Fabrikalardan diğer lokasyonlardaki sunuculara sistemin çalışmasına yönelik veriler ve üretime yönelik veriler gönderilmektedir. 3G'nin yeterli veri iletim hızı ve kolay kurulumu bu sistemlerde kullanılmasında tercih sebebi olmaktadır.
3. Uyarı Sistemi: Otomasyon sisteminde oluşan anormal durumları haber vermek, uzak yardım isteğini ve üretime yönelik bilgileri bildirmek için sistem e-posta göndermektedir. Sahada bulunan mühendisler; 3G telefonlarda veya bilgisayarlarda bulunan Outlook, Thunderbird gibi yazılımlar aracılığıyla gelen e-postalarını hemen haber alabilmektedir. Bu e-postalardan alınan mesajlar çerçevesinde sisteme anında müdahale edilebilmektedir. 3G 'deki yazılımsal gelişmeler ve sürekli internet erişimi sunması 3G'nin tercih edilmesinde rol oynamaktadır.

4.2. LİTERATÜR ÇALIŞMASI

Bin et al. makalelerinde; Samsung ARM9 serisi mikro işlemci kullanan otomasyon sisteminden 3G ile uzak lokasyondan verileri veri tabanına alma ve sistemi internet üzerinden web tabanlı bir otomasyon ile izleme üzerine çalışma yapmışlardır [29].

Yu et al. makalelerinde; 3G kullanarak bir otomasyon sisteminin uzak lokasyonunda bulunan networke bağlanan OPC sunucu ile verileri alma, izleme ve alarm mekanizması olan bir otomasyon üzerine çözüm sunmuşlardır [30].

4.3. ÖRNEK UYGULAMA

4.3.1 Amaç ve Kapsam

Endüstriyel otomasyon sistemlerinin üretime yönelik kısımlarında gerçek zamanlı işlemlerin büyük bir yer edinmesinden dolayı yakın takip edilmesi ve hızlı çözümlerin üretilmesi gereklidir. Konvansiyonel sistemlerde üretimin takip edilmesi ancak sistemlerin bulunduğu tesislerde/sahalarda mümkündür. Bu yapı kısmen üretime yönelik verilerin kritikliğinden dolayı dış müdahalelere maruz kalmaması endişeleriyle oluşmuş olmakla beraber teknolojik yetersizlikler de bunda etkin olmuştur. Internet teknolojisindeki gelişmelerle beraber farklı noktalardan sistemlere erişmeye yönelik çalışmalar yapılmıştır.

Bu çalışma kapsamında da geliştirilen uygulama ile endüstriyel otomasyon sistemlerine yönelik değişik kazanımlar sağlayacak amaçlar hedeflenmiştir. Bu kazanımlar şu şekilde listelenebilir:

1. Sistemde bir problem olduğunda veya sistemde güncelleme yapılacağı zaman uzakta masaüstü bağlantısı kullanarak sisteme destek vermeye imkân veren uzak yardım sistemi oluşturmak.
2. Verilen uzak yardım neticesinde ortaya çıkan çözümleri bir veri tabanında toplayarak sorun giderme sistemi oluşturmak.
3. Otomasyon sisteminden; sisteme ve üretime yönelik verileri bir veri tabanına alarak mühendislere ve yöneticilere raporlama ve karar verme sistemi oluşturmak.
4. Otomasyon sisteminden alınan verilerle sistemin çalışmasında oluşan anormal durumları ve üretime yönelik bilgileri mühendislere ve yöneticilere haber veren uyarı sistemi oluşturmak.

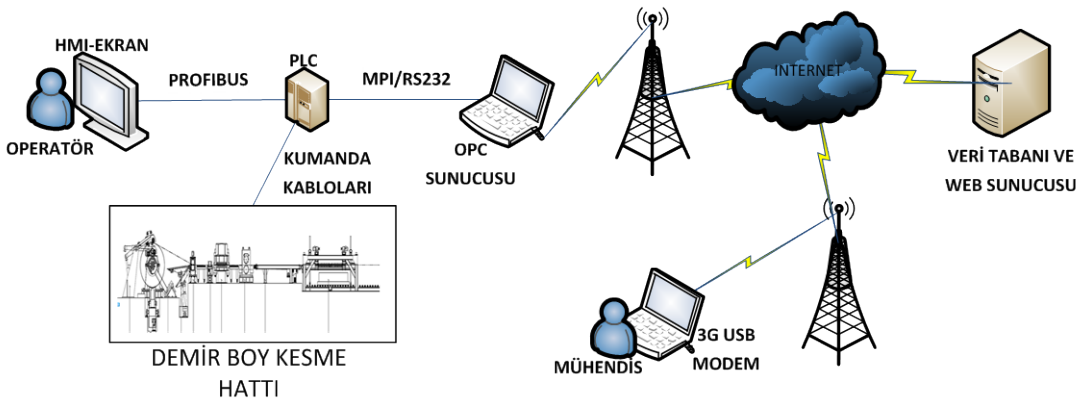
4.3.2. Kullanılan Yazılımlar

1. İşletim Sistemi: Windows 7
2. Yazılım Geliştirme Platformu: Visual Studio 2010 (ASP.NET,C#)
3. Veri Tabanı: SQL Server 2008 R2 Express
4. Web Yayını: IIS (Internet Information Service)
5. OPC (Open Process Control) Sunucusu: Kepware OPC Server
6. Siemens Simatic Manager

4.3.3. Yol Haritası

Sistem tasarlanmış ve network mimarisi ortaya çıkarılmıştır. Web sunucusu, veri tabanı sunucusu ve OPC sunucusu kurulmuştur. OPC Sunucusu üzerinden demir kesme tesisinden veri tabanına alınacak olan veriler ve web programlama aşamasında kullanılacak veriler belirlenmiştir. Veri tabanı mimarisi tasarlanmıştır; table (tablo), view (görüntü) ve triggerler (tetikleyici) oluşturulmuştur. Veri tabanı kullanıcıları ve rolleri belirlenmiştir. Uygulamada kullanılacak olan asp.net veri tabanı tabloları oluşturulan veri tabanına yönlendirilmiştir. Web uygulaması yazılmıştır. Otomasyon test edilmiş ve ortaya çıkan sonuçlar yazılmıştır.

4.3.4. Örnek Otomasyon Sistemi ve Çalışma Mantığı



Şekil 4.2. Demir boy kesme otomasyon sistemi.

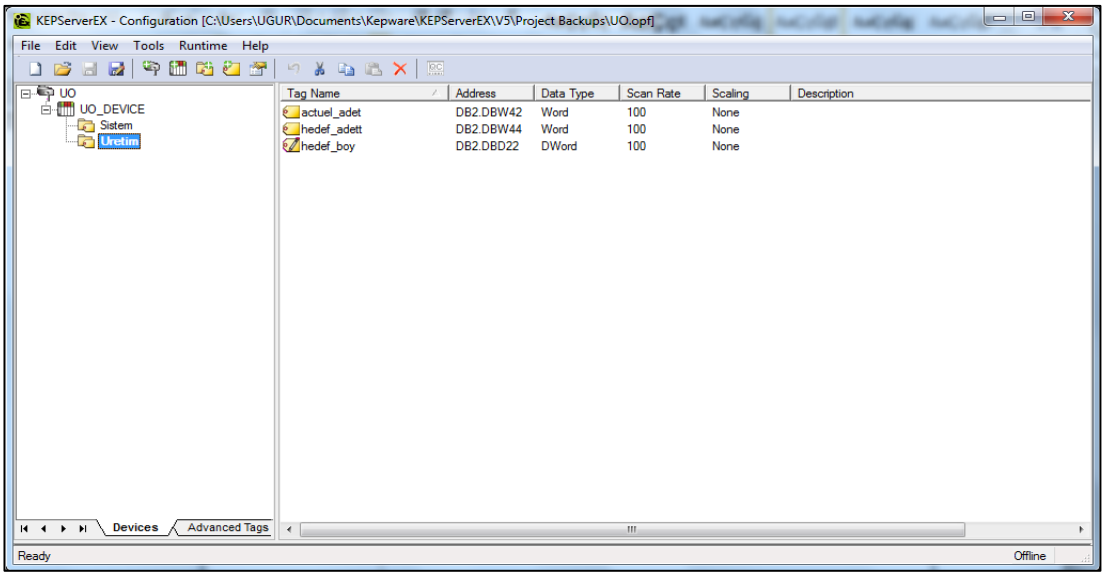
Otomasyon sisteminde PLC olarak Siemens S7-300 kullanılmaktadır. Operatör PLC'ye profibus iletişim hattıyla bağlı bulunan HMI ekrandan sistemi yönetmekte ve izlemektedir. Demir boy kesme otomasyon sisteminde, rulo olarak gelen demir malzeme açılıp plakalar halinde kesilmektedir. Kesilen plakalar paketlenerek müşterilere gönderilmektedir. Şekil 4.2'de demir boy kesme otomasyon sistemi gösterilmektedir.

4.3.5. Otomasyon Sisteminden Verilerin Alınması

Gerçekleştirilen uygulamada PLC MPI/RS232 kabloyla taşınabilir bilgisayara, taşınabilir bilgisayarda 3G usb modemle internete bağlı bulunmaktadır. Taşınabilir bilgisayar OPC sunucu olarak yapılandırılıp PLC'den alınan veriler tesiste kablolu internet bulunmadığı için 3G usb modem aracılığıyla farklı lokasyondaki veri tabanı sunucusuna gönderilmektedir. Mimari yapı Şekil 4.2'de gösterildiği gibi hem sahadan 3G modemle verilerin veri tabanı sunucusuna ulaştırılmasını hem de uzak kullanıcıların veri tabanına erişimini yine 3G bağlantısı ile gerçekleştirmesini sağlamaktadır.

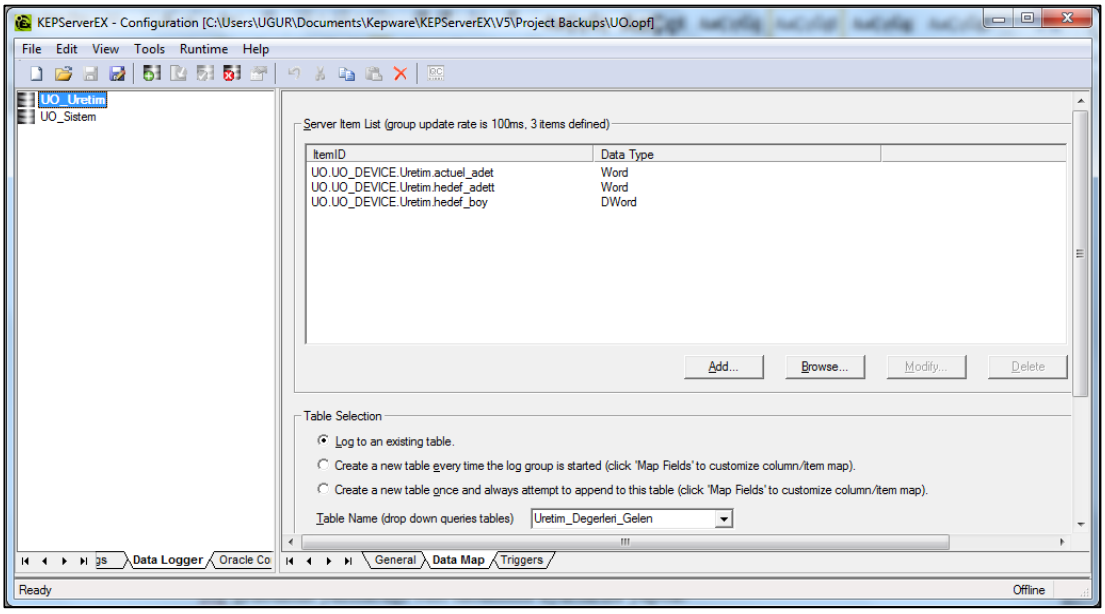
Sunucuya aktarılacak verilerin seçimi kullanıcı tipleri dikkate alınarak gerçekleştirilmiştir. Bu kapsamda yöneticilere ve işletme mühendislerine yönelik olarak demir plaka boyu ve sayısı, sistemin çalışma süresi ve motor akım değerleri örnek veriler olarak alınmaktadır. Sistemden alınan verilerden Demir Plaka boyu ve sayısı, sistemin çalışma süresi, günlük üretim raporu ve stok kontrol için, motor akım değerleri de uyarı sistemi için kullanılmaktadır.

