



YAYIN

BİLGEM

Cilt 3 Sayı 6
Mayıs-Ağustos 2011

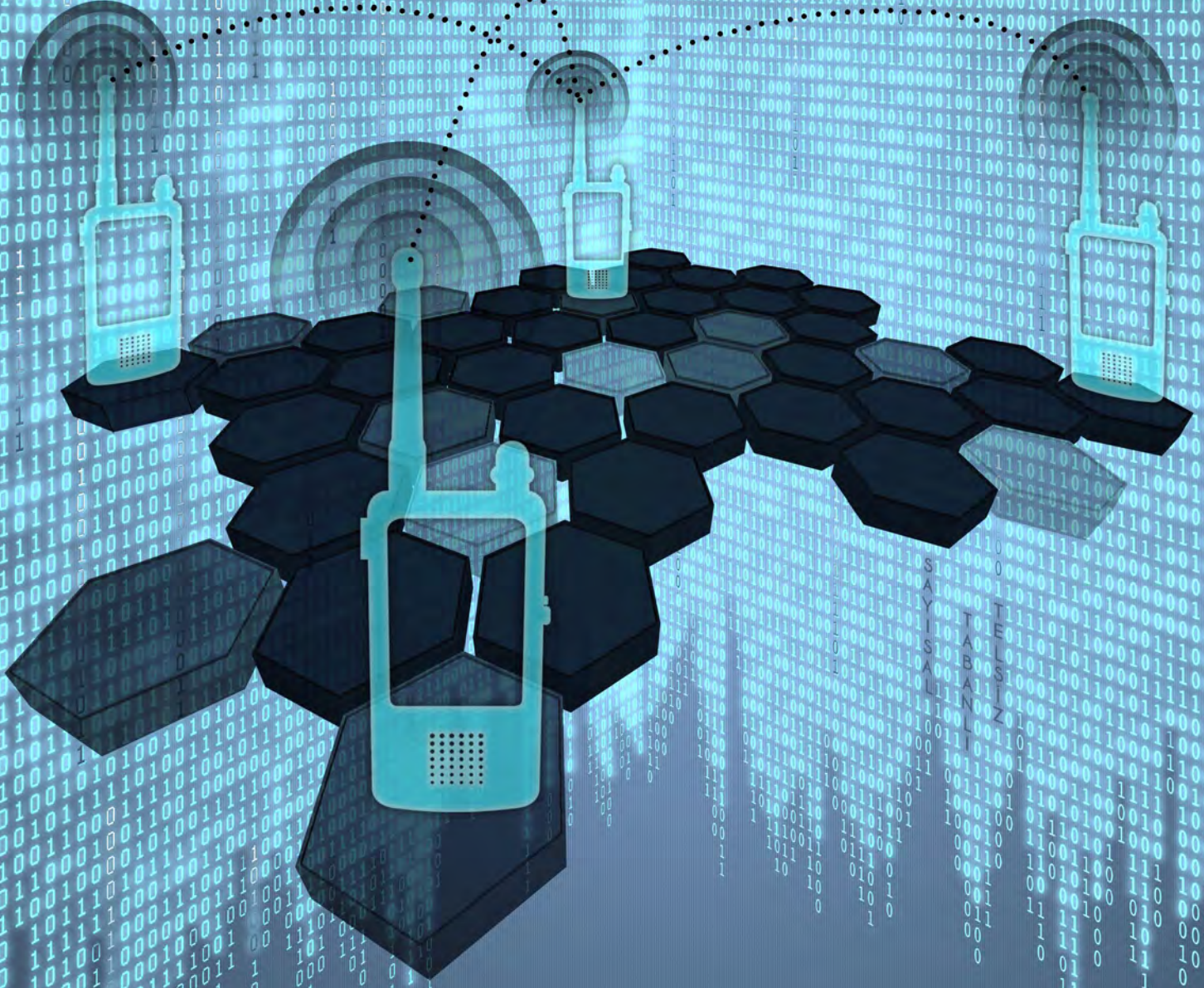
YAZILIM TABANLI
TELSİZ sf.6

MODÜLER TELSİZ
RF MİMARISI sf.30

KALİTE ÇEMBERLERİ sf.58

E-SECİM sf.96

BİLGEM



Değerli Okurlar,

Yine dolu dolu bir sayı ile karşınızdayız. Bu sayıda telsiz iletiminde büyük bir yenilik olan yazılım tabanlı yapılar üzerinde duracak ve BİLGEM bünyesinde bu alanda gerçekleştirilen çalışmalar hakkında bilgi vereceğiz.

Yazılım tabanlı telsiz ihtiyacı askeri telsizlerin birbiriyle karşılıklı çalışmamasından doğmuştur. Bu amaçla yapılan JTRS (*Joint Tactical Radio Systems*) çalışmaları günümüzdeki yazılım tabanlı iletim altyapısının oluşturulmasına öncülük etmiş ve SCA (*Software Communication Architecture*) yapısının temelini oluşturmuştur. BİLGEM 2010 yılı itibarıyla SCA uyumlu yazılım tabanlı telsiz test altyapısını kurmuş ve bu telsizlere yüklenebilecek bazı dalga şekillerini gerçekleştirmiştir.

Derginin diğer konu başlıklarını sıralayacak olursak: Ulusal işletim sistemimiz PARDUS'un son sürümündeki gelişmeleri bu sayıda sizlerle paylaştık. Umarız dergi ekindeki PARDUS 2011 DVD'sini kurup keyifle kullanırsınız. İş Sürekliliği Yönetim Sistemleri, E-İmza, Kalite Çemberleri, Fiberoptik Kablo Denetim Sistemi ve E-Seçim bu sayıdaki diğer yazılar.

Başarı öyküsü köşesinde 1992-1997 yılları arasında TÜBİTAK başkanlığı yapan Prof. Dr. Sayın Tosun Terzioğlu ile söyleşi yaptık. Serbest kürsü bölümünde ise Çinili Köşk'ü, nam-ı diğer Sırça Saray'ı ziyaret ettik. Bu sayıda yeni olarak karikatürlere yer vermeye başladık. Dergi hakkındaki görüş ve önerilerinizi künyedeki e-posta adresimizden bize yazabilirsiniz.

Sonbaharda görüşmek üzere, hoşçakalın.

Dergi Yayın Kurulu

Sahibi
TÜBİTAK BİLGEM adına Merkez Başkanı
Mehmet Önder YETİŞ

Dergi Yayın Kurulu
Ahmet Serdar ADALI
Asım ALTUNBAŞ
Aziz Ulvi ÇALIŞKAN
Mustafa Ümit ÇEŞMECİ
Ersin EVİN
Cumhur Nezih GEÇKİNLİ
Fikret HACIZADE
Bilal KILIÇ
Mehmet Aydın KUBİLAY
Ahmet Hakan KUMBASAR
Hasan Berkan ÖZDEN
Levent Balamir TAVACIOĞLU
Bahattin TÜRETKEN
Umut ULUDAĞ

Kapak Tasarımı
Serkan KONAKCI

Genel Yayın Yönetmeni
Aziz Ulvi ÇALIŞKAN

Yayın Koordinatörü
Mehmet Aydın KUBİLAY

Sorumlu Yazı İşleri Müdürü
Asım ALTUNBAŞ

Edisyon-Redaksiyon
Levent Balamir TAVACIOĞLU
Cumhur Nezih GEÇKİNLİ
Bilal KILIÇ

Mali İşler Sorumlusu
Ahmet Serdar ADALI

Grafik Tasarım
Elif SÜSLER
Serkan KONAKCI
Volkan İZGİ

Yayın Türü
Dört aylık, süreli, ücretsiz

İletişim Adresi
BİLGEM Dergisi
P.K. 74, 41470 Gebze KOCAELİ

Telefon
(262) 648 1000

Faks
(262) 648 1100

İnternet
www.uekae.tubitak.gov.tr/dergi

E-posta
dergi@uekae.tubitak.gov.tr

Baskı
Bilnet Matbaacılık
(216) 444 44 03

Baskı Tarihi
Mayıs 2011

ISSN 1309-3444

Arka planda 0,25 μm teknolojisi ile gerçekleştirdiğimiz bir çipin üzerinde bulunan fotolitografi yapıları bulunmaktadır. Görüntü alırken büyüklük kıyası yapabilmek için bir saç teli de ekledik. Küçük bir kısmını görünen saç telinin enine kesitini tamamen sığdırmak için bu sayfanın altında bir sayfaya daha ihtiyacımız vardı.

Tümdevre ve dedektör üretiyoruz. Tam 28 yıldır.

YİTAL

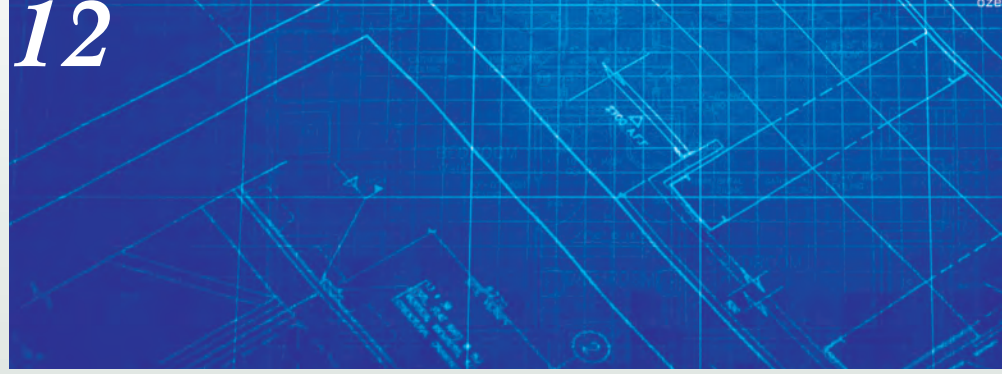
Yarıiletken Teknolojileri Araştırma Laboratuvarı

43 μm $1 \mu\text{m} = 0,000001 \text{ m}$

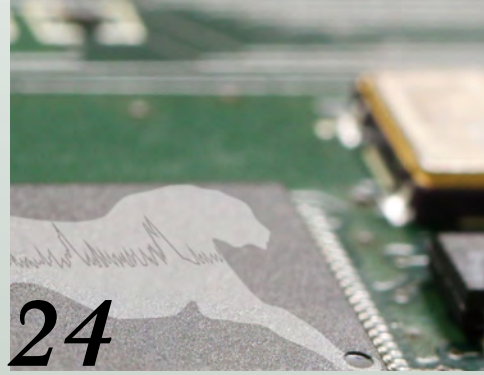
www.bilgem.tubitak.gov.tr



06



12



24



30

04 Milli İşletim Sistemi; PARDUS
Mehmet Önder YETİŞ

kapak konusu

06 Yazılım Tabanlı Telsiz
İbrahim ÖLÇER

12 Yazılım İletişim Mimarisi
Adem ZÜMBÜL

18 SCA Uyumlu Yazılım Tabanlı Telsiz Uygulaması Geliştirme
Hamza ÖZER, Murat ÇEVEN

24 ÇİTA'dan Kaçış Yok
Serkan SEMİZ, H. Ercüment ZORLU

30 Modüler Telsiz RF Mimarisi
Ali DAĞDEVİREN

36 Genişband Frekans Sentezleyici Yapıları
Hüseyin ANIKTAR

yazı dizileri

44 Bilişim Güvenliği Sistemleri: İş Sürekliliği Yönetim Sisteminde Sıkça Yapılan Yanlışlar ve Önemli Başarı Etkenleri
Ali DİNÇKAN, Ömer Deniz DEMİREL

52 Elektronik İmza: Elektronik İmza Standartları ve İlgili Mevzuat
Ersin GÜLAÇTI

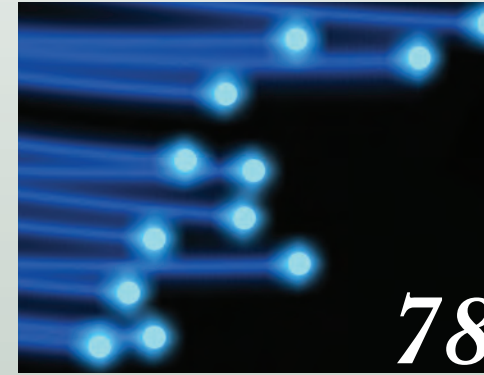
58 Kalite Çemberleri ve Sorun Çözme Yöntemleri
Bilal KILIÇ



52



58



78



96

72 Yıl 2011, PARDUS Hem 2011 Hem Kurumsal
Koray LÖKER

78 Fiberoptik Kablo Denetim Sistemi
Taner DURSUN

96 Elektronik Seçim: İnternet Üzerinden Oylama
Mehmet Sabır KİRAZ, Fatih BİRİNCİ, Uğur Kaşif BOYACI

makaleler

126 Sayısal Telsiz Sistemleri İçin Ağ Geçidi Uygulaması
Murat ÇEVEN, Hamza ÖZER

131 Olasılık Kuramına Bir Giriş – I: Temel Kavramlar
C. Nezih GEÇKİNLİ

142 Anten Ölçüm Sistemleri ve Hata Analizleri – I: Düzlemsel Yakın Alan Ölçüm Sistemi
Bahattin TÜRETKEN, Umut BULUŞ, Ömer YILMAZ

başarı öyküsü

150 Tosun TERZİOĞLU
Asım ALTUNBAŞ

serbest kürsü

160 Çinili Köşk
Melahat PARLAR

170 Şifresayar
Umut ULUDAĞ

Milli İşletim Sistemi; PARDUS

"PARDUS adı, Anadolu Parsının Latince adı olan Panthera Pardus Tulliana'dan esinlenerek seçildi. Anadolu Parsı, özgür bir hayvan olarak bilinir. Güçlü, çevik ve esnektir. Ancak nesli tükenmiştir. 2003'den bu yana ülkenin genç parsları*, PARDUS'u tekrar canlandırmak ve bilişim arenasının hakimi yapmak için elele veriyorlar."

İşletim sistemi; bilgisayarların ana ve yan belleklerinin en verimli biçimde kullanılmasını, çevre donanımlarıyla bilgisayar arasındaki iletişimi, işlemlerin ve akış işinin yönetilmesini, dosya sistemlerinin oluşturulmasını ve yönetilmesini, çeşitli hizmet ve uygulama programlarının çalıştırılmasını sağlayan bir programlar topluluğudur.

Günümüzde kullanılan işletim sistemlerinden birinci grubu oluşturan lisanslı sistemler, kullanım hakkı için ödeme yapılması gereken sistemlerdir. Kaynak kodları kapalıdır. İkinci grubu oluşturan, geliştirilmesine 1990'ların başında başlanan açık kaynaklı yazılımların ayırt edici özelliği ise kullanıcının bir bedel ödemek zorunda olmaması ve yazılımı değiştirme özgürlüğünün bulunmasıdır. Açık kaynak kodlu yazılımlar, uyarlanabilir, sağlam, hızlı ve güvenlidir. Her alanda çözümler sunarak, yazılım tekellerine karşı tüketiciye seçenekler sunar. Ücretli yazılımların aksine, işlediğiniz ve sakladığınız bilgilerin hangi aşamada ne tür işlemde geçtiğini bilirsiniz. Almanya, İspanya, Meksika, Brezilya, Çin, Kore, Hindistan gibi birçok ülke, kamu kurumlarında açık kaynak kodlu yazılımların kullanımını benimsemiş ve bilgi toplumu stratejilerinin bir parçası haline getirmişlerdir. Avrupa Birliği, UNESCO, Dünya Bankası gibi kuruluşlar güvenlik ve tasarruf gibi gerekçelerle açık kaynak kodlu yazılımları önermektedir.

Milli İşletim Sistemimizi (PARDUS) geliştirme vizyonumuz, ülkemize bağımsızlık, güvenlik ve tasarruf sağlamak, yerel bilgi birikimi oluşturarak bilişim alanında yurtiçi katma değeri yükseltmek ve geliştirdiğimiz ürünlerde kullanılan sistemleri kontrol altında tutabilmektir. Çalışmalarımız sırasında uyguladığımız stratejimiz ise, PARDUS'un ülke içinde yaygın kullanımını sağlamak, çalışmalarda sürekliliği temin için gerekli organizasyon yapısını kurmak, teknolojik gelişmeler ve kullanıcı ihtiyaçlarını izleyerek sistemi sürekli geliştirmektir.

PARDUS, Linux temelli bir açık kaynak yazılımdır. Türkçeyi tam olarak destekler. Kurulumu ve kullanımı kolaydır.

TÜBİTAK BİLGEM bünyesinde yer alan UEKAE, milli işletim sistemi çalışmalarını Mart 2003 yılında Başbakanlık tarafından yayınlanan bir genelge ile görevlendirilme sonucu başlatmıştır. 2005 yılında ilk çalışan CD, 2006 yılı başında ise PARDUS-1 çıkarıldı. 2007-2008 ve 2009'da PARDUS'un yeni sürümleri kullanıma sunuldu. Bu yılın başında PARDUS 2011 ve 2011 Kurumsal Beta sürümleri yayınlandı.

PARDUS çalışmaları 2009 yılından itibaren, başlangıçta mütevazı bir bütçe ile DPT (Devlet Planlama Teşkilatı) tarafından desteklenmeye başladı. Bu destek 2010 ve 2011 yıllarında artarak devam etmektedir.

PARDUS'un ilk kurumsal sürümü 2007'de çıktı. İlk defa, bir Milli Savunma Bakanlığı projesi kapsamında, ASAL'ın 600 şubesindeki 7500 bilgisayar üzerinde kullanıldı ve sorunsuz olarak kullanılmaya devam etmektedir. 2008 başında RTÜK için geliştirilen büyük kapsamlı bir proje de 750 terabaytlık bir veri deposu da yine PARDUS üzerinden çalıştırılmaktadır.

Bu yıl, yapılan sözleşmeler kapsamında ağ geçitlerini PARDUS işletim sistemi üzerinden çalıştırma çalışmaları devam etmekte ve bazı kurumların doküman yönetim sistemi tamamen PARDUS üzerinde düzenlenmektedir. Bunun haricinde TÜBİTAK enstitülerinde geliştirilen bütün projelerde PARDUS işletim sistemi kullanılmaktadır. Buna ek olarak PARDUS'a geçişte hazırlık aşamasında bulunan birçok kurum ile çalışmalar devam etmektedir.

PARDUS milli işletim sisteminin kullanımı kendi etrafında bir PARDUS ekosistemini şekillendirmektedir. Bu eko sistem içinde; üniversiteler, PARDUS göç ortakları, donanım ortakları, yazılım ortakları, eğitim kurumları ve PARDUS camiaları yer almaktadır.

Hedeflerimizde, her ilde en az bir PARDUS göç ortağı, 50 üniversite ile ortak proje, 250 gönüllü geliştirici ve 1500 pars yetiştirmek var. 2013 yılında kamuda kurumsal alımların %10'unu karşılamak, böylece ülkeye 50 milyon doların üzerinde bir geliri sağlamak diğer bir hedefimiz. Cumhuriyetimizin 100. yılı olan 2023 yılında ise tüm kamuda PARDUS kullanımını ve küresel rekabete çıkmayı hedefliyoruz.

Telekomünikasyon, yazılım ve donanım alt başlıklarından oluşan Bilgi ve İletişim Teknolojileri (BİT) pazarının 2011 yılında da 1,7 trilyon dolarlık büyüklüğe ulaşması bekleniyor. Yazılım alt başlığının bir bileşeni olan işletim sistemlerinin 2007 yılındaki pazar büyüklüğü 29 milyar doların üzerindedir. BİT pazarı büyüklüğü giderek artmakta, rekabet de aynı oranda kızışmaktadır. Doğal olarak, piyasaya önce girmiş firmalar, özellikle bu alandaki çok uluslu firmalar, çeşitli ülkelerde hakim oldukları pazarları kapırmamak için her türlü mücadeleyi vermektedirler. Bunun sebebi bu tür firmaların bir kere geliştirdikleri ürünleri, çeşitli ülkelere veya aynı ülkedeki farklı kurum ve bireysel kullanıcılara yıllarca mükerrer olarak satabilmeleridir. Ayrıca kullanıcılar, ilk ödedikleri faturanın %25-30 gibi bir bedeli her yıl, güncelleme, bakım-onarım, eğitim adı altında ödemeye devam ederler.

Buna ilaveten, pazara yeni üreticilerin girmesi, ülkelerin kendi sistemlerini başarılı bir şekilde geliştirmesi ve ihrac etmesi durumunda, sadece kendi ülkelerinde değil, diğer ülkelerde de rekabet gücü kazanmalarına neden olabilir ve pazara ilk girmiş firmalar için pazar kaybı anlamına gelir. Bu nedenle sektörde yapılmış firmalar, ülkelerin özgün sistemlerini geliştirmelerini istemezler.

PARDUS'un gelişmesini ve sürdürülebilir olmasını sağlamak, yaygın bir şekilde dağıtımını ve kullanımını desteklemek; TÜBİTAK BİLGEM'in yukarıda bahsettiğimiz bu önemli alandaki öncelikli ödevidir. Bunun yanı sıra, ulusal bir bilinç oluşturmak için tüm kamu kurumlarında ve özellikle Milli Eğitim Bakanlığı ve okullarda PARDUS kullanımını özendirilmeli ve desteklenmelidir. PARDUS, teknolojik bağımsızlık anlamında hepimizin sahip çıkması gereken en önemli projelerden biridir.

Bu sayıdaki yazımı sonlandırırken tüm mesai arkadaşlarım adına siz değerli okurlarımıza saygılarımı sunar, keyifli okumalar dilerim.

Mehmet Önder YETİŞ
Merkez Başkanı

*Pars: PARDUS Milli İşletim Sistemi için çalışan ülkemizin genç aydın çocukları, fotoğraflıklar ve niceleri.



YAZILIM TABANLI TELSİZ

İbrahim ÖLÇER

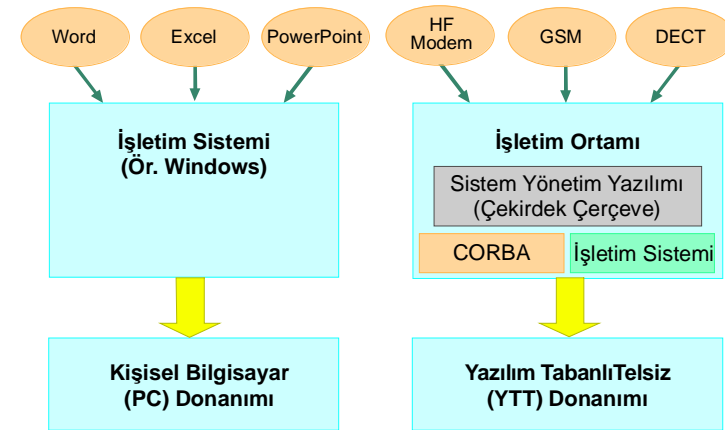
Giriş

Teknolojideki gelişmeler, birçok alanda, çok genel donanımlar üzerinde yazılım güncellemeleri ile sistemlere yeni yeteneklerin kazandırılması yolunda, yeni araştırma ve geliştirme (Ar-Ge) çalışmalarının ivme kazanmasına neden olmuştur. Gerek sivil gerekse askeri alanda kullanılan birçok sistemin, yeni teknolojik gereksinimlere uyarlanması ve hayata geçirilmesi aşamasında, sistemlerin tamamen yeniden tasarım ve geliştirilmesi yerine, üzerinde mevcut olan yazılımların güncellenmesi yolu ile, maliyet etkin ve teknolojik ömrü görece daha uzun ürünlerin kullanıma sunulması amaçlanmaktadır. Telsiz iletişimi alanında da bu konuda çok ciddi Ar-Ge yatırımları hayata geçmiştir. En başta Amerika Birleşik Devletleri (ABD) olmak üzere Avrupa ve dünyanın birçok sayılı ülkesinde “Software Defined Radio (SDR)” konulu çalışmalara başlanmıştır. Birçok teknolojik alanda olduğu gibi, yine ABD'nin başını çektiğini gördüğümüz bu çalışmaların ortak hedeflerinin, sistemlerin “yeniden yapılandırılabilirliği (reconfigurability)”, farklı sistemler ile gerektiğinde “birlikte çalışabilirliği (interoperability)” ve farklı sistemlere yeni yeteneklerin göreceli olarak daha kolay “taşınabilirliği” (portability) özelliklerinin geliştirilmesi veya iyileştirilmesi olduğunu görmekteyiz. Bütün ortak çabaların buna odaklanmasının yanında, bu gelişmeler yeni bir problemi de beraberinde getirmektedir. Farklı telsiz üreticileri aynı konu üzerinde çalışmakla beraber, nasıl bir genel donanım mimarisi üzerinde, nasıl bir standartlaşmaya gidileceği konusunda da ortak bir akıl oluşturulmasını zorunlu kılmıştır. A.B.D.'nin Müşterek Taktik Telsiz Sistemi (Joint Tactical Radio System: JTRS) programı kapsamında, üzerinde milyar dolardan fazla para harcadığı bu konu, “Yazılım İletişim Mimarisi (Software Communications Architecture:SCA)” adını verdiğimiz standartlaşma ve genel bir telsiz mimarisi oluşturma çabalarının lokomotifidir. Gerek dünyadaki bu önemli gelişmelerin uzağında kalmamak, gerekse NATO üyesi olan Türkiye'nin özellikle askeri haberleşme sistemlerinin güncellenmesi ve yeni teknolojilere hızla uyarlanabilmesi amacı ile, bu konuda Genelkurmay MEBS başkanlığı'nın öngörüsü ile gerekli test altyapısı kurulması çalışmalarına TÜBİTAK UEKAE'de 2005 yılında başlanmıştır. 2005 yılının ikinci yarısında, ilk aşamada yazılım mühendisliği alanında çalışan mühendislerden oluşan yeni bir ekip ile SCA konusunda Ar-Ge faaliyetlerine girilmiş, bu konuda gerekli test altyapısı için etüd çalışmaları gerçekleştirilmiştir. Çalışmalar sonucunda, 9 Ekim 2006 yılında Milli Savunma Bakanlığı ile imzalanan 4 yıllık bir proje kapsamında “SCA uyumluluk ve doğrulama testlerini” gerçekleştirecek, bunun yanında “SCA uyumlu dalga şekillerinin geliştirilmesi ve gerekli telsiz donanımları üzerine taşınması” çalışmalarını gerçekleştirebilecek, nitelikli insan gücü yetiştirilmiş ve gerekli teknolojik altyapı kurulmuştur.

Bu yazıda, Yazılım Tabanlı Telsiz (YTT) kavramının tanımı yapıldıktan sonra bu teknoloji kapsamında önemli görülen diğer alt başlıklara değinilerek, TÜBİTAK UEKAE bünyesinde proje kapsamında gerçekleştirilen ana çalışmalar özetlenmiştir. Bu çalışmalar ve ilgili ürünler hakkında daha kapsamlı tanıtımlar, bu derginin takip eden yazılarında yer alacaktır.

Yazılım Tabanlı Telsiz Nedir?

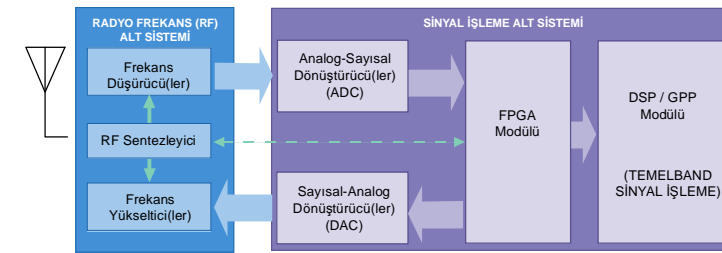
İdeal bir YTT, yeni gereksinimlerin sadece yazılımsal değişiklikler ile telsiz donanımına kazandırıldığı bir yapıyı tanımlamaktadır. Bir başka deyişle, yeni bir telsizin donanımsal olarak sil baştan geliştirilmesi veya üzerinde yer alan analog tabanlı devrelerin yeniden tasarlanması yerine, genel bir telsiz donanımı üzerinde sadece yazılımsal değişiklikler yapılarak, yeni bir telsiz özelliğinin kazandırılması hedeflenmektedir. Kabaca, bu kavramı daha iyi anlaşılması açısından kişisel bilgisayarlar (PC) güzel bir benzetme olabilir. Günlük hayatımızda çok yaygın kullandığımız PC'leri telsiz donanımına benzetirsek, PC donanımı üzerinde koşan işletim sistemini, telsizi yöneten ana sistem yazılımına, PC üzerinde yükleyip kaldırdığımız çeşitli yazılım uygulamalarını da, telsiz üzerinde koşacak farklı dalga şekillerine benzetebiliriz. Örneğin bir telsizin HF bandında farklı bir standartta haberleşirken, bu modu kapatıp VHF bandında farklı bir standartta haberleşmesi, PC üzerinde yer alan bir uygulamanın kapatılıp farklı bir uygulamanın açılmasına da benzetmek mümkündür. Dalga şekli denildiğinde kısaca, telsiz üzerinde çalışan haberleşme moduna ait temel özellikler ifade edilmektedir. Bunlar arasında frekans, bant genişliği, veri hızı, modülasyon türü, vb. değişkenler başta gelir.



Şekil 1. Kişisel bilgisayar uygulaması ile, ideal bir Yazılım Tabanlı Telsiz uygulaması arasındaki benzerlik.

Bir YTT en genel olarak iki ana donanım katmanından oluşmaktadır: RF (Radyo Frekans) alt sistem ve Sinyal İşleme alt sistemi. Telsiz antenin bağlı olduğu RF alt sistemin amacı, YTT'nin geniş bir telsiz bandında kullanımını sağlamaktır. Bu sistem aracılığı ile geniş bir telsiz spektrumunda yer alan

yayımlar, sinyal işleme alt sistemine uygun bir ara frekans bölgesine çekilir. Sinyal işleme alt sisteminin en ön katunda, bu frekans bölgesini sayısallaştırarak, yazılımsal olarak işlenmesini sağlayan analog-sayısal (A/D) dönüştürücü devreleri yer alır. A/D devreleri ardında yer alan uygulamaya özel işlemci veya günümüzde artık çok daha yaygın kullanılan Sahada Programlanabilir Kapı Dizileri (FPGA) işlemcileri sayesinde de, işaretin temel banta indirilmesi gerçekleşir. Temel bant işaret üzerinde gerçekleştirilecek modem blokları da artık Genel Amaçlı İşlemciler (GPP) veya Sayısal İşaret İşlemciler (DSP) üzerinde gerçekleşir. Antenden başlayıp RF bandından işaretin IF ve daha sonra temel banta düşürülmesi için gerçekleştirilen işlemler telsizin “almaç (receiver)” moduna, bunun tersi yönünde işlemlerin gerçekleşmesi ise telsizin “göndermeç (transmitter)” moduna denk düşmektedir.



Şekil 2. Genel YTT donanım mimarisi.

En yaygın kullanılan donanım mimarisi olarak gösterdiğimiz bu yapıda (bkz. Şekil-2), FPGA teknolojisi, yeniden programlanabilirliği ve paralel işlem gücü sayesinde, ideal bir YTT' de olması gereken birçok özelliğin gerçekleştirilmesi için çok önemli bir yere sahiptir. Üst düzey programlama dillerinin (C / C++ vb.) yaygın kullanımı ve derlenmesi açısından bakıldığında da, geliştirilen dalga şekillerinin taşınabilirliği kolaylığı hedeflendiğinde, özel Sayısal İşaret İşlemci (DSP) yongaları yerine, Genel Amaçlı Ön İşlemci (GPP) yongaları da ayrı bir tercih nedeni sayılmaktadır.

SCA (Yazılım İletişim Mimarisi) ve SCA Uyumluluk Testleri

Hem askeri hem de sivil amaçlar için farklı standartlarda çalışabilen, farklı bantlarda iletişim yeteneği olan telsizlere gereksinim artmaktadır. Günümüzdeki modern telsiz sistemlerinin çoğu YTT teknolojisine uygun tasarlanırsa da, bu sistemler belirli bir standartta göre geliştirilmemektedir. A.B.D., her yeni telsiz sisteminde tekrar sisteme özel yazılım geliştirmek yerine, JTRS programı kapsamında SCA adı verilen standartlaşma çalışmalarını başlatmış ve yeni nesil telsiz sistemlerinin bu standartta uyumlu olarak geliştirilmesini hedefleri arasına koymuştur. SCA uyumlu bir YTT sistemi fikrinin oluşmasına temel olan gereksinim, kara, hava, deniz kuvvetleri ve diğer ulusal telsiz kullanıcıları arasında farklı standartlarda bile olsa, uyumlu, kesintisiz ve güvenli telsiz iletişim yeteneği sağlamaktır.

SCA, YTT'ler arasında dalga şekillerinin taşınabilirliğini arttırmak amacıyla geliştirilmiş ve üzerinde halen çalışılan ve güncellemeler yapılan bir yazılım standardıdır. Telsiz üzerine yüklenecek olan dalga şeklinin ve telsizin ana yönetim yazılımı olan “Çekirdek Çerçeve”nin birbirleri, işletim sistemi ve ara katman yazılımı (ORB) ile nasıl konuşacağını belirleyen kurallardır. Bu kurallara ne kadar uyulduğunun belirlenmesi amacı ile yapılan SCA uyumluluk testleri, A.B.D.'de bulunan JTEL (JTRS Technical Laboratory) tarafından JTAP (JTRS Test Application) denilen bir test programıyla ve dalga şekli SCA uyumluluk testleri de, WTT (Waveform Test Tool) denilen yazılım ile gerçekleştirilmektedir. Bu test yazılımlarının şu aşamada A.B.D. dışına çıkarılmasına izin verilmemektedir.

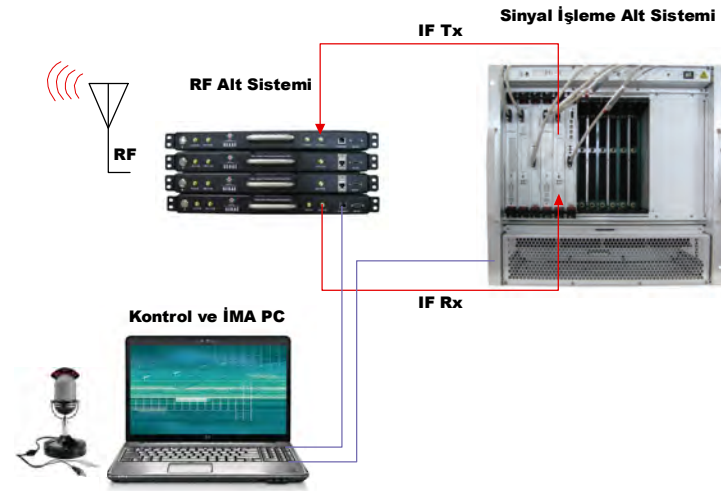
Proje kapsamında, SCA gereksinimlerinin ayrıntılı incelenmesi ve her bir gereksinimin gerçekleştirilmesi çalışmalarının doğal bir sonucu olarak, özgün ve tamamen milli bir şekilde geliştirilmiş SCA Çekirdek Çerçeve yazılımı ortaya çıkmıştır. Çekirdek Çerçeve yazılımı, SCA standardına göre telsiz içerisindeki yazılım ve donanım bileşenlerini yönetebilmek için geliştirilmiş bir katman yazılımıdır. Çekirdek Çerçeve katmanı, aynı standarda göre geliştirilmiş olan uygulama yazılımlarını yönetebilmekte ve uygulama yazılımları için farklı sistemler arasında taşınabilirlik, yeniden kullanılabilirlik, genişletilebilirlik, ayarlanabilirlik vb. çok sayıda üstünlüğü beraberinde getiren, ispatlanmış bir altyapı sunmaktadır. TÜBİTAK UEKAE Radio Control System (TURCOS) olarak adlandırılan yazılım, proje sürecinde en başta Linux işletim sistemi üzerinde geliştirilmiş, ardından VxWorks 6.4 gerçek zamanlı işletim sistemi ortamında da başarılı şekilde çalıştırılmıştır. Farklı işletim sistemi ve donanım yapılarına göre çeşitli sürümleri bulunan TURCOS, gerçek bir ticari telsiz üzerinde de kullanılabilir.

Geliştirilmesi hedeflenen test altyapısının en önemli bileşeni ve projenin temel hedeflerinden biri olarak görülen “SCA uyumluluk testleri” açısından bakıldığında, projenin en önemli ürünü olarak gösterebileceğimiz ürün, RATE adı verilen test yazılımıdır. Bu ürün, insan makine arayüzü aracılığı ile test altındaki telsizin SCA uyumluluk testlerini gerçekleştirmek amacı ile geliştirilmiştir. SCA dokümanlarında değinilen ve önemli bir kısmı otomatik olarak gerçekleştirilebilen testler, RATE aracılığı ile kullanıcının belirleyeceği test sayısı ve seçenekleri ile kolayca gerçekleştirilmekte ve test sonuçları otomatik olarak raporlanabilmektedir. RATE'nin koştugu bir bilgisayar uygun bir bağlantı arayüzü (ör. ethernet) üzerinden YTT'ye bağlanarak, YTT üzerine taşınacak özel uygulamalar aracılığı ile SCA uyumluluk testleri koşturulmaktadır. RATE kullanıcı arabirimi, seçilen test setleri arasından alt test kümeleri seçimi ve bu alt kümelerin otomatik ya da tek tek çalıştırılarak, rapor üretilmesi olanağı sağlamaktadır.

SCA Tabanlı Telsiz Platformu

İleride TSK'nın gereksinim duyacağı SCA uyumlu birçok yeni dalga şekli geliştirebilmek ve gerektiğinde bilişsel telsiz, çok-girişli çok-çıkışlı sistemler ve akıllı anten (smart antenna) konulu Ar-Ge çalışmalarında da kullanabilmek amacı ile proje kapsamında YTT-3000 adlı bir evrensel YTT test donanımı kurulmuştur. YTT-3000 sistemi, yurtdışından tedarik edilen ve VPX tabanlı gelişmiş bir sinyal işleme alt sistemi ile, tamamen milli ve özgün olarak geliştirilmiş bir RF alt sistemden oluşmaktadır. Faz uyumlu çalıştırılabilen toplam 8 ayrı A/D (Analog/Sayısal) ve 8 ayrı D/A (Sayısal/Analog) kanalı içeren bu sistem, RapidIO gibi yüksek hızlı standart iletişimlerini destekleyen, yüksek bant genişliğine sahip VPX arayüzü ve çok sayıda işlemci gücü ve anten dizileri ile huzme oluşturma (beamforming), elektronik harp ve sinyal istihbaratı (SIGINT) konusunda da, gereksinim duyulabilecek önemli uygulamaların test edilebileceği olanaklar sunmaktadır.

Özgün olarak geliştirilen RF Alt Sistem, teknolojisi sürekli olarak güncellenebilen modüler bir yapıya sahiptir. Bu yapının en önemli bileşenlerinden ve elektronik harp sistemlerinin temel yapı taşlarından biri olan geniş bantlı frekans sentezleyici modülü, 20 MHz – 3 GHz frekans bandında işaretlerin üretilmesi amacı ile geliştirilmiştir. 300 mikrosaniyeden daha hızlı frekans atlayan ürünlerin temininde yaşanan zorluklar ve ihraç kısıtlamaları nedeni ile geliştirilen bu ilk prototipin, frekans atlama hızı 50 mikrosaniyeye ulaşmaktadır. Direct Digital Synthesis (DDS) teknolojisi sayesinde ulaşılan bu hız ve düşük faz gürültüsü, frekans atlamalı telsiz gibi karmaşık dalga şekillerinin gerçekleşmesinde büyük önem arz etmektedir. Geniş bantlı sentezleyicinin yanında, diğer frekans dönüştürücü birimler de, modüler olarak teknolojik gereksinimlere hızlı uyarlanabilir yapıda gerçekleşmiştir. YTT-3000 RF alt sistemi, 40 MHz bant genişliğine sahip dalga şekillerini desteklemektedir. Sinyal işleme alt sistemi de, 70 MHz frekansındaki yayını A/D kanalı ile sayısallaştırmakta, FPGA yongaları üzerindeki sayısal işlemler sayesinde, telsiz yayınları genel amaçlı işlemcilerin işleyebileceği hızlara indirilmektedir. Bu hızlar, dalga şekli gereksinimlerine göre farklılık göstermektedir. Sinyal işleme alt sisteminde yer alan yüksek bellekli ve çok çekirdekli işlemci gücü sayesinde, yüksek işlem gerektiren farklı dalga şekillerinin aynı anda işlenmesi mümkündür. Bir başka deyişle, birden fazla RF almaç/gönderme yapıları kullanılarak, YTT-3000 üzerinde çok modlu çok bantlı telsiz haberleşmesi gerçekleştirilebilir.



Şekil 3. YTT-3000 özgün SCA test ve dalga şekli geliştirme platformu genel yapısı.

SCA Uyumlu Dalga Şekilleri : STANAG 4285 ve APCO P25

Proje isterleri gereği, iki ayrı dalga şekli SCA uyumlu olarak geliştirilmiş ve test edilmiştir. Bunlardan ilki, NATO da bir süre HF modem standardı olarak kullanılan STANAG 4285 dalga şeklidir. İlk pilot çalışma olan bu standart, kısa sürede SCA tabanlı olarak geliştirilmiştir. Yurtdışından taktik telsiz sistemini temsil edecek bir YTT olarak tedarik edilen SDR-4000 adlı sisteme de başarılı bir şekilde taşındıktan sonra HARRIS marka ticari telsiz modemi ile karşılıklı olarak çalıştırılmıştır. Bunun yanı sıra, bu dalga şekli NATO RTO grubu çalışmalarında kullanılmış ve üye ülkelerin geliştirdikleri platformlar arasında karşılıklı olarak yapılan testleri sırasında, UEKAE'de geliştirilen STANAG 4285 dalga şeklinin hem asenkron hem de senkron modda sorunsuz bir veri iletişimi sağladığı gözlenmiştir.

Başka bir çalışma kapsamında, Kamu Güvenliğinde kullanılan ve ülkemizde de Jandarmanın kullandığı bir standart olan APCO Project 25 adlı dalga şeklinin, SCA uyumlu sürümü geliştirilmiş ve test edilmiştir. APCO P25 dalga şekli de SDR-4000 sistemine başarılı bir şekilde taşınmış ve analog tabanlı Rafta Hazır Ticari (RAHAT) APCO P25 el telsizleri ile karşılıklı haberleşme testleri başarılı bir şekilde gerçekleştirilmiştir.

Sonuç ve Yorumlar

SDR (Yazılım Tabanlı Telsiz) konusu, haberleşme sistemlerini yeni bir boyuta taşıyacak bir yapıyı hedeflemektedir. Donanımdan bağımsız bir şekilde, farklı donanım yapılarını bir yazılım katmanıyla birbiriyle haberleşebilir hale getirmek, SDR ile mümkün olabilecektir. Bu büyük gelişimi sağlayabilmek amacıyla, dünyadaki birçok kurum ve kuruluşlar, şirketler bu konuyla ilgilenmekte, büyük yatırımlar yapmaktadırlar. NATO bünyesinde ve Avrupa Birliği kapsamında da, SCA temel alınarak standartlaşma çalışmalarına başlanmıştır. Ülkemizde de, TÜBİTAK destekli olarak gerçekleştirilen çalışmalarda, gerek TSK Çok-Bantlı Müşterek Sayısal Telsiz (ÇBMST) projesi kapsamında üretilecek yeni nesil telsizlerin SCA uyumluluk testlerinin gerçekleştirilmesinde, gerekse TSK'nın gereksinim duyacağı birçok yeni teknolojinin “proof-of-concept” olarak gerçekleşmesine katkı sağlayacak evrensel bir test altyapısı, UEKAE bünyesinde kurulmuş bulunmaktadır. SCA konulu çalışmaların yanında, TSK'nın gereksinim duyabileceği modern sinyal istihbarat sistemlerinin geliştirilmesinde kullanılacak çok önemli bir sinyal işleme altyapısı oluşmuştur. Proje kapsamında, benzerleri yurtdışından tedarik edilemediği için geliştirilmesi öngörülen RF alt sistem, telsiz spektrumunun çok hızlı bir şekilde izlenmesi ve kayıt altına alınmasına yönelik önemli bir yetenek kazandırmıştır. Özellikle proje kapsamına dahil edilen “frekans düşürücü” ve “genişbandlı düşük faz gürültülü sentezleyici” ürünleri, “haberleşme istihbaratı” amaçlı kullanılacak önemli yan ürünlerdir. YTT-3000 özgün test sistemi, “Frekans Atlamalı Telsizlerin İzlenmesi ve Dinlenmesi” amacı ile yeni bir proje kapsamında kullanılabilir.

Kurulmuş olan gelişmiş YTT altyapısı, sadece askeri amaçlı değil, birçok sivil amaçlı AR-GE ve kavram doğrulama çalışmasına da yeterli olanak sağlamaktadır. Örneğin, doğal afet, yangın vb. acil durumlarda, Emniyet, Sağlık, İtfaiye, yerel yönetim vb. kamu kurum ve kuruluşlarının, sorunsuz bir şekilde haberleşeceği “Acil Durum Haberleşme Sistemi” nin, YTT teknolojisine dayalı olarak geliştirilmesine yönelik çalışmalar, aynı evrensel YTT platformu üzerinde yürütülebilir. Şu ana kadar elde edilen bilgi ve tecrübeler sonucunda, bu tür bir Acil Durum Haberleşme sisteminin YTT tabanlı olabileceği değerlendirilmiştir.

Tamamen milli tasarım ve geliştirme ürünü olan SCA test altyapısının, ülkemizi konu ile ilgili alanda yurtdışına bağımlı kalmaktan kurtarılmasının yanı sıra, gerçekleştirilen çalışmaların kalitesi ve proje çıktılarının içeriği açısından, ülkemizin yurtdışındaki saygınlığını ve teknolojik alanda rekabet gücünü artırıcı yönleri olacağı değerlendirilmektedir.

yazılım iletişim mimarisi

Adem ZÜMBÜL

Bu yazıda Yazılım İletişim Mimarisi (*Software Communications Architecture*, 'SCA') standardı kısaca tanıtılacak olup, TÜBİTAK BİLGEM bünyesinde SCA standardı kapsamında yapılmakta olan çalışmalar özetlenecektir.

1. SCA Nedir?

Yazılım tabanlı telsizler (YTT), içinde yüklü dalgışekli yazılımlarının deęiştirilmesi ile farklı bir telsiz gibi davranabilme yeteneęi kazandırılabilen cihazlardır. Henüz gelişme aşamasında olan bu kavram, telsizi oluşturan donanım ve yazılım bileşenlerinin standart olmaması nedeniyle, ortaya çıkan dalgışekli yazılımları için taşınabilirlik, ayarlanabilirlik, tekrar kullanılabilirlik gibi çözüm bekleyen sorunları beraberinde getirir. SCA (Software Communications Architecture) [1], bu sorunlara cevap verebilmek için geliştirilmiş bir standarttır.

Hızla gelişmekte olan YTT teknolojisi, bu alanda ürün geliştirenler için, çok sayıda donanımsal ve yazılımsal alt bileşen yapı taşı alternatifleri ortaya çıkarmaktadır. YTT geliştiricileri için bu çeşitlilik, daha zengin ürünler üretme fırsatı sunmasına karşın, ortaya çıkan dalgışekli yazılımlarının geliştiriciye özel ve platform bağımlı olması, farklı donanımlar arasında taşınabilirliğini en aza indirmektedir. Ayrıca, geliştirilen dalgışekli yazılımlarının yeniden kullanılabilirliğinin az olması ve geliştirme aşamasında genel kabul görmüş bir yöntemin bulunmaması, geliştirme zamanının ve maliyetlerinin önemli derecede artmasına neden olmaktadır. Bu sorunların ve gereksinimlerin doğal sonucu olarak geliştirme aşamasında kullanılabilir yeni standartlar oluşturulmaya başlanmıştır. Bu standartlar içerisinde günümüzde en çok kabul gören standart SCA standardıdır.

2. SCA Standardının Gelişimi

SCA standardının ilk çıkış amacı, her ne kadar askeri birlikler arasındaki iletişim ve uyum sorunlarını çözmek olsa da sivil ve ticari alanda da benzer sorunların bulunması, SCA standardının askeri alanlar dışında da kabul görmeye başlamasını sağlamıştır. Bu sorunlara örnek olarak şunlar sayılabilir: Farklı devlet ve sivil güvenlik kuruluşları arasında zor şartlarda da iletişimi sürdürebilmek, yeni çıkan bir

modelin hızla gelişen ve deęişen teknolojik standartlar yüzünden kısa zamanda eskimesini önlemek, birçok standardı (GSM, 3G, GPRS, EDGE, WiMax, Wi-Fi, Mobil TV, GPS, mobil uygulamalar vb.) tek bir cihaz üzerinde aynı anda çalıştırabilmek ve bütün bunları olabilecek en küçük cihaz ağırlığı ve boyutları ile yapabilmek. Sayılan hedefleri gerçeklemek için son derece karmaşık donanım ve yazılım yapıları barındıran cihazlara gereksinim vardır. Dolayısıyla bu tür karmaşık cihazların yazılım yapılarının standartlaştırılması büyük önem taşımaktadır.

Amerika Birleşik Devletleri merkezli bir askeri kuruluş olan JTRS (Joint Tactical Radio System) altındaki JPO (Joint Program Office), 90'lı yılların ortalarından başlayarak YTT platformlarını standartlaştırmak için bir seri program başlatmıştır. Bu programlar daha sonra SCA adı altında toplanmıştır. Her ne kadar daha önceleri de YTT platformları için geliştirilmiş standartlar varsa da, SCA standardı, önemli telsiz üreticilerinin desteğini alması ve var olan standartlar içerisinde tutarlılık açısından en iyi durumda olması bakımından diğer standartlardan ayrılmaktadır. SCA standardı ayrıca dünya çapında birçok ticari amaçlı veya kar amacı gütmeyen kuruluş tarafından da destek görmektedir. SCA standardının en güncel sürümü 2.2.2'dir. Ancak yeni bir sürüm için çalışmalar sürmekte ve çıkacak yeni sürümünün bir yıl içinde SCA 3.0 olarak yayımlanması beklenmektedir.

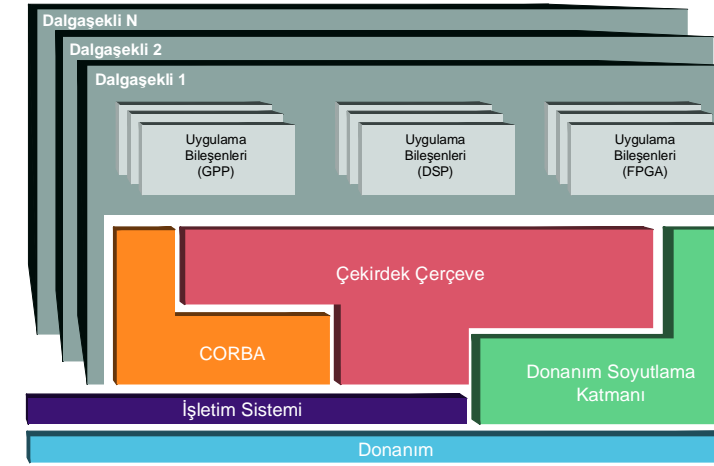
SCA standardının gelişimi her ne kadar JTRS'in son sözüne baęlı olsa da çeşitli kurum ve kuruluşlar da standardın gelişimine katkı sağlamaktadır. TÜBİTAK'ın da üyesi olduğu, ABD merkezli Wireless Innovation Forum (eski adı ile SDR Forum), bu kuruluşlar içerisinde en önemlisi olarak sayılabilir. Wireless Innovation Forum bünyesinde, büyük bir bölümü ABD ve Avrupa'da olmak üzere, dünyanın çeşitli yerlerinden çok sayıda kamu, sivil, ticari, askeri

kuruluşlar ile üniversiteler yer almaktadır. Bu kuruluşların katkılarıyla yılda 5 kez toplantı düzenlenerek SCA ve YTT'nin gelişimine katkıda bulunmaktadır.

3. SCA Katmanları

Klasik bir SCA mimarisinin katmanları Şekil 1'de gösterilmiştir. Bu yapı içerisinde, aşağıdan yukarıya doğru, işletim sistemi, donanım soyutlama katmanı, CORBA, çekirdek çerçeve ve dalgışekli yazılımları bulunmaktadır. Telsiz yazılımının katmanlar şeklinde düzenlenmesindeki amaç, telsiz donanımına özgü işlemlerin çekirdek çerçeve içerisinde, iletişim standardına özgü işlemlerin ise dalgışekli yazılımının içerisinde gerçekleştirilmesinin getireceği avantajlardır.

Bu katmansal yapıda aşağı katmanlardan yukarı katmanlara doğru çıkıldıkça programlama daha kolaylaşmakta ve taşınabilirlik daha da artmaktadır. Örneğin, bir telsiz uygulaması geliştireceğimizi varsayalım. Geliştireceğimiz bu uygulamayı doğrudan işletim sisteminin fonksiyonları ile kodlamak, işletim sisteminin detayları ile boğuşmamıza ve gereksinimimiz olan bütün fonksiyonların işletim sistemine baęlı olmasına neden olacaktır. Üstelik uygulamamızı taşıdığımız her işletim sisteminde benzer iş yapan kodların farklı sistem çağruları ile birçok kere yeniden yazılması gerekecektir. Oysaki, işletim sistemine ait detaylar çekirdek çerçeve tarafından gerçekleştirilip, dalgışekli uygulamaları tarafından standart programlama arayüzleri ile kullanıldığında, dalgışekli geliştirmek için işletim sisteminin detaylarını bilmek gerekmez. Üstelik geliştirilen dalgışekli uygulaması, farklı donanımlara taşınmak istendiğinde ortak yazılım arabirimi korunduğu sürece taşınabilirlik sorunu en aza iner. Özetle, SCA uyumlu bir dalgışekli, yine SCA uyumlu bir telsiz üzerine birkaç küçük yazılımsal deęişiklik ile taşınabilmektedir.



Şekil 1. SCA mimarisinin katmanları.

4. SCA Arayüzleri

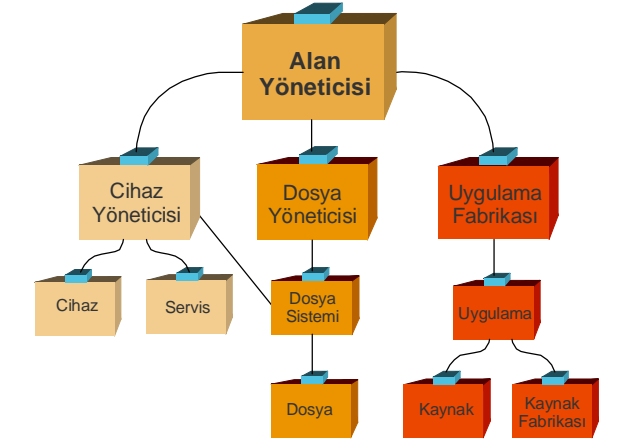
SCA standardı, telsiz donanımına bağımlı işlemler için CORBA temelli standart arayüzler tanımlayarak, dalgışekli yazılımlarını, donanımsal veya işletim sisteminin ayrıntılarından bağımsız duruma getirir.



Şekil 2. SCA arayüzleri ile telsiz işlemleri arasındaki ilişki.

Şekil 3'de ana hatlarıyla bir telsizin gerçekleşmesi gereken özellikleri ve bu özelliklere karşılık gelen SCA yazılım arayüzleri ve bileşenleri gösterilmektedir. Kısaca özetlemek gerekirse, telsize ait donanım bileşenlerinin yönetimi için Cihaz (Device) Grubu Arayüzleri, telsize yüklenecek dalgışekli uygulamalarının yönetimi için Uygulama (Application) Grubu Arayüzleri, dosya işlemlerinin yönetimi için Dosya (File) Grubu Arayüzleri, gerçekleşen olayların izlenmesi için Olay (Event) Servisi Arayüzleri, gerçekleşen olayların kaydının tutulabilmesi için Kayıt (Log) Servisi Arayüzleri, telsiz yazılım bileşenlerinin hayat

döngülerinin yönetimi için Temel Uygulama (Base Application) Arayüzleri ve bütün bu bileşenlerin tek merkezden yönetimi için de Alan Yöneticisi (Domain Manager) Arayüzü, SCA tarafından tanımlanan yazılım arayüzleri arasında bulunmaktadır.



Şekil 3. Genel hatları ile SCA arayüzleri.

Bu arayüzlerin birbirleri ile olan hiyerarşik bağlantıları ana hatlarıyla Şekil 3'de gösterilmiştir. SCA arayüzlerinin çekirdek çerçeve ve dalgışekli geliştiricileri tarafından doğru şekilde gerçekleştirilmesi, uyumluluk ve taşınabilirlik açısından oldukça önemlidir.

SCA standardı, çok sayıda kural tanımlamasına karşın, telsizin çalışma mantığını etkileyecek çoğu detay geliştiricilere bırakılmaktadır. Bunun temel nedeni, SCA standardının anlaşılabilirliğini daha fazla zorlaştırmamak ve geliştiricilerin kendi algoritmalarını gerçeklemleri konusunda onları özgür bırakmaktır.

5. TÜBİTAK BİLGEM Bünyesindeki SCA Yazılım Ürünleri

TÜBİTAK BİLGEM çatısı altında 2005 yılında başlayan SCA konulu çalışmalar sonunda, TURCOS ve RATE adlı iki temel yazılım geliştirilmiştir. Ayrıca Stanag 4285 ve APCO P25 dalgışekli yazılımları da SCA uyumlu olarak geliştirilmiş diğer ürünler arasında sayılabilir.

5.1. TURCOS (TUBİTAK UEKAE Radio Control Software)

TURCOS tamamen milli olarak geliştirilmiş bir SCA çekirdek çerçeve yazılımıdır. Bu yazılım SCA uyumlu bir sistemin kalbini oluşturmaktadır. Temel olarak, telsiz donanımının ve dalgışekli uygulamalarının yönetiminden sorumludur. Yukarıda özetlenen tüm SCA işlemlerinin yerine getirilmesi büyük oranda TURCOS yazılımının sorumluluğundadır.



Şekil 4. TURCOS logosu.

TURCOS telsiz kontrol sistemi, CORBA uyumlu bir ara katman yazılımı yardımı ile farklı işlemci bileşenleri arasında veri ve kontrol akışını yönetmektedir. Bu sayede telsiz dalgaşekilleri için geliştirilen sayısal işlem yazılımları, çok sayıda işlemci üzerinde paralel şekilde çalıştırılmakta ve bu bileşenler arasında eşgüdüm ve veri aktarımı sağlanmaktadır. Yazılım tabanlı telsiz sistemleri üzerine standart bir altyapı getirme amacı ile oluşturulan SCA standardı iki temel bileşeni tanımlamaktadır: çekirdek çerçeve ve dalgaşekli. TURCOS bu iki bileşenlenden çekirdek çerçeve bileşenidir. Bu özelliği ile standarda uygun geliştirilen dalgaşekillerinin telsize yüklenmesi, ayarlanması, çalıştırılması, durdurulması ve kaldırılması gibi temel telsiz işlevlerini gerçekleştirebilir.

TURCOS yazılımı güncel SCA standardı olan sürüm 2.2.2 ile uyumlu olarak gerçekleştirilmiştir. Geliştirme aşamasında başarılı kritik bir uygulama olduğundan, C++ dili tercih edilmiştir. İlk olarak Pardus işletim sistemi üzerinde geliştirilen yazılım daha sonra ise VxWorks gerçek zamanlı işletim sistemine taşınmıştır. Power PC ve x86, desteklenen işlemci ailelerindedir. CORBA katmanında ise, ACETAO ve ORBExpress, ara katman yazılımları ile birlikte çalışabilmektedir.

5.2. RATE (Radio Automated Test Environment)

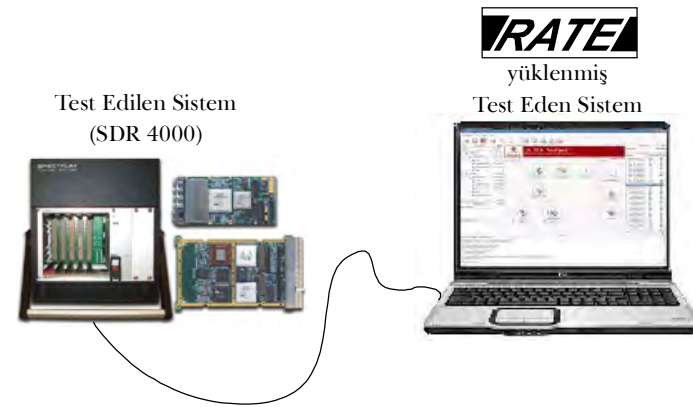
RATE yazılımı, çekirdek çerçeve ve dalgaşekli yazılımların SCA standardı ile uyumluluklarını test edebilmek amacı ile geliştirilmiş bir yazılımdır. Bir yazılımın SCA uyumlu olarak nitelenebilmesi için SCA standardının yayıncısı olan JTRS kuruluşunun yayımladığı SCA Traceability Matrix [2] dokümanında belirtilen ilgili şartları sağlaması gerekmektedir. Bu dokümanda SCA sürüm 2.2.2 için yaklaşık 550 tane madde bulunmaktadır. Bu 550 maddeden bazıları olmazsa olmaz nitelikteki maddelerdir ancak isteğe bağlı veya duruma özel maddeler de bulunmaktadır. Öte yandan, bu maddelerin tümü ile tam uyumlu bir SCA yazılımı da bulunmamakla birlikte ABD'de bulunan çekirdek çerçevelerin SCA standardı ile uyum oranı, ortalama olarak %70 dolayındadır. Bunun temel nedeni, SCA standardında çok fazla detay tanımlanmış olması ve geliştiricilerin gereksinimleri dışında kalan bölümleri gerçekleştirme gereği duymamalarıdır.

SCA maddeleri incelendiğinde, gerçekleşmesi kolay birçok madde olduğu gibi, çok zor ve karmaşık olan maddeler de çok sayıda bulunmaktadır. Bütün bu maddelerin tek bir araç ile otomatik olarak test edilmesi olanaksızdır. Kimi maddeler için tam otomatik test yöntemleri bulunurken, bazıları için -doğası gereği- el ile kontrol şeklinde gerçekleştirilen testler gerekmektedir. RATE yazılımı otomatik, yarı otomatik ve el ile olmak üzere 3 farklı seviyede test imkanı sunar. Otomatik maddeler için seç-çalıştır yöntemiyle, yarı otomatik ve el ile yapılan testler için ise test adımlarını listeleterek kullanıcıya yardımcı olma şeklinde bir kullanım sağlanmaktadır.

RATE yazılımı test edilecek olan sisteme göre şekillendirilebilen bir esnekliğe sahiptir. Test edilecek sisteme ait test maddeleri ve ilgili test parametreleri XML formatındaki dosyalarla RATE'e yüklenerek, değişik sistemler test edilebilir. Testler tamamlandıktan sonra ortaya çıkan test sonuçları ekranda görülebileceği gibi, sonuçlar HTML ve XML formatlarında raporlanabilmektedir.

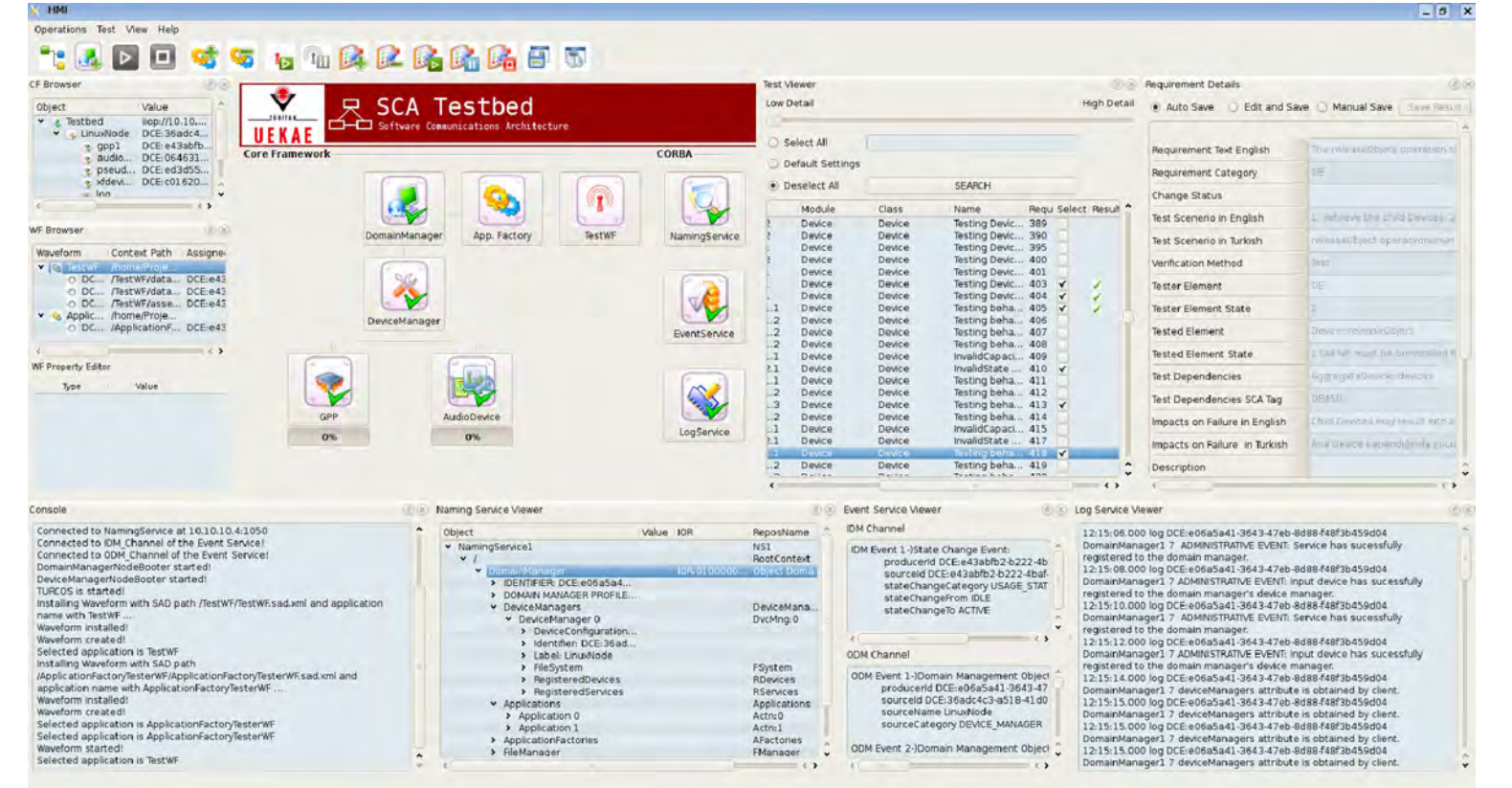
SCA testlerinin gerçekleştirilmesi için, önce, Şekil 4'te gösterildiği gibi bir test ortamı oluşturulur. SCA uyumluluğu test edilecek sistem ile RATE yüklenmiş test eden sistem birbirine ethernet bağlantısı üzerinden CORBA ile bağlandıktan sonra üç farklı test yöntemi ile testler gerçekleştirilebilir:

- Test altındaki sisteme yapılan doğrudan CORBA çağrıları
- Test altındaki sisteme yüklenen test amaçlı dalgaşekli yazılımları
- Test edilecek sisteme yüklenen test amaçlı çekirdek çerçeve bileşenleri



Şekil 5. Test ortamı.

Bugüne kadar, RATE yazılımı kullanılarak, BİLGEM bünyesinde geliştirilen TURCOS yazılımı ve referans olarak kabul edilen bir sistem olan Kanada merkezli CRC firması tarafından geliştirilmiş SDR4000 sistemi SCA uyumluluk açısından test edilmiştir. Ayrıca Aselsan tarafından geliştirilecek olan SCA uyumlu telsizlerin de RATE yazılımı ile test edilmesi planlanmaktadır. Bunların dışında yurtdışındaki çeşitli kuruluşlardan da test istekleri gelmektedir. SCA testlerinin günümüzde de yalnızca ABD merkezli bir askeri kuruluş olan JTEL tarafından yapıldığı ve test başına 75.000\$ ile 100.000 \$ gibi bir ücret istendiği göz önüne alındığında, bu sektörde dünya çapında bir açık bulunduğunu açıklar. RATE yazılımı da bu açığı kapatmaya aday bir yazılım olarak öne çıkmaktadır.



Şekil 6. RATE kullanıcı arayüzü.

6. Sonuç

SCA standardını kullanmak, dalgaşekillerinin kolay taşınabilir olmalarını sağlamanın yanında, yazılan kodların yeniden kullanılabilirliğini arttırmak, var olan kodların yeni sürümler ile güncellenebilmesini kolaylaştırmak ve geliştirme aşamasında hızlı geliştirme araçları kullanarak geliştirme zamanını azaltmak gibi avantajlar sağlar. Diğer yandan, SCA standardı, yazılım katmanları arasında hiyerarşi oluşturduğu için yazılan kodların daha yavaş çalışması, geliştiricileri dalgaşekli yazılımları için karmaşık ve hataya açık XML yapılandırma dosyaları hazırlamaya mecbur etmesi gibi sorunları da beraberinde getirir. Ayrıca SCA standardı daha çok GPP temelli bir standart olup DSP ve FPGA'ler için herhangi bir kural kümesi tanımlanmıştır. Bütün bunlara karşın, YTT geliştiricileri için SCA standardının getireceği avantajların dezavantajlarına göre çok daha fazla olduğu söylenebilir.

KAYNAKÇA

- [1] System, J. T. R., "Software communications architecture specification Final Version 2.2.2", Technical report, Space and Naval Warfare System Center, 2006.
- [2] SCA Traceability Matrix, <http://sca.jpeojtrs.mil/sca.asp>



SCA UYUMLU YAZILIM TABANLI TELSİZ UYGULAMASI BELİŞTİRME

Hamza ÖZER
Murat ÇEVEN

Bu yazıda sizlere yazılım iletişim mimarisi (SCA - *Software Communication Architecture*) [1] uyumlu dalgaşekli uygulaması geliştirme konusu, örnek SCA modelleri ve dalgaşekilleri yardımıyla anlatılacaktır. SCA ve yazılım tabanlı telsiz (SDR - *Software Defined Radio*) kavramları önceki yazılarda ayrıntılı olarak irdelendiği için, bu kavramların ayrıntılarına değinilmeyecektir. Bu yazıda SCA uyumlu dalgaşekli tanımlanacak, SCA uyumlu dalgaşekillerinin SCA uyumsuz dalgaşekillerine göre üstünlükleri anlatılacaktır [2]-[3]-[4]. Daha sonra, SCA uyumlu dalgaşekli geliştirme yöntemi, tasarım aşamasından bir donanıma yüklenip çalıştırılma aşamasına kadar adım adım incelenecektir. Son bölümde yorum ve değerlendirmeler yer almaktadır.

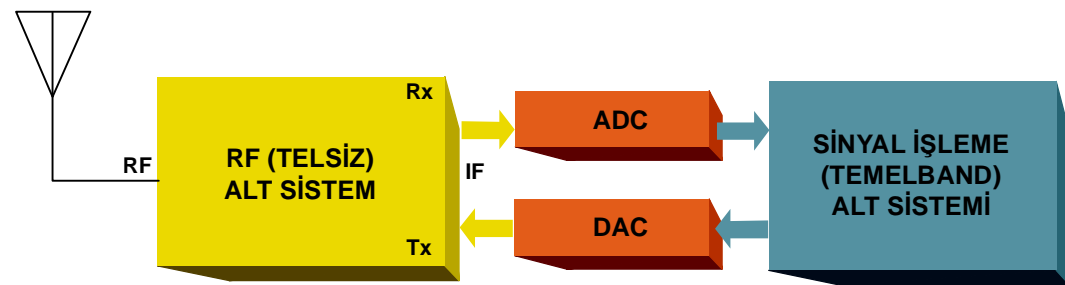
SCA Uyumlu Dalgışekli ve SDR

SCA, özellikle yazılım tabanlı haberleşme cihazları için geliştirilmiş bir yapıdır. Bu yapı, bir işletim sistemi, bir çekirdek çerçeve ve diğer altyapı yazılımlarını (*board support packages*, *CORBA Middleware services*) içeren bir uygulamadan oluşmaktadır. Geliştirilen uygulama, dalgışekli olarak adlandırılmakta ve tasarlanan işlevini gerçekleştirirken yukarıda belirtilen yazılımlar üzerinde çalışmaktadır. Geliştirilen bu uygulamanın yukarıda belirtilen yazılım katmanlarının üzerinde çalışabilmesi ve onların hizmetlerini kullanabilmesi için özel olarak yapılandırılması gerekmektedir. Bu yapıya uygun olarak geliştirilen uygulamalara SCA tabanlı veya uyumlu dalgışekli denilmektedir.

SDR, telsiz işlevlerinin, bir işaret işleme işlemcisi üzerinde yazılımsal olarak gerçekleştirildiği bir radyodur. Klasik bir SDR yapısı Şekil-1'de verilmektedir. Burada RF katmanı haricinde telsizin bütün işlevleri yazılımsal olarak gerçekleştirilmektedir. RF katmanı ile veri alışverişi bir ADC/DAC (Analog Sayısal Dönüştürücü / Sayısal Analog Dönüştürücü) modülü ile gerçekleştirilmektedir. Bu yazıda SCA uyumlu olarak gerçekleştirilen SDR dalgışekilleri hakkında ayrıntılı bilgiler verilmektedir.

Neden SCA Uyumlu Dalgışekli?

Genel bir SDR'nin klasik donanım temelli bir telsize göre en önemli üstünlüğü yeniden yapılandırma ile düşük maliyetle ve kısa zamanda gerçekleştirilebilmesidir. Doğal olarak bu avantaj SCA uyumlu bir SDR için de geçerlidir. Bununla beraber, SCA'nın getirdiği önemli bir diğer üstünlük ise platform değişikliklerinde dalgışeklinin kolayca yeni platforma taşınabilmesidir. SCA uyumlu bir dalgışeklinin model tasarımı aşamasında, geliştirilen dalgışekli bileşenleri, üzerinde çalıştırılması planlanan platform ve işlemciye göre yapılandırılır. Dalgışeklinin yeni bir platform ve/veya işlemciye taşınması durumunda sadece bu yapılandırmalar yeniden ayarlanıp, tekrar derleme yapılarak yeni platforma ve/veya işlemciye uygun yazılımlar üretilir ve yükleme gerçekleştirilir. Böylece kısa sürede yeni bir donanıma taşınma işlemi gerçekleştirilmiş olur.



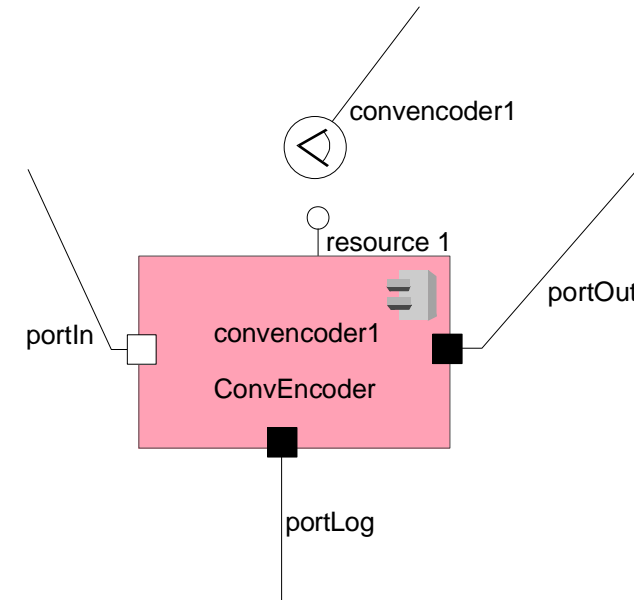
Şekil 1. Klasik bir SDR yapısı.

SCA'nın getirdiği diğer önemli bir üstünlük de aynı donanım ve/veya platformun birden fazla dalgışeklinin çalışması için tasarlanabilmesidir. Klasik bir radyoda bir donanım, üzerine yüklenen uygulama ile veya ayarlanan yapıda çalışır. Aynı yapı ile farklı bir radyo/telsiz gerçekleştirmek mümkün değildir. Farklı bir radyo/telsiz için yeni bir tasarım gerçekleştirilmelidir. SCA tabanlı bir yapıda ise, platforma yüklenen yazılım kaldırılıp yeni bir yazılım yüklenerek aynı donanım/platform yeni bir telsiz olarak kullanılabilir. Bu sayede sınırsız sayıda uygulamanın aynı donanımda gerçekleştirilmesi mümkün olabilmektedir. Bunların yanında SCA'nın getirdiği diğer bir üstünlük de SCA yapısında dalgışekli bileşenleri tamamen birbirinden bağımsız olduğu için, bir bileşenin değiştirilerek yeni bir dalgışekli gerçekleştirilmesi veya bir bileşenin farklı uygulamada tekrar kullanılabilmesinin mümkün olmasıdır. Örneğin, bir sayısal telsiz yapısında filtre, serpiştirici, çarpıcı vb. yapılar, SCA mimarisinde ayrı bileşenler olarak gerçekleştirildiği için, bu bileşenler farklı telsiz yapıları için tekrar kullanılabilir.

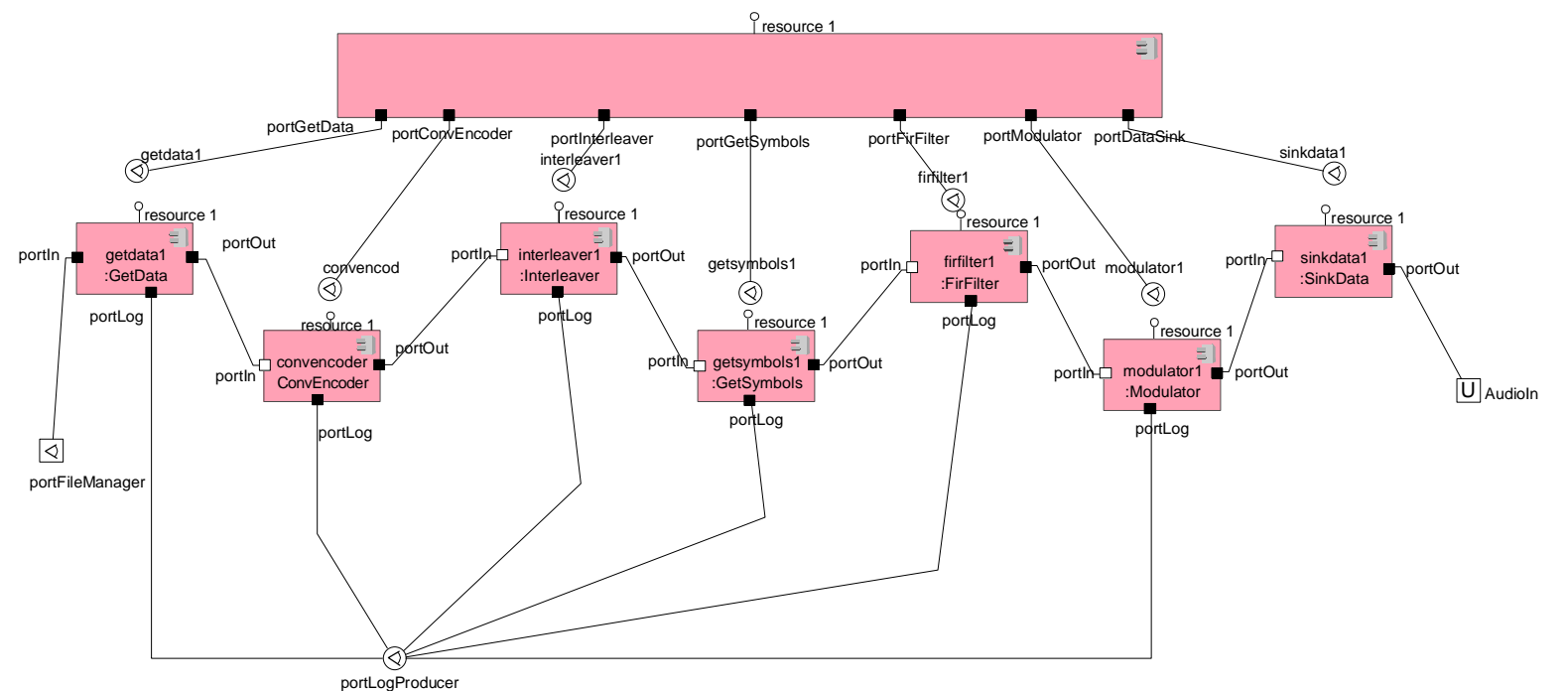
SCA Tabanlı Dalgışekli Geliştirme Yöntemi

SCA tabanlı uygulama geliştirmede, uygulama bir model tasarımı ile başlar. Model tasarımında yazılım, birbirinden ayrı bileşenler halinde tasarlanır. Bileşenler arasında veri alışverişi için, her bileşenin giriş ve çıkış kapıları tanımlanır (bu tanımlamada SCA standartlarında yer alan arayüz (IDL – *Interface Definition Language*) yapıları kullanılır). Örnek bir bileşen yapısı Şekil – 2'de verilmektedir. *ConvEncoder* isimindeki bu bileşenin bir giriş kapısı (*portIn*), bir çıkış kapısı (*portOut*), bir günlük kapısı (*portLog*) ve bir de yönetici bileşen ile haberleşme sağlayan kaynak (*resource*) kapısı vardır. Bunlar arasındaki veri aktarımı için uygun bağlantılar kurulur. Zeligsoft tasarım aracı kullanılarak tasarlanmış bir modem verici uygulamasının model yapısı Şekil-3'te görülmektedir. Burada tipik bir sayısal modem verici yapısı görülmektedir. Dalgışekli bileşenleri sırasıyla; veriyi uygulamaya alan (*GetData*), kanal kodlayıcısı (*ConvEncoder*), serpiştirici (*Interleaver*), sembol üretici (*GetSymbols*), iletim filtrelemesi (*FirFilter*), modülatör (*Modulator*) ve veriyi uygulamadan ADC'ye ileten (*SinkData*)'dan oluşmaktadır. Uygulamada, modem gerektirdiği bütün

işlemler ayrı bileşenler tarafından gerçekleştirilir ve elde edilen işlenmiş modem verisi uygulama çıkışına iletilir. Ayrıca SCA mimarisinin gerektirdiği bir *Assembly Controller* bileşeni mevcuttur. Bu bileşen, çekirdek çerçeveye yüklenen ve diğer bütün bileşenlerin bilgisini bulduran ve bağlı bileşenlerin hepsini yapılandırabilen (ayarlar parametrelerini arayüz vasıtası ile değiştiren, bileşenleri başlatıp durdurma gibi yönetsel işlevleri gerçekleyen) ana bileşendir. *PortLogProducer* ise bütün bileşenlerin, planlanan ve programlanan, standart ve hata mesajlarının yazıldığı bir günlük dosyasıdır. Uygulamanın yükleme, çalışma ve kaldırma aşamalarında oluşan bütün mesajlar bu metin dosyasına kaydedilir.



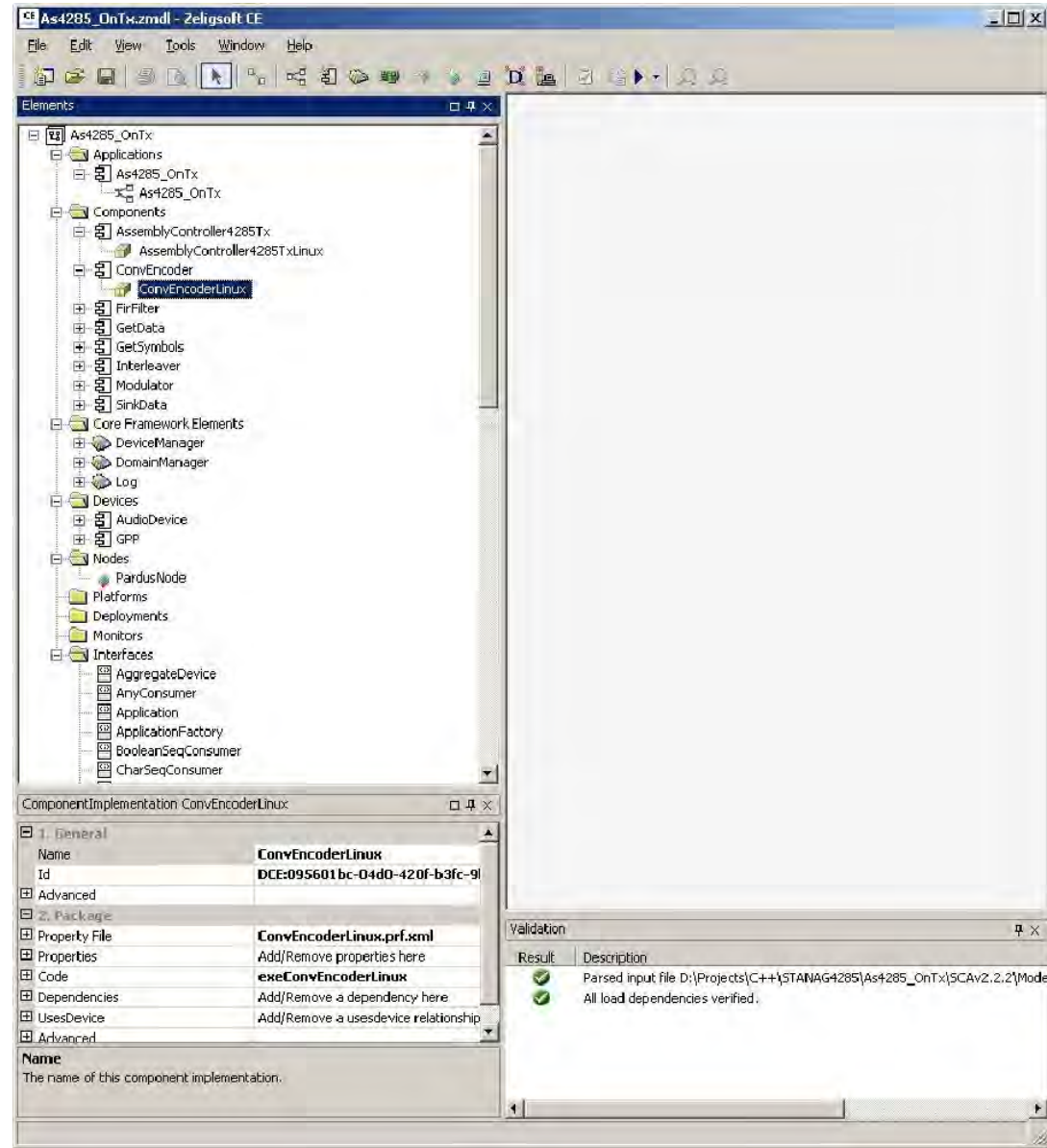
Şekil 2. Örnek bir SCA bileşeni.



Şekil 3. Sayısal bir modem vericinin Zeligsoft model geliştirme aracı ile hazırlanmış modeli.

Model tasarımından sonra, her bir bileşen için yapılandırmalar ayarlanır. Bileşenin ayarlanabilen parametrelerinin, hangi işletim sistemleri (işletim sistemi, ORB ve çekirdek çerçeve) üzerinde ve hangi işlemci üzerinde çalıştırılacağı seçilir. Bütün bu UML tasarım ve yapılandırmalarını yapmakta kullanılan yazılım uygulamaları geliştirilmiştir. *Zeligsoft*, *Prismtech* ve *CRC* gibi firmalar bu amaçla özel tasarım geliştirme uygulamaları gerçekleştirmiş ve ticari olarak satmaktadırlar. BİLGEM bünyesinde *Zeligsoft* firmasının ürünü olan *Zeligsoft CE* ürünü kullanılmaktadır. *Zeligsoft CE* tasarım aracının ana pencere yapısı Şekil-4'te verilmektedir. Model tasarımı ve bütün yapılandırmaların tamamlanmasından sonra, tasarlanan uygulamanın SCA doğrulaması (*SCA validation*) gerçekleştirilir. Yukarıda verilen tasarım araçları bu doğrulama işlevini de sağlamaktadırlar. Hatasız bir tasarım ve SCA doğrulamasından sonra yazılım üretim aşamasına geçilir.

Tasarlanan modelin yazılım üretimi üç aşamada gerçekleştirilir. Birinci aşamada SCA XML dosyaları üretilir. Bu dosyalar, tasarımcının belirleyeceği bir klasöre kaydedilir. Bu XML dosyaları, uygulamanın bütün tasarım ayrıntılarını, özel bir biçimde tutan metin dosyalarıdır. Tasarım ayrıntılarında, bileşenlerin isimleri, hangi bileşenin hangileri ile ne tür bağlantılar üzerinden haberleşeceği, bileşenlerin ayarlanabilen parametreleri gibi bilgiler yer almaktadır. Uygulamayı platforma yükleyecek olan çekirdek çerçeve, bu XML dosyalarından bütün bilgileri okur (platformdaki hangi işlemcilere hangi bileşenlerin yükleneceği, bileşenlerin arasındaki bağlantıları vb.) ve platforma yükler.



Şekil 4. SCA tabanlı model geliştirme aracı Zeligsoft CE aracı ana paneli.

XML dosyalarının üretiminden sonra, kullanılan IDL yapılarının kaynak yazılım dosyaları üretilir. Bundan sonra uygulamanın iskelet kaynak yazılımları üretilir. Böylece her bir bileşenin boş kaynak yazılımları gerçekleştirilmiş olur. Geliştirme aracı, her bir bileşen için ayrı bir dizin oluşturur. İlgili bileşen için üretilen bütün kaynak yazılım dosyaları bu dizinler içinde yer alır. Her bir bileşen dizininde *worker* isimli bir alt dizin oluşur. *Worker* dizini içinde tasarımcının programlayacağı kaynak yazılım dosyaları üretilir. Bu iskelet kaynak yazılımların içerisine her bir bileşenin gerçekleştireceği işlevi yerine getirecek işlevsel yazılımlar, tasarımcı tarafından yerleştirilir. Son aşamada yazılımlar derlenerek çalıştırılabilir dosyalar üretilir. Artık çalıştırılabilir bu dosyalar hedeflenen platforma yüklenerek çalıştırılmaya hazırdır.

Uygulama aşamasında, ilk olarak çekirdek çerçeve bütün hizmetleri ile çalıştırılır. Bunun için SCA konusunda çalışan firmalar çeşitli çekirdek çerçeveler geliştirmiş ve piyasaya sunmuşlardır. BİLGEM kendi geliştirdiği çekirdek çerçevesi TURCOS'u kullanmaktadır. Çekirdek çerçeve bir arayüz veya doğrudan konsol üzerinden çalıştırılabilir. Çekirdek çerçeve, uygulamanın *sad.xml* (*software assembly descriptor*) uzantılı XML dosyasını okur. Bu dosyadaki bilgiler kullanılarak uygulamanın diğer XML dosyaları okunur ve sisteme yüklenir. Bütün XML dosyalarının bilgileri sisteme yüklendikten sonra, buradan elde edilen bilgiler kullanılarak her bileşenin çalıştırılabilir dosyaları sistemdeki uygun işlemcilerle yüklenir ve bileşenler arasında gerekli bağlantılar kurulur. Bundan sonra, Başlat ve Durdur komutları ile çekirdek çerçeve üzerinden uygulama başlatılıp durdurulabilir, her bileşenin ayarlanabilir parametreleri, arayüz üzerinden değiştirilebilir veya uygulama tamamen kaldırılıp (*uninstall*) başka bir uygulama sisteme yüklenebilir.

Sonuçlar ve Yorumlar

Bu makalede SCA uyumlu bir dalgaşekli geliştirme, bütün aşamaları ile irdelenmiştir. SCA uyumlu bir dalgaşekli, geliştirme yönteminin, geliştirme aşamasında bir miktar ek yük getirmesi yanında oldukça yararlı üstünlükler sunmaktadır. Dalgaşekli geliştirme yöntemi yeteneği bir kez kazanıldıktan sonra, yeni dalgaşekilleri daha kısa sürede ve sorunsuz olarak gerçekleştirilebilir. BİLGEM bünyesinde gerçekleştirilmekte olan Yazılım Tabanlı Telsiz (YTT) projesi kapsamında, basit dalgaşekilleri (FM, Ses Testleri) yanında iki önemli standart (NATO STANAG 4285 ve TIA APCO Project-25) SCA uyumlu olarak gerçekleştirilmiş ve farklı donanımlar üzerinde koşturulmuştur [5]-[6]. Birbirlerinden çok farklı olan bu platformlar, hem kendi aralarında hem de geleneksel (donanım tabanlı) cihazlar ile başarılı bir şekilde karşılıklı haberleştirilmiştir.

KAYNAKÇA

- [1] JPEO JTRS, "Software Communications Architecture Specifications v2.2.2", May 2006
- [2] D. Garlan and M. Shaw, "An Introduction to Software Architecture", *Carnegie Mellon University Technical Report CMU-CS-94-166*, January 1994
- [3] SDR Forum, "Year Book", 2005
- [4] S. Singh, M. Adrat, M. Antweiler, T. Ulversoy, T.M.O. Mjelde, L. Hanssen, H. Özer, A. Zumbul, "Developing SCA based Waveforms on SDRs", *IST-092 Symposium on Military Communications and Networks*, Wroclaw, Poland, September, 2010.
- [5] Murat Çeven, H. Ercüment Zorlu, Hamza Özer, Harun Karabalkan, İbrahim Ölçer, "SCA Based APCO Project-25 Waveform Implementation on the SDR-4000", *Proceedings of the Second Annual European Reconfigurable Radio Technologies Workshop*, Mainz, Germany, June, 2010.
- [6] H. Ercüment Zorlu, Murat Çeven, İbrahim Ölçer, Hamza Özer, Hüseyin Arslan, "Blind Signaling Identification for Multimode SDR Receiver with Applications to Public Safety Communications", *Proceedings of the SDR'09 Technical Conference and Product Exposition*, Washington D.C, USA, December, 2009.

