Güven veren teknoloji

aselsan Dergi

ISSN 1300-2473

SAYI **106** AĞUSTOS **2020**

Güven

Güvenli Ağ Teknolojileri ve ASELSAN

Birliktelik

Birliktelik değerimizin ASELSAN kültüründeki karşılığı:

- Her durumda birlikte sorumluluk üstleniriz.
- Birbirimizle her durumda dayanışma içinde oluruz.
- Ortamda bulunmayanın hakkını koruruz.
- Ekip amaçları için birbirimizi cesaretlendiririz.
- İş sonuçlarına katkı sağladığını düşündüğümüz davranışları takdir ederiz.
- Bölümler arası iş süreçlerinin uyumu için bilgiyi ve deneyimi
- Paylaşır, iş birliği yaparız.
- Farklılıklara saygı gösterir, farklılıklardan sinerji yaratırız.

Güven

Güven değerimizin ASELSAN kültüründeki karşılığı:

- Söylediğimizi yapar, yaptığımızı söyleriz.
- Açık, net ve şeffaf iletişim kurarız.
- Verdiğimiz sözleri tutarız.
- İşleri zamanında ve tam olarak teslim ederiz.
- Hatayı kimin yaptığına değil, sorunun çözümüne odaklanırız.

Gelişim

Gelişim değerimizin ASELSAN kültüründeki karşılığı:

- Sürekli öğrenir ve kişisel gelişimimizin sorumluluğunu alırız.
- Potansiyelimizi zorlayıcı hedeflerle keşfeder ve geliştiririz.
- Gelişim için geri bildirim alırız ve yapıcı geri bildirim veririz.
- İç ve dış paydaşlarımızın gelişimine katkı sağlarız.

Mükemmellik

Mükemmellik değerimizin ASELSAN kültüründeki karşılığı:

- Süreçlere uygun çalışır, süreçlerin etkinliğini sürekli izler ve iyileştirme önerileri sunarız.
- Kaynaklarımızı verimli kullanırız.
- Daha iyisi için bir işin nasıl yapılmayacağını değil nasıl yapılabileceğini konuşuruz.
- İşimizin izlenebilir, tekrar edilebilir olmasını sağlarız.
- Paydaşlarımızın ihtiyaç ve beklentilerini doğru analiz ve tespit eder, karşılıklı teyit ederiz.

Yenilik

Yenilik değerimizin ASELSAN kültüründeki karşılığı:

- Rutini sorgular, yeni fikirler üretir, yaratıcı çözümler deneriz.
- Değişim ihtiyacını anlar, destekler ve değişime öncülük ederiz.
- Hata yapmaktan korkmayız ve hataları bir öğrenme fırsatı olarak görürüz.
- Bireylerin farklı fikirlerini ifade etmelerini destekleriz.
- Dünyadaki yenilikçi yaklaşımları takip eder, proaktif bir anlayışla işlerimize yansıtırız.

GÜCÜMÜZ DEĞERLERİMİZ

aselsan

Güvenli İletişimin Anahtarı ASELSAN'da

Prof. Dr. Haluk GÖRGÜN
Yönetim Kurulu Başkanı ve
Genel Müdür

21. yüzyıl ile birlikte yaşanan bilimsel ve teknolojik gelişmeler sonucunda haberleşme imkanları artmıştır. Küresel olarak artan dijitalleşme süreci ile birlikte bilgi teknoloji altyapısının temel birimi olan güvenli ağ teknolojileri, toplum ve kamu güvenliği açısından stratejik önem kazanmıştır.

Askeri veya sivil her gereksinimde çözümün en önemli unsurunu teşkil eden bilgi teknolojileri, ASELSAN bünyesinde en karmaşık haliyle ele alınarak sağlıktan sosyal platformlara, kamu ihtiyaçlarından güvenlik noktalarına kadar her alanda son teknoloji ürün ve hizmetlere dönüşmektedir.

ASELSAN'ın haberleşme teknolojilerindeki uzmanlığına paralel emniyet çözümleri olarak ortaya çıkan Bilgi Teknolojileri Ağ Cihazları ve Çözümleri ile Kripto ve Bilgi Güvenliği Sistemleri, iletişim çağı olarak anılan günümüzde ses, görüntü ve veri aktarımının güvenle sağlanmasına yönelik cihaz ve sistem çözümlerini barındırmaktadır. ASELSAN, ülkemizdeki haberleşme ağları altyapılarının mili ve yerli ürünlerle güvenli bir şekilde donatılabilmesi için ağ cihazları ve ilgili çözümler sunmaktadır. Ayrıca Kripto ve Bilgi Güvenliği Sistemleri çatısı altında, çeşitli görev gereksinimlerine uygun milli kripto cihazları ile bireysel ve yığın haberleşme unsurlarının bilgi güvenliğini sağlayan son teknoloji ürün ve sistemler geliştirmektedir.

Faaliyetlerine kuruluşunun ilk yıllarında lisans altında analog taktik telsizler üreterek başlayan ASELSAN, günümüzde özgün tasarımlı, modern elektronik cihaz ve sistemler geliştiren, üreten, tesis eden, pazarlayan ve satış sonrası hizmetlerini yürüten küresel bir şirket olarak devam etmektedir.