OPC sunucusundan SQL Veri tabanına verileri aktarmak için öncelikle Siemens Simatic Manager'de hazırlanan projeden sisteme alınacak verilerin etiket adı ve network adresleri tespit edilmiştir. OPC sunucusunda Kanal, Cihaz, Etiket Grubu ve etiketleri oluşturulmuştur. Şekil 4.3'te OPC sunucusunda oluşturulan kanal, cihaz ve etiketler gösterilmektedir.

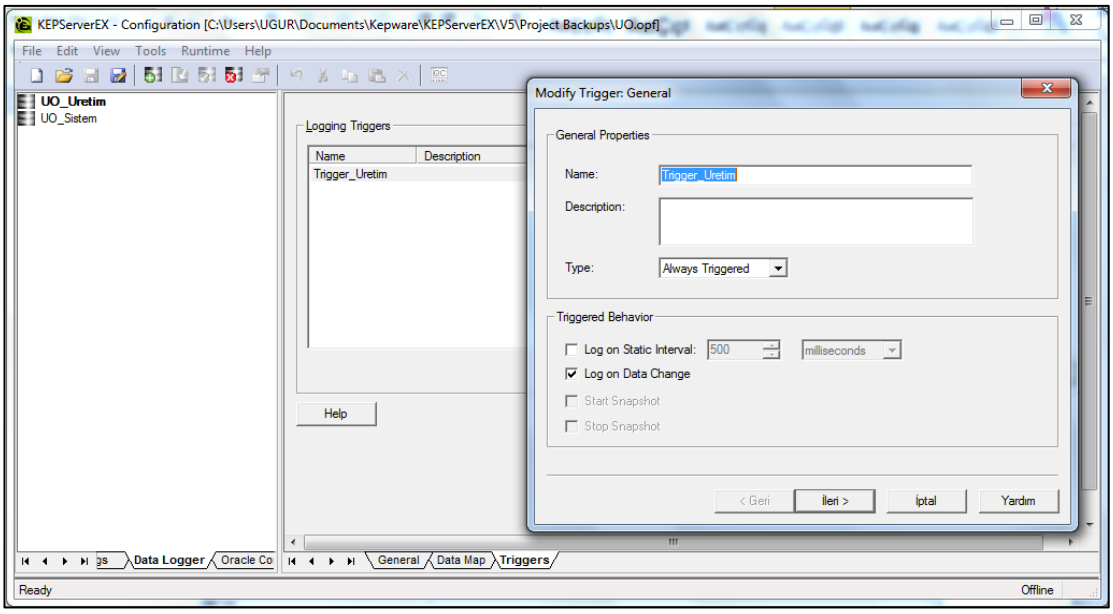


Şekil 4.3. OPC sunucusundaki kanal, cihaz ve etiketlerin oluşturulması.

Projede bulunan üretim ve sistem değerleriyle ilgili verileri almak için veri tabanında tablolar hazırlanmış, OPC sunucusunda bu tablolar üzerine verileri aktarmak için log grupları oluşturulmuştur. Daha sonra sistem ve üretim log grubuna ilgili etiketler eklenmiştir. OPC sunucusundaki log grupları ve etiketleri Şekil 4.4'te gösterilmektedir.



Şekil 4.4. OPC sunucusundaki log grupları ve etiketleri.



Şekil 4.5. OPC sunucusundaki tetikleyicilerin oluşturulması.

Son olarak değerlerin ne sıklıkla veri tabanına yazılacağını belirleyen triggerler (tetikleyici) oluşturulmuştur. OPC sunucusundaki tetikleyicilerin oluşturulması Şekil 4.5'te gösterilmektedir.

Bu ayarlar yapıldıktan sonra sistem ve üretime yönelik gerekli veriler veri tabanında tutulmaya başlanmıştır.

4.3.6. Web Uygulaması

Uygulama üç ana başlık altında değerlendirilmiştir.

1. Web Kullanıcıları ve Web Sayfaları
2. Web Güvenliği
3. Web Logları

4.3.6.1. Web Kullanıcıları ve Web Sayfaları

Web Kullanıcıları

Otomasyonda fonksiyonel bazda bir sınıflandırmaya giderek 3 farklı tipte Kullanıcı oluşturulmuştur. Bunlar;

1. Mühendis: Otomasyon sistemin takibi ve oluşabilecek arızalara müdahale edebilecek fonksiyonlara sahiptir.
2. Yönetici: Daha çok üretim sonuçları hakkında bilgileri elde edebilecek yapıda tasarlanmıştır.
3. Sistem Yöneticisi: Oluşturulan sistemin sağlıklı çalışabilmesi için gerekli hizmetlere yönelik fonksiyonlara sahiptir.

Web Sayfaları

Kullanıcılar sahip olduğu fonksiyonlara göre web sayfalarını kullanabilmektedir. Aşağıda anlatılacak olan web sayfaları işlevlerine göre anlatılmaktadır. Kullanıcı tiplerine göre sayfa erişim bilgisi bölüm sonunda çizelge 4.1.'de gösterilmektedir.

Uzak Yardım

Birçok alanda olduğu gibi endüstriyel otomasyon sistemlerinde de uzaktan yardım alıp problemleri çözmek çok sık kullanılan bir çözüm yoludur. Uzaktan yardım ile sistem gerçek zamanlı olarak izlenebilmekte, Scada veya PLC ile ilgili olarak değiştirilmesi veya eklenmesi gereken bir proje çözümü varsa uzak yardımla yüklenebilmekte ve sistemle ilgili yedekleme, bakım vb. işlemler kolaylıkla yapılabilmektedir. Ayrıca sahada çalışan mühendislerde yaptıkları çalışmaların sonucunu bu sistem üzerinden kontrol edebilmektedir.

Uzaktan yardım günümüzde değişik yazılımlar aracılığıyla yapılmaktadır. Windows uzak masaüstü web bağlantısı, teamviewer, ammyy vb. yazılımlar bu amaçla kullanılmaktadır. Uzak yardım şekillerinin hepsinde de yardım isteyen tarafın izni

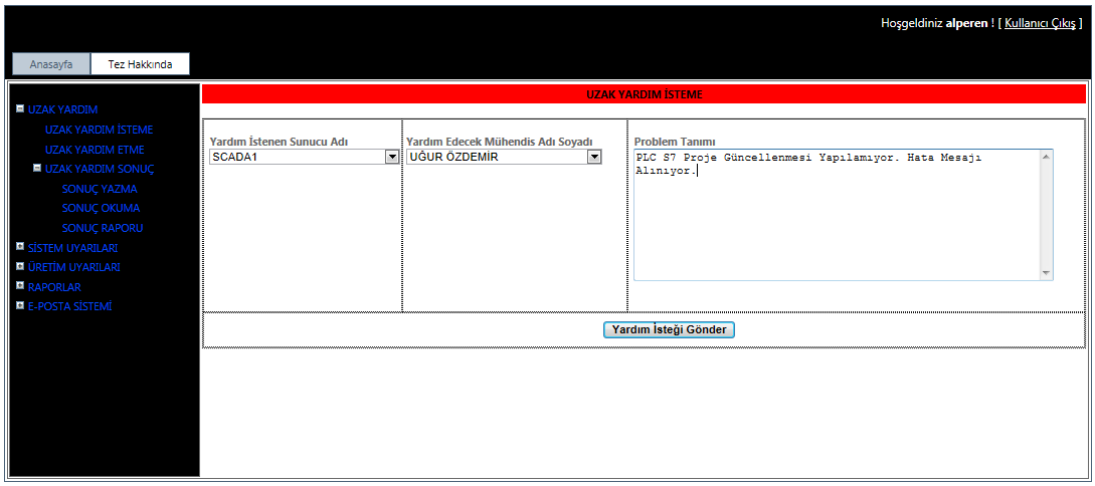
dahilinde bağlantı yapılabilmektedir. Fakat işletim sisteminin açılışında bu yazılımlar otomatik olarak çalıştırılıyorsa kullanıcı adı, parola vb. bilgilerini bilen kişiler sisteme rahatlıkla bağlantı yapabilmektedir. Farklı kişilerden yardım alınıyorsa sürekli sunucu erişim bilgilerinin bu kişilere de iletilmesi gerekmektedir ve bunun sonucunda sisteme erişim bilgileri birçok kişinin elinde bulunacağından sistem güvenliği açısından büyük bir risk ortaya çıkabilmektedir.

Örnek uygulamada; uzak yardım edilecek sunucuların IP adresi, kullanıcı adı ve parola bilgilerinin güvenliğini sağlamak için sunucuların bilgileri veri tabanı sunucusunda tutulmakta ve uzak yardım etme işlemi bu bilgilerin görülmediği bir web sayfası üzerinden yapılmaktadır. Uzak yardım işleminde arka planda Windows uzak masaüstü web bağlantı yazılımı kullanılmaktadır. Uzak yardım web sayfası veri tabanından aldığı sunucu bilgilerini uzak masaüstü web bağlantı yazılımına gönderip uzak yardımı etme işlemini başlatmaktadır.

Uzak yardım işlemi dört aşamadan oluşmaktadır.

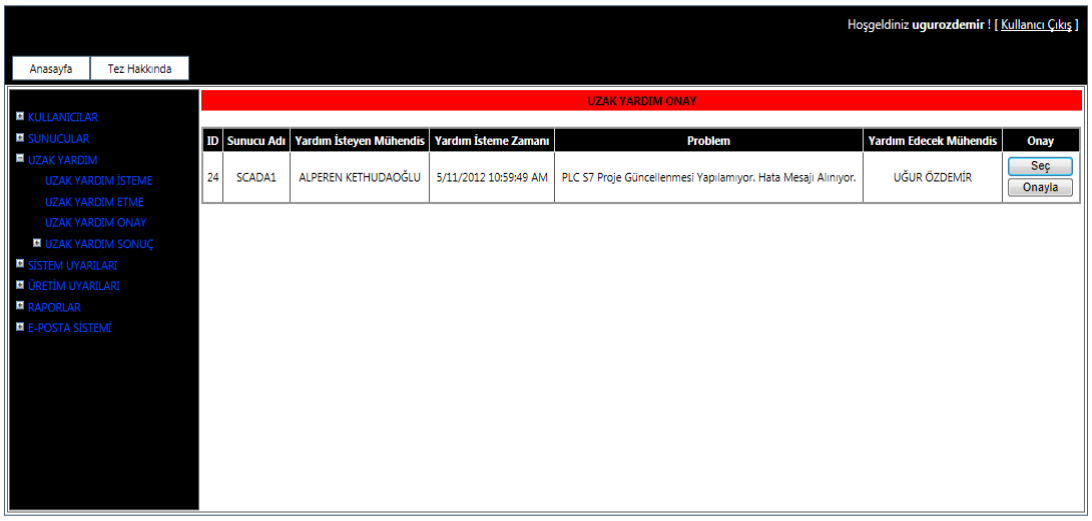
1. Uzak Yardım İsteme
2. Uzak Yardım Onay
3. Uzak Yardım Etme
4. Uzak Yardım Sonuç

Uzak Yardım İsteme: Mühendis yardım almak istediği sunucuyu, yardım istediği mühendisi kendi web sayfasından seçer ve karşılaşılan problemi tanımlayarak yardım isteğini başlatır. Uzak yardım isteme sayfa görüntüsü Şekil 4.6’da gösterilmektedir.