ÇİTA'DAN KAÇIŞ YOK

Serkan SEMİZ
H. Ercüment ZORLU

Günümüzde telsiz haberleşme uygulamaları hızla yaygınlaşırken, bir yandan da mevcut olanlardan daha karmaşık haberleşme teknikleri kullanıma sunulmaktadır. Sabit frekanslı telsizlerin yerini, farklı çalışma bantlarında ve farklı modülasyon tiplerinde çalışabilen telsizler almaktadır. Tek taşıyıcı sinyallerin yanı sıra birden fazla taşıyıcıya sahip sinyallerin kullanımı da yaygınlaşmaktadır. Bu gelişmeler, toplumun hayatını kolaylaştırmakla birlikte, radyo frekans spektrumunun izlenmesini ve kontrol edilmesini güçleştirmektedir. Bu zorluğun aşılması, radyo frekans spektrumunun daha hızlı taranması ve sinyallerin daha hızlı işlenebilmesini gerektirir. Bu tür uygulamalardaki en büyük yardımcılarımız, son yılların popüler donanım ürünü olan FPGA (Sahada Programlanabilir Kapı Dizileri) ve kapasiteleri her geçen gün hızla artan Analog Sayısal Çeviricilerdir.

Bu yazıda TÜBİTAK BİLGEM'de geliştirilen FPGA tabanlı, radyo frekans spektrumunu kontrol ve gözetleme ürünleri SGS 2.0 ve ÇİTA tanıtılacaktır.

TÜBİTAK BİLGEM'in geliştirdiği yazılım tabanlı Çok Kanallı İşaret Takip ve Analiz Sistemi (ÇİTA), 20 MHz IF bandgenişliği içerisindeki 64 farklı hedef frekansının aynı anda işlenmesine olanak sağlamaktadır. Kullanıcı müdahalesi olmaksızın, ilgilenilen frekans bantında beliren işaretlerin otomatik olarak tespit edilmesi ve kaydedilmesi yeteneği sayesinde, radyo frekans spektrumundaki haberleşmelerin takibi son derece kolay olacaktır.

Sayısal Spektrum Tarama ve Sinyal İşleme

Spektrum tarama uygulamalarının önemi, son yıllarda giderek artmaktadır. Farklı kişi ve kurumlar, farklı amaçlarla spektrum kullanım bilgisine ihtiyaç duymaktadır. Örneğin, tahsis edilmiş bir frekanstaki yetkisiz yayının tespiti veya belirli bir frekansta yayın yapma hakkına sahip bulunan kullanıcının bant ve güç sınırlarının dışına çıkıp çıkmadığının

denetimi vb. uygulamalar, spektrum izlemede önem kazanmaktadır. İstihbarata yönelik uygulamalarda ise, karşı tarafa ait sinyallerin tespit edilmesi, mümkünse dinlenmesi, değilse daha sonraki analizler için kaydedilmesi esastır. Bir başka uygulama olan istihbarata karşı koymada ise amaç, bilgi kaçaklarına sebep olan yayımların tespit edilmesidir. Bu uygulamaların her biri farklı amaçlara hizmet etse de hepsinin ortak noktası, gelişmiş bir spektrum tarama ve analiz kabiliyetine ihtiyaç duymalarıdır.

Artan kablosuz haberleşme uygulamaları, spektrum kullanımını oldukça yoğunlaştırmış ve bunun sonucu olarak bahsedilen ihtiyaçların karşılanması samanlıktaki iğne aramak kadar güçleşmiştir. Bunun yanı sıra, kullanılan karmaşık haberleşme teknikleri daha hızlı ve hassas tarama yapmayı mecbur kılmaktadır. Yayılmış spektrum (*spread spectrum*) yöntemiyle yayın yapıldığı takdirde sinyal geniş bir bant aralığına yayıldığından tespit edilmesi son derece zorlaşmakta ve gerekli alıcı hassasiyetinin artmasına yol açmaktadır. Eğer haberleşme frekans atlamalı (**frequency hopping**) olarak yapıyorsa, yayının tamamının alınabilmesi için spektrumun yeterince hızlı şekilde taranması gerekmektedir. Tespiti ve izlenmesi doğrudan tarama hızına bağlı olan bir başka yayın tipi de sürekli olmayan, anlık (*burst*) yayınlardır. Bu tip haberleşmede sinyal sürekli olarak değil, kısa bir zaman aralığında gönderilir. Spektrum tarama cihazları tasarlanırken bahsedilen gereksinimler göz önünde bulundurulmalıdır ve cihazın hassasiyeti ile tarama hızı bunlara göre belirlenmelidir. Daha sonra bu gereksinimleri karşılayabilecek olan RF Frekans Düşürücü (RF Down-Converter), ADC (Analog Sayısal Çevirici) ve FPGA bileşenleri seçilmelidir. RF frekans düşürücünün en önemli kısıtlayıcı özelliği, frekansa kilitlenme süresidir.

Sayısal olarak spektrumun nasıl tarandığını anlatmaya başlamadan önce, iki bileşenden kısaca bahsetmekte yarar var. Bunlardan ilki Analog-Sayısal Çevirici

(ADC) tümdevresi, diğeri ise sinyal işlemede önemli bir dönüşüm olan Hızlı Fourier Dönüşümü (FFT) fonksiyonudur. ADC'lerin örnekleme hızlarının ve bit çözünürlüklerinin giderek artmasıyla birlikte daha geniş bant ve daha geniş dinamik aralığa sahip analog işaretlerin sayısal olarak işlenebilmesi olanaklı hale gelmiştir. Günümüzde, örnekleme hızı 400 MHz'e kadar çıkabilen yüksek çözünürlüklü (14-bit) ADC'ler üretilmektedir.

Belirli bir örnekleme frekansına (F_s) sahip ADC ile herhangi frekanstaki bir sinyal örneklenebilir mi? Bu sorunun cevabı maalesef "hayır" dır. ADC'nin örnekeleyebileceği maksimum giriş sinyali bandgenişliği, örnekleme frekansının yarısı, $F_s/2$ 'dir (Nyquist-Shannon Örnekleme Teoremi). ADC'nin sınırlı örnekleme frekans ile tüm spektrumu kapsamak mümkün olmadığından, taranmak istenen bölge daha küçük alt parçalara bölünür. Herhangi bir alt parçayı, ADC'nin örnekeleyebileceği IF (Ara Frekans) bölgesine çekebilmek için, antenden gelen analog sinyal önce *frekans düşürme* işleminden geçirilir. Bunu takiben ADC'de sayısallaştırılan IF işareti, FFT işleminden geçirildikten sonra bu bölgeye ait frekans bilgisi çıkarılmış olur. Aynı işlemler taramak istediğimiz tüm frekans bölgesi tamamlanana kadar devam ettirilir. ADC'lerin daha da gelişerek daha da yüksek frekanslarda örnekleme yapabilmesi ile birlikte spektrum tarama sistemlerindeki analog frekans düşürme işlemine gerek kalmayacağı ve spektrum tarama sisteminin bir anten, bir ADC ve ona bağlı sayısal devrelerden oluşacağı öngörülmektedir.

FFT işlemi, zaman bölgesinden frekans bölgesine dönüşümü sağlamaktadır. Bu işlem sonucunda zaman gösterimindeki veriden frekans gösterimi bilgisi çıkartılır. FFT işlemi gerçekleştirilirken yoğun işlem gücüne ihtiyaç duyulur ve bu ihtiyaç frekans bilgisinin çözünürlüğü arttıkça daha da artmaktadır. FFT algoritması paralel olarak gerçekleştirilebilir ve bu şekilde hızlı bir şekilde sonuç elde edilebilir.

Yazılım Tabanlı Telsiz Mimarisi ile Gerçekleşmiş Alıcı Yapısı

Yazılım Tabanlı Telsiz mimarisine göre analog işaretin ADC tarafından örneklenebilmesi ile elde edilen yüksek hızlı veri üzerinde sırasıyla şu işlemler gerçekleştirilir:

- Sayısallaştırılmış işaretin temel banda indirilmesi,
- Spektrum bilgisinin çıkartılması ve kanallaştırma,
- Demodülasyon vb. analiz işlemleri.

Gerçekleştirilen ilk işlem, kullanıcının izlemek istediği frekans bölgesini belirlemesi ve bu bölgenin temel banda indirgenmesidir; bu işlem sayısal olarak gerçekleştirildiğinden DDC (Digital Down Conversion) adı verilmiştir. Bu işlem sırasında, daha dar bir frekans bölgesinde işlem yapıldığı için hem spektrum bilgisinin çözünürlüğü artar, hem de analiz işlemleri öncesinde ilgilenilen işaretin geniş bant IF işareti içersinden süzülmesi sağlanır.

ADC çıkışındaki sayısal veri yüksek örnekleme hızına sahip olduğundan bu veri üzerinde FFT ve benzeri işlemleri yeterince hızlı bir şekilde uygulayabilmek için yüksek işlem gücüne ihtiyaç duyulur. Bu gereksinimi karşılamak üzere genellikle FPGA tümdevreleri kullanılır. FPGA'lar paralel işlem yapabilme yeteneğine sahip oldukça güçlü birimlerdir. Bu güçten azami şekilde faydalanabilmek için FPGA kaynaklarının verimli olarak kullanılması gerekir. Kaynak paylaşımı sayesinde belirli işlemler zamanda serpiştirilmiş olarak

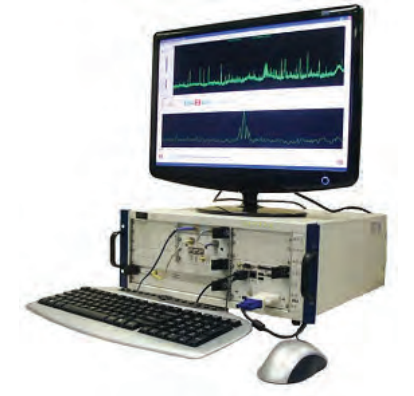
gerçekleştirilebilir ve bu sayede kaynaklar boşta beklemek yerine sürekli farklı kanallara ait verileri işlerler. Bu noktada sinyal işleme blokları için veri hızı ve saat hızı oranı önem kazanmaktadır. Yüksek bir saat hızı ile düşük hızda akan veri, bize veriyi işlemek için geniş bir aralık bırakmaktadır. Çok kanallı bir sinyal işleme yapısında girişte kullanılacak iyi tasarlanmış bir kanallaştırıcı bloğu, ilgilenilen dar bantlı işaretleri alıp veri örnek hızını düşürerek sinyal işleme için daha çok kaynak ayrılabilmesine ve bu kaynakların ortak kullanılabilmesine olanak sağlar.

TÜBİTAK BİLGEM tarafından geliştirilen SGS (Spektrum Gözetleme Sistemi) ve bu yapı üzerine inşa edilen ÇİTA, FPGA kaynaklarını bahsedilen şekilde etkin olarak kullanarak, spektrum gözetleme ve sinyal analizi çözümleri sunmaktadır.

SGS 2.0

SGS sisteminin temel amacı, belirlenen frekans bölgesini hızla taramak ve elde edilen frekans bilgisini sistem kullanıcısının istekleri doğrultusunda işlenebilir hale getirmektir. SGS sayesinde operatör, ilgilediği banttaki faaliyetleri takip etmek için telsiz alıcılarının sunduğu sınırlı yeteneğin ötesine geçip, sinyalleri görselleştirme ve spektrumunda kısa süreli olarak beliren işaretleri kolayca belirleyebilme imkânına sahip olur. Sistem hızlı veri akışı sağlayan PXI tabanlı bir şase üzerine kurulmuştur. Sayısallaştırıcı kartı olarak ise BİLGEM'de tasarlanan ve üretilen USIM-01 kartı, RF ön kuvvetlendirici olarak yine BİLGEM'de

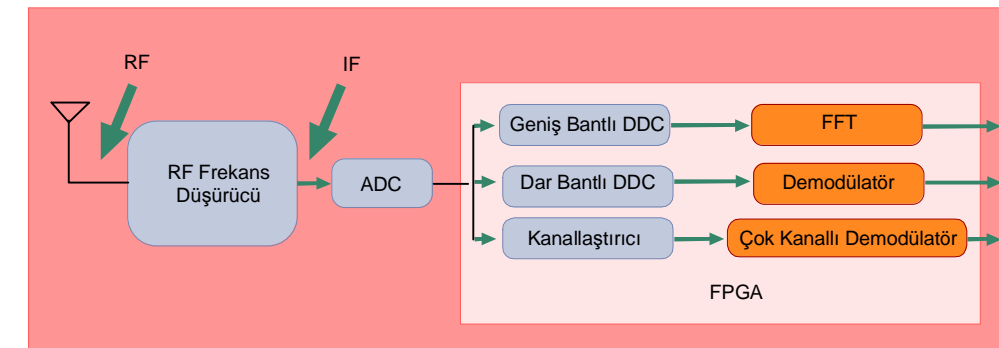
geliştirilen RFK-3001 kartı kullanılmıştır. USIM-01 kartı, üzerinde barındırdığı 16-bit çözünürlüklü 105 MSPS örnekleme hızına sahip ADC, Virtex-4 SX35 FPGA ve 2 adet Texas Instruments 6416 DSP Yongası ile geliştirilen algoritmaların gerçekleştirilmesi için uygun bir altyapı sağlamaktadır. Sistemin kontrolü, yapılandırması ve işletimi için gerekli tüm arayüz ve yazılımlar da BİLGEM'de geliştirilmiştir.



Şekil 2. Yazılım tabanlı telsiz teknolojisine dayalı 6U CompactPCI tabanlı spektrum gözetleme sistemi genel görünümü.

Sistemin frekans tarama bandı 9 kHz - 2.7 GHz aralığında seçilebilmektedir. Frekans düşürücünün bandgenişliği 20 MHz olup, IF merkez frekansı 15 MHz'dir. İzleme sırasında, sayısallaştırıcı kart analog giriş işaretini örnekler ve üzerindeki FPGA tümdevresinde işler. FPGA üzerinde sayısal frekans düşürme (DDC), pencereleme (windowing) ve FFT işlemleri gerçekleştirilmekte olup zaman bilgisinden frekans bilgisine geçilir. Sistemin çözünürlüğü, kullanıcı tarafından 0.05-62.5 kHz aralığında ayarlanabilmektedir. Sistemin duyarlılığı, frekans düşürücü üzerindeki zayıflatıcıların ya da RF ön kuvvetlendiricinin kazançlarının ayarlanması ile artırılabilir. Bu sayede -130 dBm seviyesindeki zayıf sinyallerin tespit edilebilmesi mümkün olur. Sistemin dinamik aralığı ise 96 dB'dir.

Sistem bu teknik özelliklerinin yanı sıra, operatör için kullanım kolaylığı sağlayan birçok fonksiyona sahiptir. Kullanıcı, ilgilemediği veya ekranda görmek istemediği sinyalleri maskeleyebilir, maskeleydiği sinyalleri bir listeye



Şekil 1. Yazılım tabanlı telsiz mimarisi ile gerçekleştirilmiş bir alıcı yapısı.

kaydedebilir ve ihtiyaç duyması halinde geri yükleyebilir. Kullanıcı, sadece ilgilendiği ve takip ettiği sinyallerin frekans listesini girebilir ve bu frekanslarda yayın tespit edildiğinde kendisinin uyarılmasını sağlayabilir. Operatör, ekrandaki bir yayım üzerine tıklayarak bu yayıma ait frekans, modülasyon veya bandgenişliği bilgilerini kendisine bağlı bir birime gönderebilir. (Bu bağlantı, yakınındaki bir cihazla doğrudan bağlantı olabileceği gibi, Ethernet arayüzü üzerinden uzaktaki bir alıcıyla bağlantı şeklinde de olabilir.) Bağlantı kurulan birim ise, uygun ayarları kullanarak otomatik dinleme kaydını başlatabilir. SGS 2.0 sisteminin kontrolü, ağ üzerinden de yapılabilir.

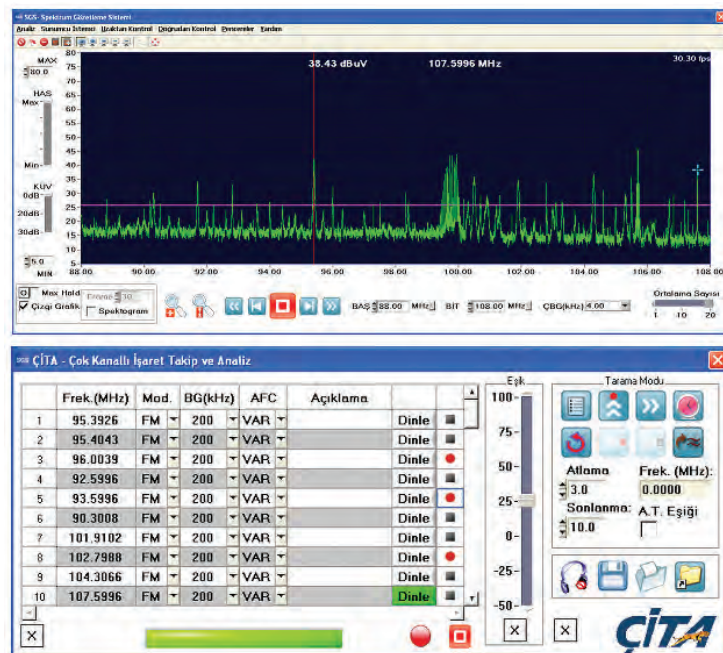
ÇİTA (Çok Kanallı İşaret Takip ve Analiz) Sistemi

ÇİTA, yayımların otomatik olarak tespit edilmesi, kaydedilmesi ve dinlenmesini sağlayan bir sistem olup geniş bir bant içerisinde birden fazla



Şekil 3. ÇİTA sisteminin logosu.

dar-bantlı işareti aynı anda işleme imkânı sunmaktadır. Hızlı spektrum tarama yeteneği ile birlikte, oldukça başarılı bir sinyal tespit ve analiz sistemi sağlar. ÇİTA bu özelliklerini hızlı ve verimli çalışan FPGA tabanlı sinyal işleme tekniklerine borçludur. Sistem PXI tabanlı bir şase üzerine kurulmuştur. RF ön-kuvvetlendirici olarak BİLGEM ürünü olan RFK 3001 kartı kullanılmıştır. Sistem üzerinde, yine BİLGEM'de geliştirilmiş olan 2 adet USİM-01 sayısallaştırıcı ve sinyal işleme kartı bulunmaktadır. Kartlardan bir tanesinin görevi belirlenen frekans bölgesini çok hızlı taramak, diğersinin amacı ise bu banttaki birden fazla dar bantlı işareti gerçek zamanlı olarak ve aynı anda işlemektir.



Şekil 4. SGS sistemi ve ÇİTA yazılımı kullanıcı arayüzü genel görünümü.

ÇİTA sistemi 20 MHz bandgenişliğine sahip bir frekans bölgesinde, bandgenişliği 200 kHz'den küçük olan 64 tane işareti aynı anda tespit ve analiz yeteneğine sahiptir. Bu işlemlerin verimli olarak gerçekleştirilebilmesi için tüm bant içerisindeki herhangi bir yayıma odaklanmak yerine, tüm bant önce alt-kanallara bölünmüştür. Daha sonra bu alt-kanalların içerisindeki bir yayıma odaklanmak tercih edilmiştir. Bu amaca yönelik olarak çok-fazlı kanallaştırıcı yöntemi ile tasarım yapılmıştır. Böylelikle sayısal işaret işleme kartının en verimli şekilde kullanılması sağlanmıştır.

Bu işlem şu adımlarla gerçekleştirilmektedir:

- 9 kHz - 2.7 GHz aralığından izlenmek istenen, 20 MHz band genişliğindeki frekans bölgesi, analog frekans-düşürücü tarafından IF'e indirilmektedir. Bu geniş bant IF sinyali, her iki USİM-01 kartında ayrı ayrı olarak sayısallaştırılmaktadır. Birinci USİM-01 kartı üzerindeki FPGA, sayısallaştırılan veriyi, seçilen çözünürlük bant genişliği değerine bağlı olarak işlemekte ve frekans bilgisi elde edilmektedir. İkinci USİM-01 kartı üzerindeki FPGA ise, geniş bantlı işareti, özel bir algoritma kullanarak 64 alt kanala böler. Diğer bazı kanallaştırma yöntemlerinin aksine, frekans bandının tamamı kapsamaktadır.

- Program tarafından otomatik olarak veya operatör tarafından 64 adet frekans ve bu frekansların ait olduğu alt kanallar belirlenir. İstenildiği takdirde, her bir kanal için uygun demodülasyon yöntemi ve bandgenişliği bağımsız olarak seçilerek, çözümlenmiş ses örnekleri elde edilebilir. Ses kaydı sırasında kullanılan sıkıştırma teknikleri ile kayıt süresi günler mertebesine çıkarılmıştır.

- Bu aşamadan itibaren, aynı anda 64 kanala ait karmaşık temel bant işaretler ya da çözümlenmiş ses verisi PXI veriyolu üzerinden alınarak kaydedilebilir ya da operatör tarafından dinlenebilir.

- Sinyallerin tespit edilmesi ve incelenmesi için "Adım Tarama", "Bant Tarama" ve "Güç Seviyesi ile Tetiklenme" modları gerçekleştirilmiştir. Adım Tarama modunda, seçili bantta tespit edilen işaretler sırayla işlenerek operatöre dinletilir ve arzu edildiği takdirde kayıt edilmeye başlanır. Bant Tarama modunda, operatör tarafından girilen hedef frekansları arasında sürekli gezilir ve yine kullanıcı etkileşimi beklenir. Güç Seviyesi ile Tetiklenme modu ise operatör müdahalesi ihtiyacını en aza indirerek girilen hedef listesinde herhangi bir faaliyet tespit ettiğinde doğrudan kayda başlar ve faaliyet sonlanana kadar devam eder.

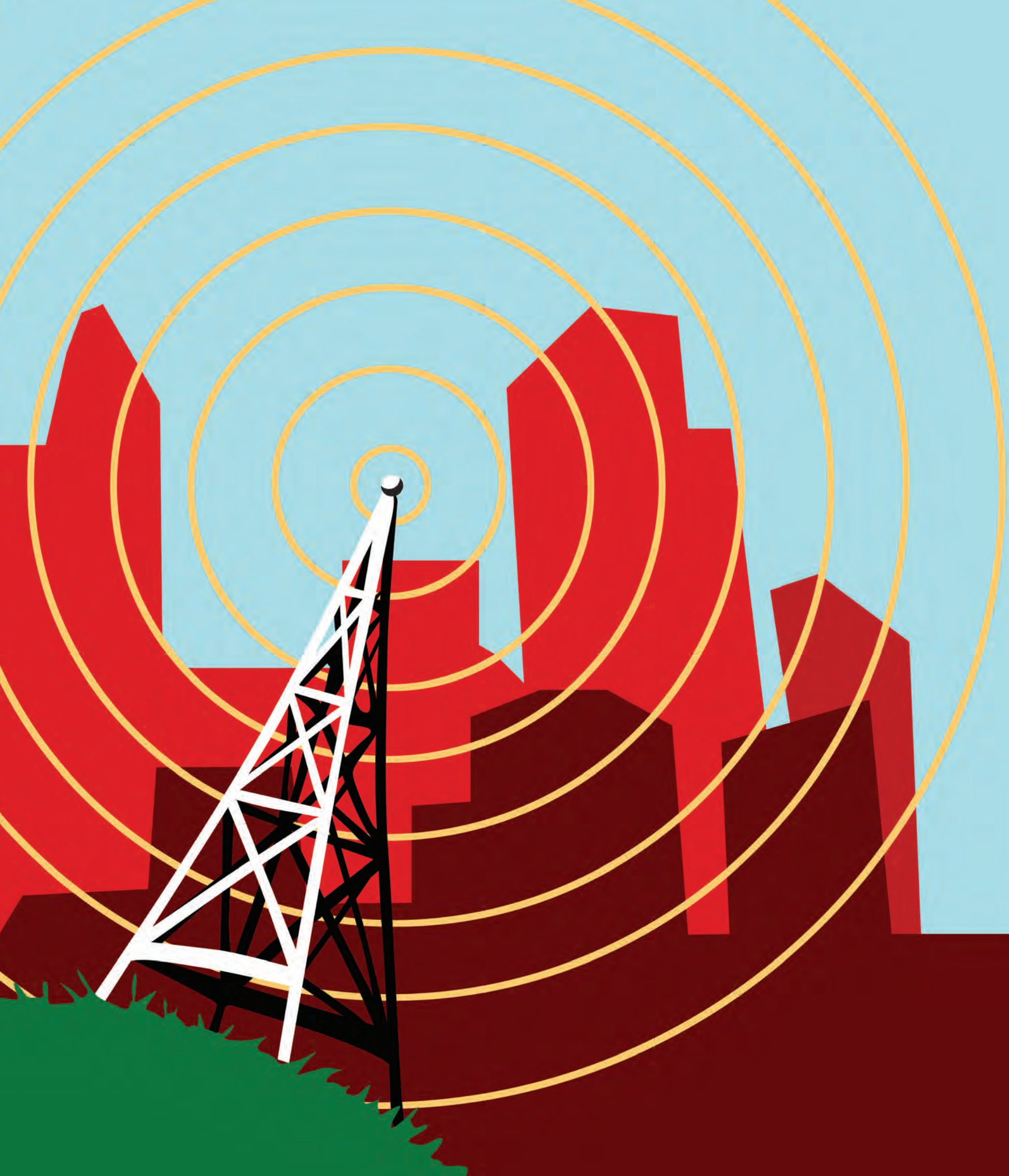
- Sistemin başında sürekli bir operatör bulunması ihtiyacı ortadan kalkmaktadır. Hedef frekanslar ve modülasyon tipleri girildikten sonra sistem bir haberleşme tespit ettiğinde otomatik olarak kayıt yapabilmektedir. Cihazın yeni sürümlerinde, bandgenişlikleri ve modülasyon tiplerinin otomatik olarak yüksek doğrulukla tespit edilmesi ve konuşma algılama



Şekil 5. SGS ve ÇİTA'nın üzerinde koştuğu sinyal işleme modülü USİM-01.

algoritmalarının geliştirilmesi ile operatör müdahalesinin en aza indirilmesi amaçlanmaktadır.

ÇİTA tamamen yazılım tabanlı telsiz teknolojisine dayanmaktadır ve kolaylıkla güncellenebilir bir yapıdadır. Güncelleme işlemi 10 dakikadan daha kısa bir sürede gerçekleştirilebilir. İleri sinyal işleme tekniklerinin kullanıldığı bu alman tek başına, uçak, helikopter, İHA (İnsansız Hava Aracı) gibi yer ve ağırlık kısıtlamalarının bulunduğu taktik platformlarda 64 analog almanın görevini tek başına yerine getirebilmektedir.



MODÜLER TELSİZ RF MİMARİSİ

Ali DAĞDEVİREN

Dilimize AM veya FM yayınlarını dinlememize yarayan cihazların ismi olarak özelleşmiş bir şekilde giren radyo kelimesinin, gerçek anlamı çok daha geniştir. Radyo, temel bantta işlenmiş veriyi elektromanyetik spektrumun 30 kHz – 300 GHz frekans aralığında, alıcı ya da verici olarak kablosuz iletimini sağlayan cihazlara verilen genel addır. Günümüz haberleşme, sanayi, sağlık, elektronik harp sistemlerinin vazgeçilmez bir unsurudur.

Radyo, anteniyle tümleşik düşünülürken, bilginin kanal (hava, su vb.) ortamından geçişini çift yönlü sağlayan, yazılımı (software) ve belgenimi (firmware) olan elektronik devrelerden oluşur. Geleneksel radyo yapısında, yüksek frekanslı RF (Radyo Frekansı) katımı bir analog işaret işleme birimi izler. İşlevsellik yönünden kısıtlı, yüksek maliyetli, sabit bant genişlikli, az sayıda (çoğunlukla sadece bir) modülasyonu destekleyen analog işaret işleme katımın yerini, özellikle son çeyrek asırda FPGA (Field Programmable Gate Array, Sahada Programlanabilir Kapı Dizileri) ve DSP (Digital Signal Processors, Sayısal İşaret İşleyiciler) tümleşik devreleri almıştır. Yarı iletken teknolojisinde yaşanan gelişmelere paralel olarak, daha karmaşık analog/sayısal çeviriciler (ADC, Analog to Digital Converters) geliştirilmiş, birim maliyet ve boyutlar küçülmüş, analog devrelerle yapılan işlemler (demodülasyon, filtrelemeler vb.) daha çok sayısal tarafa aktarılmaya başlanmıştır. Artık alıcılar, RF işaretini temel banda indirip analog/video çözümleme yerine, RF'ten bir IF'e (Intermediate Frequency, Ara Frekans) indirip ADC'ler ile sayısallaştırmakta ve

işareti FPGA ve DSP'ler ile işlemektedir. HF (High Frequency, 3 – 30 MHz) gibi düşük frekanslı yayınlar ise, entegre ön iyileştirme katı bulundurmaları koşuluyla, artık doğrudan sayısallaştırılabilmektedir. Yazılım tabanlı telsizler, temel banttaki tüm işlemlerin sayısal yöntemlerle gerçekleştirilebilmesinin sağladığı esneklikle, farklı modülasyonlarla, farklı modlarda, farklı frekanslarda, farklı fonksiyonları gerçekleştiren haberleşmeleri, hiçbir donanım değişikliğine gitmeden sadece yazılım güncellemesiyle gerçekleştirebilmektedir. ADC'lerin karmaşıklaşmasıyla birlikte (yüksek saat frekansı, geniş dinamik aralık vb.) IF frekansı daha yukarılara taşınmaya başlanmış, bu da RF analog alıcı / verici bölümlerini daha da kolaylaştırmıştır.

Özetlenecek olursa, yazılım tabanlı telsizler iki ana fonksiyondan oluşur:

- RF Katı: Analog Frekans Çevirme (Düşürme / Yükseltme / İyileştirme)

- DSP Katı: Sayısal İşaret İşleme

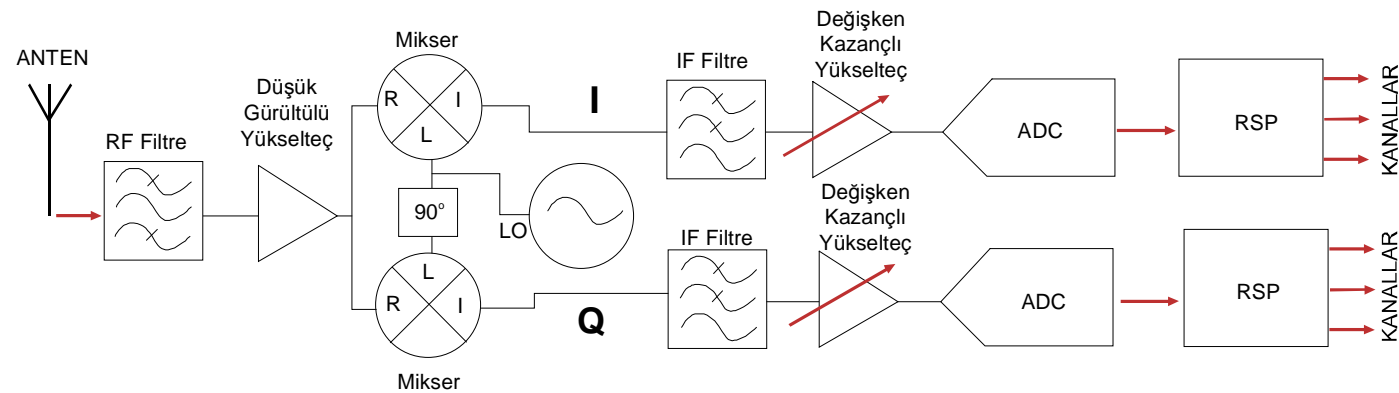
Bu yazıda yazılım tabanlı telsizlerin sadece RF katlarına değinilecek, popüler topolojiler incelenecektir.

YTT (Yazılım Tabanlı Telsiz) Alıcı Mimarisi

YTT alıcıları iki ana topolojide incelemek mümkündür:

1. Doğrudan Düşürücü Alıcılar (Homodin, Sıfır IF)

En basit yapıdaki alıcılardır ve genelde dar bantlı uygulamalarda kullanılırlar.



Şekil 1. Doğrudan düşürücü bir alıcı yapısı.

Şekil 1'de yapısı gösterilen bu mimaride RF işareti, aynı frekanstaki bir lokal osilatörle çarpılıp doğrudan temel banda indirilir, I ve Q bileşenlerine ayrılır. I ve Q verisi sayısallaştırılarak işlenir. Tek karıştırıcı kullanılıp I ve Q bileşenleri sayısallaştırıcı tarafında da doğrudan sayısal düşürücülerle ayrıştırılabilir. Sistemin bileşenlerinin işlevleri bir sonraki bölümde ele alınacaktır.

2. Süperheterodin Alıcılar:

Ana blok yapısı Şekil 2'de görünen süperheterodin alıcılarda RF işareti en az bir IF'e düşürülür.

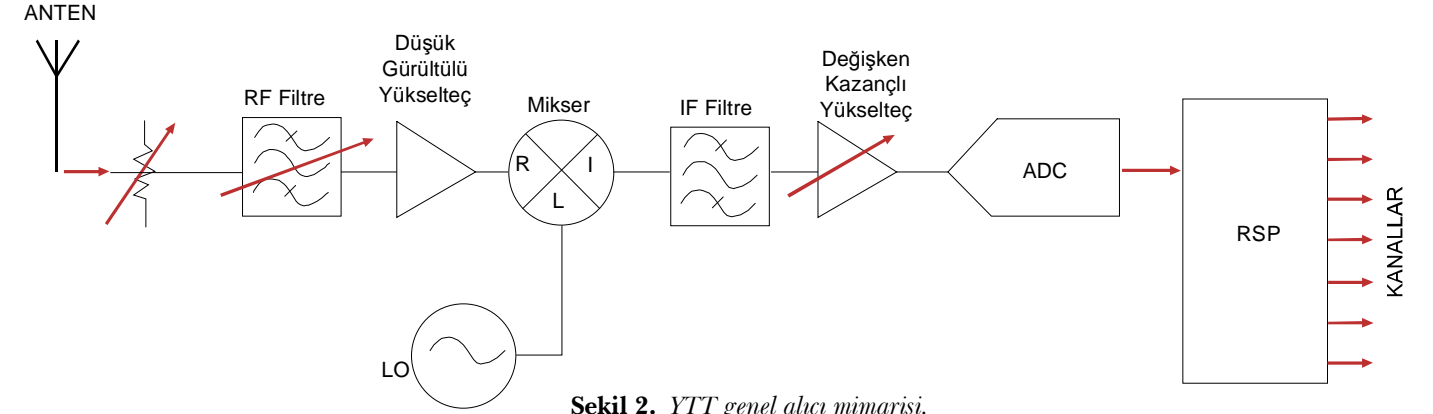
Frekans düşürme işlemi, RF bandın ve ilk LO (Lokal Osilatör) olarak kullanılan sentezleyicinin karmaşıklığına göre – yukarıda olduğu gibi – tek aşamada gerçekleştirilebileceği gibi çok sayıda çevirme katıyla da gerçekleştirilebilir. IF'e indirilen işaret, ADC'ler ile örneklenip sayısallaştıktan sonra RSP (Receive Signal Processors, Alıcı İşaret İşleyiciler) katındaki FPGA ve DSP tümleşik devrelerle sayısal filtrelenir, demodüle edilir ve kanallaştırılır.

Şekil 2'de gösterilen genel bir YTT alıcısında alt blokların işlevlerine geçmeden önce bir alıcıdaki sistem parametrelerini ve bu parametrelerin fiziksel olarak neye karşılık geldiği üzerinde durmak gerekir:

Alıcılarda Temel Sistem Parametreleri:

NF (Noise Figure, Gürültü Katsayısı): Bir alıcının girişindeki işaret gürültü oranının çıkışındaki orana denir. Cihazın duyarlılığı (sensitivity) belirleyen ana faktördür.

Modüler Telsiz RF Mimarisi



Şekil 2. YTT genel alıcı mimarisi.

NFL (Noise Floor, 'Gürültü Tabanı'): Alıcıdaki demodülatörün girişindeki toplam gürültüdür. Miktarı;

$$NFL = -174 \text{ dBm/Hz} + NF + 10 \log BW$$

eşitliği ile bulunur. Burada BW alıcının açtığı çözünürlük bant genişliğidir.

S (Sensitivity, 'Duyarlılık'): Alıcıdaki demodülatörün belirleyebileceği veya çözülebileceği en düşük işaret seviyesidir. Seviyesi, işaret belirleme durumunda, gürültü tabanı kadardır. Çözme durumunda (analog/video/veri çözümleme) ise gürültü tabanından demodülatörün istediği en düşük işaret gürültü oranı kadar fazladır. En düşük işaret gürültü oranını ise işaretin istenen kalitesi (bit hata oranı, ses veya görüntü kalitesi, demodülasyon tipi vb.) belirler. Denklemi;

$$S = NFL \quad (\text{Tespit})$$

$$S = NFL + SNR_o \quad (\text{Çıkış işaret gürültü oranı}) \quad (\text{Çözme})$$

şeklinde dir.

Arakipleme (Intermodulation): Doğrusal olmayan RF elemanların (karıştırıcı, yükselteç vs.) girişindeki iki veya daha fazla işaretin ürettiği çok tonlu ürünlerdir. Örneğin bir karıştırıcının girişindeki f_1 ve f_2 işaretleri birbiriyle modüle olarak karıştırıcı çıkışında $m f_1 \pm n f_2$ işaretleri üretir. Bunlardan $f_1 \pm f_2$, $2f_1$, $2f_2$ olanlarına ikinci dereceden ($m+n=2$) arakipleme ürünleri; $2f_1 \pm f_2$, $2f_2 \pm f_1$, $3f_1$, $3f_2$ olanlarına üçüncü dereceden ($m+n=3$) arakipleme ürünleri, vb. denir.

IIP2 (2nd Order Input Intercept Point, 'Giriş İkinci Dereceden Kesişme Noktası'): Alıcının ana işaretinin kazanç eğrisi ile 2. dereceden arakipleme bileşenlerinin kazanç eğrisinin kesişme noktasındaki giriş işaret seviyesidir.

IIP3 (3rd Order Input Intercept Point, 'Giriş Üçüncü Dereceden Kesişme Noktası'): Alıcının ana işaretinin kazanç eğrisi ile 3. dereceden arakipleme bileşenlerinin kazanç eğrisinin kesişme noktasındaki giriş işaret seviyesidir.

P1dB (1 dB Compression Point, '1 dB Sıkışma Noktası'): Alıcının kazanç eğrisinin doyum noktasına yaklaşarak ideal kazanç eğrisinden 1 dB düştüğü yerdeki giriş işaret seviyesidir.

DR (Dynamic Range, 'Dinamik Erim'): Demodülatörün aynı anda çözülebileceği en yüksek genlikli işaret ile en düşük genlikli işaret arasındaki genlik farkıdır. En düşük genlikli işareti belirleyen alıcının duyarlılığı, en yüksek genlikli işareti belirleyen ise alıcının P1dB, IIP3 veya IIP2'sidir. Dolayısıyla üç farklı şekilde hesaplanabilir:

$$DR = P1dB - S \quad (1 \text{ dB Sıkışma Noktası Dinamik Erimi})$$

$$SFDR3 = 2/3 * (IIP3 - S) \quad (3. \text{ Derece Hayal İşaretsiz Dinamik Erim})$$

$$SFDR2 = 1/2 * (IIP2 - S) \quad (2. \text{ Derece Hayal İşaretsiz Dinamik Erim})$$

Seçicilik (Selectivity): Ayarlanan kanal ile komşu kanallar arasındaki bastırma oranıdır. Anahtarlanan IF filtreye göre bastırma oranı değişir.

Bir YTT Alıcısının Alt Blokları ve İşlevleri

Şekil 2'de gösterilen bir YTT alıcısında alt blokların işlevleri şu şekildedir:

Ayarlanabilir RF Zayıflatıcı: Alıcı antene gelen yüksek genlikli işaretlerin alıcıya zarar vermesini önlemek, alıcının IIP3 (Giriş üçüncü dereceden kesişme noktası) ve P1dB (1 dB sıkışma noktası) değerlerini yükseltmek doğrusal bölgede çalışmasını sağlamak, hayal işaret seviyesini azaltmak ve VSWR'ı (Voltage Standing Wave Ratio, Gerilim Duran Dalga Oranı) iyileştirmek için kullanılır.

RF Filtre: LO geri yayılımını önlemek, hayal frekansları ve doğrudan IF işaretini bastırmak, hayal işaret seviyesini düşürmek gibi fonksiyonları vardır. Tasarımda hedef alınan RF bant genişliğine göre ayarlanabilir, anahtarlanabilir (Ön Seçici) veya tek filtre (dar RF bandı) yapısındadır.

Düşük Gürültülü Yükselteç: Gerekli olduğunda tüm alıcı sistemin gürültü katsayısını düşürerek, duyarlılığını arttırmak için kullanılır.

Karıştırıcı: İlk LO sentezleyicisiyle birlikte frekans dönüştürme (düşürme veya yükseltme) işlevini gerçekleştirir. Alıcıdaki çevirme katı sayısı kadar karıştırıcı kullanılır ve her karıştırıcıyı

süren bir LO kaynağı vardır. LO kaynakları genelde ilk çevirme katında ayarlanabilir, diğer çevirme katlarında değişmez olsa da farklı frekans planlarına göre durum değişebilir.

IF Filtre: Çevirme işleminde ortaya çıkan istenmeyen işaretleri (hayal işaretler, LO, RF sızması vb.) süzmek için kullanılır.

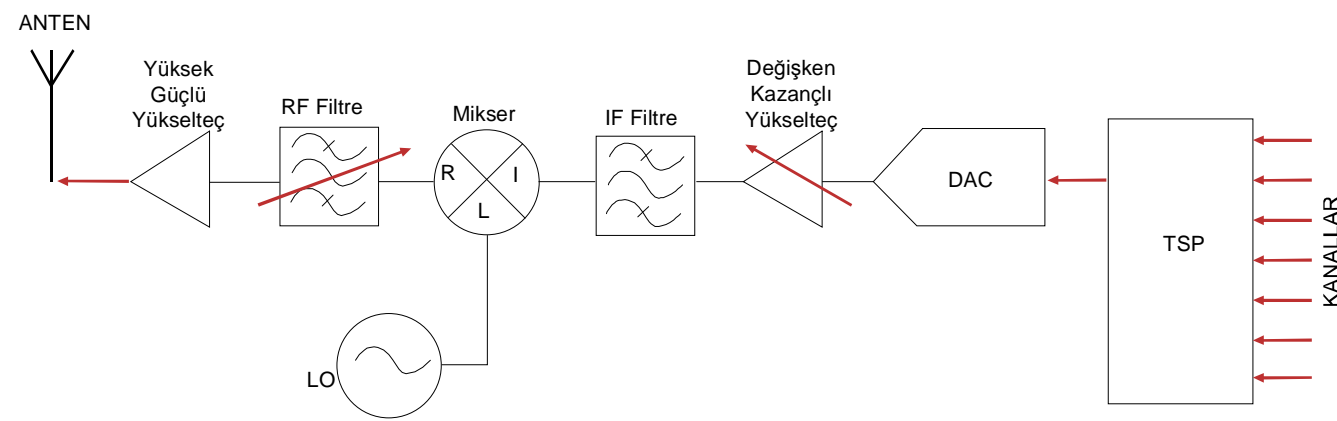
Değişken Kazançlı Yükselteç: İşaret seviyesini ADC için istenen seviyeye getiren seri zayıflatıcı ve yükselteçlerden oluşur. Otomatik ya da elle ayarlanır kazanç kontrollerinde kazanç ayarını sağlar.

YTT Verici Mimarisi

Şekil 3'te ana blok şeması görülen verici mimarileri, alıcılara göre işaret akış yönü tersten düşünüldüğünde (temel banttan RF katına) oldukça benzese de birkaç yönden ayrılır:

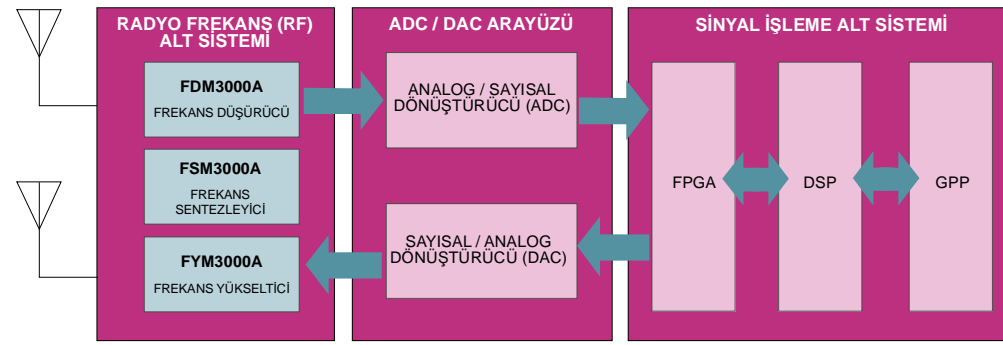
- Sayısal veri (doğal olarak) sayısalan analoga çevrilir.
- Düşük gürültülü yükselteç yerine çıkış katında (duruma göre) yüksek güçlü yükselteç bulunur.
- RF Filtre katındaki Son Seçici frekans planı, Ön Seçici frekans planı ile örtüşmeyebilir.

YTT vericileri de alıcılardaki gibi doğrudan yükseltici ya da süperheterodin mimarisine sahiptir.



Şekil 3. Yazılım tabanlı telsiz genel verici mimarisi.

UEKAE'de Geliştirilen YTT Test Platformu



Şekil 4. YTT test platformu ana blok şeması.

UEKAE'de yürütülen Yazılım Tabanlı Telsiz Test Platformu projesi kapsamında tamamen milli olanaklarla bir RF Alt Sistem geliştirilmiştir. Şekil 4'te görülen bu sistem dört ana cihazdan oluşur: FDM3000A Frekans Düşürücü (RF'ten IF'e), FYM3000A Frekans Yükseltici (IF'ten RF'e) ve 2 adet FSM3000A Frekans Sentezleyici.

FDM3000A Frekans Düşürücü



Şekil 5. FDM3000A frekans düşürücü.

FDM3000A, mimarisi Şekil 2'de görülen süperheterodin bir almac biriminin RF/IF katını oluşturur. 20-3000 MHz frekans aralığındaki RF işaretleri 70 MHz IF frekansına çevirir. En fazla 40 MHz analog bant genişliğini destekleyen cihazın özellikleri Tablo 1'de özetlenmiştir.

Tablo 1. FDM3000A Teknik Özellikleri

Frekans Aralığı	20 MHz-3 GHz
Maksimum RF Giriş Genliği	+20 dBm
Giriş Zayıflatıcılar	0-32 dB
P1dB (0dB RF ATT, LNA ON, Ortalama)	-10 dBm
IIP3 (0dB RF ATT, LNA ON, Ortalama)	0 dBm
NF (Ortalama)	5 dB
IF Frekansı	70 MHz
Analog IF band genişlikleri	40 MHz, 5 MHz, 1 MHz, 0.25 MHz
Maksimum IF çıkış genliği	10 dBm
Otomatik Kazanç Kontrolü	Var
Manuel Kazanç Kontrolü	96 dB
Genlik Çözünürlük	0.5dB
Kontrol	ETHERNET, RS232
Elektriksel	90-260 VAC giriş, 47 ~ 63 Hz
Mekanik	1U, 19" STANDART

FYM3000A Frekans Yükseltici



Şekil 6. FYM3000A frekans yükseltici.

FYM3000A, mimarisi Şekil 3'te görülen süperheterodin bir verici biriminin IF/RF katını oluşturur. 70 MHz'deki IF işaretini 20-3000 MHz frekans aralığındaki bir RF işaretine çevirir. En çok 40 MHz analog bant genişliğini destekleyen cihazın özellikleri Tablo 2'de özetlenmiştir.

Tablo 2. FYM3000A Teknik Özellikleri

IF Frekansı	70 MHz
Maksimum Band Genliği	40 MHz
Manuel Kazanç Kontrolü	63 dB
Genlik Çözünürlük	0.5dB
Maksimum IF Giriş Genliği	0 dBm
Maksimum RF Çıkış Genliği	10 dBm
RF Frekans Aralığı	20 MHz-3 GHz
Kontrol	ETHERNET, RS232
Elektriksel	90-260 VAC giriş, 47 ~ 63 Hz
Mekanik	1U, 19" STANDART

Sürdürülen / Planlanan Diğer Alıcı Çalışmaları:

- Ray tipi FDM3000A alıcısı yerine, yine aynı frekans aralığını (20-3000 MHz) kapsayan daha küçük (Compact PCI şaseye uyumlu) 6U 4hp'lik FDM3000B'nin tasarımı Mart 2011'de bitmiş ve ürün haline getirilmiştir.
- Aynı alıcının daha geniş bantlı uygulamalar için farklı IF frekansı kullanılarak (140 MHz, 160 MHz) ayrı bir sürümünün tasarımı planlanmaktadır.
- 3-8 GHz Frekans Genişletici kullanılarak frekans aralığının 3 GHz'den 8 GHz'e çıkartılması planlanmaktadır.
- Haziran 2011'de 10kHz-18 GHz'lik aralığını kapsayan (40 MHz IF bant genişliği) alıcının tasarımının bitirilmesi öngörülmektedir.



**GENİŞBAND
FREKANS
SENTEZLEYİCİ
YAPILARI**
HÜSEYİN ANIKTAR

Frekans sentezleyicilerinin ana işlevi bir veya birden fazla referans işaretini (genellikle 10MHz), belirli adım aralıklarında istenen çıkış frekanslarına dönüştürmektir. Tek ton frekans çıkışı veya dar bantlı LO (lokal osilatör) işaretleri çoğu elektronik uygulaması için yeterli olmakla beraber artık modern geniş bantlı sayısal haberleşme sistemleri için yeterli olmamaktadırlar. Gelişmiş modern haberleşme sistemleri için daha geniş bantlı (birkaç oktav) ve düşük çözünürlüklü (1Hz'den küçük adım aralığı olan) LO gereksinimi duyulmaktadır. Yapılandırılabilir (reconfigurable radio) veya yazılım tabanlı telsiz (software defined radio) uygulamaları geniş bantlı LO gereksinimlerinin duyulduğu modern haberleşme sistemlerinden bazılarıdır.

Frekans sentezleyicilerinin (veya LO) tasarım ve başarımlarını belirleyen temel parametreler, sentezleyicinin band genişliği, frekans çözünürlüğü, frekans atlama hızı (kitlenme süresi), faz gürültüsü, süpür (spurious) ve harmonik seviyeleri, çıkış güç seviyesi, boyut ve maliyet olarak sıralanabilir. Bu parametrelerin bazıları arasında ters orantı (trade-off) vardır. Bazı parametrelerde iyileştirme sağlanırken diğerlerinde bozulma olmakta bu da tasarımı zorlaştırmaktadır. Frekans sentezleyicisinin kullanılacağı uygulamanın ekstra önem gerektirdiği parametrelerde iyileştirme sağlanırken diğerlerinde kötüleşmeye göz yumulabilir. Bu da bir tasarımın eniyilemesini gerektirmektedir.

Frekans sentezleyicilerinin dar bantlı olmaları, literatüre göre, en çok %20'lik bir band genişliğine sahip olmaları anlamına gelmektedir [1, 2]. %20'lik bantdan daha geniş banda sahip olanlar, geniş bantlı frekans sentezleyici olarak adlandırılabilir. Frekans sentezleyicilerinin genel kullanım alanı almaç (receiver) yapılarında LO kaynağı olarak kullanılmalarıdır. LO'lar karıştırıcı (mixer) sürdürüklerinden çıkış güçlerinin çoğunlukla +10dBm ile +17dBm arasında değişen bir seviyede olması gerekmektedir. LO kaynaklarındaki süpürler doğrudan almaç

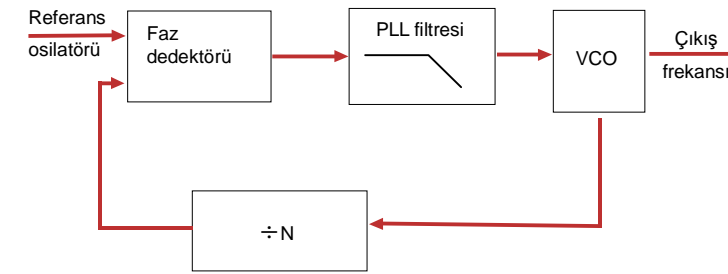
spektrumuna düşmektedirler. Bu da almaçın istenilen işareti seçebilme, yakalayabilme yeteneğini kısıtlamaktadır. Bu anlamda iyi bir almaç için LO kaynağının süpür seviyelerinin -60dBc'lerde olması beklenmektedir. Frekans sentezleyicilerinin veya LO kaynaklarının harmonik seviyelerinin ana işaretten genellikle 20 – 30dBc aşağıda olması yeterli olabilmektedir. Harmoniklerin buldukları yerlerin belirli olması ve ana işaretten belirli uzaklıkta olmaları nedeniyle kolaylıkla süzülmemektedirler. Almaçların, istenilen işareti seçebilme veya yakalayabilme (sensitivity) yeteneklerini sınırlayan en önemli ve duyarlı parametrelerden biri de faz gürültüsüdür. Faz gürültüsü genellikle, 100Hz, 1kHz, 10kHz, 100kHz ve 1MHz ofsetlerde belirlenen değerlerdir. Bir frekans sentezleyici için 100kHz'de -120dBc/Hz'lik bir faz gürültüsü iyi bir değer sayılabilir. Diğer ofset frekanslarındaki faz gürültü değerleri de kabul edilebilir seviyelerde olmalıdırlar. Frekans atlamalı telsiz veya hızlı spektrum tarama gibi uygulamalarda bir frekans sentezleyiciden beklenen en önemli parametrelerden bir diğeri de kitlenme süresi yani bir frekanstan başka bir frekansa atlama hızıdır. Orta ayarda bir frekans sentezleyici için kitlenme süresi birkaç milisaniyedir. Hızlı bir frekans sentezleyici için kitlenme süresi birkaç yüz mikrosaniyedir. Teknolojik eğilim bu hızı mikrosaniyelerin de altına indirerek nanosaniyelere çekmektedir. Frekans sentezleyicilerinden beklenen bir diğer özellik de adım aralığı yani frekans çözünürlüğüdür. Bugünkü teknoloji ile 1Hz'den küçük çözünürlüklü frekans sentezleyicileri gerçekleştirmek artık olasıdır. Son olarak, frekans sentezleyicilerini gerçekleştirirken, maliyet, boyut ve güç tüketimi de göz önünde bulundurulması gereken önemli parametrelerdir.

Frekans sentezleyicilerini gerçekleştirmek için çok çeşitli mimariler kullanılabilir. Genellikle kullanılan mimariler VCO

(voltage controlled oscillator) tabanlı PLL (phase locked loop) yapıları, YIG (Yttrium Iron Garnet) tabanlı PLL yapıları ve DDS (direct digital synthesizer) tabanlı yapılarıdır.

VCO tabanlı PLL yapılarında kullanılan referans işaretindeki faz gürültüsünün çok iyi olması tüm sistemin faz gürültüsünün iyi olması için birincil şarttır. Bu nedenle genellikle referans olarak OCXO ('oven controlled crystal oscillator') kullanılır. Uzak alanda (100kHz ofsetten sonra) VCO faz gürültüsü daha baskındır. Bu bölgede VCO'nun faz gürültüsünün iyi olması önemlidir. Yakın alanda (<100kHz) ise referansın faz gürültüsü baskındır. Dolayısıyla kullanılacak referansın iyi bir faz gürültüsüne sahip olması önemlidir. Bunların dışında faz detektörünün faz gürültüsü ile N (VCO frekans bölücü) ve R (referans frekans bölücü) bölme oranları da faz gürültüsüne önemli katkıda bulunurlar. Frekans çözünürlüğü (adım aralığı) ne kadar küçük ise N değeri de o kadar büyük ve faz gürültüsü de $20\log(N)$ kadar daha kötüdür. Bu nedenle VCO tabanlı PLL yapılarında en fazla kHz çözünürlüklere ulaşılabilmektedir. Bu çözünürlüklere ulaşmak içinde genellikle tek PLL yapısı yeterli olmayıp iç içe birden fazla PLL döngüsünün kurulması gerekmektedir bu da karmaşıklığı arttırmaktadır. Yukarıda bahsedildiği gibi VCO faz gürültüsünü kontrol etmenin en önemli yöntemi iyi bir referans (OCXO) kullanmaktır. PLL için belirlenen kesim frekansı (loop BW) faz gürültüsünü ve kitlenme hızını belirleyen en önemli parametredir. Kesim frekansı ne kadar geniş olursa VCO gürültüsü daha fazla bandın içerisine girecek ve sistemin faz gürültüsü kötüleşecektir. Ancak bu durumda PLL daha hızlı kitlenecektir. Kesim frekansını düşürdüğümüzde bandın içerisine giren VCO gürültüsü azalacak, referansın ve faz detektörünün faz gürültüsü daha baskın olacaktır. Bu durumda frekans sentezöründen daha iyi bir faz gürültü performansı elde edilecek ancak frekans kitlenme hızı yavaşlayacaktır.

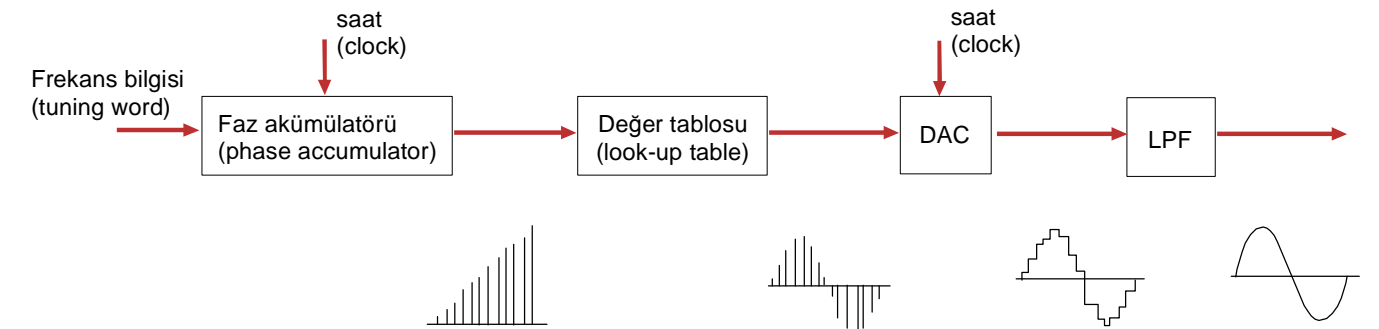
Bu aşamada eniyilemenin yapılması gerekmektedir. VCO tabanlı sentezleyiciler hem maliyet olarak hem de boyut olarak uygundur. VCO tabanlı PLL yapıları, frekans çözünürlüğü kHz seviyesinde, milisaniye hızlarında ve ortalama bir faz gürültüsü performansı gerektiren uygulamalar için çok iyidirler. Şekil 1'de VCO tabanlı klasik bir PLL yapısı görülmektedir.



Şekil 1. Klasik VCO tabanlı PLL blok diyagramı.

YIG tabanlı PLL mimarisi, VCO tabanlı yapılardan farklı olarak akım kontrollüdür. YIG tabanlı PLL yapıları ile çok geniş band ve çok iyi faz gürültü başarımı elde edilebilir. Özellikle mikrodalga frekanslarında (>3GHz) geniş uygulama alanı bulmaktadırlar. Test ve laboratuvar cihazlarında yaygın olarak kullanılmaktadır. Çok fazla ısındığı için sıcaklık kontrolü ve mekanik titreşimlerden izole olması gerekmektedir (frekansın kaymaması için). YIG tabanlı PLL yapılarının en büyük zayıflıkları YIG'lerin pahalı olması, fazla yer kaplaması, iyi bir soğutucu ve sıcaklık kontrol devresi gerektirmesi ve de çok fazla güç tüketmesidir. Boyut, maliyet ve güç tüketimi nedeniyle genellikle test cihazlarında kullanılmakta, bunun dışında gerektiğinde başka uygulamalarda da kullanılmaktadırlar.

Hem 1Hz'den küçük çözünürlüklü, hem hızlı, hem çok iyi faz gürültüsüne sahip, boyut, maliyet ve güç tüketimi bakımından da uygun olabilecek umut veren bir mimari, DDS tabanlı sentezleyicilerdir. Var olan teknoloji ile en fazla 3GHz saat frekansına sahip DDS'ler teknoloji pazarında boy göstermektedirler. Böyle bir DDS çekirdeği ile teorik olarak



Şekil 2. DDS ana blok diyagramı.

en fazla 1.5GHz, pratik olarak da en fazla 1.2GHz çıkış frekansı elde edilebilmektedir. Daha yüksek çıkış frekanslarına ulaşmak ve daha geniş band elde etmek için kullanılacak olan karıştırıcı veya frekans çarpıcıları çok güzel olan faz gürültüsünü biraz kötüleştirirse de çok iyi bir faz gürültüsü elde etmek olasıdır.

Yazılım tabanlı telsiz projesi kapsamında DDS tabanlı 50MHz-3100MHz frekans aralığında geniş bantlı, Hz çözünürlüklü, 70ns hızında, iyi bir faz gürültüsüne sahip bir frekans sentezleyici (FSM3000A) gerçekleştirilmiştir. Bu sentezleyicinin detayları bir sonraki bölümde verilmiştir.

DDS Tabanlı Sentezleyiciler

DDS (Direct Digital Synthesizer) tabanlı sentezleyiciler, duyarlı ve yüksek frekanslı bir referans saat işaretinin, sayısal-analog çeviricilerden (DAC) geçirilmesi yöntemiyle analog dalga şekli üreten yapılardır. Bu analog dalga şekilleri çoğunlukla sinüs olmakla beraber, üçgen ya da kare dalga şekli de olabilir [3].

DDS tabanlı sentezleyicilerin ana üstünlükleri; çok düşük çözünürlüklü frekans üretebilmeleri (<1Hz), çok hızlı frekans ya da faz atlama yeteneklerinin olması ve de en önemlisi çok temiz faz gürültüsüne sahip oluşlarıdır [4]. En önemli zayıflıkları ise istenmeyen harmoniklerin (spurious) frekans bandında yer almasıdır. Bu istenmeyen harmoniklerin bastırılması, DDS tabanlı sentezleyici tasarımındaki en önemli ve en zor aşamadır. Ancak bu zayıflıklara karşı DDS tabanlı sentezleyiciler PLL tabanlı sentezleyicilerin yerini hızla almakta ve daha da popüler olmaktadır. DDS tabanlı sentezleyicilerin önüne açacak ve açmakta olan en önemli teknoloji ise ayarlanabilir süzgeç ('tunable filter') teknolojisidir.

Şekil 2'de DDS'in ana blok diyagramı gösterilmiştir. Çoğunlukla sayısal ortamda gerçekleşen işlemler bir sayısal-analog çeviricinin yardımıyla analog dünyaya açılmaktadır.

DDS tabanlı sentezleyicilerin performansını belirleyen bir diğer önemli unsur da saat frekansdır. DDS tabanlı sentezleyicilerin çıkış frekansını sınırlayan en önemli parametre saat frekansdır. Nyquist teorisi, DDS çıkış frekansının en fazla saat frekansının yarısı kadar ($f_{saat}/2$) olabileceğini söylemektedir. Ancak pratik kısıtlamalar (süzme)'dan dolayı DDS çıkış frekansı, saat frekansının %40'ı kadar olabilmektedir. DDS'in saat frekansı ne kadar yüksek olursa üreteceği en yüksek çıkış frekansı da o kadar yüksek olacaktır. DDS çıkış frekansı ile saat frekansı arasındaki ilişki aşağıdaki gibi verilebilir [5]:

$$f_{çıkış} = \left(\frac{M}{2^N} f_{saat}\right) \quad (1)$$

M, ikili (binary) frekans bilgisini, N ise DDS'deki faz birikcinin toplam bit uzunluğunu göstermektedir.

Verilen bir f_{saat} ve istenen bir $f_{çıkış}$ frekansında oluşacak başlıca hayal frekansları (image frequencies), aşağıdaki gibi olacaktır:

$$\begin{aligned} &f_{saat} - f_{çıkış} \text{ (1. Hayal)}, f_{saat} + f_{çıkış} \text{ (2. Hayal)}, \\ &2f_{saat} - f_{çıkış} \text{ (3. Hayal)}, 2f_{saat} + f_{çıkış} \text{ (4. Hayal)}, \\ &3f_{saat} - f_{çıkış} \text{ (5. Hayal)}, 3f_{saat} + f_{çıkış} \text{ (6. Hayal)}, \dots \end{aligned} \quad (2)$$

Bu istenmeyen işaretlerin frekansları belirli olduğu için uygun bir frekans planlaması ve süzerek kolaylıkla bastırılabilir.

Bir diğer istenmeyen frekans kaynağı olan faz kesme ('truncation') hatasının üreteceği istenmeyen harmoniklerin (süpür - spurious) frekans spektrumunun neresine düşeceği ise belirsizdir. Bu da DDS tabanlı sentezleyici tasarımının en büyük zorluklarından biridir. Bunun için şu ana kadar önerilen bir çözüm, çıkış frekansı ve saat frekansı arasında tam bölme oranını yakalamaktır [5]. Ancak, geniş bantlı bir sentezleyici tasarımında her frekans değerinde böyle bir tam bölme oranını yakalamakta çok kolay değildir. Bunun için çok iyi bir frekans planı ile tam bölme oranı ve tam bölme oranına yakın değerler hesaplanmalıdır. Örnek verilirse 32 bitlik ve maksimum 3GHz'lik saat frekansı olan bir DDS çekirdeğinde aşağıdaki tabloya benzer bir frekans planı çıkarılabilir.

Tablo 1. DDS Örnek Frekans Planı

#	min ≤ Fclk ≤ max (MHz)	min ≤ Fout ≤ max (MHz)	M/2 ^N
1	2800 ≤ Fclk ≤ 3200	87.5 ≤ Fout ≤ 100	1/32
2	2750 ≤ Fclk ≤ 3125	343.75 ≤ Fout ≤ 390.625	1/8

Tam bölme oranının sağlanmadığı değerler için tam bölme oranına yakın oranlar seçilebilir. Burada dikkat edilecek bir diğer konu da M frekans bilgisini oluşturan bitlerin 32-bit içindeki dağılımının yoğun ('kompakt') olmasıdır. Bu da DDS'in süpür performansını olumlu yönde etkileyecektir. Yani, 000100001000011000... gibi dağınık bir bit dağılımı yerine aynı değerde 00000000111100000000... şeklindeki yoğun bir dağılım tercih edilmelidir.

FSM3000A Frekans Sentezleyici

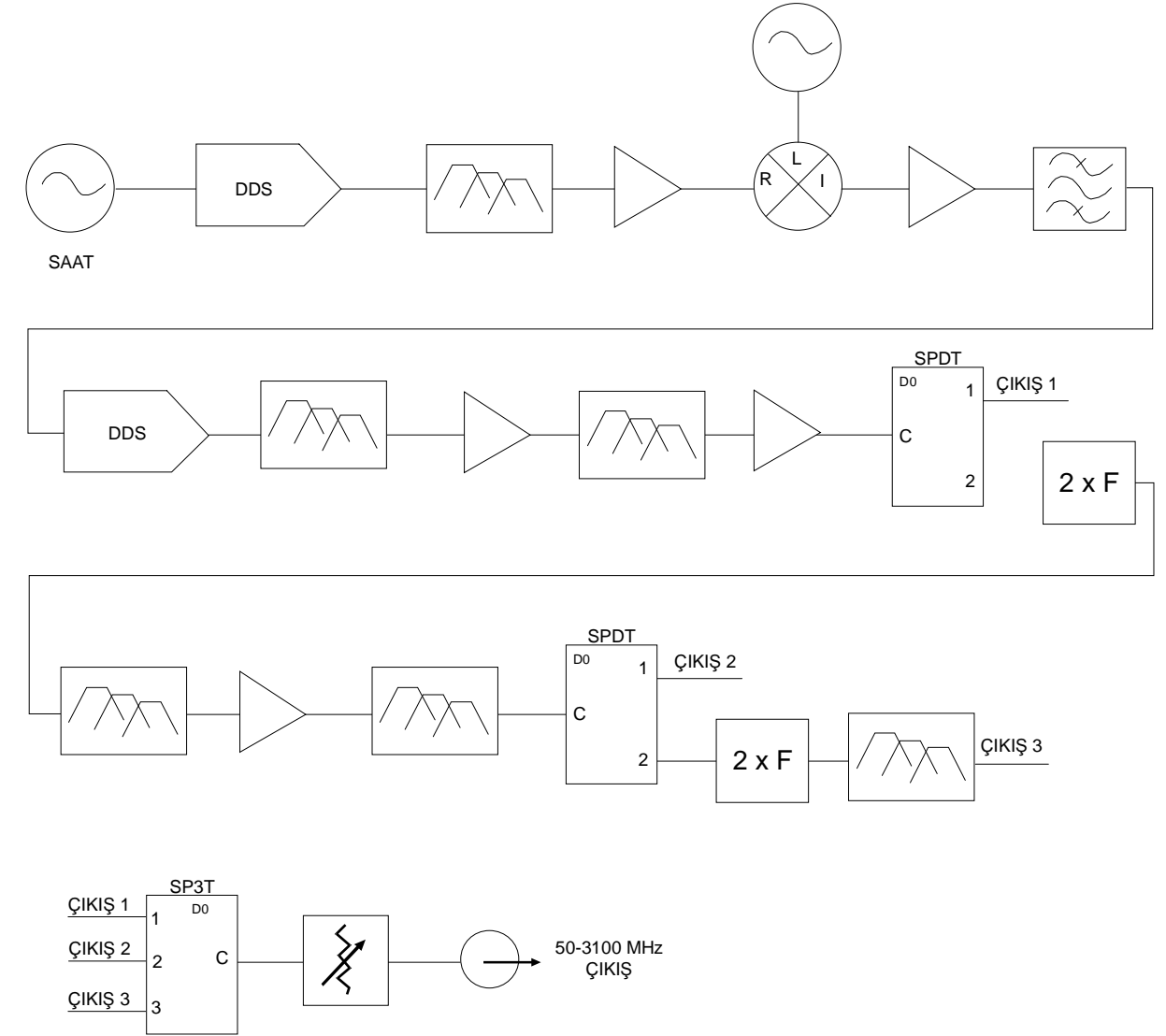
UEKAE'de, Şekil 3'de görülebilen, yazılım tabanlı telsiz (YTT) projesi kapsamında 50MHz – 3100MHz bandında 10Hz adımlarla tarayan DDS tabanlı milli bir sentezleyici gerçekleştirilmiştir (FSM3000A).



Şekil 3. FSM3000A frekans sentezleyici.

Gerçekleştirilen sentezleyici gerek çeşitli LO gereksinimlerini gerekse de işaret üretici gereksinimlerini karşılayabilecek düzeydedir. FSM3000A ve FYM3000A'yı süren bu sentezleyicinin genel blok diyagramı Şekil 4'de verilmiştir.

Bu blok diyagram üzerinde çeşitli iterasyonlar ile FSM3000A sentezleyicisinin son durumuna ulaşılmıştır. Blok diyagram FSM3000A'nın son şeklini tamamiyle yansıtmamakla birlikte genel fikir edinme açısından verilmiştir. Şekil 5'de frekans atlama hızını gösteren ölçüm sonucu verilmiştir. Ölçüm için 1230MHz ve 1795MHz arasında sürekli bir tarama yapılarak iki frekans arasındaki geçiş yüksek örnekleme hızına sahip bir osiloskop (Lecroy) ile yakalanmıştır. Ölçüm imleçleri (marker) geniş konularak elde edilen ölçüm sonucu 68.2040us'dir. Şekilden de görüldüğü gibi frekans atlama hızı aslında bu değerinden daha da altındadır. Yani FSM3000A, kabaca ölçülen 68.2040us'den daha hızlıdır.

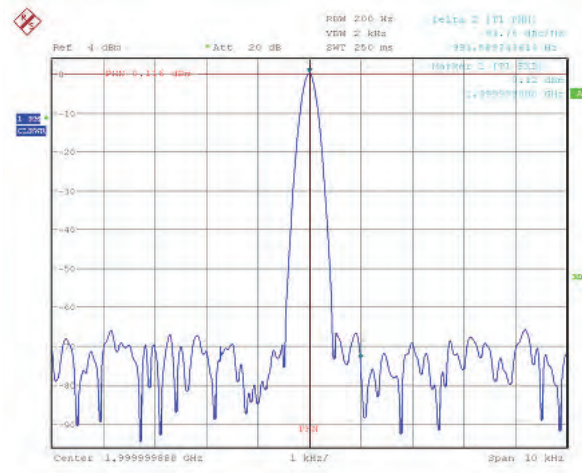


Şekil 4. FSM3000A genel blok diyagramı.

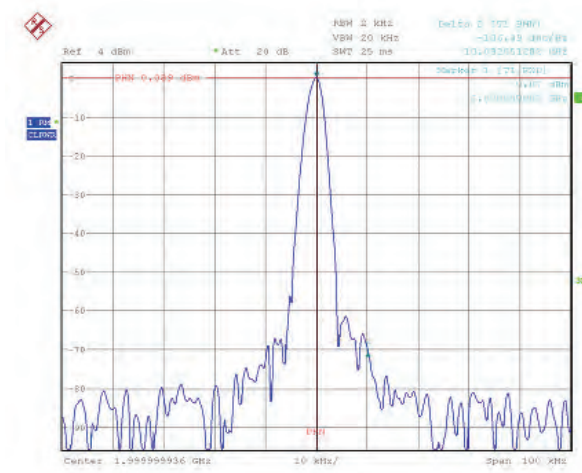


Şekil 5. FSM3000A'nın frekans atlama hızı.

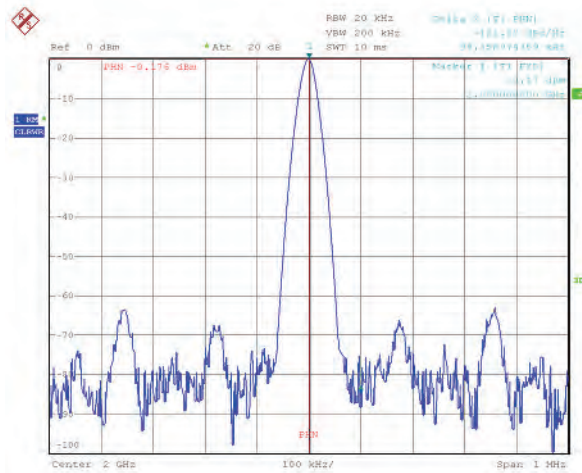
Şekil 6, 7 ve 8' de 2000MHz frekansında 1kHz, 10kHz ve 100kHz ofsetlerde alınmış faz gürültüsü ölçüm sonuçları gösterilmiştir. 1kHz ofsette ölçülen faz gürültüsü değeri, -93.75dBc/Hz; 10kHz ofsette ölçülen faz gürültüsü değeri, -106.49dBc/Hz; 100kHz ofsette ölçülen faz gürültüsü değeri, -121.82dBc/Hz'dir.



Şekil 6. FSM3000A için 2000MHz'de 1kHz ofsette alınmış faz gürültü ölçümü.



Şekil 8. FSM3000A için 2000MHz'de 100kHz ofsette alınmış faz gürültü ölçümü.



Şekil 7. FSM3000A için 2000MHz'de 10kHz ofsette alınmış faz gürültü ölçümü..

FSM3000A'nın tipik başarımlar değerleri Tablo 2'de özetlenmiştir. Verilen değerler FSM3000A'nın en kötü değerleri baz alınarak hazırlanmış olup çoğu frekans değerinde çok daha iyi başarımlara sahiptir.

Tablo 2. FSM3000A Teknik Özellikleri

Teknik Özellikler	FSM3000A
Frekans Bandı	50MHz – 3100MHz
Referans Giriş / Çıkış	10MHz (opsiyonel 20MHz)
Frekans Çözünürlüğü	<10Hz
Frekans Atlama Hızı	<70us
Harmonik Seviyesi	<-35dBc
Süpür (non-harmonic) Seviyesi	<-45dBc
Çıkış Gücü	0dBm ± 1.5dB
SSB Faz Gürültüsü	1kHz≤-90dBc/Hz 10kHz≤-100dBc/Hz 100kHz≤-115dBc/Hz
Kontrol Arayüzü	Ethernet (RJ-45) , RS-232 (DB-9)
Çalışma Sıcaklığı	-10°C to 70°C
Boyutlar	1U 19"
Ağırlık	7kg
Güç Tüketimi	90 - 260VAC giriş, 47~63Hz

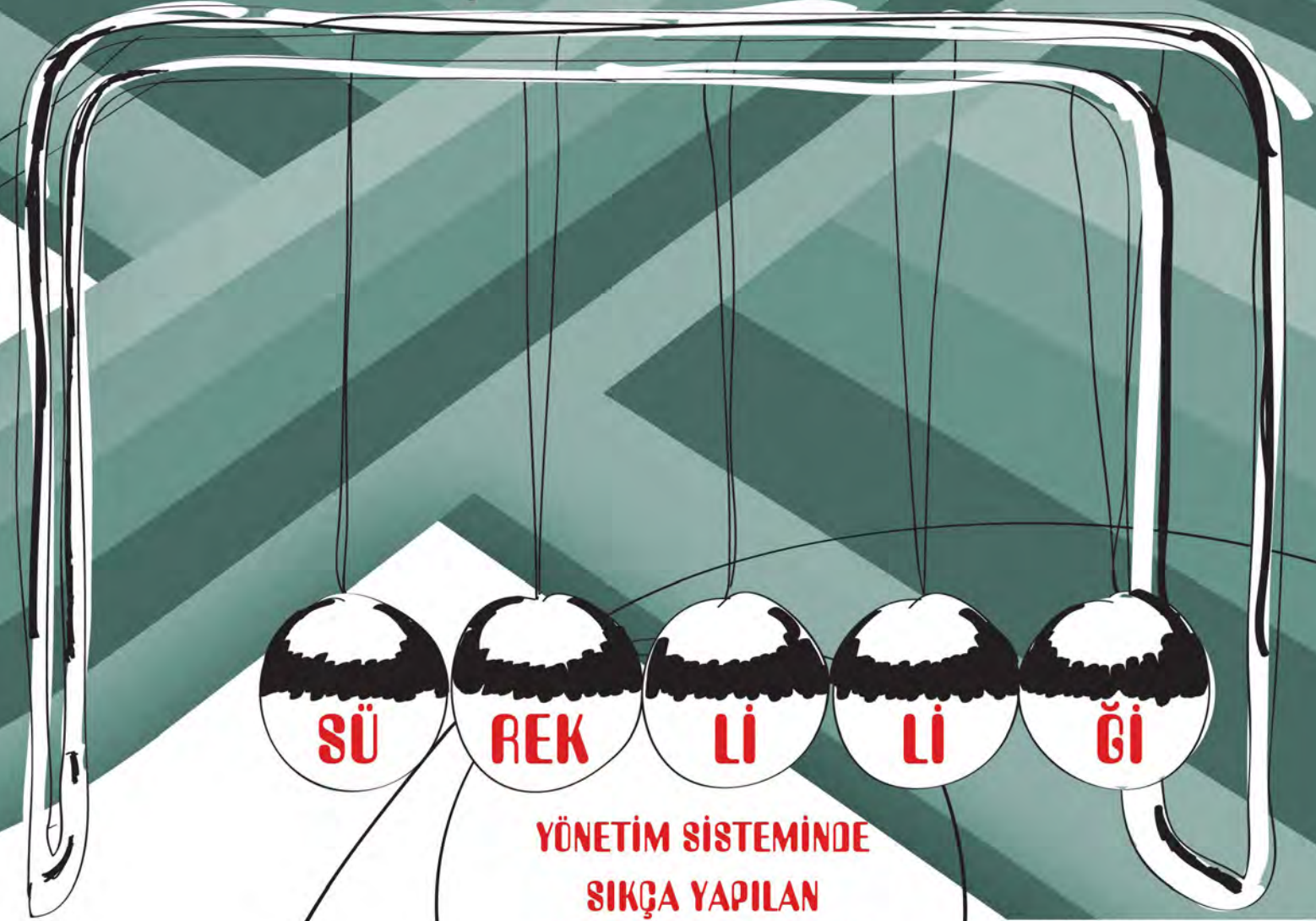
KAYNAKÇA

- [1] Alexander Chenakin, "Building a Microwave Frequency Synthesizer-Part 4: Improving the Performance," High Frequency Electronics, August 2008.
- [2] Alexander Chenakin, "Frequency Synthesis: Current Solutions and New Trends," Microwave Journal, May 2007.
- [3] Eva Murphy, Colm Slattery, "Direct Digital Synthesis (DDS) Controls Waveforms in Test, Measurement, and Communications", Analog Dialogue 39-08, August 2005 (www.analog.com/analogdialogue)
- [4] Analog Devices, "A Technical Tutorial on Digital Signal Synthesis", 1999, Analog Devices Corp.
- [5] Canadian Intellectual Property Office, Patent number: CA2491119, "Wideband Signal Generators, Measurement Devices, Methods of Signal Generation and Method of Signal Analysis", Mercury Computer Systems Inc.

BİLİŞİM GÜVENLİĞİ SİSTEMLERİ



İŞ



SÜ

REK

Lİ

Lİ

Ğİ

**YÖNETİM SİSTEMİNDE
SIKÇA YAPILAN
YANLIŞLAR VE ÖNEMLİ
BAŞARI ETKENLERİ**

Ali DİNÇKAN
Ömer Deniz DEMİREL

İş sürekliliği, bir kurumun önemli iş süreçlerinin devamlılığını sağlamak, sağlanamadığı durumlarda kabul edilebilir kesinti süreleri içerisinde, süreçleri tekrar çalıştırmak için gerçekleştirilen çalışmalar olarak tanımlanır. Son yıllarda yaşanan acı tecrübeler ve bu konuda gerçekleştirilen bilinçlendirme çalışmaları sonucunda, ülkemizde iş sürekliliği farkındalığı artmıştır. 2006 yılında İngiliz Standartları Enstitüsü'nün yayınlamış olduğu BS25999 standardı ile birlikte, gerçekleştirilen çalışmaların sayısı da artış göstermiştir. Bu bildirinin amacı, iş sürekliliği konusundaki yanlış yaklaşımları ortaya koymak ve iş sürekliliği çalışmalarının başarıya ulaşabilmesi için üzerinde önemle durulması gereken önemli başarı etkenlerini tanıtmaktır.

Giriş

İş sürekliliği, kurumun önemli süreçlerinin belirlenmesi, bu süreçlerin sürekliliği için çalışmaların gerçekleştirilmesi, sürekliliğin sağlanamadığı durumlarda, kabul edilebilir kesinti süreleri içerisinde tekrar çalışır hale getirilmesi için, gerçekleştirilecek tüm çalışmalara verilen genel isimdir.

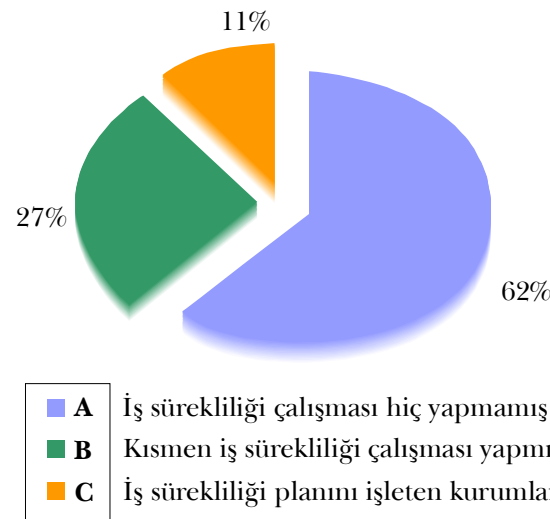
İşletmenin iş süreçlerinin ne kadar kesintiye dayanabildiği ve süreçleri bu süre içerisinde tekrar çalışır hale getirmek için neler yapılması gerektiği, iş sürekliliği çalışmalarının temelini oluşturmaktadır. İş Sürekliliği Yönetim Sistemi (İSYS) gerekliliklerini anlatan BS25999-2:2007 standardı, iş sürekliliğini: “İş süreçlerinin önceden tanımlanmış, kabul edilebilir bir düzeyde sürekliliğini/devamını sağlamak amacıyla, kuruluşun, olaylara ve iş kesintilerine karşı planlama ve müdahale etme konusundaki stratejik ve taktik kapasitesidir.” biçiminde tanımlamaktadır [1]. Bu ifade ile kastedilen; iş süreçlerinin zaman içerisinde kesintiye uğramasının kaçınılmaz olduğu, kurumun bu duruma hazırlıklı olması için kabul edebileceği kesinti sürelerini belirlemesi ve bu süre içerisinde süreci tekrar işler hale getirmek için, yapılması gerekenleri planlayarak hazırlıklı olması gerektiğidir.

İş Sürekliliğinin Önemi ve Ülkemizdeki Durum

Son yıllarda, bilgi güvenliği bilincinin artması ve finans sektörüne getirilen düzenlemeler ile birlikte, iş sürekliliğine verilen önemin arttığını görmekteyiz. Bu gelişmelere paralel olarak, 2006 yılında İngiliz Standartları Enstitüsü'nün, BS25999 İş Sürekliliği Yönetim Sistemi (İSYS) standardını yayınlamış olması, iş sürekliliğinin dünya genelinde de öneminin arttığını göstermektedir.

Günümüz işletmeleri, genellikle iş süreçlerindeki kesintileri engellemek, rekabet avantajı sağlamak, yasal yükümlülüklerini yerine getirmek, müşteri

kayıplarını engellemek, kurum itibarını korumak ve pazar payı kayıplarını azaltmak için, iş sürekliliği ile ilgilenmektedir. İşletmeler, genellikle iki nedenden dolayı iş sürekliliğine önem vermektedir. Bunlardan ilki, kurumun bu çalışmayı yasal yükümlülüklerini yerine getirmek için yapması, diğeri ise hizmet kesintisi nedeni ile zarara uğramasıdır. Bir iş sürecinin önemi, genellikle sürecin çalışmaz duruma gelmesi ile anlaşılmaktadır. Bu nedenle yapılan işin önemini önceden bilerek iş sürekliliği çalışmalarının başlatılması, maalesef sık karşılaşılan bir durum değildir. Kurumların herhangi bir kesinti yaşamadan ve zarara uğramadan bu çalışmaya başlamalarını sağlamak için, çok sayıda araştırma yapılmıştır. Bu araştırmalardan bir tanesi, çok önemli bir sonucu ortaya koymuştur. Gartner tarafından yapılmış olan bu araştırmada, felaket veya çok büyük kesintiye neden olan bir olay yaşamış olan firmaların yüzde 43'nün bir daha faaliyete geçemediği, yüzde 29'unun ise iki yıl içinde çalışmalarını noktalamak zorunda kaldıkları açıklanmıştır [2]. 2006 yılında ABD'de ve Kanada'da bulunan 261 orta ve büyük ölçekli kurum üzerinde yapılan bir araştırma sonucuna göre, kurumların %52'si iş sürekliliği planına sahiptir. Bu kurumlardan %26'sı, iş sürekliliği planını kurum çapında yaygınlaştıramamış veya güncelleyememiştir. Dolayısıyla kurumların sadece %39'u planı uygun biçimde işletmektedir [3].



Şekil 1. Kamu kurumları iş sürekliliği planlaması durum analizi, 2005 TÜBİTAK UEKAE.

Ülkemizde ise, 2005 yılında e-Dönüşüm Türkiye Projesi kapsamında, TÜBİTAK-UEKAE'ye kamu kurumlarının acil durum yönetimi konusundaki durumu ve gereksinimleri belirleyerek, çözüm önerilerini hazırlaması görevi verilmiştir. Bu çalışma kapsamında, 37 kamu kurumu ile birlikte çalışılarak durum değerlendirme yapılmıştır. Araştırmanın sonucuna göre, kamu kurumlarının sadece %11'inin iş sürekliliği planını işlettiği görülmüştür. [4]

Araştırmanın diğer bulguları aşağıdaki gibidir;

1. Kurumların %16'sında, kapsamda bilgi sistemleri bulunan ve dokümanite edilmiş bir iş sürekliliği planı olduğu tespit edilmiştir. İş sürekliliği planı bulunan kurumların yaklaşık yarısı, planı yaşam döngüsü çerçevesinde işletmemektedir. Belirli bir yaşam döngüsü çerçevesinde işletilmeyen iş sürekliliği planlarının, acil durumlarda çalıştırılması mümkün değildir.

2. Kurumların bazılarında, iş sürekliliği planlaması kapsamında yapılması gereken çalışmaların kısmi olarak yapıldığı, fakat bu işlemlerin iş sürekliliği planlamasına döndürülmediği tespit edilmiştir. Bu anlamda kurumların %19'unun önemli iş süreçlerini tanımladığı ve önceliklendirdiği, %14'ünün ise kesintilerin iş süreçleri üzerine olan etkilerini belirlediği görülmüştür.

3. İş sürekliliği planlaması yapan kamu kurumlarında, iş kesintileri durumunda uygulanacak detaylı kurtarma ve geri döndürme prosedürleri olduğu görülmektedir. Bu prosedürlere sahip olan kamu kurumlarının oranı %16'dır.

4. İş sürekliliği planlaması kapsamında, acil durumlarda nasıl hareket edileceğinin tanımlanması gereklidir. Kamu kurumlarının %19'unun, acil durum prosedürü olduğu anlaşılmaktadır.

5. Anket değerlendirmesi sonucunda, kamu kurumlarının %11'inde, kurum çapında bilinen bir acil durum operasyon merkezi (kriz masası) olduğu anlaşılmaktadır.

6. İş sürekliliği planlaması yapmış olan kamu kurumlarının, yaklaşık yarısının planın test, güncelleme ve eğitim çalışması yapmadığı tespit edilmiştir. Güncel olmayan, belirli aralıklarla test edilmeyen ve eğitimi verilmeyen iş sürekliliği planlarının, acil durumlarda istenilen yararı sağlaması mümkün değildir.

İş Sürekliliği Yönetim Sistemi Kurulumu

İş sürekliliği yönetimi konusunda yayımlanan ilk standart, 2006 yılında BS 25999-1:2006 “İş Sürekliliği Yönetimi İçin Uygulama Esasları” ismi ile, İngiliz Standartları Enstitüsü (BSI) tarafından yayımlanmıştır. 2007 yılında ise, bu standarda göre İSYS kuran kurumların denetimi için, standardın ikinci parçası BS25999-2 yayımlanmıştır. Bildirinin amacı, iş sürekliliği konusundaki hatalı yaklaşımları ve İSYS kurulumundaki önemli başarı etkenlerini açıklamak olduğundan, İSYS kurulumu için ayrıntılı bilgi verilmemektedir. Bu konuda ayrıntılı bilgi için, ilgili BS 25999 standartlarına başvurulmalıdır. İSYS kurulumu konusunda kullanılabilecek bir diğer yardımcı kaynak: Ulusal Bilgi Güvenliği Kapısında (www.bilgiguvencigi.gov.tr) yayımlanan “İş Sürekliliği Yönetim Sistemi Kurulumu” isimli kılavuzdur. Bu kılavuz, İSYS için kurulum adımlarını tanımlamakta ve açıklamaktadır.

İş Sürekliliğinde Yanlış Yaklaşımlar

İş sürekliliği konusundaki hatalı yaklaşımları 4 ana başlık altında toplamak mümkündür.

1. İş Sürekliliğinin Bir Ürün, Teknoloji Veya Hizmet Olarak Görülmesi

İş sürekliliği, sadece verilerin başka bir çalışma alanına çevrim içi aktarılması veya önemli sunucuların devamlı olarak çalışmasını sağlamak üzere kümeleme (cluster), diskleri hata toleranslı hale getirme (RAID), yedekli güç kaynağı ve yedekli ağ hatlarını kullanmak olduğu düşünülmemelidir. İş sürekliliği kurum süreçlerinden hareketle, süreçlerin devamlılık gereksinimlerinin ortaya konulması ve bunun sağlanması için gereken çalışmaların yapılmasıdır. Bu çalışmalar sırasında elbette, teknoloji, insan gücü ve mali kaynaklar kullanılacaktır.

Bu çalışmayı sadece bir ürün veya hizmet olarak görmek, olağanüstü bir durumda iş süreçlerinin tekrar çalışır hale getirilmesi için yeterli değildir. İş sürekliliği, süreçlerin devamlılığı ve devamlılığın sağlanamadığı durumda, ön görülen kesinti ile çalıştırılmasını kapsamaktadır. Süreçlerin çalışabilmesi için bilgi teknolojilerine gereksinimi olabileceği gibi, aynı zamanda süreci işleten son kullanıcıya ve dokümantasyona da gereksinimi vardır.