ASELSAN bu kapsamda, cihaz ve sistemler için sistem tasarımı, mühendislik, üretim, pazarlama, proje yönetimi ve müşteri desteği konularında etkin çözümler oluşturarak yurt içinde ve yurt dışında dünyanın önde gelen haberleşme teçhizatı üreticileri ve sistem entegratörleri ile rekabet etmektedir.

ASELSAN çözümleri, müşteri memnuniyetinin sunulan tüm hizmet ve ürün kalitesi kadar değerli olduğu anlayışı içinde; askeri, kamu, sivil kurum ve kuruluşların haberleşme ihtiyaçlarına yönelik olarak en yeni teknolojik gelişmelere uygun, hızlı, güvenilir, esnek, mobil ve ekonomik olarak sunulmaktadır. Yeni haberleşme teknolojileri sürekli takip edilerek belirlenen hedeflerin aşılabilmesi için takım çalışmasına olan inançla bilgi düzeyi sürekli olarak geliştirilmektedir. ASELSAN, güvenli ağ teknolojileri alanındaki geniş ürün seçeneği, değişik sistem çözümlerini tek elden sunabilmesi ve başarılı geçmişi ile sahip olduğu büyüme potansiyelini ve global pazardaki marka değerini gün geçtikçe artırmaya devam etmektedir.

Dergimizin bu sayısını güvenli ağ teknolojileri alanındaki çalışmalarımıza ayırdık. İletişim teknolojileri hayatımızın her alanını sararken bu sistemlerin güvenliği için yapılan çalışmaları anlatmaya çalıştık.

1975'ten beri Türkiye'nin sesi olan ASELSAN'ın çalışmalarını aktaracağımız bir sonraki sayımızda görüşmek üzere...

aselsan

ISSN 1300-2473

Yıl : 33 Ağustos 2020 Sayı : 106

ASELSAN Elektronik San. ve Tic. A.Ş. Adına Yayın Sahibi
Prof. Dr. Haluk GÖRGÜN

Genel Yayın Yönetmeni
Doç. Dr. Hakan KARATAŞ

Sorumlu Yazı İşleri Müdürü
İbrahim BİLEKLİ

Yayın Kurulu
Nazmi BOŞÇA
Esra DOĞU
Tuna GÜVEN
Berkan KARAKURT
Serkan KEKEÇ
Yılmaz OKTAY
Ayşegül PİŞKİN
İbrahim TEKİN
Şeniz ULUÇAY
Başak YÜCEKAYALI
Veysel YÜCESOY

Haber Merkezi
Kaya AKIN
Hande BİLGİN
Erkan ERDAL
Evrim ERDOĞAN

Fotoğraf
Evren BARIŞIK
Halil İ. MUŞTUCU
İbrahim ÖZTÜRK
Necdet ZABZUN

Dağıtım
Osman ARDOĞAN

Tasarım
RETA Reklamcılık ve Tanıtım Ltd. Şti.
Ziaur Rahman Cad. 285. Sok.
No: 26/19 Çankaya, ANKARA
www.reta.co

Yayın Tarihi
Sayı 106 - 19 Ağustos 2020

Yayın İdare Adresi
ASELSAN A.Ş.
Mehmet Akif Ersoy Mahallesi
296. Cadde, No: 16
Yenimahalle, ANKARA

Baskı Cilt
19 Ağustos 2020 / 09:00

DUMAT Ofset
Bahçekapı Mah. 2477. Cadde No: 6
Şaşmaz - Etimesgut, ANKARA
www.dumat.com.tr

Yayının Türü
Yerel Süreli Yayın

İÇİNDEKİLER

Haberleşme Teknolojileri Tarihçesi ve Güvenli Ağlar

Hazırlayan
Mehmet Uçak
Haberleşme ve Bilgi Teknolojileri (HBT) Sektör Başkanlığı - Sistem Mühendisliği Direktörlüğü (SMD) - Bilgi Teknolojileri Sistem Mühendisliği Müdürlüğü

Haberleşme insanoğlu için en temel ihtiyaçlardan biridir. İnsanlar tarih boyunca birbirleri ile haberleşmek için birçok yöntem geliştirmiş ve kullanmıştır. İlk insanlar, birbirlerine yüksek sesle, bağırarak ulaşmışlardır. Yeni icatlar ve teknolojiler sayesinde, bağırarak seslenme ile başlayan iletişim ya da haberleşme, günümüzde bir 'tık' mesafesine kadar inmiştir.

Genel anlamda insanoğlunun haberleşme ihtiyacı bilgiyi iletme etrafında şekillenmiş ve gelişmiştir ki insanın tarihsel gelişiminde bilginin içeriği de ses ve veri olmuştur.

İnsanın önceleri sesler çıkararak haberleşmesi, zamanla bu seslerin dillere dönüşmesi ile anlamlı bir hale gelmiştir. Dolayısıyla konuşma dilleri, aslında insanoğlunun haberleşme ihtiyacının bir sonucu olarak keşfettiği birer haberleşme aracıdır. Sesin iletilmesi, haberleşmenin tarihinde hep temel amaç olmuştur.

Bilginin veri bileşeni de insanoğlunun tarihsel gelişimi içerisinde sembollerden metinlere, fotoğraflara ve görüntülere kadar değişim göstermiştir.

Bilgiyi;
- daha uzağa iletme,
- daha fazla noktaya iletme,
- daha fazla miktarda iletme ve
- daha güvenli iletme

arayışları haberleşme araçlarının ve haberleşme teknolojilerinin gelişimini şekillendiren konular ve cevap aranan sorular olmuştur.