Şekil 4.6. Uzak yardım isteme sayfa görüntüsü.

Uzak Yardım Onay: Yapılmış olan yardım istekleri sistem yöneticisinin web sayfasında görünür. Sistem yöneticisi durumu kontrol ettikten sonra onaylar veya bu isteği iptal eder. Onaylanan yardım isteği e-posta ile yardım edecek mühendise gönderilir. Ayrıca mühendisin web sayfasında da görünür. Uzak yardım onay sayfa görüntüsü Şekil 4.7'de gösterilmektedir.



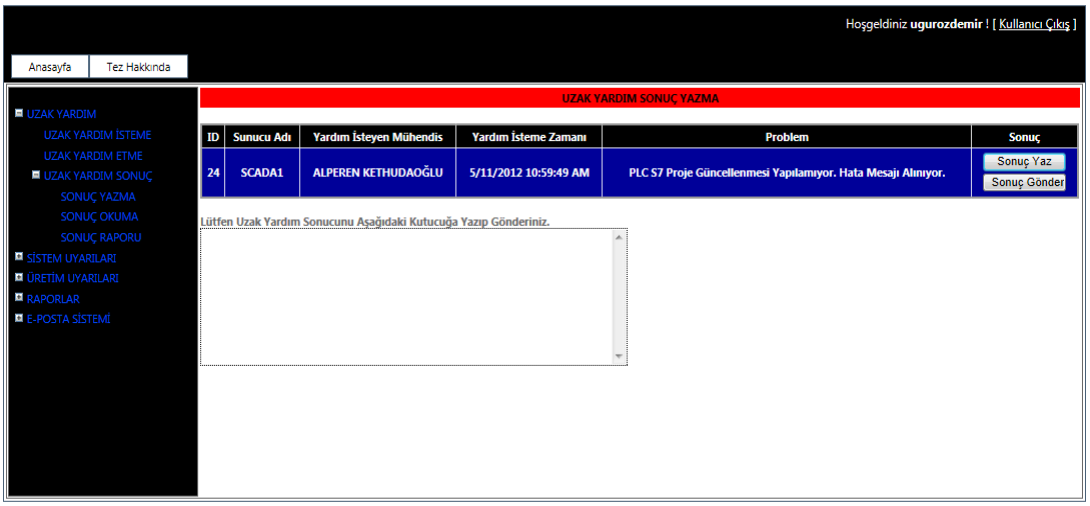
Şekil 4.7. Uzak yardım onay sayfa görüntüsü.

Uzak Yardım Etme: Uzak yardım isteğini kendisine gönderilen e-postadan veya web sayfasından haber alan mühendisin uzak yardım etme işlemini yaptığı bölümdür. Uzak yardım etme sayfa görüntüsü Şekil 4.8'de gösterilmektedir.

Şekil 4.8. Uzak yardım etme sayfa görüntüsü.

Uzak Yardım Sonuç Yazma

Uzak yardım eden mühendisin yaptığı çalışma neticesinde problemin çözümünü ve yaptığı işlemleri sisteme girdiği ve uzak yardım işleminin tamamlandığı bölümdür. Uzak yardım sonuç yazma sayfa görüntüsü Şekil 4.9'da gösterilmektedir.

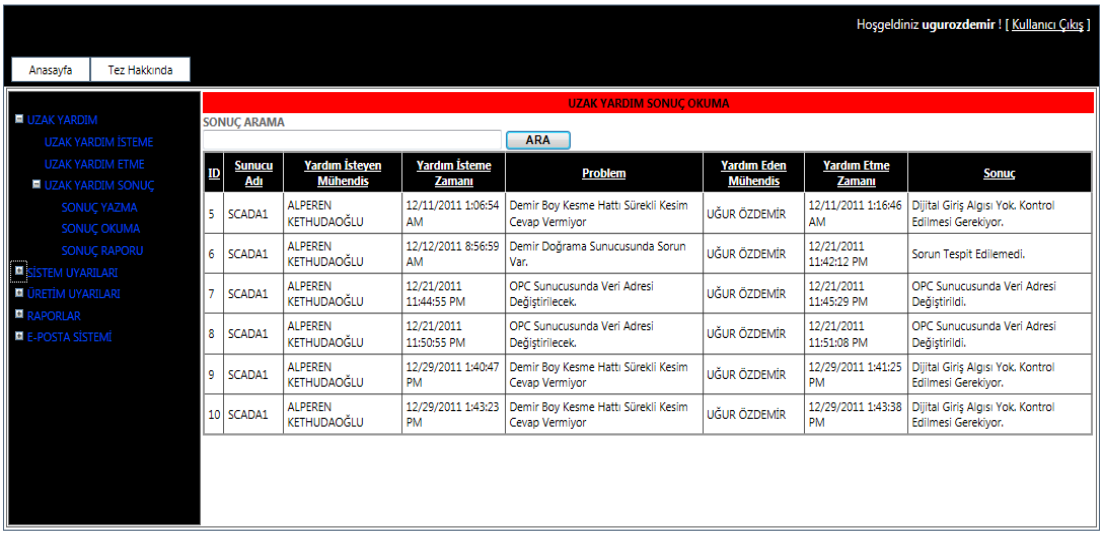


Şekil 4.9. Uzak yardım sonuç yazma sayfa görüntüsü.

Uzak Yardım Sonuç Okuma

Bu bölümde mühendisler geriye dönük uzak yardım bilgileri, sistemde yaşanan problemler ve çözümleri gibi bilgileri okuyabilmektedir. Ayrıca yeni bir problemle karşılaşıldığında bu veri tabanından sorgulama yaparak çözüm aranabilmekte ve eğer yeterli bir çözüm bulunursa uzak yardım isteği oluşturmaya gerek kalmadan problem çözülebilmektedir. Yardım isteklerinin başlatılmasında problemle ilgili olarak

çalışmış mühendisin kim olduğunun buradan görülebilmesi de çözüm sürecini kolaylaştırmaktadır. Uzak yardım sonuç okuma sayfa görüntüsü Şekil 4.10'da gösterilmektedir.

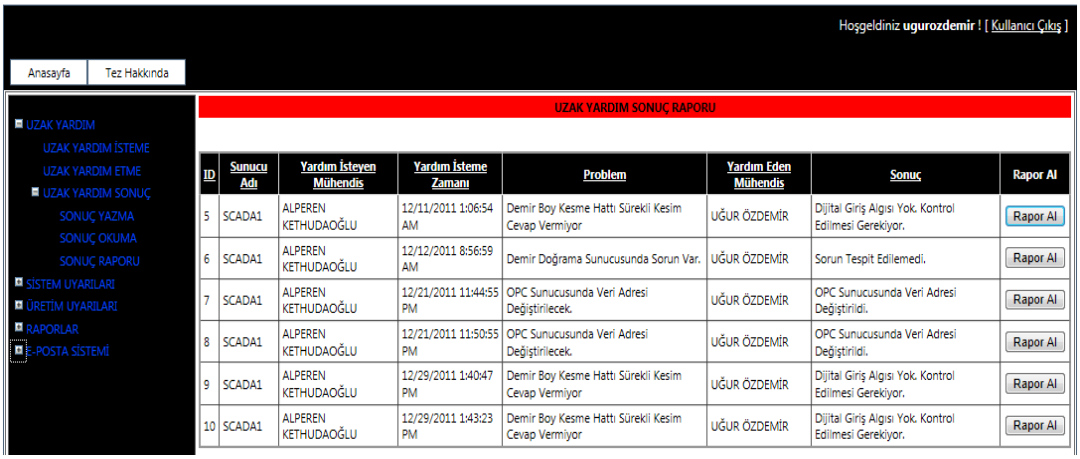


ID	Sunucu Adı	Yardım İsteyen Mühendis	Yardım İsteme Zamanı	Problem	Yardım Eden Mühendis	Yardım Etme Zamanı	Sonuç
5	SCADA1	ALPEREN KETHUDAOĞLU	12/11/2011 1:06:54 AM	Demir Boy Kesme Hattı Sürekli Kesim Cevap Vermiyor	UĞUR ÖZDEMİR	12/11/2011 1:16:46 AM	Dijital Giriş Algısı Yok. Kontrol Edilmesi Gerekiyor.
6	SCADA1	ALPEREN KETHUDAOĞLU	12/12/2011 8:56:59 AM	Demir Doğrama Sunucusunda Sorun Var.	UĞUR ÖZDEMİR	12/21/2011 11:42:12 PM	Sorun Tespit Edilemedi.
7	SCADA1	ALPEREN KETHUDAOĞLU	12/21/2011 11:44:55 PM	OPC Sunucusunda Veri Adresi Değiştirilecek.	UĞUR ÖZDEMİR	12/21/2011 11:45:29 PM	OPC Sunucusunda Veri Adresi Değiştirildi.
8	SCADA1	ALPEREN KETHUDAOĞLU	12/21/2011 11:50:55 PM	OPC Sunucusunda Veri Adresi Değiştirilecek.	UĞUR ÖZDEMİR	12/21/2011 11:51:08 PM	OPC Sunucusunda Veri Adresi Değiştirildi.
9	SCADA1	ALPEREN KETHUDAOĞLU	12/29/2011 1:40:47 PM	Demir Boy Kesme Hattı Sürekli Kesim Cevap Vermiyor	UĞUR ÖZDEMİR	12/29/2011 1:41:25 PM	Dijital Giriş Algısı Yok. Kontrol Edilmesi Gerekiyor.
10	SCADA1	ALPEREN KETHUDAOĞLU	12/29/2011 1:43:23 PM	Demir Boy Kesme Hattı Sürekli Kesim Cevap Vermiyor	UĞUR ÖZDEMİR	12/29/2011 1:43:38 PM	Dijital Giriş Algısı Yok. Kontrol Edilmesi Gerekiyor.

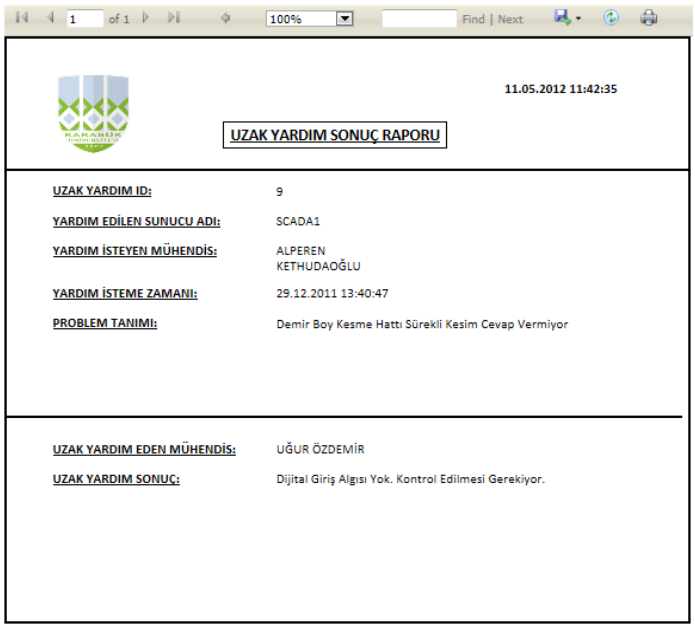
Şekil 4.10. Uzak yardım sonuç okuma sayfa görüntüsü.