2. Başlangıcı ve Sonu Belirli Olan Bir Proje Olarak Düşünülmesi

İSYS kurulumu, yeterli bilgi birikimi olduğu durumda, işletmenin kendi kaynakları ile yapabileceği bir çalışmadır. Birçok işletmede, söz konusu bilgi birikiminin olmaması nedeni ile, bu konuda dış kaynak kullanımı yoluna gidilmektedir. Bu çalışmalar genellikle bir proje olarak değerlendirildiği için, İSYS'ye de proje gözüyle bakma yanlışlığı söz konusudur. İSYS'ye bir proje olarak yaklaşmak, başlangıcı ve sonu belirli olan bir iş olarak ele almak anlamına gelmektedir. İş sürekliliği yönetim sisteminin kurulması ve çalışır hale getirilmesi, bir proje olarak ele alınabilmesine rağmen, İSYS'nin kendisi bir proje değildir. İSYS çalışır hale geldikten sonra, yönetim sisteminin yaşatılabilmesi için yapılması gereken çalışmalar vardır. Bu çalışmalar, BS25999-1 standardının iş sürekliliği program yönetimi başlığı altında ayrıntılı olarak tanımlanmıştır. Söz konusu çalışmalar gerçekleştirilirken, işletmenin yönetim sisteminin işletilebilmesi ve sürekli geliştirilebilmesi için, gerekli bilgi birikimini edinmesi gereklidir.

3. Sadece Dokümantasyondan Oluşturduğu Varsayımı

Bir diğer yanlış yaklaşım ise, iş sürekliliğine sadece dokümantasyondan oluşturduğu varsayımı ile yaklaşmaktır. Dokümantasyon, iş sürekliliğinin vazgeçilemez bir parçası olmasına rağmen, yapılması gereken tüm işleri dokümantasyon olarak ele almak, çalışmanın teknolojik ve organizasyon boyutlarını gözden kaçırmaya, dolayısıyla iş sürekliliğinden beklenen yararın sağlanamamasına neden olur. Teknolojik altyapının, gereksinimlerin üzerinde olması durumunda bile tatbikatların yapılması, eğitimlerin verilmesi ve belirli aralıklarla gözden geçirmeler vb. yapılması gereken çalışmalar vardır.

4. İş Sürekliliği Sorumluluğunun BT Bölümünde Olduğunun Düşünülmesi

İş sürekliliğinin sağlanmasında, bilgi teknolojilerinin (BT) rolünün yüksek olmasından dolayı, çalışmaların BT bölümü tarafından yapılması ve sorumluluğunun da BT bölümünde olması gerektiği inancı yaygındır. İstatistikler, iş sürekliliği çalışmalarına BT bölümünün katılımının diğer birimlerden daha fazla olduğunu göstermektedir. Öbür yandan iş sürekliliğinin sorumluluğunun, çok yüksek oranda üst yönetim, yönetim kurulu veya iş sürekliliği kurulunda olduğu

görülmektedir. İş süreçlerinin devam ettirilebilmesi veya olağan üstü bir durumda tekrar çalışır hale getirilmesi, personelin alternatif çalışma ortamına naklinden, sunucuların hazırlanmasına ve yeni cihaz satın alınmasına kadar birçok çalışmayı içermektedir. Bu nedenle iş sürekliliği, kurum içinde mümkün olduğu kadar üst seviye yönetim tarafından temsil edilmeli ve tüm çalışma grupları ile birlikte çalışarak, iş sürekliliğini sağlayacak bir ekip kurulmalıdır.

İş Sürekliliği Önemli Başarı Etkenleri

Bu bölümde, İSYS'nin başarıya ulaşabilmesi için önem verilmesi gereken başarı etkenleri açıklanmıştır. Bu maddelerden bir veya birkaçında sorun olması durumunda iş sürekliliği çalışmalarından beklenen yararın sağlanamaması söz konusudur.

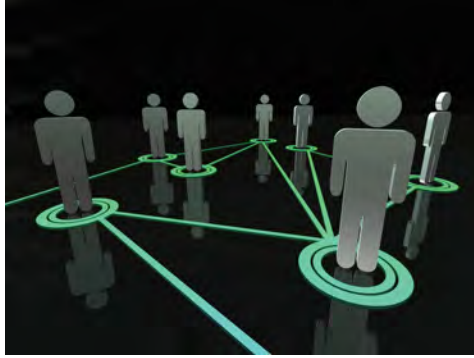
1. Üst Yönetim Desteği



İş sürekliliği çalışmaları için, en yüksek seviyede yönetim onayı ve desteğinin alınması zorunludur. Gerçekleştirilen çalışmalar ile ilgili yönetim onayı alınması, çalışmaların kurum çapında daha kolay kabul edilmesini sağlayacaktır. BS 25999 standardı, üst yönetimin iş sürekliliği sürecine katılımının İSYS'nin doğru olarak anlaşılması, desteklenmesi ve organizasyon kültürüne uyumu için anahtar bir adım olduğunu belirtmektedir. Üst yönetim desteği, sadece politika ve benzeri dokümantasyonun onaylanması biçiminde olmamalıdır. Çalışmaların gözden geçirildiği toplantılara katılımın

sağlanması, tatbikat sonuçlarının incelenmesi, bazı bilgilendirme notlarının veya çalışma sonuçlarının bizzat yönetim tarafından bildirilmesi, konunun öneminin anlaşılması açısından yararlı olacaktır. Üst yönetim desteği, ayrıca gerekli iş gücünün ve gereksinim duyulan bütçenin ayrılması gibi konular içinde oldukça önemlidir.

2. Stratejik İş Planın Parçası Olma



İş sürekliliği, kurumun stratejik hedefleri için önemli bir çalışmadır. Kurumun işlevini devam ettirmesi veya yasal yükümlülüklerini yerine getirebilmesi için, her zaman güncel ve ihtiyaca yanıt verebilir durumda olmalıdır. İş sürekliliğinin stratejik iş hedeflerine uygun olarak geliştirilmediği veya stratejik hedeflerde gerçekleştirilen değişikliklere uygun olarak gerekli çalışmalar yapılmadığı durumda, iş süreçlerinde kesintiler yaşanması kaçınılmazdır. Örnek olarak bir yıl sonrasında satışlarını %30 arttırmayı hedefleyen bir firma düşünelim. Bu hedefi gerçekleştirmek için, bilgi teknolojileri altyapısında da gerekli değişiklikler yapılacaktır. Bu değişiklikler sırasında iş sürekliliği planının, ilgili dokümantasyonunun ve kurtarma merkezinin bu hedefe uygun olarak değiştirilmesi gereklidir.

3. İş Sürekliliği Organizasyonu

İş sürekliliği çalışmaları, bir grubun veya bir kişinin tek başına yerine getirebileceği bir faaliyet değildir. Kurumun birçok bölümünün içinde bulunduğu ve kişilerin farklı görevler aldığı bir çalışmadır. Son kullanıcının dahi bilmesi ve yapması gereken işler vardır. Bazı kurumlarda iş sürekliliğinin yönetimi için ayrı gruplar



kurulmuştur. İş sürekliliği yönetim sisteminin kurum içinde yaşayabilmesi için gerekli personel gücünün ve eş güdümün sağlanması iş sürekliliğinin olağanüstü durumlarda beklenen yararı sağlaması için önemli adımlardan birisidir. İş sürekliliği çalışmaları kapsamında en üst yönetimden son kullanıcıya kadar düşen görevler vardır. Bu detayda bir kurum kültürü oluşturulmadıkça sürecin işletilmesi zordur.

4. Risk Analizi ve İş Etki Analizi

İş sürekliliği, iş etki analizi ismi verilen çalışmanın çıktuları üzerine inşa edildiği için, en önemli başarı etkenlerinden biridir. İş etki analizinin doğru yapılması, İSYS'nin sağlam temeller üzerine oturmasını sağlayacaktır. Bu sebeple kurumun ilgili bölümlerinden yetkin kişilerin, çalışmalarda yer alması gereklidir. İş etki analizi / risk analizi takımında yer alacak personelin üst yönetim tarafından seçilmesi, yönetimin konuya verdiği önemin anlaşılması açısından son derece önemlidir. Bu çalışma sonunda kurum süreçlerinin kritikliği, süreçler için hedeflenen kurtarma süreleri (RTO) ve



en fazla kabul edilebilir kesinti süreleri (MTPoD) belirlenmektedir. Bu çalışma sırasında risk analizi de kullanılarak, süreçlerde kesintiye neden olabilecek riskler belirlenmektedir. İş süreçlerinin önemini ve süreçlerde kesintiye neden olabilecek olayların belirlenmesi, uygulanacak karşı önlemlerin seçilmesi için son derece önemlidir. İş etki analizi ve risk analizi çalışmasının doğru yapılması, iş sürekliliğinin başarıya ulaşmasında, üst yönetim desteği kadar önemli bir başarı nedenidir.

5. Yeterli Bütçe Ayrılması



İSYS'nin, hem kurulumu hem de daha sonra işletimi sırasında bir takım giderleri vardır. Kurulması sırasında danışmanlık, eğitim ve benzeri hizmetlerin satın alınması, işletme içinde gerekli insan kaynağının sağlanması bu giderlere örnektir. Yönetim sisteminin kurulumu sonrasında ise, gerçekleştirilecek tatbikatlar, periyodik gözden geçirmeler, kurum içi bilgilendirme faaliyetleri, süreçlerdeki değişikliklerden sonra hazırlanacak dokümanlar ve benzeri çalışmalar vardır. Ayrıca iş etki analizi ve risk analizi çalışmalarının sonunda uygulanacak kontrollere karar verilmeye başlanacak çalışmaların yapılması da gerekebilir. Bu sebeple iş etki analizinde belirlenen kabul edilebilir kesinti sürelerinin sağlanması için gerekli bütçenin ayrılması veya planlanması oldukça önemlidir.

6. Yeterli Bilgi Teknolojileri Altyapısı



Günümüzün iş gereklilikleri nedeniyle, birçok iş sürecinin BT bağımlılığı yüksektir. Bilgi teknolojileri altyapısının süreklilik ihtiyaçlarına uygun olması, süreklilik ihtiyaçlarının karşılanması için büyük öneme sahiptir. Sunucuların, haberleşme hatlarının ve enerji altyapısının yedekli yapıda çalışması, BT'nin sürekli hizmet verebilmesi için gereklidir. Bunlara ek olarak, ana merkezde bulunan verinin kurtarma merkezine gönderilmesi gereklidir. Bu işlemleri gerçekleştirecek altyapıya sahip olmadan, olağanüstü bir durumda kabul edilebilir kesinti sürelerini sağlamak oldukça güçtür.

7. Dokümantasyon



Her yönetim sisteminde olduğu gibi İSYS içinde dokümantasyon çok önemlidir. İş sürekliliği planının, olağanüstü durum yönetim planının ve bu planlarla ilgili diğer talimat ve prosedürlerin hazır ve güncel olması gereklidir. Dokümanların hazır olması yanında, ilgili kişilere dağıtımı da yapılmalıdır. Dokümantasyonun hazırlanması aşamasında sadelik ve kolay uygulanabilirlik çok önemlidir.

8. Periyodik Tatbikatlar



Olağanüstü durumlara her an hazır olabilmek için, senaryolar üretilmeli ve tatbikatı yapılmalıdır. Tatbikatlar sonucunda, kurulmuş olan yönetim sisteminin eksikliklerini belirlemek mümkündür. İş sürekliliği planının ve ilgili diğer dokümanların, çalışma kapsamında görev alan personelin bilgi seviyesinin ve teknolojik altyapının eksiklikleri bu şekilde belirlenebilir. Tatbikatlar, dokümantasyonun gözden geçirilmesi, planın bir parçasının test edilmesi veya planın tamamının test edilmesi gibi farklı türlerde sahiptir. Her bir tatbikat türü için, senelik olarak tatbikat planlarının hazırlanması ve tatbikatların yapılması, kurumun olası bir acil durum senaryosu için hazır olmasını sağlamaktadır.

9. Eğitim ve Bilinçlendirme



İş sürekliliği çalışmalarının benimsenmesi için, kurum çalışanlarına ve iş sürekliliği organizasyonunda bulunan takımlara eğitim verilmelidir. Kurum çapında benimsenmemiş ve gerekli eğitim çalışmaları yapılmamış iş sürekliliği

planlarının, başarıya ulaşma olasılığı düşüktür. İş sürekliliği planı içerisinde, eğitim konusunda izlenecek yöntemler (anket, sınıf eğitimi, sınav vb.) belirlenmeli ve plan içerisinde yer almalıdır. Eğitim faaliyetlerini yürütmek üzere bir takım kurulması ve gereken zamanlarda eğitim işlerini organize etmesi yararlı olacaktır. Kurum içinde yapılacak iş sürekliliği bilgilendirmesi senede bir defadan az olmamalıdır.

10. Plan Bakım ve Güncelleme



İSYS, kurumun önemli süreçlerinin devamlılığını sağlamak için vardır. Bu nedenle kurumun süreçlerinde meydana gelen değişiklikler, iş sürekliliği planını doğrudan etkilemektedir. Süreç değişikliklerinin plan güncellemesi gerektirdiği, hiçbir zaman göz ardı edilmemelidir. Zaman içerisinde meydana gelen değişikliklerin, iş sürekliliği planına aktarılması için, periyodik gözden geçirmeler yapılmalı ve güncelleme gereksinimi belirlenmelidir. İş sürekliliği tabikatları, genellikle planın güncellenmesini gerektirmektedir. İş sürekliliği kapsamında yapılması gereken değişiklikler, her zaman doküman değişiklikleri olmak zorunda değildir. Kurumun süreçlerinin önem seviyesinin değişmesi nedeniyle, hizmet veren sunucuların öncelikleri, dolayısıyla da alınması gereken önlemler değişebilir. Bu nedenle, bazı durumlarda yeni yatırım gereksinimi ortaya çıkabilir. Sistem değişikliği olması durumunda, bütçe ve zaman planının hazırlanması gerekir.

Sonuç

Bu bildiriye, iş sürekliliği yönetim sistemi kurulumu sırasında yaşanan sıkıntılar ve yönetim sisteminin başarıya ulaşabilmesi için önemli başarı etkenleri tanıtılmıştır. Bu amaçla ilk olarak iş sürekliliğinin kısa bir tanımı yapılmış, daha sonra iş sürekliliğinin önemi ve ülkemizdeki durumu hakkında değerlendirmeler verilmiştir. Değerlendirmelerin ardından geçmişte yapılan projelerde görülen hatalı yaklaşımlar açıklanmıştır. İSYS kurmayı planlayan işletmelerin söz konusu hatalı yaklaşımları tekrarlamaması, kuracakları yönetim sisteminin başarıya ulaşabilmesi için son derece önemlidir. Son olarak, yönetim sistemi kurulumu sırasında dikkat edilmesi gereken konular, önemli başarı etkenleri başlığı altında sunulmuştur. Önemli başarı etkenleri, İSYS kurmayı planlayan işletmelere kurulum sırasında önemle üzerinde durulması gereken alanları işaret etmektedir.

KAYNAKÇA

- [1] BS 25999-2:2007 A Specification for BCM.
- [2] Roberta Witty, Donna Scott, Disaster Recovery Plans and Systems Are Essential, 12 Eylül 2001, Gartner.
- [3] Brenda Rood, Disaster Planning, the International Foundation of Employee Benefits Plans, 2006.
- [4] Ali Dinçkan, BGYS-0009 İş Sürekliliği Yönetim Sistemi Kurulumu, Ulusal Bilgi Güvenliği Kapısı, <http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0009-is-surekliligi-yonetim-sistemi-kurulum-kilavuzu/download.html>.
- [5] Patrick Woodman, "Business Continuity Management", Chartered Management Institute, 2007.



E-İMZA

TÜRKİYE'DE KAMU KURUMLARINDA UYGULANMASI

Türksel Kaya Benschir

Ferda Topcan

ÇIKTI

E-İmza: Türkiye'de Kamu Kurumlarında Uygulanması, TODAİE Yayın no: 356, eDevlet Merkezi Yayın no: 2, Ankara, 2010, XIII+228 s.

e-Devlet yolunda güven ve güvenliğin tesis edilmesi akılcıca yönetilmesi gereken kritik bir süreçtir. Bu sürecin önemli unsurlarından biri e-imza alt yapısının kurumlarda yürütülen uygulama yazılımlarıyla entegrasyonunun sağlanmasıdır. Kamuda karar vericilerin ve uygulayıcıların çok boyutlu olan e-imzanın başta teknik olmak üzere hukuki ve yönetsel yönlerine ilişkin bilgi sahibi olmaları beklenmektedir.

Bu kitap, başta kamu çalışanları olmak üzere; konuyla ilgili araştırmacı, uzman ve diğer ilgililerin hakkında bilgi açığını gidermeyi amaçlamak üzere kaleme alınmıştır.

Kitapta, ülkemizde kamu kurum ve kuruluşlarının e-imza uygulama profili ve yaygınlığı, uygulama sonuçları (getirileri, riskler ve olumsuzluklar), e-imza arşiv yönetimi ve mobil imza kullanımının yaygınlığının ortaya çıkarılması amacıyla gerçekleştirilen alan araştırması sonuçlarına da yer verilmiştir.

Doç. Dr. Türksel KAYA BENSGHİR

tkaya@todaie.gov.tr

Doç. Dr. Türksel Kaya Benschir Türkiye ve Orta Doğu Amme İdaresi Enstitüsü'nde öğretim üyesidir. Haziran 2009'da TODAİE bünyesinde kurulan e-Devlet Merkezi'nde (eDEM) müdürlük görevini yürütmektedir.

Yönetim Bilişim Sistemleri alanında doçent olan Kaya Benschir, TODAİE ve çeşitli üniversitelerde başta yönetim bilişim sistemleri ve e-Devlet olmak üzere, BT ve örgütsel değişim, sistem analizi, bilgi sistemleri tasarımı, e-iş ve e-ticaret konularında dersler ve kamu personeline e-devlet, bilgi yönetimi, e-imza vb. konularda seminerler vermektedir.

Kaya Benschir'in, Bilgi Teknolojileri ve Örgütsel Değişim başlıklı kitabı ve ortak yazarlığı (A. Akay) Yerel Yönetimlerde Coğrafi Bilgi Sistemleri-Türkiye Uygulamaları kitabı ile yurt içi ve yurt dışında basılan editörlü kitaplarda yayınlanan çalışmalar bulunmaktadır. Ayrıca, yönetim bilişim sistemleri, e-imza, kamu görevlilerinin yetiştirilmesinde BT eğitimi, halkla ilişkiler ve web teknolojileri ve belediye web sitelerinin değerlendirilmesi, e-yerel yönetimler, belediyelerde CBS kullanımı, internet kafeler, kamu yöneticilerin ve vatandaşların e-devletten beklentileri gibi konularda çeşitli araştırmaları, ulusal ve uluslararası toplantılarda sunulan bildirileri ve yurt içi ve yurt dışında yayınlanmış makaleleri ve sunumları bulunmaktadır.

Ferda TOPCAN

ferdat@uekae.tubitak.gov.tr

1994 yılında Ankara ODTÜ Elektrik Elektronik Mühendisliği Bölümü'nden mezun oldu. 1998'de aynı bölümde yüksek lisansını tamamladı. TÜRK TELEKOM TÜRKİYE'de 4 yıla yakın bir süre TÜRKİYE uyduları yer kontrol istasyonu bakım-onarım mühendisi olarak çalıştıktan sonra 1998 yılında TÜBİTAK BİLTEN (UZAY)'de uzman araştırmacı olarak göreve başladı. Burada açık anahtarlı altyapılar (PKI) ve e-imza konusunda AR-GE çalışmaları yaptı.

Topcan 2004 yılında geçiş yaptığı TÜBİTAK UEKAE'de e-imza konusunda başuzman araştırmacı olarak görev yapmaktadır. UEKAE'de, kamu kurumları ile görüşmeler yaparak e-imzaya geçişte kurumların yönlendirilmesi, gerekli teknik desteğin sağlanması, e-imza uygulamalarının Türkiye'deki mevzuatta belirtilen uluslararası standartlara uygunluğunun kontrol edilmesi gibi görevlerin yürütülmesinden sorumludur. Başta TODAİE olmak üzere e-imza konusunda kurumlarda sunumlar yapmaktadır.



ELEKTRONİK İMZA

ELEKTRONİK İMZA STANDARTLARI VE İLGİLİ MEVZUAT

Dizimizin beşinci yazısında e-İmza ile ilgili teknik standartlar ve hukuki mevzuat hakkında bilgi vereceğiz. E-İmza ile ilgili standartların ve mevzuatın ulusal ve uluslararası boyutta tarihsel gelişimini ve geleceğine dair öngörülerini de yazımızda ele alacağız.

ERSİN GÜLAÇTI

1.Giriş

E-imza, elektronik ortamda kimlik doğrulama ve onay verme amacıyla kullanılan en güvenli ve en yaygın teknik araçtır. Bu nedenle, dünyanın birçok ülkesinde e-imzanın elektronik ortamdaki iş süreçlerinde kullanımı, kanunlarla ve ilgili ikincil mevzuatla (yönetmelik, genelge, tebliğ vb) düzenlenmiştir. E-imza, hukuk ve teknolojinin kesiştiği bir alanda yer aldığı için konuyla ilgili ikincil mevzuat yoğun bir şekilde teknik standartlara atıfta bulunmaktadır.

E-imza ve ilgili teknolojilerin yaygın kullanıma girmesi, 1990'ların ikinci yarısında başlamış ve uluslararası standartların yazılması bu gelişmeye paralel olarak gerçekleşmiştir. Standart hazırlayan kurum ve kuruluşlar tarafından yürütülen birçok e-imza standardizasyon çalışması bulunmaktadır. Standartlarla ilgili bölümde, bu çalışmalar hakkında bilgi verilmektedir.

Dünyada e-imzanın hukuki düzenlemeleri konusunda, iki temel yaklaşım bulunduğu söylenebilir: serbest ve sıkı düzenleme yaklaşımı. Birincil mevzuat olan kanunlarda, genellikle e-imzanın teknik yönü ile ilgili bağlayıcı bir teknolojik tanım bulunmamaktadır. Ancak ikincil mevzuatta, ülkenin e-imza uygulaması ile ilgili teknik ve standartlara bağlantı kurulmaktadır. Hukuki düzenlemeleri serbest yaklaşımda gerçekleştiren ülkeler, ikincil mevzuatta daha esnek kurallar getirmektedir, örneğin e-imza araçlarının mutlaka donanım olması zorunluluğu yoktur. Hukuki düzenlemeleri sıkı yaklaşımda gerçekleştiren ülkeler ise, e-imza ile ilgili teknik kriterleri, güvenlik ve karşılıklı çalışabilirlik gerekçeleriyle çok daha ayrıntılı belirlemişlerdir.

Yazının e-imza mevzuatı ile ilgili bölümünde, Türkiye'deki ve Avrupa Birliği'ndeki mevzuat ile ilgili bilgiler verilmektedir.

2. Standartların Gelişimi

E-imza standartlarını incelemeye başlamadan önce, genel olarak standartların nasıl hazırlandığını ve bu konuda hangi kurum ve kuruluşların rol aldığını bilmek yararlı olacaktır. Standartları en genel anlamda ulusal ve uluslararası olarak sınıflandırmak mümkündür. Günümüzde uluslararası standartların önemi çok artmıştır. Ürün ve hizmetlerin tüm dünyada pazarlanabilecek şekilde geliştirilmesinin en önemli koşulu, uluslararası standartlara uyumdur.

Bilişim dünyasında geçerli olan uluslararası standartları aşağıdaki şekilde sınıflandırmak mümkündür:

- Fiili (de facto) standartlar
- İnternet standartları
- Standardizasyon kuruluşlarının hazırladığı standartlar

Fiili standartlar genellikle patent sahibi veya tekel konumunda olan özel şirketler tarafından geliştirilir. İlgili sektördeki diğer

firma ve kurumlar da, fiili standarda uyumlu ürün ve hizmetler sunarak, standardın daha yaygın ve güçlü hale gelmesine neden olurlar. Fiili standartlar genelde kamuya açık olarak yayımlanırlar.

İnternet standartları genellikle IETF (Internet Engineering Task Force: İnternet Mühendisliği Görev Gücü) ve W3C (World Wide Web Consortium: Dünya Çapında Ağ Birliği) kuruluşları tarafından oluşturulan ve internet ortamında kullanılan protokolleri ve veri biçimlerini tanımlayan standartlardır. İnternet standartları, konuyla ilgili herkesin katılabileceği süreçlerden geçerek hazırlanır ve kamuya açık olarak yayımlanır.

Standardizasyon kuruluşlarının hazırladığı standartlar belirli bir alanda uzmanlaşmış, üyelik esasına göre çalışan uluslararası kurumlar veya ulusal standart oluşturma kurumları tarafından hazırlanır. Örneğin ISO (International Organization for Standardization: Uluslararası Standardizasyon Kuruluşu), ITU (International Telecommunication Union: Uluslararası Telekomünikasyon Birliği), ANSI (American National Standardization Organization) bu tür kuruluşlardır. Bu şekilde hazırlanan standartların bazıları (örneğin ISO standartları) ancak ücret karşılığında elde edilebilir ve kamuya açık olarak yayımlanmaz.

Çoğu zaman standartlar ihtiyaçlardan dolayı ortaya çıkarlar ancak her zaman ihtiyaçları karşılamakta yeterli olmayabilirler. Özellikle çok sayıda uzmanın ve üye kuruluşun/ülkenin dahil olduğu standart oluşturma çalışmaları yavaş ilerler. Bunun başlıca nedeni, çalışmaya katılan her üyenin, hazırlanmakta olan standardı, kendi amacına ve çıkarına en uygun duruma getirme çabasıdır. Bu nedenle bazen çalışmalar yıllar boyunca sürebilir veya standart yetersiz bir içerikle yayımlanabilir.

Fiili standartların ihtiyaçları karşılama açısından üstünlüğü bulunmaktadır. Fiili standartlar genellikle bir kurumun kendi ticari ürün ve hizmetleri ile ilgili olarak oluşturduğu çalışmalardır. Bu nedenle belirli bir hedefe odaklı ve bütünlük içeren standart tanımları üretmekte daha iyi sonuç verirler. Bu standartlar da, genellikle bir süre sonra internet standardı olarak, uluslararası bir çalışma grubu tarafından yayımlanırlar (örneğin IETF tarafından).

E-imza ile ilgili çok çeşitli standartlar bulunmaktadır. Bunlar dördüncü bölümde ayrıntılı olarak görülebilir. Bu standartların bir bölümü aşağıda belirtilen uluslararası kuruluşların alt çalışma grupları tarafından hazırlanır.

ITU (International Telecommunication Union: Uluslararası Telekomünikasyon Birliği) : 1865'de kurulan birlik, 1947'de Birleşmiş Milletlere bağlı bir kuruluş haline gelmiştir. 192 üye ülke ve 700 üye kuruluşu bünyesinde barındırır. X.500-530 Dizin standartları, X.680-699 ASN (Abstract Syntax Notation: Soyut Sözdizimi Biçimi) standartları gibi çok sayıda bilişim standardını hazırlayan kuruluştur. E-imza açısından en önemli standart olan X.509 Açık Anahtar ve Nitelik Sertifikaları standardının ilk sürümünü 1988 yılında yayımlamıştır.

IETF (Internet Engineering Task Force: İnternet Mühendisliği Görev Gücü): 1986'da ABD'de devlet tarafından desteklenen araştırmacıların bir araya gelmesiyle çalışmaları başlayan bir kuruluştur. 1992'de kurulan İnternet Toplumu (İnternet Society) kuruluşu şemsiyesi altında uluslararası hale gelmiştir. İnternet ve bilişimle ilgili RFC (Request For Comments) adı verilen belgeleri oluşturan ve bir süreç sonunda bu belgelerden bazılarını internet standardı olarak yayımlayan kuruluştur. IETF altında çalışma gruplarından PKIX (Public Key Infrastructure X.509: Açık Anahtar Altyapısı X.509) elektronik sertifika ve e-imza konusundaki standartları hazırlar.

ETSI (European Telecommunications Standards Institute: Avrupa Telekomünikasyon Standartları Enstitüsü): Ağırlıklı olarak Avrupa ülkeleri ve kuruluşlarının üye olduğu, bağımsız ve kar amacı gütmeyen bir standardizasyon kuruluştur. 1988'de kurulan ETSI'nin yayımladığı GSM ve TETRA standartları tüm dünyada yaygın kullanım alanı bulmuştur. E-imza ile ilgili olarak da IETF grubu tarafından yayımlanan temel standartları geliştiren ve kullanım alanını genişleten çalışmalar ETSI ESI (Electronic Signatures and Infrastructures: Elektronik İmzalar ve Altyapılar) teknik komitesi tarafından hazırlanmıştır.

CEN (Comite Europeen de Normalisation: Avrupa Standardizasyon Komitesi): 1961'de kurulan ve 30 üye ülkenin katılımıyla çalışmalarını yürüten bir kuruluştur. Avrupa Komisyonu tarafından başlatılan EESSI (European Electronic Signature Standardization Initiative: Avrupa Elektronik İmza Standardizasyonu Girişimi) kapsamında düzenlenen çalıştaylara öncülük etmiş ve CWA (CEN Workshop Agreement: CEN Çalıştay Anlaşması) adı verilen standartların oluşturulmasını sağlamıştır.

CC (Common Criteria: Ortak Kriterler): ISO tarafından yayımlanan 15408 numaralı standarttır. Bilgi güvenliği ürünleri ve sistemlerinin güvenlik testleri ve sertifikasyonu için kullanılır. CC sertifikası Türkiye'nin de aralarında olduğu sertifika

üreticisi 14 üye ülkenin akredite olmuş laboratuvarlarından alınabilir. CC sertifikasının seviyesi EAL (Evaluation Assurance Level: Değerlendirme Güvence Seviyesi) ile ifade edilir (1-7 arasında).

FIPS (Federal Information Processing Standards: Federal Bilgi İşleme Standartları): ABD NIST (National Institute of Standards and Technology: Ulusal Standart ve Teknoloji Enstitüsü) kurumu tarafından bilgisayar sistemlerinde kullanılmak üzere geliştirilen ve yayımlanan standartlardır. ABD tarafından yayımlanmasına rağmen uluslararası kabul görmüştür.

E-imza ile ilgili en önemli fiili standartların bazıları aşağıda belirtilen kurumlarca oluşturulur.

PKCS (Public Key Cryptography Standards: Açık Anahtarlı Kriptografi Standartları): RSA firması tarafından oluşturulan ve yayımlanan, açık anahtarlı algoritmaların kullanımını ilgili standartlardır. Fiili olarak e-imza dünyasını yönlendiren standartlardır.

PCSC (Personal Computer SmartCard Workgroup: Kişisel Bilgisayar Akıllı Kart Çalışma Grubu): Microsoft, Oracle, Gemalto ve Oracle firmalarının önderliğine bilişim endüstrisinde akıllı kart ve kart okuyucuların standartlaşması için çalışan bir gruptur. Kişisel bilgisayarların işletim sistemleri tarafından kullanılan PCSC standardını oluşturan ve yayımlayan önemli bir uluslararası organizasyondur.

3. E-İmza Mevzuatı

Türk hukuk sisteminde kanuni düzenlemeler yukarıdan aşağıya doğru şu şekilde sıralanırlar: taraf olunan uluslararası anlaşmalarla yapılan düzenlemeler, anayasa, kanun, kanun hükmünde kararname, tüzük, bakanlar kurulu kararları, yönetmelik, yönerge, usul ve esaslar, genelge, tebliğ, tanım, talimat. Bu normlar hiyerarşisinde elektronik imza ile ilgili düzenleme yapmak için ilk olarak 2004 yılında 5070 sayılı Elektronik İmza Kanunu kabul edilmiştir.

Elektronik İmza Kanunu, Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) elektronik imza kanununun uygulanması ile ilgili usul ve esaslar hakkında yönetmelik hazırlanması görevini vermiştir. Yine 5070 sayılı kanun BTK'ya Sertifika Mali Sorumluluk Sigortası Yönetmeliği hazırlanması görevini de vermiştir.

BTK tarafından hazırlanan "Elektronik İmza Kanununun Uygulanması İle İlgili Usul ve Esaslar Hakkında Yönetmelik"teki 34ncü madde gereğince yine BTK tarafından "Elektronik İmza ile İlgili Süreçlere İlişkin Tebliğ" yayımlanmıştır. Yönetmelik'te yer alan 35nci madde Yönetmelikte hüküm bulunmayan durumlar için, Kurul Kararı ile düzenleme yapılabileceğini belirtmektedir.

Bu durumda Türkiye'deki e-imza mevzuatı aşağıdaki şekilde oluşmaktadır (aşağıdaki mevzuat Resmi Gazete'de belirtilen tarihte yayımlanmıştır):

- 5070 Sayılı Elektronik İmza Kanunu (23.01.2004 tarihli)
- Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (06.01.2005)
- Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (06.01.2005)
- Sertifika Mali Sorumluluk Sigortası Yönetmeliği (26.08.2004)

Sertifika Mali Sorumluluk Sigortası Yönetmeliği'ni tamamlayıcı nitelikte olan aşağıda düzenlemeler de, Hazine Müsteşarlığı tarafından hazırlanmış ve belirtilen tarihlerde Resmi Gazete'de yayımlanmıştır.

- Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları (27.01.2005)
- Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı (27.01.2005)

Bu hukuki düzenlemelere ek olarak, kamu kurumlarının elektronik sertifika temini yöntemlerini tanımlayan iki Başbakanlık Genelgesi yayımlanmıştır.



KALİTE ÇEMBERLERİ VE SORUN ÇÖZME YÖNTEMLERİ

BİLAL KILIÇ

1. Giriş

Kalite Çemberi kavramı 1960'lı yıllardan başlayarak dünyada hızla yayılmış ve pek çok alanda uygulama bulmuştur. İş yaşamında kalitenin artırılması için uygulanan önemli yöntemlerden birisi kalite çemberleridir. İşletmelerin verimliliklerinin, başarılarının artırılmasında, gereksinimlerinin karşılanmasında kalite çemberleri doğrudan etkindir.

İş ile doğrudan, iç içe çalışanların, işletmedeki sorunların çözümü için, hangi değişikliklerin nasıl yapılması gerektiği konusunda en sağlıklı bilgileri verebilecekleri düşünülmektedir; yani **“bir işi kim yapıyorsa en iyi o bilir”** anlayışı geçerlidir. Dolayısıyla, yenilikler ve iyileştirmeler konusunda danışılması gerekenler de çalışanlar olmalıdır.

Bir işi kim yapıyorsa en iyi o bilir

Kalite çemberlerinin uygulanabilmesi için en önemli koşul, üst yönetimin katılımcı, açık ve demokratik yönetim anlayışını benimsemiş ve çemberlerin yararlarına inanmış olmasıdır. Bu amaçla çeşitli anketler hazırlanarak davranış testleri yapılabilir. Çok demokratik işletmelerde bile baskıcı yönetim anlayışına sahip yöneticiler olabilir. Bu tür yöneticilerin bulunduğu bölümlerin seçilmesi uygun değildir.

Diğer önemli bir koşul da, işletmenin sosyal bakımdan ılımlı olması, ücret politikası ve işçi-işveren ilişkileri gibi konularda sorunlarının olmamasıdır. Çalışanlar arasında da anket düzenlenerek bu konular hakkında bilgi sahibi olunabilir.

Bu yazı iki kısımdan oluşmaktadır. Birinci kısımda; kalite çemberinin tanımı, tarihçesi, organizasyonu, amaçları, yararları, özellikleri ve çalışma yöntemleri anlatılmış, ikinci kısımda ise kalite çemberlerinin sorunları çözmek için uyguladığı yöntemlerden söz edilmiştir.

2. Kalite Çemberinin Tanımı

Kalite Çemberi teriminin Japonca karşılığı “Jishu Karni”, kendi kendini denetleme ve yönetme, işini denetleme gibi anlamlara gelmektedir. Bunun dışında, kalite çemberini pek çok biçimde tanımlamak mümkündür. Bunlar;

► Aynı meslekten olan veya aynı birime bağlı olarak çalışan ve sayıları 6-12 kişi arasında değişen gönüllü kişilerin oluşturduğu küçük bir gruptur.

► Bir lider tarafından yönlendirilen, düzenli ve sürekli aralıklarla toplanan gönüllü bir çalışma grubudur.

► Periyodik toplantılar yaparak, belirlenen sorunların kaynaklarını, nedenlerini araştıran, bulan, çözen ve üst kademe yönetime sunan çalışma grubudur.

Kalite çemberinde ele alınacak sorunlar yalnızca kalite ile ilgili değil, aynı zamanda maliyeti düşürme, verimlilik, iş güvenliği, etkin grup çalışmasını sağlama vb. diğer işletme sorunlarıyla da ilgili olabilir.

3. Tarihçesi

Kalite çemberi ilk defa 1960'lı yıllarda Japonya da, 1970'li yıllarda ABD ve diğer batı ülkelerinde, 1980'li yıllarda da ise ülkemizde uygulanmaya başlamıştır. Sonraki yıllarda ise geniş bir uygulama alanı bulmuş ve neredeyse tüm dünyada uygulanmaya başlamıştır.

İkinci Dünya Savaşı'ndan yenik çıkan Japonya ürettiği kalitesiz ürünler ile ünlüydü ve ekonomi iflasın eşiğindedi. Ancak Japonya kısa bir sürede kaliteli ürünlerle dünya pazarlarına girmeyi başardı.

Japonların ekonomik açıdan bu kadar çabuk toparlanmasında, savaş yılları sonrasında, Japonya'da ABD işgal kuvvetleri komutanı olarak bulunan General Douglas Mac Arthur'un büyük katkısı vardır. Mac Arthur Japonya'nın doğal kaynaklardan yoksun olmasının, ülkeyi uluslararası anlaşmalara yönlendireceğini ve Japonların kalitesiz ürünlerinin dünya pazarlarında kabulünü zorlaştıracağını biliyordu. Bu nedenle Mac Arthur Japon yetkilileri, parasal yönden kendi kendilerine yeterli olabilmelerini sağlamak amacıyla, Amerika'lı bilim adamları ve uzmanlardan yardım almaya ikna etmiştir.

1950 yılında çağrılan Amerikalı uzmanlardan Dr. Deming Japonya'nın kaderini değiştirmiştir. O dönemde Amerikan Savaş Bakanlığı'nda savaş malzemelerinin kalitesinin artırılması konusunda çalışmalar yapan ve kalite kontrol uzmanı olan Dr. Deming'in Japonya'ya davet edilmesinde, Amerika'da kendisi ile birlikte çalışan Japon öğrenciler ve Prof. İshikawa etkili olmuştur. Dr. Deming Japon genel müdürler için bir dizi seminerler vererek onları kalite kontrol konusunda bilgilendirmiştir. Bu seminerlerin sonunda, Japon işletmelerinin temel işleyiş modeli oluşturulmuştur.

Japonya'da kalitenin artırılmasında etkili olan diğer bir isim de Juran'dır. Juran 1954 yılında JUSE (Japon Bilim Adamları ve Mühendisleri Birliği) tarafından Japonya'ya davet edilmiş ve 1960 yılına kadar kalite kontrol yönetimi hakkında konferanslar vermiştir.

Tüm bunların yanı sıra, Japon hükümeti de yapılan bu çalışmalara sürekli destek vererek eğitim programları düzenlemiş, radyo ve televizyonlarda kalite konusunda çeşitli programların yapılmasını sağlamıştır.

Kalite çemberi kavramı, ilk defa Japonya'da kalite kontrol adını taşıyan derginin düzenlediği bir sempozyumda ortaya atılmıştır. Bundan sonra JUSE bu yeni kavramı denemek isteyen işletmelerin listesini yapmıştır. Kısa süre içinde kalite çemberi

kavramına olan ilgi artmış ve birçok Japon işletmesi kalite çemberlerini uygulamaya başlamıştır.

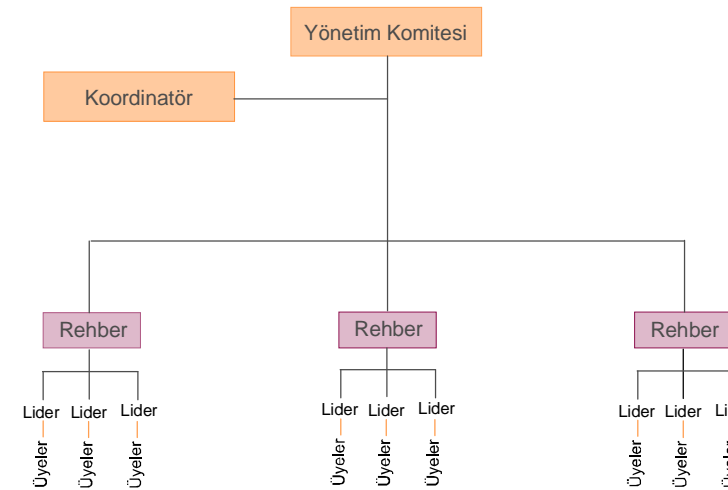
Kalite çemberlerinin Amerika ve Batı ülkelerinde tanınmaya başlaması ise, 1967 yılında Juran'ın yayınladığı “Kalite Kontrol Çemberleri” adlı yazıyla olmuştur. Juran'ın bu yazısı büyük ilgi uyandırmış ve kalite çemberleri diğer ülkeler tarafından da uygulanmaya başlamıştır.

4. Kalite Çemberlerinin Organizasyonu

Her firmanın kendine özgü koşulları olduğundan, kalite çemberlerinin organizasyonu da firmadan firmaya, ana yapısı aynı kalma koşuluyla değişiklik göstermektedir. Oluşturulan kalite çemberlerinin kalıcı olması, her kademedan yönetici ve çalışanın katılımı ve bu yapılanmayı benimsemesi ile başarıya ulaştırılabilir. Kalite çemberleri 6 ile 12 arasında kişiden oluşan, küçük çalışma gruplarıdır.

Kalite çemberlerinin oluşturulmasında, normal ve düzenli bir emir komuta zinciri kullanılır. Ast üst ilişkisinin dışına çıkmaz. İşletmedeki kalite çemberlerinin organizasyon şemasında aşağıdaki organlar vardır.

- Yönetim Kurulu
- Koordinatör
- Rehber
- Lider
- Üyeler



Şekil 1. Kalite çemberlerinin organizasyonu.

Yönetim Kurulu Üyeleri: Uzun süren kalite çemberleri çalışmalarının sürekli üyeleri olarak büyük öneme sahiptirler. Yönetim kurulu üyeleri genellikle işletmelerin ana bölüm temsilcilerinden oluşur. Üye sayısı 7-8 kişi olabilir. Gerekliğinde bu sayı daha da artabilir. Yönetim kurulu kalite çemberleri

çalışmalarını amaç ve hedefler doğrultusunda belirler. Kurulun bir lideri vardır ve tüm kararlar demokratik olarak oylama ile alınır.

Kalite çemberleri 6 ile 12 arasında kişiden oluşan, küçük çalışma gruplarıdır.

Yönetim kurulunun, hedeflerin belirlenmesi ve duyurulması, fon düzenlemeleri, çember liderinin seçimi, rehberin seçimi, eğitimlerin düzenlenmesi, toplantı sıklık ve sürelerinin belirlenmesi, çember çalışmalarının değerlendirilmesi için gerekli bilgilerin sağlanması ve çember çalışmalarının etkinliğinin denetlenmesi vb. görevleri bulunmaktadır.

Koordinatör: Koordinatör, bir organizasyon içinde yürütülmekte olan kalite çemberleri çalışmalarının koordine edilip yönlendirilmesinden sorumlu olan kişidir. Koordinatör rehberleri denetlemek ve yönetime destek sağlamakla birlikte ana görevi rehberlerle yönetim kurulu arasında iletişim kurmaktır. Yönetim kurulunun doğal üyesidir. Kalite çemberlerinin iletişim kanalları yukarıdan aşağıya olduğu kadar, aşağıdan yukarıya doğru da olumlu bir şekilde çalışmaktadır. İletişim yalnızca çember üyeleri arasında kalmaz, üyeler ile yönetim arasında da doğrudan ilişki kurulur. İletişim kanallarının açık tutulması için gerekli ortamın hazırlanması konusunda koordinatöre önemli görevler düşmektedir.

Rehber: Organizasyonda grup çalışmalarını yöneten ve koordine eden kişidir. Çemberin etkin çalışmasında kilit bir role sahiptir. Üst yönetim ile çember arasında köprü görevi görür. Rehber sayısı organizasyonun büyüklüğüne göre farklılık gösterir. Bir rehberin, iletişim gücü gelişmiş, organizatör olma eğiliminde, kalite kontrol ve istatistik hakkında temel bilgilere sahip, gayrete getirici, iyi bir dinleyici olması gerekmektedir. Görevleri ise; yönetim kurulunun belirlediği politikaları uygulamak, liderin eğitimini sağlamak, çember çalışmaları ile ilgili yönetim kuruluna rapor vermek, yönetim ile çember arasında iletişimi sağlamak, çember uygulamalarına katılmak ve sorunları çözmeye onlara yardımcı olmaktır. Rehber, kurum içinde kurulan birden çok çemberle ilişki kurup koordinasyon sağlar.

Lider: Her çemberde bir adet lider yer almalıdır. Lider çember üyelerinin eğitiminden, onların çalışmalarından sorumludur. Lider rehber tarafından yetiştirilir ve kendisine çeşitli beceriler kazandırılır. Lider, kendi bölümünde çalışanları gayrete getirip, yeterli sayıda gönüllü bularak çemberini kurar. Liderin görevleri arasında; toplantıların tarihlerini ve gündemlerini belirlemek, çember üyelerini eğitmek, grubu özendirerek etkinliklere katılımını sağlamak, üyeleri toplamak, öneriler toplayarak üyelerle birlikte çemberin üzerinde çalışacağı sorunu belirlemek, sorunların analizinde uygun yöntemleri belirlemek, çemberin çalışmalarıyla ilgili olarak bağlı olduğu üstlere bilgi vermek vardır.

Üyeler: Çemberin oluşumundaki en önemli unsurdur. Üyeler gönüllülük esasına dayalı olarak çalışır. Çembere çalışmalarıyla katkıda bulunan kişilerdir. Üyeler, grup liderinin yardımı ile rehber tarafından sorun çözme ve iletişim becerileri konusunda eğitim alırlar. Üyelerin, bütün toplantılarda bulunmak, istatistik yöntemleri öğrenmek, davranış tüzüğüne uymak, kalite çemberi ilkelerine bağlı davranmak, kalite çemberi programını tanımak, işi hoşnut olarak yapmak, çembere yeni üyeler bulmak, sorunun çözümüne katılmak, öneriler geliştirmek gibi görevleri vardır. Bir kalite çemberinde üye sayısı genel olarak 6-12'dir.

Üyeler, çemberin oluşumundaki en önemli unsurdur.

5. Kalite Çemberinin Amaçları

Kalite çemberi kavramı, bir kuruluşta birçok alanda uygulanabilir. Bunlar; kuruluş yönetimi ve iş organizasyonu, iş verimliliği, müşteri memnuniyeti, maddi değerini arttırma, satış sonrası hizmet ve destek, müşteri bilgilendirme, eğitim, bakım kolaylığı, hizmet hızı ve kalitesi, kuruluş imajı, güvenilirlik vb. alanlardır.

Kalite çemberlerinin en önemli yönü insan kaynaklarının ve teknik kaynakların bir araya getirilmesinde düzenli bir yaklaşımın sağlanmasıdır. Amaç, ürün kalitesinin, çalışma yaşamı kalitesinin ve kurumsal verimliliğin artırılmasıdır.

Kalite çemberlerinin en önemli yönü insan kaynaklarının ve teknik kaynakların bir araya getirilmesinde düzenli bir yaklaşımın sağlanmasıdır.

Kalite çemberlerinin esas amaçlarını şöyle sıralayabiliriz:

- ▶ Hataları azaltmak, kaliteyi yükseltmek,
- ▶ Üretim giderlerini düşürmek,
- ▶ Çalışanların, eğitilmelerini sağlayarak, sorunları kavrama ve çözme kapasitesini geliştirmek,
- ▶ Sorun yaratma yerine çözüm getirme alışkanlığını sağlamak,
- ▶ Sorunları daha doğmadan engelleme alışkanlığını kazandırmak,
- ▶ Daha uyumlu yönetici-çalışan ilişkisinin gelişmesine ortam hazırlamak,
- ▶ Çalışanların gayretini ve işe bağlılığını arttırmak,
- ▶ İşletmede çalışanlar arasında iletişim kanallarının geliştirmek,
- ▶ Her düzeydeki çalışanın beyni, elleri ve gönül gücü ile işe katılımını sağlamak,

- ▶ Fikir ve görüşlerin uygulanmasına olanak sağlamak,
- ▶ Grup çalışmalarını özendirme, bireyselliği önlemek,
- ▶ Bireylerin liderlik ve yaratıcılık yeteneklerinin gelişmesine katkıda bulunmak

6. Kalite Çemberlerinin Yararları

Kalite çemberlerinin hem işverene, hem çalışanlara hem de müşterilere yönelik yararları vardır. Kalite çemberlerine katılanların diğer çalışanlara göre işten geri kalma oranlarında azalma, gayretlerinde ve işe bağlılıklarında belirgin bir şekilde artma olduğu gözlenmiştir. Ayrıca kalite çemberlerinin uygulandığı pek çok işletmede her yıl milyonlarca TL'lik kazanım sağlanabildiği görülmüştür.

Kalite çemberlerinin hem işverene, hem çalışanlara hem de müşterilere yönelik yararları vardır.

Kalite çemberlerinin kuruluşu sağladığı başlıca yararlar:

- ▶ Çalışanlar arası ve bölümler arası işbirliğinde artış,
- ▶ Çalışanlarda, kuruluşun sorunlarına karşı ilgi artışı,
- ▶ Ürün ve hizmet kalitesinde artış,
- ▶ Çalışanların devamsızlıklarında azalma,
- ▶ İşveren-işçi ve yönetim-sendika arasında daha iyi ilişkilerin kurulması,
- ▶ Uzun süredir göz ardı edilen veya hiç fark edilmemiş sorunların çözümü,
- ▶ Önerilen sorunların kabulünde ve giderilmesinde artış,
- ▶ Yeni teknolojilerin yerleştirilmesi, yeni üretim ve hizmet alanlarının açılması gibi konuların çalışanlar tarafından kolay kabul edilmesi,
- ▶ İşletmede maddi kazanımın sağlanması,
- ▶ Daha az kişinin işten çıkarılması,
- ▶ Araç ve gereçlerin etkin kullanımı,
- ▶ Daha iyi eğitilmiş işgücüne ulaşılması,
- ▶ Güven ortamının oluşması,
- ▶ İş güvenliğinin artması.

Kalite çemberlerinin çalışanlara sağladığı başlıca yararlar:

- ▶ İşe katılım ve gayretin artması,
- ▶ Düşüncelerin söylenebileceği bir ortamın yaratılması,

Kalite Çemberleri ve Sorun Çözme Yöntemleri

- ▶ Çok çeşitli konularda yarar sağlayan eğitimler,
- ▶ Grup içinde işbirliği yapma ve sahiplenme duygusunun geliştirilmesi,
- ▶ Bilgi, hayal gücü, karar verme ve değerlendirme yeteneklerinin geliştirilmesi,
- ▶ Sorun çözme yöntemlerinin öğrenilmesi, tanıların başarıyla konulması, sorunların önlenmesi,
- ▶ Liderlik yeteneklerinin geliştirilmesi ve değerlendirilmesi,
- ▶ Gizli kalmış yeteneklerin ortaya çıkarılması,
- ▶ İş görenlere, çalıştıkları bölümlerdeki çalışmalarda etkin rol alabilme olanağının sağlanması.
- ▶ Çalışanlarda moral yüksekliğinin, özgüven yüksekliğinin ve iş memnuniyetinin artması,
- ▶ İşinde yükselme,

7. Kalite Çemberinin Özellikleri

Kalite çemberlerinin oluşturulması ve işletilmesi aşağıdaki özellikleri içerir:

Gönüllülük: Kalite çemberlerine katılan çalışanların gönüllü kişilerden olması gerekir. Başka bir deyişle, grubu oluşturan üyeler atama yoluyla gelmemeli, katılım konusunda üst yönetim tarafından bir baskı yapılmamalı, yalnızca üst yönetim bu konudaki kararlılığını, isteğini ve desteğini işletme çalışanlarına göstermelidir. Üyelerin çembere katılımlarında gönüllülük esası söz konusu iken, çember liderlerinin çemberlere katılımında gönüllülük esası aranmayabilir.

Kendini geliştirme: Yöneticiler ve kalite liderleri, eğitim ve yetiştirme yoluyla insanların yeteneklerini geliştirmeye önem vermelidir. Kişilerin kendilerini tanımalarına ve anlamalarına da ayrıca önem verilmelidir.

Karşılıklı gelişme: İnsanlar birbiriyle etkileşimde olduğundan, değişik bölümlerde çalışanların ortak çalışması birbirlerini geliştirir.

Bütün üyelerin katılımı: Kalite çemberinde çalışan bütün üyelerin çalışmalara katılımı zorunludur. Bununla birlikte, bir şirkette genel müdürden başlayarak herkesin belirli bir kalite çemberine girmesi gerekmez. Gerektiğinde, özel kalite çemberleri oluşturularak şirketin toplam kalite kontrol programına katılabilir. Ayrıca, kimi yöneticiler ve teknisyenler de onlara verilen normal görevler yoluyla çember çalışmalarına katılabilir. Bir kalite çemberine giren her üyenin, tüm toplantılara katılıp bir görevi üstlenmesi gerekir.

Canlılık ve süreklilik: Çember üyeleri incelenen sorun ne olursa olsun aynı kalmalı, başka bir deyişle, sorunu ele alan üyeler çözüm üretilene kadar birlikte çalışmalıdır. Süreklilik

kavramı çember üyelerinin belli bir ölçüde yenilenmesine mutlak anlamda karşı değildir. Ancak bu yenilenme, çemberin büyük bölümünü kapsayacak ölçüde ya da grubun çok sık yenilenmesi anlamında olmamalıdır.

Grup etkinliği: Grup çalışması sonucu takım ruhu ortaya çıkar, çalışanlar kendilerine verilen değeri anlar.

Ödüllendirme: Çember üyelerinin sorun çözme, öneri geliştirme ve çemberlere süreklilik kazandırma konularındaki katkılarının yönetim tarafından övülmesi, ödüllendirilmesi gerekir. Böylelikle görüşlerinin dikkate alındığını farkına varan çember üyelerinin çalışmalarına canlılık kazandırılmış olur.

8. Kalite Çemberinin Çalışma Yöntemi

Kalite çemberlerinin işleyişi sırasında, aşağıdaki işlemler gerçekleştirilir.

Sorunun belirlenmesi

Kalite çemberleri, sorunları belirlerken, kendi çember üyelerinden, yönetimden, diğer ekiplerden ve birimlerden yararlanabilir. Sorunlar belirlenirken çeşitli yöntemler kullanılır. Fakat içlerinden en etkilisinin “beyin fırtınası” olduğu söylenebilir.

Sorunun seçimi

Sorunlardan hangisinin, kalite çemberleri tarafından üzerinde tartışılmak üzere seçileceğine çember üyeleri karar verir.

Sorunun analizi

Bir sorunun analizinde “beyin fırtınası” ve “neden sonuç analizi” kullanılır. Lider, genellikle üyelere, nedenlerle ilgili fikirlerini sorar ve bu nedenleri bir kağıda liste halinde sıralar. Asıl neden, grubun onayı ile belirlendikten sonra, üyeler bu nedene çözüm aramayı sürdürebilir.

Önerilen çözüm

Sorunun gerçek nedeni belirlendikten sonra, üyeler bu nedenin ortadan kaldırılması için öneriler ileri sürer. Öneriler incelenerek çözüm için bir karara varılır.

Yönetime sunma

Çember, etkili bir çözüm bulunduğunda, üst yönetime çalışmaların sonucu göstermek istediğini bildirir. Böyle bir sunuşun yapılabilmesi için, önce bir raporun hazırlanması gerekir.

Çözümün uygulanması

Sunuştan sonra, konunun incelenmesi ve çözümün uygulanması, yönetimin görevidir. Eğer yönetim projeyi onaylarsa uygulamaya geçirir. Çalışanlar uygulamayı yapar.

9. Kalite Çemberlerini Olumsuz Etkileyen Etmenler

Kalite çemberleri çeşitli gelişme dönemleri geçirir. Bu dönemlerin uzunlukları gruplar arasında değişiklik gösterse de her kalite çemberi bulunduğu döneme ait özellikleri taşır. Kalite çemberleri başlangıç döneminde katılımcı azlığı, yetersiz parasal destek ve grup üyelerinin grup işleyişini ve sorun çözme becerilerini öğrenememesi gibi risklerle karşı karşıyadır. Çoğu kalite çemberinde bu engeller aşılar ve bir sonraki aşamaya geçilir. İlk sorun çözme aşamasında grubun karşılaşacağı çok zorluk yoktur. Bu dönemde sorunların üzerinde anlaşamama veya sorun çözümü konusunda yeterli bilgi sahibi olamama gibi zorluklarla karşılaşılrsa da bunlar çoğunlukla aşılabılır.

Grup üyelerine çalışma isteği verecek ve doyum sağlayacak olan en önemli unsur yaptıkları işe yönetim tarafından önem verilmesi ve saygı duyulmasıdır. Grubun karşılaşacağı ilk olumsuzluk, üretilen çözümlerin rapor edilmesinden sonra kabul görmemesidir. Yöneticilerin çemberin önerilerine olumsuz tepki göstermeleri veya hiç dikkate almamaları olasılığı yüksektir. Böyle bir durumda grup üyelerinin morali bozulur, zaman kaybettiklerini düşünürler ve grup dağılır. Bazı durumlarda ise moral vermek için grubun ilk önerileri olduğu gibi kabul edilir. Bu durum ise, orta kademedeki yöneticilerin grubun çalışmalarını küçümsemesine ve gelecekte pek dikkate almamasına neden olacaktır. Çoğu kez, önerilen çözümler kabul edilmekle birlikte çözümlerin uygulanması aşamasında sorunlar çıkmaktadır. Yöneticiler, pahalı olması veya gruplar arasında görüş ayrılığı oluşması nedeniyle çözümleri uygulamayabilirler. Önerilerin kabulünde olduğu gibi, eğer sunulan fikirler uygulanmaya konmazsa, yine grup zamanla çalışma isteğini kaybedecek ve dağılacaktır. Kimi zaman önerilen çözümler büyük ölçüde kazanım sağlayacağından kabul edilir ve grup bir sonraki aşamaya ilerleyebilir.

Bundan sonraki aşama, sorun çözümlerinin yaygınlaştırılmasıdır. Bu aşamada eski grupların yanı sıra yeni gruplar da oluşur. Yeni fikirler yeni insanların da işe karışmasını, dolayısıyla, daha çok para ve işgücünü gerektirecektir. Bir çemberin çok başarılı olması, gruba üye olmayan insanlarda kıskançlık, dolayısıyla üye olanlarla olmayanlar arasında bir çatışma yaratabilir. Ayrıca, ilk başarılar grup üyelerinin de isteklerini artırabilir. Üyeler, yönetime daha fazla katılmak, elde edilen kardan pay almak da isteyebilirler. Kalite çemberlerindeki başka bir sorun da gruptaki üye sayısı arttıkça bireysel sorumluluğun, dolayısıyla üretimin azalmasıdır. Bu nedenle üye sayısı uygun sınırlarda tutulmalı, gerekirse yeni çemberler oluşturulmalıdır. İlk sorunların çözümünden sonra üzerine eğilecek sorun bulunamaması veya grubun çalışmalarının çok genişlemesi nedeniyle, parasal yükün çok fazla artması gibi olumsuzluklar da ortaya çıkabilir. Bütün bu zorlukların aşılması durumunda, kalite çemberi yoluna devam edebileceği gibi,

programın gerilemeye başlaması veya başka tür bir programa dönüşmesi de sık rastlanan bir durumdur. Bunun dışında kalite çemberlerini olumsuz etkileyen diğer önemli etmenler de şunlardır:

- ▶ Temel görüşü kendi görüşüne göre oluşturmayı isteme;
- ▶ Ne pahasına olursa olsun haklı çıkmayı amaçlama;
- ▶ Saldırgan ve tepkisel davranışlar sonucu, haklı olduğu konuda bile zaman zaman eksi puan alarak başlama;
- ▶ Takım içinde erimeme/kaybolmama vb.

Kalite çemberlerinin devamlılığını sağlamak için grup üyelerinin belli aralıklarla değiştirilerek gruptaki durağanlığın giderilmesi ve taze görüşlerin eklenmesi yararlıdır.

Bu uygulama aynı zamanda diğer çalışanların da gayrete gelmesini sağlayacaktır.

Kalite çemberlerinin devamlılığını sağlamak için grup üyelerinin belli aralıklarla değiştirilerek gruptaki durağanlığın giderilmesi ve taze görüşlerin eklenmesi yararlıdır.

10. Sorun Çözme Yöntemleri (Kalite Çemberinin Kullandığı Temel Araçlar)

Kalite çemberleri sorunları belirlerken, sorunların nedenlerini araştırırken, çözümler ararken, çözüm yöntemini seçerken, çözümü yönetime sunarken, sorun çözme yöntemlerinden yararlanır.

Sorunları çözme yöntemleri Tablo 1'de verilmiştir.

Bunların dışında, Janusian yöntemi, Delphi yöntemi, Zihin haritaları başta olmak üzere daha birçok problem çözme yöntemi vardır.

Sorun çözme yöntemlerini etkin bir biçimde kullanabilmek için; sorunu tanımlamak, çözüm odaklı olmak, ilgili ve bilgili kişileri bir araya getirmek, takım çalışması yapmak, ortak akıl kullanmak, yöntemlerin kurallarını etkin bir şekilde işletmek ve etkili iletişim kurmak gerekir.

Çember üyeleri sorun çözme yöntemlerini kullanarak birbirlerini daha iyi anlayabilir, daha verimli ve dikkatli çalışabilir, sorunları daha kolay belirleyebilir, irdeleyebilir, kavrayabilir, çözüm yöntemlerini daha kolay ve doğru bir biçimde üretebilir, ürettikleri görüşleri ve yaptıkları çalışmalarını daha düzgün ve akılcı bir duruma getirebilir.

Bu yazıda, en çok kullanılan sorun çözme yöntemlerinden PUKÖ dönüşü, Beyin Fırtınası, Neden-Sonuç analizi, Kuvvet-Alan analizi, Pareto analizi, Yoklama Kağıtları, Altı Şapkalı Düşünme Yöntemi ve Histogram'dan söz edilmiştir.

Tablo 1. Sorun çözme yöntemleri.

Sıra	Sorun Çözme Yöntemlerinin Yapısal Sınıfları	Sorun Çözme Yöntemleri
1	Fikir Üretme Yöntemleri	1. Beyin Fırtınası 2. Altı Şapkalı Düşünme Yöntemi 3. Kuvvet/Güç Alanı Analizi 4. Odak Grupları 5. Görüşme
2	Sürekli Geliştirme Yöntemleri	1. PUKÖ Döngüsü 2. 5N -1K Yöntemi
3	Sorun Analiz Yöntemleri	1. Akış Çizelgesi 2. Neden-Sonuç (Balık Kılıçığı) Çizelgesi 3. Pareto Analizi 4. Ağaç Çizelgesi 5. İlgili/Yakınlık Çizelgesi 6. Yoklama Kağıtları 7. Kuvvet/Güç Alanı Analizi
4	Önerileri/Nedenleri Önceliklendirme Yöntemleri	1. İlişki Çizelgesi 2. Etkinlik Analizi
5	Karar Verme Yöntemleri	1. Nominal Grup Yöntemi 2. Çoklu Oylama Yöntemi 3. Hedef Belirleme (Benchmarking) Yöntemi
6	Veri Toplama, Veri Analizi ve Değerlendirme Yöntemleri	1. Anketler 2. Denetleme Tablosu (çetele) 3. Histogram 4. Pareto Çizelgesi 5. Serpme Çizelgesi 6. Hareket Çizelgesi 7. Kontrol Çizelgesi

10.1. PUKÖ Döngüsü

PUKÖ döngüsü dört aşamalı sürekli denetleme ve geliştirmeyi içeren bir çevrimdir. Bu aşamalar planla, uygula, kontrol et ve önlem al'dır.

P: Ne yapmak gerektiği ve nasıl yapılacağı belirlenir.

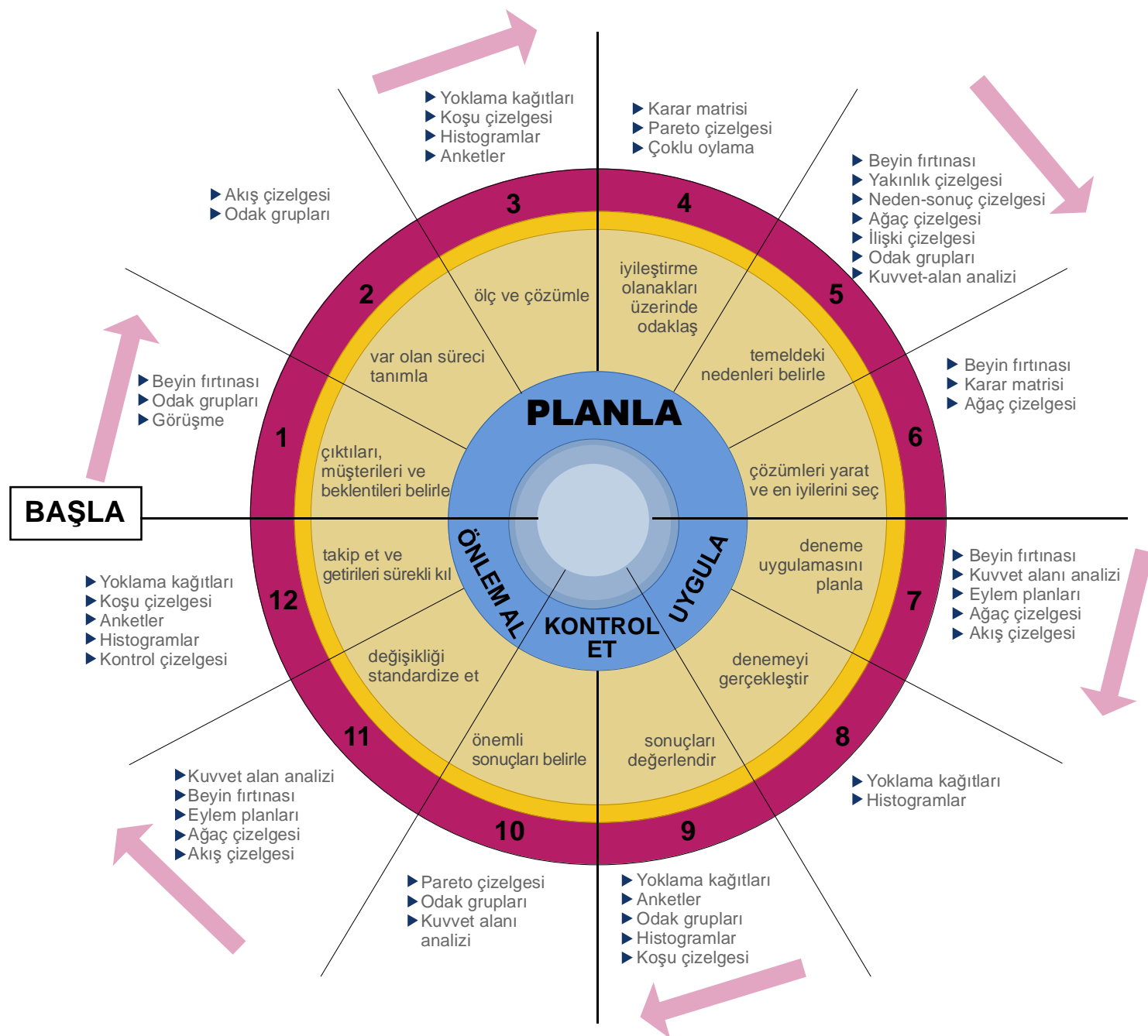
U: Plan ve ölçüm araçları uygulanır.

K: Sonuçlar değerlendirilir ve varsa sapma nedenleri belirlenir.

Ö: İyileştirme kararlı hale getirilir ve yeni çalışma kuralları düzenlenir.

Bir işin gerçekleştirilmesi için söz konusu çevrimin birçok defa tekrarlanması gerekebilir. Ancak yapılan her işte bu aşamaların aynen izlenmesi gerekmez. Bazı aşamalar birleştirilir, bazıları da iş başarılınca kadar birçok kez tekrarlanabilir. PUKÖ çevrimine göre çalışmak insan doğasına en uygun ve en verimli iş yapma şeklidir.

Şekil 2'de PUKÖ çevriminin dört temel aşaması, her aşamada yapılması gereken iş adımları ve iş adımlarında kullanılacak sorun çözme yöntemleri gösterilerek verilmiştir.



Şekil 2. PUKÖ yönetimi ve araçları.

10.2. Beyin Fırtınası

Bir problemin nasıl çözüleceği konusunda hep birlikte görüş bildirmek üzere bir grup insanın toplanmasına beyin fırtınası adı verilir. Beyin fırtınası, ortak sorunlar, toplanacak veriler, çözüm önerileri, uygulama önerileri ve karşılaşılabilecek engeller gibi konularda bir görüş listesi oluşturmak amacıyla yapılır. Kalite çemberlerinin yeni görüş üretmesini sağlayan etkili bir yöntemdir ve oldukça yansız görüşlerin çıkmasına aracılık eder.

Beyin Fırtınasının Amacı:

- ▶ Toplantılarda düzeni sağlamak.
- ▶ Herkese aynı önemi vermek, yararlı ve yenilikçi görüşlerin oluşmasını sağlamak.
- ▶ Zamanı en verimli biçimde kullanmak.
- ▶ Grubun ortak sorunlarını ortaya çıkarmak.
- ▶ Sorunlara ilişkin olarak hangi verilerin toplanacağına karar vermek.
- ▶ Sorunu ortadan kaldırmaya yarayacak önerileri oluşturmak.
- ▶ Yeni bir uygulamada çıkabilecek olası sorunları önceden belirlemek.

Beyin Fırtınasında Uyulması Gereken Kurallar:

- ▶ Zaman sınırlaması yapılmalı ve bir zaman tutucu belirlenmelidir.
- ▶ Beyinler hayalci ve yaratıcı düşünmeye özendirilmelidir.
- ▶ Görüşler belirtildiğinde üzerinde kesinlikle tartışma yapılmaz, eleştirilmez, olumsuz sözcüklerle nitelenmez (saçma, yanlış gibi) ancak anlaşılmadı ise açıklama istenebilir.
- ▶ Düşünceler özlü ve açık biçimde açıklanmalıdır.
- ▶ Üyeler birbirlerinin görüş ve düşüncelerinden yararlanılarak sinerji oluşturacak yeni düşünceler üretmelidir.

- ▶ Etkili bir oturum süreci uzun tutulmamalıdır. Ortalama 1 saat sürmelidir.

- ▶ Toplantı sabırla sürdürülmelidir. Başlangıçta belki konunun özüne inmeyen veya bilinen düşünceler üretilebilir. Ancak bu düşünceler bittiğinde gerçek beyin fırtınası başlar.
- ▶ Her üyenin çalışmalarına iyi niyetle katılması esastır.

Beyin Fırtınası Uygulaması Nasıl Yapılır:

- ▶ Görüşülecek konu belirlenir ve görünür bir yere yazılır.
- ▶ Toplantının amacı sorunu belirlemekse, grup üyeleri olası sorunlar için öneride bulunur; sorunu çözmekse, çözüm önerilir.
- ▶ Her üyeye sırayla belli bir süre verilerek düşüncesi sorulur.
- ▶ Her üye sıra ile söz alarak önceden kararlaştırılmış bir süre sınırlaması içerisinde görüş belirtir. Her söz alışta sadece bir düşünce açıklanır.
- ▶ Sırası gelen kişinin o anda aklına bir düşünce gelmeyebilir. O zaman üye görüşü olmadığını söyler.
- ▶ Tüm görüşler bir yere yazılır.
- ▶ Ortaya çıkan tüm düşünceler tanımlanarak netleştirilir.
- ▶ Düşünceler gerekirse eleştirilerek incelenir, kümelenir veya sayıca azaltılır, bulanık düşünceler yeniden yazılır.
- ▶ Tüm görüşler ortaya konduktan sonra ilk tur oylamaya geçilir. Görüşler tek tek oylanır. Üyeler istedikleri her öneriye oy verebilirler.
- ▶ İlk tur oylama sonucu en çok oy alan öneriler daire içine alınır ve bunlar üzerinde tartışılır. Yine üyeler sıra ile söz alır. Tüm üyeler önerilerini belirtince ikinci tur oylamaya geçilir.
- ▶ İkinci tur oylama sonucu öneriler önem sırasına göre belirlenmiş olur.

10.3. Neden-Sonuç Çizelgesi (Balık Kılıcı Çizelgesi)

Ishikawa Çizelgesi de denir. Bir sorunu doğuran ya da etkileyen nedenleri belirlemek amacıyla oluşturulur. Sorunlara daha geniş bir çerçeveden bakma olanağı sunar. Sorunun tanımını ve süreci iyileştirilmesini kolaylaştırır. Yöntem, beyin fırtınası yöntemi kullanılarak etkinleştirilir.

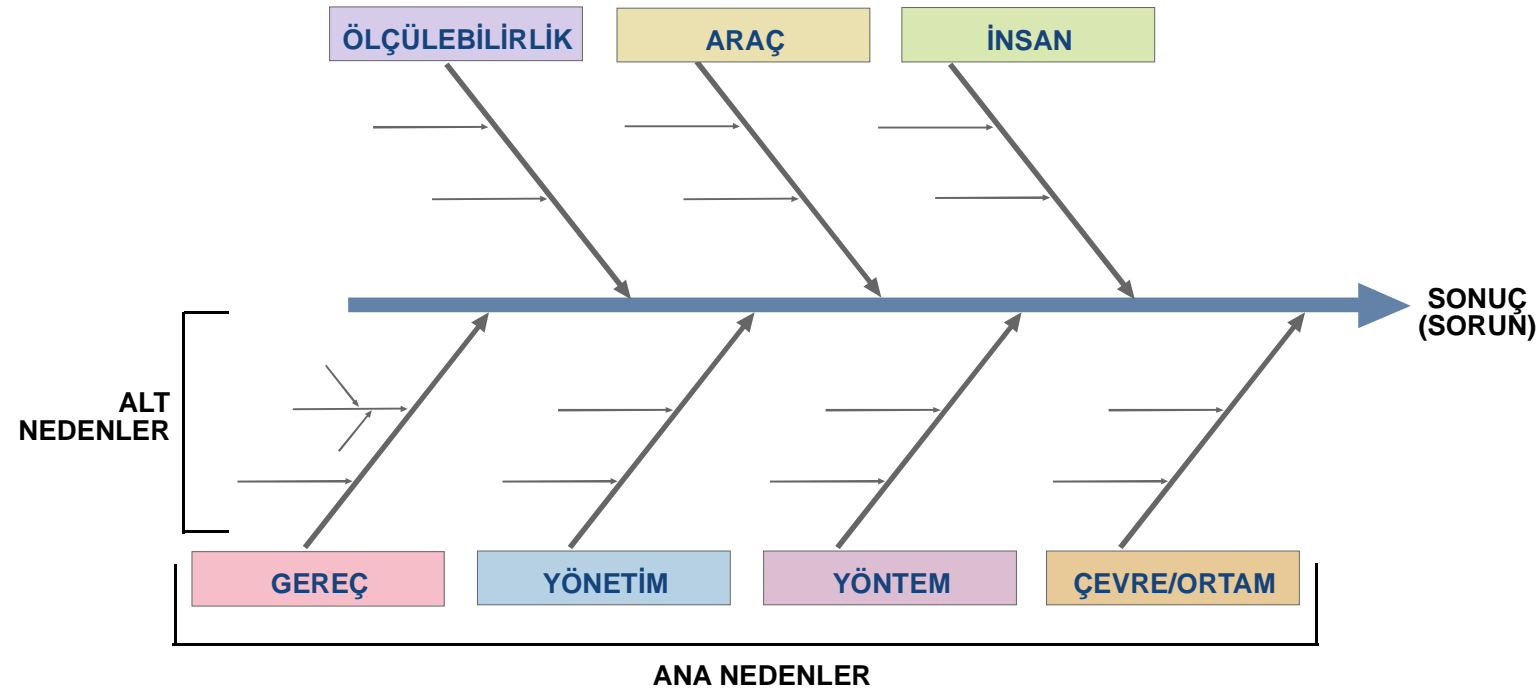
Neden-Sonuç Çizelgesinin Yararları:

- ▶ Sorunların üzerine giden etkin bir yöntemi geliştirir.
- ▶ Çizelgenin hazırlanması, iletişimi güçlendirir. Herkesin dikkatini bir noktaya toplamasını sağlar.
- ▶ Başlı başına eğitici bir çalışmadır, herkesin bilgisini geliştirir.
- ▶ Verilerin toplanmasını ve konuya bilimsel yaklaşılmasını sağlar.
- ▶ Konuya hakimiyeti sınamak için oldukça iyi bir yöntemdir.
- ▶ Tüm sorunlara uygulanabilir.

Neden-Sonuç Çizelgesi Uygulaması Nasıl Yapılır:

- ▶ Sorunu gösteren bir ok (ana kılıç) çizilir.
- ▶ Bu kılıçın üzerinde, sorunun olası ana nedenleri oklarla gösterilir. Bir üretim sürecinde en çok kullanılan ana neden sınıfları, araç, gereç, metot ve insandır. Bir hizmet sürecinde ise bu sınıflar genellikle politikalar, yönergeler, işyeri, araç ve insan şeklinde seçilir. Her iki durumda, çevre (binalar, lojistik ve alan) ve ölçme (kalibrasyon ve veri toplama) sınıfları da sık sık kullanılır. Ayrıca, bu tür sınıflar yerine, sözkonusu sürecin ana basamakları da kullanılabilir.
- ▶ Her bir ana sınıfla ilgili alt etmenler oklar ile gösterilir.

Şekil 3'te Neden-Sonuç çizelgesi verilmiştir.



Şekil 3. Neden-sonuç çizelgesi.

10.4. Kuvvet-Alan Analizi

Kuvvet-alan analizi, yapılan veya yapılacak değişiklikleri ve var olan durumla ilgili itici ve engelleyici etmenlerin gösterir. İstenen değişikliğin tüm yönlerinin görülmesini sağlar. Bir amaca doğru ilerleme veya iyileştirme için iki yol izlenebilir:

- Başarımı arttırıcı kuvvetleri güçlendirmek,
- Başarımı kötüye iten kuvvetleri zayıflatmak veya ortadan kaldırmaktır.

Kuvvet-alan analizi bu kuvvetlerin iki türünü de belirlemeye dayanır.

Kuvvet Alan Analizinin Kullanım Amaçları:

- ▶ İyileştirme fırsatlarını belirlemek.
- ▶ Düzeltildiğinde bir sorunun çözümüne olumlu katkısı olabilecek temel sebepleri belirlemek.
- ▶ Yeni bir program veya önerilen bir iyileştirmenin, gerçekten beklenen yararları sağlama olasılığını değerlendirmek.
- ▶ Engelleyici kuvvetleri yok etmek ve itici kuvvetleri desteklemek için gerçekçi bir uygulama planı oluşturmak.

Kuvvet Alan Analizinde İzlenecek Yöntem:

- ▶ İlk olarak, başarımı etkileyen itici kuvvetler ve sonra da engelleyici kuvvetler beyin fırtınası yoluyla belirlenir.
- ▶ Önerilen iyileştirme açık bir şekilde tanımlanır ve bu bir hedef cümlesi şeklinde yazılır.
- ▶ Büyük bir kağıdın üstüne, hedefe ilişkin başarımlar düzeyini gösteren düz bir çizgi çizilir.

- ▶ Var olan başarımlar düzeyi, kağıdın ortasına çizilen dikey bir çizgi ile gösterilir.
- ▶ Listeler, yalnızca amaca ulaşmada en etkin kuvvetleri göstermek üzere kısaltılır. Grup üyelerinin gerçekten güçlendirebileceklerini düşündüğü üç veya dört itici kuvvet belirlenir. Aynı şekilde, gerçekten zayıflatılabileceği düşünülen üç veya dört engelleyici kuvvet belirlenir.

Kuvvet-alan analizine bir örnek Şekil 4'te verilmiştir.



Şekil 4. Öğrenci başarısının artırılmasına yönelik kuvvet alan analizi.

10.5. Pareto Analizi

Sorun çözme çalışmasının başlangıç noktasını seçmek veya bir sorunun temel nedenini belirlemek için, sorun ya da koşulların tümünün önemini göstermek amacıyla kullanılan çizgisel bir araçtır. Sonuçların büyük bir çoğunluğunun, sebeplerin küçük bir yüzdesi yüzünden ortaya çıktığını savunan bir kavramdır. 80/20 kuralı olarak bilinir. Oluşan sorunların %80'inin, olası nedenlerin %20'si tarafından olduğu ilkesini savunur.

Kalite sorunlarının büyük kısmını çözmek için hata kaynaklarının en önemlilerini ortadan kaldırmak yetmektedir. Bundan dolayı sorunların önce ölçülmesi gereklidir.

Beyin fırtınası sonucu belirlenen önceliklere ilişkin oylama sonuçlarının bir pareto çizelgesine dönüştürülmesi mümkündür. Pareto çizelgelerinde, en önemli ya da en sık görünen probleme (sebebe) ait sütun, çizelgenin en solunda gösterilir. Amaç, kullanıcının dikkatini bu sütun üzerine çekmek ve zaman kaybını en aza indirmektir.

Pareto Analizinin Kullanım Amaçları:

- ▶ Sorunların ya da bu sorunların ortaya çıkış nedenlerinin arasında en önemlilerinin görsel olarak belirlenip değerlendirilmesi.
- ▶ Hangi problemler üzerinde durulması gerektiği kararının verilmesi.
- ▶ Değişen zaman içinde başarımlar değişimlerinin gözlenmesi.

Pareto Analizinde İzlenecek Yöntem:

- ▶ Veri toplamak için bir zaman dilimi belirlenir.
- ▶ İstenen veriler toplanır ve yoklama kağıtlarına yazılır.
- ▶ Bu veriler, azalan puan sırasına sınıflandırılarak özetlenir.
- ▶ Çıkarılan sonuçlar soldan sağa azalacak biçimde Pareto çizelgesine yerleştirilir. Çizelgenin dikey eksenini yüzdelere ya da sıklığı, yatay eksenini ise oluşturulan sınıfların (sorun ya da nedenlerin) adlarını göstermelidir.
- ▶ Çizelgenin sağ dik ekseninde toplam yüzde gösterilir.
- ▶ Her sütun bir solundaki sütunun üstüne eklenerek, her sütunun üstündeki toplam yüzde belirlenip, bu yüzdelere sağ ekseninde belirtilir.
- ▶ Çizelgenin adı verilir.
- ▶ Çizelge zaman içinde toplanan yeni verilerle değiştirilir ve önceki çizelge ile farklar değerlendirilir.

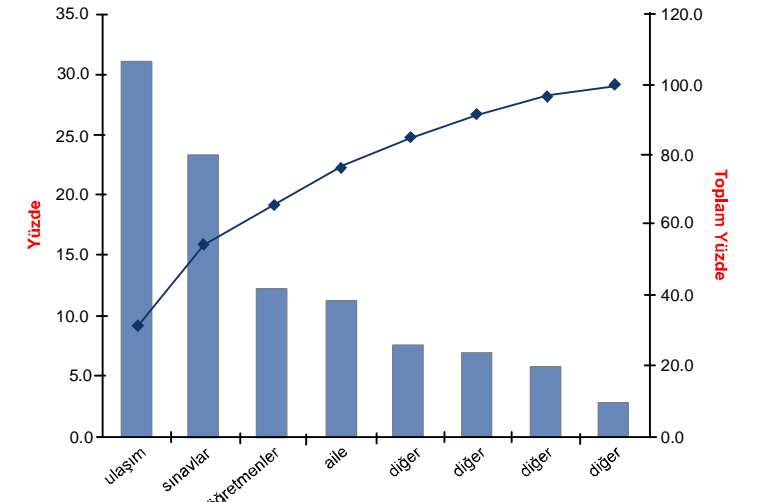
Pareto analizine bir örnek Şekil 5'te verilmiştir.

10.6. Yoklama Kağıtları

Veri kaydetmeyi kolaylaştıran bir çizelge veya tablodur. Bir gözlemi, eylemi veya gerçekleşmeyi yansıtmak için bir "✓" veya "/" işareti koymak yeterlidir.

Kullanım Amaçları:

- ▶ Başarımı ve tartışmayı güçlendirmek.
- ▶ Temel nedenleri araştırmak.



Şekil 5. Öğrenci devamsızlığı ile ilgili Pareto analizi.

- ▶ Bir çözümün veya iyileştirmenin sonuçlarını ölçmek.
- ▶ Başarımı izlemek. (Önceki sorunların tekrar ortaya çıkıp çıkmadığını yoklamak.)

Yoklama Kağıtları Nerelerde Kullanılır:

- ▶ Hatalı yerleri belirlemede.
- ▶ Hataların zamana, operatöre, makineye vs. göre dağılımını bulmada.
- ▶ Boyutlar, sertlik, ağırlık vb. nin dağılımını bulmada.
- ▶ Araç ve gereçleri gözden geçirme ve işlerliğini yoklamada.


10.7. Altı Şapkalı Düşünme Yöntemi


Düşünce ve önerilerin belirli bir düzen içinde sunulması için kullanılan bir yöntemdir. "Şapkalar", düşüncelerin ayrıştırılması için kullanılan bir semboldür. Şapkaların rengi değiştiğinde, düşünceler rengin simgelediği düzen içerisinde ortaya konur.

Altı Şapkalı Düşünme Yönteminin Üstünlükleri

- ▶ Bir konu üzerinde daldan dala atılarak belirtilen görüşler bir düzene sokulmuş olur.
- ▶ Gereksiz zaman kaybı önlenir.
- ▶ Bir karara varma ve sonuçların ortaya çıkması kolaylaşır.

Altı Şapkalı Düşünme Tekniği nasıl uygulanır:

 **Beyaz (Tarafsız) Şapka** (Kesin bilgileri simgeler): Görüşülen konu ile ilgili kesin bilgiler, sayılar, araştırmalar, kanıtlanmış veriler ortaya konur.

 **Kırmızı (Duygusal) Şapka** (Duyguları simgeler): Görüşülen konu ile ilgili olarak, kişilere hiçbir dayanağı olmadan duygularını söyleme şansı verir.



Siyah (Kötümser) Şapka (Tehlikeleri simgeler):

Görüşülen konunun riskleri, gelecekte doğuracağı sorunlar, eleştiriler ortaya konur.



Sarı (İyimser) Şapka (Üstünlükleri simgeler):

O işin üstünlükleri ortaya konulur. Getirileri göz önüne alınır.



Yeşil (Yenilikçi) Şapka (Yaratıcılığı simgeler):

Konuyla ilgili değişik seçenekler araştırılır. Yaratıcılık öne çıkarılır ve toplantıya katılanların yaratıcı olmaları özendirilir. Önemli olan, görüşün saçma olup olmaması değil, orijinal, yeni, üretken olmasıdır.



Mavi (Serinkanlı) Şapka (Sonuçları simgeler):

Düşünceler düzene konur. Toplantıda varılan sonuçlar ortaya çıkarılır, durum analizi yapılır ve özetlenir.

10.8. Histogram

Histogram, ölçülebilir bir nitelik ile ilgili gözlem değerlerinin dağılımını gösteren bir çubuk grafiğidir.

Kullanım Amaçları:

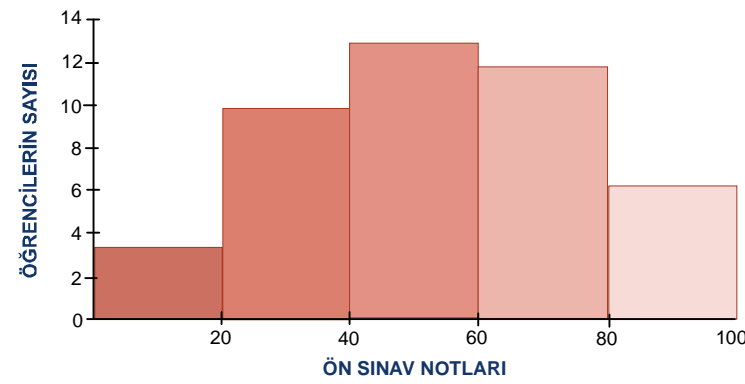
- Süreçlerin yapısında olan değişkenliği anlamak. (Tutarlı bir şekilde kabul edilebilir sonuçlar alabilmek için değişkenlik azaltılmalıdır.)
- Süreçlerin yapısı, sorunların kaynağı hakkında kavramlar geliştirmek ve bunları sınamak.

Histogram Yönteminin Uygulanması:

- Veriler elde edilir; toplam veri sayısı belirlenir.
- Veriler artan sırada dizilir.
- En küçük veri en büyük veriden çıkarılarak, elde edilen verilerin yayıldığı aralığın genişliği belirlenir.
- Histogramda kullanılacak sütun sayısı belirlenir. (En az 6, en fazla 20 sütun önerilir). Yayılım aralığı bu sayıya bölünerek her çubuğun (sınıfın) eni hesaplanır.
- Yatay x eksenine üzerine veri sınıfları yazılır. Frekans ölçeği (sayılar veya yüzdeler) dikey y eksenine üzerine yazılır.
- Her bir sınıf için, o sınıfın içerdiği verilerin toplam sayısı veya bu sayının toplam veri sayısı ile orantılı dikey bir çubuk çizilir.
- Her eksen dikkatlice isimlendirilir; histograma isim verilir; verilerin toplandığı dönem yazılır.
- Ortalama, varyans gibi değerler hesaplanır.

Histograma bir örnek Şekil 6'da verilmiştir.

Bilal KILIÇ



Şekil 6. Öğrenci notları ile ilgili histogram.

Sonuç

1960'lı yıllarda Japonya' da ortaya çıkan ve 25 yıl içerisinde tüm dünyayı saran kalite çemberi anlayışı, işletmelerin ürün ve hizmet kalitelerini artırmakla kalmayıp, işletmelerde çalışanların iletişimini ve gayretini artırarak, işletmeleri daha kazançlı ve daha verimli hale getirmiştir.

Gelişen teknolojiyle birlikte iş dünyasında, sanayide, okullarda, üniversitelerde, hastanelerde ve hizmet sektöründe kullanımı hızla artan kalite çemberleri, çalışanların özgüvenlerini önemli ölçüde artırmış, iş verimliliğini azaltan sorunları etkin bir biçimde çözebilecek düzeye ulaşmış ve birçok şirkette de önemli kazanımlar sağlamıştır. İşletmelerin ve çalışanların başarımını artırmış, ülkeyi ekonomik ve teknolojik açıdan geliştiren bir itici gücü oluşturmuştur.

1960'lı yıllarda Japonya' da ortaya çıkan ve 25 yıl içerisinde tüm dünyayı saran kalite çemberi anlayışı, işletmelerin ürün ve hizmet kalitelerini artırmakla kalmayıp, işletmelerde çalışanların iletişimini ve gayretini artırarak, işletmeleri daha kazançlı ve daha verimli hale getirmiştir.

Bir işletmede kalite çemberlerini uygulamak için uygun ortamın olup olmadığını belirlemek gerekir. Uygun ortamın bulunmadığı veya oluşturulamadığı bir işletmede yapılacak girişimler başarısız olacaktır.

Kalite çemberleri bir ekip çalışması ruhunu barındırdığı için verim katlanarak artar ve çember üyeleri, sorunları, nedenleri belirleme ve analiz etme yoluyla önlemler alarak, yeni yönergeler oluşturabilir.