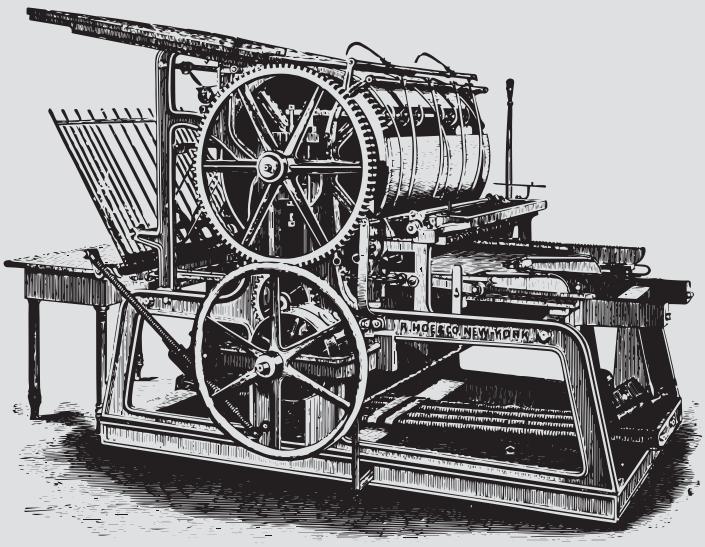
Yüzbinlerce yıllık insanlık tarihinde şaşırtıcı olan bir başka gerçek ise haberleşme araçları ve haberleşme teknolojileri ile ilgili gelişmelerin özellikle son elli yıl içerisinde baş döndürücü bir hıza ulaştığıdır. Bu sayede, ellili yaşlarındaki birçok insan, çocukluklarında ve gençliklerinde haberleşmenin zirvesi olan PTT'nin mektup, telgraf ve telefon ağlarından günümüzün IP tabanlı ağlarına uzanan yola şahitlik edebilmiştir. Hiç şüphesiz ki bu muhteşem değişim, özellikle elektrik-elektronik mühendisliği, bilgisayar mühendisliği ve bunların alt disiplinleri ile ilişkili birçok buluşun ve gelişimin bu zaman dilimi içerisinde gerçekleşmesiyle olmuştur. Bugün itibarıyla da haberleşme bir ihtiyaç olmanın ötesine geçmiş ve bilginin üretilmesi, iletilmesi, depolanması, korunması ve kullanımı hem bireylerin hem de toplumların yaşantılarının merkezine yerleşerek sosyal, kültürel, ekonomik ve siyasal olarak vazgeçilmez bir güç çarpanı haline gelmiştir.

İnsanlığın ilk çağlarında iletişim adına yalnızca ses vardı. İnsanlar birbirlerine yalnızca seslenerek haberleşebiliyorlardı. Bu nedenle konuşma, iletişimin ve haberleşmenin başlangıcı olmuştur. Devirler değişim gösterdikçe, iletişimin de farklı yolları ortaya çıkmaya başlamıştır. Bağırarak haberleşme yöntemi mesafe olarak çok kısıtlı kaldığından, insanlar haberleşmeyi daha uzak mesafelere taşımanın yollarını aramışlardır.

Ses çıkarmanın başka yollarını keşfetmeye başlayan insanoğlu, önce davullar ile daha uzak mesafeye haber göndermenin mümkün olduğunu fark etmiştir. Sonrasında ise ateşin bulunmasını takiben daha da uzağa, uzak tepelere haber ulaştırmak için dumanın kullanılması süreci başlamıştır. Duman ile haberleşmenin keşfi, bu anlamdaki ilk gelişim basamağı olarak kabul edilmektedir.

Antik çağlarda insanlar, iletişim adına yeni yollar keşfetmeyi sürdürmüşlerdir. Nasıl ateşin bulunması haberleşmede bir dönüm noktası olduysa yazının bulunması da ikinci bir dönüm noktası olmuştur. Bu anlamda, görsellik devreye girmiş ve insanlar, anlatmak istediklerini duvarlara çizdikleri figürlerle aktarmaya başlamışlardır. Mezopotamya'da çivi yazısı kullanılırken, M.Ö. 3000'e doğru gelindiğinde, dönemin büyük medeniyeti Antik Mısır'da hiyeroglifler kullanılmaya başlanmıştır.

Yazıyla haberleşmenin gelişimi, tarihin en önemli olaylarından birinin meydana gelmesine sebep olmuş ve matbaa icat edilmiştir. M.S. 1. yüzyıla ve 2. yüzyıla ait, çok ilkel baskı tekniklerine dair tarihsel kalıntılar bulunmuş olmakla birlikte matbaanın 1045'te Çin'de ortaya çıktığı kabul edilmektedir. Uzak Doğu'da kullanılan matbaacılık teknikleri daha sonra tüm dünyaya yayılmış, 1450'de Johannes Gutenberg'in modern anlamdaki matbaayı icat etmesiyle seri baskı anlayışı mümkün kılınmış ve matbaacılık gelişerek günümüzdeki son halini almıştır.