Uzak Yardım Sonuç Raporu

Uzak yardım sonuç raporu ile sistemden Excel, Pdf ve Word formatında yapılan uzak yardım sonuç raporu alınabilmekte veya yazıcıdan çıktı alınabilmektedir. Bu raporda yardım edilen sunucu, yardım isteyen mühendis, yardım eden mühendis gibi uzak yardım ile ilgili bütün bilgiler bulunmaktadır. Alınan yazıcı çıktısı mühendise imzalatılarak bu uzak yardımın yazılı ortamda da resmiyet kazanması sağlanabilmektedir. Uzak yardım sonuç raporu sayfa görüntüsü Şekil 4.11'de ve uzak yardım sonuç raporu görüntüsü Şekil 4.12'de gösterilmektedir.



Şekil 4.11. Uzak yardım sonuç raporu alma sayfa görüntüsü.



Şekil 4.12. Uzak yardım sonuç raporu görüntüsü.

Raporlar

Bu bölümde; otomasyon sisteminden OPC sunucusu aracılığıyla veri tabanına aktarılan verilerden sistemin çalışmasına ve üretime yönelik raporlama yapılmaktadır. Mühendisler ve yöneticilerin ihtiyaçları doğrultusunda raporlar oluşturulabilmektedir. Örnek uygulamada sistemden alınan raporlar maddeler halinde belirtilmektedir.

1. Sistem Raporları

Demir boy kesme hattının günlük ve genel çalışma sürelerine yönelik raporlar sistemden alınabilmektedir.

2. Üretim Raporları

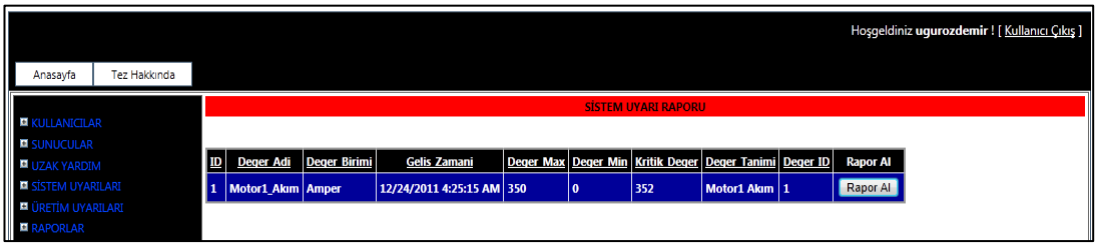
Demir boy kesme hattında farklı boylarda kesilen demirlerin üretimine yönelik günlük ve genel üretim raporları alınabilmektedir.

3. Uyarı Raporları

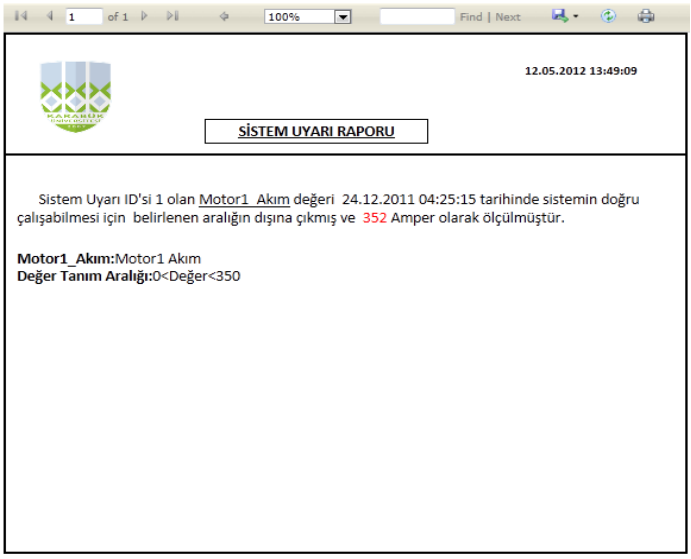
Demir boy kesme hattında oluşan sisteme ve üretime yönelik uyarıların raporları alınabilmektedir.

Sistem Uyarı Raporu

Sistem uyarı raporu bölümünde ise uyarı mesajı ile ilgili bilgileri Excel, Pdf, Word belgesi veya yazıcı çıktısı olarak alınabilmektedir. Sistem uyarı raporu sayfa görüntüsü Şekil 4.13'te ve sistem uyarı raporu görüntüsü Şekil 4.14'te gösterilmektedir.



Şekil 4.13. Sistem uyarı raporu sayfa görüntüsü.



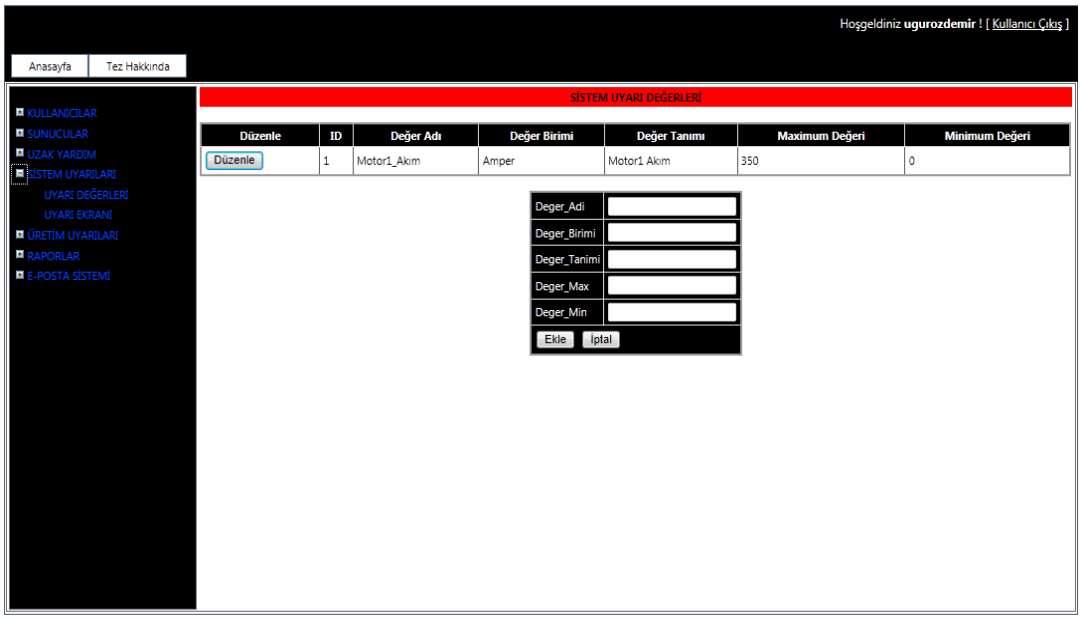
Şekil 4.14. Sistem uyarı raporu görüntüsü.

Sistem ve Üretim Uyarıları

Bu bölümlerde sisteme ve üretime yönelik belirlenen değerler takip edilmektedir ve bu değerler tanım aralıklarının dışına çıktığında mühendis ve yöneticiler uyarı sisteminin gönderdiği uyarı e-postaları ile haberdar edilmektedir.

Sistem Uyarı Değerleri

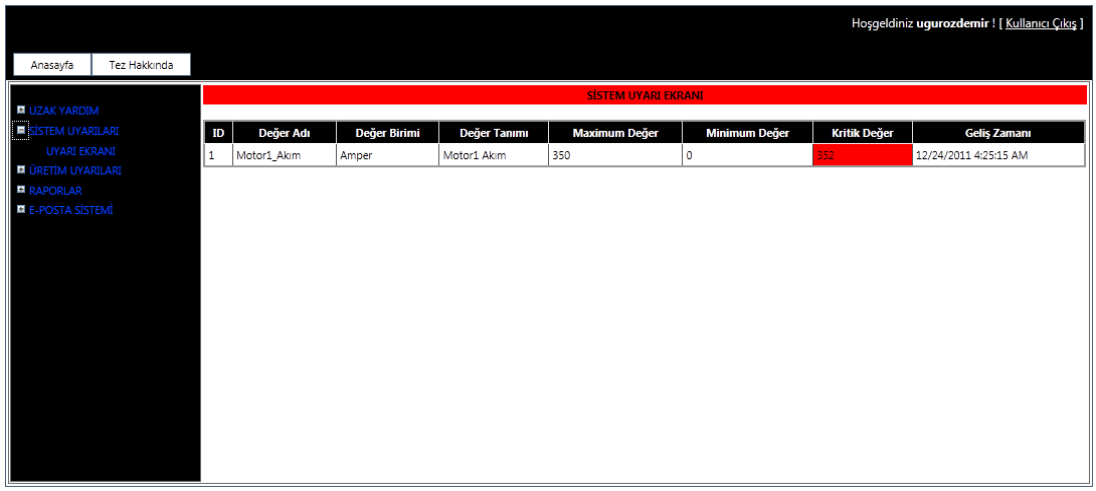
Endüstriyel otomasyon sistemlerinin performanslı ve doğru bir şekilde çalışabilmesi için sürekli kontrol edilmesi gereken bazı değerler (akım, gerilim, basınç, yağ seviyesi vb.) vardır. Bu değerler belirlenen tanım aralıklarının dışına çıktığı zaman sistemi tehlikeye sokabilecek durumlar ortaya çıkabilmektedir. Birçok sistemde bu durumu kontrol eden bir mekanizma bulunmaktadır. Örnek uygulamada bu mekanizmalara ek olarak Kepware OPC sunucusu aracılığıyla Siemens S7 300'den demir boy kesme hattındaki motor akım değerleri veri tabanı sunucusuna aktarılmaktadır. Sistem uyarı değerleri web sayfasında motor akım değerinin tanım aralıkları sisteme girilebilmektedir. Sistem uyarı değerleri sayfa görüntüsü Şekil 4.15'te gösterilmektedir.



Şekil 4.15. Sistem uyarı değerleri sayfa görüntüsü.

Sistem Uyarı Ekranı

Veri tabanı sunucusuna gelen değerler içerisinden tanımlanan aralığının dışına çıkan değerleri triggerler yardımıyla oluşturulan kritik değerler tablosuna gönderilmektedir ve sistem uyarı ekranına bu değerler yansıtılmaktadır. Şekil 4.16'da sistem uyarı ekranı sayfa görüntüsü gösterilmektedir.



Şekil 4.16. Sistem uyarı ekranı sayfa görüntüsü.

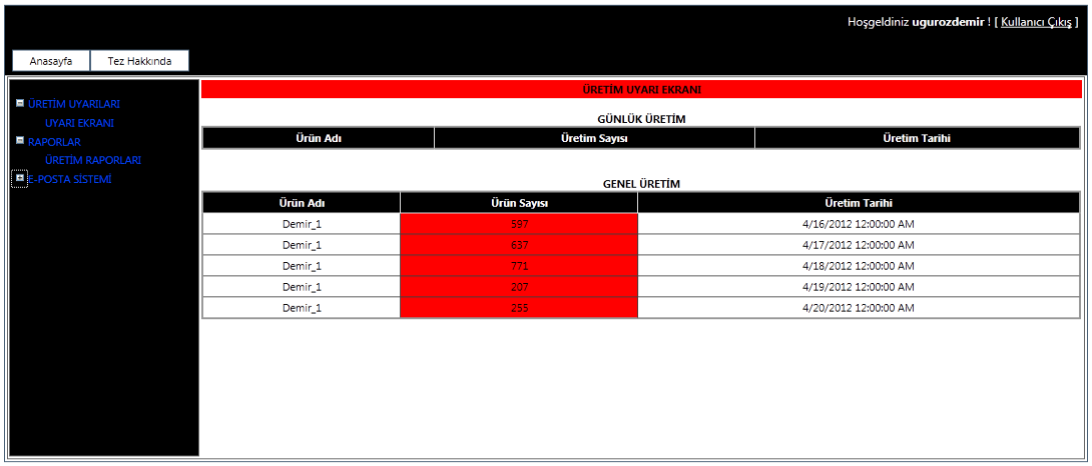
Tanımlanan aralığın dışına çıkan değer ile ilgili uyarı mesajı görevli mühendise e-posta olarak gönderilmektedir ve bu durumdan haberdar olan mühendis sisteme uzaktan müdahale ederek oluşabilecek tehlikeleri önleyebilmektedir.