Kalite Çemberleri ve Sorun Çözme Yöntemleri

KAYNAKÇA

- [1] R. Aguaya, *Dr.Deming: Japonlara Kaliteyi Öğreten Amerikalı, Japon Mucizesinin Mimarı*, Form Yayınları, İstanbul, 2004.
- [2] R. Bozkurt, C. Eşit, *Kalite Çemberleri*, MPM Yayınları, No:662, 2.Basım, Ankara, 2003.
- [3] C. Çetin, B. Akın, V. Erol, *Toplam Kalite Yönetimi ve Kalite Güvence Sistemi (ISO 9000:2000 Revizyonu)*, Beta Yayınları, 2.Baskı, İstanbul, Şubat 2001.
- [4] G. M. Dengiz, *Takım Çalışması Teknikleri*, Academy Plus Yayınevi, 1.Baskı, Ankara, Ekim 2002.
- [5] İ. Efil, *Yönetimde Kalite Çemberleri ve Uygulama Örnekleri*, Alfa Yayınları, 5.Baskı, İstanbul, Ekim 1999.
- [6] T. Keçecioglu, *Takım Kimyası ve Mimarisi*, Literatür Yayıncılık, 1.Basım, İstanbul, Ekim 2002.
- [7] A. Kovancı, *Toplam Kalite Yönetim: Fakat Nasıl?*, Sistem Yayınları, İstanbul, Haziran 2001.
- [8] C. J. Maxwell, *Liderlik Nitelikleri*, Beyaz Yayınları, Çev.İbrahim ŞENER, 1.Basım, İstanbul, Kasım 1999.
- [9] N. Mungan, *Liderlik ve Takım Kurma*, Mühendis Makina Dergisi, Cilt 37, Sayı 442, Kasım 1996.
- [10] H. Müftüler, *Kalite Çemberleri Uygulama El Kitabı*, İstanbul, 1994.
- [11] M. Şimşek, *Kaizen'in İlk Basamağı: Kalite Çemberleri*, Mühendis Makina Dergisi, Cilt 37, Sayı 447, Kasım 1996.
- [12] İsmail Efil, *Yönetimde Kalite Çemberleri ve Uygulama Örnekleri*, ALFA Yayınları, Ekim 1999.
- [13] Timur T. Göksel, *Grup Halinde Problem Çözme Metodu*, Enstitü-DW, Bursa, 1992.
- [14] Nurdoğan Arkış, *Yönetim Bilim Açısından Sorun Çözme Grupları ve Türkiye'deki Bazı Uygulamalar*, MPM Yayınları, Ankara, 1985.
- [15] Nurdoğan Arkış, *Grup Davranışlarının Organizasyon Açısından Önemi ve Kalite Kontrol Grupları Semineri*, MPM Yayınları, Ankara, 1985.
- [16] Ülkü Dicle, *Kalite Kontrol Çevrimleri*, SEGEM, Ankara, Mart 1984.



YIL 2011;
PARDUS

**HEM 2011,
HEM KURUMSAL**

Koray LÖKER

TÜBİTAK BİLGEM bünyesinde geliştirilen ulusal işletim sistemi PARDUS, 2011 yılına ürün ailesine iki yeni kararlı sürüm ekleyerek girdi. Tüm dünyada ilgiyle karşılanan, masaüstü kullanımı, teknoloji meraklıları, ev tipi kullanıcılar için hızlı, albenili, birçok yeni özellik içeren PARDUS 2011 ve kurumsal bilişim altyapılarına yönelik özellikleriyle, özellikle KOBİ'ler ve özgün bilişim çözümlerine yönelen kurumlar tarafından bir süredir beklenen PARDUS Kurumsal 2.

PARDUS 2009'un tüm dünyada düzenlenen bir ankette en iyi beş Linux tabanlı işletim sisteminden biri olarak seçilmesinin ardından yeni ürünler, TÜBİTAK BİLGEM kalitesi ve gücünü gözler önüne sermeye devam ediyor.

Yeni başlayanlar için PARDUS: Ulusal İşletim Sisteminin doğuşu

PARDUS projesi, 2003 yılında, artık TÜBİTAK BİLGEM'e bağlanmış olan BİLGEM çatısı altında, bir olurluk ve planlama projesi olarak başladı. Ulusal bağımsızlık, güvenlik ve tasarruf amacıyla, kritik uygulamaların üzerinde çalışabileceği, açık ve standart bir veri yapısını destekleyen, güvenlik izlemesine imkan verecek şekilde kaynak kodu açık olan ve finansal yük oluşturmadan yaygınlaştırılabilecek bir işletim sistemi geliştirmek üzere harekete geçildi. 2003 yılı güzünde Linux temelli, açık kaynaklı, GPL lisanslama yöntemini kullanan bir işletim sistemi dağıtımını oluşturulmasına karar verildi.

2004 yılı başında çekirdek teknik ekibin oluşturulması ile proje fiilen başlamış oldu. Farklı Linux dağıtımlarının incelenmesi, mevcut dağıtımlardaki eksikliklerin, olası gelişim alanlarının, yapılması gerekenlerin ve bunların iş gücü ve kaynak gereksinimlerinin irdelenmesinin ardından yol haritası belirlendi.

1 Şubat 2005 tarihinde ilk ürün olan PARDUS Çalışan CD 1.0 yayımlandı. Projenin amaçları ve teknik yaklaşımı hakkında Linux camiası ve kullanıcıları bilgilendirmeyi amaçlayan Çalışan CD beklenenin üzerinde ilgi gördü. Sonrasında geliştirme daha çok özgün yenilik projelerine yoğunlaştırıldı ve nihayet 26 Aralık 2005'te PARDUS'un ilk kurulabilir sürümü olan PARDUS 1.0 Web üzerinden yayımlanmaya başladı.

Beş yıl içinde hızlı bir gelişim gösteren PARDUS, 2007 ve 2009 yıllarında yayımlanan kararlı sürümlerinin ardından, 2011 başlarında peş peşe PARDUS 2011 ve Kurumsal 2 kullanıma sunuldu.

PARDUS'u dünya liginde başarıya ulaştıran yenilikler

PARDUS ilk günden bu yana araç temelli ve teknoloji merkezli bir tasarımla, kolay kullanılır, güvenli ve yüksek performanslı bir altyapı sunmayı hedefliyor. Bugüne dek sunulan tüm ürünler, hazırlandıkları günlerin teknoloji ve beklentileri doğrultusunda bu yaklaşımın devamını sağlayacak güncellemeler içeriyor.

TÜBİTAK bünyesinde geliştirilen yönetim araçları PARDUS 2011'de neredeyse baştan tasarlandı. Kullanıcı grafik arayüzlerinde yapılan yenilikler kullanım kolaylığı ve ciddi performans artışı sağladı. Böylece, kullanıcı hesapları, sistem ayarları ya da güvenlik duvarı ayarlamak isteyen PARDUS kullanıcıları eskisinden de rahat olabilecekler. Özellikle başka işletim sistemlerinden sonra PARDUS'u yeni kullanmaya başlayanlar için bu geçişi kolaylaştırmak için daha sezgisel tasarımlar yapılmaya çalışıldı.

PARDUS Kurumsal 2

Kullanıcılar hep en yeni teknolojileri isterler. Yazılım geliştirmenin bir gereği de dünyadaki gelişmeleri yakından takip etmektir. Bu veriler ışığında PARDUS 2011 en yeni teknolojilerle donatılmış olarak geliyor.

Öte yandan kurumlar, yenilikten daha çok kararlılık, güvenilirlik bekliyor. Üstelik sadece teknolojide değil, ürün politikalarında da... Bu beklentileri daha iyi karşılamak üzere, PARDUS ailesine Kurumsal 2 de katıldı.

PARDUS Kurumsal 2, 1.0 sürümünden itibaren PARDUS kullanan kurumların (MSB-ASAL, RTÜK, çeşitli hastane ve üniversiteler) geri dönüşleri ve beklentileri ışığında, kurumsal altyapılara uygun özellikleri barındırıyor.

Yıllardır sağlamlığını ispat eden KDE 3 ailesini masaüstü ortamı olarak seçen Kurumsal 2, sunucu servislerine yönelik geniş uygulama desteğine karşın son kullanıcıyı hedefleyen uygulamalarda seçenek çokluğu yerine kararlılığı hedefleyen bir uygulama deposu sunuyor. Bireysel (2011 gibi) sürümlere kıyasla çok daha sert kurullarla, güvenlik öncelikli güncellemelerle sürdürülen depo ve altyapının üç yıl boyunca PARDUS ekibi tarafından destekleneceği Uzun Dönem Destek (LTS) garantisi de yeni özellikler arasında.

PARDUS Kurumsal 2, altyapısında ulusal işletim sistemini tercih etmek isteyen her ölçekte kurum için, üzerinde stratejik planlar yapmaya her zamankinden daha uygun.

Üniversite - TÜBİTAK işbirliği modelinde yeni başarı öyküleri

Bir işlemleri gerçekleştirmek isteyen kullanıcının, aklına ilk gelen yöntemi denediğinde başarılı olabildiğini hedefleyen sezgisel tasarım yaklaşımı, bir eğitim almadan PARDUS kullanmayı mümkün hale getiriyor. Tasarımların bu yaklaşıma göre iyileştirilmeleri ve daha basit hale getirilerek kolay kullanılabilir olmaları için Bahçeşehir Üniversitesi Görsel İletişim Tasarımı bölümüyle başlayan çalışmalar sürüyor. PARDUS 2011, ortaya çıkan fikirlerin ancak bir bölümünü hayata geçiriyor. Kullanıcılar da yaşadıkları sorunları PARDUS Hata Takip Sistemine rapor ederek ürünü geri bildirimlerle iyileştiriyor.

PARDUS'ta bir başka işbirliği de geçtiğimiz yıl Çanakkale 18 Mart Üniversitesi'yle gerçekleşti. PARDUS 2011'de 64 bit ve 32 bit olmak üzere iki ayrı işlemci, kendi olanaklarına uygun derlenmiş sistemler çalıştırarak daha yüksek verim sunuyor. Bunu sağlayan 64 bit altyapı, 18 Mart Üniversitesi Bilgisayar Mühendisliği bölümü öğrencileri tarafından geliştirildi. Projeyi hayata geçiren üç çiçeği burnunda mühendis ise artık birer BİLGEM çalışanı.



İlk başarının yarattığı olumlu rüzgârla, bu sene de aynı danışman öğretim görevlisi liderliğinde, Çanakkale 18 Mart Üniversitesinde yeni öğrenci arkadaşlar farklı masaüstü ortamlarının PARDUS'a entegre edilmesi çalışmasını yürütmeye başladı. Haziran ayında hem TÜBİTAK BİLGEM dâhilinde geliştirilmiş olan yönetim araçları ve teknolojileri daha gelişmiş olacak hem de daha geniş bir masaüstü dünyası seçenekleri kullanıcılara sunulacak.

Kullanıcı beklentilerine en iyi cevap veren işletim sistemi: PARDUS

Bilişim teknolojilerinin hızlı ilerlemesi, kullanıcıların bilgisayarlarından beklentilerini değiştiriyor. PARDUS 2011, kullanıcılardan gelen onlarca isteği hayata geçiren bir sürüm olmayı da başardı. Bu yenilikler arasında göze çarpanlar:

Tak-çalıştır 3G desteği

PARDUS 2011'de önceki sürümlerde kullanılan ağ yöneticisi yerine yeni bir özgür projeden yararlanıldı. Yeni ağ yöneticisi de, daha önceki sürümlerde olduğu gibi otomatik ayarlanan kablolu bağlantı, tek tuşla mekan hafızalı kablosuz bağlantı gibi özellikleri destekliyor. Bunun yanında kablosuz ağlar ile aynı kolaylıkta kullanılabilir 3G bağlantı desteğine sahip. Böylece USB modem çubukları ya da cep telefonlarıyla İnternet bağlantısı kurmak isteyen kullanıcılar karmaşık kurulum ve yapılandırmalar ile uğraşmak zorunda kalmıyor.

Profil fotoğrafınız: Kaptan Masaüstü

Sosyal medyanın hayatımızdaki önemi artarken, sohbet programlarından, e-posta uygulamalarına her yerde profil fotoğrafı kullanılıyor. Kullanıcılar, PARDUS'u ilk çalıştırdıklarında kişisel ayarlarını yapmaya yardımcı olan Kaptan Masaüstü ile tanışıyorlar. PARDUS 2011'de Kaptan profil fotoğrafçılığına soyunuyor ve bilgisayara bağlı bir kamera varsa fotoğraf çekerek profil fotoğrafı olarak kaydediyor. Eğer herhangi bir kamera yoksa sabit diskteki albümlerden seçmek de mümkün.

Anadolu Parsı

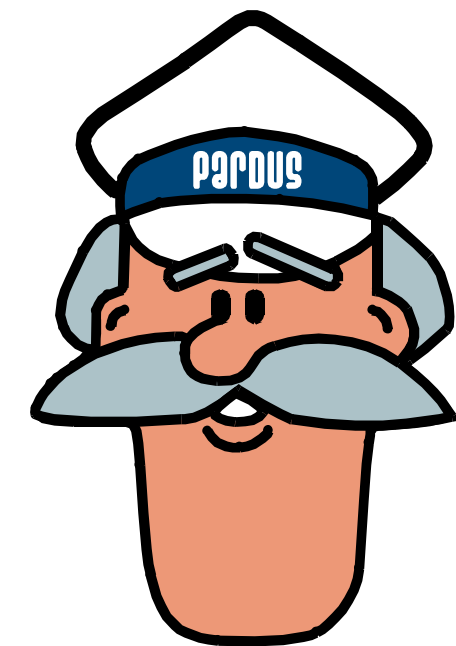
Anadolu Parsı (Panthera pardus tulliana) leopar alt türündeki büyük kedilerin Anadolu'daki son temsilcilerinden biri. Boyu 2-2.5 metreyi, ağırlığı dişilerde 35-50 kilogram, erkeklerde 45-70 kilogramı buluyor. Yaklaşık ömrü 20 yıldır. Çevik ve etobur bir hayvan olan Anadolu parsının avını geyik, yaban keçisi, yaban domuzu, küçük memeliler ve kuşlar gibi birçok hayvan oluşturuyor. Anadolu parsının Ege ve Batı Akdeniz, Doğu Akdeniz ve Doğu Anadolu bölgelerinde, daha çok ormanlık ve dağlık alanlarda yaşadığı biliniyor. Doğal yaşam alanları ve av kaynaklarının azalması parsaları insanların yaşadığı yerlere yönlendirdi ve bu da genellikle vurularak ya da zehirlenerek öldürülmelerine yol açtı. Anadolu parsının varlığını kanıtlamak ve koruma altına almak için doğa gönüllülerinin çabaları aralıksız olarak sürüyor.

Daha özgür, daha serbest

Özellikle oyun dünyasının iyi tanınan 3B destekli ekran kartları PARDUS gibi Linux sistemler için özel sürücüler yayınlıyor. Bununla birlikte, özgür yazılım dünyasının bu kartlar için hazırladığı özgür sürücüler de mevcut. Her birinin ayrı avantaj ve dezavantajları olan bu sürücüler, kullanım sırasında ayarlanabiliyor ancak kurulum sırasında PARDUS sizin yerinize bu kararı veriyordu. Kullanıcılardan gelen talep doğrultusunda, PARDUS 2011 kurulum sırasında ekran kartını hangi sürücü ile çalıştırması gerektiğini sormaya başladı.

Disk yönetiminde yeni nesil teknolojiler

PARDUS'un kolayca kurulmasını sağlayan kurulum sihirbazı YALL, yine kullanıcı istekleri doğrultusunda kullanıcıların elle kimlik numarası (UUID) seçebilmelerini ve disk bölümleri için Linux Mantıksal Hacim Yönetimi (LVM) ve RAID teknolojileri kullanabilmelerini sağlıyor.



Kaptan Masaüstü

“Daha fazla özgürlük” diyenlerin buluşma noktası: Özgürlükİçin.com

PARDUS'un daha fazla kullanıcıya ulaşmak ve sesini yükseltmek için kurduğu bir topluluk sitesi olan Özgürlükİçin.com'un kullanımı giderek artıyor.

Özgürlükİçin.com'da, PARDUS ailesine yeni katılan kullanıcılara yardımcı olmak amacıyla, genellikle geliştiriciler ve deneyimli PARDUS kullanıcıları tarafından kaleme alınan paket tanıtımı, inceleme yazıları ve kullanım kılavuzlarını da içeren zengin bir içerik sunuluyor. Site yeni kullanıcıların özgür yazılıma geçişini kolaylaştırmayı hedefliyor.

Özgürlükİçin.com'da “Ajans PARDUS” adlı online yayını da ziyaretçilerden büyük ilgi görüyor. 2010 yılı Nisan ayından bu yana her cumartesi güncellenen yayında özgür yazılım dünyasından ve PARDUS'tan gelişmelere ve röportajlara yer veriliyor.

En yeni uygulamalar, yeni teknolojilerle

PARDUS'un ilk günlerinde piyasada kullanılan teknolojiler incelenerek yapılan değerlendirme sonucu, kullanıcıların sistemlerine yeni programlar eklemesi ya da güncelleme yapmalarını kolaylaştırmak için en baştan bir sistem oluşturmanın uygun olduğu kararlaştırılmıştı. Bu karar doğrultusunda hayat bulan paket yöneticisi PiSi, alanında uzman birçok yazılım mühendisi tarafından incelenerek takdirle karşılanmış ve en doğru çözümler arasında listelenmişti

Yakın zamanda cep telefonları ve tabletler sayesinde mobil işletim sistemlerinin önemi arttıkça PiSi benzeri çözümler daha çok tanınmaya, masaüstü işletim sistemlerinde de tercih edilmeye başlandı. PARDUS, tek tuşla uygulama kurmayı ve yenilikleri yönetmeyi yıllardır kullandığı için yine kullanıcı talepleri ön plana çıktı ve paket yöneticisi arayüzünde kurulabilir durumdaki programların ekran görüntüleri ve diğer kullanıcıların verdiği oyların görülebildiği bir vitrin devreye sokuldu. Böylece programları kurmadan önce haklarında daha çok fikir sahibi olmak mümkün olabiliyor.

PiSi ile ulaşılabilen depolar ise en güncel ve popüler uygulamalarla dolu. Skype, VLC, Google Chrome, Mozilla Firefox ya da OpenOffice.org temel alınarak geliştirilen LibreOffice gibi her platformda tanınan ve sevilen programların yanında Linux dünyasına ya da PARDUS'a özgü 3000'den fazla paket tek tuşla kurulabilir durumda bekliyor. Bu programların seçilen bir bölümü DVD içinde kurularak çalışmaya hazır bir sistem sunuyor.

Kolay Kurulum

PARDUS kurulumunu, temel bilgisayar bilgisine sahip kullanıcılar için bile çok kolay hale getiren kurulum sihirbazı YALI da bu sürümde baştan aşağı yenilendi.

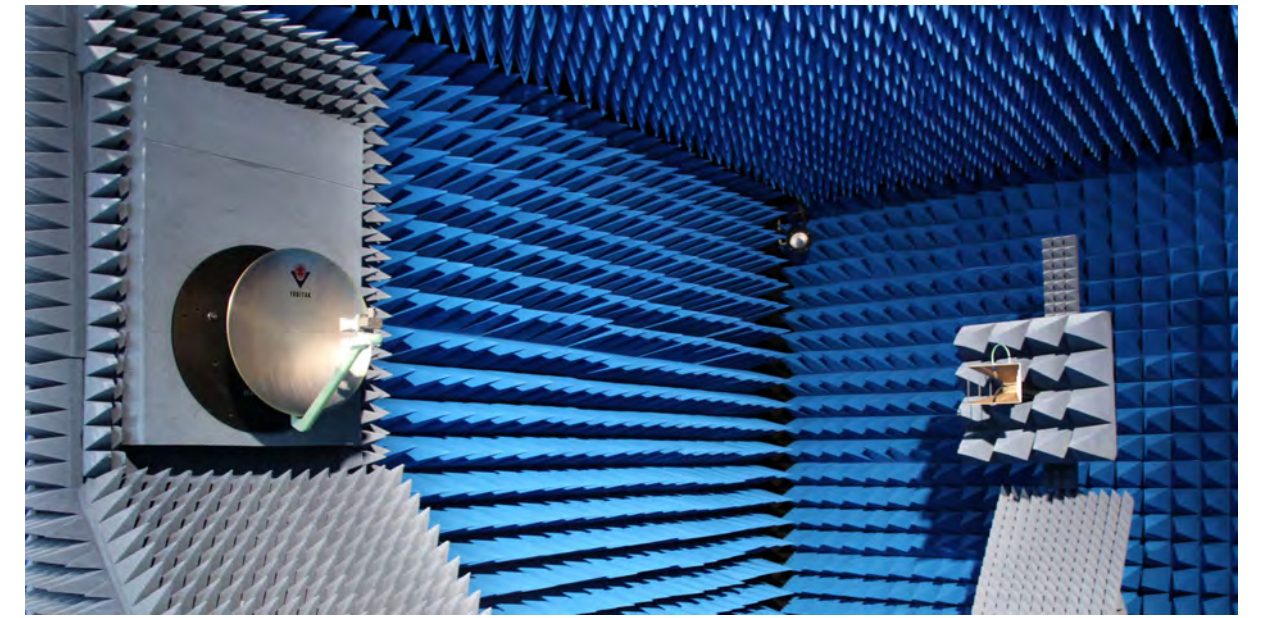
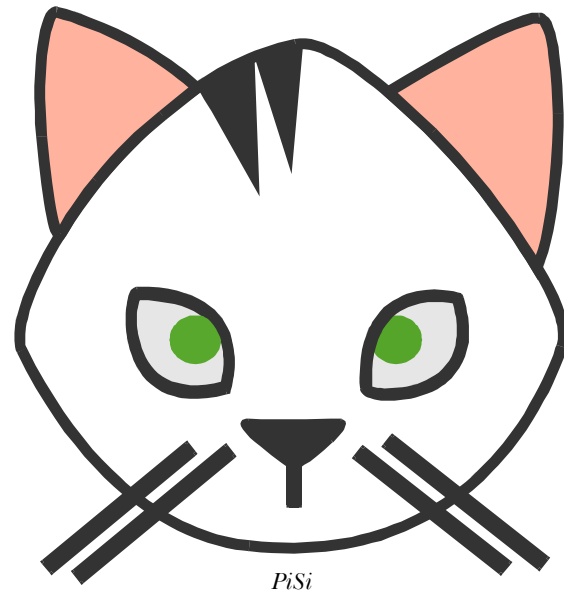
Bilgisayarınızı DVD'den başlattığınızda YALI sizi yönlendirerek bilgisayarınıza kurulumu gerçekleştirecek. Bilgisayarın DVD'den başlatılması için yeni bilgisayarlarda F5-F6 gibi fonksiyon tuşlarından biri, tek seferlik olarak bu sırayı değiştirmenizi sağlar. Alternatif olarak BIOS'u da açılış diskleri sırasını değiştirmeniz gerekebilir.

YALI başladıktan sonra klavye, zaman dilimi gibi bilgisayarı kullanan herkes için ortak olan bilgileri sorduktan sonra kurulum yapılacak sabit disk seçilir.

DİKKAT: Bilgisayarında başka bir işletim sistemi bulunan ve iki sistemi aynı anda kullanmak isteyen kullanıcılar burada “Kendi Düzenini Yarat” seçeneği seçmelidir. “Diskin Tamamını Kullan” seçeneği, mevcut işletim sistemini ve dosyalarınızı siler.

Eğer PARDUS kurmaya ayırdığınız bir disk bölümü varsa, “Kendi Düzenini Yarat” seçeneğinde karşınıza çıkacak olan disk bölümü tablosunda büyüklüğünden tanıyarak bu alanı seçebilir ve Sistem Dosyaları için atayabilirsiniz. Temel bir kurulum için bu yeterli olacaktır. Eğer kullanıcı dosyalarını ayrı bir disk bölümünde saklamak ya da gelişmiş özelliklerden yararlanmak isterseniz, PARDUS'un web sitesi ya da kullanıcı topluluğunun bir araya geldiği Özgürlükİçin.com adresindeki yardım belgelerinden yararlanabilirsiniz.

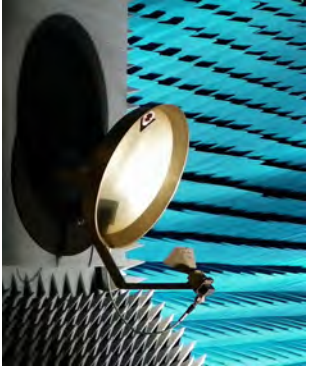
Güle güle kullanın!



Küresel Yakın Alan Ölçüm Laboratuvarı

Türkiye'nin en büyük kapalı ortam ölçüm ve anten araştırma faaliyetlerinin yürütüldüğü, Anten Test ve Araştırma Merkezi (ATAM) kompleksinin ilk sistemi “Küresel Yakın Alan Ölçüm Laboratuvarı” hizmete girdi.

Yansımaz Oda	
<i>Boyutları</i>	7.5x4.7x3.3 m (BxExY)
<i>Soğurucular</i>	2 kW / m ²
Test Edilen Anten	
<i>Ağırlığı (max)</i>	95 kg
<i>Boyutu (max)</i>	1.8 m
Ölçüm Sistemi	
<i>Çözünürlüğü</i>	0.01° Phi ve Theta
<i>Pozisyon Tekrarlanabilirliği</i>	0.03°
<i>Dönme Hızı (Theta ve Phi)</i>	10°/sec Theta, 20°/sec Phi
<i>Hizalama Kabiliyeti</i>	Otomatik, Elektronik
<i>Tarama Kabiliyeti</i>	360°
<i>Frekans Aralığı</i>	0.75 - 20 GHz
<i>Ölçüm</i>	Uzak Alan, Yakın Alan, Holografik



Ülkemizin askeri ve sivil anten ihtiyaçlarına milli gözlemler üretiyoruz.

Geliştirdiğimiz antenleri artık daha hassas ölçüyoruz.

FIBEROPTİK
KABLO
DENETİM
SİSTEMİ

FKDS

Taner DURSUN

1.1. Giriş

F/O (Fiberoptik) kablolar, yüksek band genişliği sağladığı için telekomünikasyon alanında giderek daha çok kullanılmaktadır. Önceleri, şebeke omurgalarının ana trafik yükünü çeken F/O kablolar, son yıllarda ev kullanıcılarına kadar ulaşmıştır.

Diğer iletim teknolojileri (bakır kablo, kablosuz iletişim, optik) için var olan, güvenlik ve servis kalitesi gibi konulardakis sorunlar, farklı seviyelerde de olsa F/O kablolar için de geçerlidir. F/O kablolar, bilgi sızdırma ve iletişimi kesme amaçlı saldırılar yapılabilmektedir. Ayrıca, çeşitli kazalar sonucu F/O kablolar hasar gördüğünde iletişim sorunları yaşanabilmektedir.

Telekomünikasyon servisi sağlayıcıları gibi sivil kurumlar için iletişim kesintileri önemli sorun iken, askeri ve diğer devlet kurumlarının şebekelerindeki gizliliği korumak daha önemli olmaktadır.

Gelişen teknoloji ile birlikte hizmet kalitesi, hizmeti alanlar açısından önem kazanmakta ve servis sağlayıcılar ile daha somut hizmet kalitesi maddeleri içeren SLA (Service Level Agreement, Bakım Onarım Antlaşması), imzalanmaktadır. Çok iyi hazırlanmış SLA sözleşmeleriyle, F/O şebekenin çalışır durumda tutulması, kesintilere daha hızlı müdahale edilmesi ve kesintiler nedeniyle oluşan SLA ihlallerinin maddi boyutunun doğru hesaplanabilmesinin önemi de gittikçe artmaktadır. Bu nedenle FKDS (F/O Kablo Şebeke Denetim Sistemi) sistemleri geliştirilmeye başlanmıştır. Bu tür sistemler, F/O test cihazları ve onları yöneten yazılımlardan oluşur. Test cihazları koşullandırılarak, F/O şebeke üstünde periyodik testler gerçekleştirilir. Böylece, F/O kablolar üzerindeki yaşlanma, ek yerlerindeki kayıplar ve konnektör sorunlarının, başarımlı düşüklüğüne neden olacak Bit Error Rate (BER) hatasına dönüşmeden belirlenmesi ve hatalar oluşmadan önce bakım yapılarak düzeltilmesi mümkün olur. Dolayısıyla MTTR (Mean Time To Repair, Ortalama Arıza Giderme Zamamı) azaltılarak yüksek hizmet kalitesi sağlanır.

FKDS sistemlerinin kullanılmasıyla birlikte aşağıdaki yararlar sağlanmış olur:

- Kablo yaşlanmaları ve kötü montaj işçiliği nedeniyle oluşabilecek hatalar belirlenerek kesinti olmadan önce düzeltme olanağı sağlanabilir.
- Arızanın olduğu konum gerçeğe yakın zamanda belirlenip müdahale süresi kısaltılarak şebekenin uygunluğu (network availability) artırılır.
- MTTR'nin azalmasıyla hizmet kalitesi artırılmış ve üretilen Arıza İstatistik raporları ile SLA yönetimi kolaylaştırılmış olur.
- Otomatik test yapılandırılmaları, çeşitli formattaki uyarılar (ses, e-posta, sms, vb.) ve görevlerin otomasyonu ile operatörler üzerindeki F/O şebeke yönetim yükü azalır.

• Kablolarla saldırılar belirlenerek şebeke güvenliği artırılmış olur.

• F/O şebeke bilgileri ve arızalar coğrafi koordinatlarla ilişkilendirilerek şebekenin daha anlaşılır bir biçimde yönetilmesi sağlanmış olur.

• Şebekenin sayısal ortamda modellenmesi ile birlikte hem şebeke ile ilgili dokümantasyon yükü azaltılmış, hem de raporlama ve güncelleme kolaylaştırılmış olur.

• F/O şebekede yapılacak değişiklikler için planlamayla ilgili bilgi desteği sağlanmış olur.

F/O pazarında çeşitli FKDS sistemi bulunmakla birlikte, TÜBİTAK BİLGEM bünyesinde de bir FKDS geliştirilmiştir. Kurumun güvenlik alanındaki uzmanlığı nedeniyle geliştirilen ürünü benzerlerinden ayıran önemli özelliklerden birisi sistemin daha yüksek seviyede bir güvenliksağlıyor olmasıdır. Bu sistemin geliştirilme amacı aşağıdaki iki maddede özetlenebilir:

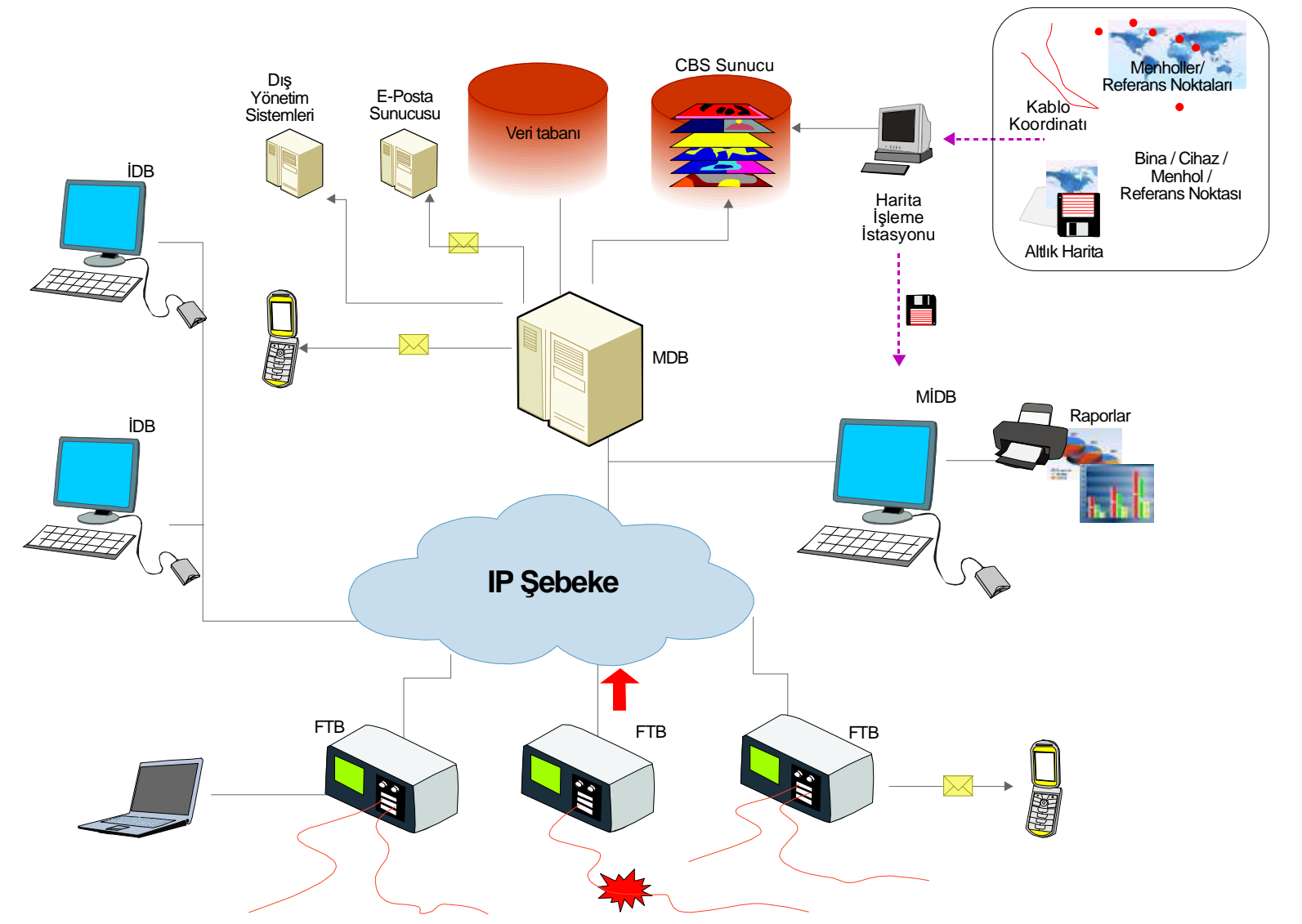
- F/O kablo ile ilgili envanterin ayrıntılı yönetimi
- F/O kablo altyapısının, aşımına, kopma, sızma olaylarına karşı çevrim içi izlenmesi

FKDS kapsamında, bir yönetim sistemi ve UDB (Uzak Denetim Birimi) adı verilen bir F/O kablo test cihazı geliştirilmiş olmakla birlikte, bu yazıda yalnızca FKDS'nin yönetim sistemi bölümü tanıtılmaktadır. Yönetim sisteminin,, geliştirilmekte olan evrensel FTB (F/O Test Birimi) arayüzü kullanılarak, uzaktan yönetim arayüzleri bilinen bütün FTB cihazlarıyla birlikte çalışabilmesi hedeflenmektedir.

1.2. Genel Mimari

Bu bölümde, FKDS sisteminin genel mimarisi, Şekil 1'de özet olarak tanıtılmaktadır. FKDS sistemi, F/O şebeke altyapısını merkezi bir denetim birimi ve ona bağlı istemci denetim birimleri ile FTB cihazları üzerinden sürekli izleyerek, şebekenin işlerliğinin sağlanması ve tehditlerden korunması olanağını sağlar.

MDB (**Merkezi Denetim Birimi**) cihazı, sistemin merkezi yönetim sunucusu olarak hizmet gören yazılım ve donanımdan oluşur. MDB, sistemin hata, başarımlı, güvenlik, envanter ve yapılandırma konulu yönetimini gerçekleştirir [1]. Bütün sistemin verileri bu sunucuda saklanır. İDB (**İstemci Denetim Birimi**) cihazları, MDB cihazına terminal olarak erişebilen istemci bilgisayarlarıdır ve MDB'den yetki kontrolü yaparak sistemle ilgili bilgileri isteyip ekranlarında gösterirler. İDB'ler, MDB'ye iletişim güvenliği sağlanmış web tabanlı kanal ile erişim yönetim işlemlerini yerine getirirler.



Şekil 1. FKDS'nin kavramsal birimleri.

F/O kablo şebekesinin ayrıntıları, İDB cihazları üzerinden, coğrafi koordinatları ile birlikte denetim merkezine aktarılır ve gerektiğinde güncellenebilir. Sistemi yöneten MDB, tüm bilgileri toplar, saklar, analiz eder ve CBS [2][3] verileri ile birleştirerek kullanıcıya sunar. MDB, kablo izleme birimi olarak çalışan FTB cihazlarını yönetir.

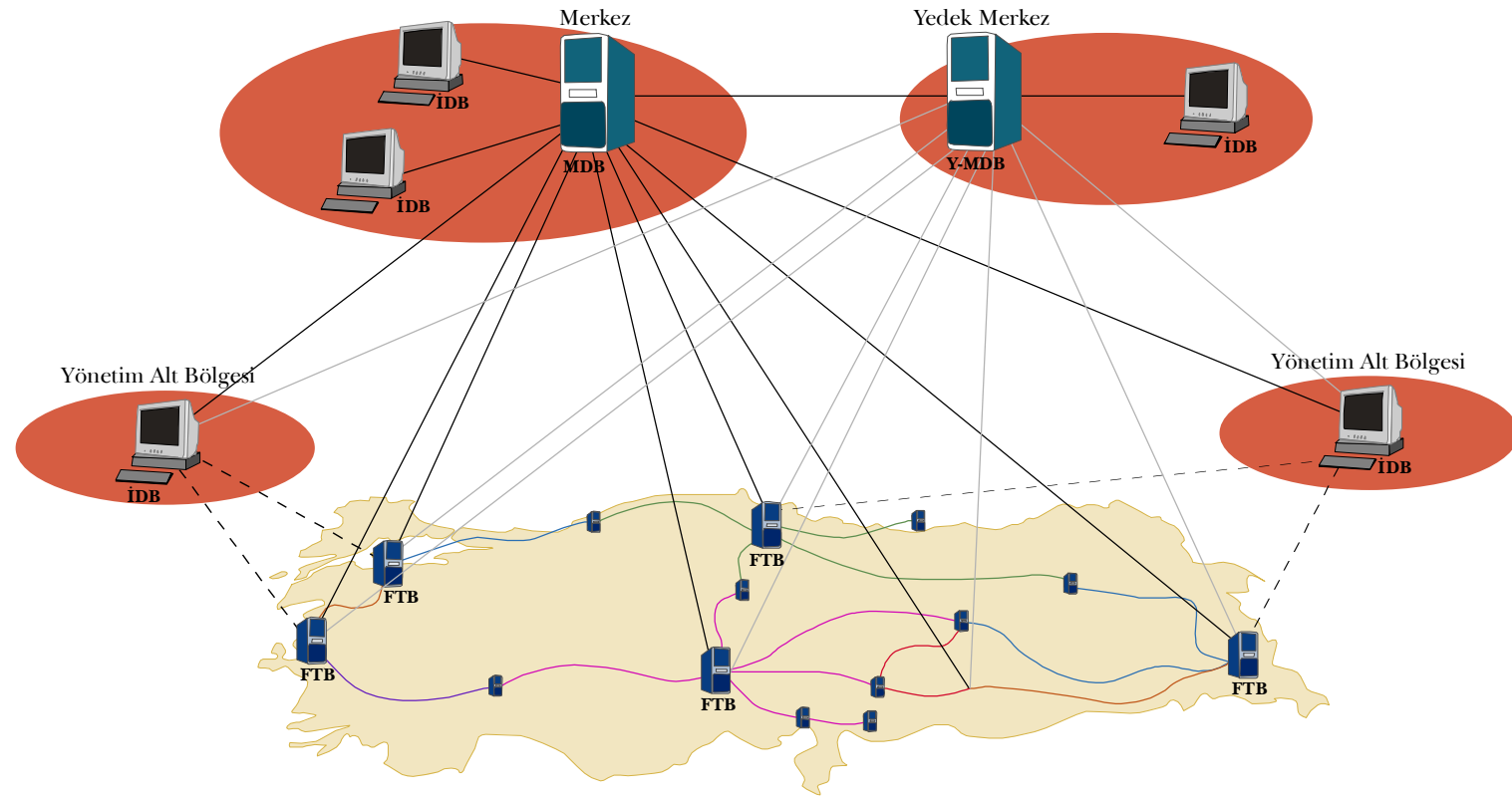
FTB cihazları F/O şebeke üzerinde uygun düğüm noktalarına yerleştirilen, kablo lifleri üzerinde optik ölçümler yapan, ölçüm sonuçlarını ve alarm durumlarını gerçek zamanda MDB'ye aktaran uç birimlerdir. FKDS yönetim sistemi TÜBİTAK BİLGEM'nin üretimi olan UDB adlı FTB cihazı ile çalışabildiği gibi, geliştirilmekte olan Evrensel FTB Adaptasyon katmanını kullanarak uzaktan yönetimi destekleyen bütün FTB cihazları ile de çalışabilecektir. UDB cihazı web servisi ile yönetim arayüzü sunmaktadır. F/O pazarında, RMI (Remote Method Invocation), CORBA (Common Object Request Broker), SNMP (Simple Network Management Protocol) ve özel IP (Internet Protocol)

tabanlı yönetim arayüzü sunan diğer FTB cihazları da bulunmaktadır.

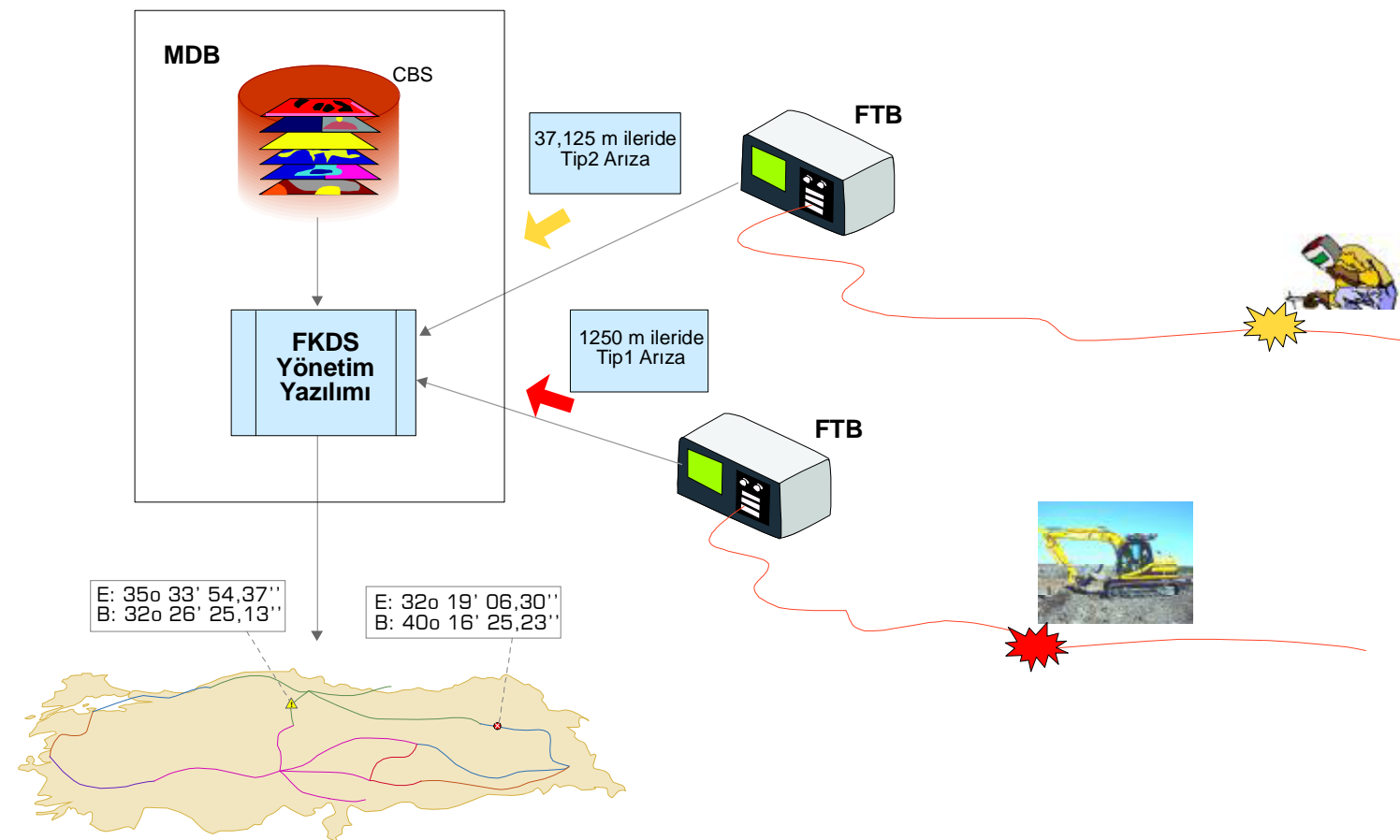
FTB'ler periyodik olarak F/O kablolar üzerinde çeşitli ölçümler yaparak sonuçlarını değerlendirip MDB'ye iletirler. Bu cihazların uzaktan yapılandırılmaları ve test koşullamaları yapılarak F/O ağ yapısındaki zayıflama, kopma ve bilgi çalma girişimleri gerçek zamanlı izlenip belirlenir.

F/O ağ yapısı üzerinde FTB'lerin yaptığı ölçümlerin sonuçları, normal durumlarda periyodik olarak, alarm durumlarında ise anında MDB'ye aktarılır ve veritabanlarına kaydedilir.

Sistemin durumu web tabanlı arayüz sunan İDB terminallerinden canlı olarak izlenebilir. İDB cihazları, operatörlere, F/O envanter verilerini yönetme ve kabloları izleme olanağı sunar. Alarm bilgileri CBS (Coğrafi Bilgi Sistemi) bilgileri ile birleştirilerek İDB ekranlarında görüntülenir.



Şekil 2. Yedekli bir FKDS iletişiminin yapısı.



Şekil 3. Kablolar üzerindeki arızaların belirlenmesi.

MDB, ana yönetim merkezine, İDB'ler, F/O şebekesini yöneten kurumların idari ve işlevsel seviyedeki çeşitli birimlerine (bölge ve alt bölge ofislerine); FTB'ler ise F/O kablo ağının test edilebilmesini sağlayacak biçimde, F/O şebeke üzerindeki uygun düğüm noktalarına yerleştirilir (Şekil 2).

1.2.1. F/O Kablo izleme yöntemi

FTB cihazları, optik anahtarlama yaparak birden fazla F/O kablo lifini, insan müdahalesi gerekmeksizin test edebilirler. FTB cihazlarının liflerde yaptıkları ölçüm sonunda, sorunların çeşidi ve kablunun ucundan itibaren kaç metre uzakta olduğu tespit edilir. Bu sorunun coğrafi koordinatının belirlenmesi ise MDB'de, daha önce girilmiş F/O şebeke coğrafi koordinat bilgileri kullanılarak yapılır (Şekil 3).

FTB'ler, iletişim trafiği olmayan lifleri ölçebildikleri gibi, iletişim trafiği olan lifleri de şebekeye yerleştirilen WDM (Wavelength Division Multiplexing) bileşenleri sayesinde ölçülebilmektedirler. Aktif kabloyu ölçmeyi amaçlayan örnek bir senaryo Şekil 4'de gösterilmiştir.

Bu senaryoda da görüldüğü gibi, F/O şebekedeki birden fazla kablo lifi, test

trafiğinin baypas bağlantıları ile kesintisiz iletilmesi yöntemiyle oluşturulan bir Ölçüm Yolu (F/O kablo lif dizisi) kapsamında, tek bir FTB girişi üzerinden test edilebilir. Ölçüm yolunun yapılandırılması (her bir lifin F/O karakteristik parametreleri, yürütülecek testlerin parametreleri, olay ve alarm belirleme eşikleri) MDB tarafından yapılır.

FTB'nin ölçüm yolu üzerinde belirleyeceği sorunlu noktaların uzaklıkları, daha sonra MDB'de analiz edilerek sorunlu kablolar belirlenir (Şekil 5). FTB giriş bağlantısının maliyeti yüksek olduğu için, FTB girişlerinin izin verdiği maksimum lif uzunluğunu aşmayacak biçimde bu baypas bağlantıları kurularak daha çok kablo tek bir giriş üzerinden test edilebilmektedir.

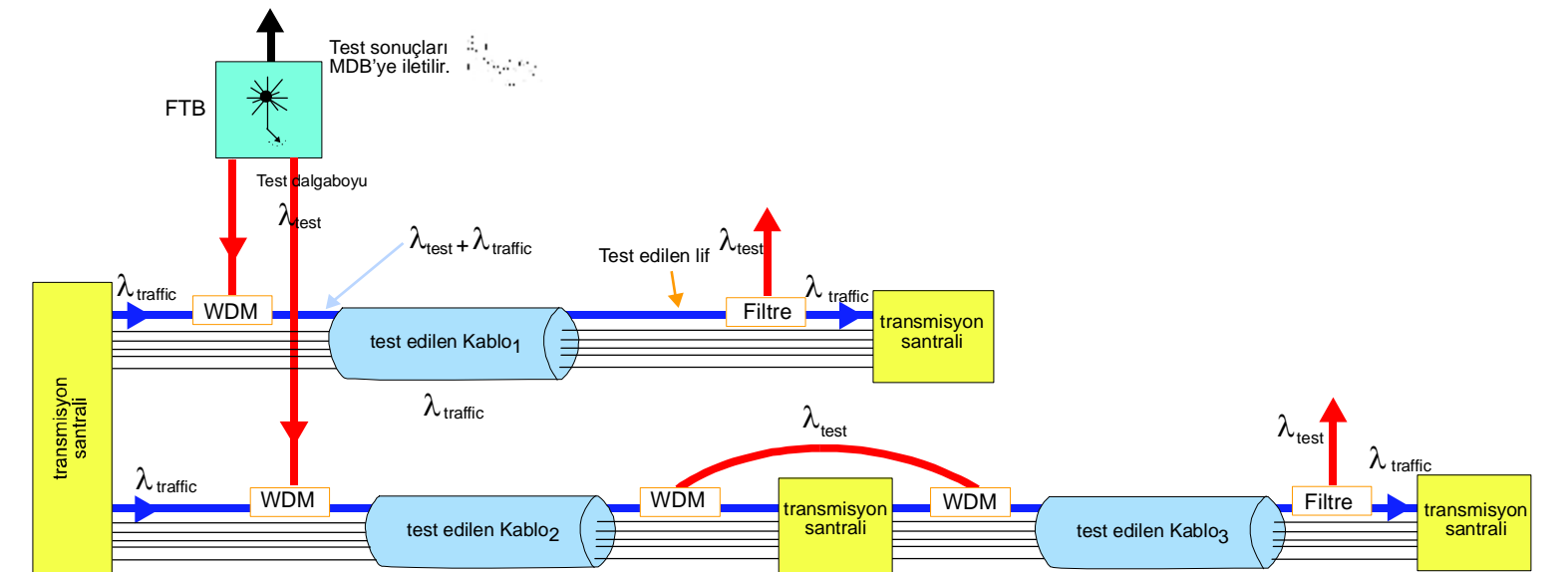
Sistemdeki FTB'ler sahaya ilk kurulduğunda, girişlerine bağlanan lifler üzerinde kablunun normal durumunu belirleyecek olan bir referans ölçümü yaparlar. Daha sonra yapacakları ölçümleri bu referans ölçüm ile karşılaştırarak kablo üzerindeki anormal durumları belirlemeye çalışırlar. Ölçüm sonucunda kablo üzerinde, ek yeri, filtre, kablunun başlangıç ve bitiş noktaları, kablunun eğilmesi gibi bir dizi olay belirlendiğinde, kopma,

kırılma, yaşlanma ve kabloya saldırı durumlarında referans değerler ile ölçülen değerler arasında fark oluşur ve sistem alarm verir.

1.3. FKDS Modülleri ve Teknik Özellikleri

Sistemin yönetim işlevlerini yerine getiren yazılım modülleri Şekil 6'da gösterilmiştir. Yazılım modülleri, yaklaşık 200 bin satırlık kaynak kod ve 300 adet kullanım senaryosu (usecase) boyutunda gerçekleştirilmiştir.

MDB yazılımının bileşenlerinin türleri Şekil 7'de gösterilmiştir. Sistemde coğrafi bilgilerin saklanması ve yönetilmesi için MDB'ye bir CBS sunucu yazılımı eklenmiştir. MDB'de uygulama mantığını içeren yazılımlar, J2EE tabanlı uygulama sunucusu üzerinde çalışır. Bu yazılımlardan kullanıcı arayüzünü oluşturan JSF (Java Server Faces) [4] sayfaları web barındırıcıda (Web Container), veri yönetimi ile ilgili kodlar EJB (Enterprise Java Bean) [5] olarak gerçekleştirilir ve EJB barındırıcıda çalışır. Akıllı kart, sesli uyarı ve ölçüm grafiklerinin ayrıntılı incelenmesi amacıyla sayfalar içine gömülmüş olan Applet'ler [6] kullanılır.



Şekil 4. Üç fiber kabloyu denetleyen bir ölçüm senaryosu.

1.4. Temel İşlevler ve Önemli Özellikler

Bu bölümde, sistemin özellikleri, OSI (Open System Interconnection) yönetim alanları başlıklarına bölünerek tanıtılmıştır.

1.4.1. Hata Yönetimi

Sistemde oluşabilecek sorunlu durumların belirlenmesi ve raporlanması kapsamındaki özellikleri içerir.

F/O kablo ölçüm yolları (Bkz. Bölüm 1.2.1) üzerinde yürütülecek testlerin tanımlanması ve belirlenmiş alarm kayıtlarının, ilgili ölçüm grafikleri ve arıza giderme işleri ile ilişkilendirilmiş olarak yönetilmesi hata yönetimi kapsamında yapılır.

Sistemde iki tür alarm tanımlıdır:

- Cihaz Alarmı: MDB ve FTB cihazlarının kendi yazılım ve donanımlarında oluşan arızalara ilişkin alarmlar
- Lif Alarmı : F/O kablolardaki kopma, eğilme, yaşlanma vb. nedenlerle oluşan alarmlar

Sistemde lif başına alarm ve olay belirleme eşikleri seçilebilir. Böylece bir takım liflerde daha farklı eşiklerle çeşitli amaçlara uygun alarm tespiti yapılabilir. FTB cihazının alarm mesajında MDB'ye bildirdiği uzaklık bilgisi, ölçüm yolu üzerindeki bakım payları, kabloların 3D modeli, altlık harita katmanları ile birlikte hesaba katılarak alarmın oluştuğu kablo lifi, coğrafi koordinatı, yakınındaki önemli noktalar, etkilenen müşteri hizmetleri belirlenebilir.



Şekil 8. Dış sistemlere ekleme ayarı penceresi.

Belirlenen kullanıcılara, alarm durumunda dış e-posta sistemleri üzerinden mesaj gönderilmesi sağlanabilir. Alarm çeşitlerinin seviyeleri etkin olarak sistem genelinde kolayca değiştirilebilir. Alarmlar, SNMPv1 ve v2 protokolüne uygun olarak dış yönetim sistemlerine, İDB terminallerinden de sesli uyarı şeklinde bildirilebilir.

Ayarlar görünümünde iken "Dış Sistemler" seçeneğinden SNMP Trap olarak alarm bildirilecek yönetim sistemleri tanımlanır.

Bu yönetim alanı kapsamında, sistemin şu özellikleri vardır:

- Alarm kaydını toplama
 - F/O lif ve FKDS cihaz alarmları
- Alarm belirleme eşiklerini tanımlama
 - Lif ve cihaz alarmlarının kayıtlarını tutma
- Alarm seviyesinin yapılandırılması
- Alarm Arşivini tutma
- Alarm Bildirme (SNMP, e-Posta, SMS, sesli uyarı)
 - İstatistiksel alarm, arıza raporlarını hazırlama
- Alarm izleme
 - Canlı alarm izleme
 - Alarm sorgulama
 - Alarm onaylama
- Arıza Yönetimi
 - Arıza nedeni ve oluşma tarihi
 - Müdahale tarihi

– Çözüm yöntemi, çözüm tarihi ve kullanılan malzemeler

– Çözen kişiler

• Ölçüm Yönetimi

– Ölçüm yollarının tanımlanması ve kontrollü olarak devreye alınması

– Ölçüm test parametrelerinin ve ölçüm sonuçlarının yönetimi

• Kablolarda değişik türde ölçümlerin gerçekleştirilmesi

• Kabloların referans ölçümlerinin yapılması, hata belirlemede kullanılması

• Kablo üzerindeki tüm zayıflama noktalarının belirlenmesi

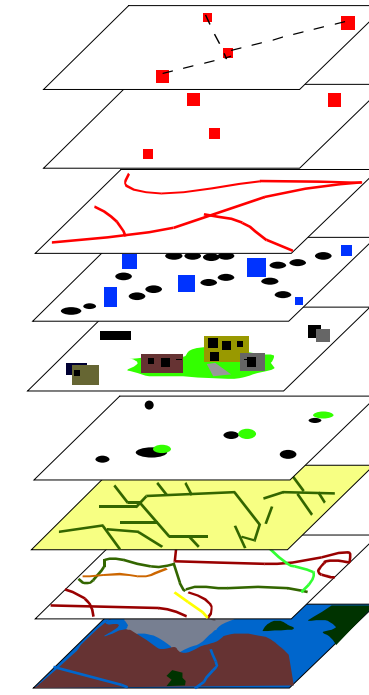
• Ölçüm sonuçlarının kullanıcıya sunulması

1.4.2. Envanter Yönetimi

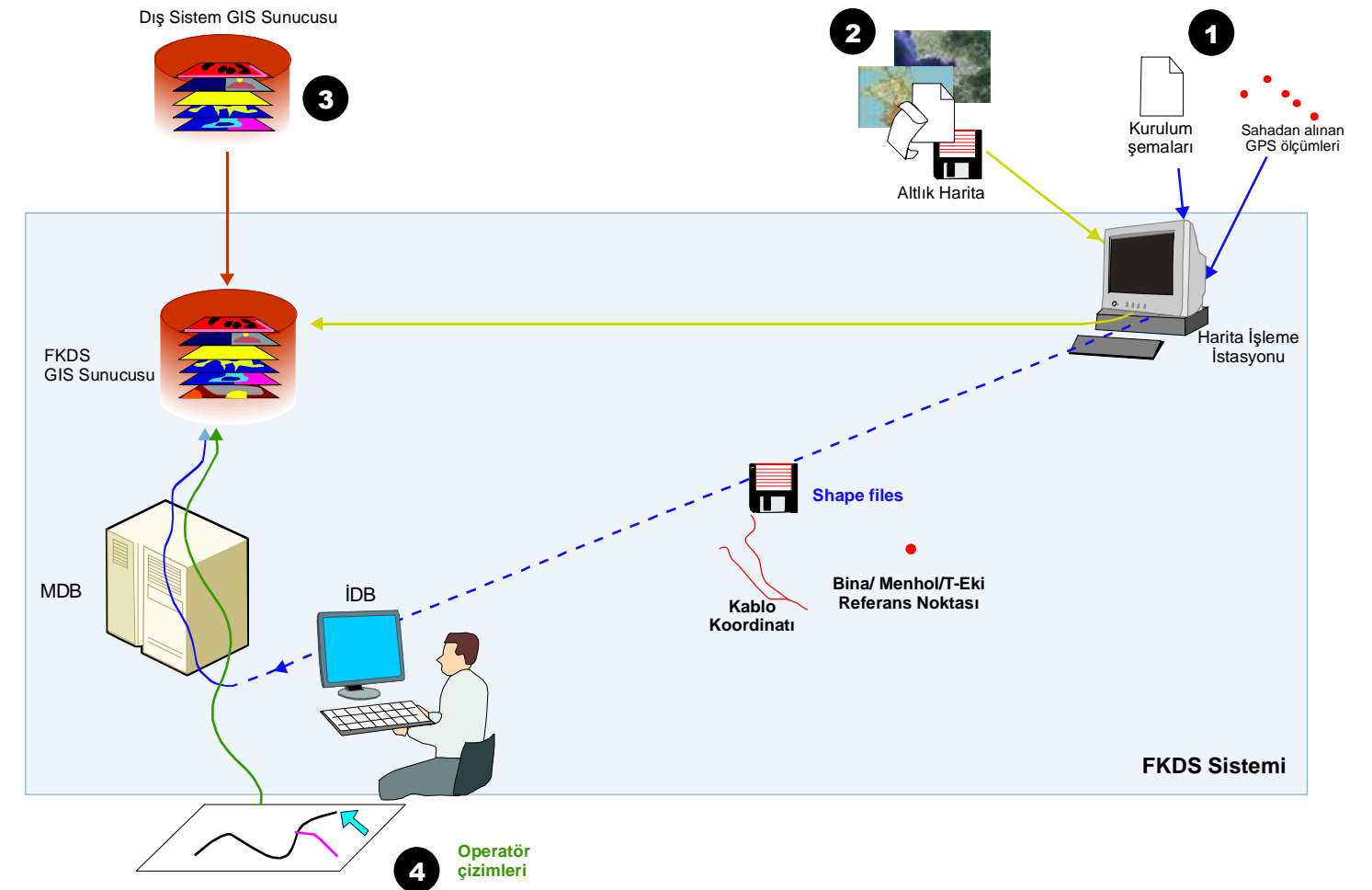
FKDS, F/O kablolarını, liflerinin rengine kadar modellemeye olanak sağlar. Bu amaçla, sahada kurulu kabloların profilleri, marka ve modellerine göre tanımlanır. Daha sonra bu kablo profillerinden yararlanılarak kablolar tanımlanabilir. Envanter varlıkları (fiber optik kablo, radyolink, menhol/direk, bina, t-eki kutusu, ODF, referans noktası) coğrafi bilgi sisteminde konum bilgileri ile birlikte tutulur (Şekil 9).

CBS alt sisteminde, varlıklar çeşitli katmanlar şeklinde modellenir. Sistemde kablo koordinatları, üç boyutlu uzayda (enlem, boylam, yükseklik olarak) tanımlanır. Saha kablo incelemeleri sonucunda kablo koordinatları GPS (Global Positioning System) koordinatları olarak toplanıp CBS katmanlarına eklenir.

Ayrıca, CBS servisi içinde tutulan haritalarla envanter bilgilerinin operatörler tarafından anlaşılır bir biçimde yönetilebilmesi sağlanır. Altlık haritaların kullanılmasının en önemli amaçlarından birisi de FTB'lerin bir kablo üzerinde - kablunun bir ucundan itibaren- optik uzaklık olarak belirledikleri olayların,



Şekil 9. FKDS kapsamında kullanılan CBS katmanları.



Şekil 10. FKDS sistemine coğrafi veri giriş yöntemleri.

coğrafi koordinat karşılıklarına dönüştürülmesidir. Bu dönüşümü yapabilmek için kabloların üç boyutlu modelinden yararlanılır. Bu tanımlamaların yapılabilmesi için, sistem kullanıcılara çeşitli olanaklar sunar (Şekil 10).

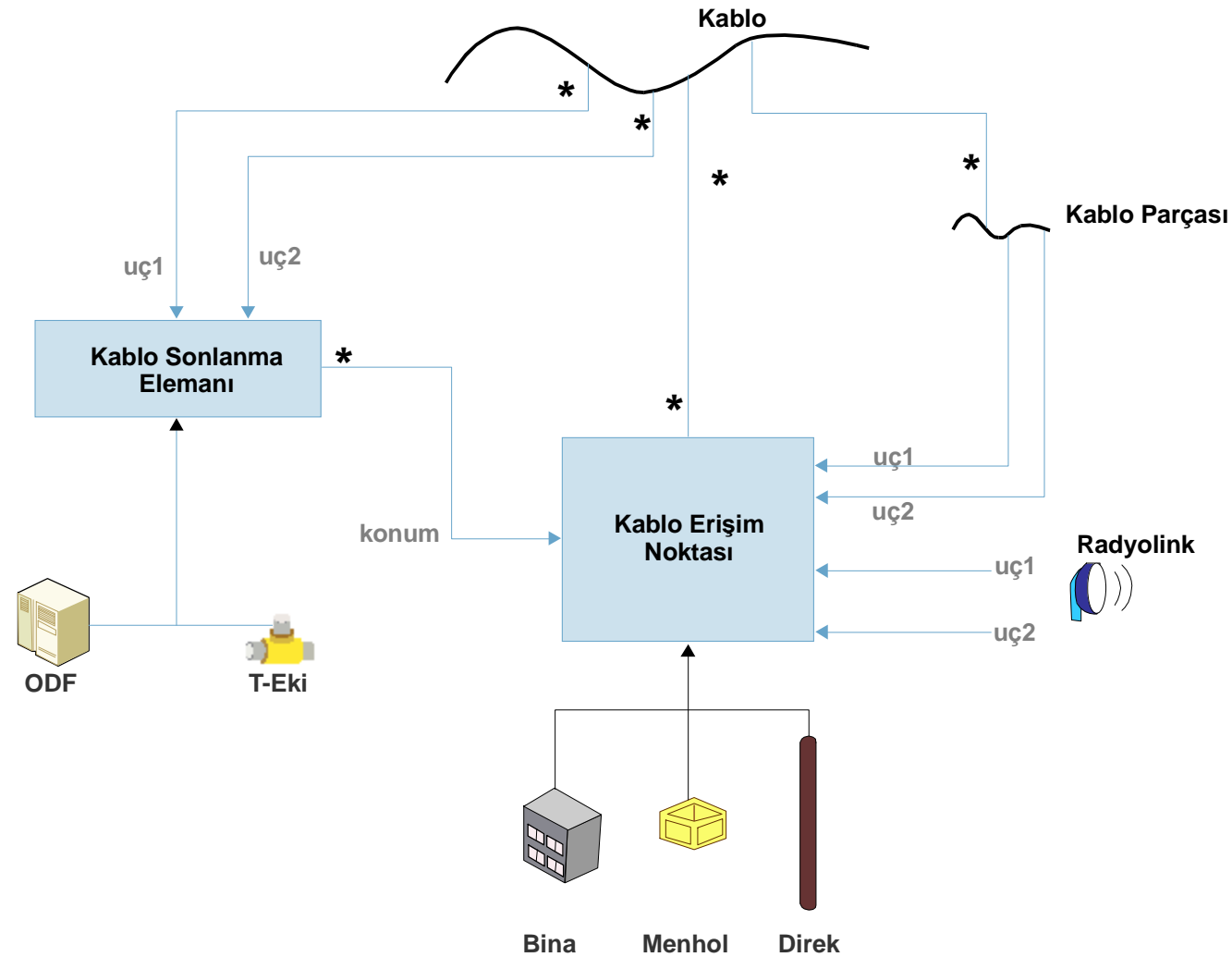
F/O şebekeye ilişkin bilgiler, doğrudan İDB terminali kullanıcı arayüzünde sağlanan çizim araçları ile sisteme girilebileceği gibi, bilinen CBS dosyaları formatında taşınabilir ortamdan sisteme girilebilir. Şekil 10'daki harita işleme istasyonunda, sahadan toplanan veriler, CBS Uygulaması ile ön işlemden geçirilerek standart CBS dosya türlerine dönüştürülür. Dönüştürülen bu dosyalar, herhangi bir İDB terminalinden sisteme yüklenebilir. Ayrıca, dış CBS sistemlerinden, bilinen harita servisleri formatında da veri kullanılabilir.

Sistemde kaydı tutulan envanter varlıklarından önemlileri Şekil 11'de gösterilmiştir.

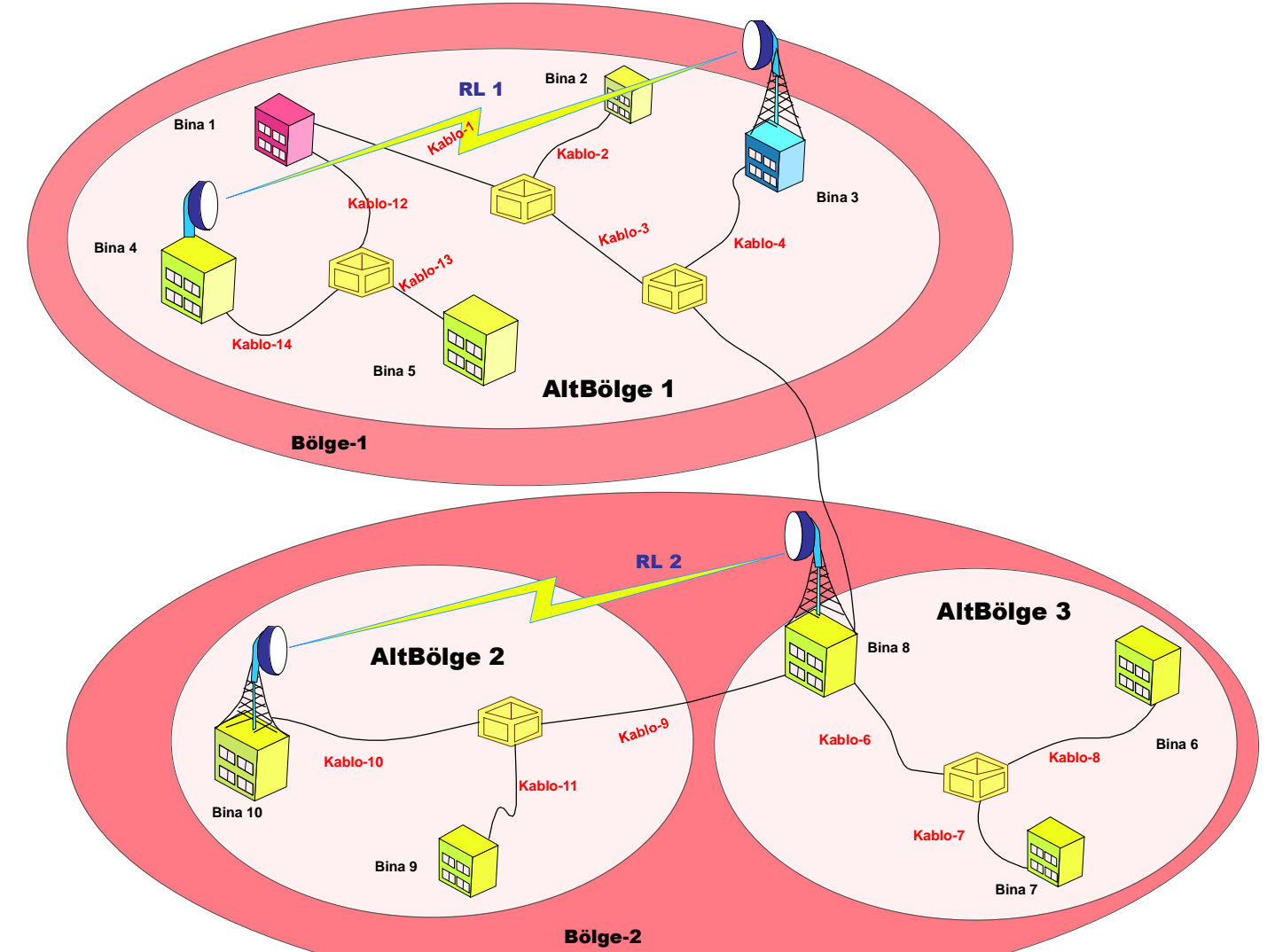
F/O envanteri, **bölge** ve onun altında bulunan alt **bölgeler** içindeki şehirlere göre gruplanır. Dolayısıyla F/O varlıkları tanımlanmadan önce **bölge** ve onun altında **alt bölge** tanımlanmış olmalıdır. Her alt bölge kapsamında bir dizi **şehir** tanımlanır (Şekil 12).

Envanter yönetimi kapsamında sisteminin şu özellikleri vardır:

- Varlıkların envanterini tutar
 - Cihazlar (terminal, FTB)
 - Envanter elemanları ve bunlara iliştilmiş dosyaların yönetimi
- Kablolar, kablo parçaları, lifler, bakım payları
- Kablo sonlanma elemanları (ODF, T-Eki)
- Kablo erişim noktaları
 - Binalar (8 farklı tip),
 - Menholler/direkler
- Radyolinkler



Şekil 11. Önemli envanter varlıkları ve aralarındaki ilişkiler.



Şekil 12. Örnek bir veri senaryosu.

- Kablo güzergahları,
- Linkler (devreler)
- Kablo profilleri
- Yönetim bölgeleri, alt bölgeler, şehirler,
- Envanter raporlarını hazırlar
- Envanter değişikliklerini iki aşamada onaylar
- Envanter varlıklarına ilişkin idari bilgileri yönetir
 - Grup, safha, iş paketi tanımlama
 - Kurulum, devreye almaya aşamaları durum/tarihleri
 - Mülkiyet sahibi kuruluşlar
 - Açıklamalar

- CBS ile ilişkili veri yönetimi (alarm, bölge, bina, kablo, bakım payı, menhol/direk, T-Eki, ODF, radyolink, referans noktası, link, ölçüm yolu, FTB, İDB)

Sistemin bir diğer özelliği ise envanter bilgileri üzerinde yapılan değişikliklerin iki aşamalı onaydan geçtikten sonra kalıcı duruma geçebilmesidir. Değişiklikten etkilenen envanter elemanı üzerindeki işleme ilk onay verebilme yetkisine sahip olan kullanıcılar sistem tarafından posta kutularına gönderilen mesaj ile uyarılır. Mesajlar yalnızca söz konusu envanter elemanın bulunduğu alt bölge sahasında yetkili olan ve birinci onay verme yetkisine sahip kullanıcılara gönderilir. Birinci onay verildikten sonra, benzer olarak ikinci onayı verme yetkisine sahip ve söz konusu envanterin olduğu alt bölge sahasında da yetkili olan kullanıcıya ikinci onayı vermesi için mesaj gönderilir. Posta kutusuna bakan ilgili kullanıcı,

kendisinden onay beklendiğini bildiren mesajın üzerine tıklayarak ilgili envanter elemanının sayfasını açıp inceledikten sonra onay verir veya reddeder.

Sistemde İDB kullanıcı arayüzleri üzerinden operatörlerin kullanımına sunulan çizim araçları ile yapılabilen işlemler aşağıda listelenmiştir:

- CBS ile ilişkili olarak envanter bilgileri üzerinde yapılan işlemler:

- Bina, menhol/direk, kablo, T-Eki, ODF, referans noktası, bakım payı

- Ekleme, silme, taşıma

- Koordinatları içeren dosya ile ekleme

- Kablo, bina, T-Eki, güzergâh, cihaz (FTB, İDB), radyolink

- Odaklanma, aydınlatma

- Kablo

- Tüp/lif bazında ayrıştırma görme, ölçüm yapma

- İçinden geçen linkleri ve ölçüm yollarını aydınlatma

- Parçalama (iki ayrı kabloya dönüştürme)

- Birleştirme (iki kabloyu tek bir kabloya dönüştürme)

- Yükseklik histogramını görme

- Koordinatlarını dosyadan yükleme

- Radyolink

- Çizerek ekleme

- T-Eki

- İçini (sonlanan kabloların liflerinin birleşme çizimini) gösterme

- FTB

- Denetlediği kabloları görme

- Alarm

- Görme ayrıştırma inceleme

- E-Postaya eklemek için alarm görüntüleri üretme

- Diğer CBS yetenekleri

- Yakınlaşma/uzaklaşma/kaydırma/önceki ya da sonraki görünüme geçme,

- Katmanları açıp kapatma

- Tanımlanan kriterlere göre varlıkları Filtreleme

- Tanımlanan kriterlere göre varlıkları renklendirme

- Arama, bulma, odaklanma

- Bölgelere odaklanma

- Harita görüntülerini dosyaya kaydetme

- Bakı (sight), eğim analizi, alan, uzaklık, yükseklik ölçüm araçları

1.4.3. Yapılandırma Yönetimi

Yapılandırma yönetimi kapsamında sistem aşağıdaki özelliklere sahiptir:

- FTB veritabanlarını ilklendirme ve güncel tutma (Ölçüm yolu, kullanıcı, vb. bilgiler)

- FTB cihazlarını düşük seviye komutlar ile uzaktan yönetmek için konsol

- Destekleyen FTB (şimdilik yalnızca UDB) cihazlarının kodunu güncelleme

- FTB donanım birimlerinin (Sabit disk, OTDR, CPU, optik kartlar, akıllı kartlar, vb.) yapılandırılmasının ve durumlarının yönetimi

- Ölçüm yollarına ilişkin referans F/O ölçümlerinin oluşturulması ve güncellenmesi

- Ölçüm yollarını izlemeye alma, izlemeden çıkarma

1.4.4. Güvenlik Yönetimi

Sistemin güvenlik yönetimi, kullanıcı yönetimi ve iletişim güvenliği, başlıkları altında ele alınabilir.

1.4.4.1. Kullanıcı Yönetimi

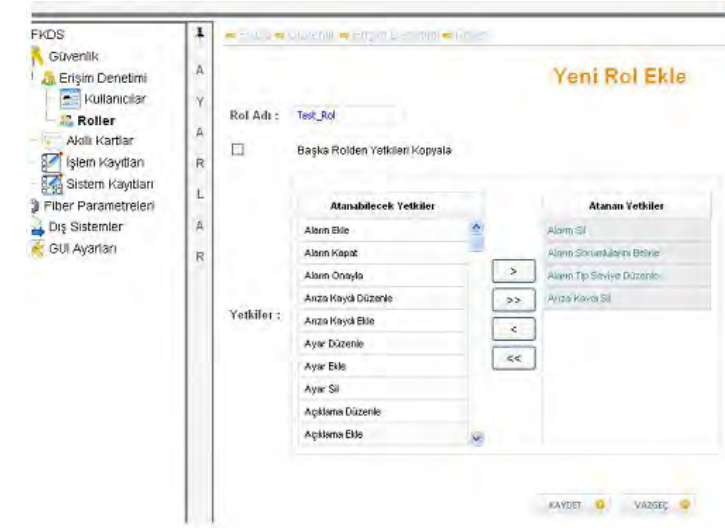
FFKDS sisteminde kullanıcı yönetimi kapsamında kullanıcı ekleme, silme, düzenleme, listeleme, kullanıcı için akıllı kart üretme, parola değiştirme işleri yerine getirilir. Böylece roller, kullanıcılar, yetkiler, akıllı kartlar ve işlem kayıtları yönetilir.

Kullanıcı **kimlik doğrulama** (authentication) için merkezi olarak tanımlanan kullanıcı hesapları kullanılır. Sistem, kullanıcıların hem akıllı kart ile hem de kullanıcı adı ve parola ile sisteme girişine olanak sağlayabilir. Kullanıcıların akıllı kartları yine sistemde üretilir ve içlerine kullanıcılara ait X509v3 sertifikaları yerleştirilir.

Erişim denetimi (access control) kapsamında esnek rol tabanlı erişim denetimi uygulanır. Sistemde tanımlı yetkiler (yapılabilecek işlemleri) vardır. Yine sistemde tanımlanan her bir rol, bu tanımlı yetkilerden bir kümeyi içerir ve istenirse

düzenlenebilir. Kullanıcılara, atandıkları roller dolayısıyla gelen yetkilerin yanında ek yetkiler de yazılımı değiştirmeye gerek kalmaksızın atanabilir. Dolayısıyla, kullanıcıların sistemde neleri yapıp neleri yapamayacağı etkin olarak yapılandırılabilir.

Roller arasında yönetim hiyerarşisi vardır. Her rol ancak kendisinin tanımladığı alt roller ve onların altındaki rolleri ve onlara atanmış kullanıcıları yönetebilir. Sistemde ön tanımlı (default) olarak ekli olan roller vardır. Bu rollere istenirse yenileri eklenebilir. Eklenen bu rollere istenilen yetkiler tanımlanabilir ve istenirse sonradan değiştirilebilir. Rol ekleme, başka bir rolden kopyama ile veya yetkiler tek tek tanımlanarak yapılabilir.



Şekil 13. Rol ekleme kullanıcı arayüzü.

F/O Envanter bilgileri ve FTB'ler üzerinde de erişim denetimi yapmaya olanak sunar. Bu amaçla, kullanıcılara alt bölgeler ve cihazlar üzerinde işlem yapma yetkisi etkin olarak atanabilir. Kullanıcılar, ancak kendilerine izin verilen alt bölgelerde bulunan F/O envanter bilgileri ve FTB cihazları üzerinde yönetim işlevlerini kullanabilirler. Bir takım kullanıcılar alarm sorumlusu olarak tanımlanır ve alarmların yalnızca bu kullanıcılara e-posta yolu ile bildirilmesi sağlanır.

Güvenlik servisi kapsamında, sistemde kullanıcılar tarafından yapılan veya sistemin çalışması gereği gerçekleşen her türlü işlemin kaydı tutulur (auditing, denetleme). Sistemde bu amaçla,

- Kullanıcının neden olduğu olaylar ile sistemde otomatik olarak ortaya çıkan olayların izlenmesi

- İşlem kayıtlarının sorgulanması ve raporlanması özellikleri bulunur. Yönetilen kayıtlar iki tür olabilir:

- **Sistem Kayıtları:** FTB cihazlarının ve MDB'nin sisteminde gerçekleşen önemli olayların kayıtları.

- **İşlem Kayıtları:** Kullanıcının sisteme bağlı olduğu süre içerisinde yaptığı (başarılı ya da başarısız) tüm işlemlerin bilgileri.

1.4.4.2. İletişim Güvenliği

FFKDS cihazları arasında iletişim güvenliği için şifreleme, bütünlük koruması ve kimlik doğrulama algoritmaları kullanılır. MDB ile FTB, MDB ile terminaller ve MDB ile yedek MDB arasında iletişim güvenliği için TLS (Transport Layer Security) [12] tabanlı protokol kullanılabilir. TLS iki makine arasında güvenli bir kanal oluşturmak için kullanılan bir protokoldür.

İletişim güvenliğinin çalışabilmesi için kriptografi parametrelerinin üretilip ilgili cihazlara yerleştirilmesi gerekir. Bu işlemler **kriptografik ilklendirme** adı verilir. Sistemde kullanıcı ve cihazlar için X509 sertifikaları [13] üretilir ve kullanılır. Bu sertifikaların yönetimi için MDB'nin kök (ve tek) sertifika makamı olduğu bir PKI (Public Key Infrastructure) sistemi bulunmaktadır. Tüm sertifikalar MDB'de üretilir ve MDB'nin kök sertifikası ile imzalanır.

MDB'nin diğer cihazlar (terminaller ve destekleyen FTB'ler ile iletişimde kullanılan sertifikalar, üretilen akıllı kartlara yerleştirilir. İstenirse şifreli anahtar depoları formatında da dağıtılıp cihazlara yerleştirilir.

MDB ile Yedek MDB arasındaki iletişimin (çevrim içi yedekleme) güvenliğini sağlamak için, sistemde üretilen MDB ve yedek MDB'nin sertifikalarıyla kurulan SSL(Secure Socket Layer) iletişimi kullanılır. MDB ile yedek MDB arasındaki SSL tabanlı iletişim, OAS (Oracle Advanced Security) [14] paketi kullanılarak yapılandırılır.

1.4.5. Başarım Yönetimi

Sistemin bütün veritabanı MDB cihazında tutulur. MDB cihazının arızalanması durumunda devreye girmek üzere bekletilen yedek MDB cihazı üzerindeki veritabanı da asıl MDB'deki değişikliklerle sürekli güncellenir. Asıl MDB devre dışı kaldığında, yedek MDB dakikalar içinde İDB terminalleri ve FTB cihazlarının bağlanabileceği duruma gelir. Başarım yönetiminin özellikleri aşağıda listelenmiştir:

- FTB bağlantı durumlarının izlenmesi

- Güvenilir oturum yönetimi (MDB ile FTB arasında)

- Yedekli sunucu mimarisi

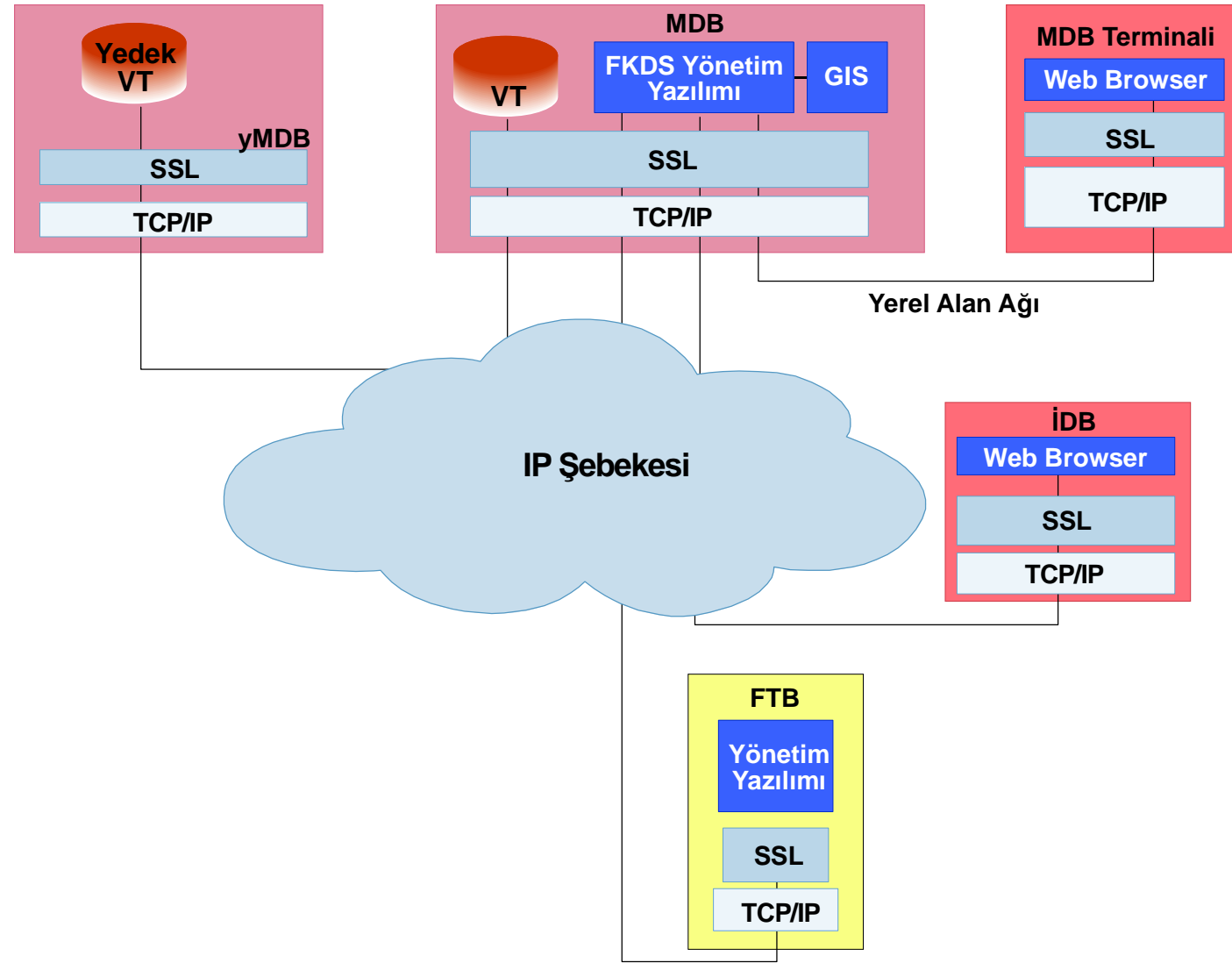
- Ölçüm yollarının devreye alınmasının izlenmesi

- Linklerden yararlanan kullanıcılar için SLA Yönetimi

- Terminallerden giriş yapan kullanıcıların izlenmesi

- Destekleyen FTB cihazlarına uzaktan CİT (Cihaz İçi Test) yapma

MDB yazılım bileşenleri (veritabanı, uygulama sunucusu, CBS Sunucusu ve kullanıcılara hizmet eden servisleri) ayrı makinelere dağıtılarak sistemin başarımını artırılabilir. Sistem web tabanlı



Şekil 14. İletişim protokolleri.

olduğu için MDB, İDB ve FTB'ler arasındaki iletişim düşük band genişliğinde yapılır

1.4.6. Muhasebe Yönetimi

Sistemden hizmet alan müşterilerin hesaplarının yönetilmesi, özellikle telekomünikasyon dünyasında çok önemlidir.

Link (kullanıcı devreleri) kavramı kabloların lifleri kullanılarak iki **bina** arasında oluşturulan F/O yollarını içerir. Devre adı da verilen Linkler üzerinden, iki ucunda yer alan Binalardaki elektronik teçhizat arasında veri iletimi gerçekleşir. Sistemde hangi linkler üzerinden hangi tür veri iletişiminin (video, TCP/IP, ses, ATM vb.) gerçekleştiği bilgileri de tanımlanabilir. **Kablolarda** oluşacak arıza durumlarında, hangi **binalar** arasındaki hangi müşterinin hangi hizmetlerinin ne kadar süre kesildiği de belirlenebilir.

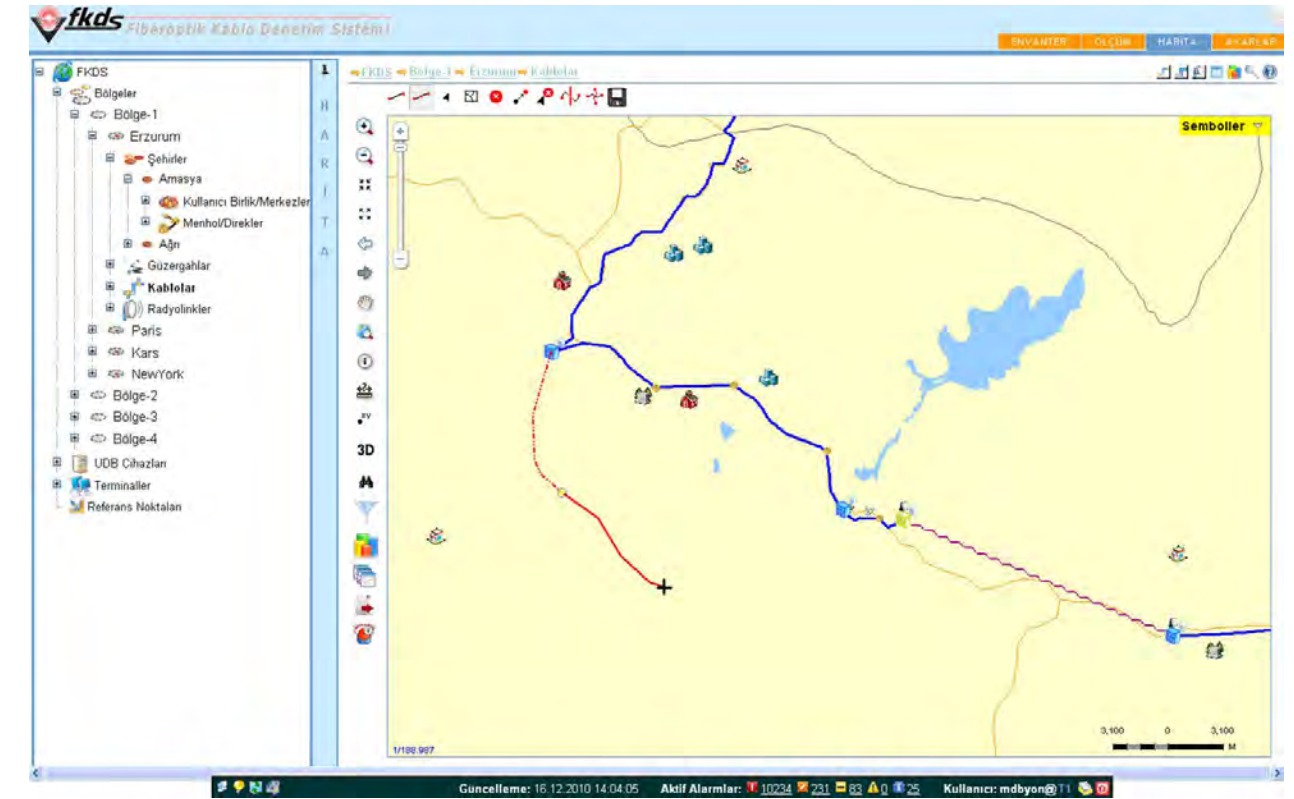
FKDS sisteminin aşağıdaki özellikleri vardır:

- Müşteri hesaplarının yönetimi

- Servis yönetimi
 - Liflerin kullanım türü
 - Liflerden yararlanan müşteriler
 - Liflerden geçen müşteri servisleri (ses, data, görüntü, IP, ATM, vb.)
- SLA Yönetimi
 - SLA tanımlama
 - SLA ihlal izleme

1.5. Kullanıcı Arayüzleri

İDB terminallerinde kullanıcıya web tabanlı arayüzler sunulur. Bu arayüzler JSF teknolojisi üzerine kurulu IceFaces [15] kütüphaneleri ve geliştirilen diğer özel bileşenler kullanılarak hazırlanmıştır. Kimi kullanıcı arayüzlerinde Applet teknolojisi de kullanılmıştır.



Şekil 15. İDB Kullanıcı arayüzünün parçalı kablo çizme anındaki görüntüsü.

Kullanıcı arayüzleri, görünüm (perspektif) kavramı kullanılmıştır. Birbiri ile ilişkili işlemler görünüm altında gruplanmıştır. Web tabanlı kullanıcı arayüzü kullanılmamaktadır, tüm değişiklikleri, bütün kullanıcı ekranlarına canlı olarak yansıtan yöntemler geliştirilmiştir.

Her türlü bilgi için “ayrıntılı esnek, yeniden kullanılabilir sorgulama filtreleri” tanımlanarak veriler üzerinde sorgular yürütülebilir ve sorgu sonuçları çeşitli formatlarda dosyalara aktarılabilir. Semboloji filtreleri ise haritada, varlıkların, çeşitli özelliklerine göre istenilen renklerde görünmesini sağlamak için kullanılır. Filtreler kaydedilip yeniden kullanılabilir. Tüm sayfalarda bağlama duyarlı (context-sensitive) yardım olanağı bulunur. Kullanıcı arayüzleri, birden çok dili destekleyecek biçimde geliştirilmiştir (internationalization).

2. Benzer Sistemler

BİLGEM tarafından geliştirilen FKDS sistemine benzeyen, belli başlı beş adet yabancı kaynaklı FKDS sistemi vardır. Bunlar:

- JDSU firmasının “ONMS” adlı ürünü [16]
- EXFO firmasının “FIBERVISOR” adlı ürünü [17]
- ANRITSU firmasının RFTS Remote Fiber Test System adlı ürünü[18]
- NETTEST firmasının QUESTFIBER adlı ürünü[19].
- LANCIER firmasının ModBus ve Unified Monitoring System adlı ürünü[20].

sisteminin sağladığı güvenlik seviyesini sağlayabilen bir ürün yoktur. Sistemlerin çoğunda, kullanıcı adı / parola ile kimlik doğrulamasının yapılması dışında güvenlik önlemi yoktur. Bu durum ise özellikle askeri kullanım alanında sistemimize üstünlük sağlamaktadır.