Çanakkale Savaşında telgraf hattı çeken Türk askeri

Haberleşmedeki üçüncü dönüm noktası elektrikle ilgili icatlardır. 18. yüzyılda Benjamin Franklin, elektrik hakkında çok geniş bir çalışma yapmıştır. Haziran 1752'de fırtınalı bir günde, uçurtma ipine bağladığı metal bir anahtarla bir deney yapmış ve uçurtmaya yıldırım düşmesini beklemiştir. Anahtardan eline zıplayan kıvılcımlardan, yıldırımın da elektriksel bir doğa olayı olduğunu kanıtlamıştır. 1771'de, Luigi Galvani, biyoelektrik üzerine olan keşfini yayınlamış ve elektriğin sinir hücreleri denen hücreler ile kaslara sinyaller yolladığını göstermiştir. Alessandro Volta, 1800'de voltaik pili icat etmiştir. Hans Christian Ørsted ve Andre Marie Ampere tarafından 1819-1820 yıllarında elektrik ile manyetizmanın etkileşimi ve elektromanyetizma bulunmuştur. Michael Faraday, 1821'de elektrik motorunu bulurken Georg Ohm, 1827'de matematiksel olarak elektriksel devreleri açıklamış ve devre teorisinin temellerini oluşturmuştur. James Clerk Maxwell de 1864'te yayınladığı Maxwell Denklemleri ile elektromanyetik dalga teorisinin temellerini atmıştır.

Bu gelişmelerden yararlanan insanoğlu; konuşma, duman, çivi yazısı, hiyeroglif, posta güvercini, ulak, mektup derken yeni bir icat ile haberleşmede çığır açmıştır. Claude Chappe, 1792 yılında uzak mesafelerle haberleşmeyi sağlayan bir sistem geliştirmiş ve adını telgraf koymuştur. Bu sistemde tepelerin üzerine kurulmuş kulelerden bir ağ oluşturulmuş ve her kulenin üzerinde 49 değişik konuma ayarlanabilen iki uzun kola sahip bir makine yerleştirilmiştir. Her konumun bir harfe veya bir rakama karşılık geldiği bu sistem çok başarılı olmuş ve 19. yüzyılın ortalarında Fransa'daki kule ağı 4828 kilometreye ulaşmıştır. 1830 yılında Joseph Henry, elektrik akımını teller vasıtasıyla uzaklara taşıyıp oradaki bir elektromıknatısa bağlı zili çalıştırmıştır; bu, elektrikli telgrafın doğuşu olmuştur. 1835 yılında Samuel Morse, ilk elektromıknatıslı telgrafı yapmıştır. Bu telgrafta elektromıknatısa bağlı bir kalem bulunmakta ve bu kalem, kağıt bir şerit üzerine elektromıknatıstan aldığı hareketle zik zak çizgiler çizmekteydi. Bu sistem pek başarılı olmamıştır. Daha sonra Samuel Morse bunu geliştirmiş ve nokta ve çizgilerden oluşan bir kodlama sistemi ortaya çıkarmıştır. Bu kodlama sistemi, daha sonra tüm dünyada kabul gören Mors Alfabesi idi. O yıllarda telgraf en popüler iletişim aracı olmuştur.

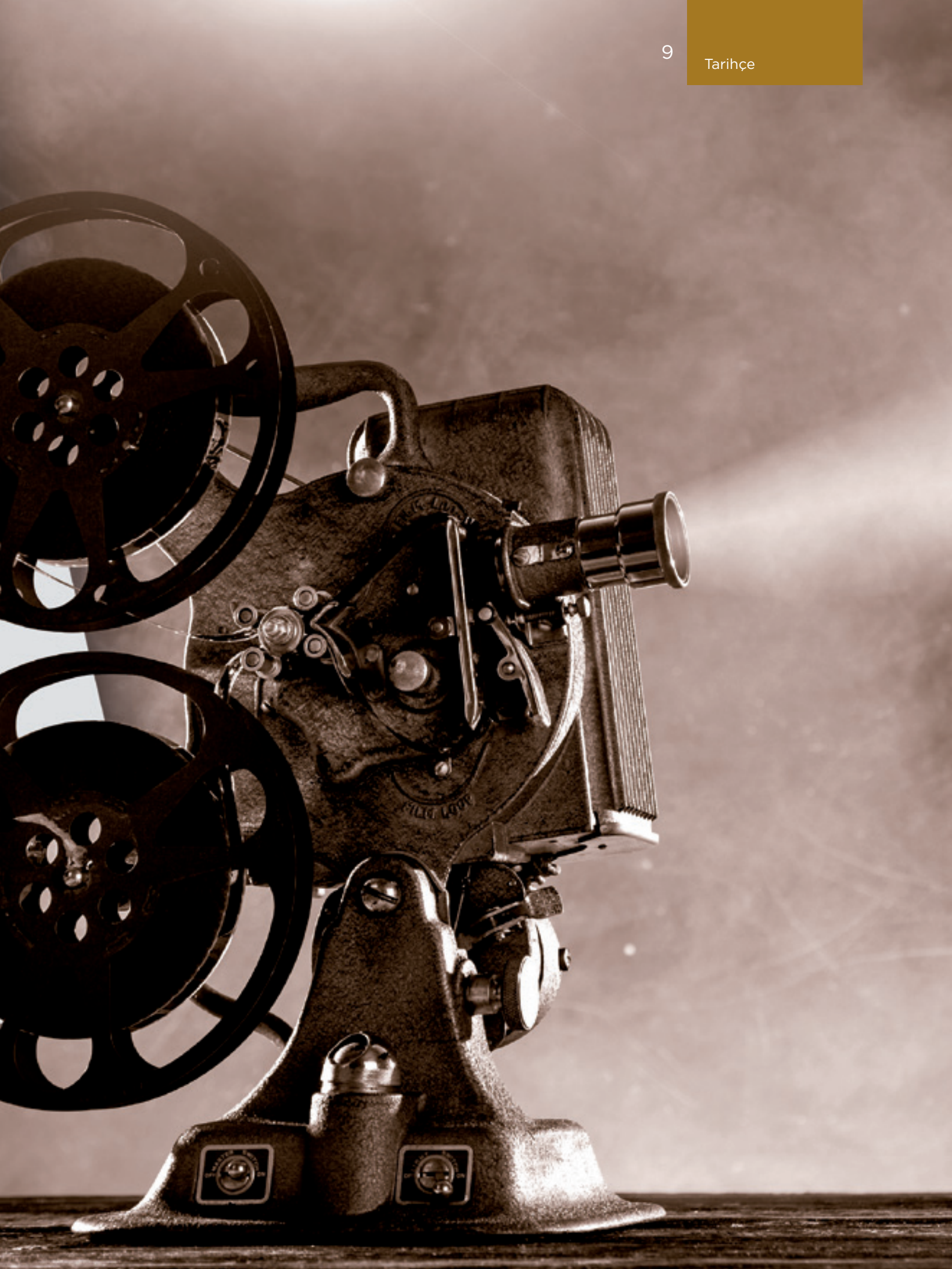
1843'te Alexander Bain, ilk faks makinesini icat etmiştir ki bu tasarım günümüzün faks makinesinden biraz uzaktır ancak faks makinesi olarak patenti alınan ilk üründür.