Üretim Uyarı Değerleri

Endüstriyel otomasyon sistemlerinde üretime yönelik veriler satın alma, satış, stok kontrol, sipariş ve finansal işlemlerin gerçekleştirilmesinde yol gösterici bir rol oynamaktadır. Bu sebeple sistemden alınıp sürekli kontrol edilmesi gerekmektedir. Bu üretim değerleri belirlenen tanım aralıklarının dışına çıktığı zaman iş akışını geciktirecek durumlar ortaya çıkabilmektedir. Birçok sistemde bu durumu kontrol eden bir mekanizma bulunmaktadır. Örnek uygulamada bu mekanizmalara ek olarak Kepware OPC sunucusu aracılığıyla Siemens S7 300'den demir boy kesme hattından demir boylarına göre üretim değerleri veri tabanı sunucusuna aktarılmaktadır. Üretim uyarı değerleri web sayfasında demir boy tipleri ve tanım aralıkları sisteme girilebilmektedir.

Üretim Uyarı Ekranı

Veri tabanı sunucusuna gelen üretim değerleri yönetici tarafından tanımlanan aralığının dışına çıkan değerleri triggerler yardımıyla oluşturulan kritik değerler tablosuna gönderilmektedir. Ayrıca günlük ve genel üretim bilgileri de uyarı ekranına yansıtılmaktadır. Şekil 4.17’de üretim uyarı ekranı sayfa görüntüsü gösterilmektedir.



Şekil 4.17. Üretim uyarı ekranı sayfa görüntüsü.

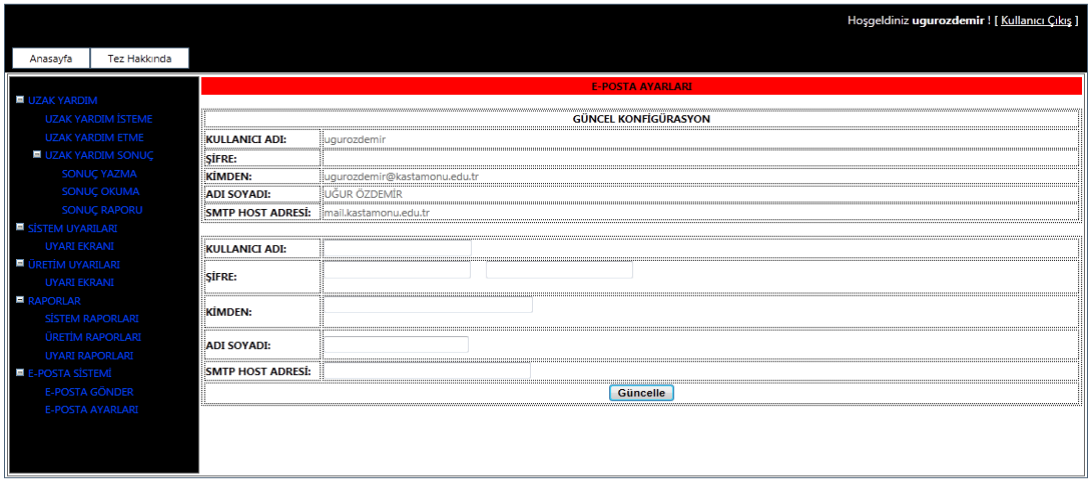
Tanımlanan aralığın dışına çıkan değerler için ilgili uyarı mesajı görevli yöneticiye e-posta olarak gönderilmektedir. Bu durumdan haberdar olan yönetici satış, stok kontrol ve ürün teslimi gibi işlemleri zamanında gerçekleştirebilmektedir ve oluşabilecek aksaklıklar engellenmektedir.

E-Posta Sistemi

Uygulamanın birçok bölümünde kullanılan ve sistem tarafından gönderilen e-postaların dışında; bu bölümde kullanıcılar sistem üzerinden kendi e-posta hesaplarına girmelerine gerek kalmadan e-posta gönderebilmektedir. E-posta gönderme işlemi e-posta sunucularının belirledikleri kimlik doğrulama yöntemleri çerçevesinde gerçekleştirilmektedir. Open-Relay, Basit Kimlik Doğrulama, SSL/TLS'li kimlik doğrulama yöntemleri bunlardan bazılarıdır. Uygulamada bu üç yöntemde kullanılabilmektedir.

E-Posta Ayarları

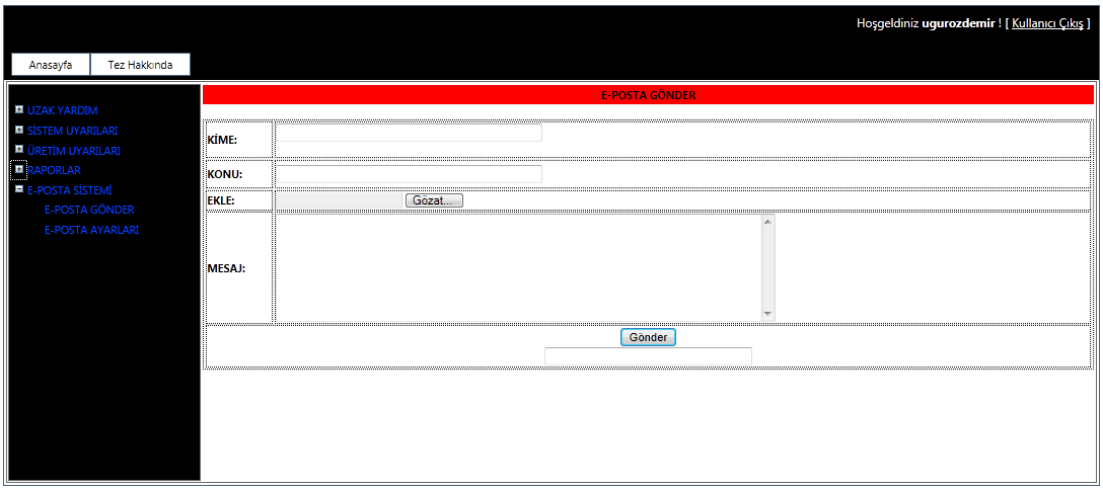
E-posta gönderebilmek için kullanıcıların smtp sunucu adı, kullanıcı adı ve parola bilgilerinin sisteme girildiği bölümdür. E-Posta ayarları sayfa görüntüsü Şekil 4.18'de gösterilmektedir.



Şekil 4.18. E-Posta ayarları sayfa görüntüsü.

E-Posta Gönder

Kullanıcılar e-posta ayarlarını yaptıktan sonra bu bölümden Kime, Konu, Ekle, Mesaj alanlarını doldurarak e-posta gönderebilmektedirler. Şekil 4.19'da e-posta gönder sayfa görüntüsü gösterilmektedir.



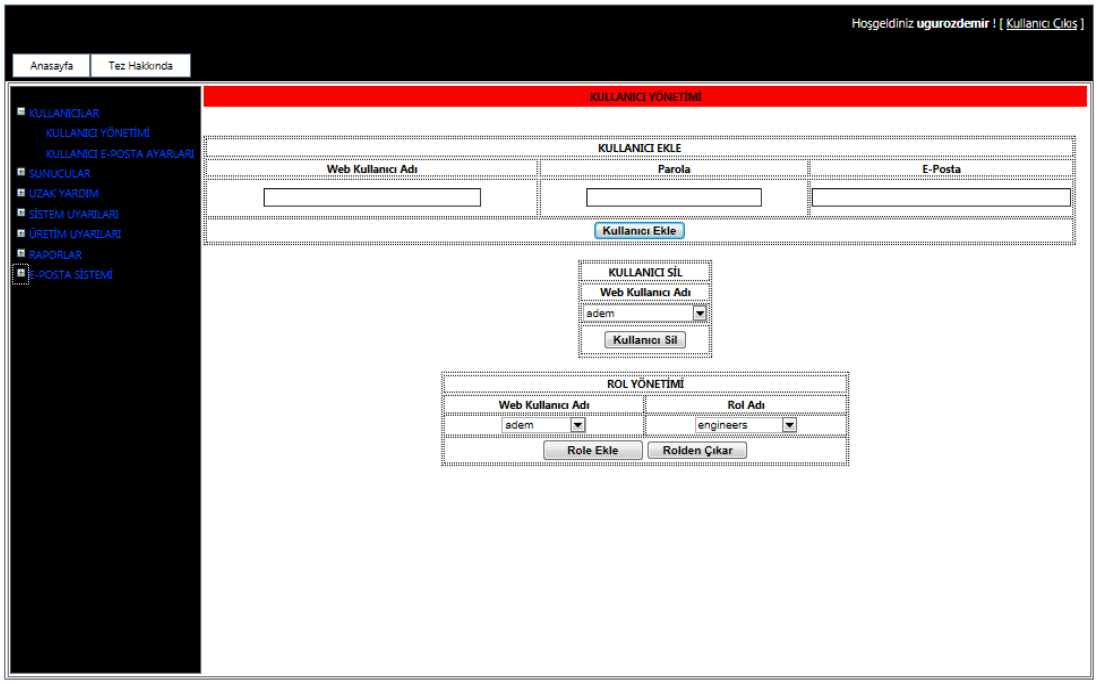
Şekil 4.19. E-Posta gönder sayfa görüntüsü.

Kullanıcılar

Sistemde bulunan kullanıcıların (mühendis, yönetici vb.) oluşturulduğu, düzenlendiği ve kullanıcı e-posta ayarlarının güncellenebildiği bölümdür.

Kullanıcı Yönetimi

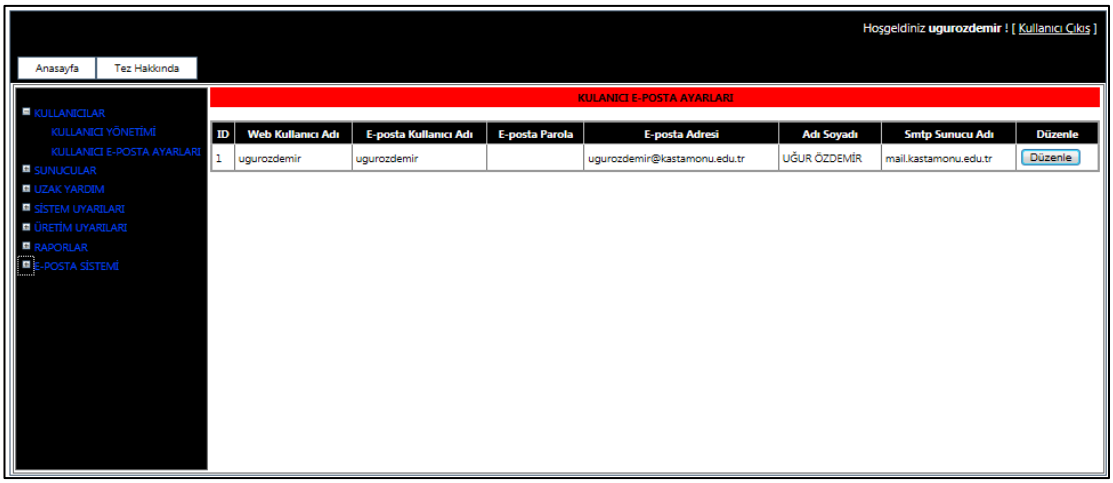
Sistemde bulunan kullanıcıların bilgilerinin düzenlenebildiği sayfadır. Kullanıcı yönetimi sayfa görüntüsü Şekil 4.20'de gösterilmektedir.