Ürünlerin tamamına yakını kalın istemci (thick-client) terminaller içerir. Kimilerinde ise sınırlı bir takım işlemler için web tabanlı arayüz ek olarak sunulur. Bizim sistemimizden başka, bütün işlemleri tümtüyle web tabanlı arayüzler üzerinden çalışan başka bir ürün yoktur.

3. Sonuç

Fiberoptik teknolojinin ülkemizde gün geçtikçe daha yoğun olarak kullanılmaya başlanması ile birlikte F/O kablolar kullanan şebekelerin sürekliliğinin sağlanması amaçlı sistemler de önem kazanmaktadır. FKDS sistemi bu gereksinimi karşılamak üzere geliştirilmiştir.

Bu sistemin önceki bölümde sözü edilen yabancı eşdeğerlerinin maliyetleri yüksek olup son ürün olmaları nedeniyle yeni özellik eklemeye açık değildir. Rakip ürünlerin güvenlik özellikleri yok denecek kadar azdır. Geliştirilen bu sistem ile FKDS alanında ülkemizin dışa bağımlılığını azaltılması yanında, yurtdışı F/O pazarını da hedefleyecek duruma gelinmiştir.

Sistem için şebekenin topolojisi, F/O kablo test cihazlarının giriş sayısı, ölçümuzaklığı, ölçüm süresi ve çeşitli işlevsel kısıtlamalar dikkate alınarak tüm F/O şebekesi denetim altında tutmaya olanak sağlayacak test cihazı sayısı ve yerleşim yerlerini

belirlemek için en iyileme tekniklerini kullanan yöntemlerin geliştirilmesi sürmektedir.

Geliştirilen sistem, konum tabanlı envanter varlıkları yönetiminin yoğun olarak kullanıldığı, boru hatlarının, elektrik dağıtım şebekelerinin, demiryollarının, karayollarının planlanması, modellenmesi ve izlenmesi alanlarına da kolayca uyarlanabilir.

TEŞEKKÜR

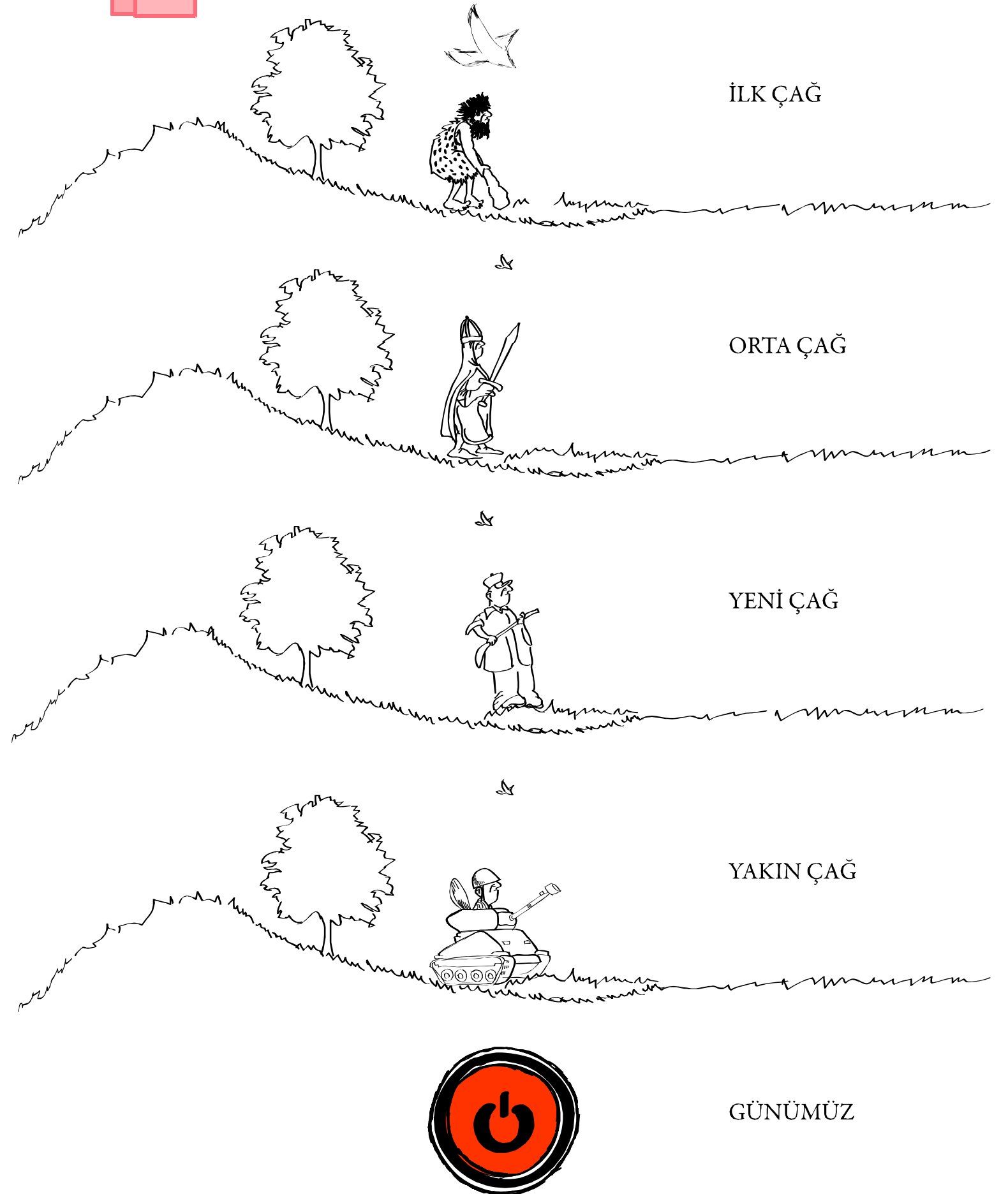
FKDS Projesinin yazılımının gerçekleştirilmesi süresince emekleri geçen değerli proje arkadaşlarım, Ahmet Ziyen, Serhan Tuysun, Hasan Genç, Muhammet Yıldız, Osman Davulcu, Ufuk Ünlü, Kemal A. Taşkıran, Hicran E. Taşkıran, Ahmet Başgöze, Hasan Er, Asiye B. Kılınç, İbrahim Coşgun, İlyas Takçı, birim yöneticimiz Meral Yücel, G204, UG-BODE ve G205 birimlerinin çalışanlarına teşekkürü borç bilirim.

KAYNAKÇA

- [1] ISO/IEC-7498-4, 1989. Information Processing Systems-Open Systems Interconnection-Basic Reference Model-Part 4: Management Framework, ISO/IEC.
- [2] GIS: <http://www.gis.com/whatisgis/index.html>
- [3] GIS in Telecommunications, ESRI Press, 2001
- [4] JSR-314-JavaServer Faces (JSF) 2.0, <http://www.jcp.org/en/jsr/detail?id=314>
- [5] JSR-220-Enterprise Java Beans (EJB) 3.0, <http://www.jcp.org/en/jsr/detail?id=220>
- [6] Applet, <http://java.sun.com/applets>
- [7] JSR-317-Java Persistence (JPA) 2.0, <http://www.jcp.org/en/jsr/detail?id=317>
- [8] JSR-224-Java API for XML-Based Web Services (JAX-WS) 2.0, <http://www.jcp.org/en/jsr/detail?id=224>
- [9] SOAP-1.2 - Messaging Framework, <http://www.w3.org/TR/soap12-part1>
- [10] IETF RFC-2571, SNMP
- [11] Oracle Data Guard Concepts and Administration B14239-01
- [12] IETF RFC-2246, Transport Layer Security
- [13] IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate.
- [14] Oracle Database Security Guide 10g Release 2 B14266-01

- [15] IceFaces, http://www.icefaces.org/v1_8/javadocs/icefaces
- [16] JDSU, ONMS, www.jdsu.com
- [17] EXFO, FIBERVISOR, www.exfo.com
- [18] ANRITSU, RFTS Remote Fiber Test System, www.us.anritsu.com
- [19] NETTEST, QUESTFIBER, www.nettest.com
- [20] LANCIER, ModBus, www.lancier-monitoring.de

KRİPKATÜB



İLK ÇAĞ

ORTA ÇAĞ

YENİ ÇAĞ

YAKIN ÇAĞ

GÜNÜMÜZ

Yazan: Umut ULUDAĞ
Çizen: Elif SÜSLER

ELEKTRONİK SEÇİM

İNTERNET ÜZERİNDEN OYLAMA:

ÜLKELERDEKİ DURUM VE KRİPTOGRAFİK
ALTYAPILARI

Mehmet Sabır KIRAZ

Fatih BİRİNCİ

Uğur Kâşif BOYACI

Yazı dizimizin geçen sayılarında elektronik seçim (e-seçim) hakkında genel bilgiler ve kullanılan kriptografik yapı taşlarını anlatmaya çalışmıştık. Bu sayıdaki yazımızda elektronik seçimi dünyada uygulayan bazı ülkelerin uyguladıkları çözümlere yer vereceğiz. Elektronik seçimi, uygulama metotları açısından "internet" ve "kiosk" tabanlı sistemler olarak ikiye ayırmıştık. Türkiye'de internet üzerinden oylamanın, yurt dışındaki seçmenler, oda seçimleri, belediyeler gibi kullanım alanları olabileceğini belirtmiştik.

Bu yazıda, internet kanalıyla uygulanan elektronik seçim sistemlerini inceleyeceğiz. İnternet üzerinden e-seçimi ülke çapında 2005 yılında ilk defa uygulayan ülke Estonya'dır. Norveç ise 2011 yılının sonunda yerel seçimlerde uygulamaya koyacaktır. Bu ülkelerde, internet üzerinden seçimin yapılabilmesi için seçmenlerin elektronik kimlik kartına sahip olmaları gereklidir. Elektronik kimlik kartı olmadan yurtdışındaki seçmenlerine internet, telefon ve faks üzerinden oy kullandırmayı planlayan ABD ise güvenlik konusunda birçok eleştiri almaktadır. Ülkemizde yakın zamanda yaygınlaştırılması planlanan elektronik kimlik kartı uygulaması, seçmenlerin kendi kişisel bilgisayarlarını kullanmasıyla yapılacak seçim uygulamaları konusunda bize avantaj sağlayacaktır.

Bu yazımızda sadece seçmen bilgisayar ve internet kullanarak oylamanın yapıldığı seçim sistemleri üzerinde yoğunlaşacağız. Yazı dizisinin bir sonraki bölümünde DRE (kiosk) tabanlı elektronik seçim sistemleri anlatılacaktır.



1. Doğrudan demokrasi için kriptografi kullanımı

Yazı dizimizin geçen sayılarında elektronik seçim sisteminin kritik bir teknoloji olduğundan, bilgi güvenliğinden insan psikolojisine, kriptolojiden hukuka kadar birçok konuda çözüm gerektiren sorunlar barındırdığından bahsetmiştik [1, 2].

Güvenlik risk ve tehditleri incelendiğinde kriptografi olmadan güvenli ve güvenilir bir e-seçim sistemi yapılamayacağı anlaşılmaktadır. E-seçimin sadece kriptografi ile de kolayca gerçekleştirilebileceği söylenemez. Sistemin açıkları vardır: oy verenlerin yerine başkaları oy kullanabilir, oy verenler sistemi alt etmeye kalkışabilir, yetkililer sistemi kurcalayabilir, oy verme herkesin gözü önünde yapılmadığı için oy verenler de etki altına alınabilir. Diğer taraftan elektronik oy verme sistemlerinden beklenen bazı özellikler birbiriyle çelişir görünmektedir. Örneğin, seçmenin verdiği oyun sayılmasını ve oyun geçerliliğinin kolayca denetlenebilmesini isterken, seçmenin kime oy verdiğinin de kendi dışında kimsenin bilmemesini isteriz. Birçok güvenlik özelliğini barındırması istenen e-seçim çözümleri kolayca bulunamamaktadır. Bunun altında ya temel kriptografik yapıtaşlarının yetersizlikleri ya da teoride çözülmüş gibi görünen problemin gerçek hayatta performans, ölçkleme, yazılım güvenliği veya kullanıcı kolaylığı gibi pratik gereklere yenik düşmesi yatar.

Basit bir çözüm var mı?

E-seçime herhangi bir çözüm ya da uygulanmış örnek sunmadan önce alışlageldik temel yapıtaşlarının neden yetersiz kalabileceği ile ilgili bir fikir jimnastiği yapalım: (Derginin ilk sayısında temel yapıtaşları ile ilgili bilgi bulabilirsiniz [3].)

E-seçimin sağlanması gereken önemli özelliklerden birisi kullanılan oyun gizliliği idi. Oy kullananın adı Bora, sayımı yapanın adı Seçim Kurulu (SK) olsun. Gizlilik nasıl sağlanabilir? Şifrelemeyle. O zaman Bora oy verdiği adayın ismini SK'ya şifreli yollasın. Şifrelemeyi simetrik şifreleme ile deneyelim [3].

Birinci sorunumuz, her seçmen ile SK arasında bir anahtar paylaşımı gerekliliğidir. İkinci sorunumuz, SK güvenilir değilse Bora adına kendisi istediği adaya oy kullanabilir. Çok daha temel bir sorun daha. SK kullanılan oyun gerçekten sayıldığını başkalarına nasıl ispatlayacak? Daha farklı birçok sorun belirtebiliriz fakat sadece simetrik şifreleme ile bu sorunun çözülemeyeceği ortada.

Peki, asimetrik şifrelemeyi deneyelim [3]. Bora, SK'nın açık anahtarını kullanarak şifreleme yapsın ve oyunu göndersin. Fakat bunu Bora'dan başkası da yapabilir. Mesela Bora yerine Erol, Bora'nın gönderdiği adayın ismini değiştirip kendi tarafından gönderilmediğini ispatlamak ve değiştirilmemesini sağlamak için önce imzalasın daha sonra başkaları tarafından öğrenilmemesi için ise SK'ya açık anahtar şifrelemesi ile göndersin. Tercih, sadece gizli anahtara sahip SK açabilir ve

açığında oyun geçerli bir kullanıcıya ait olduğundan emin olabilir çünkü Bora'nın imza açık anahtarını kullanarak imzayı doğrulayabilir ya da imza algoritması mesaj geri kazanımlı ise oyu öğrenebilir. Peki, SK kendisine gönderilen tercihin imzasını nasıl kontrol edileceğini nereden bilecek? Bunun için kendisine gelen mesajın içerisinde Bora'nın kimliği ya da Bora'nın imza sertifikası bulunmalıdır. Bora'nın oyunu başkalarından gizledik fakat Bora arkasında inkar edemeyeceği bir iz bıraktı. Hangi adaya oyunu kullandığını SK'dan da gizlemeliydi! Diğer bir deyişle, anonimlik ortadan kalktı ve oy mahremiyeti ilkesi bozuldu [2].

Bora kullandığı geçerli bir oyu SK'nın açık anahtarı ile şifresin ve bunu kendi özel anahtarı ile imzalasın. Daha sonra bir Kimlik Doğrulama Sunucusu'na (KDS) kimliğini ve oy kullanabilme hakkı olduğunu ispatlasın. KDS geçerli kullanıcıyı doğruladıktan sonra SK'ya sadece şifreli oy pusulasını yollasın. Daha sonra SK kime ait olduğunu bilmediği şifreli mesajları özel anahtarı ile açsa bu mahremiyet sorunumuzu halledebilir. Ancak, burada da Kimlik Doğrulama Sunucusu'nun hile yapmayacağını, geçerli mesajı kimin gönderdiğini SK'ya bildirmeyeceğini ya da Bora'nın oyunu değiştirmeyeceğini varsaymamız gerekir. Ayrıca, Bora oyunun doğru bir şekilde sayıldığından da emin olmalıdır.

Eğer kimlik doğrulayan merkez ile oyu sayan merkezi birbirinden “yeterince” ayırt edebilirsek ve bağımsız hale getirebilirsek belki çözüme bir derece daha yaklaşabiliriz. İşte dergimizin geçen sayısında anlatıldığı üzere “karıştırıcı ağlar” dediğimiz ileri kriptografik yapıtaşları bu nedenle kullanılmaktadır [1].

Çözüm için kullanılacak olası bir başka yöntem de atılan imzanın oyun geçerli olduğu hakkında bilgi vermesi fakat içeriği hakkında bilgi sızdırmaması olabilir. Bu ileri kriptografik yapıtaşı türüne de kısaca “anonim imza” demiştik [1].

Elektronik seçimlerde kullanılacak bir başka parlak fikir ise adayların her pusulada rasgele permütasyonla dizildiği makbuzlu oy pusulalı sistemlerdir. Bu sistemleri “görsel kriptografik” olarak adlandıracağız. “Punchscan”, “Three Ballot”, “Scantegrity”, “Prêt à Voter” gibi görsel kriptografik sistemleri ileriki yazı dizisinde anlatmaya çalışacağız [4, 5, 6, 7].

Elektronik seçim türlerini daha kolay sınıflandırmak için

- kağıt tabanlı görsel sistemlere **k-seçim**,
- makine tabanlı sistemlere **m-seçim**,
- internet kanalıyla oy kullanmaya da **i-seçim** diyeceğiz.

Elektronik seçim kullanan seçmenlere de **e-seçmen** diyeceğiz. Bu türlerin hepsi **e-seçim** olarak kabul edilir.

İnternet tabanlı seçim sistemleri (i-seçim)

Oyumuzu seçim zamanı süresince istediğimiz zaman, istediğimiz yerden hatta yurtdışından dahi kullanabilirsek ne güzel olurdu değil mi? İnternet tabanlı bir oylama sistemi bize bunu sağlayabilir. Özellikle sandık başına gelmesi çok müşkül engelli seçmenlerin oy kullanabilmeleri demokrasi adına da büyük bir kazanç olabilir. Diğer yandan, kullanıcılar alışkanlık kazandıkça zaman içerisinde seçim otoritelerinin yükünün azalacağı, oyların çok daha hızlı ve zahmetsiz sayılacağı ve bu sayede seçim maliyetlerinin düşeceği de tahmin edilmektedir

İnternet tabanlı elektronik seçimi 2005 yılında ülke genelinde ilk defa uygulamaya koyan ülke Estonya'dır. Bu ülkedeki deneyimi yakından inceleyen Norveç ise 2011 yılı sonlarına doğru internet üzerinden seçimi uygulamaya koyacak bir diğer ülkedir. ABD yurtdışındaki vatandaşlarının oy kullanabilmesi için bir çalışma yürütmektedir [8]. 2011 Ekim ayından itibaren uygulamaya konulması planlanmaktadır [9]. Bu yazımızda sadece Norveç ve Estonya'nın internet tabanlı seçim sistemlerini inceleyeceğiz. Kullanılan kriptografik yöntemler kısaca anlatılacak, öngörülerimizin ne kadar gerçekçi olduğunu irdeleyecek ve muhtemel bazı sorunlara değineceğiz.

2. Estonya'da i-seçim

Estonya'da e-seçim araştırmaları 2001 yılında koalisyon hükümetinin e-devlet konularını desteklemesi sayesinde hızlandı. K-seçimin yanında i-seçimin de yapılabilmesi için 2002 yılında i-seçimin yürütmesinden sorumlu yasal bir kurum oluşturuldu. 2003 yılında Ulusal Seçim Kurulu tarafından i-seçim projesi resmi olarak başlatıldı. 2005 yılında dünyada internet yoluyla yerel seçimlerde ülke çapında vatandaşlarına oy kullandıran ilk ülke oldu. Bunu; 2007 genel seçimleri, 2009 belediye seçimleri ve Avrupa Parlamentosu seçimleri takip etti. Dergiye yazı hazırladığımız şu günlerde kimlik doğrulama sisteminin de devreye girdiği

2011 genel seçimlerinde i-seçim kullanıcılarının sayısı daha önceki seçimlerdeki i-seçim kullanıcılarının sayısından çoktan geçmişti [10, 11, 12, 13].

Estonya i-seçim sistemi kullanıcı geri beslemeleri ve güvenlik analizleri sonucu güncellenmekte, yeni özelliklerle geliştirilmektedir. Bu sayede zaman içerisinde daha sağlam, daha güvenli ve daha güvenilir bir sistem haline gelmektedir.

Estonya'da nispeten başarılı görünen i-seçim uygulamasında hükümetin konuya verdiği destek kadar halkın internet okuryazarlığının da önemi büyüktür. 2010 yılı tahminlerine göre 1.3 milyonluk ülkede 1000'den fazla ücretsiz internet kullanım alanı bulunmaktadır. Uluslararası Telekomünikasyon Birliği (ITU) rakamlarına göre 2000 yılında %30'un altında olan internet kullanıcı oranı hızla artarak 2010 yılında %75'i geçmiştir. Dijital kanalların kullanımı giderek artmakta olup hanelerin %60'ında internet erişimi vardır ve bunun %90'ı geniş bant erişimlidir. Devlet sadece evlerde değil kafelerde, restoranlarda hatta benzin istasyonlarında dahi yüksek bant erişimini yaygınlaştırmaktadır. İnternet bankacılığı kullanım oranı % 86, mobil penetrasyon % 95 olarak ölçülmüştür. Estonya'da 2 milyon cep telefonu hesabı bulunmaktadır.

Estonya, uzaktan kimlik tanımlama ve sayısal imza fonksiyonlarını içeren ulusal elektronik kimlik kartının kullanımının zorunlu olduğu ilk ve tek ülkedir. Nüfusun neredeyse tamamı elektronik kimlik kartına sahiptir. İnternette vergi beyannamesinin gönderilmesi gibi

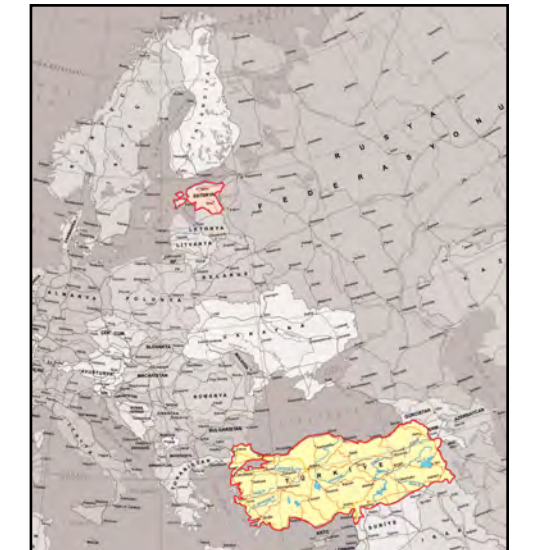


Şekil 1. Estonya haritası.

hizmetlere Estonyalılar alışkıdır. Birçok e-devlet hizmetinin verilmesinden dolayı eJournalUSA dergisinde “Estonya, e-Stonya oluyor” başlıklı bir yazı bile yayımlanmıştır [14].

2001 yılında başa gelen koalisyon hükümetinin diğer e-hizmetlerinin de ana gayesi olan kamu sektörünün daha etkin, verimli ve müşteri odaklı çalışabilmesi amacıyla dijital teknolojiyi kullanma iradesi sonucu Estonya'da e-seçim konusunda çalışmalara büyük destek verilmiştir. İlk uygulama olarak 2005 yılı yerel yönetim konseyi seçimleri hedeflenmiş ve başarıyla uygulanmıştır. Birçok ülkede, elektronik seçim yöntemi olarak sandık yerine elektronik oylama makineleri kullanılmakta iken Estonya bunu tercih etmemiş, internet üzerinden uzaktan oylama yöntemini seçmiştir. Estonya hükümetinin ana hedefi klasik sandıklı sistemlere benzeyen bir oy kullanımı yerine seçmenlere gerçekten farklı bir alternatif oluşturmak, yeni bir oy kullanma fırsatı yaratmak ve dolayısıyla seçmen katılımının artırılmasını sağlamak olmuştur.

Aşağıdaki iki fonksiyonel gereksinim genelde farklı ülkelerde uygulanmak zorunda kaldığı, ancak Estonya hukukunda bulunmayan ve teknik çözümün de doğrudan desteklenmediği durumlardır: Aslında her ikisi de geleneksel kağıt tabanlı oylamanın üstünlüğü ilkesi temelinde gerçekleştirilmektedir.



Estonya'da internetten oy kullanma dört defa uygulanmıştır:

» Ekim 2005 yılında Yerel Yönetim Kurulları seçimlerinde

- 9317 e-seçmen 9681 elektronik oy kullandı.
- E-seçmen katılımı % 0.9 idi. Bu oran, o günden bu yana giderek büyüdü.
- Ulusal Seçim Otoritesine veya mahkemelere hiç şikayet gelmedi.

- Teknik sorun yaşanmadı.
- IT gözlemcilerden olumlu geri dönüşler alındı.
- » Mart 2007'de Parlamento seçimleri
- Bağlayıcı resmi sonuçlar olarak kabul gören ülke çapındaki ilk defa internet kanalıyla e-seçim uygulandı.
- 30275 elektronik oy kullanıldı.
- » 2009 yılı Haziran ayında Avrupa Parlamentosu seçimleri ve 2009 yılı Ekim

ayında Yerel Yönetimler Konseyleri seçimleri

- Yerel Yönetim Kurulları seçimlerinde, 2009 yılında 104413 e-seçmen ve 104313 elektronik oy kullandı.
- E-seçmen katılımı % 9,5 idi.
- » Estonya'daki internetten oylama sistemini 10.000 e-seçmen kullanmıştır. Rakam fazla olmamasına rağmen e-seçime olumlu bakıldığını göstermesi açısından başarı olarak kabul edilebilir.

• Oyların seçmen tarafından iptali:

Elektronik olarak verilen oyun iptal edilmesinin mümkün olması.

• **Boş oy :** Hiç kimseye oy verilmemesi veya boş oy verilmesine imkan tanınması.

Dergimiz yayına hazırlandığı sıralarda 2011 genel seçimlerinde de i-seçim uygulandı. (140.846 seçmen, yani katılan seçmenlerin yaklaşık %25'i i-seçimle oy kullandı [15, 16].)

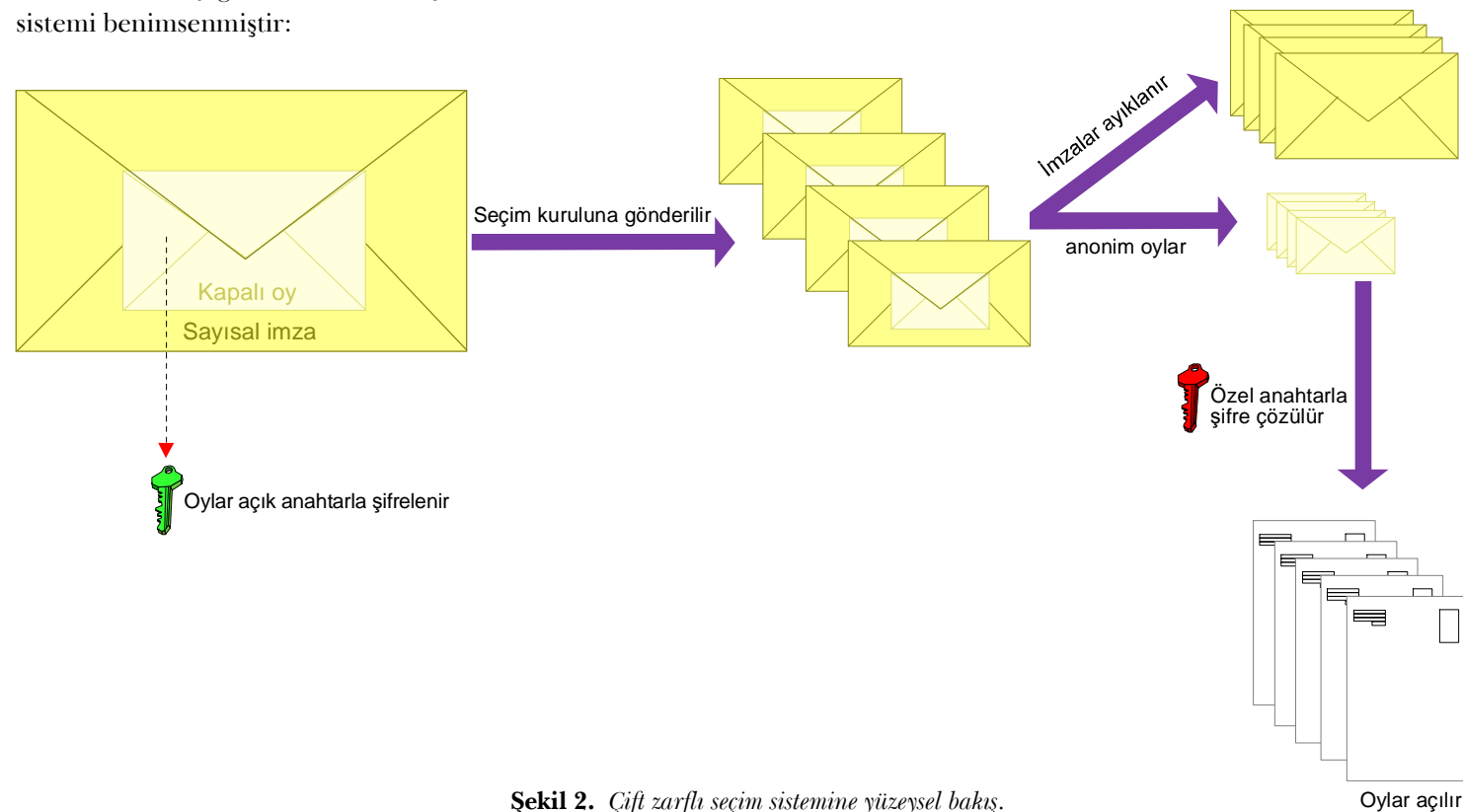
2005 yılından itibaren seçimlerde sisteme yeni özellikler eklenmiş ve nihayetinde temel esasları aşağıda belirtilen i-seçim sistemi benimsenmiştir:

- Seçmenlerin kimlik tanımlama ve kimlik doğrulamaları elektronik kimlik kartları veya cep telefonu ile yapılabilir.
- E-seçmen oylama süresince istediği sayıda oy verebilir. Sadece, son kullanılan oy sayılacaktır.
- Geleneksel kağıt tabanlı oy sistemi her zaman önceliklidir. Eğer seçmen k-seçimde oy kullanırsa elektronik olarak kullandığı oylar iptal edilecektir.

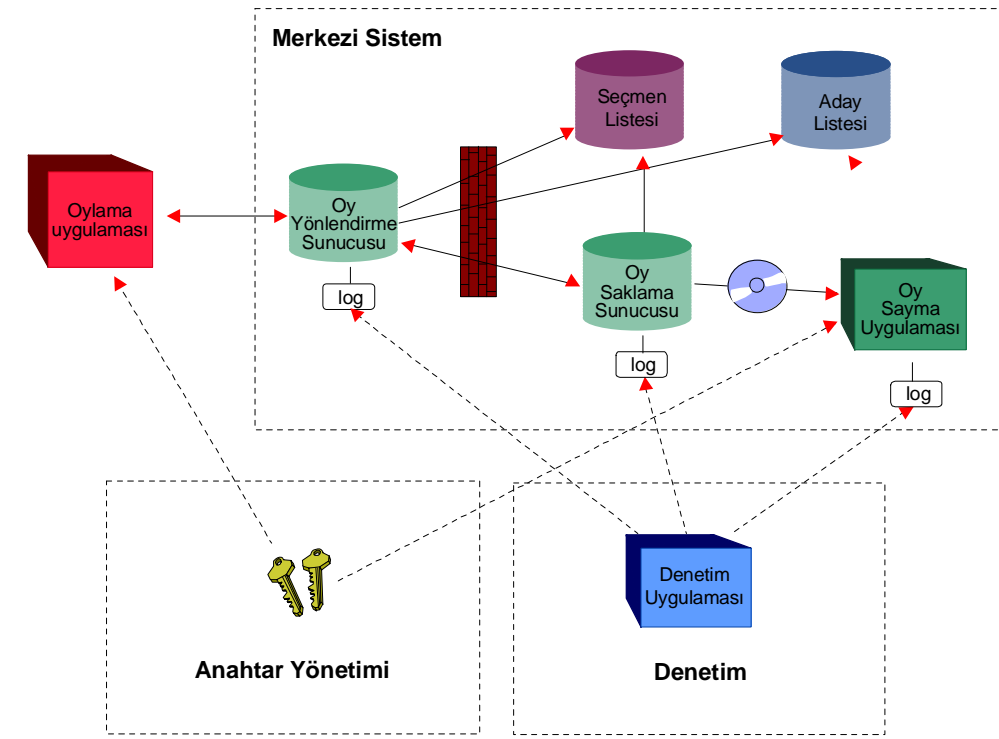
2.1. Estonya i-seçim sistemi adımları

Estonya'daki e-seçim sistemi genel olarak şu adımlardan oluşur (Şekil 2):

1. Seçmene, bilgisayar ortamında şifreli oy olan bir "iç zarf" ve sayısal imzalı bir "dış zarf" oluşturulur.
2. Seçmen kurumsal bir e-seçim web sitesini açar ve kendisine ait elektronik kimlik kartı ile web sitesine kimliğini doğrular. Kimlik doğrulandıktan sonra istemci uygulaması indirilebilir.



Şekil 2. Çift zarflı seçim sistemine yüzeysel bakış.



Şekil 3. Estonya e-seçim sistemi mimarisi.

3. Seçmen, istemci uygulamasını çalıştırır ve seçim sistemine kimliğini doğrular. İstemci uygulaması, seçmeni Oy Yönlendirme Sunucusuna bağlar.

4. Kimlik doğrulanmasının ardından, Oy Yönlendirme Sunucusu seçmene aday listesini gönderir. Seçmen bu listeden bir aday seçer.

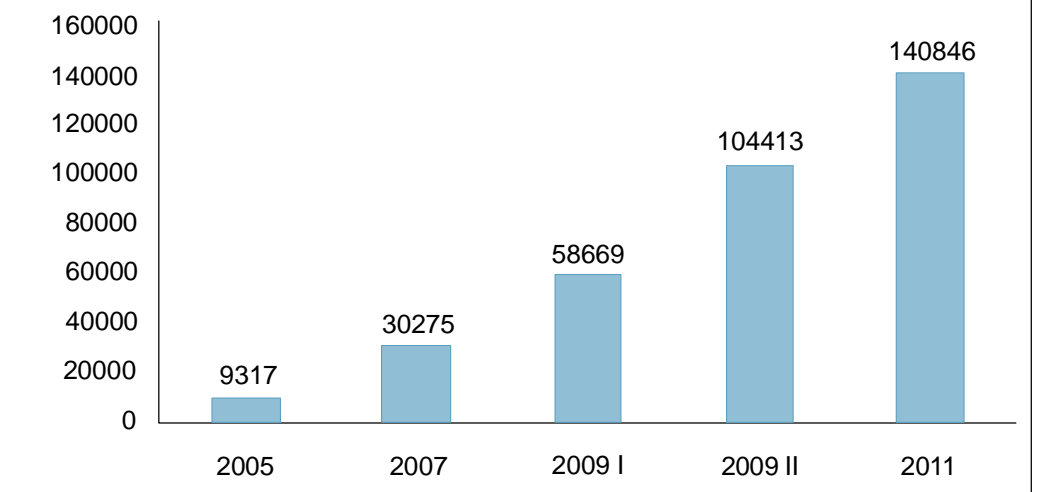
5. İstemci uygulaması Oy Sayım Sunucusunun özel anahtarı ile seçmenin oyunu şifreler ve kendisine ait imza özel anahtarı ile imzalar.

6. Oy Yönlendirme Sunucusu seçmenin bu oyunu Oy Depolama Sunucusuna gönderir.

7. Oy Depolama Sunucusu Açık Anahtar Altyapısı (AAA) sistemi ile iletişim kurar ve kişinin kimliğini doğrular. Oy Depolama Sunucusu oyu veritabanına kaydeder ve Oy Yönlendirme Sunucusuna onay gönderir. Oy Yönlendirme Sunucusu da istemciye oyun başarıyla alındığını gösteren onay bilgisi gönderir.

8. Oy kullanma süresi sona erdiği zaman Oy Depolama Sunucusu oyları sıralar ve çift oyları veya kağıt tabanlı sistemde oy

kullanıcıları iptal eder. Oy Depolama Sunucusu daha sonra oyların üzerindeki elektronik imzayı kaldırır. Bu kaldırma işlemi pek çok farklı kesimden gelen gözetmenler tarafından izlenir (bu gözetmenler başta seçim otoritesi olmak üzere partiler, sivil toplum örgütleri, dernekler gibi farklı gruplardan oluşabilir).



2005 - Yerel seçimler
2007 - Milletvekili seçimleri
2009 I - Yerel seçimler
2009 II - Avrupa Parlamentosu seçimleri
2011 - Milletvekili seçimleri

Şekil 4. Estonya'da yıllara göre i-seçmen sayısı.

Estonya'daki uzmanlar geçen dört uygulamadan sonra şu derslerin çıkarıldığını belirtmişlerdir:

- **İ-seçim için bilgisayar okuryazarlığı önemlidir:** Bilgisayar okuryazarlığı yeterince yüksek ise internetten oy kullanma çabucak benimsenmektedir.
- **İ-seçim için Elektronik Kimlik Kartı kullanımı gereklidir:** Eğer seçmenlerin kimlikleri ile açık anahtarları arasındaki ilişkiyi kanuni hükümler çerçevesinde resmileştiren güvenilir ve yaygın bir Açık Anahtar Altyapısı bulunuyor ise internetten oy kullanma mümkündür.
- **İ-seçim başarılı bir şekilde uygulanabilir:** Elektronik seçim özenli ve dikkatli bir şekilde tasarlanırsa kullanıcıların benimseyeceği bir i-seçim gerçekleştirmek mümkündür.
- **E-seçim sadece farklı bir oy kullanma kanalıdır:** Elektronik seçim sadece seçmenlere farklı tercihleri sunmanın başka bir yoludur. Farklı kanallar sunarak katılımın artırılması hedeflenmektedir.

• **Seçmen tutum ve davranışlarının değişimi zaman alır:** İnsanların davranış ve tutumlarının değişiklikleri birkaç gün içinde değişmez. Estonya'nın yüksek internet okuryazarlığının dünyada zirvelerde yer aldığı ve birçok ülkenin bu konuda çok geride olacağı düşünülürse, i-seçim gibi teknolojilere vatandaşların alışması bazı ülkelerde on yıllarca hatta nesiller boyu sürebilir.

• **İ-seçim ve internet bankacılığı arasındaki fark:** İ-seçim en az internet bankacılığı kadar güvenlidir, hatta gözlenen durum analizlerine bakılırsa daha güvenli olduğu bile söylenebilir.

2.2. Estonya'da i-seçim için elektronik kimlik kartı altyapısı



Estonya'da, internetten oy kullanma deneyimindeki büyük başarının önemli etkenlerden biri de hükümet ve ülkenin büyük bankalarının elektronik kimlik kartları uygulamalarını

desteklemesidir. İ-seçimlerde Estonya ID (elektronik kimlik) kartı kullanılmıştır.

E-devlet işlemlerinde bütün vatandaşlar tarafından kimlik doğrulama için zorunlu olarak kullanılan ID kartı kriptografik uygulamaları ve Estonya Açık Anahtar Altyapısı desteğiyle, i-seçim güvenli bir şekilde bağlanmayı ve kimlik doğrulamayı mümkün kılmıştır. Mart 2007 itibarıyla 1.3 milyonluk nüfusa yaklaşık 1,1 milyon elektronik kimlik kartı dağıtılmıştır.

2.3. Seçim süresi

Estonya seçimlerinde vatandaşlara kağıt tabanlı seçimin ilk gününden 6 ila 4 gün öncesine kadar internet üzerinden oy kullanımı imkanı sağlanmıştır. Bu süre içerisinde seçmenler istedikleri kadar oy kullanabilir, fakat en son kullandıkları oy geçerli sayılacaktır. Ayrıca, seçmenlerin seçim günü, oy merkezlerinden de oy kullanabilmelerine müsaade edilmiştir. Yasal olarak seçim merkezlerinde kullanılan oy internet ortamında kullanılan oya üstünlük sağlamıştır, yani eğer kişi hem elektronik ve hem de seçim merkezlerinden oy kullanırsa seçim merkezindeki oy geçerli sayılacaktır. Seçim günü elektronik oylamayı değiştirmek mümkün değildir, tek yolu seçim merkezine uğrayıp tekrar oyunu kullanmaktır.

Ağustos 2005'te Estonya Cumhurbaşkanı Arnold Rütel, elektronik seçim sisteminin seçmene potansiyel olarak birden fazla oy kullanıma imkan tanıdığı, bunun da "Bir kişi, bir oy" ilkesine aykırı olduğu yönünde itiraz ederek Estonya Anayasa Mahkemesi'ne başvurmuş fakat itiraz reddedilmiştir.

Bakın geçmişte kimler ne söylemiş? [17, 18]:

- IBM'in kurucu başkanı Thomas J. Watson – 1943: "Sanırım dünyaya 5 bilgisayar yeter de artar bile."
- Kenneth Olsen, Digital Equipment Corp. – 1977: "İnsanların evlerinde bilgisayar bulundurmaları için herhangi bir neden göremiyorum."
- Warner Brothers Pictures kurucusu Harry Warner – 1927: "Kim film izlerken aktörlerin sesini duymak ister ki?"

Estonya'daki seçimlerde kullanılan teknolojiler

- **İşletim sistemi:** Windows (Microsoft Active Accessibility dahil), Linux, Macintosh
- **Güvenlik:** Oy gizliliği için Asimetrik Şifreleme, Seçmenin kimlik doğrulaması için Sayısal İmza, Seçmen ile sunucu arasındaki iletişimin güvenliği için HTTPS
- **Program dili:** C/C++
- **Kullanılan araçlar:** İnternet, akıllı kartlar, bilgisayar, sunucular

2.4. Estonya seçimlerinde mobil telefon kullanımı

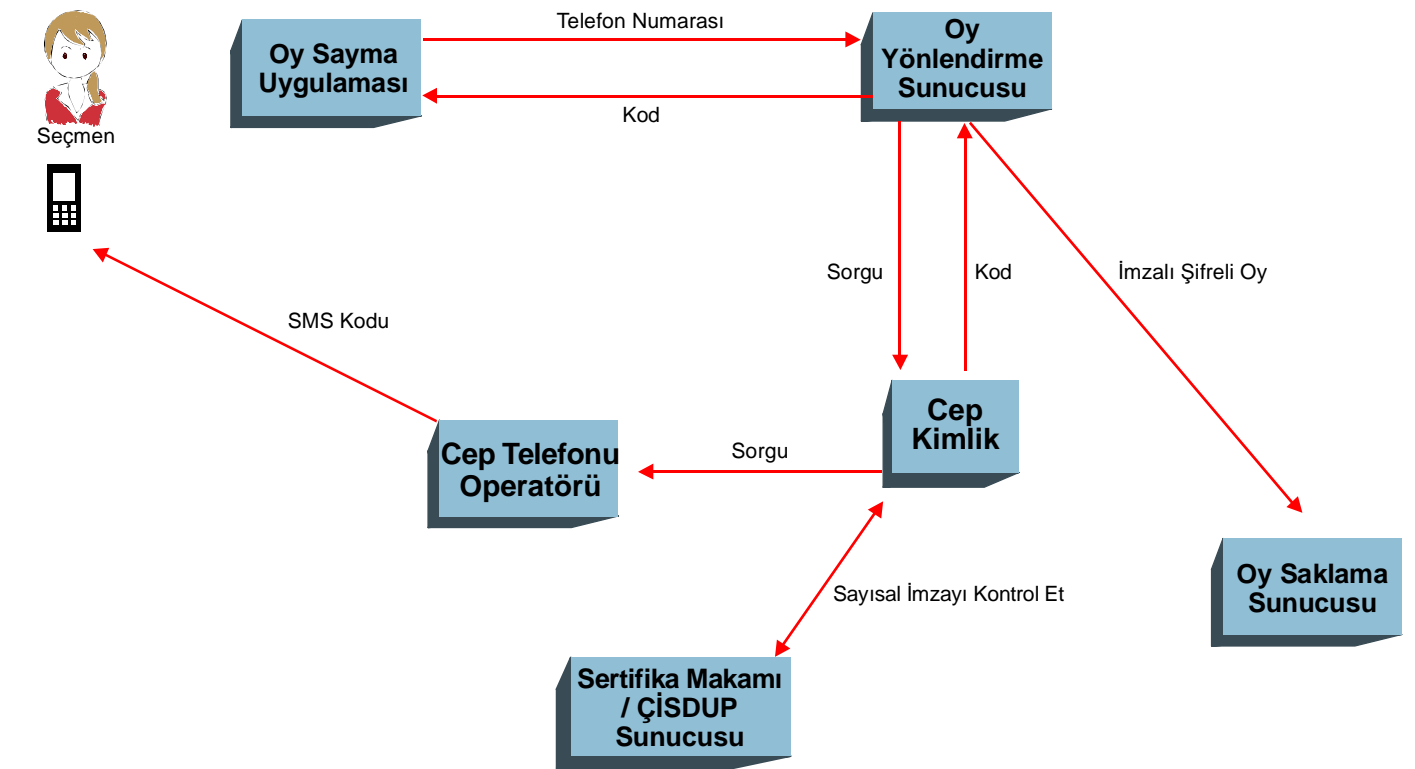
Estonya, vatandaşlarının cep telefonu ile oy kullanmasına izin vererek dünyada bir ilki daha gerçekleştirmiştir. Aralık 2009'da çıkan bir yasayla Estonya vatandaşları cep telefonu yardımıyla kimlik doğrularak oy kullanabileceklerdir. Yasanın ilk uygulaması 2011 genel seçimleri olacaktır.

Elektronik Seçim: İnternet Üzerinden Oylama



Şekil 5. Bilgisayardan oy kullanma örneği.

Cepten oylama sistemi, seçmenlerin kimlik doğrulama sistemleri için gerekli olan ve seçmenlere ücretsiz bir şekilde verilen bir çip aracılığı ile olur. Şu anda oylama için kimlik doğrulaması ve dijital sertifikalar içeren çipleri sadece Eesti Mobil Telefon (EMT) operatör şirketi müşterilere ulaştırmaktadır. Bunun yanında özel SIM kartı sağlayan diğer mobil operatörleri de kendi programları üzerinde çalışmaktadır. Estonyalı yetkililer; bilgisayar korsanlığı saldırıları, kimlik sahtekarlığı ve sahte oy kaygılarına rağmen 2007 yılında



Şekil 6. Mobil ID sistem mimarisi.

Bir ulusal güvenlik kurumu sistemin güvenliğini sağlamaktan ve garanti etmekten sorumlu olacaktır. Aynı zamanda, cep telefonu da sistemde yer alacaktır. Bu nedenle, hükümet ile cep telefonu operatörleri arasında güçlü bir güven gereklidir. Çoğu cep telefonu operatörlerinin özel sektöre ait olmasından dolayı, her türlü güvenlik ihlaline karşı bu konuya özel bir ilgi verilmektedir.



Şekil 7. Hepsini aynı kapıya çıkıyorsa hangi yöntemle oy kullandığımızın ne önemi var?

2.5. Estonya i-seçim sonuçları ve istatistikleri

2005 yılında Estonya'da ulusal ve yerel seçimlerde kullanılan i-seçimde 9317 kişi elektronik oy kullandı [19]. Şubat 2007 yılında kullanılan genel seçimleri için ilk i-seçimde 30.275 vatandaş oy kullanmıştır, bu da her 30 seçmenden birinin internet kanalıyla oy kullandığı anlamına gelmektedir [20]. 2009 yerel seçimlerinde, 104.415 kişi internet üzerinden oy kullanmıştır [21]. Yani, seçmenlerin yaklaşık % 9,5'i internet üzerinden oy kullanmıştır [22]. Dikkatle incelenirse katılımın 2004 yılında 2009 yılına kadar on kat arttığı görülür.

2.6. Uygulama ve yönetim yaklaşımı

İnternet yoluyla oy kullanma projesine (iVote projesi), kamu ve özel sektörden çok sayıda aktörler katılmıştır. Kamu ve Özel sektör tarafları arasındaki sağlam işbirliği, iVote'u başarılı kılmıştır. İnternet oylama projesinin lideri Ulusal Seçim Kurulu (www.vvk.ee) olmuştur. Ana ortakları ise:

- 1) Estonya Parlamentosu (www.riigikogu.ee) internet yoluyla oylama yapılabilmesi için yasal olanakları sağlamıştır.
- 2) Estonya Parlamentosu, Başbakanlık ve Ulusal Seçim Kurulu için operasyonel ve büro destek sağlayıcısı olarak da görev üstlenmiştir.

Tablo 1. Estonya'nın internet yoluyla yapılan seçimlerin istatistikleri

	2005 Yerel Seçimleri	2007 Milletvekili Seçimleri	2009 Avrupa Parlamentosu Seçimleri	2009 Yerel Seçimleri
Toplam seçmen	1 059 292	897 243	909 628	1 094 317
Oy kullanan seçmen	502 504	555 463	399 181	662 816
Seçmen katılımı	% 47,40	% 61,90	% 43,90	% 60,60
İnternette kullanan seçmenler	9 317	30 275	58 669	104 413
İnternette oy kullanan seçmenlerin tüm seçmenlere oranı	% 0,9	% 3,4	% 6,5	% 9,5
İnternette oy kullanan seçmenlerin oy kullanan tüm seçmenlere oranı	% 1,9	% 5,5	% 14,7	% 15,8
İptal edilen internet oy (kağıt oy pusulası ile değiştirildi)	30	32	55	100
Birden fazla internet oyu	364	789	910	2 373
Uzaktan oy kullanan seçmenlerin (posta, internet, konsolosluk vb) internet kanalını kullanma oranı	% 7,20	% 17,60	% 45,40	% 44
İnternet oylama dönemi	3 gün	3 gün	7 gün	7 gün

Elektronik Seçim: İnternet Üzerinden Oylama

3) İçişleri Bakanlığı (www.sisemin.gov.ee) nüfusun kimlik onaylama sistemlerinin kaydını ve değişikliklerini yürütmüştür.

4) Estonya'nın başkenti ve en büyük şehri olan Tallinn'de (www.tallinn.ee) ilk deneme yapılmıştır.

5) Sertifikasyon Merkezi Ltd Şirketi (www.sk.ee) elektronik kimlik doğrulama kartlarından sorumlu olmuş ve altyapı ve değişiklikleri yürütmüştür.

6) Cybernetica Ltd Şirketi (www.cyber.ee) yazılım geliştirici olarak görev almıştır.

7) KPMG Baltık Ltd Şirketi (www.kpmg.ee) ve PricewaterhouseCoopers şirketi (www.pwc.ee) denetçi olarak görev almıştır.

8) Estonya Bilişim Merkezi ise (www.ria.ee) hizmet/barındırma ortağı ve güvenlik olaylarının işleyicisi olarak görev almıştır.



Şekil 8. Ülkemizde elektronik seçim uygulanmalı mı?

Bakın geçmişte kimler ne söylemiş? [17, 18]

- ABD Patent Dairesi Başkanı Charles Duell – 1899: "Keşfedilecek her şey çoktan keşfedildi.
- Microsoft kurucu başkanı Bill Gates – 1981: "640 Kb'lık hafıza herkese yetecektir."
- Henry Ford'un kredi talebi üzerine otomotiv sektörünün geleceği konusunda ekspertiz veren bir banka müdürü - 1903 : "Atlar her zaman kullanılacaktır. Otomobil ise ancak geçici bir moda olabilir."

iVote projesinin sistem yönetimi, ana işlevsel görevleri yanında büyük ölçüde güvenliğe odaklanmıştır. Sistem yalnızca oy sırasında çevrimiçi hale getirilmiş, oy gizliliği gelişmiş ileri şifreleme teknolojileri kullanılarak garanti altına alınmıştır. Tüm kritik işlemler denetlenmiş ve videotıyp aracılığı ile kayıt altına alınmıştır.

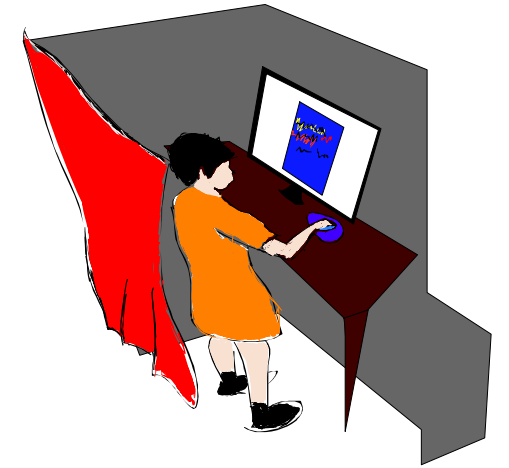
Unutulmamalıdır ki iVote projesi seçmenlere sadece oylama için ek bir kanal sağlar. İnternette oylama geleneksel yollarla kullanılan oylamadan vazgeçmek anlamına gelmez. Bu proje kullanıcılar açısından tam bir hizmet sunmaktadır. Seçimlerden önce her seçmene takvim ve farklı oylama yöntemlerini anlatan bir seçmen kartı posta yoluyla gönderilir. Seçmen kayıtları nüfus kaydına dayalı olduğu için yeni ön kayıt gibi ekstra iş yüküne gerek kalmamaktadır. Bir seçmen eğer interneti diğer yöntemlere tercih etmek isterse nüfusun % 90'u tarafından kullanılan ve kolayca elde edilebilen elektronik kimlik kartını kullanarak hiçbir ekstra çaba sarf etmeden seçimini yapabilir.

2.7. Estonya'da i-seçimin etkileri

Estonya'da yerel seçimler 7 gün sürmüştür. İ-seçim ise klasik kağıt tabanlı seçimin bitimine 4 gün kalana kadar gerçekleşmiştir. Yeni nesil kimlik kartı, seçmen kimlik doğrulaması için kullanılmıştır. Kimlik doğrulamasıyla oy kullanabilecek seçmenler, seçimlerden önce ulusal nüfus kayıt merkezindeki veritabanına kaydedilmiştir. Merkezi kayıt sayesinde seçmenlerin ek kayıt için fazladan iş yapmalarına gerek kalmamıştır. İ-seçim uygulamasıyla birlikte seçmenlerin belirli bir merkezde oy kullanmaları zorunluluğu ortadan kalkmıştır. Engelli

vatandaşlardan tutum da işlerinden dolayı oy kullanamayanlar veya yurtdışında yaşayan vatandaşlar için sayısız avantajlar ortaya çıkmıştır.

Araştırma ve tecrübeler yeni bir ek oylama kanalının seçmen katılımı üzerinde mutlak bir etkisinin olmadığını göstermektedir. Seçimlerde oy kullanma gibi geleneksel davranışları değiştirmek zaman almaktadır. İnternet kanalıyla oy kullanımını artırmak için elektronik kimlik kartı kullanımının toplumda çok daha geniş kitlelerce benimsenmesi gerekmektedir. Ancak yine de, dört yıl sonraki ikinci seçimlere (2005-2009) elektronik ortamda 10 kattan daha fazla bir katılımın olması, bu yöntem zaman içerisinde daha fazla güven duyulacağını göstermektedir.



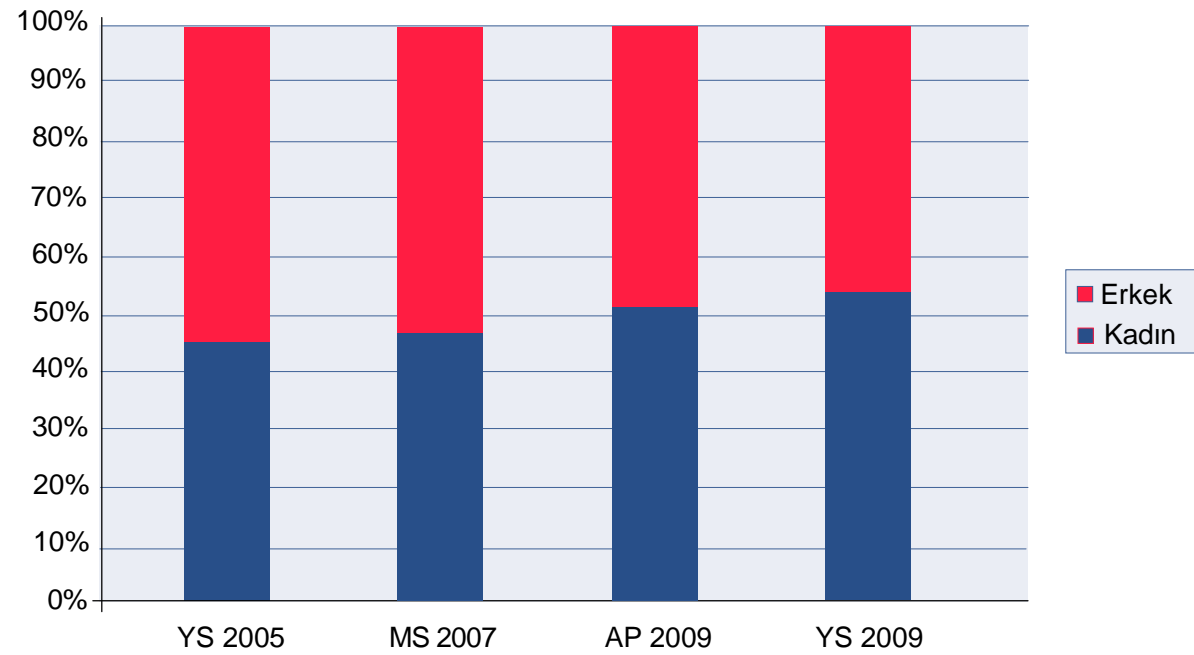
Şekil 9. Seçim merkezinde de internette oy kullanabilirsiniz.

Estonyalı uzmanlar elektronik kimlik kartlarının olmaması durumunda masrafların çok daha fazla olacağını altını çizmişlerdir. Seçim Kurulu geliştirme aşamasında 6 yıl içerisinde 500.000 €dan daha az masrafla sistemi kurduklarını belirtmişlerdir. 2005 yılındaki ilk uygulamasından sonra yeni oylama sisteminin maliyeti tüm seçim masraflarının yaklaşık % 20'sini oluşturuyordu. 2009 seçimlerinde ise bütün maliyetler göz önüne alındığında, elektronik seçimin maliyeti toplam masrafların % 5'ine düşmüştür. Uzun vadede uygulama maliyetinin ciddi bir şekilde yükselmesi de beklenmemektedir. Ayrıca yine uzun vadede internette oylamanın tamamen geleneksel kâğıt tabanlı sistemin yerine geçmesi öngörülmektedir.

Teknoloji, demokratik sürecin önemli bir parçasıdır. iVote projesi kamu-özel sektör ortaklığının meyvesidir ve teknolojinin getirilerini demokrasi adına kullanmak yönünden iyi bir örnek olabilir. Yine de bu projenin sürdürülebilirliği, sadece gelişmiş teknolojilerin kullanılmasına değil, katılımcı sayısına ve devlet tarafından güvence altına alınmasına bağlıdır. Bununla beraber seçmenin internette oylamayı kabulü ve katılımı konusundaki tavrının anlaşılması için belirli bir sürenin geçmesi gerekmektedir.

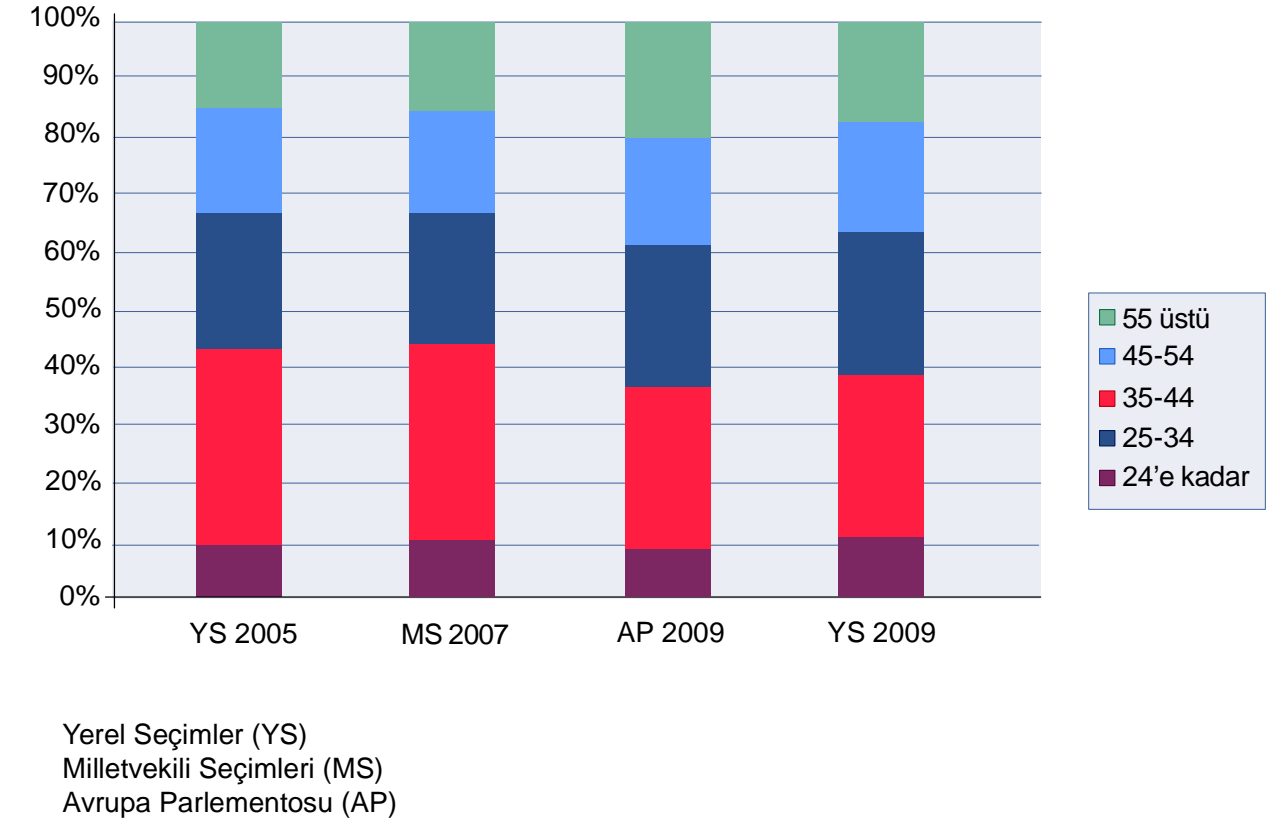
2.8. İ-seçimin getirdiği yenilikler

Gelişmiş ülkelerin çoğunda oy kullanım oranı düşmektedir. Düşük katımlı bir seçim toplumun genel temayüllerini yansıtmakta eksik kalabilir. Bu problemi çözebilmek için, özgür ve adil seçimler ilkesine uyularak ve teknolojik eğilimler göz önünde bulundurularak seçmenlere farklı oylama olanakları üzerinde yoğun çalışmalar yapılmaktadır. Temsili demokrasiyi teşvik etmek ve güçlendirmek için anayasal prensiplere uygun olarak seçimlerde farklı yöntemlere başvurulmuştur. Örneğin, i-seçim son yıllarda kullanılan yeni ve farklı yöntemlerden biridir. İ-seçimin uygulanmasıyla seçmenlerin özellikle de genç kuşakların ilgileri çekilerek oy kullanmaya teşvik edilebilir. Böylece başta bahsettiğimiz düşüş tersine çevrilebilir. İ-seçim bilgi toplumu bünyesinde yeteri kadar kabul gördüğünde şu anki kâğıt tabanlı oylama sistemi gibi "geleneksel" bir yöntem dönüşebilir.



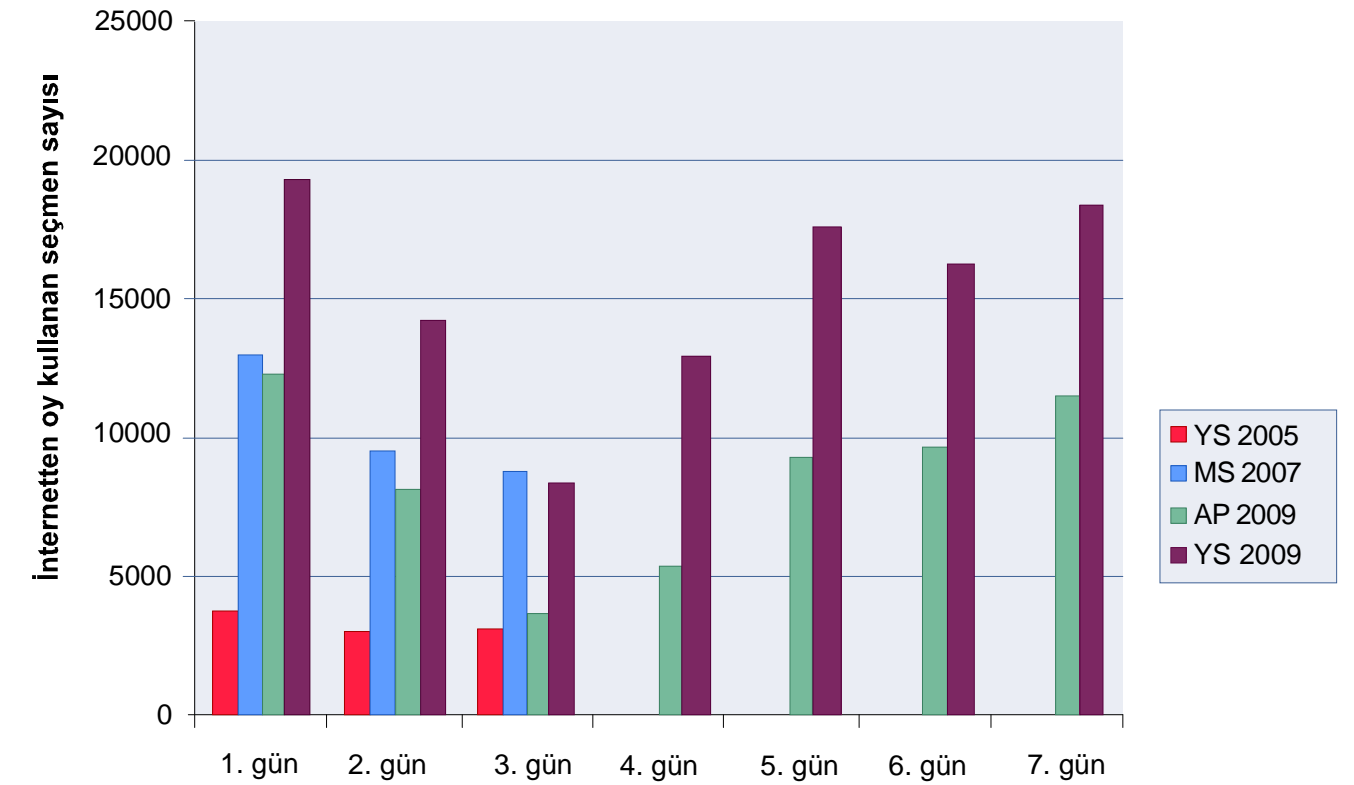
Yerel Seçimler (YS)
Milletvekili Seçimleri (MS)
Avrupa Parlamentosu (AP)

Şekil 10. Cinsiyetlere göre internette oy kullanma oranı.



Yerel Seçimler (YS)
Milletvekili Seçimleri (MS)
Avrupa Parlamentosu (AP)

Şekil 11. Yaşa göre internette oy kullanma oranı.



Yerel Seçimler (YS)
Milletvekili Seçimleri (MS)
Avrupa Parlamentosu (AP)

Şekil 12. Günlere göre internette oy kullanma oranı.

3. Norveç'te 2011'de uygulanacak i-seçim sistemi

Norveç'in oylama sistemini anlatmadan önce bu ülkeyle bir kaç bilgi vermek faydalı olacaktır.

Norveç dünyada işsizliğin en düşük, çalışanların hayat standartlarının ve kişi başına düşen verimliliğin en yüksek olduğu ülkelerden birisidir. Eğitim, teknoloji ve demokrasi anlamında da dünyanın en gelişmiş ülkeleri arasındadır. Teknoloji kullanımı ve iletişim altyapısı çok iyi durumdadır ve hayatın her noktasında kullanılmaktadırlar.

4,9 milyon nüfuslu bir ülke olan Norveç'in 2000 yılında 2,4 milyon internet kullanıcı bulunmaktayken bugün nüfusun %95'i internet kullanmaktadır. Birçok ülkede kullanıcı alışkanlıkları nedeniyle benimsenmeyeceği düşünülen bazı uygulamalar Norveç için geçerli olabilir. Örneğin, bazı ülkeler için uygulaması zor olan bir uygulama olan çift zarf yönteminin elektronik versiyonu. Norveç seçimlerinde zaten mevcut kağıt tabanlı sistemde bu yöntem kullanılmaktadır. Birçok ülkede elektronik seçim sistemlerinde büyük sorun çıkaracağı düşünülen sistemin zorlama ve oy satın almayı kolaylaştıracağı ve dolayısıyla oy mahremiyetini kaldıracağı algısı, Norveç vatandaşları arasında çok yüksek olmayabilir.



Şekil 13. Norveç haritası.

Norveç Yerel Yönetimler ve Bölgesel Kalkınma Bakanlığı (KRD), e-seçimin uygulanabilirliği açısından halkın beklentilerinin önemli bir rol oynayacağını bilinciyle, 26 Mayıs 2004 tarihinde bir çalışma komitesi atamıştır. Bu komitenin başlıca amacı ülkedeki elektronik seçimin uygulanabilirliği hakkında ülkedeki potansiyelin araştırılması ve potansiyelin yüksek olması durumunda ülkeye uygun bir sistemin önerilmesidir.

Yetkinliklerine göre komite üyeleri aşağıdaki araştırılacakları konular açısından dört alt gruptan oluşmuştur:

1. E-seçim teknikleri,
2. Ekonomik ve idari hususlar,
3. Demokratik yönleri üzerinde araştırmalar
4. Hukuki durum

Alt komisyonların kendi arasında yaptıklarının yanı sıra bir dizi genel komite toplantıları düzenlenmiş ve görüşler e-seçim raporunda sunulmuştur [23].

E-toplum sürecinde Norveç, elektronik seçim uygulamayı düşünmekle kalmamış, 2011 yılındaki yerel yönetim seçimlerinde hayata geçirmeyi planlamış ve bunun için gerekli çalışmaları sürdürmektedir. Norveç, 2011 yılındaki seçimlerinde internet

üzerinden oylama yapmayı planlanmaktadır. Bu seçimlerde başarı elde edilmesi durumunda 2017 yılındaki milletvekili seçimlerinde de internet üzerinden oylamanın uygulanması planlanmaktadır. 2009 yılında KRD (ve geniş anlamda Norveç hükümeti), 2011 yılındaki yerel seçimlerinde uygulanması hedeflenen elektronik seçim pilot projesini bir ihale prosedürüyle başlatmıştır. İ-seçim sisteminin 2017'deki milletvekili seçimlerinde uygulanacağı tarihlerde, ulusal bir açık anahtar altyapısı ve ulusal elektronik kimlik kartının hazır olacağı varsayılmıştır.

Norveç hükümetinin internet üzerinden elektronik oylamayı deneyecek olmasının en belirgin nedeni sayım sürecini hızlandırmak için en uygun yöntem olarak i-seçimi görmesidir. Tüm seçmenler elektronik oylama yoluyla oyunu kullanırsa, sayma işlemi potansiyel olarak sandık kapanışından sonra birkaç dakika içerisinde sonuçlandırılabilir. Başka bir neden de elektronik seçimle beraber, özellikle genç nüfustaki seçimlere katılım oranının hissedilir oranda yükseleceğinin düşünülmesidir. Toplumun farklı kesimlerinden de yenilik nedeniyle ilginin artması nedeniyle seçimlere katılım oranının olumlu yönde etkileneceği de öngörülmektedir. Elektronik seçim engelli vatandaşlarının da oy kullanmalarını sağlayacaktır, örneğin görme engelli vatandaşların diğer insanların yardımı olmadan ekran okuyucular aracılığıyla oy kullanabilmesi sağlanabilir. Diğer bir sebep de elektronik seçim çalışmasının maliyet-etkin şekilde gerçekleştirilebilmesidir. İ-seçimler kuruluş maliyeti nedeniyle kısa vadede daha masraflı görünebilir. Fakat uzun vadede k-seçimlere kıyasla çok daha az zaman ve para gerektirecektir.

Avusturya deneyimi

Diğer ülkelerdeki deneyimler göstermiştir ki, e-seçim projeleri ancak topluma elektronik oy kullanma konusunda açık ve anlaşılır bilgiler verildiği müddetçe başarılı olabilmektedir. Örneğin, Avusturya'da sistemin kriptografik bazı detaylarının topluma açıklanmamasından dolayı sayıları çok az denilebilecek bir



kesim tarafından eleştirilmiş, bu eleştiriler medyada çok sık dile getirilerek halkın güveni azalmıştır. Avusturya hükümeti bunun üzerine sınırlı miktarda kaynak kodu detaylarına bakmak için gönüllü katılımcı uzmanlardan oluşan çok küçük bir grup seçmiştir. Bu davranış tamamen kapalı bir yazılım ile açık kaynak kodlu olması arasında bir uzlaşma olarak kabul edilebilirse de, toplumda oluşan güven eksikliği giderilememiş ve akabinde e-seçim projeleri rafa kaldırılmıştır [24]. Aslında sistemin her detayının açık ve şeffaf olması durumunda dahi sistemin doğruluğunu ve güvenilirliğinin tam anlamıyla kontrol edilmesi ya da halkın büyük bir bölümü tarafından anlaşılması olanaksızdır.

Norveç sistemi

Norveç'in seçim mimarisi genel olarak yazılım ilk bölümünde incelediğimiz Estonya seçim sistemi ile benzerlik taşımaktadır [25]. Estonya'dan farklı olarak Norveç'teki internet tabanlı elektronik seçim sistemi (muhtemelen Avusturya'dan edinilen deyim sayesinde) açık ve şeffaftır. İnternette oylamaya güven duyulmasını sağlamak amacıyla, Norveç hükümeti sistemin kriptografik mimarisinden diğer teknik konulara kadar ilgili bütün belgeler ve detaylar dahil neredeyse bütün önemli belgeleri yayınlamıştır. Bu yolla, toplumda sisteme karşı güven inşa etmeye çalışmıştır. Bunun yanında topluma, sistemin güvenlik açıklarını araştırma olanağı sağlayabilmek için kaynak kodunu da açmaya karar vermişlerdir. Norveç sisteminin mimarisi iki önemli güvenlik tedbirleri üzerine yoğunlaşmıştır

- seçmen bilgisayarlarının tehlide açık olması (kötü amaçlı yazılım (malware), kurban saldırganlar ağı (botnet), palıkkılık (phishing)) ve
- zorlama ve oy satmaya karşı tedbirler.

Norveç sisteminin önemli farklarından bir diğeri, seçmen bilgisayarındaki tehditlerin engellenmesi için internetin dışında farklı ve bağımsız iletişim kanalları kullanılmasının önerilmesidir. Seçim öncesi

ve seçim sonrası diye adlandırılan bu iletişim kanallarına posta servisi ve kısa mesaj servisi (SMS) örnek gösterilebilir. Seçim öncesinde doğrulama kodları posta yoluyla seçmenlerin eline ulaştırılır. Elektronik oyu kullanırken cep telefonuna gelen kısa mesaj ile posta yoluyla gelen kod karşılaştırılır. Bu yolla oyun başarılı bir şekilde merkezi sistem tarafından alındığı ve yol boyunca hiçbir güvenlik tehdidine uğramadığı doğrulanır. Bu kontrol aynı zamanda seçmen bilgisayarında da hiçbir tehdidin olup olmadığını doğrular. Klasik k-seçimlerde bu doğrulama yöntemi yoktur. Örneğin, k-seçimlerde oy kullandığımızda oyumuzun sayılıp sayılmadığını veya oyumuzun geçersiz oyların içerisine düşüp düşmediğini bilemeyiz. İ-seçimde yapılan bu ek güvenlik kontrolleri klasik sistemlerdeki bu tür problemlerin çözümüne yöneliktir.

Sistemin kriptografik protokolü, İspanyol elektronik seçim şirketi Scyt tarafından tasarlanmıştır. Ancak ulusal ve uluslararası uzman danışmanlar tarafından pek çok değişikliğe uğramıştır. Scyt şirketi standart seçim çerçevesi ve iki farklı kanal mekanizması önermiştir. Önerilen standart seçim çerçevesi genel olarak bilinen standart kriptografik protokol ve mekanizmalarından oluşmaktadır.

Norveç seçimlerinde de Estonya'da olduğu gibi, i-seçim yoluyla seçmenler istedikleri kadar oy kullanabilmekte fakat kağıt tabanlı oy kullanılmadığı takdirde en son kullandıkları i-seçim oyu sayılmaktadır.

i-seçim sistemlerinde oy verme aşamasında homomorfik şifreleme yapılmakla birlikte, oy sayımı için genelde aşağıdaki iki yöntemden biri tercih edilir:

- Şifreli oyların hepsi çarpıldıktan sonra, ortaya çıkan şifre bir çeşit eşik sır paylaşımı yoluyla çözülür. Derginin bir önceki sayısında, homomorfik şifrelemede şifreli oyların çarpımının sonucunda ortaya çıkan değer oyların toplamlarının şifrelenmesine eşit olduğunu açıklamıştık.

Dolayısıyla, şifresi çözülen sonuç oy toplamlarıdır. Basit ve küçük seçimler için uygulanabilir fakat yüksek ölçekli seçimlerde verimli olmayabilir.

- Karıştırıcı ağlar kullanılarak oylar anonimleştirilir, sonrasında şifreli oylar (eşik sır paylaşımı yoluyla) tek tek deşifre edilir. Oylar yetkili gözetmenler huzurunda toplanır [1].

Norveç seçimlerindeki oy sayımlarında çok basit ve popüler olan homomorfik sistemler yerine, daha hızlı, güvenlik seviyesi daha yüksek ve verimli olan karıştırıcı ağlar tercih edilmiştir [1].

Evden oy kullanılabildiği için maalesef kriptografik yöntemler, zorlamayla oy kullanımını engelleyemez. Zorlamayı bir ölçüde gidermek için, seçmenlerin birden çok oy kullanmasına izin verilebilir. Seçmen zorlama altında oyunu internet üzerinden oy kullansa dahi klasik kağıt tabanlı yöntemle de oyunu tekrar kullanabilir. Dolayısıyla, zorlama problemi bu yolla bir ölçüde giderilir. Estonya'da olduğu gibi seçmenlerin kağıt tabanlı oy kullanması durumunda kağıttaki oy sayılacak, elektronik oyları dikkate alınmayacaktır.

Zorlamaya karşı alınan önlemler aynı zamanda oy satılmasını da bir ölçüde engellemektedir.

3.1. İ-seçim için Norveç'te değişikliğe uğrayan yasalar

Her ülkenin elektronik seçimi uygulaması yasaların müsaade ettiği çerçevede mümkündür. Bu yüzden de yasaların elektronik seçime uygun hale getirilmesi en önemli konulardan birisidir. Norveç anayasası ve hukuk sisteminde elektronik sistem için düzenlemeler yapılmıştır. Anayasada yer alan elektronik seçimin temel direktifleri aşağıdaki gibidir:

- Oylama sonuçlarını bozmak veya değiştirmek yasadışıdır.
- Seçmeni oy vermeye zorlamaya veya zorla istediği birine oy verdirmek yasadışıdır.

• Oy satmak ve oy satın almak yasasıdır.

• Oy sayımına etki edebilecek her türlü davranışta bulunmak yasaktır.

Norveç elektronik seçim sistemi için yapılan düzenlemeler ve yenilikler aşağıdakileri içermektedir:

- Seçim mevzuatı
- Elektronik imza mevzuatı
- Gizliliğin korunması hakkında mevzuat
- Elektronik yönetim yönetmeliği
- Seçmen kayıtlarının tutulması
- Özgür ve Gizli Seçme Hakkı ve İlkeleri
- Eşit Seçme Hakkı İlkesi
- Evrensel Seçme Hakkı İlkesi
- Seçim Konularındaki Uygulama Kodu
- İnsan Hakları Avrupa Sözleşmesi
- Ceza kanunu (elektronik seçimi kapsar)

3.2. Norveç i-seçim akışı

Özellikle internet üzerinden yapılan oylama sistemlerinin kalbinin kriptografik protokoller olduğunu belirtmiştik. Bu protokollerin güvenliği ve güvenilir olması i-seçime güven duyulması için gereklidir. Seçim sonuçlarının açıklanması uzun sürmemeli, hatta yasalar çerçevesinde belirli bir zaman içerisinde açıklanması sağlanmalıdır.

Güvenilirliği ve gizliliği sağlamak için çift zarf yöntemini kullanan i-seçim sistemi şu adımlardan oluşmaktadır (Şekil 14):

1. Seçimlerden önce seçmenlerin adreslerine seçimde aday olan kişilerin adlarını ve doğrulama kodlarını içeren bir posta ulaşır.

2. Seçmen oy kullanmak için seçim merkezinin web sayfasına bağlanır ve seçmenin bilgisayarına seçim uygulaması yüklenir.

3. Seçmen seçim uygulamasını kullanarak

ulusal kimliği ile oy sunucusuna kimliğini doğrular.

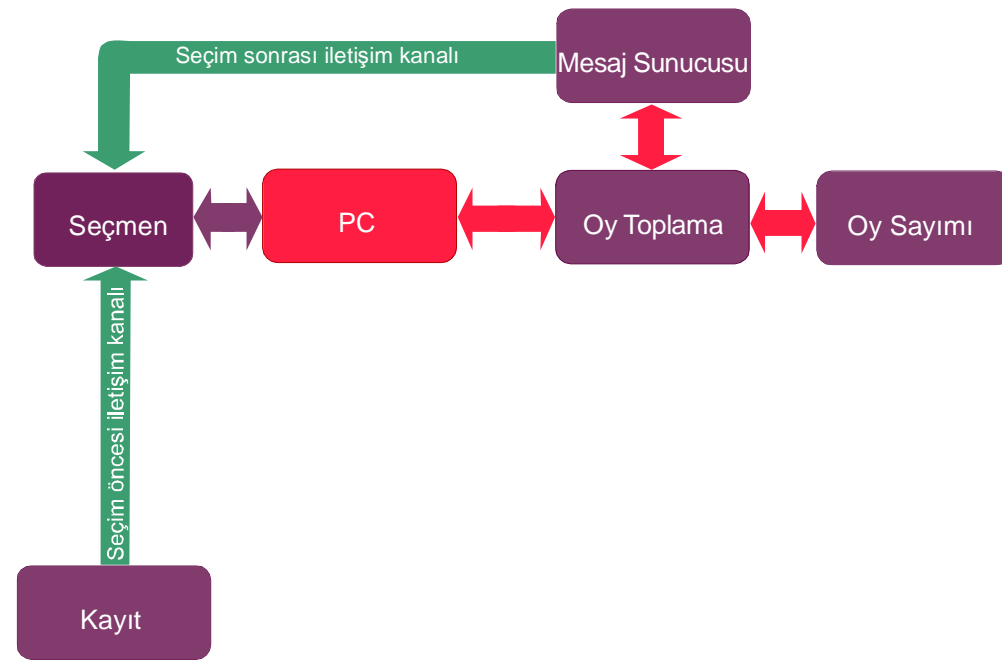
4. Seçim uygulaması güvenli bir kanal üzerinden partileri ve adayların listesini alır. Bu liste, aynı bölgedeki tüm seçmenler için aynıdır ve şifreli değildir.

5. Seçim uygulaması partilerin listelerini rasgele bir şekilde görüntüler.

6. Seçmen oy vermek istediği partiyi seçer ve bir sonraki adıma geçer. Seçmen için boş oy seçeneği de mevcuttur.

7. Bu aşamada, seçilen parti için aday listesi gösterilir ve seçmenlerin istediği adaylara oy vermesi sağlanır. Seçmenlerin oyları şifreli ve imzalıdır (saldırgan tarafından da üretilebilir), sonrasında elektronik oy sandığına gönderilir.

8. Son adımda, seçmene, karar verdiği oyun bir özeti sunulur. Seçmen yaptığı seçimden memnun ise İleri butonuna basar. Bu şekilde oyunun oy sayım sunucusunun açık anahtarı ile şifrelenmesini ve kendi imzalama özel anahtarı ile elektronik olarak imzalanmasını sağlar.

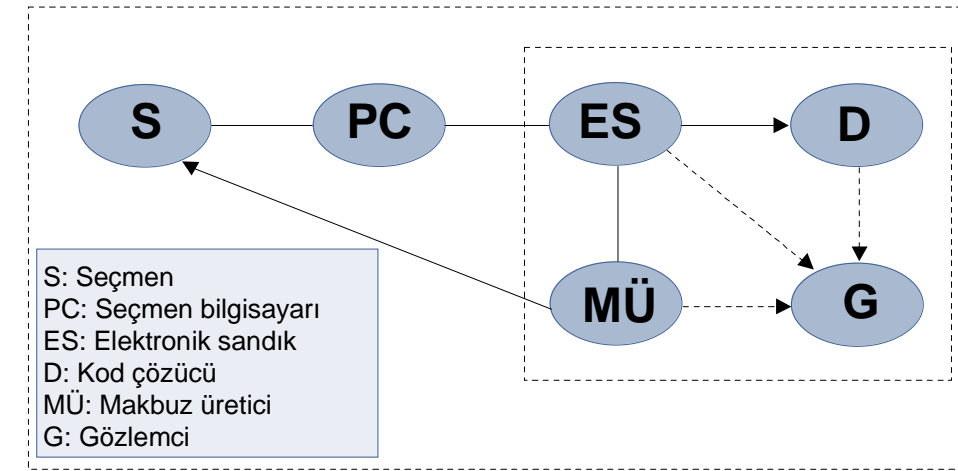


Şekil 14. Çift kanallı Norveç i-seçim sistemi.

9. Oy kullanıldıktan sonra seçmenin cep telefonuna bir doğrulama kodu gönderilir: "Siz, Bora Yılmaz, 27-Şubat-2011 yılında saat 19.45'te bir oy kullandınız. Onay kodunuz [kod]'dur".

10. Seçmen cep telefonuna gelen doğrulama kodunu posta yoluyla evine gelen kodla eşleştirerek kullandığı oyun başarılı bir şekilde kullanılıp kullanılmadığını kontrol edebilir. Seçmen SMS ile gelen bu mesajla posta yoluyla gelen mesajlardan farklı olduğu durumlarda (veya oy sandığı bulunamadı gibi durumlarda veya oy vermediği halde mesaj geldiği durumlarda) itiraz eder. Bu durumda seçmen tekrar oy kullanır, ya da k-seçim yapabilir.

3.3. Norveç i-seçim kriptografik protokolü



Şekil 15. Norveç i-seçim sistemi mimarisi.

Bu bölümde Norveç sisteminin kriptografik protokolünü anlatmaya çalışacağız [35].

3.3.1 Oy kullanma protokolü

Uzaylar ve protokol katılımcıları: Aday listesini $O = \{1, 2, 3, \dots, k_{max}\}$ şeklinde ifade edelim öyle ki k_{max} toplam aday sayısı olsun. (v_1, \dots, v_k) ise bir seçmenin oy verdiği adaylar olsun öyle ki $v_i \in O$ ($k < k_{max}$).

- Kodlama uzayı C,
- Seçmen S,
- Kişisel bilgisayar PC,
- Elektronik sandık ES,
- Makbuz üretici MÜ,
- Kod çözücüsü D,
- Sıfır bilgi protokolünü SBP ile ifade edelim.

G, g eleman tarafından üretilen (asal) q mertebeli bir çarpımsal grup olsun. Seçmene posta yoluyla gönderilen doğrulama kodlarının uzayı C olarak ifade edilsin. Sanki rassal fonksiyon F uzayı G 'den C 'ye gitsin. f bire-bir kodlama fonksiyonu, d kod çözme fonksiyonu olarak tanımlansın.

Anahtar üretimi: Anahtarlar güvenli bir otorite tarafından üretildiği varsayılır (örneğin, Yüksek Seçim Kurulu). Bu anahtarlar eşik sır paylaşımı kriptografik yapı taşı kullanılarak üretilir [20]. Seçimden önce otorite tarafından a_1, a_2 ve a_3 parametreleri seçilir öyle ki $a_1 + a_2 = a_3 \pmod{p}$. a_1, a_2 ve a_3 anahtarları sırasıyla D, ES ve MÜ'ye dağıtılır. Açık anahtarlar ise şu şekilde hesaplanır: $y_1 = g^{a_1}, y_2 = g^{a_2}$ ve $y_3 = g^{a_3}$. Seçmen, oyunu bu açık anahtarları kullanarak şifreler ve ES'ye gönderir. ES ve MÜ özel anahtarları a_2 ve a_3 'ü kullanır ve çıkan sonucu D'ye gönderir. D ise özel anahtarı a_1 'i kullanarak oyları sayar. Burada ES, MÜ ve D fiziksel ve organizasyonel olarak farklı olmak zorundadır, aksi takdirde farklı servisler olarak algılanmazlar. Bunun yanında, ES, MÜ, D ve gözletmenler arasındaki iletişim güvenli bir kanal olması gerekmektedir (örneğin, TLS veya IPSEC protokolleri çalıştırılabilir).

Makbuz üretimi: Makbuzlar seçimden önce şu şekilde oluşur: Her seçmen için $s_i \in_R \{0, \dots, q\}$ ve $d \in_R F$ seçilir öyle ki $f : x \mapsto x^{s_i}$ ve $r : O \mapsto C$. f ve d fonksiyonlarının bileşke fonksiyonu $r(v) = d((f(v))^{s_i})$ olarak hesaplanır. Seçimden önce, $\{(v, r(v)) \mid v \in O\}$ ikilisi seçmene posta yoluyla gönderilir. Bu ikilisi makbuz denir ve seçmenin verdiği oyun seçmen bilgisi dışında hiçbir şekilde değiştirilemeyeceğini garanti eder.

Protokol adımları:

1. Oy kullanımı: Seçmen oylama esnasında $O = \{1, 2, 3, \dots, k_{max}\}$ aday listesinden (v_1, \dots, v_k) seçeneklerine karar verir. PC, seçmenin yaptığı k seçiminden arta kalan adaylar için

$v_{k+1} = v_{k+2} = \dots = v_{k_{max}} = 0$ olarak belirler. Daha sonra PC her aday $t_i \in_R \mathbb{Z}$, $(x_i, w_i) \leftarrow (g^{t_i}, y_1^{t_i} f(v_i)) \forall i = 1, \dots, k_{max}$ homomorfik şifreler. PC yaptıklarının doğruluğunu ispatlamak için sıfır bilgi protokollerini

$\pi \leftarrow \text{SBP}(S, x_1, \dots, x_{k_{max}}, t_1, \dots, t_{k_{max}})$ hesaplar, $\sigma_S \leftarrow \text{İmza}_S(S, (x_i, w_i)_{i=1}^{k_{max}}, \pi)$ imzaladığından sonra ES'ye $(x_i, w_i)_{i=1}^{k_{max}}$ bilgilerini gönderir.

2. Onaylama ve İmzalama: İlk olarak ES π 'yi ve σ_S 'yi doğrular. Daha sonra, ES $\text{sayac}++$, $S, (x_i, w_i)_{i=1}^{k_{max}}, \pi, \sigma_S$ bilgilerini kaydeder.

$ES \leftarrow (x_i, w_i) \leftarrow (x_i^{s_i}, (w_i x_i^{a_2})^{s_i})_{i=1}^{k_{max}}$ şeklinde hesaplar ve MÜ'ye gönderir.

MÜ ise $\forall i = 1, \dots, k_{max}$ için şu hesapları yapar: $r_i \leftarrow w_i x_i^{-a_3}, k \leftarrow i, \check{r}_i \leftarrow d(r_i)$. MÜ daha sonra $\sigma_{MÜ} \leftarrow \text{İmza}_{MÜ}(\text{Özet}(S, (x_i, w_i)_{i=1}^{k_{max}}), \pi, \sigma_S)$ şeklinde imzalar ve bu $\sigma_{MÜ}$ imza değerini PC'ye gönderir. Makbuz üretici tarafından C uzayından $SMS = \check{r}_1, \dots, \check{r}_k$ makbuzu üretilir ve seçmene SMS yoluyla da gönderilir.

3. Doğrulama: S öncelikle $\sigma_{MÜ}$ değerini doğrular. $k \stackrel{?}{=} \check{k}$ eşitliğini kontrol eder, eşit değilse oylama esnasında bir problem olduğu kabul edilir. SMS yoluyla gönderilen $(v_1, \check{r}_1), \dots, (v_k, \check{r}_k)$ makbuz ile posta yoluyla gelen $\{(v, d(f(v))^{s_i})\}$ makbuz karşılaştırılır. Eğer farklı ise S'nin oyu PC'deki kötü amaçlı yazılım tarafından değiştirilmiş veya yol boyunca bozulmuş olabilir.