1876 yılı, haberleşme adına en ciddi adımlardan birinin atıldığı yıl olmuştur. Alexander Graham Bell, elektrik telleri üzerinden ilk kez ses iletmeyi başarmış ve bu icadına telefon adını vermiştir. Telgraf, kablo ile bilgileri yazılı olarak bir yerden bir yere iletebilirken telefonun, kablo ile sesi iletebiliyor olması insanları oldukça etkilemiş ve Amerika sokaklarını telefon direkleri ve kabloları sarmaya başlamıştır.

Telefonun icadı, insanoğlunun bilgiyi iletme ve daha uzağa iletme ihtiyacını bir noktadan birden çok noktaya iletme boyutuna taşımıştır. Haberleşme sağlanması istenen noktalar arası kablolar ile bağlantı kurulmasının pratik olmaması, insanoğlunu bu konuda da çözümler üretmeye zorlamıştır. Belki de haberleşme ağlarının anlamlı bir şekilde hayatımıza girmeye başlaması bu ihtiyacın bir sonucu olmuştur. Nitekim telefonun icat edildiği zamanlarda telefonlar yani farklı noktalar arasındaki anahtarlama ve yönlendirme işlevleri için ilk telefon santralleri kurulmuş ve bu işlevler manuel olarak operatörler tarafından gerçekleştirilmiştir. Sonrasında bu mekanik telefon santralleri gelişerek elektronik telefon santrallerine ve yakın geçmişimizde de IP santrallerine dönüşmüştür. Bilgisayarların hayatımıza girdiği dönemlere kadar, telefon santralleri ile kurulan ve PSTN (Public Switched Telephone Network) denilen ağlar da en büyük haberleşme ağları olarak hizmet vermişlerdir. Bu noktada belirtmekte fayda vardır ki PSTN'in kıtalararasına yaygınlaşması 1956 yılında gerçekleşmiş, okyanus altına İrlanda ile Kanada arasında telefon kablosu döşenerek ilk kıtalararası kablolu telefon haberleşmesi gerçekleştirilmiştir.

Takvimler 1894 yılını gösterirken iki kardeş, Louise Lumiere ve Aguste Lumiere, ilk sinema makinesini icat etmişlerdir. Böylece herhangi bir görüntünün kayıt edilmesi, arşivlenmesi ve yeniden gösterilmesi mümkün hale gelmiştir ve insanoğlu için haberleşmedeki bilginin veri bileşeni sembollerden ve metinlerden fotoğraflara ve görüntülere genişlemiştir.

İnsanoğlunu kablolu haberleşmeden kablosuz haberleşmeye taşıyan ise Guglielmo Marconi tarafından 1906'da antenin icadıdır. Marconi her ne kadar radyo olarak adlandırılan kablosuz haberleşmenin mucidi olarak kabul edilse de Reginald Fessenden, radyo aracılığı ile ses iletimini sağlayan ilk kişi olmuştur. Radyo, telefondan sonra insanların yaşamlarında ve evlerinde yerini alan ikinci büyük haberleşme aracı olmuştur.