Şekil 4.20. Kullanıcı yönetimi sayfa görüntüsü.

Kullanıcı E-Posta Ayarları

Sistemde bulunan kullanıcıların girmiş olduğu ayarların bulunduğu ve bu ayarların düzenlenebildiği sayfadır. Kullanıcı e-posta ayarları sayfa görüntüsü Şekil 4.21'de gösterilmektedir.



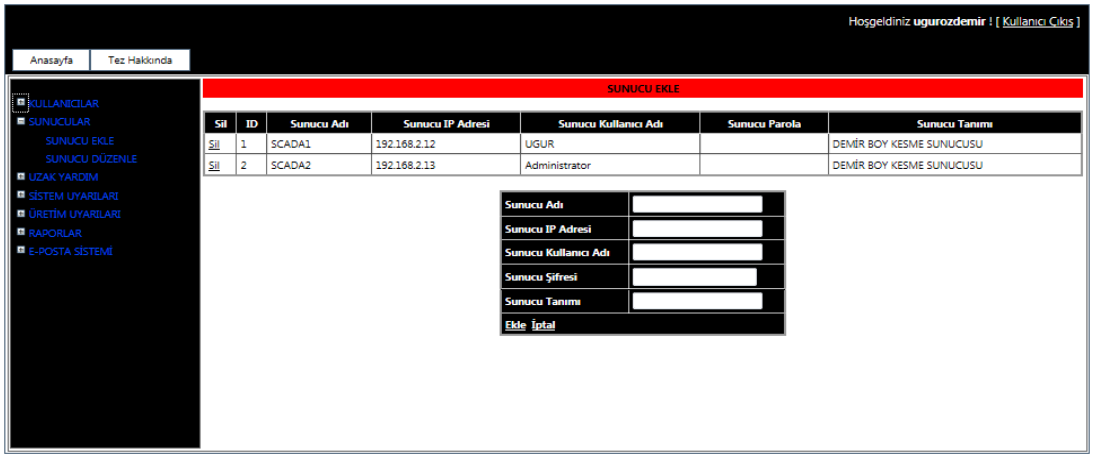
Şekil 4.21. Kullanıcı e-posta ayarları sayfa görüntüsü.

Sunucular

Otomasyon sisteminde uzak yardım edilecek sunucuların eklendiği ve düzenlendiği bölümdür.

Sunucu Ekle

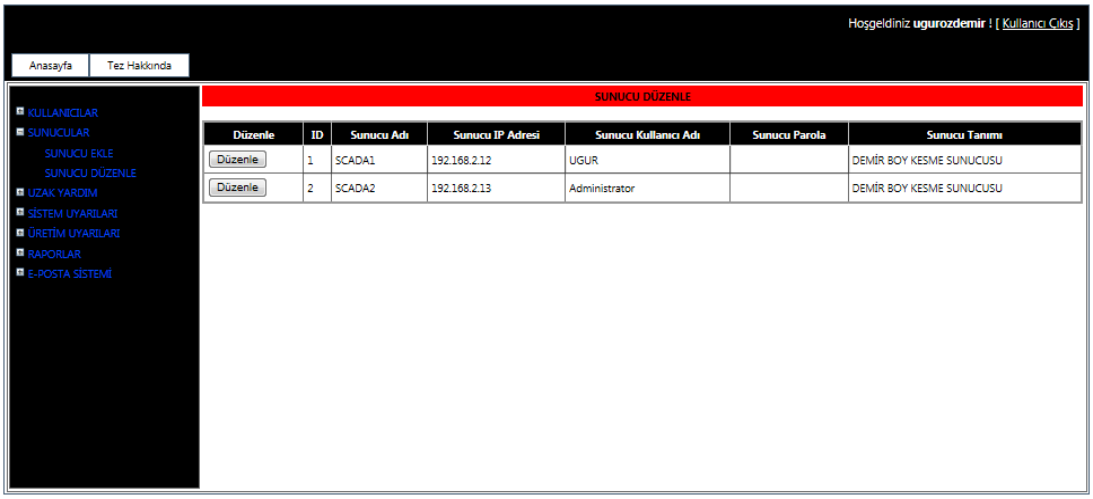
Uzak yardım edilecek sunucuların eklenebildiği uzak bağlantı için gerekli olan kullanıcı adı, parola, ip adresi vb. bilgilerin girilebildiği Uzak yardım edilecek sunucuların eklendiği sayfadır. Şekil 4.22'de sunucu ekle sayfa görüntüsü gösterilmektedir.



Şekil 4.22. Sunucu ekle sayfa görüntüsü.

Sunucu Düzenle

Sunucuların kullanıcı adı, parola vb. bilgilerinin güncellenebildiği sayfadır. Sunucu düzenle sayfa görüntüsü Şekil 4.23'te gösterilmektedir.



Şekil 4.23. Sunucu düzenle sayfa görüntüsü.

Çizelge 4.1. Kullanıcıların web sayfası erişim yetkileri.

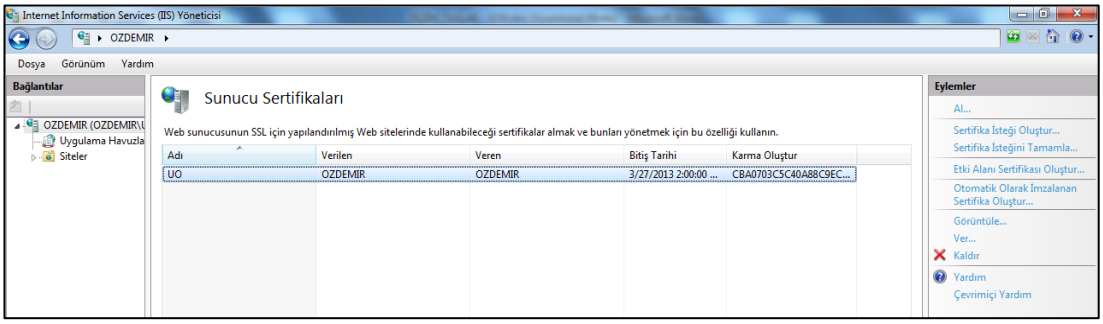
Kullanıcı Web Sayfaları	Mühendis	Yönetici	Sistem Yöneticisi
Uzak Yardım İsteme	X	-	X
Uzak Yardım Etme	X	-	X
Uzak Yardım Onay	-	-	X
Uzak Yardım Sonuç	X	-	X
Sistem Uyarı Değerleri	-	-	X
Sistem Uyarı Ekranı	X	-	X
Üretim Uyarı Değerleri	-	-	X
Üretim Uyarı Ekranı	-	X	X
Sistem Raporları	X	-	X
Üretim Raporları	X	X	X
Sistem Uyarı Raporu	X	-	X
Üretim Uyarı Raporu	-	X	X
E-Posta Sistemi	X	X	X

4.3.6.2. Web Güvenliği

İnternetten yapılan saldırılar arasında web sunucularına yapılan saldırılar ilk sıralarda yer alır. Bu saldırılarda amaç öncelikli olarak web sayfası üzerinden önemli bilgilere erişmek ve bu bilgileri kötü amaçlar için kullanmaktır. Bu saldırılarda elde edilen kullanıcı adı, parola ve IP adresi gibi önemli bilgiler saldırganların sunuculara ve veri tabanlarına rahat bir şekilde erişmesine imkân sağlamaktadır. Kullanıcılar internet üzerinden bir web uygulamasındaki hesablarına girecekleri zaman kullanıcı adı ve parola gibi bilgileri HTTP (Hypertext Transfer Protocol) veya HTTPS (Secure Hypertext Transfer Protocol) protokolü aracılığıyla gönderilmektedir. Bu iki protokol arasındaki en önemli fark http'de bilgiler açık formatta gönderilirken, HTTPS'de SSL (secure sockets layer) adı verilen ve kullanıcının bilgisayarı ile sunucu arasında gönderilen bilgilerin şifreli bir şekilde iletildiği güvenlik katmanı üzerinden gönderilmektedir. Bu bilgiler HTTP'de TCP port 80 HTTPS'de ise TCP port 443'ten gönderilmektedir. HTTPS protokolünün ortaya çıkmasında E-ticaret sistemlerinin yaygınlaşması ve bu sistemlerin güvenliğinin sağlanmasının büyük rolü vardır. Günümüzde hemen hemen her web uygulamasında HTTPS protokolü üzerinden kimlik doğrulaması yapılmaktadır. Bu protokolde kullanılan güvenlik algoritmasının çözülmesi çok zordur. Bu algoritmaların çözülmesi için güçlü donanımlara sahip sistemler ve çok uzun zaman gerekmektedir. Fakat bu güvenlik önlemini aşmak için başka yöntemler kullanılmaktadır. Network üzerinden yapılan saldırılar neticesinde bu şifreleme algoritmasının çözümlenmesine gerek kalmadan kullanıcılar aldatılarak bilgileri elde edilmektedir. ARP spoofing ve DNS spoofing yapan saldırgan kullanıcıyı iki şekilde kandırabilmektedir. Bunlardan birincisinde, kendi sertifikasını sunucunun sertifikası gibi gönderir ve kullanıcı kabul ederse tüm verileri kolayca okuyabilir. İkinci yöntemde ise HTTPS isteğinde bulunan kullanıcıyı DNS spoofing yaparak HTTP sayfasına yönlendirir ve eğer kullanıcı sayfanın HTTP olduğunu fark etmezse yine tüm bilgileri saldırgan rahatlıkla okuyabilir [31]. Bu saldırıları önlemek network saldırıları bölümünde anlatılan önlemlerin alınması gereklidir.

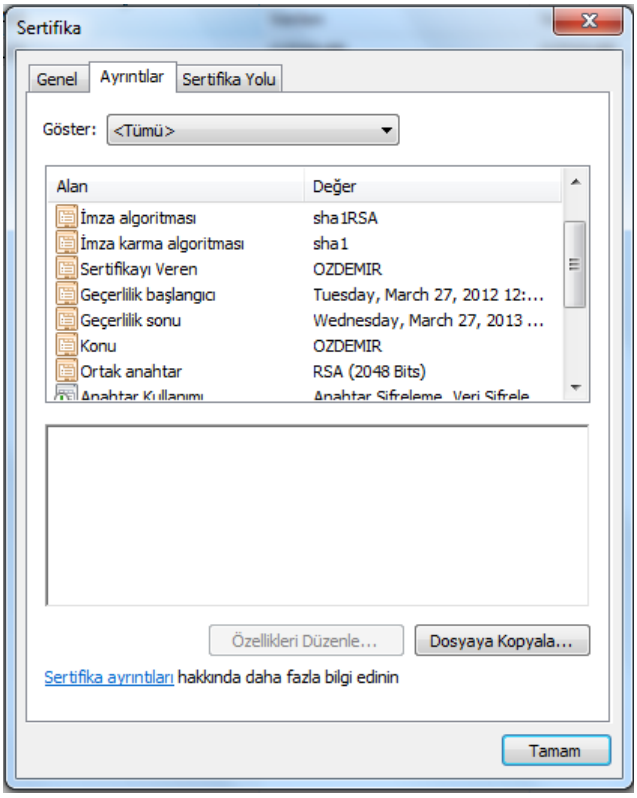
Endüstriyel otomasyon sistemlerinin güvenliğinin çok önemli olmasından sebebiyle örnek uygulamada veriler HTTPS protokolü kullanılarak gönderilmektedir. Bu protokol için gerekli olan SSL sertifikası windows internet information servisindeki

sunucu sertifikası bölümünde otomatik olarak oluşturulabilmektedir. Şekil 4.24. IIS sunucu sertifikası oluşturma bölümü gösterilmektedir.