Seçmen (S + PC)	Sunucu (ES + MÜ)
Açık Anahtar: y_1	ES'nin gizli anahtarı: a_2
Oy kodlama fonksiyonu: f	MÜ'nün gizli anahtarı: a_3
Onay kodları: $\{(v, \tau(v))\}$	ES'nin gizli üssü: s_i
Maksimum sayıda seçenek: k_{max}	MÜ'nün gizli sanki-rassal fonksiyonu: d_i
	Durum: $sayac$

1. Adım: Oy Kullanımı

S (v_1, \dots, v_k) adaylarını seçer PC $v_{k+1} = v_{k+2} \dots = v_{k_{max}} = 0$ olarak belirler PC hesaplar: $\left(\begin{array}{c} t_i \in_R \mathbb{Z}_q \\ (x_i, w_i) \leftarrow (g^{t_i}, y_1^{t_i} f(v_i)) \end{array} \right)_{i=1}^{k_{max}}$	
PC hesaplar: $\pi \leftarrow \text{SBP}(S, x_1, \dots, x_{k_{max}}, t_1, \dots, t_{k_{max}})$ PC imzalar: $\sigma_S \leftarrow \text{İmza}_S(S, (x_i, w_i)_{i=1}^{k_{max}}, \pi)$	
	$S, (x_i, w_i)_{i=1}^{k_{max}}, \pi, \sigma_S$

2. Adım: Onaylama ve İmzalama

	ES π doğrular ES σ_S doğrular ES kaydeder: $sayac^{++}, S, (x_i, w_i)_{i=1}^{k_{max}}, \pi, \sigma_S$ ES hesaplar: $(\tilde{x}_i, \tilde{w}_i) \leftarrow (x_i^{s_i}, (w_i x_i^{a_2})^{s_i})_{i=1}^{k_{max}}$ ES $(\tilde{x}_i, \tilde{w}_i)$ değerini MÜ'ye gönderir. MÜ hesaplar: $\left(\begin{array}{c} r_i \leftarrow \tilde{w}_i \tilde{x}_i^{-a_3} \\ \check{k} \leftarrow i \\ \check{r}_i \leftarrow d(r_i) \end{array} \right)_{i=1}^{k_{max}}$
	MÜ imzalar: $\sigma_{MÜ} \leftarrow \text{İmza}_{MÜ}(\text{Özet}(S, (x_i, w_i)_{i=1}^{k_{max}}), \pi, \sigma_S)$
	$\sigma_{MÜ}$ SMS: $\check{r}_1, \dots, \check{r}_k$

3. Adım: Doğrulama

S $\sigma_{MÜ}$ değerini doğrular S $k \stackrel{?}{=} \check{k}$ eşitliğini doğrular S $(v_1, \check{r}_1), \dots, (v_k, \check{r}_k) \in \{(v, d(f(v))^{s_i})\}$ doğrular

Doğrulama adımında yapılan posta ve SMS ile gelen kodlar arasındaki kontrol kağıt tabanlı sistemlerde bulunmamaktadır, çünkü kağıt tabanlı sistemler doğrulanabilir sistemler değildir. Örneğin, oyumuzu verdiğimizde gerçekten doğru olarak sayıldığını, geçersiz oyların içerisinde olmadığını veya sayımın

içerisinde bulunduğunu bilemeyiz. İnternet tabanlı seçim protokolündeki bu kontrol bu tür problemleri engellemek amacıyla uygulanmaktadır. Bu sayede seçmen oyunun sayılmadığını anladığından farklı bir PC'de oyunu tekrar kullanabilir, benzer problemler sürerse kağıt tabanlı sistemde oyunu kullanabilir.

3.3.2 Oy sayma protokolü

1. Gözetmen listeyi alır: Gözetmen i-seçmen listesi L 'yi şu şekilde oluşturur: en yüksek $sayac$ değerini seçer, $S, (x_i, w_i)_{i=1}^{k_{max}}, \pi, \sigma_S$. $(x, w) \leftarrow \prod_{i=1}^{k_{max}} (x_i, w_i)$. $L \leftarrow L + \text{ekle}(x, w)$ ve bütün i-seçmen listesini L sıralı bir şekilde gönderir.

2. Şifre çözülür ve oylar sayılır: Öncelikle gözetmen listenin doğruluğunu onaylar. $|L| = n$ olsun. D, $\forall i \in \{1, \dots, n\}$ ve

$s_i \in_R \mathbb{Z}_q$ değerleri için $(x'_i, w'_i) \leftarrow (x_{\prod(i)} g^{s_i}, w_{\prod(i)} y_1^{s_i})$ hesaplar. Sonrasında $\mu_i \leftarrow w'_i (x'_i)^{-a_1}$ hesaplar. $\pi_i \leftarrow \text{SBP}$ sıfır bilgi protokolünü kontrol eder ve şifre çözülür. En sonunda da $\forall i = 1, \dots, n$ değerleri için $\pi' \leftarrow \text{SBP}$ Karıştırıcı işlemi yapılarak oylar karıştırılır. D, bu yapılan işlemleri gözetmene ispatlar. Oylar $\phi(\mu_1), \dots, \phi(\mu_n)$ şeklinde ortaya çıkar (öyle ki ϕ kod çözme fonksiyonudur).

Elektronik Sandık (ES)

Maksimum sayıda seçenek: k_{max}

Kod Çözücü(D)

D'nin gizli anahtarı: a_1
Maximum sayıda seçenek: k_{max}
Oy kodlama fonksiyonu: f

1. Adım: Gözetmen listeyi alır

	$ L = n$ Rasgele $\prod \in \{1, \dots, n\}$
	$\left(\begin{array}{c} s_i \in_R \mathbb{Z}_q \\ (x'_i, w'_i) \leftarrow (x_{\prod(i)} g^{s_i}, w_{\prod(i)} y_1^{s_i}) \\ \mu_i \leftarrow w'_i (x'_i)^{-a_1} \\ \pi_i \leftarrow \text{SBP Şifre Çözme} \end{array} \right)_{i=1}^n$
	$\pi' \leftarrow \text{SBP Karıştırıcı}$ Sonuç (kod çözme): $\phi(\mu_1), \dots, \phi(\mu_n)$

2. Adım: Şifre çözülür ve oylar sayılır

$L \leftarrow ()$ En yüksek $sayac$ değeri seç, $S, (x_i, w_i)_{i=1}^{k_{max}}, \pi, \sigma_S$	
$\left(\begin{array}{c} (x, w) \leftarrow \prod_{i=1}^{k_{max}} (x_i, w_i) \\ L \leftarrow L + \text{ekle}(x, w) \end{array} \right)_S$	
	Bütün sıralı i-seçmen listesi L

3.3.3 Protokolün bütünlüğü

Önceki yazımızda da belirttiğimiz gibi bir protokolün bütün olup olmadığının kontrolü dürüst modelde incelenir [20], yani bütün katılımcıların dürüst olduğu durumunda protokoün doğru işlemi yaptığı kontrol edilir. Bu seçim protokolü bütündür çünkü bütün dürüst katılımcılar için şifreli oylar doğru bir şekilde açılı ve üretilen makbuzların seçmene önceden gönderilen makbuzlarla aynı olması beklenir.

Seçmenin doğruladığı makbuz kodu hariç diğer protokol kısımları bütündür. Sadece seçmene gönderilen (v_i, \check{r}_i) makbuz kodunun doğruluğunu göstermeliyiz (öyle ki $\check{r}_i = d(r_i)$):

$$\begin{aligned} r_i &= \tilde{w}_i \tilde{x}_i^{-a_3} \\ &= w_i^{s_i} x_i^{a_2 s_i} x_i^{-a_3 s_i} \\ &= w_i^{s_i} x_i^{(a_2 - a_3) s_i} \\ &= w_i^{s_i} x_i^{-a_1 s_i} \\ &= (w_i x_i^{-a_1})^{s_i} \\ &= (f(v))^{s_i} \end{aligned}$$

Böylece, eşik sır paylaşımı kriptografik yapıtaş özelliğinden dolayı a_1, a_2 ve a_3 özel anahtarları kullanılarak $r_i = (f(v))^{s_i}$ değerinin sağlandığını ve bu sayede makbuz üretimi sürecinde gönderilen doğrulama kodlarının $\{v, r_i(v) | v \in O\}$ doğruluğunu göstermiş olduk.

3.4. Norveç i-seçim protokolü güvenlik analizi

3.4.1 SMS saldırıları ve güvenlik problemleri

SMS saldırısı Norveç sisteminde önemli ve hassas olduğu için ayrı olarak ele alınacaktır. Estonya sisteminde ise mobil kimlik doğrulama için bir prosedür olduğunu da belirtmiştik. Bu yüzden, cep telefonu sistemi ile tüm SMS saldırılarını incelemek çok önemlidir. Mesaj göndermek için kullanıcı etkileşimi gerekli olmadığından bu tür saldırıları engellemek çok kolay görünmemektedir. SMS saldırılarından bazıları aşağıda listelenmiştir:

- SMS servis sağlayıcısına güvenlik duvarının eklenmesi mümkün değildir.

- SMS mesajlarını filtreleyen bir mekanizmanın eklenmesi mümkün değildir

- Bir mesajın orijinal biçiminde hedef telefona ulaşım ulaşılmadığının belirsizdir

- Cep telefonu operatörleri gönderilecek mesajları filtreleyebilme ve kısa mesajları değiştirebilme yeteneğine sahiptir

- SMS servisi güvenilir bir hizmet değildir, mesajlar gecikebilir ya da hatta hiçbir sebep olmadan atılabilir

- Hizmet dışı bırakma (Denial-of-Service) saldırıları yapılabilir

- Telefonların SMS sorunları bulunabilir. Örneğin bazı telefonlara gelen özel formatlı mesajlar gönderildiğinde telefonun SMS servis hizmeti bozulabilir ve servis dışı bırakılabilir. Bu yolla telefona gönderilen hiçbir SMS/MMS mesajı telefona ulaşamaz [26].

- Akıllı telefonlarda güvenlik açıklarından yararlanmanın güncel farklı yolları vardır. Örneğin, SMS Enjeksiyonu cep telefonuna karşı bilinen en ciddi saldırılardan biridir [26].

- Yeni akıllı telefonlar SMS virüslerine karşı daha savunmasızdır. Nokia, iPhone ve Android platformları için çok sayıda

yeni SMS virüsleri rapor edilmiştir. Örneğin, zararlı mesajlar alındığı takdirde Nokia telefon yazılımında bir hata belirir ve bu telefonları tamamen kullanılamaz hale getirir.

- Bilgisayarlara Truva Atı benzeri yüklenebilir ve cep telefonlarına istenmeyen e-posta/mesajlar gönderilebilir.

- Kötü niyetli kişiler cep telefonlarının numaralarını bir veritabanına kaydedebilir ve istenmeyen mesajları yağdırabilir.

4. Estonya ve Norveç i-seçim sistemlerinin karşılaştırılması

Norveç e-seçim sisteminin Estonya sistemine göre daha güvenli olduğu bilinmektedir. Norveç sisteminde, kötü niyetli seçmen bilgisayarlarına karşı önlemler geliştirilmiştir. Gözetim sistemi de Norveç sisteminde daha iyi organize edilmiştir. Norveç sistemi daha güvenli ve sağlam olmasına rağmen bazı güvenlik açıkları da vardır. Karşılaştırma şu şekilde gösterilebilir

1. Seçmen onayı: Estonya sisteminde kime oy verdiğini bilmenin hiçbir yolu yoktur. Ancak Norveç sisteminde seçmen “Oy Depolama Sunucusu”nda kime oy verdiğini bilir. Bu yüzden, seçmen yanlış oy verdiğinde yeniden oy kullanabilir. Estonya sisteminde ise seçmen sadece oyun oy depolama sunucusunda depolanmış olup olmadığını bilir.

2. Savunmasız seçmen bilgisayarına karşı savunma: Estonya sisteminde savunmasız seçmen bilgisayarına karşı seçmen oyunu korunmak için bir mekanizma geliştirilmemiştir. Ancak Norveç sisteminde bulunan iki farklı kanal mekanizması seçmen bilgisayarına yönelik olası saldırıları engellemek için kullanılır. Hatta bilgisayar seçmen oyunu bozmaya kalkışsa dahi seçmen her zaman anlayabilir.

3. Verilen oy işlemleri için karıştırıcı ağlar yöntemi kullanma [1]: Norveç sisteminin daha verimli ve sağlam olması için karıştırıcı ağlar metodu kullanılır.

4. Mobil kimlik doğrulama sistemi: Norveç sisteminde mobil kimlik doğrulama uygulaması yoktur. Ancak, Estonya sisteminde seçmen mobil kimliği ile kayıt olabilir.

5. Matbaa: Seçim öncesi ve sonrası olan iletişimlerde, seçmen seçim öncesinde her bir adayın adresine yazılı bir kod gönderileceğini belirtmiştik. Seçim otoritesi her vatandaşa bu kodu göndermek zorundadır. Bu yüzden baskı hacmi büyük olacaktır. Matbaalarda çalışan (yöneten kişi) bu kodları çalabilir ve kötü niyetle seçmenin mahremiyetini zedeleyebilir. Kötü niyetli kişiler oradan kodu almak için matbaanın bilgisayar altyapısına saldırabilir.

5. E-seçim sistemlerinin açık kaynak kodlu olmasının önemi

Seçmenlerin seçim sistemine olan güvenlerini arttırmanın bir yolu da sistemin tüm detaylarını ve kaynak kodlarını yayınlamaktır. Seçmenlerinin güvenini kazanmak için Norveç de bu yolu tercih etmiş ve sistemin detaylarını ve kaynak kodlarını açıklamıştır [27]. Seçim sisteminin açık kaynak kodlu olmasının getireceği avantaj ve dezavantajların çok iyi incelenmesi gerekmektedir.

Açık kaynak kodlu sistemlere güvenilmesi akla ilk gelen avantajlardan birisidir. Açık kaynak kodlu sistemlerin detaylarını bir çok kişinin incelediği ve daha az açık içereceği düşünülür. Sınırlı sayıda grup veya teknik uzman, sistemin detaylarını ve kodlarını inceleyerek sistemin güvenliği hakkında bilgi sahibi olacaktır. Bu grup veya uzmanların fikirleri seçmenlerin sisteme güven duymaları konusunda çok etkili olacaktır. İster pozitif yönde olsun ister negatif konusunda kabul görmemiş ve uzmanlaşmamış kişilerin sistem hakkındaki görüşleri sadece marjinal grupları etkileyebilir. Böyle kişilerin seçmenler üzerindeki etkisinin çok sınırlı olacağı değerlendirilmektedir.

Sistemin detaylarını içeren dokümanların İngilizce gibi dünyada yaygın olarak kullanılan bir dilde yayımlanmasıyla diğer ülkelerdeki uzmanların sistemi incelemesi ve görüşlerini açıklaması sağlanabilir.

Dikkat edilmesi gereken en önemli nokta seçmenlerin hükümetlere veya kamu kuruluşlarına güvenmek zorunda kalmadan sistemi kabiliyetleri ölçüsünde inceleyebilme olanağının bulunması ve uzman görüşleri doğrultusunda sisteme güvenip güvenemeyeceğine karar verebilmesidir.

Sistemin açık kaynak kodlu olmasının en büyük dezavantajı kötü niyetli kişilerin ve bilgisayar korsanlarının da sistemin detaylarına ve kaynak kodlarına erişebilecek olmasıdır. Bu kişiler de sistemi inceleyerek zayıflığını bulmaya çalışacaklardır. Bu kişilerin yukarıdaki bahsettiğimiz uzmanlardan farkı ise buldukları zayıflıkları açıklamayıp bunları saldırı yapma amacı ile gizleyecek olmalarıdır.

Açık kaynak kodlu olmayan sistemlerde bile istemci (seçmen) tarafında çalışan yazılımlar saldırganlar tarafından kaynak koda dönüştürülebilir. Kaynak kodun derlenmeden önce perdelenmesi bu işi sadece zorlaştıracaktır. E-seçim sürecinin uzun olabileceği düşünüldüğünde (Norveç’te bu süreç üç ay sürmektedir) perdeleme işleminin getireceği yarar tartışılabilir. Dolayısıyla, sistemin açık kaynak kodlu olması daha çok sonucu güvenliğini ilgilendirmektedir. Sistemin açık kaynak kodlu olması sonucunda saldırganlar sonucu tarafındaki detaylara ve kodlara da sahip olacaklardır. Sistemin kaynak kodunun ve diğer bütün detaylarının açıklanması bu noktada dezavantaj olarak görülebilir. Fakat sistemin detaylarının gizlenmesinin seçmenlerin güvenini azaltabileceğinden dolayı daha büyük dezavantaj getireceği kabul görmektedir. Avusturya’daki e-seçim sisteminin kullanılmaması ve bunun sonucunda e-seçim projesinin rafa kaldırılmasının en büyük nedeni sistemin detaylarının gizlenmesinden dolayı sisteme olan güvenin azalmasından kaynaklanmaktadır [19].

Bir sonraki bölümde internet tabanlı sistemler için yapılan tehdit analizlerini incelemeye çalışacağız.

6. İ-seçim tehdit analizi

Tehdit analizinde saldırganın e-seçim sistemine gizlilik, bütünlük, erişim denetimi ve kullanılabilirlik yönlerinden yapabileceği saldırılar incelenecektir [28, 29, 30]. Bu saldırıların yapılabilmesi için saldırganın sahip olması gereken bilgi düzeyi ve kaynak miktarı da dikkate alınmalıdır. Bu tehditlerin önlenmesi için alınabilecek önlemler konusunda fikir verilmeye çalışılacaktır. Farklı uzmanlar i-seçimin başlangıçta %5’lik kısmında uygulanmasını veya öncelikle yurtdışındaki seçmenlerin kullanabilmesini tavsiye etmişlerdir. Bu yolla zorlama gibi engellenmesi zor problemlerin uygulanması zorlaşabilir.

1. Tehdit

Güvenliği etkileyebilecek olay ve durumlardır. Seçim sistemine yapılabilecek bazı saldırılar birçok kişi tarafından yapılabilirken, bazılarını yapmak için bilgi birikimi, kaynak gereksinimi veya seçim sistemindeki cihazlara erişim gerekebilecektir. Kaynak gereksinimi içerden ve dışarıdan olmak üzere iki sınıfa ayrılır. İçeriden olan kaynaklar, seçim sistemindeki cihazlara veya iç ağa belirli seviyede erişimi olan kişi veya gruplardır. Dışarıdan olan kaynaklar ise seçim sistemindeki cihazlara veya iç ağa erişim için özel izni olmayan kişi veya gruplardır. İnternet tabanlı seçim için aşağıdakiler tehdit kaynağı olabilmektedir.

a. Sistem içi tehdit kaynakları

i. *Seçmen:* Seçim sistemine sınırlı erişim imkanları vardır. Her bir seçmen, kayıt olmak, oy vermek ve seçim sonrası doğrulama amaçları için seçim sistemi ile etkileşim içinde olacaktır.

ii. *Seçim Görevlisi:* Seçim sistemine ve verilerine kullanıcı düzeyinde erişim imkanları vardır. Fakat sistem operatörleri gibi yönetsel hakları yoktur.

iii. *Sistem Yöneticisi:* Seçim sisteminde yönetsel düzeyde erişim imkanları vardır ve sistemin düzgün işlemesinden ve hata durumunda müdahale edilmesinden sorumlulardır.

iv. *Diğerleri:*

1. Seçim sisteminin üreticileri, geliştiricileri
2. Sistemin entegrasyonunu yapanlar
3. Destek/Bakım elemanları
4. Doğrulama kodlarının üretildiği yerler(matbaa veya cep telefonu operatörleri)

b. Sistem dışı tehdit kaynakları

i. *Kötü niyetli kişiler:* Seçim sisteminin zayıf yönlerinden yararlanmak isteyen kişilerdir.

ii. *Kötü niyetli gruplar:* Bu saldırılar organize veya terörist bir gruptan oluşabilir. Kötü niyetli kişilerden iş gücü ve teknik kaynak miktarı açısından daha güçlülerdir.

2. Etkisi

Saldırının sisteme, yapılan seçime ve seçmenlere vereceği zarardır.

3. Tespit Etme

Saldırılar tespit edilebilirse önleme imkanı olabilir ve yapacağı tahribat sınırlı tutulabilir.

6.1. Kriptografik yönüyle tehdit analizi

Tablo 2. E-seçimin kriptografik açısından olası tehdit analizi

	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınan Önlem	Önlem Sonrası Tehdit Seviyesi
1	Erişim Denetimi, Kimlik ve Kaynak Doğruluğunun Düzgün Yapılmaması	Kayıtlı olmayan kişilerin oy vermesi Kayıtlı seçmenlerin yerine oy verme Oyların değiştirilmesi Birden fazla oy verme	Yüksek	Parola tabanlı erişim denetimi	Yüksek
				Sayısal İmza	Düşük
				Güçlü kriptografik kimlik doğrulama yöntemleri	Düşük
2	Seçmenlerin kime oy verdiği ortaya çıkması	Oy gizliliğinin ihlali Oyların değiştirilmesi Ara sonuçların öğrenilmesi Zorlama	Yüksek	Ağ katmanında Şifreleme	Yüksek
				Uygulama katmanında Şifreleme (uçtan uca şifreleme)	Düşük
3	Oyların Bütünlüğünün Sağlanması	Oyların değiştirilmesi	Yüksek	Mesaj Doğrulama Kodu Kullanımı	Düşük
				Sayısal İmza	Düşük
4	İmzalı ve Şifreli Oyların Ele Geçmesi	Anahtar uzunluklarına bağlı olarak oy gizliliğinin ihlali Saldırganın seçim sonrasında (örn, yıllar boyu çalışarak) belirli seçmenlerin kime oy verdiği anlaşılması	Orta	Anahtarların yeterince uzun olması veya anahtar uzunluğundan bağımsız olarak güvenlik sağlanması [1] Anahtarların korunması Sistemdeki şifreli verilere eşik sır paylaşımı ile erişilmesi	Düşük
5	Seçim Sisteminin Özel Anahtarının Korunamaması	Oy gizliliğinin ihlali Ara sonuçların öğrenilmesi Zorlama Servis Dışı Bırakma	Yüksek	Basit Erişim Denetimi	Yüksek
				Sır Paylaşımı	Düşük
6	İmzasız ve Şifreli Oyların Ele Geçmesi	Anahtar ortaya çıkmadığı takdirde tehdit oluşturmamaktadır	Düşük	-	-
7	Oyların Anonimliğinin Sağlanamaması	Oy gizliliğinin ihlali Zorlama Ara sonuçların öğrenilmesi	Yüksek	Sadece Şifreleme/ Deşifreleme	Orta
				Karıştırıcı Ağlar	Düşük
				Homomorfik Sayım	Düşük
8	Denetlemenin Güvenilir Olmaması	Oy gizliliğinin ihlali Oyların değiştirilmesi Zorlama Birden fazla oy verme	Yüksek	Standart Kayıt (Log)	Yüksek
				Değiştirilemez Kayıt (immutable log)	Orta
				Standart Makbuz	Yüksek
				Bireysel Doğrulanabilirlik (seçmenin niyeti oya doğru şekilde yansıdı)	Düşük
				Bireysel Doğrulanabilirlik (oylar doğru sayıldı)	Düşük
				Evrensel Doğrulanabilirlik	Düşük

6.2. Bilgisayar ve ağ güvenliği yönleriyle tehdit analizi

Estonya i-seçim sisteminin en temel sorunu seçmenlerin bilgisayarlarına güvenmektir. Seçmen bilgisayarları kötü niyetli saldırganlar tarafından ele geçirilebilir. Estonya bu problem farkında olup Norveç sistemi gibi bu saldırıları engelleyen sistemler üzerinde çalışmaktadır.

Bu bölümde genel bir tehdit analizi yapılacaktır. Ülkemizde e-seçim uygulanması düşünüldüğü takdirde geliştirilen sisteme özgü bir tehdit analizi yapılması gerekmektedir.

6.2.1 Seçmen tarafında güvenlik

Zorlama deyince aklımıza sadece arkamızda bir tabanca ile bir kişi olmak zorunda değildir, hiç belli etmeyen çok ince bir durumda da zorlama yapılabilir. Örneğin, belirli bir grup

düşünün. Bu grubun ülkemizde nükleer tesis için fikirleri belli olsun ve açıkça karşı olduklarını gösterebilirler. Ülkemizde nükleer tesis kurulmasının yasaklanıp yasaklanmaması için bir oylama yapıldığını düşünelim. Bu grup, üyelerine “Salı akşamı oylama yapabilmek için bilgisayarları şu salonda kuracağız, hepimiz gelin ve burada oyunuzu kullanın, sonrasında büyük bir parti vereceğiz.” diyebilir. Bu davet çok iyi huylu görünebilir, ancak grup üyeleri aralarında çok rahatsız edici ve korkunç olabilir, “Ayşe’yi partide görmedik, nasıl oldu da gelmedi?” veya “Bora geleceğini söylemişti, hala gelmedi?” gibi sorularla karşılaşmamak ve grup dışına itilmemek için kendilerini partiye katılmak zorunda hissedebilirler.

Tablo 3. E-seçimin bilgisayar ve ağ güvenliği açısından olası tehdit analizi

	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	Seçmen bilgisayarındaki kötü amaçlı kodların (örneğin, Truva atı) seçmenin oyunu öğrenmesi, silmesi veya yerine oy vermesi	Oy gizliliğinin ihlali Oyların değiştirilmesi Seçmenin haberi dışında oy kullanma Oy verememe Sunucuya saldırı amaçlı kullanım	Yüksek	Seçmen bilgisayarından tehdit gelmeyeceğinin garanti edilmesi farklı ve bağımsız iletişim kanalları kullanılması (örn., posta, SMS) Virüs, Truva atı, Casus yazılımlar, vs. güncel olmalıdır ¹ . Seçmenin bilgisayar başında bulunduğunun kanıtlanması - Kart - Parola, PIN - Parmak izi kullanımı vb.
2	Seçmenin başka siteye yönlendirilmesi	Oy gizliliğinin ihlali Oyların değiştirilmesi Oy verememe	Yüksek	Virüs, Truva atı, Casus yazılımlar, vs. güncel olmalıdır ¹ . Seçmenler yapılabilecek saldırılar konusunda bilgilendirilmelidir.
3	Zorlama	Oyların değiştirilmesi	Yüksek	Seçmenlerin seçim sonuna kadar oylarını değiştirmesine müsaade edilebilir. Seçmen fiziksel olarak oy sandığına ulaşamayacağı bir noktadan i-seçim bitmesine yakın kullandığında cebine mesaj gelir. Mesaj geldiğinde ne zaman oy kullandığı bilinecektir. Sonraki zamanda tekrar oy kullanamayacağına ve fiziksel olarak da oy sandığına gidemeyeceğine göre oy satışı veya zorlama gerçekleştirilebilir.
4	Aileler evinden oy kullanırken baskı altında kalabilirler (Bu probleme literatürde Aile Oylaması denilir).	Seçmenlerin kendi inisiyatifleri doğrultusunda oy kullanamaması	Yüksek	Aile oylamasını uzaktan seçim uygulandığı müddetçe engellemek mümkün değildir.
5	Oy Satma	Seçim sonucunun değiştirilmesi	Yüksek	Seçmenlerin seçim sonuna kadar oylarını değiştirmesine müsaade edilebilir.

¹ Bu sorumluluk seçmene ait olacaktır. Devletin görevi seçmenleri olası tehditlere karşı uyararak ve alınabilecek önlemler konusunda bilgilendirmek olacaktır.

	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
6	Seçmen doğru olduğu halde bazı işlemlerin yanlış gerçekleştiğini iddia edebilir (SMS kontrolü)	Seçime olan güvenin azalması	-Düşük (kişisel olursa) -Orta (büyük grup olursa)	Yasal olarak bunu iddia eden kişilerin k-seçime yönlendirilmesi <i>kod gönderildiğini iddia ederse, onun yanlış veya yalan söylediğini doğrulayan anlık bir kasıtlı olarak uygularsa bu durum vatandaşlar arasında güvensizlik oluşturabilecektir. Bu teknik bir saldırı değildir fakat vatandaşlar arasında yanlış kanı doğurabileceğinden önemlidir.</i>

6.2.2 Sunucu güvenliği

Sistemde Oy Sayım Sunucusu, Oy Yönlendirme Sunucusu, Oy Depolama Sunucusu vb bulunmaktadır. Bu sunucuların güvenliği genel anlamda bu başlık altında incelenecektir.

Tablo 4. E-seçimin sunucu güvenliği açısından olası tehdit analizi

	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	Kullanılmış oy pusulalarının bazı kısımlarına yetkili personel tarafından erişilmesi (okuma, silme veya değiştirme).	-Oy gizliliğinin ihlali -Oyların değiştirilmesi -Seçimin sonucunun değiştirilmesi	Yüksek	Bknz. Resim-18, Bölüm 6.1 E-seçimin kriptografik yönüyle olası tehdit analizi (Örneğin, Kimlik Doğrulama, Oyların Bütünlüğünün Sağlanması Deşifrelemede Oyların Anonimleştirilmesi)
2	Kullanılmış oy pusulalarının bazı kısımlarına yetkisiz personel tarafından erişilmesi (okuma, silme veya değiştirme).	-Oy gizliliğinin ihlali -Oyların değiştirilmesi -Seçimin sonucunun değiştirilmesi	Düşük	Erişim denetiminde ve kimlik doğrulamada güçlü kriptografik yapılar kullanılması (Bknz. Tablo-18, Bölüm 6.1 Kriptografik Yönden Tehdit Analizi)
3	Yetkisiz personelin sunuculara uzaktan erişerek kullanılmış oy pusulalarını okuması, silmesi veya değiştirmesi.	-Oy gizliliğinin ihlali -Oyların değiştirilmesi -Seçimin sonucunun değiştirilmesi	Düşük	Sunuculara uzaktan erişimin zorunlu olduğu durumlarda güçlü erişim denetim ve kimlik doğrulama mekanizmalarının kullanılması
4	Sunuculardaki kötü amaçlı kodların (örneğin, Truva atı, Casus Yazılım) seçmenin oyunu öğrenmesi, silmesi veya değiştirmesi	-Oy gizliliğinin ihlali -Oyların değiştirilmesi -Seçimin sonucunun değiştirilmesi	Orta	Virüs, Truva Atı, casus yazılımlar, vs. programları güvenilir ve güncel olmalıdır.
5	Sunucu yazılımındaki hatalar nedeniyle seçmen oylarının yanlış kaydedilmesi	Seçim sonucunun seçmenlerin niyetini yansıtmaması	Düşük/Orta	-Yazılımın geliştirilmesinde endüstri standartlarına uyum, -Sistemin ve yazılımı sertifikasyonun yapılması, -Kaynak kodların açıklanması
6	Seçmenlerin yanlış bir sunucuya yönlendirilmesi (Örneğin, Phishing yoluyla)	-Oy gizliliğinin ihlali -Oyların değiştirilmesi -Oy verememe	Yüksek	-Seçmenlerin saldırı yöntemleri konusunda bilgilendirilmesi -Kriptografik yöntemlerle sunucunun taklit edilmesinin önüne geçilmesi.
7	DNS sistemine yapılan bir saldırı sonucunda seçmenlerin yanlış sunucuya yönlendirilmesi	-Oy gizliliğinin ihlali -Seçmenlerin oy kullanamaması -Oyların değiştirilmesi	Düşük	-DNS güvenlik önlemleri alınmalıdır. -Kriptografik yöntemlerle sunucunun taklit edilmesinin önüne geçilmesi. -Siber saldırılar için acil müdahale ekibinin bulundurulması
8	Sunuculara yönelik servis dışı bırakma saldırısında bulunulması	-İ-seçimde oy kullanmanın engellenmesi -İ-seçimin sabote edilmesi	Orta	-Birden Fazla Seçim Kanalı -Kiosk (DRE) kullanımı -Siber saldırılar için acil müdahale ekibinin bulundurulması
9	Sunucuların normal seçim trafiğini kaldıracak altyapıda olmaması	Seçmenlerin i-oy kullanamaması	Düşük	-Planlamanın iyi yapılması -Sistemin sertifikasyonunun yapılması

	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
10	Doğal afetler veya acil durumlar	Seçmenlerin i-seçimde oy kullanamaması	Düşük	Seçimin tekrarlanması veya Seçmenlerin k-seçime yönlendirilmesi
11	Başarısızlıklar veya istemci uygulamasının kalitesi sorunları	Seçmenlerin oy kullanamaması	Orta	Tekrar oy kullanabilme imkanı verilmesi
12	Oy Yönlendirme Sunucusuna servis dışı bırakma saldırısı da düzenlenebilir.	Seçmenlerin oy kullanamaması	Orta	-Sunucuların yedeklemesi -Siber saldırılar için acil müdahale ekibinin bulundurulması
13	Açık Anahtar Altyapısı ile Oy Depolama Sunucusu arasında da bir saldırı gerçekleştirilebilir.	Seçmenlerin oy kullanamaması	Orta	-Sunucuların yedeklemesi -Siber saldırılar için acil müdahale ekibinin bulundurulması
14	Oy Yönlendirme Sunucusu ve Oy Sayım Sunucusu aynı anda saldırı altında olması	Oy gizliliğinin ihlali	Orta	Her ne durumda olursa olsun Oy Yönlendirme Sunucusu ve Oy Sayım Sunucusu birlikte işbirliği yapamayacağına prosedürel yöntemlerle garanti altına alınması gerekmektedir. Bu sunucular bağımsız merkezlerin sorumluluğunun altında olması gerekmektedir.
15	Oy Sayım Sunucusuna içeriden gelen saldırılar (dışarıya bağlantısı olmadığından dışarıdan saldırı beklenmemektedir)	-Oyların değiştirilmesi -Seçimin sonucunun değiştirilmesi	Düşük	-Oy Sayım Sunucusu diğer sunuculara nispeten en güvenli sistemdir, çünkü hatta bağlı değildir. Bu yüzden sadece içeriden tehdit gelebilir. Bunların engellenmesi için de Eşik Sır Paylaşımı kriptografik yöntemleri kullanılabilir. -Ayrıca bu işlemler gözetmenler tarafından yapılmalıdır. -Bireysel ve evrensel doğrulanabilir yöntemleriyle ve sunucuda kötü niyetli kod olmadığı anlaşılabilir.

6.2.3 İletişim kanallarının güvenliği

Tablo 5. E-seçimin iletişim kanalları güvenliği açısından olası tehdit analizi

	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	İnternet ortamının güvensizliği nedeniyle seçmen bilgisayar ve sunucu arasındaki iletişimin içeriğinin öğrenilmesi, değiştirilmesi, engellenmesi	-Oy kullanamaması -Oy gizliliğinin ihlali -Oyların değiştirilmesi -Seçimin sonucunun değiştirilmesi	Yüksek	Bknz. Bölüm 6.1 Kriptografik yönüyle tehdit analizi Bknz. 6.2 Bilgisayar ve ağ güvenliği yönleriyle tehdit analizi
2	Posta sisteminin zafiyetlerinden dolayı postanın seçmenin eline geçmemesi (postanın dağıtılmaması, başkası tarafından kasıtlı olarak alınması) veya seçmenden habersiz içeriğinin öğrenilmesi	Seçmen güvenli ve güvenilir bir şekilde oy verdiğini doğrulayamaz	Düşük	Bu sayının çok olması durumunda seçmenler arasında huzursuzluk doğurabilir. Bunun yanında sistemin doğru çalışıp çalışmadığının anlaşılması için bütün seçmenlerin bu doğrulamayı yapmasına gerek yoktur. Belirli oranda seçmenin bu doğrulamayı yapması yeterlidir.
3	Kötü niyetli kişiler cep telefonu altyapısına veya bireysel cep telefonuna saldırı yaparak servis vermesini/almasını engelleyebilir. (Servis dışı bırakma, SMS virüsleri, SMS enjeksiyon gibi farklı saldırı türleri olabilmektedir.)	Seçmen güvenli ve güvenilir bir şekilde oy verdiğini doğrulayamaz	Orta	Bu tür saldırılar seçmenin farkına varabileceği türlerdendir. Seçmen herhangi bir saldırı altında kaldığını hissederse tereddüt etmeden k-seçimde oyunu kullanabilir.

7. Sonuç ve ülkemiz için ön değerlendirmeler

Bu yazıda 2005 yılından itibaren internet kanalıyla elektronik seçim uygulayan ülke Estonya ile 2011 sonlarına doğru uygulayacak olan Norveç sistemlerini inceledik. Norveç sistemi daha güvenli ve şeffaftır.

Elektronik seçim sistemi hakkında topluma genel bilgiler sağlamak ve üçüncü güvenli bir otoritenin bu sistemi resmi olarak nitelikli hale getirmesi toplumda güven duyulmasını artıracaktır. E-seçim projesinin bütün detaylarıyla açık kaynak kodlu olması çok önemlidir. 2009 yılında Avusturya’da yapılan seçimlerde detayların gizlenmesi dolayısı ile endişelerin dile getirilmesi ve sonuçta projenin rafa kaldırılması bundan sonra neler yapılması gerektiği konusunda örnek olabilir.

Ülkemizde de, özellikle TÜBİTAK’ın geliştirdiği e-kimlik kartının yaygınlaştırılmasının konuşulduğu şu günlerde e-seçimin gerekliliği tartışılmaya ve çeşitli e-seçim teknikleri araştırılmaya başlanmıştır. Ne var ki, e-seçim uygulamasına geçmeden önce detaylı bir fayda-maliyet analizi yapılmalı, öngörü ve kestirimler yapabilmek için bazı temel sorular hakkında bilgi toplanmalıdır.

- Mevcut sistemin olası sorunları ve riskleri
- Kullanılacak yeni teknolojinin faydaları
- E-seçim teknolojisinden beklenen hedefler
- Kullanılacak e-seçim sisteminin belirlenmesi: i-seçim, m-seçim, “PunchScan”, “Scantegrity”, “Three Ballot” veya “Prêt à Voter” sistemleri gibi veya ülkemize özgü geliştirilen sistemler, gerekirse farklı seçimler için farklı sistemler kullanılabilir.
- Yeni teknoloji kullanımı ile beraber olası yeni problemler ve yeni riskler
- Kullanılacak yeni teknoloji seçim sürecinin demokrasi bilinci ve kurumların şeffaflığına etkileri
- Yeni teknoloji ile ilgili donanım, yazılım ve altyapı için gerekli iletişim, ulaşım, personel, danışmanlar, bakım ve güncellemeler ilgili tüm masraf kestirimleri
- Yeni teknolojinin uygulanması için detaylı bir zaman çizelgesi
- Kullanılacak sisteme bağlı olarak gerekli hukuki altyapımın hazır olması adına gerekli düzenlemeler
- Uygulanan yeni teknoloji başarısız olursa ilgili maliyet tahmini
- Sistemi işletenlerin ve seçmenlerin sistem çalışması hakkında eğitim ve bilgilendirilmesi için gerekli planlamanın yapılması

Yukarıda saydığımız genel hususların yanı sıra, e-seçim sistemi tasarlarken e-güvenlik açısından yapılacak çalışmaların aşağıdaki ilkeler çerçevesinde olması beklenir:

- Sistemin kesin gerekli güvenlik özellikleri belirlenmelidir [2].
- Biçimsel analiz (formel analiz) ve sistemin güvenilirliğinin ispatı uzman ulusal ve uluslararası yetkililer (veya danışmanlar) tarafından yapılmalıdır.
- Tehditler ortaya çıkartılmalı ve sınıflandırılmadır. Bunun yanında güvenli modeller tasarlanmalıdır.
- Tehdit önleme stratejileri geliştirilmelidir.
- Muhtemel hata işleme, yönetme ve kurtarma senaryoları çıkarılmalıdır.
- Sosyo-teknik sistem analizi geliştirilmelidir.
- Küçük ölçekli prototip seçimlerle ara tasarımlar denenmeli, geri beslemeler ışığında olası güvenlik açıkları kapatılarak ve kullanıcı kolaylığını artırıcı yöntemlerle sistem geliştirilmelidir.

Elektronik seçimin birçok avantajının olmasına rağmen hala problemlerinin olduğu görülmektedir. Ancak zaman içerisinde edinilen bilgi birikimi ve tecrübe ile beraber bu problemler azaltılabilmektedir. Estonya’da 2005, 2007 ve 2009 yılında başarılı uygulaması Norveç hükümeti için bir ilham kaynağı olmuş bu başarıyı kendi ülkelerinde de uygulamak istemişlerdir.

İngiltere, Amerika, Belçika, Estonya ve Norveç gibi e-seçim uygulayan ya da uygulamayı planlayan ülkeler incelendiğinde elektronik seçim sistemini hyata geçirmeden önce geniş yelpazeli konsorsiyumlar oluşturulduğu gözlenmektedir. Bu konsorsiyumlarda sistemin teknik yönlerinin incelenmesinden sosyo-ekonomik gelişmişliğe, hukuki değişikliklerden kültürel değerlere kadar geniş yelpazede birçok araştırma yapılmaktadır. Ülkemizde de e-seçimin uygulanabilirliği için bir konsorsiyum oluşturulmalı ve bu tür araştırmalarla bir yol haritası çıkarılmalıdır [31, 32, 33, 34].

Bu yazımızda i-seçim üzerine yoğunlaştık. Yazı dizimizin gelecek sayısında makine tabanlı seçim sistemlerini anlatacak, bu sistemleri gerçekleyen ülkeleri ve analizlerini aktaracağız.

KAYNAKÇA ²

- [1] F. Birinci ve M.S. Kiraz, Elektronik Seçim: İleri Düzey Kriptografinin Yapı Tasarımları ve Uygulamaları, BİLGEM Dergisi, Cilt: 3, Sayı: 5, S: 84-101, Ocak-Nisan 2011, http://www.uekae.tubitak.gov.tr/uekae_content_files/flash/UEKAE_dergi_sayfa_flash/sayi_5/BILGEM_Dergisi_Sayi_5.pdf
- [2] M.S. Kiraz, F. Birinci ve U. Uludağ: Elektronik Seçim: Yöntemler, Uygulamalar, Kriptoloji Altyapısı ve Ülkemizdeki Geleceği, UEKAE Dergisi, Cilt: 2, Sayı: 4, S: 76-87, Ocak-Nisan 2011, http://www.uekae.tubitak.gov.tr/uekae_content_files/flash/UEKAE_dergi_sayfa_flash/sayi_4/UEKAE_Dergisi_Sayi_4.pdf
- [3] U. K. Boyacı, Günümüzde Kriptoloji, UEKAE Dergisi, Cilt: 1, Sayı: 1, S: 34-43, Eylül-Aralık 2009, http://www.uekae.tubitak.gov.tr/uekae_content_files/flash/UEKAE_dergi_sayfa_flash/sayi_3/UEKAE_Dergisi_Sayi_3.zip
- [4] <http://www.punchscan.org/>
- [5] <http://scantegrity.org/>
- [6] <http://www.pretavoter.com/>
- [7] <http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf>
- [8] Uniformed and Overseas Citizens Absentee Voting, Act, <http://www.fvap.gov/reference/laws/uocava.html>
- [9] Federal Voting Assistance Program (FVAP) Views on Solutions & Challenges, http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/CAREY_FVAP_Presentation_to_NIST-EAC-FVAP.pdf
- [10] http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf
- [11] Tarvi Martens, Internet Voting in Estonia, NationalElectoralCommittee, http://porvoo9.gov.si/pdf/THU_11c_1415_Country_update_Estonia_EVoting_Porvoo9.pdf
- [12] Internet voting in Estonia, <http://www.epractice.eu/en/cases/ivote>
- [13] Internet Voting Statistics in Estonia, <http://www.vvk.ee/index.php?id=11178>
- [14] Estonia Becomes E-stonia, <http://www.govtech.com/e-government/Estonia-Becomes-E-stonia.html>
- [15] New record in e-voting 2011, <http://www.ega.ee/node/835>

² Burada kısayolu verilen web sitelerine yazının hazırlık çalışmaları sırasında en son 05.03.2011 tarihinde erişilmiştir.

- [16] <http://estonia.eu/about-estonia/economy-a-it/e-voting.html>
- [17] The 7 Worst Tech Predictions of All Time – PCWorld, http://www.pcworld.com/article/155984/the_7_worst_tech_predictions_of_all_time.html
- [18] 12 Worst Tech Predictions Of All Time, <http://www.informationweek.com/news/galleries/global-cio/interviews/showArticle.jhtml?articleID=229218884>
- [19] Overview of Technical Developments, <http://www.coe.int/t/dgap/democracy/Source/EVoting/EVotingReview06/PPT%20LEITOLD%20Austria.pdf>
- [20] Epp Maaten, Elections Department, Chancellery of the Riigikogu (Parliament), Lossi pl. 1A 15181 Tallinn, ESTONIA, <http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-9.pdf>
- [21] E-Vote 2011- Pilot Project, Norway, <http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658>
- [22] Estonia E-Voting System, <http://www.vvk.ee/public/dok/Yldkirjeldus-eng.pdf>
- [23] Electronic voting– challenges and opportunities www.umic.pt/images/stories/publicacoes1/evalg_rapport_engel.sk.pdf
- [24] E-voting for the 2009 elections of representatives of the Association of Austrian students of post-secondary level education http://www.oeh-wahl.gv.at/Content.Node/33092_3.php
- [25] Arne Ansper, Sven Heiberg, Helger Lipmaa, Tom Andre Overland, and Filip van Laenen, Security and Trust for the Norwegian E-voting Pilot Project E-valg 2011, http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/Tilbud_computas/SSA-U_Appendix_2A_Attachment_1_Security_and_Trust_for_the_Norwegian_E-voting_Pilot_Project.pdf, 2009
- [26] Collin Mulliner and Charlie Miller, Injecting SMS messages into smart phones for security analysis, WOOT’09 Proceedings of the 3rd USENIX conference on Offensive Technologies, USENIX Association, Berkeley, USA, 2009
- [27] www.lastenparlamentti.fi/slp_kunnissa/opetusmaterialit/videot/videot/files/eh-overiview-2008-10.ppt
- [28] A Threat Analysis on UOCAVA Voting Systems, <http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf>

[29] Workshop on UOCAVA Voting Systems,
<http://www.nist.gov/itl/csd/ct/uocava-2010-workshop-agenda.cfm>

[30] D., Rubin Jefferson, B. A., Simons, D. Wagner, (2004)
A security analysis of the Secure Electronic Registration and
Voting Experiment (SERVE), January 2004, Available at
www.servesecurityreport.org

[31] BeVoting- Study of Electronic Voting Systems
http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections2011/1/fr/presentation/bevoting-2_gb.pdf

[32] Electronic voting – challenges and opportunities
http://www.umic.pt/images/stories/publicacoes1/evalg_rapport_engelsk.pdf

[33] Electronic Voting- A challenge to democracy?
<http://www.openrightsgroup.org/uploads/org-evoting-briefing-pack-final.pdf>

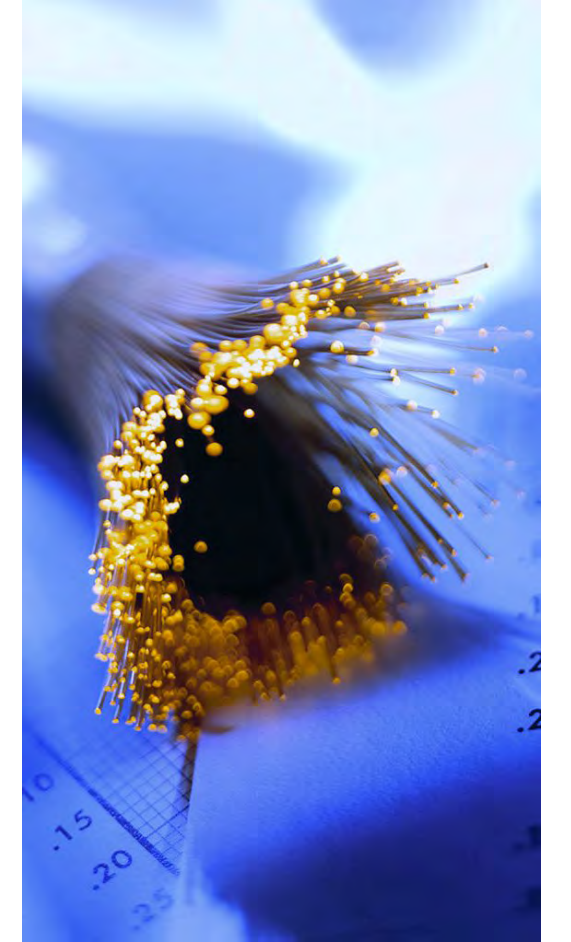
[34] Electronic Voting and Electronic Counting of Votes- A
Status Report http://www.eca.gov.au/reports/electronic_voting.pdf

[35] Kristian Gjøsteen, Analysis of an internet voting protocol,
Cryptology ePrint archive, <http://eprint.iacr.org/2010/380>, 2010.



IPKC-G

- » Yerel alan ağına bağlı ya da bağımsız çalışan IP tabanlı cihazların güvensiz ağlar üzerinden güvenli haberleşmesinin sağlanması
- » Şebeke yapısında aynı anda bir noktadan bir çok noktaya gigabit hızında veri iletimi
- » IPv4, IPv6, IPsec, TCP, UDP, ICMP protokolleri
- » "Gizli" güvenlik düzeyinde kullanım
- » Veri gizliliği, trafik akış gizliliği, kimlik doğrulama, veri bütünlüğü
- » Güvenlik Yönetim Merkezi aracılığıyla uzaktan yönetim
- » Renkli TFT LCD ekran ve tuştakımı aracılığıyla kullanıcı dostu, ikon bazlı menüler ile kolay kurulum ve işletim, lokal cihaz yönetimi
- » EKADAS Anahtar Üretim & Dağıtım Sistemi / anahtar yükleme cihazları üzerinden çevrimiçi, çevrimdışı anahtar yükleme
- » Otomatik anahtar üretimi & değişimi, IKE
- » 155Mb/s band genişliğinde veri şifreleme, çözme
- » QoS ile servis önceliklendirmesi
- » Elektriksel, fiberoptik arabirimler
- » Sertifika tabanlı çalışma
- » Akıllı-kart / parola ile iki aşamalı cihaz erişim denetimi
- » Muhasebe, işlem, olay, alarm, trafik günlükleri
- » MIL-STD-461E EMI/EMC, SDIP- 27, MST-401-1 (Level A) TEMPEST standartlarına uygunluk
- » Ticari ve endüstriyel sıcaklık çalışma aralığı



**Gigabit hızındaki ağlarda da,
Bilgileriniz güvence altında.**

www.bilgem.tubitak.gov.tr

126

131

142

makale

126 Sayısal Telsiz Sistemleri İçin Ağ Geçidi Uygulaması

Murat ÇEVEN, Hamza ÖZER

Ağ geçitleri, farklı sistemlerin birbiriyle haberleşebilmesini sağlayan arayüz ve çevirici yapılarıdır. Bu çalışmada, iki farklı sayısal telsiz sisteminin birlikte çalışmasına olanak sağlayacak, yazılım tabanlı bir ağ geçidi uygulaması önerilmiş; Amerika ve Avrupa'da, başta kamu güvenliği ve acil durum haberleşmesinde kullanılmak üzere farklı kurumların kullandığı Kamu Güvenliği Telsiz Operatörleri Birliği ('Association of Public-Safety Communications Officials', APCO) Proje 25 (P25, 'Project 25') ve Karasal Trunk Telsiz ('Terrestrial Trunk Radio', TETRA) telsiz sistemlerinin birlikte kullanılabilmesine imkân verecek yeni bir uygulama tanımlanmıştır. Makalede öncelikle bu iki sistemin ana yapıları tanıtılmış ve sonrasında, önerilen uygulamanın nasıl gerçekleştirileceği ve arkasındaki yapı, blok şema üzerinden açıklanmıştır. Zaman ve iletişimin kritik olduğu olağanüstü durum ve kriz ortamlarında farklı iki standardın haberleşmesi kamu güvenliği için büyük önem arz etmekte olup, bu ihtiyacı karşılayabilecek ağ geçidi uygulamasının önemli oranda fayda sağlayacağı öngörülmektedir.

131 Olasılık Kuramına Bir Giriş – I: Temel Kavramlar

C. Nezir GEÇKİNLİ

Günlük yaşamda sıkça kullandığımız olasılık kavramı kolay anlaşılır modeller yardımıyla açıklanmakta, olasılık kuramının temel özellikleri örneklerle tanıtılmaktadır.

142 Anten Ölçüm Sistemleri ve Hata Analizleri – I: Düzlemsel Yakın Alan Ölçüm Sistemi

Bahattin TÜRETKEN, Umut BULUŞ, Ömer YILMAZ

Anten ölçümleri, kapalı veya açık ölçüm alanlarında (iç veya dış ortamlarda, tam yansız odalarda veya açık saha test alanlarında) yapılır. Uzak alan ve yakın alan ölçüm sistemleri ile antenin ışıma diyagramı elde edilir. Bu çalışmada, ölçülmek istenen anten parametreleri ile uzak ve yakın alan ölçüm sistemleri hakkında bilgi verilecek, düzlemsel yakın alan ölçüm sistemi ile hata çözümlenmeleri (analizleri), ölçümlerle desteklenerek sunulacaktır.

Sayısal Telsiz Sistemleri İçin Ağ Geçidi Uygulaması

Murat ÇEVEN, Hamza ÖZER

Özet - Ağ geçitleri, farklı sistemlerin birbiriyle haberleşebilmesini sağlayan arayüz ve çevirici yapılarıdır. Bu çalışmada, iki farklı sayısal telsiz sisteminin birlikte çalışmasına olanak sağlayacak, yazılım tabanlı bir ağ geçidi uygulaması önerilmiştir; Amerika ve Avrupa'da, başta kamu güvenliği ve acil durum haberleşmesinde kullanılmak üzere farklı kurumların kullandığı Kamu Güvenliği Telsiz Operatörleri Birliği ('Association of Public-Safety Communications Officials', APCO) Proje 25 (P25, 'Project 25') ve Karasal Trank Telsiz ('Terrestrial Trunk Radio', TETRA) telsiz sistemlerinin birlikte kullanılabilmesine imkân verecek yeni bir uygulama tanımlanmıştır. Makalede öncelikle bu iki sistemin ana yapıları tanımlanmış ve sonrasında, önerilen uygulamanın nasıl gerçekleştirileceği ve arkasındaki yapı, blok şema üzerinden açıklanmıştır. Zaman ve iletişimin kritik olduğu olağanüstü durum ve kriz ortamlarında farklı iki standardın haberleşmesi kamu güvenliği için büyük önem arz etmekte olup, bu ihtiyacı karşılayabilecek ağ geçidi uygulamasının önemli oranda fayda sağlayacağı öngörülmektedir.

Anahtar Sözcükler - Ağ geçidi (gateway), sayısal telsiz (digital radio), elektromanyetik.

1 GİRİŞ

Telsiz haberleşmesi, başta itfaiye, güvenlik, belediye, acil yardım ve lojistik hizmetleri gibi kamu kurumları olmak üzere, sosyal ve ticari hayatta yoğun bir şekilde kullanılmaktadır. Bu sistemler idari ve ticari kuruluşların oluşturduğu haberleşme trafiğini karşılamamın yanı sıra şehir merkezlerinde, köylerde veya kırsalda kamu güvenliği kurumlarının (jandarma, polis, zabıta vb.) sorumluluk alanına giren bütün bölgeleri tam olarak kaplamaktadır. Telsiz sistemleri afet, yangın, terör olayları ve benzeri kriz durumlarından en az etkilenecek çalışmasını sürdürüp haberleşme gereksinimini karşılayacak nitelik ve ölçüdedir. Telsiz haberleşme sistemlerinin 17 Ağustos 1999 Marmara depremi, 11 Eylül 2001 NewYork Dünya Ticaret Merkezi'ne yapılan terör saldırısı, 26 Aralık 2004 Güney Asya tsunami felaketi ve bunların öncesinde veya sonrasında yaşanan olağanüstü durumlarda, Gezgin İletişimde Küresel Sistem ('Global System for Mobile Communications', GSM) ve "sabit hat" olarak bilinen Genel Aktarmalı Telefon Şebekesi ('Public Switched Telephone Network', PSTN) gibi diğer haberleşme sistemlerine göre birçok açıdan üstünlüğü görülmüştür. Bu nedenle telsiz haberleşme sistemlerine olan talep sürekli olarak artmıştır. Şüphesiz ki bu artışta telsiz haberleşmesinin gezgin olmasının payı büyüktür. Bu artışa paralel olarak da telsiz haberleşmesince kullanılan frekans spektrumunun

doluluk oranı artmakta ve sınırlı olan frekans kaynaklarını daha verimli kullanmayı sağlayacak çözümler beklenmektedir.

Sayısal Telsiz Sistemleri, telsiz haberleşmesi için kısıtlı kaynak olan frekans spektrumunun etkin kullanımı ve veri iletişimi gereksinimlerine yanıt verebilmek amacıyla, sayısal donanım teknolojileri kullanılarak gerçekleştirilmiş sistemlerdir [1]. Sayısal teknolojilerin kullanımıyla birlikte, vericiden gönderilmeden önce veya alıcıdan alındıktan sonra dijital forma dönüştürülen bilgi üzerinde sayısal yöntemler uygulanabilmektedir. Örneğin verimli bir ses sıkıştırma yöntemiyle, iletilen sesin spektrum kullanım oranı düşürülerek spektrum verimliliği artırılabilir. Spektrum verimliliğine ek olarak, iletilen ses belirli bir anahtar ile şifrelenerek, yetkisiz kişilerin (haberleşme trafiğini izlese bile) içeriğini çözmesi engellenebilir. Sayısal sistemlerin analog sistemlerden üstün bir diğer yönü de, sayısal sistemlerde işaretin üzerindeki gürültünün, belirli bir değeri aşmadığı sürece, sinyal üzerinde bozucu etkisinin olmamasıdır. Ayrıca, sayısal teknolojiler sayesinde, ses haberleşmesinin yanında, modeme gerek duyulmadan veri haberleşmesi de gerçekleştirilebilmektedir.

Hâlihazırda dünya üzerinde en çok kullanılan sayısal telsiz sistemlerinden ikisi, ülkemizde de kullanılmakta olan APCO P25 ve TETRA sistemleridir. APCO P25'in ülkemizde en büyük kullanıcısı Jandarma Genel Komutanlığı'dır. TETRA'nın kullanıcıları arasında başta Emniyet Genel Müdürlüğü, Karayolları Genel Müdürlüğü ve bazı belediyeler sayılabilir. İki farklı sistemi kullanan birimlerin birbiriyle görüşme şansı yoktur. Her kurum kullanacağı standardı kendine özgü ihtiyaçlar doğrultusunda belirlediği için, kullanılan standartların farklı olması çok doğaldır. Bu durum farklı standartları kullanan kurumların birlikte çalışması gereken durumlarda sorunlara neden olmakta; olağanüstü durum sayılabilecek bir afet veya kriz halinde, birlikte çalışacak kurumlar arasında koordinasyon eksiklikleri oluşmaktadır. Bu eksikliklerin en büyük nedeni kurumların kendi içlerinde farklı standartları kullanmasıdır. Örneğin böyle bir durumda, GSM ve PSTN gibi kapsamlı haberleşme sistemleri de zarar görmüş veya yoğunluktan hizmet veremez duruma gelmişse, sahada APCO P25 kullanan Jandarma personeli TETRA kullanan Emniyet

güçleriyle iletişim kuramamaktadır. Öncelikle, kamu güvenliğinin söz konusu olduğu böyle durumlar için veya ihtiyaç duyulan tüm durumlarda bu iki standardın birlikte çalışabilirliği büyük önem arz etmektedir. Farklı kurumların telsiz haberleşme şebekeleri ve bunların birbiriyle haberleşebilmeleri için gerekli yapı Şekil 1'de sunulmaktadır. Merkezde yer alan ağ geçidi yapısının bütün kurumların haberleşme standardını algılaması ve birbirine dönüştürme kabiliyetine sahip olması öngörülmektedir. Bu çalışma kapsamında, APCO P25 ve TETRA sistemleri arasında birlikte çalışmayı sağlayacak ağ geçidi uygulaması sunulmuştur. Günümüzde özellikle yazılım tabanlı telsiz ('Software Defined Radio', SDR) teknolojisinin gelişmesi ile böyle bir ağ geçidi geliştirme imkânı doğmuştur. SDR teknolojisinde telsiz işlevleri yazılımla gerçekleştirilir; dolayısıyla, gerçekleştirilen bir tasarımda, daha düşük bir maliyetle, daha kısa sürede iyileştirme ve değişiklik yapmak mümkündür. Özellikle sayısal işlemci hızlarının artmasıyla, SDR teknolojisi hızla gelişmektedir. Bu çalışmada SDR tabanlı bir uygulama olan, iki sayısal telsiz sistemi arasında iletişim kurulmasına olanak sağlayan bir ağ geçidi tasarımı önerilmektedir. Bu uygulamayla farklı iki standardı kullanan kullanıcılar kendi içlerinde veya karşılıklı haberleşebileceklerdir. Çalışmanın başında her iki standart ile ilgili genel bilgiler verilmiş ve sonrasında önerilen ağ geçidi uygulaması sunulmuştur.



Şekil 1. Farklı kurumların haberleşme şebekeleri ve ortak haberleşme yapısı.

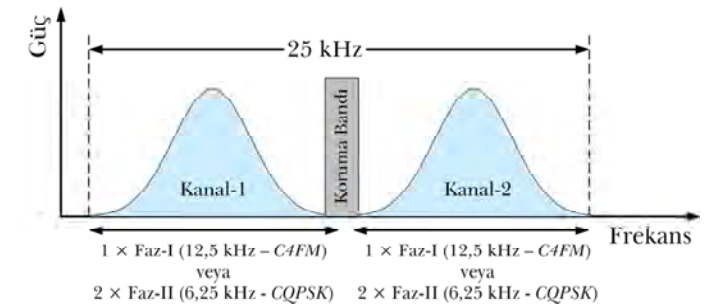
2 APCO P25 TELSİZ STANDARTI

APCO P25; Amerika Birleşik Devletleri'nde APCO tarafından 1989 yılında, başta Kamu Güvenliği olmak üzere iç güvenlik, acil durum yardım/destek ve teknolojik altyapı yönetimindeki gereksinimleri karşılamak için, analog telsizlerin çalışma bandını da kapsayacak ve karşılıklı konuşabilecek biçimde geliştirilmeye başlanan, açık mimarili sayısal telsiz haberleşme standardıdır [2]. P25 standardını

geliştirme çalışmalarına APCO ile birlikte; kullanıcı gereksinimlerinin belirlenmesi ve standart seçiminde Ulusal Devlet Telekomünikasyon Yöneticileri Birliği ('National Association of State Telecommunications Directors', NASTD) ve federal kurumlar, standartların geliştirilmesi ve onaylanmasında Telekomünikasyon Endüstrisi Birliği ('Telecommunications Industry Association', TIA) ve yayımlanmasında da Amerikan Ulusal Standartlar Enstitüsü ('American National Standards Institute', ANSI) katkı sunmaktadır.

APCO P25 standardı, geriye uyumluluğu da sağlayarak (analog telsizlerle) ilerlemesini iki fazda sürdürmüştür: Faz-I ve Faz-II. Faz-I standardında telsizler 12,5 kHz kanal aralığında, Sürekli 4 Düzeyli FM ('Continuous 4-Level Frequency Modulation', CFM) doğrusal olmayan modülasyon tekniği kullanarak analog, sayısal ya da karışık modda çalışmaktadır. Sayısal modda 4800 sembol/s veri iletim hızına ve - her sembol 2 bit olduğu için - iletilen kanalda toplam 9600 bit/s'lik hıza ulaşılmaktadır. Faz-II, geriye uyumluluğu da sağlayarak frekans spektrumunun daha verimli kullanılması amacıyla geliştirilme çalışmaları devam eden standarttır. Faz-II'de kanal kullanım aralığı, Uyumlu Dörtlü Faz Kaydırmalı Anahtarlama ('Compatible Differential Offset Quadrature Phase Shift Keying', CQPSK) modülasyon tekniği kullanılarak 6,25 kHz'e taşınmıştır. CFM için tasarlanan alıcılar, CQPSK gibi faz kaydırma tekniğini kullanan tüm vericilerle uyumludur. Bu çözümle Faz-I ve Faz-II arasında uyum sorunu olmamaktadır.

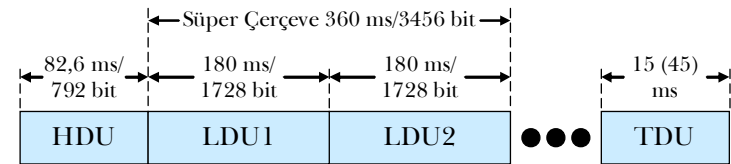
P25 sistemleri Genel Hava Arayüzü'nü ('Common Air Interface', CAI) kullanmaktadır [3]. Bu arayüz standardı P25 uyumlu telsizlerin gönderdiği işaretin tipini ve içeriğini tanımlamaktadır. Üreticiden bağımsız olarak bir P25 telsiz CAI'ı kullanarak herhangi bir P25 telsiz ile Frekans Çoğullamalı Çoklu Erişim ('Frequency Division Multiple Access', FDMA) kanal erişim tekniğiyle haberleşebilmektedir. FDMA tekniği spektrumu, frekans tanım bölgesinde birbirinden bağımsız frekans bölümlerine ayırır. Bu bölümler haberleşme birimlerden gelecek talebe göre kendilerine atanmaktadır. FDMA tekniği ile bugün 12,5 kHz kullanan



Şekil 2. APCO P25 sistemlerinde kullanılan FDMA erişim tekniği.

Faz-I telsizlerle 25 kHz'lik kanalda iki farklı görüşme yapılabileceği gibi, 6,25 kHz kullanan Faz-II telsizlerle bu sayı dörde çıkmaktadır (Şekil 2). *APCO* P25 telsizler analog modda 25 kHz veya 12,5 kHz kanal aralıklarıyla çalışabilmelidir. Bu geriye uyumluluk P25 kullanıcılarının eski analog sistemlerden sayısal sistemlere geçişini kolaylaştırmaktadır.

P25 sistemlerde haberleşme *CAI* üzerinden kodlanmış konuşmanın gönderilmesi ve alınması ile yapılmaktadır. Ses mesajının yapısı Şekil 3'te verilmiştir. P25 standardı konuşmayı kodlayıp sayısal bit akışı elde etmek için Gelişmiş Çok Bantlı Uyarma (*Improved Multi-Band Excitation*, *IMBE*) ses kodlayıcısı kullanılmaktadır. *IMBE*, sayısal bit akışını, her biri 88 bit uzunluğunda olan (20 ms konuşma) ses çerçevelerine (*voice frames*) parçalamaktadır. Ses çerçevelerini korumak için hata düzeltme kodları kullanılır; bunun sonunda 56 bit parite (artıklık) kontrol bilgisi eklenir. Böylece, ses çerçevesinin boyutu 144 bit olur. Ses çerçeveleri, her biri dokuz tane ses çerçevesinden oluşan iki farklı Mantıksal Bağlantı Veri Birimi (*Logical Link Data Unit*, *LDU*) ile gruplandırılır (LDU1 ve LDU2). Her bir *LDU* 180 ms uzunluğundadır ve ikisi bir araya gelerek 360 ms'lik Süper Çerçeve (*Super Frame*) oluşturur. Ses mesajı bir Başlık Veri Birimi (*Header Data Unit*, *HDU*) ile başlar. Bu birimde mesajın şifrelenmesi ve bağlantı kontrolleri için ilklendirme işlemleri yapılmaktadır. *HDU*'dan sonra *LDU*'ların oluşturduğu süper çerçeveler mesajın sonuna kadar yollar. Mesajın sonunda Sonlandırıcı Veri Birimi (*Terminator Data Unit*, *TDU*) gönderilmektedir.

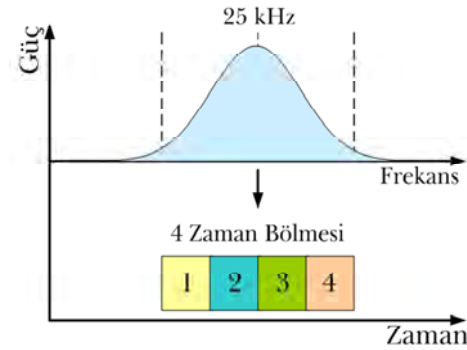


Şekil 3. *APCO* P25 standardı ses çerçeve yapısı.

3 TETRA TELSİZ STANDARTI

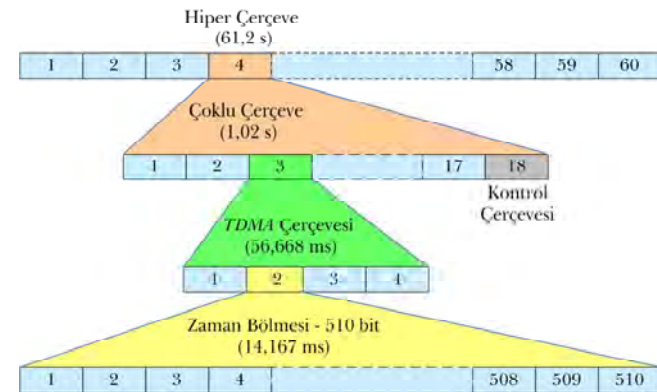
TETRA, Avrupa Telekomünikasyon Standartları Enstitüsü (*European Telecommunications Standards Institute*, *ETSI*) tarafından geliştirilmiş, açık mimarili sayısal trunk telsiz standardıdır. *ETSI* tarafından profesyonel telsiz kullanıcıları (Özel Gezgın Telsiz (*Private Mobile Radio*, *PMR*) ve Ortak Kullanımlı Gezgın Telsiz (*Public Access Mobile Radio*, *PAMR*)) için geliştirilmiş bir standart olan *TETRA* yaygın olarak, polis, itfaiye, ambulans ve sivil savunma gibi kamu güvenliğinden sorumlu kurumlar ile, ticari olarak lojistik ve güvenlik hizmet veren işletmeler tarafından kullanılmaktadır [4].

TETRA sistemleri Zaman Çoğullamalı Çoklu Erişim (*Time Division Multiple Access*, *TDMA*) kanal erişim tekniğini kullanılmaktadır. Sistemde 25 kHz'lik kanal aralığını zaman paylaşımını kullanan dört bağımsız zaman bölmesi (kullanıcı kanalı) bulunmaktadır (Şekil 4). Her bölme 14,167 ms uzunluğundadır. Birinci bölmeyi kullanan kullanıcı 14,167 ms iletim yaptıktan sonra durur ve sırayla diğer bölmelere atanmış kullanıcılar 14,167 ms iletim yaparlar. Dördüncü bölmedeki kullanıcı da iletimini tamamladıktan sonra tekrar birinci bölmedeki kullanıcı iletim yapar. Dört bölmedeki kullanıcı toplamda 56,668 ms'lik bir çerçeve oluşturur. Kanal yoğunluğunun fazla olduğu sistemlerde bu erişim tekniği ile frekans spektrumu oldukça verimli kullanılmaktadır.



Şekil 4. *TETRA* sistemlerinde kullanılan *TDMA* erişim tekniği.

TETRA çerçeve yapısında her *TDMA* çerçevesi için 4 zaman bölmesi bulunmaktadır. Her bölme 510 bit bilgi taşımaktadır. 18 *TDMA* çerçevesi bir araya getirilerek Çoklu Çerçeve (*Multi-Frame*) yapısını, altmış çoklu çerçeve bir araya gelerek Hiper Çerçeve (*Hyper-Frame*) yapısını oluşturur (Şekil 5). Çoklu çerçeve yapısında ses ve veri haberleşmesi yapılan on yedi *TDMA* çerçevesinin trafik kontrol işaretleri on sekiz *TDMA* çerçevesinde toplanır ve böylece haberleşme bölmelerinde kesilme olmadan kontrol işlemleri bu çerçeve üzerinden yürütülür.

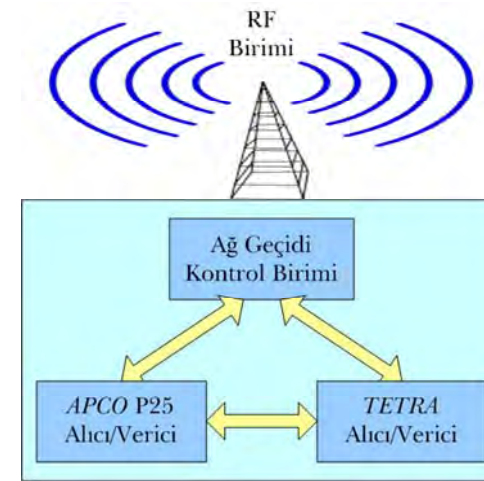


Şekil 5. *TETRA* standardı çerçeve yapısı.

TETRA sisteminde ses, 8 kbit/s ile örneklenir ve *ACELP* (*Adaptive Code Excited Linear Prediction*, Doğrusal Hareketli Cebirsel Kod Tahmini) tekniğini kullanan *'vocoder'* (*voice encoder/decoder* - ses kodlayıcısı/kod çözücüsü) tarafından sıkıştırılarak 4,567 kbit/s'lik veri akışı elde edilir. Elde edilen veri, iletim kanalının neden olacağı hatalara karşı iletimden önce kodlanmıştır. *TETRA* sistemi farklı iletim oranlarında ve farklı hata koruma düzeylerinde ses iletimini, devre anahtarlamalı ve paket anahtarlamalı veri iletimini desteklemektedir. *TETRA* sistemi sayısal modülasyon olarak ise faz kaydırmalı anahtarlama tekniği olan $\pi/4$ Diferansiyel Dörtlü Faz Kaydırmalı Anahtarlama (*Differential Quadrature Phase Shift Keying*, *DQPSK*) kullanılmaktadır. Sembol hızı (*baud*) 18 ksembol/s'dir. Her sembol 2 bit bilgi taşıdığı için toplam hız, brüt 36 kbit/s olur.

4 AĞ GEÇİDİ UYGULAMASI

Telsiz sistemlerinin birlikte çalışma ihtiyacı, aralarında Türkiye'nin de üyesi bulunduğu Uluslararası Telekomünikasyon Birliği (*International Telecommunication Union*, *ITU*) ve Avrupa Posta ve Telekomünikasyon İdareleri Birliği (*European Conference of Postal and Telecommunications Administrations*, *CEPT*) tarafından da görülmüş ve 380–385/390–395 MHz frekans bandının tüm üye ülkelerde kamu güvenliği ve acil durum haberleşmesinde kullanılması kabul edilmiştir. *APCO* P25 telsiz sistemi 136–174 MHz, 403–512 MHz ve 800 MHz çevresi frekans aralıklarında çalışmaktadır. Farklı üreticilerin daha özel frekans aralıklarını kapsayan ürünleri de mevcuttur. *TETRA* telsiz sistemi ise 380–400 MHz, 410–430 MHz ve 800 MHz çevresi frekans aralıklarında çalışmaktadır. Aşağıda adımları verilen ağ geçidi uygulamasında *APCO* P25 veya *TETRA*'yı kullanan kurumların kamu güvenliği ve acil durumla ilgili bir durum için 380–385 veya 390–395 MHz frekans bandını kullandığı varsayılmaktadır.



Şekil 6. Ağ geçidi uygulamasının blok şeması.

Önerilen ağ geçidi yapısı Şekil 6'da verilmektedir. Bu yapıda *APCO* veya *TETRA* vericisi tarafından gönderilen RF yayını, önerilen Ağ geçidi yapısının RF Birimi ile algılanmaktadır. Ağ Geçidi Kontrol Birimi'nde yazılım tabanlı bir tanıma algoritması ile yayın tipi (*APCO* P25 veya *TETRA*) tanımlanmakta ve ilgili alıcıya iletilmektedir. İlgili alıcı iletilen mesajı çözer ve diğer yapının vericisine iletir. Diğer standardın vericisi, mesajı kendi standardına göre modüle eder ve Ağ geçidi üzerinden RF birime ileterek yeniden gönderilmesini sağlar. Sistem bloklarının genel yapısı ve işlevi aşağıda verilmektedir.

- Öncelikle RF Birim anten vasıtasıyla havadan yayını alır ve frekans düşürücüden geçirip analog formdan sayısal forma çevirerek Ağ Geçidi Kontrol Birimi'ne (AGKB) iletir;
- AGKB öncelikle, aldığı bu işaretin *APCO* P25 ya da *TETRA* olduğuna karar verir. Bunun için işaretin bant genişliğine dayalı bir sınıflandırma yapar. *TETRA* 25 kHz bant genişliğine sahiptir. *APCO* P25 ise Faz-I için 12,5 kHz, Faz-II için ise 6,25 kHz bant genişliğine sahiptir. Bant genişliği kestiriminde Welch yöntemi kullanılarak işaretin güç spektral yoğunluğu (*Power Spectral Density*, *PSD*) elde edilir [5]. *PSD* kestiriminde %50 örtüşme oranı için 1024 nokta *FFT* ve Hamming pencerelemesi kullanılır. *PSD*'de değeri belirli bir eşik düzeyinin üzerinde olan nokta sayısı işaretin bant genişliği ile ilgilidir. Eşik düzeyi merkez etrafındaki 512 değer en düşük 75'inin (%15) ortalaması olarak kestirilir. Daha sonra bu değer üzerindeki nokta sayısı hesaplanır, *TETRA* ve *APCO* P25 (Faz-I veya Faz-II) için atanan sayıyla kıyaslanarak gelen işaretin türüne karar verilir;
- *TETRA* veya *APCO* P25 (Faz-I veya Faz-II) olarak sınıflandırılan işaret AGKB tarafından alt düzeyde koşan uygun alıcı/verici birimine yollar. Alıcı/verici birimi aldığı işaret üzerinde, standartla tanımlanan temel bant işlemleri yaparak çerçevelere ayırır ve sonrasında bu çerçeveleri de parçalayarak iletilen veri elde edilir;
- Elde edilen veri alıcı/verici biriminden ötekine ağ geçidi uygulaması üzerinden iletir. Bu veriyi alan diğer alıcı/verici birimi standartla tanımlı uygun çerçeve yapısını oluşturur ve bunu AGKB'ye iletir;
- AGKB gelen bu işareti sayısal formdan analog forma çevirir ve uygun frekansa yükselterek anten vasıtasıyla gönderir.

Böylece, bir standardın formunda iletilen veri diğer forma dönüştürülmüş ve diğer form alıcılarının da veriyi algılayabilmesi sağlanmış olmaktadır. Uygulamada en kritik nokta yukarıda belirtilen işlevlerin hızlı bir biçimde

gerçeklenmesidir. Çünkü alıcı ile verici arasında standartların öngördüğü bir alış ve veri işlevleri gecikmesiyle birlikte, fazladan bir alıcı ve verici işlevleri gecikmesi daha eklenmektedir. Ancak, günümüzde çok yüksek hızlı sayısal işlemciler kullanarak bu işlemler gerçekleştirilebilmektedir. Bu çalışma kapsamında, *APCO* alıcı/verici (modülasyon/demodülasyon) yapılarına ilişkin yüksek hızlı sayısal işlemciler *FPGA* (Xilinx Virtex-4SX35) üzerinde gerçekleştirilmiş ve standart isteklerinden çok daha kısa sürelerde gerçekleştirilebileceği görülmüştür. Böylece ağ geçidinin araya girmesiyle oluşacak fazladan gecikme en düşük düzeye indirilmiştir.

5 SONUÇ

Farklı kurumların kullandığı iki açık sayısal telsiz sistemi incelenmiş ve birbirleriyle haberleşebilme olanağı irdelenmiştir. Bu çalışmanın amacı, başta kamu güvenliği ve acil durumlar için olmak üzere, farklı kurumların kullandığı *APCO* P25 ve *TETRA* telsiz sistemlerinin birlikte kullanılabilmesine olanak sağlayacak yeni bir uygulama geliştirmektir. Bugün için birlikte kullanılmayan bu sistemler ağ geçidi uygulaması üzerinden birlikte çalışabilecektir. Özellikle, zamanın kritik olduğu kriz anlarında iletişim aksaklıkları ortadan kalkacak ve farklı ihtiyaçlar sonucu temin edilmiş bu iki altyapı birlikte de kullanılabilir.

TEŞEKKÜR

Bu yazının gözden geçirilmesi sırasında gösterdikleri büyük titizlik nedeniyle Sayın Doç. Dr. Bahattin Türetken'e ve Sayın Dr. Levent Balamir Tavacıoğlu'na teşekkür ederiz.

KAYNAKÇA

- [1] B. P. Lathi, *Modern Digital and Analog Communication Systems*, 3rd ed. New York: Oxford University Press, 1998, pp. 5–18.
- [2] Telecommunications Industry Association, *APCO Project 25 System and Standards Definition*, TSB-102-A, 1995.
- [3] Telecommunications Industry Association. *APCO Project 25 FDMA Common Air Interface New Technology Standards Project Digital Radio Technical Standards*, TIA/EIA-102.BAAA, 1998.
- [4] TETRA-MOU, 1996-2010, TETRA Association [online], <http://www.tetramou.com/tetramou.aspx?id=44>.
- [5] E. H. Zorlu *et al.*, “Blind signaling identification for multimode SDR receiver with applications to public safety communications,” *Software Defined Radio Forum Tech. Conf. (SDR'09)*, Washington, D.C., Dec. 2009.

Olasılık Kuramına Bir Giriş – I: Temel Kavramlar

C. Nezih GEÇKİNLİ

Özet - *Günlük yaşamda sıkça kullandığımız olasılık kavramı kolay anlaşılır modeller yardımıyla açıklanmakta, olasılık kuramının temel özellikleri örneklerle tanıtılmaktadır.*

Anahtar Sözcükler - *Olasılık kuramı.*

1 GİRİŞ

Olasılık kuramı (*probability theory*), rasgele davranan (davranışları önceden tam ve doğru olarak kestirilemeyen) [1] olayları inceleyip modelleyen, tündengelimli (dedüktif), belitler (aksiyomlar) üzerine kurulu bir bilim dalıdır [2]. Hemen her bilimsel çalışma alanında (örneğin fizik, kimya, biyoloji, istatistik, bilişim, tıp, mühendislik alanlarında) sıkça başvurulan olasılık kuramı, matematiğin bir konusu olmasına karşın, bilgisayarların yaygın ve etkin kullanımıyla birlikte, fizik gibi deneysel bir bilime dönüşmüştür: Nasıl ki, dalından kopup düşen elmaları gözleyen Newton, kütleler arası çekim yasasının matematiksel bağıntısını yazdıysa [3], olasılık kuramında da, benzetimi (simülasyonu) bilgisayarla gerçekleştirilerek gözlenen rasgele olayların matematiksel modeli kurulabilir. Tersine, nasıl ki, Einstein'ın salt dehasını kullanarak yazdığı Genel Görelilik Kuramı'nın doğruluğu, tam güneş tutulması sırasında, güneşin yakınından geçerek bize ulaşan ışıkların sapması ölçülerek kanıtlandıysa [4], olasılık kuramında da, bilinen olasılık yasalarından akıl yürütme yoluyla elde edilen yeni bir olasılık bağıntısı ya da yasası, bilgisayar yardımıyla sınanabilir.

Bilgisayar, sayılar kuramı konusunda çalışan matematikçilerin dünyasına da, *Mathematica*, *Maple*, *Magma* gibi, matematiksel işlemleri hem sayısal hem de simgesel olarak yapabilen yardımcı programlarla girmiş [5]; üstelik, 124 yıl boyunca çözülemeyen, görünüşte kolay Dört Renk Problemi (iki boyutlu haritayı, bir çizgi boyunca komşu olan iki ülke aynı renkte olmayacak biçimde boyamak için dört rengin yeterli olduğunu kanıtlama) bilgisayar yardımıyla çözüldüncə, kanıtın geçerliliği matematikçileri ikiye bölmüş, yıllarca süren tartışmalara neden olmuştur [6].

Temelini, yaklaşık 350 yıl önce Pascal ile Fermat'ın attığı olasılık kuramına, son 200 yıl içinde üç yaklaşım önerilmiştir [2], [7]:

1°) 1800'lerin başında, Laplace ile Bernoulli'nin **sezgisel**, **klasik** ya da **önsel** (apriori) olarak adlandırılan, (eşit

olasılıklı N sayıda olası çıktısı olan fiziksel olaylara uygulanabilen) matematiksel yaklaşımı;

2°) 1900'lerin başında, von Mises'in **deneysel**, **bağlı sıklık** (*relative-frequency*) ya da **sonsal** (aposteriori) olarak adlandırılan, (gözlemlenen fiziksel bir olayın olasılığı, gözlem sayısı sonsuza giderken, olayın gözlenme sayısının toplam gözlem sayısına oranı olarak alınan) sistematik yaklaşımı;

3°) 1933'te, Kolmogorov'un ölçüm kuramı (*measure theory*) üzerine kurduğu **belitsel** (aksiyomatik) yaklaşımı.

Bugün matematikçiler, olasılık kuramını Kolmogorov'un belitsel yaklaşımı ile incelerler [8]. Uygulamalı bilimle uğraşanlar ise, öğrenilmesi güç olan ölçüm kuramı yerine, küme kuramı (*set theory*) üzerine kurdukları belitsel bir yaklaşım kullanırlar ve gerektiğinde de diğer (sezgisel ve deneysel) yaklaşımlardan yararlanırlar [2]. Uygulamalı bilimcilerin matematikçilerce pek kabul görmeyen bu yaklaşımla yazılmış kitapları da, kütüphanelerde, matematikçilerin olasılık kuramı kitaplarına ayrılmış raflarda yer alır.

2 OLAY

Gerçek ya da düşsel bir düzen ya da düzeneğin kimi rasgele özellikleri, önceden belirlenen koşullar altında, önceden belirlenen kurallara göre gözlemleniyor olsun ya da gözlemleniyor varsayalım. Bu işlem, anlatım kolaylığı için, gözlemlenen rasgele değerleri üreten, durağan (istatistiksel özellikleri zamanla değişmeyen), belleksiz (yeni üretilenin eski üretimlerden etkilenmediği) bir **kaynak** (bilgi kaynağı) olarak modellensin ve olası çıktı değerlerinin oluşturduğu küme (**kaynağın abecesine**) de **örnek uzayı** denilsin. (Bu işlemi, uygulamalı bilimciler “deney” olarak tanımlar [2], [7]; matematikçiler ise, gerçel sayı doğrusu üzerindeki bir aralıktan rasgele bir sayı çekme olarak modeller [8] (sf. 45). “Kaynak” ve “kaynağın abecesi” kavramları bilgi kuramından alınmadır [9] ve gözlemlenebilen rasgele değerlerin her türünü, buyruk altına alamadığımız, güneşteki patlamalar gibi doğal olayları da kapsar. Kaynak bellekli olabilir, ancak, olasılık kuramına girişte belleksiz varsayılır; bellekli olanları, belirli bir yetkinliğe ulaşıldıktan sonra incelenir.)

Kaynak-1: 3-6 aylık bebeklerin cinsiyeti, kilograma yuvarlanmış ağırlıkları ve santimetreye yuvarlanmış boyları, çıktı olsun. Erkek E , kız K ile; 3'ten küçük ağırlıklar 3, 12'den büyük ağırlıklar 12 ile; 50'den kısa boylar 50, 79'dan uzun boylar 79 ile gösterilsin. Bu kaynağın örnek uzayı, $2 \times 10 \times 30 = 600$ ögeli $\{(E,3,50), (E,3,51), \dots, (K,12,79)\}$ kümesidir.

- Örnek uzayının her alt kümesine **olay** denir [9].

Kaynak-2: Bir bozuk para, geniş düz bir alanda, en az bir metre yukarıya doğru, en az 10 kez dönecek biçimde elle atıldığında, dik olanları dışında art arda gelen iki atış sonucu, çıktı olsun. Yazı Y , tura T ile gösterilsin. Bu kaynağın örnek uzayı

$$S = \{YY, YT, TY, TT\} \quad (1)$$

kümesidir. Bu 4 ögeli kümenin olası $2^4 = 16$ alt kümesinin her biri ayrı bir olayı gösterir:

$$\begin{aligned} O_0 &= \{\} = \phi, \\ O_1 &= \{YY\}, \quad O_2 = \{YT\}, \quad O_3 = \{TY\}, \quad O_4 = \{TT\}, \\ O_5 &= \{YY, YT\}, \quad O_6 = \{YY, TY\}, \quad O_7 = \{YY, TT\}, \\ O_8 &= \{YT, TY\}, \quad O_9 = \{YT, TT\}, \quad O_{10} = \{TY, TT\}, \\ O_{11} &= \{YY, YT, TY\}, \quad O_{12} = \{YY, YT, TT\}, \\ O_{13} &= \{YY, TY, TT\}, \quad O_{14} = \{YT, TY, TT\}, \\ O_{15} &= \{YY, YT, TY, TT\} = S \end{aligned} \quad (2)$$

Bir başka deyişle, kaynak hiçbir çıktı üretmediğinde O_0 olayı; YY ürettiğinde, $O_1, O_5, O_6, O_7, O_{11}, O_{12}, O_{13}$ ve O_{15} olayları; YT ürettiğinde, $O_2, O_5, O_8, O_9, O_{11}, O_{12}, O_{14}$ ve O_{15} olayları; TY ürettiğinde, $O_3, O_6, O_8, O_{10}, O_{11}, O_{13}, O_{14}$ ve O_{15} olayları; TT ürettiğinde de $O_4, O_7, O_9, O_{10}, O_{12}, O_{13}, O_{14}$ ve O_{15} olayları gerçekleşir. Kaynak herhangi bir çıktı ürettiğinde, O_{15} olayı mutlaka gerçekleşmektedir.

- Kümesi boş ($\{\}$) olan olaya, “olanaksız olay” (ϕ); kümesinde tek öge olan olaya, “temel olay”; kümesi örnek uzayı S olan olaya da “kaçınılmaz olay” (S) adı verilir.

Örneğin, Kaynak-2’de O_0 , olanaksız olay; O_1, O_2, O_3 ve O_4 , temel olaylar; O_{15} , kaçınılmaz olaydır.

- Olaylar kümelerine verilen adlar olduğu için, kümeler için geçerli olan tüm kavram ve işlemler olaylar için de geçerli olmaktadır.

- Kümelerinde ortak ögesi olmayan olaylara **kesişmeyen olaylar** denir.

Örneğin, temel olaylar kesişmez.

- Kesişmeyen olaylardan herhangi biri gerçekleştiğinde, diğerleri gerçekleşmez.

Örneğin, temel olaylardan biri gerçekleştiğinde, diğer temel olaylar gerçekleşemez.

- Kümesinde ortak ögeleri olan olaylara **kesişen olaylar**, kesişen olayların ortak ögelerinin oluşturduğu olaya **kesişim olayı** denir. Kesişim olayı gerçekleştiğinde, kesişen olayların hepsi birden gerçekleşir.

Örneğin, Kaynak-2’de, kesişen O_{12} ile O_{14} olaylarının kesişimi O_9 olayıdır: $O_{12} \cap O_{14} = O_9$. O_9 olayı gerçekleştiğinde, yani, kaynağın çıktısı YT ya da TT olduğunda, O_{12} ile O_{14} olayları da gerçekleşir.

- Kesişen ya da kesişmeyen **olayların bileşimi**, bu olayların kümelerindeki ögelerin tümünü içeren olaydır.

Örneğin, Kaynak-2’de, O_7 ile O_{10} olaylarının bileşimi O_{13} olayıdır: $O_7 \cup O_{10} = O_{13}$

- Her olay, olayın kümesindeki ögelere karşı düşen temel olayların bileşimidir.

Örneğin, Kaynak-2’de: $O_{14} = O_2 \cup O_3 \cup O_4$

- Bir olayın kümesinde olmayan ögelerin oluşturduğu olaya, **tümleyen olay** ya da **olayın tümleyeni** denir. Bir olay gerçekleştiğinde, olayın tümleyeni gerçekleşmez.

Örneğin, Kaynak-2’de, O_6 olayının tümleyeni O_9 ; O_9 olayının tümleyeni O_6 ’dır: $O_6' = O_9$, $O_9' = O_6$

- Olanaksız olayla kaçınılmaz olay birbirini tümler.

Örneğin, Kaynak-2’de: $O_0' = O_{15} = S$, $O_{15}' = O_0 = \phi$

- Bir olay ile onun tümleyeni olan olay kesişmez.

Örneğin, Kaynak-2’de: $O_6 \cap O_6' = O_6 \cap O_9 = O_0 = \phi$

- Bir olay ile onu tümleyen olayın bileşimi kaçınılmaz olaydır.

Örneğin, Kaynak-2’de: $O_6 \cup O_6' = O_6 \cup O_9 = O_{15} = S$

- Bir olayın başka bir olayla ve o olayın tümleyeniyle kesişimleri kesişmeyen olaylardır.

Örneğin, Kaynak-2’de:

$$(O_8 \cap O_6) \cap (O_8 \cap O_6') = (O_8 \cap O_8) \cap (O_6 \cap O_6') = O_0 = \phi$$

- Bir olayın başka bir olayla ve o olayın tümleyeniyle kesişimlerinin bileşimi, olayın kendisini verir.