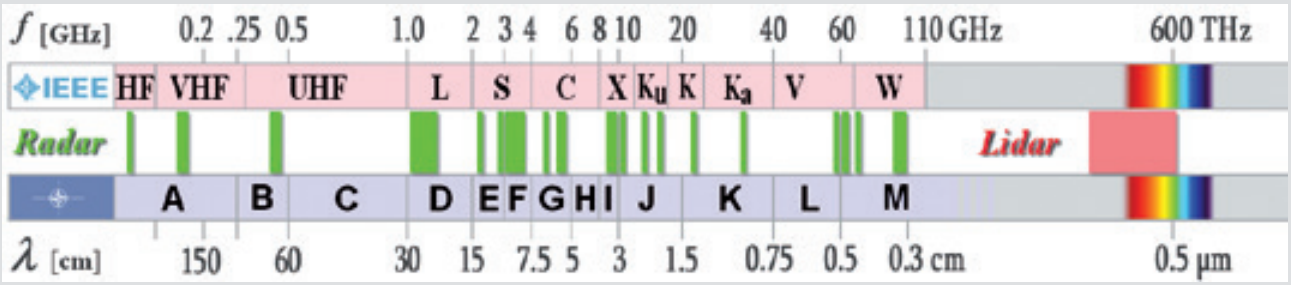


Reginald Fessenden, 1906'da Genlik Modülasyonunu (AM) bulmuş ve kablosuz ses haberleşmesini gerçekleştirmiştir. Böylelikle haberleşmenin tarihçesine modülasyon kavramı da girmiştir. 1933'te de Edwin Howard Armstrong tarafından Frekans Modülasyonu (FM) geliştirilmiştir. Nitekim modülasyon teknolojilerinin gelişmesiyle insanoğlu bilgiyi iletme ve bilgiyi bir noktadan çok noktaya iletme yeteneklerine bilgiyi daha fazla iletme yeteneğini de eklemiştir.

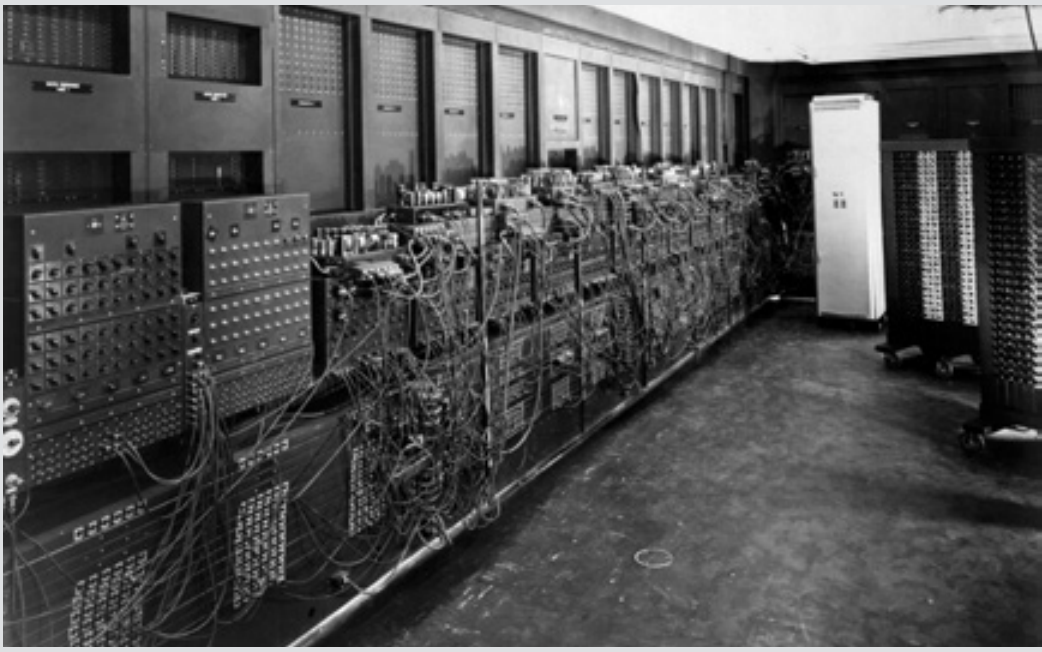
Bu arada 1922'de Arthur Korn, radyo dalgaları aracılığıyla görüntü (fotoğraf) gönderebilen ilk faks makinesini icat etmiş, 1924'te Amerikan Radio Corporation of America (RCA) şirketinden Richard H. Ranger'in araştırmaları sonucunda modern faks makinesine ulaşılmıştır.

1926 yılında John Logie Baird'den, haberleşmeye yepyeni bir yön verecek bir buluş gelmiştir. Baird, görüntüyü, radyo dalgaları kullanarak çok uzaklara bile gönderebilen televizyonu icat etmiştir. Televizyon, 2. Dünya Savaşından sonra ticarileşip yaygınlaşarak radyodan ve telefondan sonra insan yaşamına giren üçüncü büyük haberleşme aracı olmuştur.

Artık hem haberleşme araçlarının ticarileşmesi ve yaygınlaşması hem de kablosuz haberleşmedeki gelişmeler insanoğlunu kablosuz haberleşmenin esasını oluşturan frekans dünyasını belirli disipline göre yönetme problemiyle karşı karşıya bırakmıştır. Bunun için de hem ulusal otoriteler tarafından hem de uluslararası düzeyde düzenlemeler yapılarak frekans spektrumu teknolojik olarak uygun bantlara ayrıştırılmış, haberleşme araçlarının ve ilgili haberleşme teknolojilerinin kullanacağı bandlar belirlenmiştir.



1946 yılına gelindiğinde, John Mauchly ve Presper Eckert askeri amaçlara hizmet etmesi planlanan yeni bir cihazı ortaya çıkarmıştır: ENIAC. Bu cihaz, elektrikle çalışan ve veri işleme kapasitesine sahip, bilinen ilk bilgisayar olmuştur. ENIAC, 30 ton ağırlığında, 4 apartman dairesi büyüklüğündeydi ve içinde 18 bin adet elektronik tüp bulunuyordu ki modern bilgisayarların atası olarak haberleşme araçları tarihçesinde yerini almıştır.