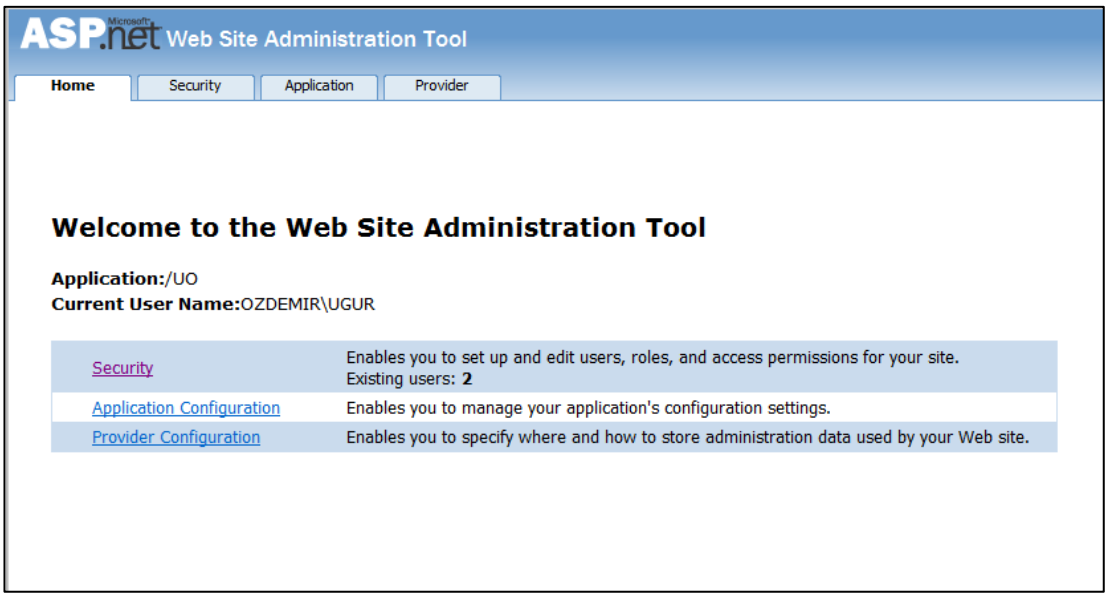
Şekil 4.24. IIS sunucu sertifikası oluşturma bölümü.

Oluşturulan sertifikada sha1 şifreleme algoritması kullanılmaktadır. Bu algoritma 160 bitlik bir hash yapısı kullanmaktadır. IIS (Internet Information Servis)'te oluşturulan sunucu sertifikası özellikleri Şekil 4.25'te gösterilmektedir.



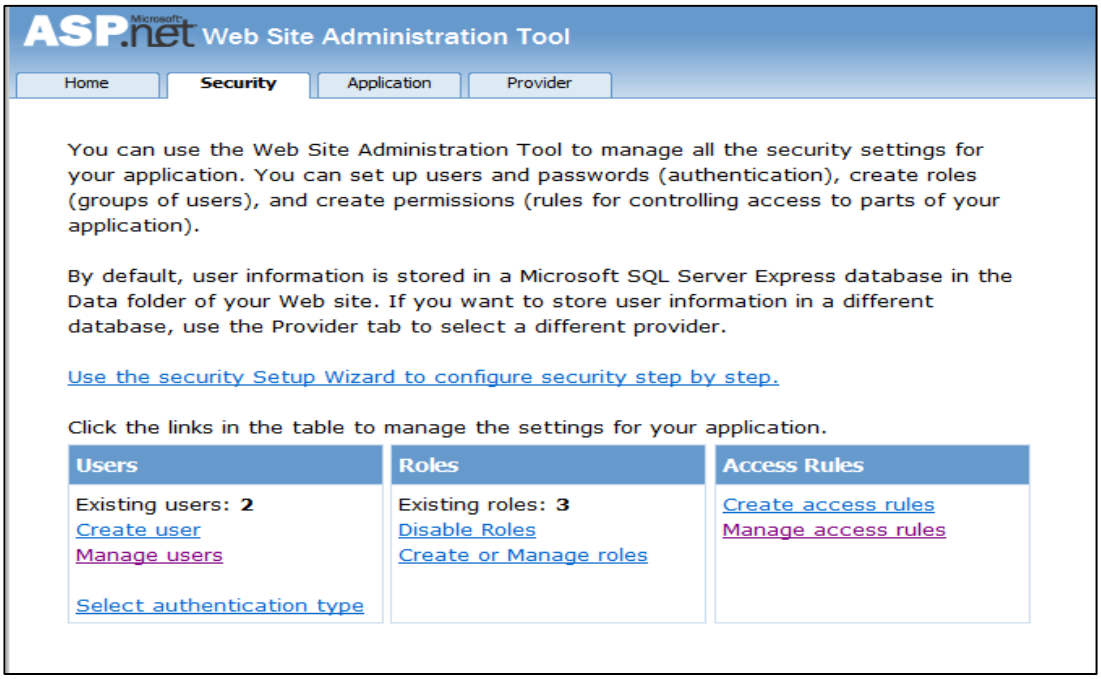
Şekil 4.25. IIS'te oluşturulan sunucu sertifikası özellikleri.

Web güvenliğini sağlamak için göz önünde bulundurulması gereken diğer bir konuda kullanıcı yetkilendirmesi ve dizin güvenliği konusudur. Çünkü kullanıcıların yetki ve izinleri dâhilinde olmayan alanlara erişebilmesi sistem güvenliğini riske atabilmektedir. Örnek uygulamada Visual Studio 2010 yazılımının sunmuş olduğu ASP.NET Web Sayfası Yönetim Aracı yardımıyla mühendis, sistem yöneticisi ve yönetici rollerinin yetkilendirilmesi yapılıp dizinler yetkisiz kullanıcıların erişimine kapatılmaktadır. Şekil 4.26'da asp.net web sayfası yönetim aracı arayüzü gösterilmektedir.



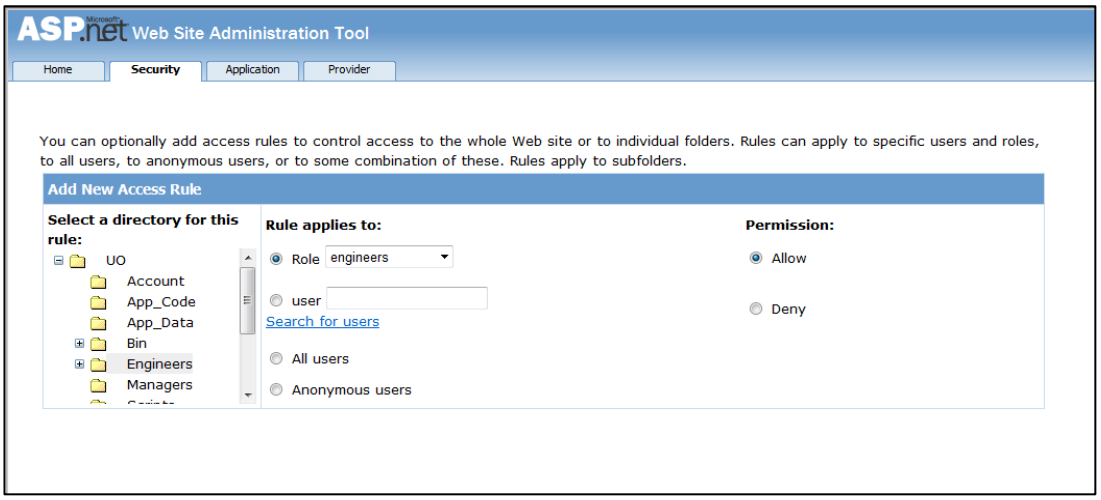
Şekil 4.26. ASP.NET web sayfası yönetim aracı arayüzü.

Bu yönetim aracının güvenlik bölümünde kullanıcılar, roller ve erişim kuralları tanımlanmaktadır. Şekil 4.27'de kullanıcı, rol ve erişim kuralı tanımlama arayüzü gösterilmektedir.



Şekil 4.27. Kullanıcı, rol ve erişim kuralı tanımlama arayüzü.

Kullanıcılar ve roller tanımlandıktan sonra hangi dizine kimlerin erişeceğine dair erişim kuralları yapılandırılıp kullanıcıların yetkili olduğu alanlarda çalışması sağlanmaktadır. Erişim kuralı tanımlama arayüzü Şekil 4.28'de gösterilmektedir.



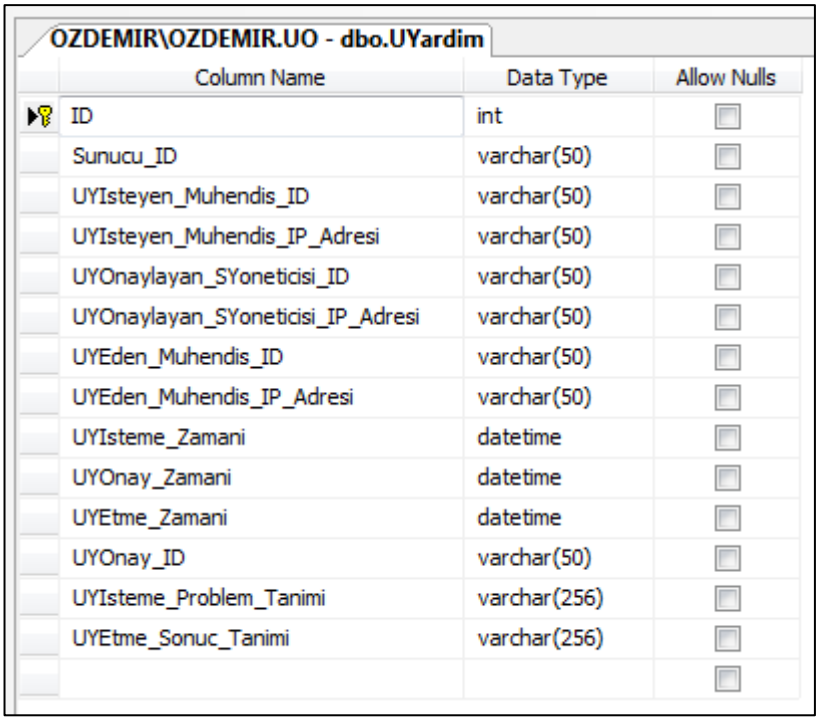
Şekil 4.28. Erişim kuralı tanımlama arayüzü.

Kullanıcıların kullandıkları kullanıcı adları ve parolalarında güvenlik açısından büyük önemi vardır. Çünkü bu bilgilerin kötü amaçlı kişiler tarafından elde edilmesi kullanıcının yetkisi dahilinde büyük tehlikelere sebep olabilir. Bu yüzden

kullanıcıların parola seçme aralığını belirli bir güvenlik seviyesinde tutmak gerekir. Bu güvenlik seviyesi belirlenirken minimum parola uzunluğu, parolanın içerisinde bulunan alfanümerik olmayan karakter sayısı önemlidir. Ayrıca dışarıdan yapılan parola kırma denemelerini de kısıtlamak için yanlış girilen parola sayısına göre hesabın belirli süre ile kapatılması da faydalı olmaktadır. Uygulamada bu yöntemler kullanılmaktadır.

4.3.6.3. Web Loglama

Web uygulamasında sistemde bulunan kullanıcıların yaptığı işlemler, işlem tarihleri, IP adresleri, e-posta gönderme zamanı gibi önemli olan bilgiler veri tabanında tutulmaktadır. Bu sayede herhangi bir problem olduğunda geriye dönük kayıtlara erişim sağlanabilmektedir. Şekil 4.29'da bulunan uzak yardım log tablosu web loglamaya örnek olarak gösterilmektedir.