Örneğin, Kaynak-2’de:

$$\begin{aligned} (O_8 \cap O_6) \cup (O_8 \cap O_6') &= (O_8 \cap O_6) \cup (O_8 \cap O_9) \\ &= O_3 \cup O_2 = O_8 \end{aligned}$$

3 OLASILIK

N ögeli örnek uzayı $S = \{s_1, s_2, \dots, s_N\}$ üzerinde tanımlanan **olasılık dağılımı fonksiyonu**

$$P(s) \geq 0, \quad s \in S \quad (3)$$

örnek uzayındaki her ögeye karşı,

$$\sum_{i=1}^N P(s_i) = 1 \quad (4)$$

koşulunu sağlayan bir olasılık değeri atar [9]. (Bu koşullar, $P(s_i) \leq 1$ olmasını gerektirir. Örnek uzayı, gerçel sayı doğrusu üzerindeki bir $[a, b]$ aralığı olduğunda, örnek uzayındaki öge sayısı sonsuz olur ve ikinci koşul (4)

$$\int_a^b P(s) ds = 1 \quad (5)$$

haline gelir.)

Olasılık değerleri değişik yollardan elde edilebilir:

- Dengeli (hilesiz) bir zar atıldığında, her yüzün gelme olasılığı aynı olduğundan, her bir sayının gelme olasılığı $1/6$ ’dır:

$$P(1) = P(2) = \dots = P(6) = \frac{1}{6} \quad (6)$$

Atanan bu olasılık değeri akıl yürütme yoluyla elde edilmektedir.

- Türkiye İstatistik Kurumu’nun Boşanma İstatistikleri Veri Tabanı’na göre [10], 2007 yılında boşanan 94219 çiftten 3779’unun evlilik süresi 1 yıldan azdır:

$$\begin{aligned} P(B) &= \{\text{Boşanan çiftin 1 yıldan az evli kalma olasılığı}\} \\ &= 0,040 \end{aligned} \quad (7)$$

Atanan bu olasılık sayım yoluyla elde edilmektedir.

- Türkiye İstatistik Kurumu’nun açıkladığı, Türkiye ile birlikte 14 ülkede gerçekleştirilen 2008 yılına ilişkin, Küresel Yetişkin Tütün Araştırması’nın sonucu elde edilen, gençlerin sigara kullanma alışkanlığı [11],

$$\begin{aligned} P(G) &= \{15 - 24 \text{ yaş arası sigara kullanma olasılığı}\} \\ &= 0,253 \end{aligned} \quad (8)$$

örnekleme yoluyla kestirilmektedir.

- Bir doktorun tedavi etmeye başladığı hasta için söylediği iyileşme olasılığı, örneğin %80,

$$\begin{aligned} P(T) &= \{\text{Tedavi edilen hastanın iyileşme olasılığı}\} \\ &= 0,800 \end{aligned} \quad (9)$$

doktorun kişisel görüş ve deneyimlerine dayanarak yaptığı değerlendirme sonucu verdiği, 0–1 arası nottur.

Yukarıda verilen, akıl yürütme, sayım, örnekleme ve duygusal değerlendirme yoluyla elde edilen olasılık değerlerinin güvenilirliği, sırasıyla azalmaktadır. Ancak yine de, olasılık kuramında, atanan her olasılık değerinin tam doğru olduğu varsayılır.

- S örnek uzayının s_i ögesine karşı düşen O_i temel olayının olasılığı, olasılık dağılım fonksiyonunun s_i ’deki değeriyle aynı olur: $P(O_i) = P(s_i)$. (Örnek uzayı, gerçel sayı doğrusu üzerindeki bir aralık olduğunda, bu aralık herhangi bir biçimde N parçaya ayrılarak, N ögeli bir kümeye dönüştürülebilir. Bu durumda, her ögeye karşı düşen temel olayın olasılığı, o ögeye ait aralıkta, $P(s)$ ’nin altında kalan alan olur.)

- Herhangi bir olayın olasılığı, o olayın kümesindeki ögelere karşı düşen temel olayların olasılıklarının toplamına eşit olur. (Örnek uzayı, gerçel sayı doğrusu üzerindeki bir aralık olduğunda, herhangi bir olayın olasılığı, o olaya ait aralık ya da aralıklarda, $P(s)$ ’nin altında kalan toplam alan olur.)

Örneğin, Kaynak-2’de, $P(O_{11}) = P(O_1) + P(O_2) + P(O_3)$

- Olanaksız olayın olasılığı $P(\phi)$, kümesi boş olduğu için 0; kaçınılmaz olayın olasılığı $P(S)$, kümesinde, örnek uzayın tüm ögeleri olduğu için 1’dir.

Örneğin, Kaynak-2’de:

$$\begin{aligned} P(O_0) &= P(\phi) = 0, \\ P(O_{15}) &= P(O_1) + P(O_2) + P(O_3) + P(O_4) = P(S) = 1 \end{aligned}$$

- Kesişmeyen olayların bileşimi olan olayın olasılığı, bu kesişmeyen olayların olasılıklarının toplamı olur.

Örneğin, Kaynak-2’de:

$$\begin{aligned} P(O_{11}) &= P(O_1 \cup O_8) = P(O_1) + P(O_8) \\ &= P(O_1) + P(O_2 \cup O_3) = P(O_1) + P(O_2) + P(O_3) \end{aligned}$$

- Bir olay ile onu tümleyen olayın olasılıklarının toplamı 1’dir.

Örneğin, Kaynak-2’de: $P(O_6) + P(O_6') = P(O_6) + P(O_9) = 1$

- Kesişen iki olayın bileşimi olan olayın olasılığı, iki olayın olasılıklarının toplamından iki olayın kesişimi olan olayın olasılığı çıkarılarak elde edilebilir.

Örneğin, Kaynak-2’de:

$$\begin{aligned} P(O_5 \cup O_9) &= P(O_5) + P(O_9) - P(O_5 \cap O_9) \\ &= [P(O_1) + P(O_2)] + [P(O_2) + P(O_4)] - P(O_2) \\ &= P(O_1) + P(O_2) + P(O_4) = P(O_{12}) \end{aligned}$$

4 KOŞULLU OLASILIK

Yeni bir kaynak tanımlansın; öyle ki, eski kaynağın ürettiklerinden, yalnızca, olanaklı bir B olayının kümesinde olanları dışarı çıkartsın, diğerlerini çıkartmasın, göz ardı etsin. Bir başka deyişle, örnek uzayı S olan kaynaktan, örnek uzayı S ’nin alt kümesi B olan yeni bir kaynak elde edilsin. Sonra, B ’deki temel olayların (öğelerin) olasılıkları, bu olasılıkların toplamı olan $P(B)$ ’ye bölünerek, yeni

kaynaktaki kaçınılmaz olayın olasılığı 1 yapılış. (Bölme işlemi, temel olayların olasılıklarının birbirlerine göre oranlarını koruduğu için, bulunan yeni olasılık değerleri doğrudur.) Tanımlanan bu yeni kaynağın yardımıyla, **koşullu olasılık** olarak adlandırılan, B olayı gerçekleştiğinde A olayının da gerçekleşme olasılığı $P(A|B)$, kolayca hesaplanabilir:

Eski kaynaktaki A olayını oluşturan temel olaylardan, yalnızca, A olayı ile B olayının kesişimindekiler yeni kaynağın çıkışında gözükür. Yeni kaynaktaki her çıktı B olayının gerçekleştiğini gösterdiği için, A ile B olayının kesişimindeki temel olayların yeni kaynaktaki ($P(B)$ 'ye bölünerek bulunan) olasılıklarının toplamı, B olayının gerçekleşmesi koşulu altında A olayının gerçekleşmesi olasılığını, eski kaynaktaki olasılıklar cinsinden

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \quad (10)$$

olarak verir. Doğal olarak, bu eşitlik, A ile B yer değiştirdiğinde de geçerlidir:

$$P(B|A) = \frac{P(B \cap A)}{P(A)} \quad (11)$$

Son iki eşitlik, $P(A|B)$ ile $P(B|A)$ koşullu olasılıkları arasındaki ilişkiyi verir:

$$P(A \cap B) = P(A|B) P(B) = P(B|A) P(A) \quad (12)$$

Bu ilişki, koşullu olasılıkların oranının koşulsuz olasılıkların oranıyla aynı olduğunu gösterir:

$$\frac{P(A|B)}{P(B|A)} = \frac{P(A)}{P(B)} \quad (13)$$

Örneğin, atılan dengeli bir zarın çift geldiğini bildiğimizde gelen sayının 4 olma olasılığı

$$P(4|\{2,4,6\}) = \frac{P(4 \cap \{2,4,6\})}{P(\{2,4,6\})} = \frac{P(4)}{P(\{2,4,6\})} = \frac{1}{3}, \quad (14)$$

4 geldiğini bildiğimizde gelen sayının çift olma olasılığı

$$P(\{2,4,6\}|4) = \frac{P(\{2,4,6\} \cap 4)}{P(4)} = \frac{P(4)}{P(4)} = 1 \quad (15)$$

ve ikisinin oranı da

$$\frac{P(4|\{2,4,6\})}{P(\{2,4,6\}|4)} = \frac{P(4)}{P(\{2,4,6\})} = \frac{1}{3} \quad (16)$$

olmaktadır.

Yukarıda $k=2$ olay için bulunan koşullu olasılık bağıntıları (10) ve (11), $k>2$ için de $k!$ biçimde yazılabilir. Örneğin, A, B, C ve D olayları için bağıntılardan biri

$$\begin{aligned} P(A \cap B \cap C \cap D) &= P(A) \frac{P(A \cap B)}{P(A)} \frac{P(A \cap B \cap C)}{P(A \cap B)} \frac{P(A \cap B \cap C \cap D)}{P(A \cap B \cap C)} \\ &= P(A) P(B|A) P(C|A \cap B) P(D|A \cap B \cap C) \end{aligned} \quad (17)$$

olur [12]. Diğerleri, bu bağıntıdan, olaylar yer değiştirilerek elde edilebilir.

5 BAĞIMSIZ OLAYLAR

A ile B birbirinden **bağımsız iki olay** ise, A olayının gerçekleşmesi ya da gerçekleşmemesi B olayının gerçekleşmesine ya da gerçekleşmemesine ve tersine, B olayının gerçekleşmesi ya da gerçekleşmemesi A olayının gerçekleşmesine ya da gerçekleşmemesine bağlı olamaz. Bu durumda, aşağıdaki eşitliklerin tümü sağlanır:

$$\begin{aligned} P(A|B) &= P(A), \\ P(B|A) &= P(B), \\ P(A|B') &= P(A), \\ P(B'|A) &= P(B'), \\ P(A'|B') &= P(A'), \\ P(B'|A') &= P(B'), \\ P(A'|B) &= P(A'), \\ P(B|A') &= P(B) \end{aligned} \quad (18)$$

Bu eşitliklerden, (12) eşitliği kullanılarak, şu dört eşitlik elde edilir:

$$\begin{aligned} P(A \cap B) &= P(A)P(B), \\ P(A \cap B') &= P(A)P(B'), \\ P(A' \cap B') &= P(A')P(B'), \\ P(A' \cap B) &= P(A')P(B) \end{aligned} \quad (19)$$

Bu dört eşitlikten herhangi birini sağlayan A ve B olayları, yukarıda verilen sekiz eşitlikten ikisini sağlar, yani, birbirinden bağımsızdır. Örneğin, (19)'un ilk eşitliği kullanılarak (18)'in ilk iki eşitliği kanıtlanabilir:

$$\begin{aligned} P(A|B) &= \frac{P(A \cap B)}{P(B)} = \frac{P(A)P(B)}{P(B)} = P(A), \\ P(B|A) &= \frac{P(B \cap A)}{P(A)} = \frac{P(B)P(A)}{P(A)} = P(B) \end{aligned} \quad (20)$$

Ayrıca, (19)'daki dört eşitlikten herhangi birini sağlayan A ve B olayları diğer üç eşitliği de sağlar. Nitekim, bu eşitliklerin birincisinden ikincisi, ikincisinden üçüncüsü, üçüncüsünden dördüncüsü ve dördüncüsünden birincisi elde edilebilir. Örneğin,

$$\begin{aligned} A &= (A \cap B) \cup (A \cap B') \Rightarrow P(A) = P(A)P(B) + P(A \cap B') \\ &\Rightarrow P(A \cap B') = P(A)(1 - P(B)) = P(A)P(B') \end{aligned} \quad (21)$$

bağıntısını elde edebiliriz.

Böylece, (18) ve (19)'daki toplam on iki eşitlikten herhangi birini sağlayan A ve B olaylarının birbirinden

bağımsız olduğu ve diğer on bir eşitliği de sağladığı kanıtlanmış olur.

A ve B olayları birbirinden bağımsız iki olaysa, insan, genellikle yanlış, bu iki olayın kesişmediğini düşünür. Oysa, birbiriyle kesişmeyen iki olay arasında güçlü bir bağ vardır: Olaylardan biri gerçekleştiğinde diğeri gerçekleşemez. Bir başka deyişle, olasılığı 0 olmayan iki olayın birbirinden bağımsız olabilmesi için, birbiriyle kesişiyor olması gerekir. Örneğin, atılan dengeli bir zarın çift (2, 4 ya da 6) gelmesi ile 3'ten küçük (1 ya da 2) gelmesi olayları, birbiriyle kesişen, ancak, birbirinden bağımsız iki olaydır:

$$\begin{aligned} P(\{2,4,6\} \cap \{1,2\}) &= P(2) = \frac{1}{6}, \\ P(\{2,4,6\}) P(\{1,2\}) &= \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6} \end{aligned} \quad (22)$$

A, B, C gibi üç olayın birbirinden bağımsızlığı söz konusu olduğunda, herhangi iki olayın birbiriyle bağımsız olması,

$$\begin{aligned} P(A \cap B) &= P(A) P(B), \\ P(A \cap C) &= P(A) P(C), \\ P(B \cap C) &= P(B) P(C), \end{aligned} \quad (23)$$

ayrıca, herhangi iki olayın kesişiminin de üçüncüden bağımsız olması gerekir:

$$\begin{aligned} P(A \cap B \cap C) &= P(A \cap B) P(C) \\ &= P(A \cap C) P(B) \\ &= P(B \cap C) P(A) \\ &= P(A) P(B) P(C) \end{aligned} \quad (24)$$

Örneğin,

$$\begin{aligned} S &= \{1,2,3,4,5,6,7,8\}, \quad P(1) = P(2) = \dots = P(8) = 1/8, \\ A &= \{1,2,3,4\}, \quad B = \{3,4,5,6\}, \quad C = \{2,4,6,8\}, \\ P(A) &= P(B) = P(C) = 1/2, \\ P(A \cap B) &= P(\{3,4\}) = 1/4 = P(A) P(B), \\ P(A \cap C) &= P(\{2,4\}) = 1/4 = P(A) P(C), \\ P(B \cap C) &= P(\{4,6\}) = 1/4 = P(B) P(C), \\ P(A \cap B \cap C) &= P(4) = 1/8 = P(A) P(B) P(C) \end{aligned} \quad (25)$$

özelliklerine sahip A, B, C olayları birbirinden bağımsızdır.

Benzer biçimde, A, B, C, D gibi dört olayın birbirinden bağımsız olması için, her üç olayın birbirinden bağımsız olması, yani

$$\begin{aligned} P(A \cap B) &= P(A) P(B), \quad P(A \cap C) = P(A) P(C), \\ P(A \cap D) &= P(A) P(D), \quad P(B \cap C) = P(B) P(C), \\ P(B \cap D) &= P(B) P(D), \quad P(C \cap D) = P(C) P(D), \\ P(A \cap B \cap C) &= P(A) P(B) P(C), \\ P(A \cap B \cap D) &= P(A) P(B) P(D), \\ P(A \cap C \cap D) &= P(A) P(C) P(D), \\ P(B \cap C \cap D) &= P(B) P(C) P(D) \end{aligned} \quad (26)$$

eşitliklerinin sağlanması ve ayrıca, her üç olayın kesişiminin de dördüncüden bağımsız olması gerekir:

$$\begin{aligned} P(A \cap B \cap C \cap D) &= P(A \cap B \cap C) P(D) \\ &= P(A \cap B \cap D) P(C) \\ &= P(A \cap C \cap D) P(B) \\ &= P(B \cap C \cap D) P(A) \\ &= P(A) P(B) P(C) P(D) \end{aligned} \quad (27)$$

Genel olarak, n olayın birbirinden bağımsız olması için, gerek ve yeter koşul, her $k=2,3,\dots,n$ olay için, olayların kesişiminin olasılığının, olayların olasılıklarının çarpımına eşit olmasıdır. n olay için sağlanması gereken eşitlik sayısı n 'ye üstel bağımlı olarak artmakta, $2^n - (n+1)$ olmaktadır [2]. Öte yandan, birbirinden bağımsız n olay üzerinde yapılan kimi küme işlemleri bağımsızlığı korumaktadır [13]:

Teorem: A_1, A_2, \dots, A_n , birbirinden bağımsız n olay olsun. B_i 'nin rasgele A_i ya da A_i' seçilmesiyle oluşturulan B_1, B_2, \dots, B_n olayları da birbirinden bağımsızdır. Ayrıca, $\{B_1, B_2, \dots, B_n\}$ olaylar kümesinin birbiriyle kesişmeyen kimi alt kümelerinin her birinin içindeki olayların ya tümünün bileşimi ya da tümünün kesişimi alınarak elde edilen olaylar da birbirinden bağımsızdır.

6 BAĞIMSIZ KAYNAKLAR

Bir kaynağın çıktısı, birbirinden bağımsız, birden çok sayıda özelliğın bileşkesi ise, bu kaynak, bağımsız özelliklerden her birini birisinin ürettiği, birbirinden bağımsız, paralel çalışan kaynaklar olarak da modellenebilir.

Örneğin, bir kaynağın art arda ürettiği n çıktı, kaynak durağan ve belleksiz varsayıldığı için, birbirinden bağımsızdır. Dolayısıyla, art arda n çıktıyı çıktı kabul eden bir kaynak, birbirinden bağımsız, paralel çalışan n kaynağın çıktılarını çıktı kabul eden bir kaynak olarak da düşünülebilir [2] (§3, Yinelenen Deneyler, 'Repeated Trials').

Örneğin, art arda iki kez atılan paranın çıktılarını çıktı kabul eden ve dört ögeli örnek uzayı $\{YY, YT, TY, TT\}$ olan Kaynak-2, örnek uzayları

$$\{Y, T\} \quad (28)$$

ve temel olaylarının olasılığı

$$P(Y) = p, \quad P(T) = q, \quad p + q = 1 \quad (29)$$

olan, bağımsız, paralel çalışan **iki kaynağın bileşkesi** olarak düşünülebilir. Bu durumda, $O_5 = \{YY, YT\}$, birinci kaynağın Y üretmesine, tümleyenini $O_5' = O_{10} = \{TY, TT\}$, birinci kaynağın T üretmesine; $O_6 = \{YY, TY\}$, ikinci kaynağın Y üretmesine, tümleyenini $O_6' = O_9 = \{YT, TT\}$, ikinci kaynağın T üretmesine karşı düşer. Dolayısıyla,

$$\begin{aligned} P(O_5) &= P(O_6) = P(Y) = p, \\ P(O_{10}) &= P(O_9) = P(T) = q \end{aligned} \quad (30)$$

$$\begin{aligned} P(A_1 | B_1) + P(A_2 | B_1) &= 1, \\ P(A_1 | B_2) + P(A_2 | B_2) &= 1, \\ P(A_1 | B_3) + P(A_2 | B_3) &= 1 \end{aligned} \quad (50)$$

bağıntıları da geçerlidir.

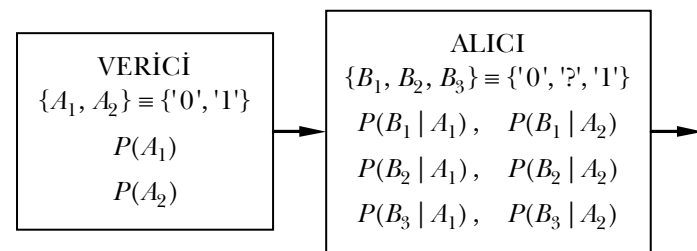
Yukarıda, $P(B_1)$, $P(B_2)$, $P(B_3)$ bulunurken kullanılan (42) bağıntısı

$$P(B_j) = \sum_{k=1}^n P(B_j | A_k) P(A_k), \quad (51)$$

toplamlı olasılık teoremi olarak bilinir [2], [7]. Bu bağıntı, $P(A_i | B_j)$ koşullu olasılıkları bulunurken kullanılan (44) bağıntısında yerine konulduğunda da, ünlü **Bayes bağıntısı** elde edilir [2], [7]:

$$P(A_i | B_j) = \frac{P(B_j | A_i) P(A_i)}{\sum_{k=1}^n P(B_j | A_k) P(A_k)}. \quad (52)$$

İletişim sisteminin Şekil 1a'daki verici olasılık modeli, vericiyi modelleyen bağımsız bir kaynak ve onun çıkışına bağlı, alıcıyı modelleyen bir bağımlı kaynakla da modellenabilir (Şekil 2). Bu modelde, verici kaynağı, $P(A_1)$ olasılıkla A_1 , $P(A_2)$ olasılıkla A_2 üretmektedir. Verici kaynağı A_1 ürettiğinde, alıcı kaynağı, $P(B_1 | A_1)$ olasılıkla B_1 , $P(B_2 | A_1)$ olasılıkla B_2 ve $P(B_3 | A_1)$ olasılıkla B_3 üretmektedir. Verici kaynağı A_2 ürettiğinde ise, alıcı kaynağı, $P(B_1 | A_2)$ olasılıkla B_1 , $P(B_2 | A_2)$ olasılıkla B_2 ve $P(B_3 | A_2)$ olasılıkla B_3 üretmektedir. Şekil 1b'deki alıcı olasılık modeli için aynı tip modelleme, olanaksızdır; çünkü, olasılık modelindeki, kolay anlaşılabilir diye konulan ters yönlü oklar nedenselliğe aykırı düşmezken, kaynaklar arasında, nedenselliğe aykırı yönde (veri akışının tersine, alıcıdan vericiye doğru) ok koymak yanlış olur.



Şekil 2. Şekil 1a'daki verici olasılık modelinin, birbirine bağlı iki kaynakla modellenmesi.

İletişim sistemi, kanal çok gürültülü olduğunda da çalışıyor olsun. Öyle ki, iletişim hattı koptuğunda bile, alıcı, iletişimin sürdürdüğünü sanarak, B_1 , B_2 ve B_3 üretmeyi sürdürsün. Bu durumda, verici A_1 de gönderse, A_2 de

gönderse, alıcı, değişmeyen olasılıklarla, B_1 , B_2 ve B_3 üretmeyi sürdürür; yani,

$$P(B_j | A_1) = P(B_j | A_2), \quad j = 1, 2, 3 \quad (53)$$

bağıntıları geçerli olur. Dolayısıyla,

$$\begin{aligned} P(B_j) &= P(B_j | A_1) P(A_1) + P(B_j | A_2) P(A_2) \\ &= P(B_j | A_1) (P(A_1) + P(A_2)) \\ &= P(B_j | A_1), \quad j = 1, 2, 3 \end{aligned} \quad (54)$$

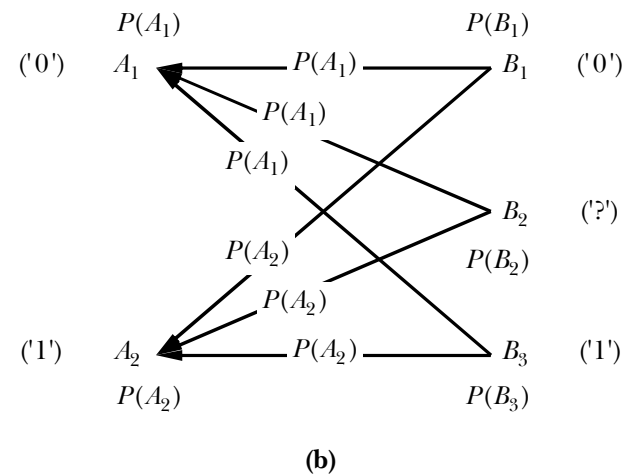
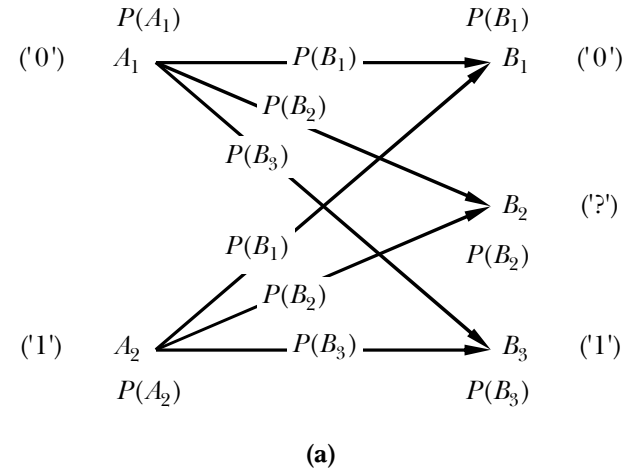
olur. Yani,

$$P(B_j | A_1) = P(B_j | A_2) = P(B_j), \quad j = 1, 2, 3 \quad (55)$$

bulunur (Şekil 3a). Dolayısıyla,

$$\begin{aligned} P(A_1 | B_j) &= \frac{P(B_j | A_1) P(A_1)}{P(B_j)} = P(A_1), \quad j = 1, 2, 3 \\ P(A_2 | B_j) &= \frac{P(B_j | A_2) P(A_2)}{P(B_j)} = P(A_2), \quad j = 1, 2, 3 \end{aligned} \quad (56)$$

olur. Yani,



Şekil 3. Şekil 1'deki iletişim sisteminin iletişim hattı koptuğunda, (a) verici olasılık modeli, (b) alıcı olasılık modeli.

$$P(A_i | B_1) = P(A_i | B_2) = P(A_i | B_3) = P(A_i), \quad i = 1, 2 \quad (57)$$

bulunur (Şekil 3b)). Özetle, iletişim hattı koptuğunda,

$$\begin{aligned} P(B_j | A_i) &= P(B_j | A_{i+1}) = P(B_j), \\ P(A_i | B_j) &= P(A_i | B_{j+1}) = P(A_i) \end{aligned} \quad (58)$$

olur. Dolayısıyla,

$$\begin{aligned} P(A_i \cap B_j) &= P(A_i | B_j) P(B_j) \\ &= P(B_j | A_i) P(A_i) \\ &= P(A_i) P(B_j) \end{aligned} \quad (59)$$

bulunur. Bu da, beklenildiği gibi, iletişim hattı koptuğunda, verici ile alıcının birbirinden bağımsız çalışan iki kaynağa dönüştüğünü gösterir.

8 DENEYSEL YAKLAŞIM

Rasgele olayların olasılıkları, von Mises'in deneysel yaklaşımı (§1) kullanılarak, **benzetim programı**yla kestirilebilir. Bu yolla, hem ulaşılan analitik sonuçlar doğrulanabilir, hem de analitik çözümü güç ya da olanaksız olasılık değerleri istenildiği kadar küçük yanılma ile bulunabilir. Bunun için, öncelikle, rasgele davranan sistemin kaynaklarla modellenmesi, sonra da, [0,1] aralığında rasgele sayı üretebilen *C*, *Mathematica*, *Maple* gibi bir programlama diliyle kaynakların, dolayısıyla, tüm modelin benzetimini yapmak gerekir. Bu benzetim programı n kez çalıştırılarak, olasılığı bulunmak istenilen A olayının gerçekleşme sayısı n_A belirlenir. Bulunan bu sayının n 'ye oranı, n_A/n , A olayının gerçekleşme olasılığı $P(A)$ 'nın yaklaşık bir değerini verir ve n büyüdükçe, yanılmanın standart sapması küçülür. Benzer biçimde, B olayının gerçekleşme sayısı n_B , A ile B olaylarının birlikte gerçekleşme sayısı $n_{A \cap B}$, A ile B olaylarından en az birisinin gerçekleşme sayısı $n_{A \cup B}$ belirlenerek, $n_{A \cap B}/n$ ile $P(A \cap B)$ olasılığının, $n_{A \cup B}/n$ ile $P(A \cup B)$ olasılığının, $n_{A \cap B}/n_B$ ile $P(A | B)$ koşullu olasılığının yaklaşık değerleri bulunabilir.

Örnek uzayı ve örnek uzayındaki öğelerin olasılıkları bilinen bir kaynağın benzetim programını yazmak çok kolaydır. Öncelikle, [0,1] aralığında, her öğeye, olasılığı genişliğinde bir yer ayrılır. Kaynağın her çıktısı için, [0,1] aralığında bir rasgele sayı üretilir. Bu sayı, hangi öğenin bölgesine düşüyorsa, kaynak tarafından o öğenin üretildiğine karar verilir.

Örneğin, olasılık modeli Şekil 1'de, kaynak modeli Şekil 2'de verilen iletişim sistemin tanımlayan olasılıklardan yalnızca

$$\begin{aligned} P(A_1) &= 0,6 & P(A_2) &= 0,4 \\ P(B_1 | A_1) &= 0,7 & P(B_2 | A_1) &= 0,1 & P(B_3 | A_1) &= 0,2 \\ P(B_1 | A_2) &= 0,3 & P(B_2 | A_2) &= 0,2 & P(B_3 | A_2) &= 0,5 \end{aligned}$$

biliniyor olsun. Bu değerlerden, (12), (42), (10) ve kesişen iki olayın bileşimi olan olayın olasılığını veren bağıntı (§3) kullanılarak hesaplanabilen diğer olasılık değerleri, yani

$$\begin{aligned} P(A_1 \cap B_1) &= 0,42 & P(A_2 \cap B_1) &= 0,12 \\ P(A_1 \cap B_2) &= 0,06 & P(A_2 \cap B_2) &= 0,08 \\ P(A_1 \cap B_3) &= 0,12 & P(A_2 \cap B_3) &= 0,20 \\ P(B_1) &= 0,54 & P(B_2) &= 0,14 & P(B_3) &= 0,32 \\ P(A_1 | B_1) &= 0,778 & P(A_2 | B_1) &= 0,222 \\ P(A_1 | B_2) &= 0,429 & P(A_2 | B_2) &= 0,571 \\ P(A_1 | B_3) &= 0,375 & P(A_2 | B_3) &= 0,625 \\ P(A_1 \cup B_1) &= 0,72 & P(A_2 \cup B_1) &= 0,82 \\ P(A_1 \cup B_2) &= 0,68 & P(A_2 \cup B_2) &= 0,46 \\ P(A_1 \cup B_3) &= 0,80 & P(A_2 \cup B_3) &= 0,52 \end{aligned} ;$$

[0,1] arası rasgele sayı üretebilen bir benzetim programının yardımıyla kestirilebilir:

• İlk değerleri ata:

$$\begin{aligned} n &= n_{A_1} = n_{A_2} = n_{B_1} = n_{B_2} = n_{B_3} = 0 \\ n_{A_1 \cap B_1} &= n_{A_2 \cap B_1} = n_{A_1 \cap B_2} = n_{A_2 \cap B_2} = n_{A_1 \cap B_3} = n_{A_2 \cap B_3} = 0 \\ n_{A_1 \cup B_1} &= n_{A_2 \cup B_1} = n_{A_1 \cup B_2} = n_{A_2 \cup B_2} = n_{A_1 \cup B_3} = n_{A_2 \cup B_3} = 0 \end{aligned}$$

• Üretilen her (r_1, r_2) rasgele sayı çifti için şu işlemleri yap:

$$\begin{aligned} a_1 &= a_2 = b_1 = b_2 = b_3 = 0 \\ n &++ \\ \text{eğer } r_1 < 0,6 &: a_1 ++, \\ &\text{eğer } r_2 < 0,7 &: b_1 ++ \\ \text{eğer } 0,7 \leq r_2 < 0,8 &: b_2 ++ \\ \text{eğer } r_2 \geq 0,8 &: b_3 ++ \\ \text{eğer } r_1 \geq 0,6 &: a_2 ++, \\ &\text{eğer } r_2 < 0,3 &: b_1 ++ \\ \text{eğer } 0,3 \leq r_2 < 0,5 &: b_2 ++ \\ \text{eğer } r_2 \geq 0,5 &: b_3 ++ \end{aligned}$$

$i = 1, 2$ ve $j = 1, 2, 3$ için,

$$\text{eğer } a_i > 0, \quad n_{A_i} ++$$

$$\text{eğer } b_j > 0, \quad n_{B_j} ++$$

$$\text{eğer } a_i b_j > 0, \quad n_{A_i \cap B_j}$$

$$\text{eğer } a_i + b_j > 0, \quad n_{A_i \cup B_j}$$

• $n_{A_i}, n_{B_j}, n_{A_i \cap B_j}, n_{A_i \cup B_j} \geq N$ olduğunda,

$$P(A_i) = \frac{n_{A_i}}{n} \quad P(B_j) = \frac{n_{B_j}}{n}$$

$$P(A_i \cap B_j) = \frac{n_{A_i \cap B_j}}{n} \quad P(A_i \cup B_j) = \frac{n_{A_i \cup B_j}}{n}$$

$$P(A_i | B_j) = \frac{n_{A_i \cap B_j}}{n_{B_j}} \quad P(B_j | A_i) = \frac{n_{A_i \cap B_j}}{n_{A_i}}$$

değerlerini hesapla.

Benzetim programıyla kestirilen olasılık değerlerindeki yanılma oranının beklenen değeri, çoğu olasılık değeri için, $1/\sqrt{\text{gözlenme sayısı}}$ 'ndan küçüktür. Örneğin, *Mathematica* programlama dilinde yazılan bir benzetim programıyla $N=10000$ seçilerek kestirilen olasılık değerleri ve bu değerleri bulurken yapılan gözlem sayıları, programın sıradan bir çalışması sonunda, şöyle bulunmuştur:

$$\begin{aligned} P(A_1) &= 0,600 & P(A_2) &= 0,400 \\ P(B_1 | A_1) &= 0,700 & P(B_2 | A_1) &= 0,0992 & P(B_3 | A_1) &= 0,201 \\ P(B_1 | A_2) &= 0,297 & P(B_2 | A_2) &= 0,201 & P(B_3 | A_2) &= 0,502 \\ P(A_1 \cap B_1) &= 0,420 & P(A_2 \cap B_1) &= 0,119 \\ P(A_1 \cap B_2) &= 0,0595 & P(A_2 \cap B_2) &= 0,0807 \\ P(A_1 \cap B_3) &= 0,120 & P(A_2 \cap B_3) &= 0,201 \\ P(B_1) &= 0,539 & P(B_2) &= 0,140 & P(B_3) &= 0,321 \\ P(A_1 | B_1) &= 0,779 & P(A_2 | B_1) &= 0,221 \\ P(A_1 | B_2) &= 0,424 & P(A_2 | B_2) &= 0,576 \\ P(A_1 | B_3) &= 0,375 & P(A_2 | B_3) &= 0,625 \\ P(A_1 \cup B_1) &= 0,718 & P(A_2 \cup B_1) &= 0,820 \\ P(A_1 \cup B_2) &= 0,680 & P(A_2 \cup B_2) &= 0,460 \\ P(A_1 \cup B_3) &= 0,801 & P(A_2 \cup B_3) &= 0,521 \\ n &= 168186 & n_{A_1} &= 100843 & n_{A_2} &= 67343 \\ n_{B_1} &= 90594 & n_{B_2} &= 23566 & n_{B_3} &= 54026 \\ n_{A_1 \cap B_1} &= 70607 & n_{A_1 \cap B_2} &= 10000 & n_{A_1 \cap B_3} &= 20236 \\ n_{A_2 \cap B_1} &= 19987 & n_{A_2 \cap B_2} &= 13566 & n_{A_2 \cap B_3} &= 33790 \\ n_{A_1 \cup B_1} &= 120830 & n_{A_1 \cup B_2} &= 114409 & n_{A_1 \cup B_3} &= 134633 \\ n_{A_2 \cup B_1} &= 137950 & n_{A_2 \cup B_2} &= 77343 & n_{A_2 \cup B_3} &= 87579 \end{aligned}$$

Programın, değişik rasgele sayılarla her çalıştırılışında, değişik olması olası, ancak, beklenen değerlere yakın sonuçlar vereceği açıktır.

9 SONUÇ

Bu yazı hazırlanırken, kimi zaman, alışılmışın dışına çıkmıştı. Özellikle, olasılık kuramının gölgesinde doğup gelişen, bulunduğumuz çağa adını veren **bilgi kuramındaki** kimi kavram ve örneklerden yararlandı.

Deneysel bilimcilerin, zar atma, yazı tura atma gibi, rasgele çıktısı olan deneylerden esinlenerek tanımladıkları, kapsamı dar olan “deney” yerine, bilgi kuramındaki “**kaynak**” kullanıldı (§2).

Olasılığın tanımı için, matematikçilerin verdiği, “olayların ölçümü” [8] (sf. 46); deneysel bilimcilerin verdiği, “olaylara atama” [2] (sf. 26) ya da “olaylar üzerinde tanımlanan küme fonksiyonu” [7] (sf. 22) yerine, Togneri ve deSilva’nın verdiği [9] (sf. 3), örnek uzayı üzerinde tanımlanan “**dağılım fonksiyonu**” benimsendi (§3).

Çoğunlukla tanım olarak verilen **koşullu olasılık** bağıntısı §4’te, **bağımsız olayların** bağıntıları da §5’te, temel kavramlardan yola çıkılarak elde edildi.

Deneysel bilimcilerin, “bağımsız deneyler” ya da “yinelene deneyler” başlığı altında inceledikleri konular, “**bağımsız kaynaklar**” başlığı altında §6’da, “toplam olasılık teoremi” ve “Bayes bağıntısı” kapsamında inceledikleri “bağımlı deneyler” konusu da “**bağımlı kaynaklar**” başlığı altında §7’de incelendi.

Bilgisayarların ortaya çıkmasıyla deneysel bilime dönüşen olasılık kuramında, **benzetim programları** yazılarak, hem kuramsal olarak bilinen bağıntıların sınanabileceği, hem de bulunması güç olasılık değerlerinin kestirilebileceği vurgulandı (§8).

Bu yazının, dergimizin ileriki bir sayısında yayımlanacak olan ikinci bölümünde, olasılık kuramında sıkça düşülen yanlışlar tartışmaya açılarak, bu yazıda verilen kavramların pekiştirilmesine çalışılacaktır.

TEŞEKKÜR

Bu yazının doğru ve kolay anlaşılabilir olması için özen gösteren Sayın Dr. Levent Balamir Tavacıoğlu’na teşekkür ederim.

KAYNAKÇA

- [1] C. N. Geçkinli, “Rasgelelik (Rastlantısallık) kavramına genel bir bakış”, *UEKAE Dergisi*, sa. 1, sf. 97–103, Eylül-Aralık 2009.
- [2] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York: McGraw-Hill, 1965.
- [3] G. E. Christianson, *Isaac Newton - Bilimsel Devrim*, 5. basım. Ankara: TÜBİTAK, 2008, sf. 34–37.
- [4] J. Bernstein, *Albert Einstein - Fizik’in Sınırları*. Ankara: TÜBİTAK, 2006, sf. 115–122.
- [5] M. Erickson and A. Vazzana, *Introduction to Number Theory*. Boca Raton, FL: Chapman & Hall/CRC, 2008.
- [6] J. P. King, *Matematik Sanatı*. Ank McGraw-Hill, 1965.ara: TÜBİTAK, 1997, sf. 79–82.
- [7] T. K. Chandra and D. Chatterjee, *A First Course in Probability*. New Delhi, India: Narosa Publishing House, 2001.
- [8] M. Capinski and E. Kopp, *Measure, Integral and Probability*, 2nd ed. London: Springer-Verlag, 2004.
- [9] R. Togneri and C. J. S. deSilva, *Fundamentals of Information Theory and Coding Design*. Boca Raton, FL: Chapman & Hall/CRC, 2003.
- [10] TÜİK, “Boşanma İstatistikleri”: <http://www.tuik.gov.tr/demografiapp/bosanma.zul>
- [11] TÜİK, *Küresel Yetişkin Tütuin Araştırması - 2008*. Ankara: TÜİK, 2009: http://www.tuik.gov.tr/Kitap.do?metod=KitapDetay&K_T_ID=1&KITAP_ID=215.
- [12] P. E. Pfeiffer, *Concepts of Probability Theory*. New York: McGraw-Hill, 1965, p. 44.
- [13] M. Woodroffe, *Probability with Applications*. Tokyo: McGraw-Hill Kogakusha, 1975, p. 74.
- [14] A. Juels, M. Jakobsson, E. Shriver and B. K. Hillyer, “How to turn loaded dice into fair coins,” *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 911–921, May 2000.

Anten Ölçüm Sistemleri ve Hata Analizleri – I: Düzlemsel Yakın Alan Ölçüm Sistemi

Bahattin TÜRETKEN, Umut BULUŞ, Ömer YILMAZ

Özet - Anten ölçümleri, kapalı veya açık ölçüm alanlarında (iç veya dış ortamlarda, tam yansımaz odalarda veya açık saha test alanlarında) yapılır. Uzak alan ve yakın alan ölçüm sistemleri ile antenin ışınma diyagramı elde edilir. Bu çalışmada, ölçülmek istenen anten parametreleri ile uzak ve yakın alan ölçüm sistemleri hakkında bilgi verilecek, düzlemsel yakın alan ölçüm sistemi ile hata çözümlenmeleri (analizleri), ölçümlerle desteklenerek sunulacaktır.

Anahtar Sözcükler - Anten ölçümü, uzak alan ölçüm sistemi, yakın alan ölçüm sistemleri, düzlemsel yakın alan ölçüm sistemi, hata çözümlenmeleri (analizleri).

1 GİRİŞ

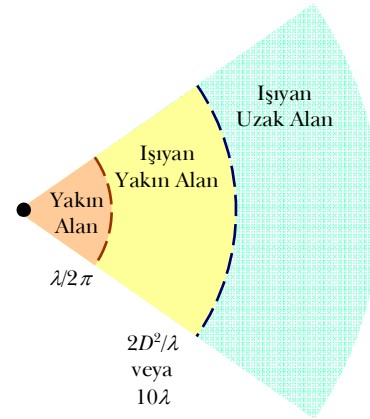
Elektromanyetik ve anten problemlerinin çözümünde üç değişik yöntem bulunmaktadır. Bunlar analitik yöntemler, benzetim ve ölçüm yöntemleridir. Analitik çözümü mevcut olmayan ve benzetim yöntemlerinin imkân verdiği ölçüde çözümlenebilen (analiz edilebilen) problemlere önerilen çözümler, ölçümler ile desteklenmelidir. İyi tanımlanmış bir yöntem ve hassas ölçüm alt yapısıyla desteklenmiş bir düzenek ile yapılan ölçümler gerçeğe en yakın yaklaşımı verir. Bundan dolayı, çoğu zaman analitik olarak tam çözümü bulunmayan anten problemlerinde ölçümler hayati önem taşımaktadır. Anten ölçümleri, uzun aşamalı ve oldukça maliyetli olup, anten tasarım sürecinin önemli bir ayağını oluşturur.

Bu çalışmada anten parametreleri, ölçüm yöntemleri, düzlemsel yakın alan ölçüm sistemi ve bazı ölçüm hataları anlatılacaktır.

2 ANTEN IŞINMA BÖLGELERİ

Antenler en genel tanımıyla, elektriksel akım ve gerilimi elektromanyetik enerjiye dönüştüren veya bunun tersini yapabilen, bu enerjiyi belirli bir frekans aralığında istenilen uzaysal dağılıma yönlendiren, düşük geriye dönüş kaybına sahip elemanlardır. **E**, elektrik alanı, **H**, magnetik alanı göstermek üzere, bir antenden ışıyan alan karmaşık poynting vektörü $\mathbf{E} \times \mathbf{H}^*$ ile ifade edilir. Bu ifade antenin yakınında sanal (imajiner) bir değere sahiptir ve antenden uzaklaştıkça hızlı bir şekilde azalır [1]. Bu durum anten etrafında 3 değişik alan bölgesinin oluşmasına sebep olur.

Reaktif yakın alan, Poynting vektörünün reaktif olduğu (ışınma yapmayan) bölge olup, kaynağın hemen yakınında başlar ve $\lambda/2\pi$ 'ye kadar devam eder. Burada alanın bütün bileşenleri $1/r$ 'den oldukça hızlı olarak azalır. Reaktif yakın alanın hemen ötesinde "ışıyan yakın alan" başlar ve D antenin en büyük boyutu olmak üzere $2D^2/\lambda$ 'ya kadar devam eder. Bu bölge ise kendi içinde iki ana bölgeye ayrılır: Birisi $D^2/4\lambda$ 'ya kadar olan bölge olup, burada alan bileşenleri $1/r$ 'den oldukça hızlı azalır ve r 'ye oldukça bağlıdır. Diğer bölge ise $D^2/4\lambda < r < 2D^2/\lambda$ koşulunun sağlandığı bölgedir; alan bileşenleri $1/r$ oranında azalır ve r 'ye bağlıdır.



Şekil 1. Işınma bölgeleri.

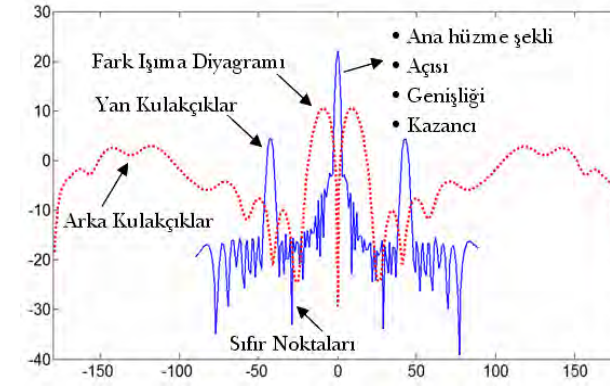
Burada ışınma diyagramı, antenin açıklığındaki alan dağılımının Fourier dönüşümü ile bulunur. Faz hatası $22,5^\circ$ olup, $r \rightarrow \infty$ oldukça sıfır değerini alır. Bu bölge "Fresnel" bölgesi diye adlandırılır. Işıyan yakın alanın hemen ötesinde "uzak alan" başlar (Şekil 1). Burada Poynting vektörü gerçel (real) bir değer alır ve iki bileşeni bulunur. Alan $1/r$ ile azalır ve ışınma diyagramı r 'den bağımsızdır. Bu bölgedeki ışıyan alan da $22,5^\circ$ 'den daha az bir hatayla anten açıklığındaki alan dağılımının Fourier dönüşümüyle hesaplanır [2].

3 ANTEN PARAMETRELERİ VE ÖLÇÜMLER

3.1 Anten Parametreleri

Antenin hangi parametrelerini ölçeriz? Bir antende, giriş kapısı (port), (geriye dönüş kaybı, duran dalga oranı (VSWR),

'Voltage Standing Wave Ratio'), S parametreleri), ışınma diyagramı, (ana, yan ve arka kulakçıklar, sıfır noktaları, fark diyagramı, hüzmeye şekli, hüzmeye genişliği, verimlilik, yönlendiricilik/kazanç, ana hüzmeye bakış yönü) ve polarizasyon (doğrusal, dairesel ve çapraz/aynı) olmak üzere üç ana ölçüm gerçekleştirilir (Şekil 2).

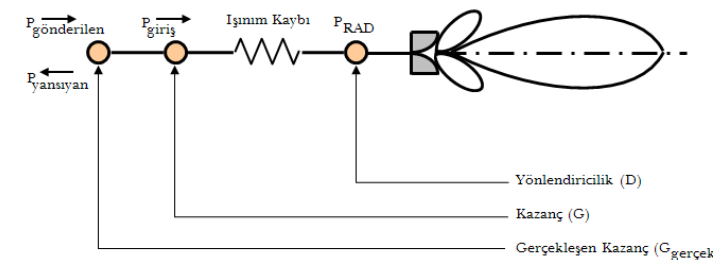


Şekil 2. Işınma diyagramına ilişkin parametreler.

Bir antenin polarizasyonu anten tarafından yayılan dalganın polarizasyonunu ifade eder. Polarizasyon, genel olarak doğrusal, dairesel ve eliptik olmak üzere üçe ayrılır.

Giriş empedansı, antenin giriş ucundaki gerilim ile akım arasındaki oranı belirler ve eğer antende iyi empedans uyumluluğu söz konusu değilse, duran dalgalar oluşur [2]

Yönlendiricilik, belirli bir yöndeki ışınım yoğunluğunun, tüm yönlerde yayılan ortalama ışınım yoğunluğuna oranıdır. (Ortalama ışınım yoğunluğu, toplam gücün 4π 'ye bölünmesine eşittir.) Eğer bir yön belirtilmemişse, yönlendiricilik en yüksek ışınım yoğunluğu değeri olarak verilir. Diğer bir deyişle, yönlendiricilik bir antenin belirli bir yöndeki ışınma şiddetinin, izotropik bir kaynağın aynı ışınma gücü için oluşturduğu ışınma şiddetine oranı olarak tanımlanır.



Şekil 3. Anten yönlendiriciliği, kazanç ve gerçekleşen kazanç gösterimi.

- D : Yönlendiricilik [-]
- D_0 : Maksimum Yönlendiricilik [-]
- U : Işınım Yoğunluğu [W/sr]

- U_{max} : Maksimum Işınım Yoğunluğu [W/sr]
- U_0 : İzotropik Kaynağın Işınım Yoğunluğu [W/sr]
- P_{rad} : Toplam Işıyan Güç [W]

olmak üzere yönlülüğün matematiksel ifadesi şu şekildedir:

$$D = \frac{U}{U_0} = \frac{4\pi U}{P_{rad}} \quad (1)$$

Eğer bir yön belirtilmemişse, yönlendiriciliğin en yüksek olduğu değer ifade edilir:

$$D_{max} = D_0 = \frac{U_{max}}{U_0} = \frac{4\pi U_{max}}{P_{rad}} \quad (2)$$

Kazanç, antenin yönlendiriciliğini göstermesinin yanı sıra ışınım verimliliğini de dikkate alır. Kazanç en genel anlamda yönlendiriciliğin ışınım verimi (e_{rad}) ile çarpımına eşittir:

$$G = e_{rad} D \quad (3)$$

Burada ışınım verimi olarak ifade edilen değer, antene gelmiş olan gücün ne kadarının ışıdığı gösterir. Zira antene gelen gücün bir kısmı ısıya dönüşür ve kayba neden olur.

Gerçekleşen kazanç ise, antenin ışınım veriminin yanında empedans uyumsuzluğundan kaynaklanan kaybı da hesaba dahil eder. Böylece, e_r uyumsuzluk verimi olmak üzere, gerçekleşen kazanç

$$G_{gerçek} = e_r e_{rad} D \quad (4)$$

olarak ifade edilir [1].

Işınma diyagramı bir antenin uzaysal koordinatlarda (θ, ϕ) ışınma özelliklerini gösterir. Işınma diyagramı, aksi belirtilmedikçe antenin uzak alandaki ışınmasını gösterir. Işınma diyagramında ana lob, yan loblar, arka lob, sıfır noktaları, hüzmeye genişliği gibi parametreler görülür (Şekil 3).

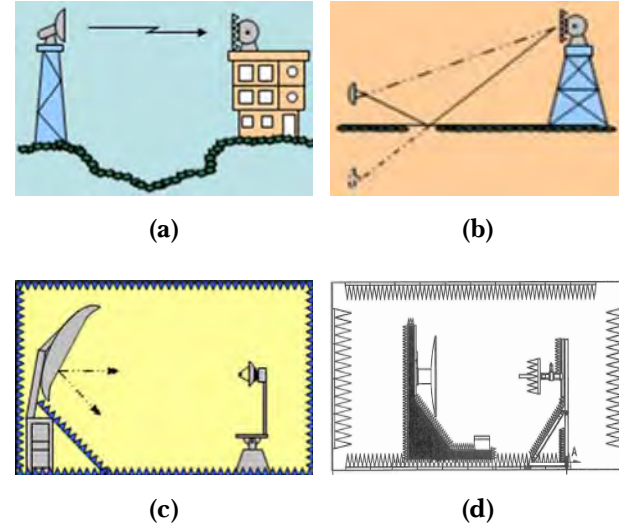
Anten gürültü sıcaklığı, istenilen frekanstaki anten tarafından alınan gürültü gücünü tanımlayan bir ölçüdür. Anten gürültü gücü, genel olarak $KT_a B$ olarak ifade edilir, burada K Boltzman değişmezini, T_a anten gürültü sıcaklığını B ise sistemin bant genişliği gösterir. G kazanç, T alıcı sistemin Kelvin cinsinden gürültü gücünü göstermek üzere G/T oranı da önemli bir parametre olarak karşımıza çıkar ve anten tarafından alınan işaret gürültü oranıyla orantılı bir değerdir [2].

Önemli anten parametrelerinden biri de yarım güç hüzmeye genişliğidir. Yarım güç hüzmeye genişliği, antenin ışınma diyagramının maksimum olduğu noktadaki güç düzeyinin yarısına (3 dB aşağısına) düşüldüğü noktalar arasındaki açıdır.

3.2 Anten Ölçümleri

Antenlerin ölçüldüğü yerlere anten ölçüm alanı (*antenna ranges*) denir. Bunlar ikiye ayrılır: kapalı (iç) ortamlar (tam yansımaz odalar), açık (dış) ortamlar (açık saha test alanları).

Anten ışınma diyagramı ölçümleri ise, ölçüm noktası ile anten arasındaki uzaklığa göre, “uzak alan” ve “yakın alan” olmak üzere ikiye ayrılır [3]. Yakın alan ölçümleri, antenin yakın alanında ölçülen genlik, faz ve polarizasyon verisinin analitik teknikler kullanılarak uzak alan verisine çevrilmesiyle olur. Bu ölçümler iyi tanımlanmış bir yüzeyde (düzlemsel, silindirik, küresel, eliptik silindir, koni vb.), belirli adımlarla elektrik alanın teğetsel bileşenin genlik ve fazının ölçülmesidir. Bu veri düzlemsel, silindirik veya küresel yüzeyin açılal spektrumunun hesaplanmasında kullanılır. Buna “modal açılım” adı verilir. Uzak alan ölçümleri ise, antenin uzak alan koşulunun sağlandığı bir ortamda genlik diyagramının çıkarılmasıdır. Ayrıca, yaklaşık eş dağılımlı (*uniform*) düzlemsel dalgaların elde edildiği Toplu Menzil Ölçüm Sistemleri de (*Compact Antenna Test Range*) antenlerin ışınma diyagramlarının ölçüldüğü diğer bir ortamdır (Şekil 4). Her iki ortamda da yakın alandan uzak alana dönüşüme gerek olmadan ışınma diyagramı doğrudan elde edilmektedir [2].



Şekil 4. Anten ölçüm sahaları: (a) dış saha, (b) yer ortamı, (c) yansımaz toplu menzil alanı ve (d) yakın alan ölçüm sistemi.

Ölçümü yapılacak antenin boyutları, frekansı, ışınma diyagramı, ölçülmesi gereken kritik anten parametrelerine göre farklı ölçüm sistemleri kullanılabilir. Ölçüm sistemlerinin, sistem maliyeti, hız, karmaşıklık, frekans ve hassasiyet derecesine göre sınıflandırılmış bilgisi Tablo 1’de verilmiştir.

Tablo 1. Yakın Alan - Uzak Alan Ölçüm Sistemlerinin Karşılaştırılması

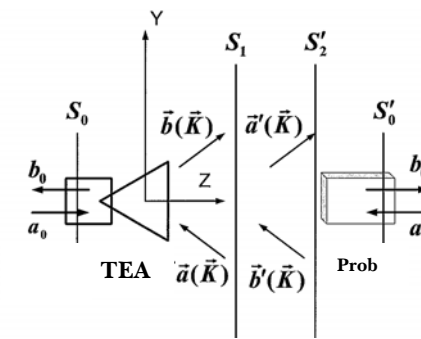
	Yakın Alan			Uzak Alan		
	Düzlemsel (Planar)	Silindirik (Cylindrical)	Küresel (Spherical)	Dış Ortam (Outdoor Range)	İç Ortam (Anechoic Chamber)	Toplu Menzil (Compact Range)
Yüksek Kazançlı Antenler	Mükemmel	İyi	İyi	Orta	Orta	Mükemmel
Düşük Kazançlı Antenler	Zayıf	İyi	İyi	Orta	İyi	Mükemmel
Yüksek Frekans	Mükemmel	Mükemmel	Mükemmel	Zayıf	Zayıf	Mükemmel
Düşük Frekans	Zayıf	Zayıf	İyi	İyi	Ortanın altı	Zayıf
Kazanç Ölçümü	Mükemmel	İyi	İyi	Mükemmel	İyi	Mükemmel
Yakın Yan Kulakçıklar	Mükemmel	Mükemmel	Mükemmel	İyi	Zayıf	Mükemmel
Uzak Yan Kulakçıklar	Yeterli (Orta)	Mükemmel	Mükemmel	İyi	Zayıf	İyi
Eksenel Oran (Axial Ratio)	Mükemmel	Mükemmel	Mükemmel	İyi	Zayıf	İyi
Çoklu Yansıma	İyi	İyi	İyi	Yeterli	Yeterli	İyi
Hava, Sıcaklık, Nem	Mükemmel	Mükemmel	Mükemmel	Zayıf	Mükemmel	Mükemmel
Güvenlik	Mükemmel	Mükemmel	Mükemmel	Zayıf	Mükemmel	Mükemmel
Sistem Maliyeti	Düşük	Makul	Makul	Yüksek	Makul	Çok yüksek
İşletme Maliyeti	Makul	Makul	Makul	Yüksek	Makul	Makul
Hız (Complete Measurements)	Mükemmel	İyi	Orta	Orta	Orta	Orta
Hız (Simple Cuts)	İyi	Orta	Orta	Orta	Orta	Orta
Karmaşıklık	Makul	Makul	Yüksek	Makul	Düşük	Yüksek
Mekanik Yüzey Ölçümü	Mükemmel	Yok	Yok	Yok	Yok	Yok
Anten Erişebilirliği	Mükemmel	Mükemmel	Mükemmel	İyi	İyi	Zayıf
Anten Hizalama	Kolay	Makul	Zor	Makul	Makul	Zor

4 YAKIN ALAN ÖLÇÜMLERİ – DÜZLEMSEL YAKIN ALAN ÖLÇÜM SİSTEMİ

Yakın alan testleri, ölçümü yapılan antene çok yakın bir yüzey üzerinde, alan örnekleri alınarak yapılır. Toplanan faz ve genlik verileri, alan değerlerinin toplandığı yüzeyin şekline göre farklı matematiksel dönüşümler ile işlenir ve uzak alan ışınma diyagramı çıkarılır. Yakın alan ölçüm sistemleri düzlemsel, silindirik ve küresel olmak üzere üç ana gruba ayrılmaktadır [3].

En yaygın olarak kullanılan düzlemsel yakın alan ölçüm yönteminde “Test Edilen Anten” (TEA) verici olarak kullanılır. Yaklaşık 3λ uzaklıktaki düzlemsel açıklıkta alıcı prob $0,25\lambda$ aralıklarla, tarama alanının tamamını tarayarak her adımdaki genlik ve faz bilgisini alıcıya ulaştırır. Bu işlem her iki polarizasyon için tekrar edilir. Alınan bu değerlerden açılal spektrum verisi elde edilir. Sonra probtan kaynaklanan hataların giderilmesi için prob kalibrasyon verisi ile birleştirilir ve elde edilen yeni spektrum verisinin Fourier dönüşümü alınarak uzak alan ifadesi elde edilir.

Düzlemsel yakın alan hesaplamaları ilk defa David Kerns tarafından ortaya konulan Saçılma Matrisi Kuramı’ndan (*Scattering Matrix Theory*) faydalanarak yapılmıştır. Bu



- O : TEA koordinat sistemi
- O' : Prob koordinat sistemi
- S_0 : TEA kapısı (port)
- S_0' : Prob kapısı
- a_0 : Karmaşık genlik (TEA kapısına gelen)
- b_0 : Karmaşık genlik (TEA kapısından giden)
- a_0' : Karmaşık genlik (Prob kapısına gelen)
- b_0' : Karmaşık genlik (Prob kapısından giden)
- $a(K)$: Karmaşık genlik (TEA kenar açıklığına gelen)
- $b(K)$: Karmaşık genlik (TEA kenar açıklığından giden)
- $a'(K)$: Karmaşık genlik (Prob kenar açıklığına gelen)
- $b'(K)$: Karmaşık genlik (Prob kenar açıklığından giden)
- F' : Empedans uyumsuzluğu faktörü
- $t_{10}(K)$: TEA'nın düzlemsel veri fonksiyonu
- $s_{02}'(\vec{K})$: Probu düzlemsel dalga alışı fonksiyonu
- $e^{iyd} e^{i(k_x x + k_y y)}$: Prob düzlemsel dönüştürme çarpanları

Şekil 5. Düzlemsel yakın alan ölçüm yöntemi ve ilgili parametreler.

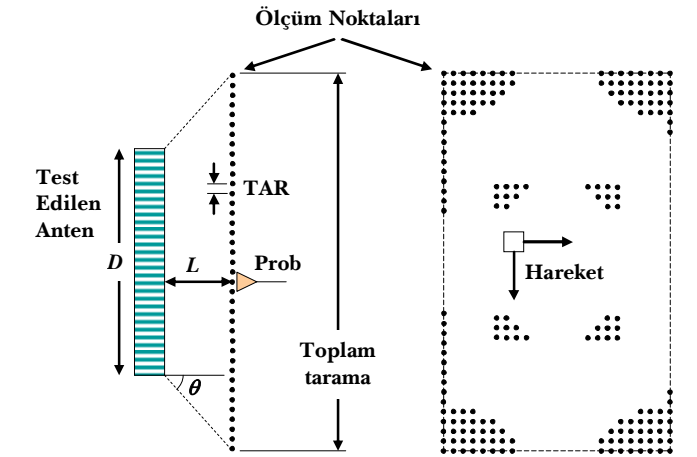
kurama göre antenin (TEA) ve probun verici, alıcı ve saçıcı özellikleri saçılma matrisi ile ifade edilebilir (Şekil 5) [4]. Çoklu yansımaların ihmal edildiği düzlemsel iletim eşitliği

$$b_0'(x, y, d) = F'a_0 \iint t_{10}'(\vec{K}) \cdot s_{02}'(\vec{K}) e^{iyd} e^{i(k_x x + k_y y)} dk_x dk_y \quad (5)$$

olup, bu eşitliğe prob ışınma diyagramı ve polarizasyonundan kaynaklanan düzeltme faktörlerinin eklenmesi gerekmektedir.

4.1 Ölçüm Alanı

Düzlemsel yakın alan ölçüm sisteminde çözümleme için toplanacak verinin ölçüldüğü açıklık, anten açıklığından daha büyük olmaktadır (Şekil 6). Ölçüm tarama alanı, anten boyutu, ilgili frekans, görülmek istenen arka lob konumları, oda boyutuna bağlıdır. D , tarama eksenindeki anten boyutu olmak üzere, tarama alanı şu şekilde hesaplanır: L antenden olan uzaklığı, θ tarama açısını göstermek üzere, ölçüm tarama alanı (*Scanning Area*, SA) $SA = D + 2L \tan \theta$ 'dir. Pratikte θ en fazla 75° ile sınırlıdır. L ise, $3\lambda \sim 4\lambda$ civarındadır.



Şekil 6. Düzlemsel yakın alan ölçüm sistemi tarama alanı.

Dolayısıyla düzlemsel yakın alan ölçüm sistemiyle bir antenin arka loblarının tamamını ölçmek mümkün değildir. Tüm açılardan ölçüm yapabilmek için küresel yakın alan ölçüm sistemleri ile küresel yakın alan yüzeyinde ölçüm alınır [5].

Ölçüm $\lambda/2$ 'den daha küçük aralıklarla (Tarama Aralığı, *TAR*) faz ve genlik değerleri alınarak yapılmaktadır. Bunun için teknik özellikleri uygun işaret üretici ve alıcı gerekmektedir. Testlerin birkaç saat sürdüğü düşünülürse, kararlılığa ve sıcaklığa duyarlılık daha çok önem taşır.

4.2 Yakın Alan Ölçüm Probu

Yakın alan ölçüm probunun sağlaması gereken bir takım özellikler bulunmaktadır. Mekanik sağlamlık, zamanla

değişmeyen anten kazancı ve yüksek bant genişliği probun en önemli özelliklerindedir. Probu ön tarafındaki yarım kürede "sıfır" (*null*) noktalarının bulunmaması istenilen diğer bir özelliktir. İstisnai olarak Grimm, sıfır noktalarının bulunmamasının istenmeyen işaretlerin yok edilmesi için kullanılabileceğini belirtmiştir [3]. Anten ölçümlerinde genellikle ana hüzmeye kadar yan hüzmeler de önem içermektedir. Bu durumda probun ana hüzmeye tarafından aldığı alan değeri, yan hüzmelerin bulunduğu taraftakinden daha büyük olduğu için istenilen yönde bir "sıfır"ı olan prob kullanılması daha uygundur. Bu sıfır sayesinde ana hüzmeye bastırılırken, yan lobtan gelen alan değeri almır. Böylece yan hüzmeler daha net görülebilir.

Prob, aynı zamanda, düşük saçılma kesitine ve yansıma katsayısına sahip olmalıdır. Probu konumundaki sapmalara karşı duyarlılığı azaltmak ve soğuruculardan gelen yansımalarla az etkilenmek için probun ön/arka oranının (*front-to-back ratio*) iyi olması gerekmektedir. Geniş hüzmeye genişliği probun sağlaması gereken diğer bir koşuldur. Yakın alan problemleri genelde silindirik dalga kılavuzu, dikdörtgen dalga kılavuzu, tırtıklı huni anten (*corrugated horn antenna*) veya piramit huni anten biçimindedir (*pyramidal horn antenna*) [6] (Şekil 7).



Şekil 7. ATAM Laboratuvarı'nda kullanılan bazı problar.

Probtan yayılan dalgaların bir kısmı antenin yüzeyinden yansıyarak proba ulaşır ve probun üzerinden yansıyarak tekrar antene döner. Bu durum ölçümde hataların olmasına neden olur; bu yüzden probun küçük boyutlu olması istenir. Prob genel olarak ölçümü yapılan antenden birkaç dalga boyu uzaklığa yerleştirilir. Böylece, probtan yayılan yansımalarla daha az etkilenilmiş olur. Yansımaların azaltılması için probun arkasına soğurucular yerleştirilmiştir. Şekil 8'de yansımalarla ve probun ön/arka oranından kaynaklanan saçılmalar gösterilmektedir.

4.3 Performans ve Hatalar

Yakın alan ölçümünün önemli avantajlarından biri, test edilen antenin hatalarını tanımlayabilme yeteneğidir. Bu durum, uzak alan ışınma diyagramının matematiksel olarak anten yüzeyindeki yakın alana dönüştürülmesiyle elde edilir.

Bu yöntem dizi antenlerde kullanılmakta ve dizi elemanlarından çalışmayanlar olduğunda, bunlar tespit edilebilmektedir.

Yakın alan ölçüm hataları, diğer mikrodalga ölçümlerinden çok daha fazla dikkat çekmiştir. (Hataların birçok kaynağı bulunabilir, ancak bunların her birinin etkilediği anten parametreleri bilindiğinde, ölçüm sırasında karşılaşılan hataların kaynakları saptanabilir).

4.3.1 Prob Konumlandırma Hatası

Antenin hizalanmasından kaynaklanan hata, antenin kazancının en yüksek olduğu noktanın kaymasına neden olur. Buna yönelme hatası (*boresighting error*) denir. Prob konum hataları, anten dizilerinde eleman konumu hatalarına benzerlik gösterir. Eğer hüzmeye (*beam*) antene dik ışıyor ise, sadece z yönünde hatalara yol açar; hüzmeye yönündeki hata bileşeni tahmin edilebilen bir faz hatası doğurur. Sıcaklık, kablo uzunluğu değişimi ve prob sarkması faz hatalarına neden olan diğer etkenlerdir. Bu hatalar ana hüzmeyi ve ilk sıfırları etkiler. Antenden L kadar uzaklıkta θ açısı kadar bir sapma, hüzmeye $\theta\lambda/2\pi L$ kadar döndürme hatasına neden olur. Faz hatalarından kaynaklanan parabolik faz dağılım eğrisi, hüzmeye omuzların (*skirt*) oluşmasına neden olur.

4.3.2 Prob Işıma Diyagramı

Probu ışınma diyagramından kaynaklanan hatalar, anten ölçümünde kazanç ve yan lob düzeyini etkiler. Probu yansıma saçılmalarını kestirmenin en iyi yollarından biri, prob ile anten arasındaki uzaklığın (z yönünde) değiştirilerek, doğrudan ve yansımalarla gelen işaretlerin toplamını gösteren sonuçlardaki dalgalanmanın (*ripple*) gözlemlenmesidir. α , dB olarak tepeden tepeye dalgalanma ve $R = 10^{\alpha/20}$ olmak üzere, yansıyan işaret doğrudan gelen işaretten $20 \log[(R-1)/(R+1)]$ dB kadar düşüktür.

4.3.3 Tarama Sınırlandırma ve Oda Kaynaklı Yansımalar

Anten yüzeyini prob ile tarayarak ölçüm alınabilecek aralık sınırlı olduğundan antenin yaydığı tüm alan ölçülememektedir. Antenin etrafındaki $D + 2L \tan \theta$ kadar alanda alınan veriler matematiksel işlemlerle uzak alan ifadesine dönüştürülmekte, fakat alınmayan verilerin getirdiği bir hata her zaman bulunmaktadır. İşte bu hatalara "tarama sınırlandırma hatası" (*scan truncation*) adı verilir.

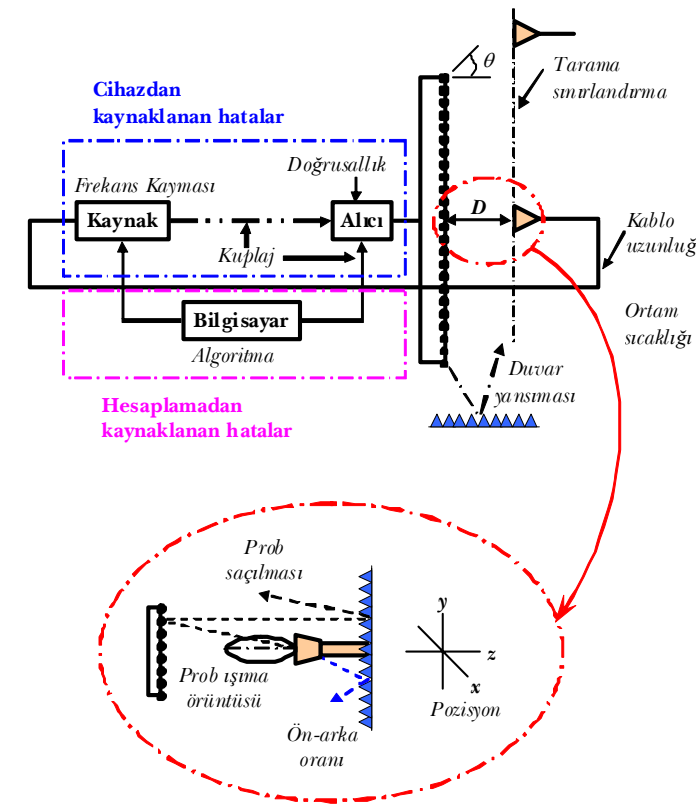
Oda kaynaklı yansımalar, odanın içinde anten ve prob dışında kalan kısımdan kaynaklanan yansımalarla. Bu yansımalar, antenin oda içinde $\lambda/4$ kadar hareket ettirilmesiyle meydana gelen değişimler ve bilinen soğurucu yansıtma oranı kullanılarak saptanır. Eğer yanlamasına kaydırılırsa, oda kaynaklı dalgalanmaların kayması beklenir.

Dikey olarak hareket ettirildiğinde ise, tavan ve zeminden gelen yansımalar görülür.

Devre çözümleyicisinin duyarlılığı, dinamik aralıkları, kapılara bağlı konnektörlerden sızan akımlar vb. de diğer hata kaynaklarıdır.

4.3.4 Tipik Ölçüm Hataları

Prob konumlandırma, prob yeri, prob titreşimi, prob yönelme hatası, prob ışınma diyagramı, prob saçılması, tarama sınırlandırma, oda saçılması, kaçak ve örtüşme hataları yan lobları etkileyen hatalardır (Şekil 8).

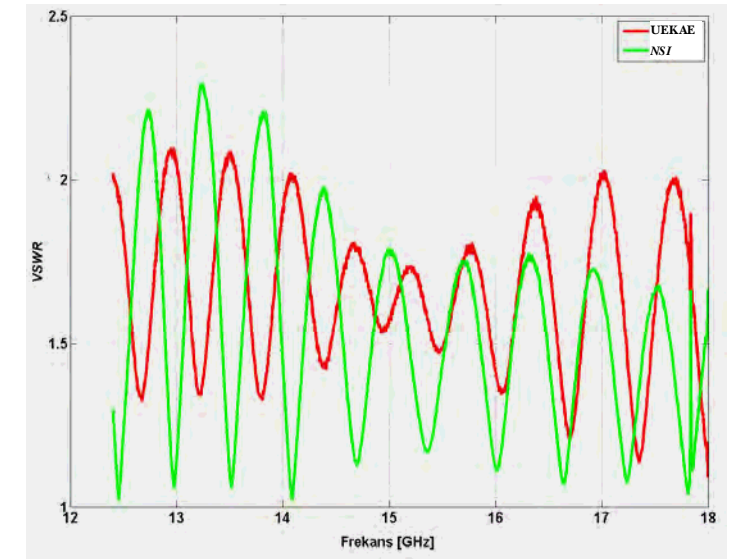


Şekil 8. Yakın alan ölçüm hataları.

Fazda ve genlikte meydana gelen rastlantısal hatalar da yine yan lobları etkiler. Test edilen antenin hizalama hatası ölçülen ışınma diyagramında kayıklığa neden olur. Prob kazancı hatası, genlikte doğrusal olmayan hatalar ve dinamik aralık, ölçümde kazanç sonucunu etkileyen faktörlerdir [3].

Prob kaynaklı hataların bir kısmı, iyi tasarlanmış ve doğrulama faktörleri düzgün çıkarılmış problemler yardımıyla en düşük düzeye indirilebilir. Bu amaçla, 12,4–18 ve 18–26,5 GHz frekans aralıklarında çalışan 2 adet prob tasarlanmış ve gerçekleştirilmiştir. Daha sonra UEKAE'de bu problemler, düzeltme faktörleri bulunan, kalibre edilmiş diğer problemlerle karşılaştırılmıştır. *VSWR* ve ışınma diyagramı olarak iki farklı grafik Şekil 9 ve Şekil 10'da verilmiştir. Hem ışınma

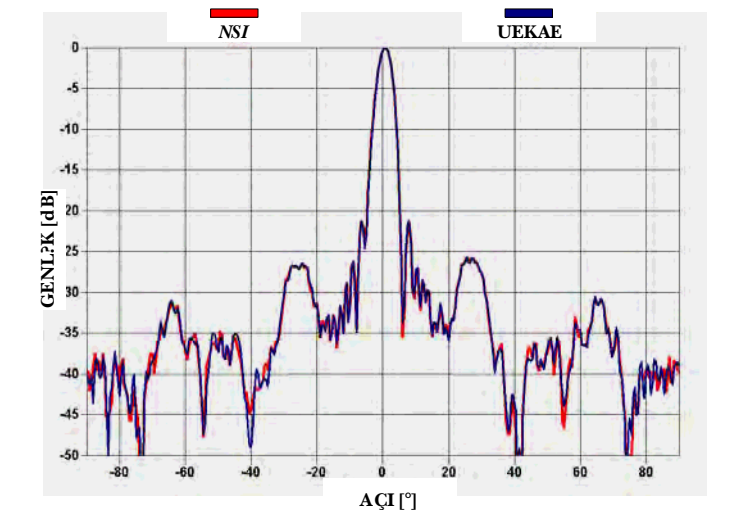
diyagramı hem de *VSWR* grafiklerinde, UEKAE probunun sonuçlarının piyasadan alınan probun sonuçlarıyla örtüştüğü görülmektedir.



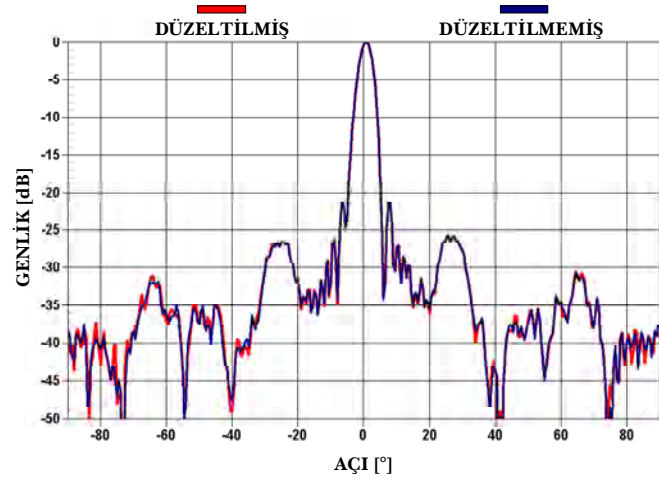
Şekil 9. Prob geriye dönüş kaybı.

4.4 Prob Doğrulama Hataları

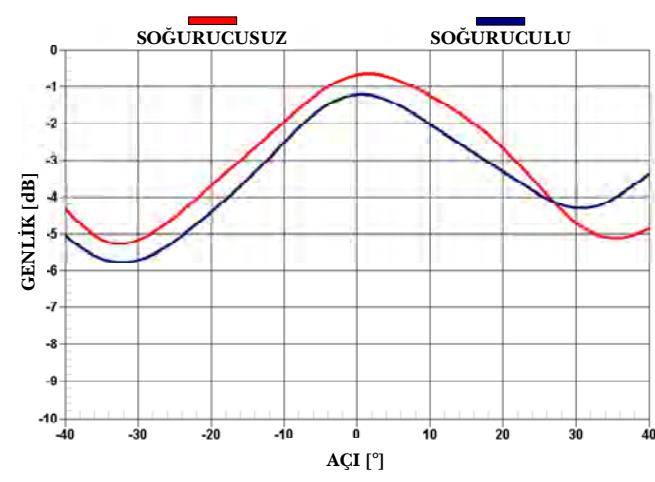
Prob doğrulama hatası, yakın alan ölçüm sistemlerindeki hatalardan biridir. Probu ışınma diyagramı kadar, eş genlik ve faz yüzeylerinin oluşturulması da önemlidir. Bu durumu test etmek amacıyla, Küresel Yakın Alan Ölçüm Sistemi'nde prob doğrulama verisi kullanılarak ve kullanılmadan, iki farklı ölçüm yapılmıştır. Sonuçlar, küresel yakın alan sisteminde prob doğrulama (*probe correction*) hatasının çok az etki ettiğini göstermektedir. Şekil 11'de alınan ölçüm sonuçları görülmektedir.



Şekil 10. X bandında çalışan bir antenin elevasyon ışınma diyagramının farklı problemler ile küresel yakın alan ölçüm sistemi kullanılarak elde edilmesi.



Şekil 11. Prob doğrulama hatasına ilişkin örnek bir ölçüm.



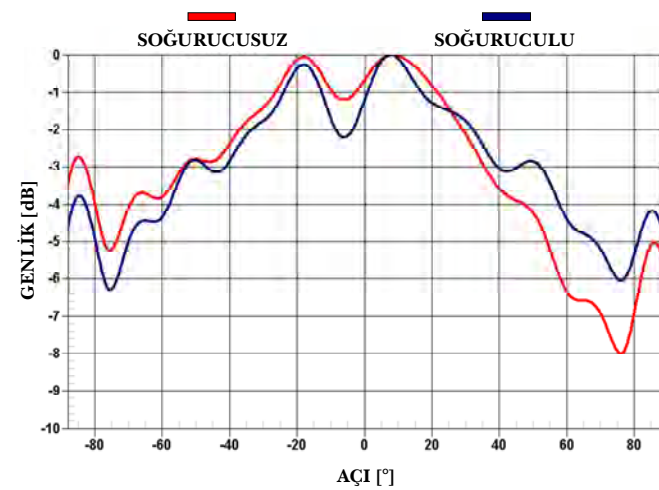
Şekil 13. Kelebek antenin H-düzlemi ışın diyagramı için soğurucuların olduğu ve olmadığı durum testi.

soğurucunun olduğu ve olmadığı durumlar arasındaki fark da artmaktadır. E ve H-düzlemi ışın diyagramlarında 2 dB'e kadar hata görülmektedir.

5 ANTEN TEST VE ARAŞTIRMA MERKEZİ (ATAM) KURULUM PROJESİ

TÜBİTAK UEKAE gerek kendi bünyesindeki projelere, gerekse ülkemizin çeşitli kurum ve kuruluşlarında, özel sektörde ihtiyaç duyulan anten gereksinimlerine tasarım ve ölçüm seviyesinde hizmet vermektedir. Bu alanda kazanılan tecrübe ve bilgi birikimi sayesinde, çok yakın gelecekte ülkemizin zorunlu ihtiyacı olan akredite ve hassas bir Anten Test ve Ölçüm Laboratuvarının oluşturulması kaçınılmaz görülmüştür. Bundan yola çıkılarak, TÜBİTAK UEKAE'nin bünyesinde yer alması önerilen **Anten Test ve Araştırma Merkezi (ATAM)** altyapı proje tasarısı hazırlanmış ve DPT'den proje desteği sağlanmıştır.

Proje tasarısı oluşturulurken yalnızca kurum içi ihtiyaçlar değil, ülkemizde benzer faaliyetlere belirli standartlarla uyumlu hizmet ve destek vermek hedefi de göz önünde bulundurulmuştur. ATAM kompleksinde yer alması planlanan 4 ana laboratuvar; Düzlemsel Yakın Alan Ölçüm (*Near Field Antenna Measurement*), Küresel Yakın Alan Ölçüm (*Spherical Near Field Antenna Measurement*), Uzak Alan Ölçüm (*Far Field Antenna Measurement*) ve Toplu Menzil Ölçüm (*Compact Range*) laboratuvarlarıdır. Ayrıca burada, tasarım ve geliştirme grubunun da yer alacağı bölümler ve bir de Elektromekanik Laboratuvarı olacaktır. ATAM projesi sistem çalışması aşamasında fiyat verimliliği göz önünde bulundurulmuş, düzlemsel yakın alan sistemi, anten konumlayıcı üzerinde yapılan bir değişiklikle (konumlayıcının yatay düzlemde 360° dönüştürülebilir hale getirilmesiyle) silindirik yakın alan ölçüm sistemine dönüştürülebilir hale getirilmiştir (Tablo 2).



Şekil 12. Kelebek antenin E-düzlemi ışın diyagramı için soğurucuların olduğu ve olmadığı durum testi.

Tablo 2. ATAM Düzlemsel Yakın Alan Ölçüm Sistemi Özellikleri

Düzlemsel ve Silindirik Yakın Alan Ölçüm Sistemi	
Oda Boyutları (En×Boy×Yükseklik)	~17×18×4 m ³
Maksimum Test Anten Boyutu	6×6×6 m ³
Maksimum Test Anten Ağırlığı	3000 kg
Tarama Düzlem Genişliği	9×9 m ²
Frekans Aralığı	0,75 – 40 GHz

Bu haliyle, ATAM kompleksi içerisinde bir oda yapılarak iki farklı ölçüm sistemi kullanılabilir. Buna uygun oda tasarımı, vinç, konumlandırma, havalandırma vb. özelliklerin uygun tasarımı yapılmıştır.

6 SONUÇ

Düzlemsel yakın alan ölçüm sistemi özellikle büyük hacme sahip, yüksek kazançlı antenlerin ölçülmesinde en iyi sonuçları vermektedir. Ölçüm hata çözümlemesi iyi yapıp, hata kaynakları düşük düzeyde tutularak hassas sonuçlar almak mümkündür. ATAM içerisinde yüksek kazançlı ve her bir boyutu 6 metreye kadar olan antenler düzlemsel yakın alan ölçüm sistemi içinde ölçülebilecektir.

KAYNAKÇA

- [1] C. A. Balanis, *Antenna Theory - Analysis and Design*, 2nd ed. New York: John Wiley & Sons, 1997.
- [2] B. Türetken, "Radar anten ölçümleri: TÜBİTAK UEKAE Anten Test ve Araştırma Merkezi kabiliyetleri", *V. URSI-Türkiye'2010 Bilimsel Kongresi ve Ulusal Genel Kurul Toplantısı*, Güzelyurt, KKTC, Ağu. 2010, sf. 448-451.
- [3] G. E. Evans, *Antenna Measurement Techniques*. Boston: Artech House, 1990.
- [4] *Near-field Antenna Measurement- Short Course 2009*, Nearfield Systems, Inc., Torrance, CA, 2009.
- [5] <http://www.nearfield.com/theory.htm>.
- [6] S. Gregson, J. McCormick and Clive Parini, *Principles of Planar Near-Field Antenna Measurements*. London: IET, 2007.



Bazı insanların özgeçmişine baktığınızda alt alta sıralanmış başarılar görürsünüz ve etkilenirsiniz. Tosun Terzioğlu onlardan biri. Fakat söyleşiye başlayınca dünyaya çok farklı perspektiften bakan aynı zamanda mütevazı biri olarak çıkıyor Tosun Hoca karşımıza. Düşünceli, hayalleri uzaklara erişen, tecrübeli, bilge.

Olumlu bakıyor hayata. Olumlu düşünüyor, düşündüklerini düşüncede bırakmıyor, gerçeğe dönüştürüyor.

Önde gelen matematikçi ve bilim insanı. 92-97 yıllarında TÜBİTAK başkanlığı yapmış. Sabancı Üniversitesi'nin kurucu rektörü.

Sayın hocam Prof. Dr. Tosun Terzioğlu ile samimi bir söyleşi yaptık. Bize hayat serüveninden, yakın tarihteki anekdotlarından, geleceğe dair fikirlerinden bahsetti. Umarız beğenirsiniz.

Transkripsiyon: Vural ÇELİK
Fotoğraflar: Elif SÜSLER

Tosun TERZİOĞLU kimdir?

1942 yılında İstanbul'da doğan Tosun Terzioğlu, 1961 yılında Robert Koleji'nden mezun olduktan sonra, lisans derecesini 1965 yılında matematik dalında İngiltere Newcastle Üniversitesi'nden; aynı daldaki doktorasını 1968 yılında Almanya Frankfurt Üniversitesi'nden almıştır. Michigan Üniversitesi, Wuppertal Üniversitesi ve Orta Doğu Teknik Üniversitesi'nde ders veren Terzioğlu, 1974-1975 ve 1989-1991 yıllarında Orta Doğu Teknik Üniversitesi Matematik Bölümü başkanlığı; 1977-1982 yıllarında ise aynı üniversitede Fen ve Edebiyat Fakültesi dekanlığı yapmıştır.

Tosun Terzioğlu 1977-1981 yılları arasında TÜBİTAK Temel Bilimler Araştırma Grubu üyesi, 1979-1981 yılları arasında Üniversitelerarası Kurul üyesi, 1990-1991 arasında ODTÜ Senato üyesi ve 1992-1997 yılları arasında da TÜBİTAK başkanı olarak hizmet vermiştir. Aynı dönemde Türkiye Teknoloji Geliştirme Vakfı Yönetim Kurulu, KOSGEB İcra Kurulu üyeliği ve 1993-1997 döneminde de NATO Bilim Komitesi Türkiye Temsilciliği yapan Tosun Terzioğlu, 1996-1997 yıllarında Bilimsel ve Teknik Araştırma Vakfı-BİTAV Yönetim Kurulu Başkanlığı görevini üstlenmiş, 1997-2000 döneminde TÜBİTAK Marmara Araştırma Merkezi Yönetim Kurulu başkanlığını yürütmüştür.

1997-2001 yılları arasında TÜBİTAK Bilim Kurulu üyeliği yapan Tosun Terzioğlu, Şubat 1998'den Temmuz 2001'e kadar TÜBİTAK UEKAE Yönetim Kurulu başkanlığını yürüterek bu enstitünün hızlı gelişimine katkıda bulunmuştur. 1997-2009 tarihleri arasında Sabancı Üniversitesi kurucu rektörlüğünü üstlenmiştir. Türk Matematik Derneği Onur Kurulu üyesidir. Türkiye Üçüncü Sektör Vakfı Yönetim Kurulu üyeliğini de sürdürmektedir. Editörlük ve Yazı Kurulu üyelikleri de bulunan, matematik alanında 50'nin üzerine bilimsel makalenin ve iki kitabın yazarı olan Prof. Dr. Tosun Terzioğlu, 1974 yılı TÜBİTAK Teşvik Ödülü ve 1986 yılı TÜBİTAK Bilim Ödülü sahibidir. Evli ve 2 çocuk babası olan Terzioğlu halen Sabancı Üniversitesi'nde çalışmalarını sürdürmektedir.

Akademisyen bir aileden geliyorsunuz. Babanız ve anneniz üniversitede profesör. Sizin geçmişten gelen "Ben de akademisyen olacağım, ben de üniversitede hoca olacağım" öyle bir planınız, amacınız, rüyanız var mıydı?

Yani yoktu ama başka da şansım yoktu diyebiliriz (gülüyoruz). Çünkü tek çocuktum. 5 yaşından itibaren hep üniversite konuşulurdu evde. Onun için benim akademisyen olmam doğal bir şeydi. Hangi konu olacağı, hangi alana kayacağım o son dakikaya kadar belli olmadı.

Sonra matematiği tercih ettiniz. Matematik sevdanız ne zaman başladı?

Ben okulu sevmeyen bir öğrenciydim ilkokulda (gülüyoruz). İyi bir lisede, Robert Koleji'nde okudum. Okulu sevmezdim ama iyi bir öğrenciydim. Fakat nedense lise sonun ortasına kadar çok kararsızdım. Aklımda matematik vardı, arkeoloji vardı, gemi mühendisliği vardı. Birbirinden bayağı farklı konular.

Lafınızı bölüyorsunuz. O zamanki karar vermede çektiğiniz güçlük Sabancı Üniversitesi'nin üniversiteye girdikten sonra bölüm seçme metodolojisini benimsemesinde etkili olmuş mudur acaba?

Tabii tabii (gülüyoruz). Tabii var. Annem biyoloji okumamı istirdi. Kendisi fizyologdu çünkü. Biyolojiye karşı bir merakım, hevesim yoktu. Babam matematikçiydi. Sonunda bana "Artık bir karar vermelisin" dediler. Ben de "Matematiği seçtim" dedim. Babam "Emin misin?" diye sordu. "Eminim" dedim ama çok doğru değildi (gülüyoruz). İngiltere'de öyle bir üniversite seçtim ki kendime matematik bölümünde öğrenci olacaktım. Birinci yılın sonunda kredi kaybetmeden gemi mühendisliğine geçebilecektim. İyi de bir gemi mühendisliği bölümü vardı. Arkeolojiye de geçebilecektim ama o zaman kredi kaybetme ihtimalim vardı. Fakat bir yıl matematik okuduktan sonra sevdim. Üniversite hayatını ve matematiği sevdim. Matematikte kaldım, hiç pişman olmadım. Sonradan anlıyorum ki gemi mühendisliği benim denize olan merakımdanmış. Yani o sıralar deniz biyolojisi bölümü olsa pekala oluyabilirdim (gülüyoruz).

İngiltere'de lisans okudum. Sonrasında Almanya'da Frankfurt Üniversitesi'nde doktora yaptım. Doktoradaki üç yılın bir yılı Amerika'da geçti. Çünkü doktora danışmanı hocam Amerika'ya misafir profesör olarak gitti. Benle onunla beraber gittim.

Ardından ODTÜ'ye mi geldiniz?

Ondan sonra ODTÜ'ye geldim. 1968'de doktorayı bitirir bitirmez geldim. Başladığımda matematik bölümünün onbirinci öğretim üyesiydim. Bölüm o kadar küçüktü. İçinde yöneylem araştırma ve istatistik de vardı. Şimdiki binanın bir katını dolduramazdık. Şu an bina taşıyor.

ODTÜ'deki yıllarınızdan biraz bahsetsek?

Ben İstanbulluyum. Ailem de İstanbullu. Ankara'ya tamamen ODTÜ için gittik, evlenmiştim o sırada. İkimizde daha önce Ankara'da yaşamamıştık. Heyecanlı, zor yıllardı. Çalkantılı ve



bu çalkantıların üniversiteye çok yansıdığı yıllardı. ODTÜ'ye özellikle de. Ama öbür taraftan da matematik, araştırma, bir üniversitenin kuruluşunu görme bakımından da çok tatmin edici yıllardı.

ODTÜ Matematik'te babamın jenerasyonundan Cahit Arf vardı. Daha sonra da Ege Üniversitesi'nden Japon asıllı Gündüz İkedo geldi. Dolayısıyla bir çekim merkezi oluştu ODTÜ'de.

Bir de daha ziyade benim yaşında o zamanın gençleri vardı. O yıllarda devamlı araştırma seminerleri yapardık. Gözümüzü kestirdiğimiz öğrencileri daha üçüncü sınıfta zorla araştırma seminerine sokardık. Sonrasında bu öğrenciler yurtdışında doktora çok iyi yerlere gittiler. Tabii biz "Git doktora yap" şeklinde yapmadık. "Şurda yapsan, şu konuda yapsan, yaptıktan sonra tekrar gelsen" tarzında yönlendirdik. ODTÜ Matematik

iyi öğrencileri yurtdışında doktora yaptırıp sonra tekrar kendi bünyesine çekerek bu konuma tlaştı.