Haberleşmedeki dördüncü dönüm noktası 1947 yılında Bell Araştırma Laboratuarlarında, William Shockley başkanlığında John Bardeen'den ve Walter Brattain'den oluşan ekip tarafından gerçekleştirilmiş ve bugün sahip olduğumuz teknolojilere ulaşmamızı sağlayan transistör icat edilmiştir. 20. yüzyılın en önemli buluşlarından biri olarak kabul edilen ve elektronik devrelerin can damarı olan transistörler ile başlayan süreç, analog elektronik kavramının yanına sayısal elektronik kavramının kazandırılmasını sağlamıştır. Bu sayede insanoğlu, belki yüzbinlerce yılda kazandığı teknolojik gelişmeyi elli yıl gibi kısa bir sürede katlayacak kadar hızlı bir gelişime tanıklık etmiştir. Sayısal elektronik tabanlı gelişmeler, sayısal sinyal işlemenin ve sayısal modülasyon tekniklerinin öncülük ettiği teknolojiler, çok yüksek frekanslara fiziksel olarak erişebilme yeteneği ile insanoğlu; bilgiyi iletme, daha uzağa iletme ve daha fazla noktaya iletme yeteneklerinin yanına bilgiyi daha fazla miktarda iletme yeteneğini de koyabilmiştir.

Elektronikteki gelişmelerle bilgisayarlar da gelişmiş ve insanoğlu 1981'de ENIAC'tan PC olarak bilinen kişisel bilgisayarlara ulaşmıştır. PC, modern anlamdaki ilk bilgisayar olarak haberleşmede devrim niteliğinde bir adım atılmasını sağlamıştır.

Bu sırada, teknoloji alanında sağlanan gelişim ile insanoğlu hem uzaya ilk adımlarını atmış hem de uzayı haberleşme için kullanmaya başlamıştır. 1962'de NASA'nın fırlattığı ilk haberleşme uydusu olan TELSTAR-1 ile artık uydu haberleşmesi mümkün olmuş ve kıtalararası haberleşmenin temel aracı haline gelmiştir.

1970'li yılların ortalarında, ABD'de üniversiteler arasında bilgisayarlar arası bilgi transferi sağlama amacı ile ARPA adında bir haberleşme sistemi geliştirilmiş ve bu sistem sayesinde, aynı şehirdeki bilgisayarların birbirlerine bağlanabilmeleri mümkün olmuştur. Bu gelişme, bilgisayar ağlarının ve günümüzdeki anlamıyla modern haberleşme ağlarının temelini oluşturmuştur.

Bilgisayarların ve haberleşme ağlarının gelişimine paralel olarak insanoğlu yeni bir haberleşme aracı olan cep telefonu ve ilgili teknolojileri ile tanışmıştır. 1983'te, Martin Cooper tarafından ilk cep telefonu tasarlanmış ve MOTOROLA tarafından üretilmiştir ki bu cihazın bir ekranı yoktu ve şarj olması yaklaşık 10 saat sürüyordu. Aynı dönemlerde arabalarda kullanılmaya başlayan araç telefonları da ilk cep telefonlarının piyasaya sürülmesi ile kısa sürede ortadan kalkmıştır. Nitekim yine aynı dönemlerde icat edilen ve kullanılan bir başka haberleşme aracı olan çağrı cihazları da cep telefonlarının SMS (Short Message Service) ve MMS (Media Message Service) yetenekleri kazanması ile kısa süreli kullanım bulabilmiştir.

Bugünün akıllı telefonlarına uzanan ve ilk cep telefonuyla başlayan süreç yaklaşık yirmi yıl sürmüştür. Teknolojideki gelişim ve akıllı telefonlarımıza yüklenen çok çeşitli mobil uygulamalar, hayatımızda büyük yer kaplamaya başlamış ve vazgeçilmez olmuştur. Bugün çeşitli yazılımların da aracılığı ile tek bir dokunuşla görüntülü konuşabildiğimiz bir dönemde yaşıyoruz. Kronolojik olarak baktığımızda bu alandaki gelişmeleri de şöyle özetleyebiliriz:

1979
Japonya Tokyo'da GSM (Global System for Mobile Communications) hücre teknolojisi kullanan bir mobil haberleşme ağı ilk kez ticari kullanıma sunulmuştur.

1974-1984
GSM hücre teknolojisine dayalı haberleşme ağı Japonya'nın tümünü kapsayacak şekilde genişletilmiş 1G (Birinci Nesil) mobil haberleşme ağı kurulmuştur.

1991
2G (İkinci Nesil) sayısal mobil haberleşme ağı kullanıma sunulmuştur.

1998
Japonya'da 3G (Üçüncü Nesil) sayısal mobil haberleşme ağı kullanıma sunulmuştur. 3G, 2002'de ABD'de ve 2003'te Avrupa'da kullanılmaya başlanmıştır.

2009
4G (Dördüncü Nesil) sayısal mobil haberleşme ağı kullanılmaya başlanmıştır.