Şekil 4.29. Uzak yardım log tablosu.

BÖLÜM 5

SONUÇLAR

Bu çalışmada, güncel bir konu olan dijital fabrika kavramının getirdiği endüstriyel otomasyon sistemlerindeki her türlü verinin erişilebilir ve sunulabilir olması çerçevesinde bir çalışma yürütülmüştür. Bu kapsamda gerek çalışan mühendislere, gerek yöneticilere gerekse teknik destek sağlayan kişilere esneklik sağlayacak olan günümüzün gözde iletişim teknolojisi 3G'nin endüstriyel otomasyon sistemlerinde farklı amaçlarla kullanılabileceği gösterilmiştir. 3G'nin sunmuş olduğu yüksek veri transfer hızı kullanılarak sistemin çalışmasına ve üretime yönelik veriler farklı lokasyonlara transfer edilmiştir. Bu veriler ile sistemin çalışması gerçek zamanlı olarak takip edilmiştir, üretime yönelik raporlama yapılmıştır. Uyarı sistemi oluşturularak meydana gelebilecek tehlike ve kaza riski azaltılmıştır.

Ayrıca 3G'nin sunmuş olduğu mekândan bağımsız olarak internet erişim hizmeti ile yetkili personel uzak yardım sisteminden gelen çağrılardan hızlı bir şekilde haberdar olabilmiş ve vakit kaybetmeden uzaktan yardım edebilmiştir. Uzak yardım sistemine girilen problem ve sonuç verilerinden hazırlanan uzak yardım sonuç sistemiyle de personeller aynı problemlerle karşılaştıklarında yardıma ihtiyaç duymadan problemleri çözebilmiştir. Geliştirilen sistem, farklı yetkilerdeki kişilerin farklı sistem kaynaklarına erişebilmesini sağlayacak şekilde tasarlanmıştır. Oluşturulan bu yapı çerçevesinde uzak erişime yönelik görüntü aktarımı ve video konferans gibi özelliklerde sisteme entegre edilebilecektir.

İnternet tabanlı uygulamaların endüstriyel otomasyon sistemlerinde kullanılması güvenlik boyutunu önemli bir noktaya taşımıştır. Otomasyon sistemlerin herhangi bir şekilde hatalı konuma geçmesi, sistemde istenmeyen durumların oluşmasına sebep olabilecektir. Bu açıdan dış dünyaya açılan sistemde network ve sistem güvenliği araştırılmış, güvenli sistem modeli oluşturulmuş ve meydana gelebilecek güvenlik

tehditlerine karşı önlemler alınmıştır. İnternet uygulamalarına kontrollü bir geçiş yapılmıştır.

Otomasyon sistemlerinde bulunan farklı üreticilerin ürettiği cihazların bir arada kullanılabilmesi ve yönetilebilmesi amacıyla geliştirilen OPC sistemlerinin günümüzde geldiği son nokta itibariyle sunmuş olduğu önemli özelliklerden biri olan veri loglayıcı özelliği kullanılmıştır. Bu özellik sayesinde otomasyon sisteminin izlenmesinden üretime yönelik bilgilerin elde edilmesine, kaynak planlamasının yapılmasından karar destek sistemlerinin çalışmasına kadar ihtiyaç duyulan bütün veriler elde edilmiştir. Yapılan çalışmanın ilerde yapılacak olan veri madenciliği ve karar destek sistemleri çalışmaları için faydalı bir açılım olacağı düşünülmektedir.

3G'nin sunmuş olduğu kablosuz internet hizmeti ve veri iletim hızları hazırlanan örnek uygulamada test edilmiş ve sonuç olarak kapsama alanı ve veri iletim hızlarının bölgelere göre değiştiği görülmüştür. Fakat 3G altyapısının hızla kuvvetlendirilmekte (Baz istasyonlarının kurulması, fiber optik hatların çekilmesi vb.) olduğu göz önüne alındığında yakın zaman içerisinde aynı sistem yapısının tüm bölgelerde endüstriyel otomasyon sistemlerine uyarlanabilmesi mümkün olacaktır.

KAYNAKLAR

1. Dahlman, E., Parkvall, S., Sköld, J. and Beming, P., "3G Evolution HSPA and LTE for Mobile Broadband 1st ed.", Elsevier ltd, ***San Diego***, USA, 3-7 (2007).

2. Smith, C. and Collins, P. E. D., "3G Wireless Networks 1st ed.", ***McGraw Hill***, New York, USA, 3-5 (2001).

3. Asif, S. Z., "Wireless Communications Evolution to 3G and Beyond 1st ed.", Artech House, ***Norwood***, MA, USA, 7-20 (2007).

4. Büyükbaş, A., "CDMA ve UMTS: Üçüncü nesil mobil haberleşme teknolojilerinin karşılaştırılması", Uzmanlık Tezi, ***Telekomünikasyon Kurumu***, Ankara, Türkiye, 13-20 (2005).

5. İnternet: Bilgi Teknolojileri ve İletişim Kurumu, "3.Nesil Mobil Haberleşme Sistemleri", **http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/arastirma_raporlari/dosyalar/3G_Raporu_Aralik_2002.PDF**, 17-19 (2002).

6. Gülseren, D., "Mobil iletişim sistemlerinin öğrenci bilgi sistemlerinde kullanımı ve bir uygulama", Yüksek Lisans Tezi, ***Anadolu Üniversitesi Fen Bilimleri Enstitüsü***, Eskişehir, Türkiye, 46-49 (2006).

7. İnternet: Sabah Gazetesi, "Turkcell, 4G Hızını Test Etti", **http://www.sabah.com.tr/Ekonomi/2012/04/06/turkcell-4g-hizini-test-etti**, (2012).

8. Abeta, S., "Toward LTE commercial launch and future plan for LTE enhancements (LTE-Advanced)", ***2010 IEEE International Conference on Communication Systems (ICCS 2010),*** Singapore, Singapore, 146-150 (2010).

9. İnternet: Bilgi Teknolojileri ve İletişim Kurumu Sektörel Araştırma ve Stratejiler Dairesi Başkanlığı, "WiMAX: Diğer Genişbant Telsiz Erişim (GTE) Teknolojileri İle Karşılaştırılması", **http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/arastirma_raporlari/dosyalar/wr.pdf**, 5-14 (2009).

10. Nordell, D. E., "Communication systems for distribution automation", ***Transmission and Distribution Conference and Exposition***, Chicago, USA, 2-14 (2008).

11. Zheng, Y., Luo, G., Sun, J., Zhang, J. and Wang, Z., "PLC modeling and checking based on formal method", ***Journal of Software Engineering & Applications***, 3 (11): 1054-1059 (2010).

12. Liu, T., Cai, G. and Peng, X., "OPC server software design in DCS", ***Proceedings of 2009 4th International Conference on Computer Science & Education***, Nanning, China, 456-458 (2009).

13. Endi, M., Elhalwagy, Y. Z. and Hashad, A., "Three-layer plc/scada system architecture in process automation and data monitoring", ***IEEE***, 2:776-779 (2010).

14. İnternet: OPC Foundation, "OPC Specifications", **http://www.opcfoundation.org/Products/ProductSearch.aspx?FN=Advanced**, (2012).

15. Guohuan, L., Hao, Z. and Wei, Z., "Research on designing method of CAN bus and modbus protocol conversion interface", ***2009 International Conference on Future BioMedical Information Engineering***, Sanya, China, 180-182 (2009).

16. Fovino, N. I., Carcano, A. and Masera, M., "A Secure and survivable architecture for scada systems", ***Second International Conference on Dependability***, Athens, Greece, 34-39 (2009).

17. Cai, N., Wang, J. and Yu, X., "Scada system security: complexity, history and new developments" , ***6th IEEE International Conference on Industrial Informatics***, Daejeon, South Korea, 571-574 (2008).

18. İnternet: Tübitak Bilgem, "İkinci Katman Saldırıları - 5", **http://www.bilgiguvenligi.gov.tr/aktif-cihaz-guvenligi/ikinci-katman-saldirilari5.html**, (2011).

19. İnternet: Tübitak Bilgem, "Dns Önbellek Zehirlenmesi: Açıklık ve Kapanması", **http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=294&Itemid=6**, (2008).

20. İnternet: Chip Dergisi; "DHCP Snooping", **http://www.chip.com.tr/konu/Guvenli-aglara-giden-yol-DHCPSnooping_12045_4.html**, (2011).

21. Kwak, D. H., Kizzier, D. M. and Jung, E., " Spyware knowledge in anti-spyware program adoption: effects on risk, trust, and intention to use", ***Proceedings of the 44th Hawaii International Conference on System Sciences***, Hawaii, USA, 1-7 (2011).

22. Shahzad, R. K., Lavesson, N. and Johnson H., "Accurate adware detection using opcode sequence extraction", ***Sixth International Conference on Availability, Reliability and Security***, Vienna, Austria, 189-195 (2011).

23. Liu, Y., Zhang, L., Liang, J., QU, S. and NI Z., "Detecting trojan horses based on system behavior using machine learning method", ***Proceedings of the Ninth International Conference on Machine Learning and Cybernetics***, Qingdao, China, 856-860 (2010).

24. Akın, G. ve Güneş, A., "Bir worm'un anatomisi", ***Akademik Bilişim Konferansı***, Kütahya, Türkiye, 1-4 (2007).

25. İnternet: McAfee, "McAfee Regional Virus Information", **http://home.mcafee.com/virusinfo/regional?ctst=1**, (10.04.2012 23:34).

26. Cristea, M., Groza, B. and Iacob, M., "Some security issues in scalance wireless industrial networks", 2011 ***Sixth International Conference on Availability, Reliability and Security***, Vienna, Austria, 493-498 (2011).

27. Johnson, R. E., "Survey of scada security challenges and potential attack vectors", ***International Conference for Internet Technology and Secured Transactions (ICITST)***, Liverpool, UK , 2-5 (2010).

28. İnternet: Siemens, "Siemens Simatic Net Telecontrol Scalance M875 Operating InstructionsC79000-G8976-C258-01", **http://cache.automation.siemens.com/dnl/DE/DExOTQ3AAAA_58122394_HB/BA_SCALANCE-M875_76.pdf**, 11-18 (2012).

29. Bin, Q., Xuanang, M., Junda, Z. and Fang, L., "Design of remote data acquisition system based on 3G", ***2012 International Conference on Intelligent Systems Design and Engineering Application***, Sanya, China, 1315-1318 (2012).

30. Yu, Z., Zhisheng, W., Hong, H. and Feng, L., "Remote monitoring application based on modbus and China unicom 3G", ***2010 IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS)***, Xiamen, China, 445-448 (2010).

31. Chomsiri, T., "HTTPS hacking protection", ***21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)***, Ontario, Canada, 2-5 (2007).

ÖZGEÇMİŞ

Uğur ÖZDEMİR 1982 yılında Elazığ'da doğdu. İlkokulu Elazığ Evren Paşa İlkokulu'nda, ortaokulu Elazığ Mezre Ortaokulu'nda okudu. Liseyi ise sırasıyla Diyarbakır Cumhuriyet Fen Lisesi ve Elazığ Mehmet Akif Ersoy Lisesi'nde okudu. 2005 yılında Fırat Üniversitesi Elektrik-Elektronik Mühendisliği Bölümü'nden mezun oldu. 2008 yılında Kastamonu Üniversitesi Bilgi İşlem Daire Başkanlığı'nda uzman kadrosunda çalışmaya başladı ve halen çalışmaya devam etmektedir.

ADRES BİLGİLERİ

Adres: Kastamonu Üniversitesi
Bilgi İşlem Daire Başkanlığı
Kuzeykent Kampüsü / KASTAMONU

Tel: (366) 280 15 11
E-posta: ugurdan@hotmail.com