12 Mart geçti, 12 Eylül geçti. O çalkantılarda sarsıldı sistem. Ama ODTÜ'nün bir avantajı Yüksek Öğretim Kanunu çıkıncaya kadar kendi kanunuyla yönetilmesiydi. Kendi sınavı, kendi kanunu ve mütevelli heyeti sistemi vardı. Fakat mütevelli heyeti sistemi hem içeriden hem dışarıdan hızla dejeneredildi.

12 Eylül sonrasında diğer üniversiteler gibi Yüksek Öğretim Kanunu'na tabi oldu. Yine de kendi iç dinamikleri sayesinde çizgisini korudu. Sağlam kurulmuştu, şimdiki öğretim üyelerinin önemli bir bölümü en az bir derecelerini ODTÜ'den almışlardır.

Gündüz Bey'den (İkeda) bahsettiniz. Geçen sene Mayıs sayımızda biz de Gündüz Bey'e yer vermiştik. ODTÜ kökenli olup TÜBİTAK bünyesinde görev almış birçok değerli bilim insanı var.

Evet. Çünkü Cahit Bey (Arf) TÜBİTAK'ın kurucularındandır. UEKAE ilk kuruluş yıllarında küçük bir gruptu tabii. İki grup insan vardı. Bir kısmı mühendis; elektronikçi, bilgisayarçı. Bir kısmı da matematikçi. Ama matematikçilerin hemen hemen hiçbiri "coding theory"de araştırma yapmış değil. Çoğu cebirci. Ne var ki bir arada çok çok güzel çalıştılar. Çok güzel bir etkileşim kurdular. Matematikçiler o etkileşimin başarıyla ortaya çıkmasında Gündüz İkeda'ya çok şey borçludur. Gerçek bir liderlik yaptı.

Peki hocam ODTÜ'den TÜBİTAK 'a geçişiniz nasıl oldu?

Erdal Bey (İnönü) istedi, TÜBİTAK 'a geçtim. ODTÜ'de yarı zamanlı ders veriyordum. 95 başında emekliliğimi istedim. TÜBİTAK 'ta tam zamanlı oldum.

Sizin TÜBİTAK başkanlığı yaptığınız yıllarda bahsettiğiniz çabalarla ve dediğiniz gibi matematikçilerin de katkılarıyla özellikle UEKAE'de bir palazlanma oluyor. Gerek Türkiye çapında gerekse NATO'da ismini duyuruyor.

Ben 92-97 yılları arasında 5 yıl TÜBİTAK başkanlığı yaptım. Erdal İnönü o zaman devlet bakanı ve başbakan yardımcısıydı. Kurum Erdal İnönü'ye bağlıydı. İnönü de dahil olmak üzere 5 yılda 8 farklı bakanla çalıştım (gülüyoruz). Koalisyonlar değişiyordu. Bu 8 bakan da aynı partiden değillerdi. Bir kısmıyla tanışmadan ayrıldılar (gülüyoruz).

İlk başta Erdal Bey sayesinde -Demirel de başbakandı- iyi destek aldık. Şubat 93'te

Bilim ve Teknoloji Yüksek Kurulu yapıldı. Bir takım kararlar hayata geçmeye başladı. Ben "Prensipte çok güzel kararlar alalım, ama bir kenarda dursun" yaklaşımına hiç inanmam. Hayır, prensipte o kadar sağlam kararlar olmasın, ziyarı yok. Yeterki bir şeyleri hemen hayata geçirebilelim. Güzel kararlar alındı. Bunların içinde dağılan Sovyetler Birliği'ndeki bilim adamlarını Türkiye'ye çekmek için kullandığımız DOPROG (Eski Sovyetler Birliği Cumhuriyetleri ve Doğu Avrupa ülkelerinden bilim adamı getirtilmesi programı) vardı ki onun sayesinde birçok bilim adamı bizim üniversitelerimizi tercih etti.

Bir ulusal gözlem evi inşa edildi. TÜBİTAK'ın kanunu değiştirildi. Türkiye Bilimler Akademisi kuruldu. Yani 1993 Şubat ayında yapılan Bilim ve Teknoloji Yüksek Kurulu'nda alınan kararlar hayata geçirildi. Ondan sonra, Erdal Bey politikadan ayrılınca TÜBİTAK farklı bakanlara bağlı olmaya başladı. Bir kısmı TÜBİTAK'a pek sempatiyle bakmadılar. Fark etmez, biz aynen çalışmaya devam ettik. Başka şeyler de yapmaya çalıştık. Marmara Araştırma Merkezi (MAM) içinde başka yerlerde başka enstitüler vardı. Bunlar hep merkezden idare ediliyordu. MAM başta olmak üzere tüm enstitüler yerinden daha iyi idare edilsin diye belli prensipler dahilinde oluşan yönetim kurulları kurduk. Harcama yetkisi de dahil olmak üzere yetki devri ile yerinden idare edilmesine çok özen gösterdik. Her şey Ankara'ya sorulmaz. O zamanki MAM Başkanı Ömer Kaymakçalan çok uğraştı. MAM başından beri sanayiye araştırma yapmak için kurulmuş. Ama bünyesine sonradan temel bilimler eklenmiş, şu-bu eklenmiş. Mesela temel bilimlerin misyonuyla MAM'ın diğer enstitülerinin misyonları birbirlerinden çok farklı. Bu yüzden ister istemez kendi ayaklarına çok basıyorlardı. Bir taraf diğerine diyorki "Siz makale üretmiyorsunuz". Onların görevi makale üretmek mi? Sanayiye araştırma yapmak. Diğeride diyorki "Biz de sizi sanayide göremiyoruz, sadece makale yazıyorsunuz" (gülüyoruz).

Evet birbirlerinin gözüne batıyor.

Onları ayırtırdık. Temel bilimler oradan ayrıldı ve Boğaziçi'nde Feza Gürsey adı altında kuruldu. Çok güzel gelişti ve hala da geliyor. Bu şekilde yerinden yönetime geçtik, orada başarılı olduk.

1996 yılından itibaren sanayi ar-ge teşviğinde TÜBİTAK önemli bir rol almaya başladı. Zaten tebliğin hazırlanmasında arka planda o zamanki Hazine ve Dış Ticaret Müsteşarlığı ve Türkiye Teknoloji Geliştirme Vakfı ile çok ciddi çalışmıştık. Bu TÜBİTAK 'la ve sanayici arasında mecburi bir bağ kurdu. Platonik bir bağ değildi. Türkiye'de üniversite-sanayi işbirliği oluyordu olmuyordu, bunları konuşmayı çok severiz. Bunlar boş laflar. Biz sanayiye ar-ge teşviğini TÜBİTAK olarak ortaya çıkarttık. Hem de öyle bir şekilde çıkarttık ki sanayici üniversiteler ile işbirliği yaparsa daha fazla teşvik alıyor. Öncelikli alanlarda araştırma yaparsa daha fazla teşvik alıyor. Tüm bunlar ortaya çıktı.

O tarihlerde bizim sanayicileri, sanayi odalarını dolaşarak TÜBİTAK olarak anlatmaya çalıştığımız şeyleri şimdilerde sanayiciler reklamlarında bile kullanıyorlar. "Biz bu teknolojiyi geliştirdik", "bu bizim ürünümüz" gibi. Bu bana fevkalade büyük bir mutluluk veriyor. Şimdi Sabancı Üniversitesi'nde görev yapan Cemil Arıkan o zaman 1 yıl içinde 30'a yakın ile gitti. Biz sanayicinin ayağına giderdik. Daha önceki teşviklerde sanayiciler Ankara'ya gelirdi. Teşviği kim veriyorsa onun kapısına gider ve bekler, almaya çalışırdı. Hayır biz gidiyorduk, anlatıyorduk.

Onunla ilgili çok büyük önyargılar vardı belki de? Gideceksiniz Ankara'ya ama teşvik vermeyecekler. Eliniz boş döneceksiniz.

Tabii, biz gidip anlatıyorduk. Bu şöyle bir şey. Anlatıyorduk, bütün sorularına cevap veriyorduk. Saatlerce sürüyordu toplantılar. Güzel bir birliktelik kuruldu. Zaten, bir anlamda kendi müşterimize - bu sanayici olabilir, Silahlı Kuvvetler olabilir- gidiyorduk. Araştırma yaparak başarı kazananlar öne çıkmaya başladı. Yani Kriptoloji Enstitüsü 90'larda kurulduğunda 14-15 kişiydi. Şimdi kaç kişi olduğumuz daha iyi biliyoruz.

BİLGEM yaptığı işlerle buraya geldi. İş yapabildiği için gelişti. 97'de TÜBİTAK'tan ayrılıp Sabancı Üniversitesi'ne geldim. Fakat TÜBİTAK Bilim Kurulu'ndaydım ve 2000 yılına kadar da UEKAE'nin yönetim kurulu başkanıydım. Oraya diğer enstitülerden çok çok farklı bir yönetim sistemi kurduk. Ama kriptoloji farklı olmak zorundadır. Bir takım sivil olmayan üyeleri vardır. Sivil üyeleri, başkanı da dahil, bazı şeyleri bilmemek durumundadır. O zaman gayet güzel işleyen bir sistemdi, şu an da çok iyi bir şekilde işliyor sanırım.

Hocam şu çok dikkatimi çekti. Sanayici ile TÜBİTAK'ı, sanayici ile ar-geyi bir araya getirmek için çok uğraşmışsınız. Şimdi bunun önünü açan bir çok kurum var. KOSGEB olsun, Devlet Planlama Teşkilatı'na bağlı Kalkınma Ajansları olsun, Türk Teknoloji Geliştirme Vakfı olsun; bunlar akla ilk gelenler. Yatırımın o tarafa yönlendirilmesi ve yine bu vatanın insanının teşvikler sayesinde güzel şeylerin altına imza atması gurur verici. İnşallah Türkiye'yi çok kalkındıracak, çok farklı noktalara taşıyacak hamleler.

Evet çok güzel. Ama daha yapılacak çok işler var.

Mesela zamanın İstanbul Sanayi Odası Başkanı Hüsamettin Bey'e (Kavi) ar-ge teşviklerini anlatmaya çalışıyordum. Ondan sonra 98'de, artık Sabancı Üniversitesi'nde iken "Türk Sanayisi ve Ar-ge" konulu İstanbul Sanayi Odası'nın bir toplantısına

beni de çağırdılar. Benden önce Hüsamettin Bey konuştu. Sonra başka bir arkadaş konuştu. Ben konuşmamda şunu söyledim "Hem başkanımız hem de diğer arkadaşımız ar-genin sanayi için yaşamsal önemini o kadar güzel anlattı ki bana söyleyecek bir şey kalmadı". Oturdum ben (gülüyoruz).

Anlatmaktan öte güzel örnekler insanın aklını açıyor. Şu kişi de şunu yapmış, bu kişi de bunu yapmış başarılı olmuş, çok kar etmiş. Başarı örnekleri çok önemli.

Peki TÜBİTAK'ta iken yaşadığınız aklınıza gelen hoş bir anınız var mı?

Yani çok var (gülüyoruz). Hangisini anlatayım bilemiyorum. Mesela şunu anlatayım. Bilim ve Teknoloji Yüksek Kurulu olacak, çok acele hazırlandık. Şubat 1993'te. Önceki gün Erdal Bey telefon etti. Beni yarın sabah saat 8'de köşkte başbakan bekliyor. 9'da da kurul var. Başbakan "Nedir bu diye soracak?" dedi. Elimizde bir doküman var, yarısı kabul edilse çok memnun olacağız. Gittim, Süleyman Demirel ve yanında birileri daha vardı. Demirel hemen lafa başlar. "Sana çay verdiler mi?" dedi. "Teşekkür ederim" dedim. "Nedir bu böyle?" dedi. Anlatmaya başladım ve ikimiz de saatimize bakıyoruz. "Sayın başbakan, biz toprağı çok iyi sürdük, yağmur da yağacak zannediyoruz, ama tohum için paramız yok" dedim (gülüyoruz). "Tohum nerden çıktı şimdi?" dedi, sonra "Anladım, anladım, tamam"



Tosun Hoca sorularımız içtenlikle yanıtladı.

dedi. "Sen şimdi git, sen bunları bilmezsin, beni sen kapıda karşılayacaksın. Biz bunları hallederiz sen merak etme" dedi. Ben gittim 15 dakika sonra da o geldi. Erdal Bey ve bir sürü kişi oradaydı. Biz şimdi anlatıyoruz, Demirel başkanlık yapıyor. Tabii para istiyoruz biz şimdi. O zamanki hazine müsteşarı "Sayın başbakan, bu fondan o kadar çok para istendi ki" dedi. Biz de 9 milyon dolar istiyorduk. Ama bizim için çok kritikti. "Nasıl yapacağız?" dedi müsteşar. "Öbürlerini geri iteceksin, bu kadar basit işte" dedi (gülüyoruz). Ondan sonra kendi partisinden bir milletvekili "Efendim, bu kalın bir doküman, biz henüz iyi inceleyemedik" dedi. "Ben hepsini okudum" dedi başbakan (gülüyoruz). "Çok iyi bir doküman, eğer itirazın varsa bir hafta içinde TÜBİTAK'a yazılı olarak yazarsın" dedi. Bütün her şeyi kabul etti, çıktı. Ondan sonra Erdal Bey'e "Hem başbakan yardımcısız, hem de TÜBİTAK size bağlı, kararları kamu oyu ile paylaşsınız" dedi.

Demirel her zaman çok güzel destekledi. Antalya Bey Dağları'nda 2500 metrede gözlem evi açılıyor. Onun açılışına bile geldi. Helikopterle inanılmaz bir yere indi. Ben oradan inmeme, ama o indi (gülüyoruz). Ondan sonra Erdal Bey basın toplantısı yapacak. Biz önceden konuşuyoruz, şunu sorsalar ne cevap vereceğiz diye. Basın geldi. Erdal Bey yarım saat araştırmanın önemini, hem teorik taraftan önemini, hem sanayiye önemini çok güzel ders gibi anlattı. Ama basın açıklamasına girmeden önce bize dedi ki "Şimdi bunlar sol ne zaman birleşecek diye sorarlar" dedi. Net, berrak bir şekilde anlatacağımı anlattıktan sonra "Sorunuz var mı?" diye sordu. İlk soru; "Efendim, sol ne zaman birleşecek?" (gülüyoruz). Erdal Bey başta olmak üzere hepimiz gülmekten masanın altına girdik. Fakat çok kötü oldu, çok utandı soruyu soranda. Erdal Bey "Onun yeri farklı" deyip onun da gönlünü aldı. TÜBİTAK Ulusal Gözlemevi'nin açılışındaydı.

Ben 78-79'da TÜBİTAK Temel Bilimler Grubu'nda çalıştım ve o sırada yıllardan beri devam eden gözlemevi yer seçimi projemiz vardı. Genç astronom arkadaşlarımız Türkiye'de

nerede gözlemevi olabilir diye dağ tepelerinde kimi yerde katırlarla çıkarak, kimi yerde uçurumdan düşme tehlikesi geçirerek özveri ile çalıştılar. Bey Dağları'nda bu yer seçildi. Güzel bir yer. Fakat para yok. Bilim ve Teknoloji Yüksek Kurulu'nda bir para aldık, fakat bu para teleskoba yetmeyecek. O zaman astrofizikçi iki arkadaşımız Tatar asıllı Sovyet olan meşhur astrofizikçi Raşit Sunyaev ile temasa geçtiler. Şöyle bir şey yaptık. Rusya'nın imal etmek üzere olduğu bir teleskop gelecek, Antalya Bey Dağları'na monte edilecek. Onun karşılığında o teleskopun belirli bir zamanını biz Ruslara tahsis edeceğiz. Bedava teleskop bulduk. Şimdi artık bu aşama Bilim Kurulu'ndan kararı çıkarmak lazım. O sıralarda da Erdal Bey artık politikayı, başbakan yardımcılığını bıraktı ve Bilim Kurulu üyesi oldu.

Ben Bilim Kurulu'na hesabımı veriyorum, "Şu kadar paramız var" diyorum. Dediler ki "Ya bu teleskop gelmezse". Anlaşma var ama bedava gelmezse ne olacak? O zaman Bilim Kurulu'ndan bir üye sordu "Maliyeti kaç çıkacak her şeyin?". "4 milyon dolarla 9 milyon dolar arası" diye söyledim. O da ekonomist Atilla Karaosmanoğlu idi, "Olur mu öyle şey?" dedi. "Eğer Rusya'dan hibe çıkarsa 4 milyon dolara, alamazsak 9 milyon dolara mal olur." dedim. Dışarda teleskopun ucuzu 5 milyon dolar. Erdal Bey söz aldı, "Yaparlar, yaparlar onlar" dedi bizim için (gülüyoruz). Hakikaten de yaptık. Fakat çok komik bir şey oldu. Ben Ankara dışındayım, acilen Dış Ticaret Müsteşarlığı'ndan arıyorlar. Ne oldu derken, teleskop 7 tane 'lowbed' treylerle gelmiş. Samsun'da gümrüğe girmiş. Her şey hibe. Fakat Samsun'da demişler ki biz bundan ithalat vergisi alacağız. TÜBİTAK'tan ithalat vergisi alacaklar. Zaten öyle bir paramız yoktu. Neyse dış ticaret müsteşarımız Necat Bey sağolsun çok güzel anlattı, halledildi. O da geldi. Monte edilecek. Dağa 13 tane korkunç virajla çıkılacak. neyse çıkıldı. Montajı yapıldı, ondan sonra açılış için az önce bahsettiğim gibi Demirel'i davet ettim. O sırada Mesut Yılmaz başbakan, o da gelecek. Ben dağda bekliyorum. Demirel askeri helikopterle geldi. Dağın zirvesinde acaip rüzgar var, bir bu yandan esiyor,

Sabancı Üniversitesi'nde.

bir diğer taraftan. O askeri helikopter inanılmaz bir ustalıkla bu odanın yarısı kadar ufak bir kayanın üstüne indi. Ben hoş geldiniz diye konuşmaya başladım. Törende birden gözüüm ön sıralara takıldı. Daha önce görmemiştim. Annemin ve babamın arkadaşı astronom Nüzhet Gökdoğan. O sıralar 80 küsur yaşındaydı ve oradaydı. Bizim gözlemevini açarken güvencemiz şuydu; Türkiye'deki bütün asronomlar buna sahip çıkarlar. İlk kadın gökbilimcisi olan Nüzhet Hanım, o yaşta o dağa o heyecanla çıkıyorsa tamam dedim, doğru yapmışız.

Peki Ruslar teleskopu kullanmaya geldi mi?

Tabii geliyorlar arada. Hala geliyorlar, mülkiyet onların. Ama mülkiyet onların, al da götür değil tabii ki (gülüyoruz). 78'de yer aranıyordu, anlaşma 94'te yapıldı.

SSCB ile değil, Rusya'yla yaptık yani anlaşmayı?

Rusya ile yaptık ve oldukça karışık bir anlaşmaydı. Rusya, Tataristan Özerk Cumhuriyeti, Rus Bilimler Akademisi falan, oldukça detaylı bir anlaşmaydı.

Belkide Tataristan'a kurulacaktı da sonra bize kuruldu.

Evet evet, öyle bir şey oldu. Çünkü Saint Petersburg'tan yola çıktı ama Moskova'dan geçmek zorundaydı.

Hocam ben şunu da öğrenmek istiyorum. Uzun zamandır akademik hayatın içindesiniz. Ar-ge ile içli dışlı oldunuz. Bu bağlamda geçmiş ile şimdikiyi nasıl kıyaslıyorsunuz?

Türkiye'de eskiden beri bir şeyleri biz yapalım, bizim bilim adamımız mühendisimiz yapalım hevesinde olan insan çok vardı. Ama bizim bir de kötü tarafımız var, acelecimiz. Yani bugün başlayalım, yarın aya roket yollayalım. Eğer yollayamıyorsak başarısız. Hedefi doğru seçmiyoruz bazen. Eğer hedef yanlış seçiliyorsa ve neticesinde başarılı olunamıyorsa insanlarda hayal kırıklığı oluyor.

Tabanımın geniş olması, tabana yayılması herhangi bir aktivite için çok önemli. Türkiye büyük bir ülke. 75 milyon deniyor. Dolayısıyla falanca alanda 10 tane çok iyi insanın olması çok bir şey ifade etmiyor. Çok daha yaygın olması lazım. Orada bir takım yanlışlıklar yapıyoruz. Ancak şu artık gözükiyor. Türkiye'deki sanayici; risk almasını bilen, giderek misyonunu daha iyi tanımlayabilen, dünyaya açılabilen müthiş bir girişimci grubu portresi çiziyor.

Dünyaya açılmak deyince aklıma geldi. Yıllar önce Bursa'da bir girişimci tekstilciden duyduğum bir şey. TÜBİTAK yıllarımda, Bursa'dayım. Dedi ki "Benim babam da tekstilci, bana derdi ki: Ya biz Bursa'dan dünyaya bakmaya çalışırken şaşkınlıktaydık." "Ne demek o?" diye sordum. "Bir Ankara'ya bakıyoruz, bir İstanbul'a. İstanbul bir şey diyor, Ankara başka bir şey diyor. Biz şimdi böyle yapmıyoruz. Bursa havaalanında bilmem kaç tane özel uçağımız var veyahut kiralayabildiğimiz. Mesela Milano'da tekstil fuarı oluyor, biz oraya toplanıp gidebiliyoruz. Ne İstanbul'a uğruyoruz, ne Ankara'ya." dedi. Yani dünyaya bakmaya başladılar, dünyada her yerde olmaya başladılar ve bir çok alanda da kendi know-how'ını yaratma beceresini göstermeye başladılar.

Sanayi ar-ge teşviği başladığı zaman Kayseri'deyiz, Küçük bir sanayicinin imalat yerini geziyoruz. TÜBİTAK başkan yardımcısı Cemil Bey'le (Arıkan) beraberiz. Cemil Bey'e biri çok hoş bir şey gösterdi. Cemil Bey dedi ki "Buna patent alsana?". Hakkikaten çok güzel bir şey, patentlik bir şey. Cevap şu oldu: Estağfurullah (gülüyoruz). Orta okul mezunu fakat müthiş cin fikirli bir sanayici. Kendi alanında gerçekten fevkalade iyi. Çünkü ona göre patent işte üniversiteyle oturulur, 2 yıl araştırma yapılır. Ondan sonra çıkan bir şeydir. Başka türlü çıkmaz. Bahsettiğim sanayiciyi görmedim ama işlerini çok daha büyütüğünü biliyorum. Kendi demeçleri var. Ne yaptıysa, nereye geldiyse, kendi know-how'ını geliştirerek başardı. Benzer şekilde Antep'in makine imalatçıları. Taklitle başladılar, doğrudur. Kendi ifadelerine göre Çukurova'daki traktörleri tamir ederek başladılar (gülüyoruz). Sonra taklit ettiler. Şimdi tekstil makinelerinde özgün tasarımlı makineleri var, dünyaya satıyorlar. Bir yerden çıkabiliyor. Keza aynı şekilde beyaz eşya. Arçelik'in hikayesini biliyorum, Vestel'in hikayesini biliyorum. Giderek bu otomotivde de olacak. Bunu yapmazsak tabii sanayi kaybolmuyor, el değiştiriyor. Mesela ilaç sektörü. Türk ilaç sektörünün devleri yabancı sermaye oldu. Yine burda imalat oluyor, yine buranın insanı çalışıyor, ama yabancı firmalar altında. Böyle olmasının da nedeni vakti zamanında ar-geye girmemeleri veya girememeleri. Kendileri "Giremezdik, çok pahalıydı" diyorlar, ben o fikirde değilim. Bir yerden girebilirlerdi. Eczacıbaşı artık Eczacıbaşı ilaç şirketi değil, satıldı.

Ben de otomotive üzülürüm. Ünlü bir restoran düşünün. Restoranın işletme kalitesine uygun sebze, meyve, et var. Bunları pişireceğiniz, servis edeceğiniz teçhizat var. Çok iyi ahçılarınız var. Restoranda gelip yemek yiyecek müşteriniz var. Fakat restoranınız yok. Sebzenizi başka restorana sebze fiyatına satıyorsunuz. Teçhizatınızı başkası kullanıyor. Ahçılarınız başka restoranlara hizmet ediyor. Otomotiv sektörümüzde katma değer en üst seviyesini verecek olan %100 yerli otomobil üretme hayalini gerçekleştiremedik.

Evet, onlar üzücü şeyler. Kaçırılan fırsatlar var. TÜBİTAK'tayken de şunu konuştuk, Casa askeri nakliye uçakları TAI tarafından yapılıyordu. Onlar, İspanyol tarafı, bir tane mühendis yollamışlardı. Konuşmuştuk, "Ben 2 sene burda kalacağım, 1 senede baktım TAI zaten F16 yapıyor. Casa'da öyle büyük bir teknoloji yok. Ben de boş kaldım, havacılık sanayinizi inceledim neler yapmışsınız diye. Siz 1950'lerde bizden ilerdeymişsiniz. Rüzgar tüneli yaptırılmışsınız. Ama sonra bütün onları kapatmışsınız. Her şey NATO'dan gelecek diye bunlara ne gerek var demişsiniz. Biz ise oradan yavaş yavaş geldik. Casa dünyanın en iyi uçağı değil. Ama siz alıyorsunuz, biz kullanıyoruz, başka ülkeler de alıyor." dedi. Kaçan çok büyük fısatlar var. Yine kaçan başka bir büyük fısat demiryolu. Sadece vagonlar değil, lokomotifini, hızlı trenini, metrosunu yapabilmek.

Şimdi yeni yeni oluyor.

Şimdi yeni yeni oluyor, evet. Çünkü oradaki teknoloji dünyanın en iyi teknolojisi değil. 60'lardan itibaren onları geliştirmeye başlasaydık, ki Fransa, İspanya da o tarihlerde başladı, farklı bir resim ortaya çıkabilirdi. Atlanan birtakım şeyler var. Belirli bir dönemde bu hazıra konma -mesela NATO bize nasılsa Amerikan silahı veriyor, üretmeye gerek yok- düşüncesi çok yanlış, çok kısa vadeli, çok miyop bir strateji.

Bir de hocam, bu düşünceler kısa vadeli olduğu gibi yalnızca iyi günde geçerliliği olan stratejiler.

Evet. Türk sanayisine ve Türk Silahlı Kuvvetleri'ne Kıbrıs Barış Harekati sonrası bize uygulanan ambargo çok öğretici olmuştur. 1 dolarlık parça yetmezliği yüzünden tanklar yollarda kalmıştır.

Biraz Sabancı üniversitesi'nden bahsetmek ister misiniz?

Hay hay, olur. Ben 97'de başladım, üniversite 99'da açıldı. Benim için heyecan verici olan üniversitenin özgün tasarımıydı. Tasarımda bir serbestlik vardı. Hep Güler Hanım (Sabancı) şunu anlatır, iki şey onun için önemlidir. Amcalarımdan dinlediği şeyler, rahmetli Sakıp Bey (Sabancı) ve rahmetli Hacı Bey'den (Sabancı). O sıralar 27 üniversite varmış. Onlar demişlerki "Biz diğer 27 üniversiteye benzeyen 28. bir üniversite istemiyoruz, eğer onu yapacaksan vazgeçelim, yapmayalım. Biz farklı bir şey istiyoruz. Nasıl bir şey olacak? Onu da sen düşün, bul, bize de anlat". Hacı Bey'in söylediği başka bir şey daha vardır. Güler Hanım odasına gitmiş, bu işin kendisine verileceğini tahmin ediyormuş. Güler Hanım şöyle anlatır: Sonra Hacı amcam aradı, "Güler bana bir gelebilir misin?" diye. Gittim. "Sen aldığın görevin farkında mısın?" dedi. "Tabii farkındayım. Şu kadar iş programı olacak, iş yükü olacak, şu kadar yatırım yapacağım" diye cevap verdim. "Biliyorum, biliyorum, onları tabii yaparsın. Ben onu söylemiyorum. Bu derslik yapmaya benzemez. Sen insanların çocuklarını alıp eğiteceksin. Büyük sorumluluk. Onlara "Bu defolu çıktı sana ithal edilmişini verelim." diyemezsin." demiş. Bu iki kişi de, Sakıp Bey de Hacı Bey de, bildiğim kadarıyla üniversite mezunu değiller. Ama Anadolu bilgeliliği diye bir şey var. Bu yaklaşım benim çok hoşuma gitti ve tabii bir de özgün tasarım. Biz üniversite açılmadan önce çalışanlar aşağı yukarı 20 kişiydik. Çalışanlar, akademisyenler, yöneticiler müthiş çalıştık. Önce holdingin binasında, sonra Karaköy'deki binamızda.

Temel Geliştirme Programı oradan çıktı, bizim şimdi Toplumsal Duyarlılık Projeleri dediğimiz programlar oradan çıktı, bölümsüz olması oradan çıktı, programların öğrenciler tarafından seçilmesi oradan çıktı, hangi programların olacağı

Erdal İnönü'yle beraber TÜBİTAK'ta.



oradan çıktı. Tabii bölümsüz olması ve öğrenciye seçme özgürlüğü verilmesi programların birbirine yakın olmasını gerektiriyor. Bu sistemin büyük avantajları var, çok doğru, ama mesela bu sistemde tıp olamaz, hukuk olamaz. Çünkü burada 2. sınıftan sonra tıpı seçebilirsin dediğin vakit bu uygun olmaz. Sonra 99 Mart ayında mütevelli heyetine son defa anlatım. Herkes memnun görünüyor. Mekatronik programı bazılarının akıllarına takılmış. "Ben şimdi size soruyorum" dedim, "4 yıl sonra, 5 yıl sonra şu şu programdan mezun birisi gelse, işe alır mısınız?" Biri kalktı dedi ki "O mekatronik dediğinizden ben bir tane alırım" (gülüyoruz).

Siparişler gelmeye başlamış (gülüyoruz).

Tabii bunu YÖK'ün kabul etmesi lazım. Güler Hanım "Ne yapacağız şimdi?" dedi. "Kamp kuracağız, bunları anlatacağız" dedim. O sıralar YÖK'te Kemal Bey var, Kemal Gürüz. Onun bir sempatisi vardı zaten. 2-3 defa gittik biz YÖK'e. Bize açıkça şunu söylediler: Bakın, bu Türkiye'de olmaz. Neden? Siz diyorsunuz ki herkese aynı temeli vereceğiz, sonra herkes istediği bölümü seçecek. Bir kere herkes mühendisliği seçer. Mühendislikten de herkes ya bilgisayar seçer veya elektroniği seçer. Mekatroniği falan kimse bilmez, seçmez. Ben de anlatmaya çalışıyorum. Sonra dediler ki "Sizin hatrımız için kabul edelim, ama 1 sene sonra geri geleceksiniz, vazgeçtik diyeceksiniz". Ama öyle olmadı, şimdi uzun yılların ortalamasına bakıyoruz. En fazla seçilen program bilgisayar değil, bilgisayar 5.-6. sırada. Çünkü biz öğrenciye sorumluluk verdik. "Düşün, taşın, ders al, bak, arkadaşlarıyla konuş, gel bizle konuş, tanıtım programlarına katıl. Ondan sonra da sen seçeceksin, kimse seçmeyecek." dedik. Bu öyle bir sistem ki öğrenciye büyük bir özgürlük veriyor, büyük de bir sorumluluk veriyor. Kendine karşı sorumluluk.

Öğrencilere Sabancı Üniversitesi'nde eğitime başlarken bilgi edinme amaçlı olarak hangi programı seçmek istediklerini soruyoruz. 2-3 sene sonra da seçtikleri programlarla kıyaslıyoruz. %48'i fikrini değiştiriyor. Bu demektir ki programları tanıyıp öğrenip ders aldıktan sonra öğrencilerin yarısı farklı mesleklerle yöneliyorlar, fevkalade önemli bir istatistik.

Rektörlüğüm sırasında mezun olacak öğrencilerle rektör evinde grup grup toplanıp konuşurdum. Ne yapmak istediklerini sorardım tek tek. Herkes bu sistemden çok memnun. Ama bazı anne-babanın şikayeti var. Ben çocuğumu size mühendis olacak diye yolladım, çocuğum kültürel çalışmalar programına gitti (gülüyoruz). Memnun mu hayatından? Çok memnun. Benim için önemli olan öğrencinin memnuniyeti. Çünkü bazı anne-baba çocuğum kendilerinin hayatlarını, yani anne-babasının hayatını yaşamasını ister. O çok yanlış bir görüş bence. Çünkü o kendi hayatını yaşayacak. 17 yaşında, 18 yaşında karar vermesini öğrenecek ve kendi hayatını yaşayacak.

Benim için hoş olan bir şey mezunlarımızın üniversitedeki, çalışma hayatındaki başarılarını duyuyorum. Müthiş bir şey. Kendilerine bir güven var ve haklı bir güven var. Bugün bizim ilk mezunlarımızdan 3 tanesi Amerika'da iyi üniversitelerde yardımcı doçent. Yönetim bilimlerinde doktora yapan bir mezunumuz doktorasını bitirmek üzereyken Hollanda'da bir üniversiteye post-doc olarak başvurdu. "Tezimin konusu şöyle, doktoramı bitirmek üzereyim, çalışma alanım da şöyle, sizde post-doc olarak çalışmak istiyorum" diye yazdı. Hollanda'dan gelen cevap şuydu: Maalesef sizi post-doc olarak alamıyoruz, buyrun yardımcı doçent olarak gelin (gülüyoruz). Bunlar çok güzel şeyler. Çalışma hayatına giren, kendi şirketini kuran, işini geliştiren insanlar bizim için çok çok önemli.

Türkiye'de maalesef bir çok üniversitenin, akademisyenin kötü bir huyu vardır. Ben 67 senesinde Amerika'daydım öğrenci olarak. O zaman zenci lider Martin Luther King'in Washington Anıtı önünde Amerika'daki ırk ayrımına karşı meşhur bir konuşması vardır. Zaten sonra da öldürüldü. "I have a dream" diye tekrarlayan, "Benim bir rüyam var, benim bir hayalim var, bir gün gelecek Amerika'da siyah-beyaz ayrımı yapılmayacak. Hatta bir gün gelecek bir siyah başkan bile olacak." diyordu. Obama'nın seçildiği gün aklıma o geldi. Şimdi maalesef bizde bir çok öğretim üyesi, bazı siyasilimiz ve bazı köşe yazarlarımız "I have a dream" demiyorlar, "I have a nightmare" diyorlar. Yani "Benim bir kabusum var". Herkesin kabusu da farklı sağolsun. Bunu gençlere sunmak çok yanlış bir şey. Yaşlı bir insanın hayal edebileceği

fazla bir şey yoktur, olmayabilir daha doğrusu. Ama bir gençin rüyası vardır, olmalıdır. Bizim işimiz üniversitede gençlerin hayallerini şekillendirmek ve gerçekleşmesi için onlara yardımcı olmak. Üniversitemizin amacı bu, başka bir şey değil. Dolayısıyla üniversite heyecanlı, mutlu belki de zaman zaman yaramaz (gülüyoruz) olabilecek insanların bir arada olduğu bir yerdir.

Son olarak şunu ekleyeyim. Şimdilerde çok azaldı, eskiden çok daha fazla vardı. "Biz okumuş insanlarız, aydın insanlarız, diğerlerine yol göstermemiz lazım, onlar bir şey anlamıyorlar, onlar anlamazlar" tarzı yaklaşımlar gösteriliyordu. Çok ayıp bir davranış bu, çok da yanlış. Çünkü insanların hele de Türkiye gibi zengin bir geçmişi olan coğrafyadan yetişmiş insanların bazen okul okumadan da edindikleri muazzam bilgiler var. Her şey sadece kitaptan okuyarak olmuyor.

Hocam bu güzel sohbet için çok teşekkür ederiz. Ufkumuzu açtınız. Ülkemiz sizin gibi insanlar sayesinde önemli kazanımlar elde etti. Gençler bu meşaleyi daha ileriye taşıyacaklardır.

Rica ederim. Daha ileriye taşıyacaklarından kuşku yok.

Torunuyla birlikte.



Çinili Köşk

“Gönül bir Sırça Saray’dır, kırılırsa yapılmaz” atasözünü duymuşsunuzdur. Peki nedir bu “Sırça Saray”, hiç merak ettiniz mi? Gönül kadar hassas, narin olan bu saray gerçekte var mıdır? Varsa acaba nerededir?

Sırça Saray, Topkapı Sarayı’nı çevreleyen ihtişamlı surların içinde bulunan, nadide mimarisiyle görenleri kendine hayran bırakan “Çinili Köşk”ün ta kendisidir. Osmanlı dönemine ait belgelerde bu şekilde anılmıştır.

Melahat PARLAR



Topkapı Sarayı Müzesi'nde bulunan ve 16. yüzyılda Saray Şehnamecisi Seyit Lokman'ın yazdığı, Nakkaş Osman¹ yönetimindeki bir ekip tarafından hazırlanan minyatürlerin² olduğu "Hünernâme"³ isimli eser ile binanın kitabesinden "Çinili Köşk"e "Sırça Saray" dendiği öğreniyoruz.

Bunun dışında duvarı kaplayan çini anlamına gelen "kâşi" kelimesinin kullanımıyla Kasr-ı Kâşi⁴ de denilmektedir. Niye o dönemde bu yapıya böylesine zarafet ve kırılabilirlik yükleyen bir isim verildiğini anlamak için o dönemde Bizans yapılarının büyük taşlardan oluşan görkemine dikkat etmek gerekir. O devasa sağlam görünümlü yapıların arasında girişi çinilerle süslü ve incelikli mimarisiyle bu yapı ismini o dönemde belki fazlasıyla hak etmişti.

İstanbul Arkeoloji Müzeleri kompleksinin sergi alanlarından biri olan Çinili Köşk; kapısındaki çini kitabeye göre 1472 yılında Fatih Sultan Mehmet tarafından Selçuklu üslubunda yaptırılmış, Osmanlı sivil mimarisinin İstanbul'daki en erken örneğidir. Mimarı bilinmemektedir.

Aslında o dönemde Sultan'ın bu bölgede Çinili Köşk'ten başka 2 tane daha köşk yaptırdığı biliniyordu. Osman Hamdi Bey, Arkeoloji Müzesi'nin yapımındaki temel kazılarında bulunan kalıntıların bu köşklere ait olduğunu tahmin etmiştir. Üçüncü köşk hakkında ise şimdiye kadar hiçbir iz çıkmadı.

Av köşkü olarak yapıldığına dair gerçek olmayan görüşler vardır. Bina konaklamak üzere kullanılmamıştır. Fatih Sultan Mehmet, İstanbul'un bir numaralı tepesi olan "Zeytinlik Tepesi"ne saray kompleksi yapmaya başlamıştı. Çinili Köşk de kompleksin tamamlayıcı binalardan biri olmak üzere korunaklı bir yapı olarak inşa edilmiştir.



Köşkün girişi.

¹ 16.yy ikinci yarısında saray baş minyatürcüsü.

² Çok küçük boyutlu ince işlenmiş resim sanatı. Daha çok kitap süslemelerinde kullanılmıştır.

³ Birinci cildinde Osmanlı soyu, ikinci cildinde Fatih Sultan Mehmet'in hayatı anlatılır.

⁴ Duvarda kullanılan çini.

Köşk, konumu itibariyle tarihte birçok olaylara şahitlik etmiştir. Nitekim Hünernâme'de bulunan minyatürlerde gösterildiği üzere binanın önünde bulunan "Kum Meydanı", "Ağa Vekili Bahçesi" veya "Kalfa Yeri" olarak tanımlanan alanları görmesinden dolayı birçok tarihsel olaya tanıklık etmiş olmalıdır. Padişah ve yakınlarının Kum Meydanı'ndaki binicilik, cirit, güreş, tomak⁵ gibi spor karşılaşmalarını seyrettiği aynı eserde anlatılmaktadır. Bunun dışında Hac zamanında "Surre⁶ (Surra) Alayı"nın yolculanması, sultanların "Kılıç Alayları"na gidişleri de binanın revakından⁷ seyredilmiştir.

Sonraki dönemlerde ne amaçla kullanıldığı bilinmeyen köşk 16. yüzyıl sonunda darphane olarak kullanılmıştır. Bazı zamanlar da saray halkının kullanımına tahsis edilmiştir. 1880'de Müze-i Hümayûn olarak ziyarete açılmasından ardından 1981 yılında İstanbul Arkeoloji Müzeleri'ne bağlanıncaya kadar çoğunlukla müze olarak kalmıştır. Tarihinde birkaç defa tadilat ve restorasyondan geçmiş, atlattığı yangının izleri silinmeye çalışılmıştır.

Günümüzde bina üzerinde görebileceğiniz çinilerin mozaik⁸ tekniğinde kullanılmış örnekleri bulunmaktadır. Diğer yapı süsleme sanatları (revzen, malakari, künde-kari, yıldız vb.) ile nadide çini ve seramik örneklerini bu ihtişamlı yapıda bir arada görebilirsiniz.

Binanın Temel Mimarisi

İki katlı taş bir bina olarak inşa edilen köşk, merkezi sofa etrafında tonozlarla⁸ kapatılmış dört eyvan⁹ ile köşelerde birer odadan oluşur. Arka cephede de köşeli bir oda vardır. Merkez sofa ve odaların üstü kubbe ile örtülüdür. Yapımında beyaz köfeki¹¹ taşı, yan ve arka cephede kırmızı tuğla dolgular kullanılmıştır. 2 katlı kareye yakın bir plana sahiptir. Arkeoloji Müzeleri avlusu tarafından tek katlı, Gülhane Parkı tarafından ise 2 katlı olarak görülmektedir. Yapıldığında revak ahşap iken I. Abdülhamit devrinde 1737'de yandıktan sonra 14 sütunlu mermer revak haline dönüştürülmüş. Müze olarak kullanılmaya karar verince de sağ ve sol eyvanlar demir şebeke ve cam ile kapatılmıştır.

⁵ İp ucuna bağlı meşin topla rakibin sırtına vurarak puan alma suretiyle oynanan eski türk sporlarından.

⁶ Osmanlı İmparatorluğu'nun Mekke-Medine halkına hediyeler götürme alayına denir.

⁷ Bkz. sayfa 164.

⁸ Küçük, birbirinden farklı, üç boyutlu parçaları bir yüzey üzerinde yan yana getirerek resim oluşturma tekniği.

⁹ Mimarlıkta kemerlerin bir araya gelmesiyle oluşturulan, genellikle tavan örtüsü olarak işlev gören yapı parçası.

¹⁰ Üç tarafı ve üstü kapalı, bir tarafı bütün genişliği ile bir avluya ya da diğer bir mekana açılan yapı birimi.

¹¹ İnşaatta kullanılan açık renkli, delikli ve hafif, işlenmesi kolay zamanla sertleşen bir çeşit taş.



Kubbeden bir görünüm.

Bina Süslemeleri

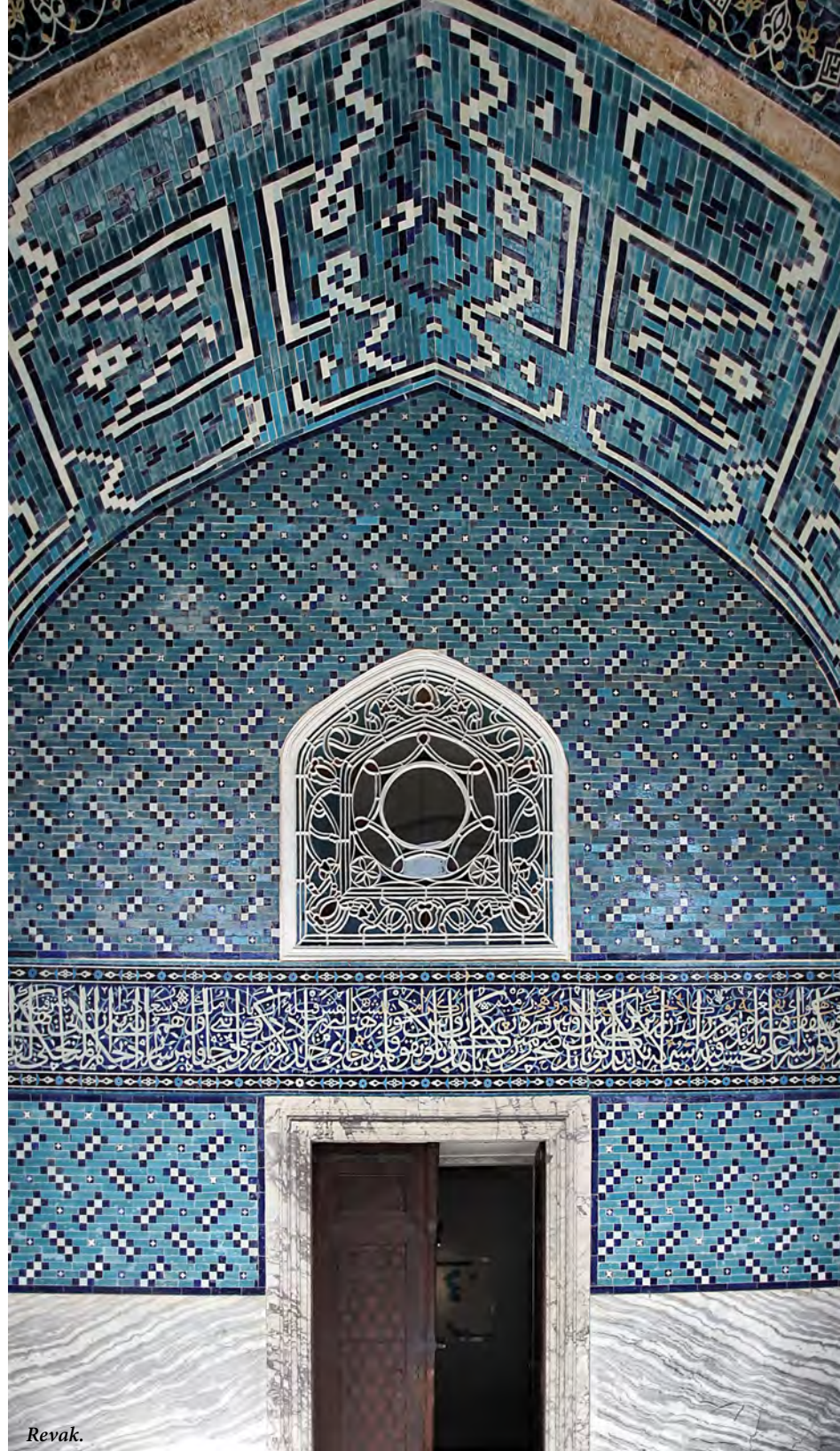
Binanın dikkati çeken bölümlerini ve süslemeleri incelediğimizde birçok Türk bezeme sanatlarını ile tanışmış oluyoruz. Çini, künde-kari, malakari, revzen, hat bunlardan bazıları. Şimdi tek tek binanın parçalarını gözden geçirelim ve süsleme şekillerini keşfedelim.

Revak

Bir binanın en önemli kısmı, konuklarını karşılayan girişidir. İnsanlarla ilk karşılaştığımızda bizde birtakım izlenimler bırakırlar. Binalar hakkındaki görüşlerimiz de böyle oluşur. Bu bakımdan Çinili Köşk, ziyaretçiyi ilk görüşte etkileyecek özelliklere sahiptir. Giriş kapısının ile eyvan kemerinin üstünü süsleyen mozaik çiniler Selçuklu üslubunda yapılmıştır. Firuze, mor, beyaz ve lacivert renkli mozaik çinilerle oluşturulan renk uyumu ileri bir süsleme zevkini yansıtır.

Kapının üst kısmındaki mozaik frizde¹² nesih-sülüs hatla iki satır halinde yazılmış Farsça kitabe bulunur. Kitabede, köşkün yapımının 1472 Eylül ayı sonunda bittiği ve o zamanda içinde bulunduğu doğanın güzelliği anlatılmaktadır. Kitabenin üzerinde 18. yüzyılda takılan ancak bozulduğu için orijinalinden yeniden üretilen alçı çerçeveli revzen¹³ bulunmaktadır.

Eyvan kemerinde küfi hatla “Tevekkülüm Yaradan’ımadır” yazar. Eyvanın kenar bordüründe ise “Allah” ve “Muhammed” kelimeleri dönüşümlü olarak yer alır. Ayrıca bunların arasında “La ilahe illallah” ve “Muhammedün Resulullah” yazılı iki pafta bulunur.



Revak.

¹² Bir iç duvarın üst bölümünde yapılan süsleme kuşağı.

¹³ Osmanlı mimarisinde vitray, revzen olarak bilinir. Revzende vitraydan farklı olarak renkli camlar kurşun şerit yerine alçı çerçevelerle birleştirilir.

Kapı

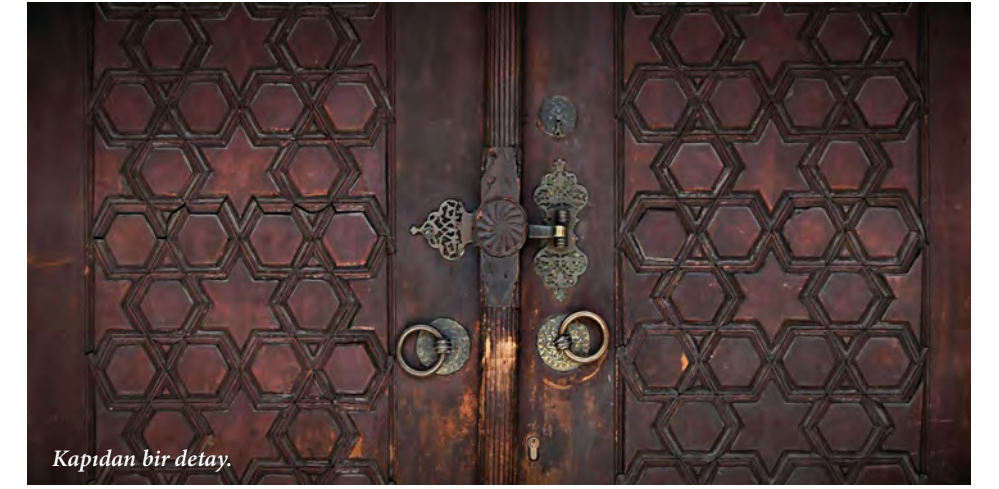
Geniş ahşaptan bir kapı binanın tam ortasında misafirleri karşılar. Kapının alt bölümleri künde-kari¹⁴ tekniğinde süslenmiş altıgenler ve altı köşeli yıldızlarla kaplıdır. 18. yüzyılda geçirdiği yangın sonrası (günümüzde kullanılan) bu kapı kanatları Fatih Semaniye Medreseleri'nden Çifte Kurşunlu'nun dershanesinden getirilmiştir. Kapının üst bölümünde bir kitabe dikkati çeker. Kitabe alçak oyma¹⁵ tekniğinde küfi¹⁶ ve nesih¹⁷ hatla¹⁸ yazılmış, rûmili¹⁹ kıvrımlarla süslenmiştir. Ancak kitabenin içeriğine dair bir bilgi bulunmamaktadır.

Çeşme

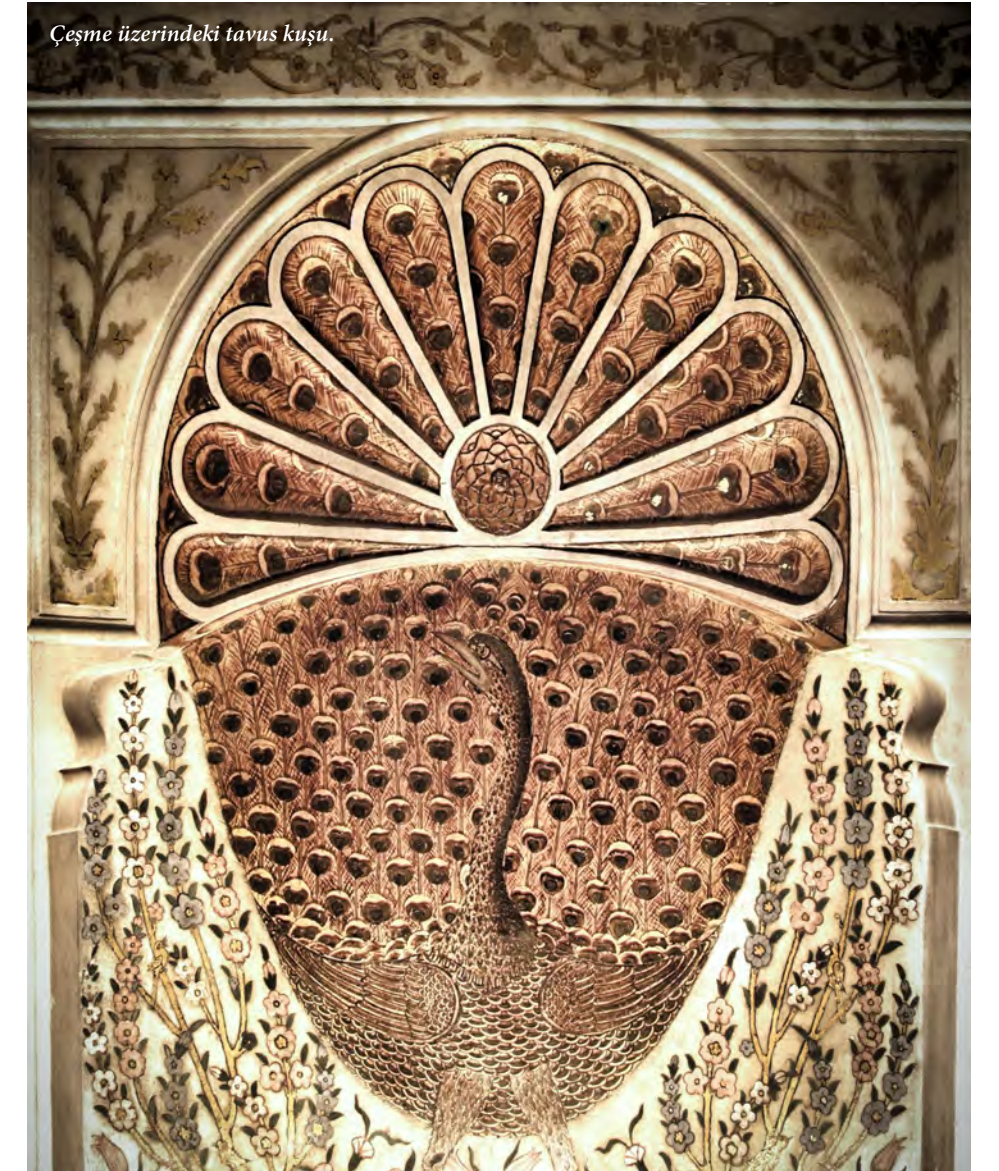
Köşkün odalarından birinin nişi²⁰ Kanuni'nin torunu III. Murad zamanında selsebil tarzında çeşmeye dönüştürülerek çevresindeki sarnıçlara bağlanmıştır. Çeşmenin ayna taşı bahar dalları içinde güzel bir tavus kuşu süsler. Tavus kuşu “cennet kuşu” olarak da bilinir. Kuş figürleri kültürümüzde Orta Asya'dan beri süslemelerde kullanılan en yaygın motiflerden biri olmuştur. Köşkte sergilenen eserlerde de bol miktarda kuş figürleri ile karşılaşmak mümkündür.

Çeşmenin yan duvarlarındaki mermer kitabede (talik²¹ hatla yazılmış) çeşmenin 1590 tarihinde yapıldığını ve buraya “Sırça Saray” dendiğini öğreniyoruz. Çeşmenin karşısında ise çeşmenin arka planda betimlendiği Osman Hamdi Bey'in “Ab-ı Hayat²² Çeşmesi” isimli tablosunun posterisi yer alır.

Çeşmenin bulunduğu odanın duvarlarında kalem işi tekniği ile yapılmış altın yıldız süslemeler de dikkati çeker. Ancak ne yazık ki bu süslemelerin restorasyonu olması gerektiği gibi fırça ile yapılmamıştır. Bu sebeple suni bir görüntü oluşmuştur.



Kapıdan bir detay.



Çeşme üzerindeki tavus kuşu.

¹⁴ Sekizgen, baklava ve yıldız biçiminde şekillerden oluşan, içi arabesk kabartmalı ahşap parçalarla birbirine bağlayan oluklu ahşap girişler içine geçerek bağlanan bir çatma tekniği.

¹⁵ Diğer adı “alçak kabartma usulü”dür. İstenen ve tasarlanan biçim ve şekiller sert bir aletle herhangi bir maddenin üzerine oyarak yapılır.

¹⁶ Düz ve köşeli çizgilerle geometrik biçimlere indirgenerek yazılan eski bir Arapça yazı şeklidir. 8.yy'da Kufa'da ortaya çıkmıştır.

¹⁷ Özellikle Osmanlılar tarafından yazmalarda kullanılan, yumuşak, köşeleri yuvarlaklaşmış, işlek bir yazı türü.

¹⁸ Arap harfleri ile yapılan, genellikle dekoratif amaçla kullanılan güzel yazı yazma sanatı ve görsel sanat türü.

¹⁹ Selçukluların kullandığı bir bezeme tarzıdır ve yaprağa benzer bir şekil adır.

²⁰ Mimari yapılarda duvar içinde bırakılan boşluk.

²¹ Yatık olarak yazılan Arapça yazı türüdür. 16.yüzyılda İran'da ortaya çıkmıştır.

²² İçene ölümsüzlük kazandırdığına inanılan efsanevi su.

Kubbe

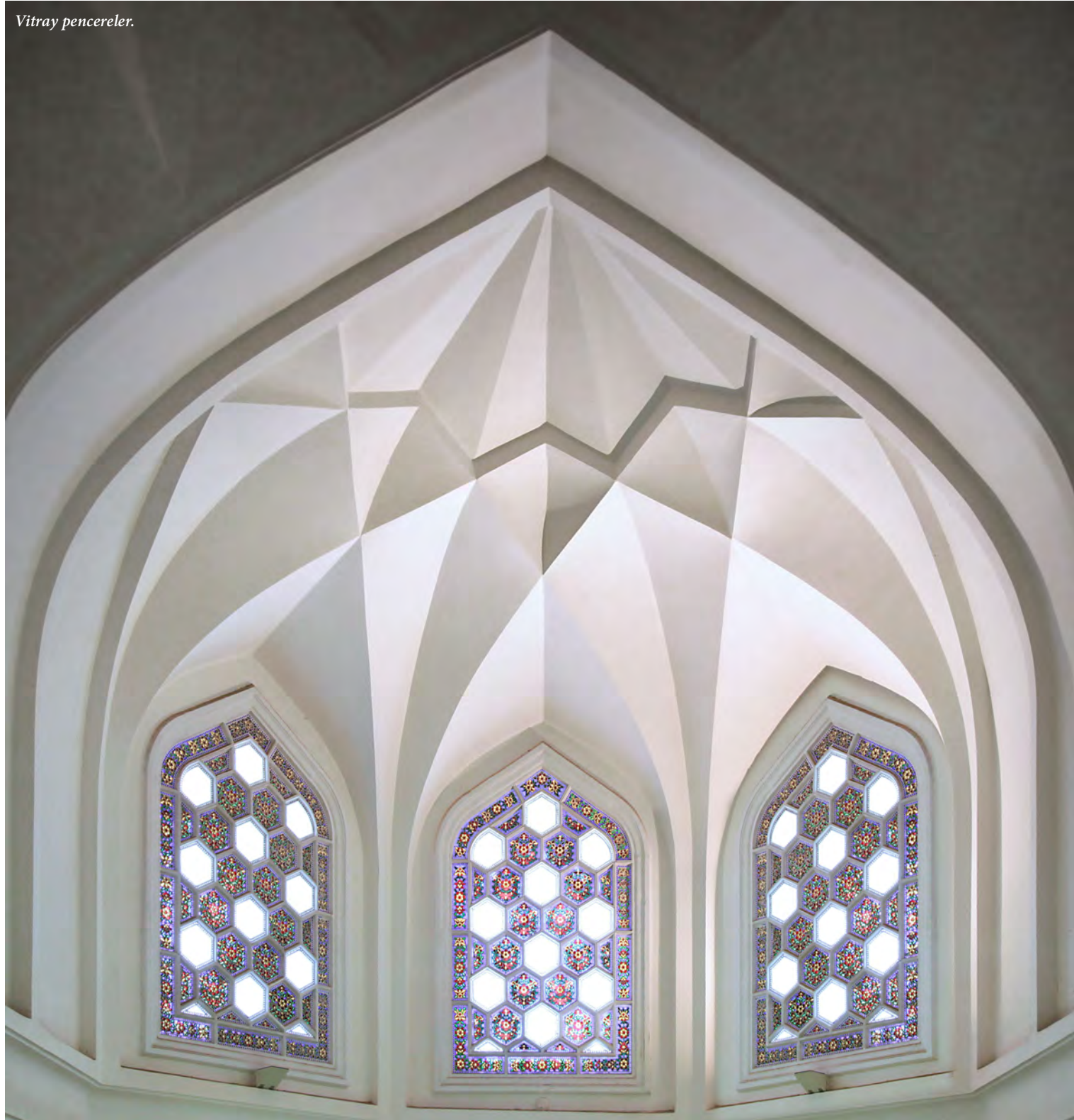
Kubbeye malakari süsleme yapılmıştır. Malakari, mala benzeri küçük aletlerle tavan ve duvarlara uygulanan alçı kabartma süslemesidir. Bu süsleme aynı zamanda boya ile renklendirilebilir. Geleneksel bir sanat olan malakari süslemeyi el ile yapılan kartonpiyere benzetebiliriz.

Bodrum kattaki orijinalliyini koruyan malakari kubbe beyaz renktedir. Sergileme katındaki kubbede görülen süsleme ise restorasyon sırasında renklendirilmiştir.

Pencereler

Binanın aydınlatması için bolca pencere kullanılmıştır. Pencereler renkli ışıltıları ile iç mekâna hoşluk veren vitraylardan oluşur. Ayrıca iç mekânlarda havalandırma sağlamak üzere açık pencere yapısı kullanılmıştır. Bu pencereler, karşıdan bakıldığında ilk anda duvar izlenimi vermektedir. Fakat aynı düzlemde olmayan duvarların aralarında boşluk bırakılarak pencere görevi görmesi sağlanmıştır.

Vitray pencereler.



Sergileme

Çinili Köşk Müzesi'nde sergilenen eserler, 11. yüzyıldan 20. yüzyıl başlarına kadar tarihlenen Selçuklu ve Osmanlı dönemlerine aittir. Toplam 142 adet eser bulunmaktadır. Selçuklu, Slip ve Milet, İznik, Kütahya ve Çanakkale olmak üzere 4 sergileme grubuna ayrılmıştır.

Selçuklu grubunda 11-13. yüzyıl İran ve Anadolu Selçuklularına ait çini ve seramiklerin sırlı-sırsız örnekleri sergilenmektedir. Konya'daki II. Kılıç Arslan Köşkü'ne ait 12. yüzyıla tarihlenen minai²³ tekniğindeki çiniler köşkün önemli ve az sayıdaki eserlerindedir. Kazıma ve slip tekniklerinin bir arada kullanıldığı bir kâse de dikkati çekmektedir. Bunların yanı sıra matara ve ibrik sergide bulunan diğer formlardandır.

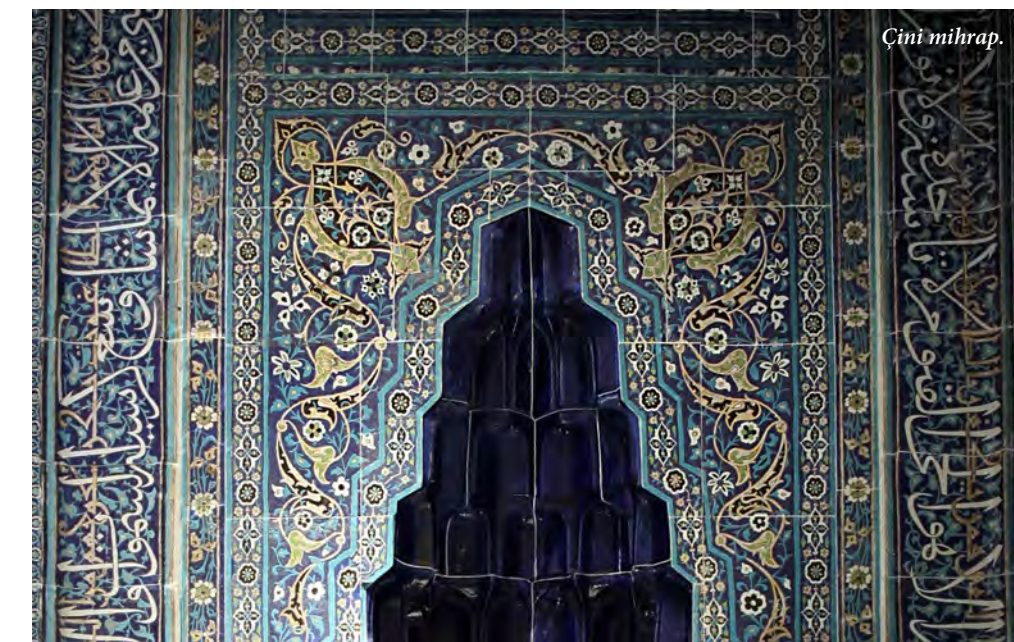
Sergi salonlarında bulunan Osmanlı dönemi eserlerinden önemli bir kısmı 14.yüzyılın ortalarından 17. yüzyılın sonlarına kadar Anadolu'da en önemli çini ve seramik merkezi olan İznik'te üretilmiştir. 14-15. yüzyıla tarihlenen slip ve Milet işi seramiklerin sergilendiği eyvanlı mekân, erken Osmanlı sanatını yansıtan az sayıda ancak önemli bir grup eseri barındırmaktadır.

1432 tarihli Karamanoğlu İbrahim Bey İmareti'ne ait "çini mihrap" merkezi salonda bulunur. Mihrap, bitkisel ve geometrik bezemeli, altın yıldızlı çini levhalardan oluşmaktadır. Kitabesinde Bakara Suresi'nin 255. ayeti nesih hatlarla, 256. ve 257. ayetleri de kufi hatlarla yazılıdır.

Ayrıca 1540 tarihli İstanbul Haseki²⁴ Hürrem Sultan Medresesi'ne ait pencere alınlıkları da bu mekânda sergilenmektedir.

Kütahya yapımı eserlerde bitkisel, geometrik motiflerle insan ve hayvan figürleri çok canlı bir şekilde betimlenmiştir. Berrak ve parlak yeşil, turuncu, mavi, lacivert ve kırmızı ile birlikte bol miktarda limon sarısı dikkati çeker. Ayrıca eserlerin formları arasında matara, gülabdan²⁵, şerbet süzgeci, tütsü kabı gibi değişik kullanım amaçlarına uygun tasarımlar görülebilir.

Çanakkale sergisinde ise gemi, köşk, cami tasvirlerinin kullanıldığı tabakların yanı sıra Bektaşî kavuğu, tavuk ve civcivli, halka gövdeli ilginç formlu testiler dikkati çeker. Yakın tarihlere kadar fazla tanınmayan Çanakkale seramiklerinin yurt dışındaki müze ve özel koleksiyonlarda sergilenen çeşitli ve ilginç örnekleri bu konuya ilgiyi arttırmaktadır.



Çini mihrap.

Zürafa Motifli Tabak

19. yüzyıl ikinci yarısına tarihlenen tabak üzerinde yer alan zürafa motifli ile dikkat çekicidir. Boynundan iplerle bağlı olarak gösterilmiştir. İstanbul'a saray hayvanat bahçesine konmak üzere gemilere yüklenmiş zürafanın Çanakkale'de mola verildiğinde seramik ustalarına esin kaynağı olduğu tahmin edilmektedir.



Zürafa motifli tabak.

Cami-Mescid Betimli Tabak

Tabak üzerinde dönemeçli bir yolun alt ve üst ucunda yer alan sarı kubbeli ve beşer minareli iki cami ve arada iki minareli mescid dikkati çeker. 18. yüzyıl sonu - 19. yüzyıl başına tarihlenmektedir.



Cami-mescid betimli tabak.

Süs (Askı) Topları

Yumurta ve küre biçimli süs topları, kendileri üzerine gelecek şekilde kandille aynı veya ayrı bir zincirle asılır. Hacıların yanında getirdikleri devekuşu yumurtaları da aynı amaçla kullanılıyordu. Üstleri melek figürleriyle (kerubin) bezemeli olanlar ise Kütahya'dan Kudüs'e giden hacılar tarafından hangi kiliseye vakfedilmişse oraya süs eşyası olarak asılmaları için yapılmıştır.

²³ Sır altı ve sır üstü tekniklerinin bir arada kullanıldığı çini türüdür. Sır altında; mavi, firuze ve yeşil, sır üstünde; beyaz, kahverengi, siyah ve kırmızı renkler kullanılır.

²⁴ Osmanlı haremde padişaha çocuk doğuran kadın efendilere verilen unvan.

²⁵ Gülsuyu dökmek için kullanılan armut biçimli kap.

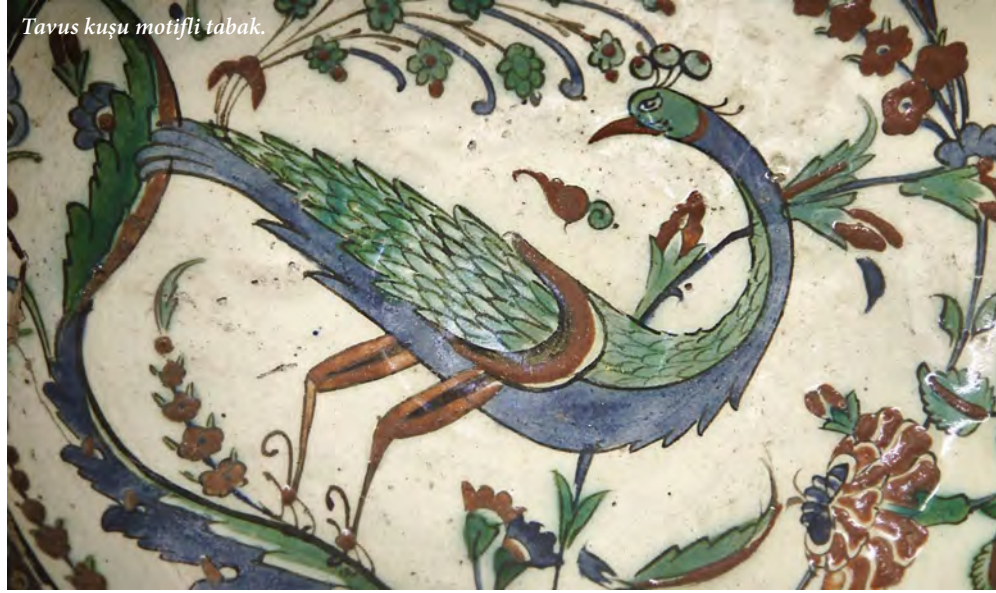
Kapaklı Kase

18.yüzyıl ilk yarısında yapılan kâse, şeffaf sır altına çok renk bezemelidir. Beyaz zemin üzerine kırmızı, sarı, mavi ve yeşil renkler kullanılarak çiçek motifleriyle süslenmiştir. Özellikle limon sarısı dikkat çekicidir.



Kapaklı kase.

Tavus kuşu motifli tabak.



Tavus Kuşu Motifli Tabak

Tabak üzerindeki tavus kuşu motifinde başını geriye atmış, gövdesi ile başı mavi-yeşil, ayakları, kanadı ve gagası kiremit kırmızı ile süslüdür. Çevresinde stilize bulut ve dalga motifleri kullanılmıştır.

Pencere Alınlığı

İznik yapımı eser, Haseki Hürrem Sultan Medresesi'ne aittir. Lacivert zemine beyaz celi sülüs hatla bir ayet yazılmıştır.

Mavi-Beyaz Cami Kandili

II. Beyazıt Türbesi'nden gelen cami kandilidir. 1510-1510 olarak bilinen yapım zamanında beğenilerek eserler üzerine uygulanan paftaların içine "Allah, Muhammed, Ali" yazılmıştır. Rûmiler, hatayiler, düğümlü Çin bulutu kıvrımları, örgülü küfi hatlı madalyonlar sıralanır. Dip kısmında meandr süsleme dikkati çeker. Meandr, zigzag şeklinde süregelen bir desen şeklindedir.



Pencere alınlığı.

Figürlü Çini Parçası

Minai tekniğinde bezemeli beş parçadan oluşan figürlü çini parçası, 12. yüzyıl ikinci yarısında yapıldığı tahmin edilmektedir. Sekizgenler ve dört kollu yıldızlar şeklinde bir düzenleme olduğu, sekizgenlerin birinin içinde ise elinde doğan tutan bir atlı avcı görülmektedir. Bindığı at ve koşum takımı ayrıntılarıyla görülmektedir. Konya II. Kılıç Arslan Köşkü kalıntılarında bulunmuştur.



Figürlü çini parçası.

Selçuklu Tabak

13. yüzyıla tarihlenen Aksaray-Niğde menşeli tabak, filizi yeşil zemine kazıma (sgraffito) ve geniş oyma (champleve) tekniğinde bezemelidir. Ortasında karşılıklı iki büyük kuşun kanatları arasında üç küçük kuş görülmektedir. İyi bir ışıkta görünen tabak saray için sipariş edilmiş olmalıdır.



Selçuklu tabağı.

Dergimizin bu sayısında sizlere Çinili Köşk'ü gezerek tarih ve sanat molası vermek istedik. Umarım yazımızı beğenir ve köşkü kendi gözlerinizle görmek istersiniz.

Anadolu tarihine, çini-seramik ve yapı süsleme sanatlarına farkındalık yaratmayı amaçlayan bu yazıya katkı ve yardımlarından ötürü İstanbul Arkeoloji Müzeleri müdür yardımcısı Tuğçe Akbaytogan'a ve Çinili Köşk sorumlusu arkeolog Nilüfer Aydın'a için çok teşekkür ederiz.

Dilim Desenli Tabak

1490-1500 yıllarına ait tabakta metal eserlerden etkilenerek yapılan dilim motifli görülmektedir. Bunun dışında hatayili, rumili kıvrım dallar görülmektedir.



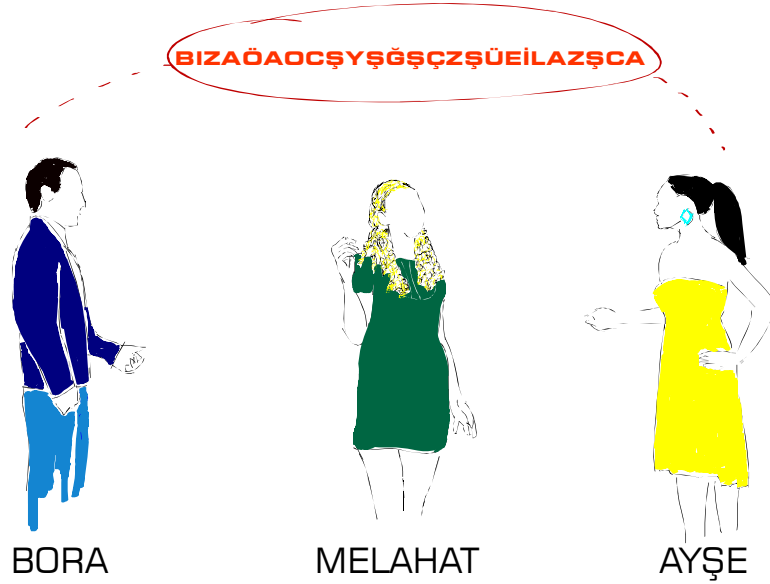
Dilim desenli tabak.

KAYNAKÇA

[1] A. Pasinli ve S. Balaman, "Türk Çini ve Keramikleri, Çinili Köşk", A Turizm Yayınları, İstanbul, 1992.

[2] N Aydın, "Çinili Köşk Müzesi" İstanbul, 2007.

soru 13



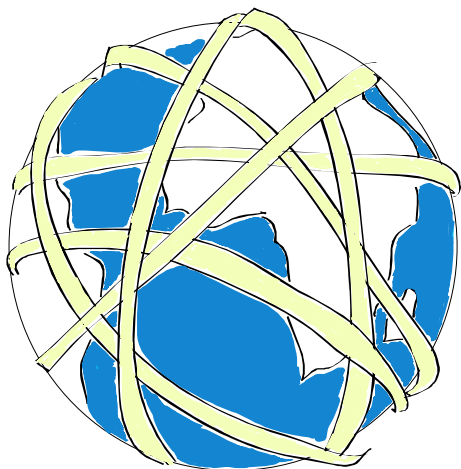
Ayşe ile Bora bir şifreleme sistemi kullanarak haberleşiyorlar. Açık ve gizli yazılarında yalnızca alfabemizin büyük harflerini kullanıp, noktalama işareti, boşluk, rakam vb. kullanmıyorlar. Melahat ise onların ne konuştuklarını öğrenmek istiyor. Uzun zaman yaptığı gözlemler sonucu, şu bilgileri ediniyor:

- Her ayın 1. gününde, Ayşe ile Bora şifresiz (doğrudan açık yazılarını iletirerek) haberleşiyorlar.
- Kullandıkları şifreleme sistemi, yalnızca, artık olmayan yılların Şubat aylarının her bir gününde (1. gün dışında her gün) ayrı bir anahtar kullanabilecek kapasitededir. Diğer aylarda, bazı günler, kullanılan anahtar aynı olmaktadır.
- Melahat, bu ikili arasındaki tüm haberleşmeyi dinlediği bir gün, Ayşe'den Bora'ya, ve Bora'dan Ayşe'ye olan birçok şifreli iletinin en başında: BIIÖACA ... dizisini görmüştür. Aynı gün, Melahat: BIZAÖAOCŞYSŞĞŞÇZŞÜEILAZŞCA şifreli iletisini gözlemlerse ne yapmalıdır?

soru 14

Açık Yazı	Gizli Yazı
MILLİKRIPTOLUCEPTELEFONU	MKİLROPLİLİPUTFOECTELNUEA
?	İRMZYİŞMAAGZGTKAÜİEİLLRTNEÜMİEPSİHA

soru 15



Alman matematikçi Georg Cantor (1845-1918), aşağıdaki sanıyı (conjecture) öne sürmüştür:

$$p_0 = 2, p_{n+1} = 2^{p_n} - 1$$

kuralına göre oluşturulan tüm $p_i, \forall i$ sayıları asaldır.

- $p_1 \cdot p_2 \cdot p_3$ sayıları asal mıdır?
- p_5 sayısının on tabanındaki yazılışının yeterli uzunluktaki kağıttan bir şeride (şeridin kalınlığı önemsizdir), bir milimetreye bir rakam düşecek şekilde yazıldığını varsayalım. Oluşacak kağıt şerit dünyanın ekvatordaki çevresine sarılırsa kaç tam tur yapar? (Dünyanın ekvatordaki yarıçapını 6378,14 km alınız, $\pi = 3.14$)

soru 16

6, 1, 8, 0, 3, 3, 9, 8, 8, 7, 4, 9, 8, 9, 4, ?

soru 17

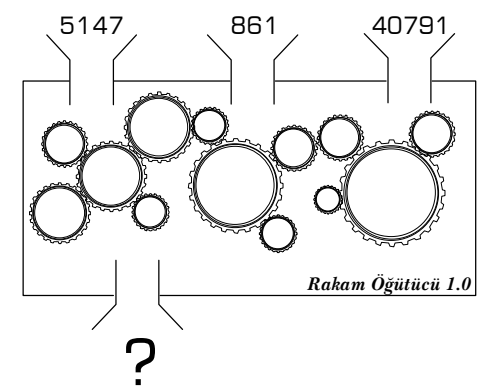
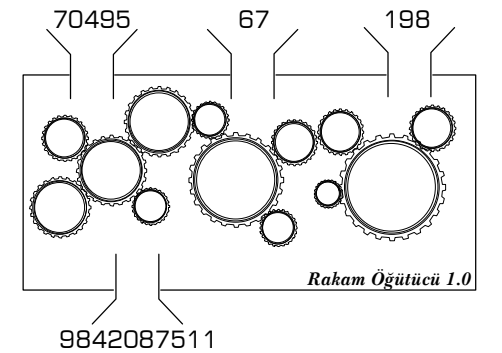
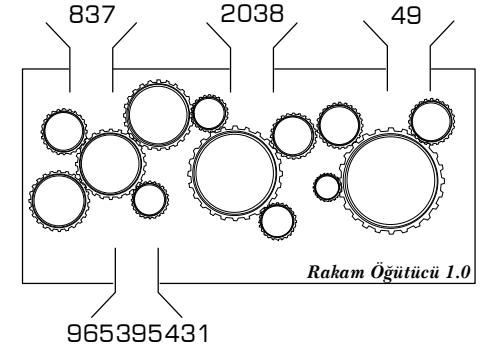
KRİPTO CİHAZLARI GENELLİKLE KOLAY ERİŞİLEMEYEN FİZİKSEL GÜVENLİĞİ SAĞLANMIŞ YERLERDE MUHAFAZA EDİLİR VE SINIRLI SAVIDAKİ YETKİLİ KİŞİLERİN CİHAZA MÜDAHALE ETMESİNE İZİN VERİLİR. BU NEDENLE KRİPTO CİHAZLARININ MÜMKÜN OLDUĞUNCA AZ KULLANICI MÜDAHALESİ GEREKTİRECEK BİÇİMDE ÇALIŞMASI VE BUNA UYGUN TASARLANMASI ÖNEMLİDİR. EĞER BİR SİSTEMDE ÇOK SAVIDA KRİPTO CİHAZI KULLANILACAK İSE İŞLETME KOLAYLIĞI BAKIMINDAN KRİPTO CİHAZLARININ UZAKTAN YÖNETİM FONKSİYONLARININ DA OLMASI GEREKMEKTEDİR. BU DURUMDA UZAKTAN YÖNETİM FONKSİYONLARI İÇİN GEREK YÖNETİM MERKEZİ OLARAK TASARLANAN CİHAZLARDA GEREKSE KRİPTO CİHAZLARINDA PEK ÇOK EK GÜVENLİK ÖNLEMLERİNİN ALINMASI LAZIMDIR. AYNI ŞEKİLDE YETKİSİZ KULLANICILARIN CİHAZA MÜDAHALELERİNİN ENGELLENMESİ AMACIYLA KRİPTO CİHAZI ÜZERİNDE ÇEŞİTLİ TEDBİRLER ALINIR.

(Alıntı: UEKAE Dergisi, Sayı: 2, Sayfa: 16, "Kripto Cihazı Tasarlamak")

Yukarıda verilen paragrafa göre,

- Kelimelerin başında yer alan harflerden (ör. CİHAZLARI), en sık geçen 3 harf hangileridir?
- Kelimelerin sonunda yer alan harflerden (ör. CİHAZLARI), en sık geçen 3 harf hangileridir?

soru 18



ŞİFRESAYAR

Umut ULUDAĞ

cevap7

1204 asır

Şifrelerin karakterlerinin seçilebileceği K kümesinde, 29 büyük harf, 29 küçük harf, ve 10 rakam vardır. Yani, K'nın toplam eleman sayısı 68 dir. Olası toplam şifrelerin sayısı ise,

$$68^8 = 457163239653376$$

dir. Her vatandaşımız haftada 1 şifre kullanacağından, tüm Türkiye nüfusu için, 1 yılda

$$73000000 \cdot 52 = 3796000000$$

şifre gereklidir. Bir asırda (yüz yıl), ise

$$3796000000 \cdot 100 = 3,796 \cdot 10^{11}$$

şifre gerekli olacaktır. Olası toplam şifre sayısını, bir asırda gereken şifre sayısına bölersek, tüm şifrelerin yetebileceği asır sayısını yaklaşık

$$\frac{457163239653376}{3,796 \cdot 10^{11}} \approx 1204$$

olarak buluruz.

cevap8

- (i) A, E, İ, L
(ii) J, P
(iii) C, F, H, Ö, V

A	B	C	Ç	D	E	F	G	Ğ	H
37	12	2	4	17	42	2	6	9	2
I	J	K	L	M	N	O	Ö	P	
24	44	0	21	40	13	21	10	1	0
R	S	Ş	T	U	Ü	V	Y	Z	
27	7	6	16	9	7	2	6	11	

6 cümle, 58 kelime, 398 harften oluşan bu paragraftaki harflerin sayısal dağılımı şöyledir:

Bu dağılım tablosundan yukarıda verilen cevaplara kolayca ulaşılır.

cevap9

KENDİ İŞLETİM SİSTEMİMİZ PARDUS

Açık yazılar, verilen anahtarlar kullanılarak, Vigenere (Gronsfeld) sistemiyle gizli yazılara dönüştürülmüştür. Şöyle ki, "ELEKTRONİK HARP" açık yazısındaki her harf, periyodik olarak tekrar eden 41470 (bu anahtar BİLGEM'in posta kodudur) anahtarında belirtildiği gibi ötelenerek:

E	L	E	K	T	R	O	N	İ	K
+4	+1	+4	+7	+0	+4	+1	+4	+7	+0
H	M	H	R	T	U	Ö	R	Ö	K
H	A	R	P						
+4	+1	+4	+7						
K	B	U	V						

verilen gizli yazı bulunur.

M	İ	Ö	İ	M					
-2	-6	-2	-6	-4					
K	E	N	D	İ					
P	T	M	E	T	K	S			
-8	-1	-1	-0	-0	-2	-6			
İ	Ş	L	E	T	İ	M			
T	O	Ü	C	F	N	İ	M	K	E
-2	-6	-4	-8	-1	-1	-0	-0	-2	-6
S	İ	S	T	E	M	İ	M	İ	Z
S	F	U	J	Ü	Ş				
-2	-6	-4	-8	-1	-1				
P	A	R	D	U	S				

Dolayısıyla, verilen gizli yazıdan açık yazıya ulaşmak için, verilen anahtar (2626481100, ki bu anahtar da BİLGEM'in faks numarasıdır) periyodik olarak yukarıdaki gibi tekrar ettirelim.

Aradığımız açık yazıya ulaştık!

cevap10

2, 3, 5, 7, 11, 23, 29, 41, 43, 47, 61, 67, 83, 89, 101, 113, 131, 137

Dizinin kuralı: Rakamlarının toplamı bir asal sayı olan asal sayılar yazılmıştır. Bu özelliğe uyan sıradaki asal sayı, rakamları toplamı 11 olan 137' dir.

cevap11

(i) Verilen teorem 2, 3, 5, 7, 11 için doğrudur (gösterim aşağıdadır)

(ii) Çok büyük sayılarla hesaplama gereksinimi dolayısıyla pratikte bu teorem bir asallık testi olarak kullanılamaz.

İlk 5 asal sayı için teoremi deneyelim:

$$2: (2-1)! = 1! = 1 = -1 \pmod{2}$$

$$3: (3-1)! = 2! = 2 = -1 \pmod{3}$$

$$5: (5-1)! = 4! = 24 = -1 \pmod{5}$$

$$7: (7-1)! = 6! = 720 = -1 \pmod{7}$$

$$11: (11-1)! = 10! = 3628800 = -1 \pmod{11}$$

Böylece, teoremin ilk 5 asal sayı için doğru olduğu bulunur (bu teoremin ispatı birçok kaynakta mevcuttur, ör. M. R. Schroeder, *Number Theory in Science and Communication*, 3. Ed., Springer, 1997).

Bu teoremi bir asallık testi olarak kullanmak istediğimizi varsayalım, ve RSA benzeri algoritmalar için aslında çok küçük olacak 1000003 sayısı için yukarıdaki deneylerin benzerini uygulamaya çalışalım:

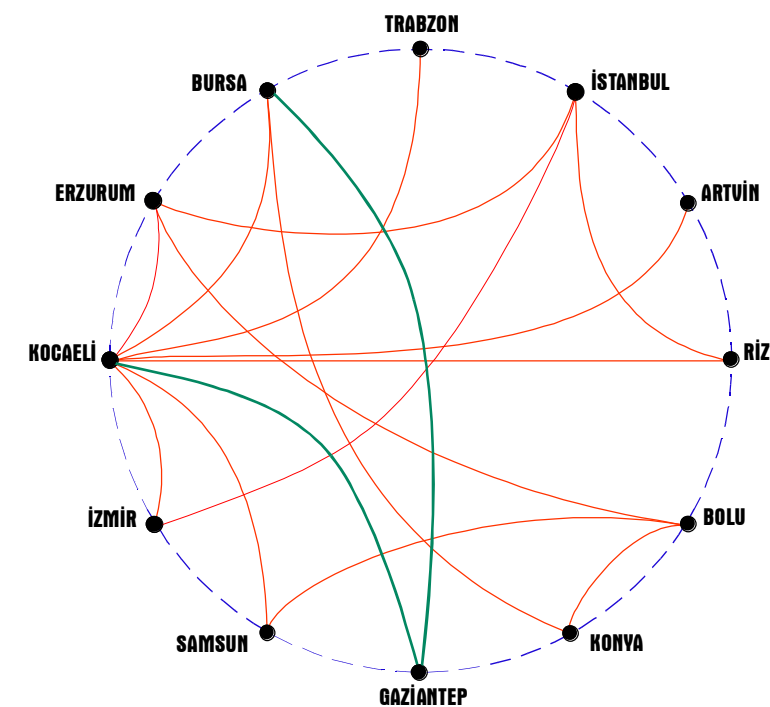
$$1000003: (1000003-1)! = 1000002! = ? \pmod{1000003}$$

1000002! sayısının ne kadar büyük bir sayı olduğunu görebilmek için, Stirling yakınsama kuralını kullanalım:

$$1000002! \approx \sqrt{2 \cdot \pi \cdot 1000002} \cdot \left(\frac{1000002}{e}\right)^{1000002} \approx 1,6 \cdot 10^{5565721}$$

Görüyoruz ki, asimetrik şifreleme ölçeğinde çok küçük olan 1000003 sayısının bile asal olup olmadığını bu testle belirlemek için, yukarıdaki 5.565.722 basamaklı sayıyı hesaplamak gerekmektedir. Bu pratik olmadığından, kesin sonuç vermesine rağmen, Wilson teoremi büyük sayılar için asallık testi olarak kullanılamamaktadır.

cevap12

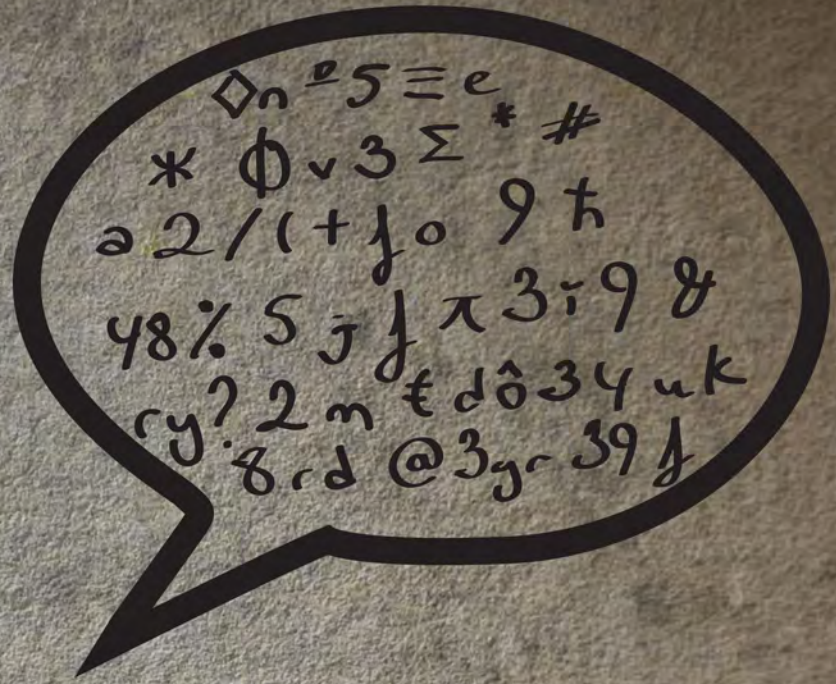


Verilen şemada, iki il ismi (örneğin, İSTANBUL ve ERZURUM) sadece şu şartları sağladığında birbirine eğrilerle bağlanmıştır:

(i) Sesli harfleri en az bir kere örtüşür: yani, ortak en az bir $x \in \{A, E, İ, O, Ö, U, Ü\}$ harfine sahiptirler,

(ii) Sessiz harfleri hiç örtüşmez: yani, ortak hiçbir $y \in \{B, C, Ç, D, F, G, Ğ, H, J, K, L, M, N, P, R, S, Ş, T, V, Y, Z\}$ harfine sahip değildirler.

Bu durumda, GAZİANTEP, ortak sessiz harfi olmayan illerden, "A" harfini ortak kullandığı BURSA, ve "A" ile "E" harflerini ortak kullandığı KOCAELİ ile bağlanmalıdır.



Anlaşılmamak bazen iyidir



MİLCEP-K2 Milli Kriptolu Cep Telefonu

- » 600 MHz ARM Cortex-A8 ana işlemci
- » 256 MB bellek
- » 256 MB hafıza kartı
- » Açık/kapalı ses iletimi
- » Kapalı veri iletimi
- » Kapalı anlık mesajlaşma
- » GSM 850/900/1800/1900 MHz
- » GPRS Class 12, EDGE Class 12, CSD (V.110, V.32)
- » SCIP (Secure Communications Protocol) desteği
- » Milcep-K1 ve Milsec-4 ile uyumlu
- » Türkçe ve İngilizce dil seçeneği
- » Konuşma süresi -9.5 saat
- » Kapalı Konuşma süresi -8.5 saat
- » Uyku Durumu -7 gün