2019
Standartları geliştirilmekte olan 5G (Beşinci Nesil) sayısal mobil haberleşme ağı kullanılmaya başlanmıştır.

Bilgisayarlar ile başlayıp günümüzün akıllı telefonlarına ve bilgisayar tabanlı birçok cihaza uzanan bu süreçte artık dünya üzerinde her insanın her insanla ve her noktanın her nokta ile haberleşebildiği, çok yüksek miktarlarda bilginin iletilebildiği bir haberleşme ağına ulaşılmıştır. Şüphesiz ki bunda haberleşme araçlarındaki gelişmeler kadar haberleşme ağlarında kullanılan teknolojilerdeki gelişmelerin de büyük rolü olmuştur. Nitekim 1970'de ARPA adıyla ortaya çıkan sistem ve IP (Internet Protocol), 1985'te internete ve TCP/IP (Transmission Control Protocol/ Internet Protocol)e dönüşmüş ve bir dizi teknolojik gelişim ile bugünkü halini almıştır. Bu süreçte haberleşme ağlarında kullanılan ağ cihazları ve bunların birbirleri ile iletişiminde kullanılan teknolojiler de değişmiş, tüm haberleşme biçimleri IP'ye dayalı tek bir sistem etrafında birleşmeye başlamıştır. Böylelikle tüm haberleşme cihazları ve dolayısıyla ağ cihazları IP tabanlı haline gelmiştir. Ayrıca artık sadece insanlar değil nesneler de haberleşme ağlarının bir parçası haline gelmiştir.

Bu tarihsel gelişiminin sonunda bugün yaşantımızı, en basit tanımlama ile PAN (Personal Area Network), LAN (Local Area Network) ve WAN (Wide Area Network) gibi kategorize edilen bir haberleşme ağı içerisinde sürdürüyoruz ve hangi büyüklükte olursa olsun bütün ağlar da birbirleriyle kesintisiz bir şekilde haberleşebiliyorlar. Kullandığımız bilgisayarlar, akıllı telefonlar ve benzer diğer haberleşme araçları yakın mesafelerde Wi-Fi, Bluetooth vb. teknolojiler ile kolaylıkla

haberleşebiliyor. Daha uzak mesafelerdeki ve daha fazla sayıda benzer haberleşme araçları ile haberleşebilmek için de ethernet anahtarlar, IP yönlendiriciler, baz istasyonları, radyolinkler, uydu terminalleri, telsizler gibi haberleşme araçlarını kullanılarak haberleşme ağı genişletilebiliyor.

Haberleşmenin bu kadar yaygınlaştığı günümüzde insanoğlu artık her türlü bilgiyi iletmek, bilgiyi her istediği noktaya iletmek ve bilgiyi istediği miktarlarda iletmek ve hatta depolayabilmek yeteneğini kazanmıştır ve bu yeteneklerinin limitlerini zorlamaktadır. İşte bu noktada insanoğlu için ortaya çıkan ve çözülmesi gereken yeni problem bu haberleşme yeteneklerinin sürekliliğinin, kullanılan haberleşme araçlarının ve ağlarının güvenliğinin ve bilginin güvenliğinin sağlanmasıdır.

Ağ Güvenliği, ağ trafiğini de kapsayan dijital varlıkları korurken, izinsiz ağ saldırılarını izlemek, önlemek ve bunlara yanıt vermek için tasarlanmış araçları, taktikleri ve güvenlik politikalarını tanımlayan bir terimdir. Ağ Güvenliği, ağı hedef alan tüm potansiyel tehditlere yanıt vermek üzere tasarlanan donanım bileşenlerini yani ağ cihazlarını ve yazılım bileşenlerini içerir. Başka bir deyişle, yanlış insanları hassas verilerimizden uzak tutmak için kullandığımız savunmalardır.

Bu tanım içinde, herhangi bir Ağ Güvenliği stratejisinin temelde hizmet etmesi gereken üç ana odak vardır: **koruma**, **saldırı tespit** ve **saldırı engelleme**.

Koruma, ağa kötü niyetli kişilerin girmesini önlemek için tasarlanmış herhangi bir araç veya politika gerektirir. Algılama, ağ trafiğini analiz etmeye ve ağa zarar vermeden önce, sorunları hızla tanımlamaya olanak sağlayan kaynakları ifade eder. Müdahale ise tespit edilen tehditlere tepki verme ve mümkün olduğunca çabuk çözme yeteneğidir.

Bilgi Güvenliği, bilgilerin izinsiz kullanımından, izinsiz ifşa edilmesinden, izinsiz yok edilmesinden, izinsiz değiştirilmesinden, bilgilere hasar verilmesinden koruma veya bilgilere yapılacak olan izinsiz erişimleri engelleme işlemidir.

Bilgi Güvenliği de üç başlık altında incelenmektedir: **gizlilik**, **bütünlük**, **kullanılabilirlik**.

Gizlilik, bilgilerin yetkisiz erişime karşı korunmasıdır. Bütünlük, bilgilerin eksiksiz, tam, tutarlı ve doğru olmasının sağlanmasıdır. Kullanılabilirlik ise kullanıcılar tarafından ihtiyaç duyulduğunda bilgilere erişilebilir olmasının sağlanmasıdır.

İnsanoğlunun temel bir ihtiyacı olan iletişimi sağlamak üzere geliştirdiği teknolojiler 21. yüzyılda, iletişimin içeriği olan bilginin etkin bir şekilde kullanılması ve böylelikle katma değeri yüksek kişisel, toplumsal, ekonomik ve siyasal çıktılar elde etme yarışına zemin oluşturmuştur. Artık insanların haberleşme ihtiyacı bir araç olmuş ve bu araçla taşınan bilgiyi değerlendirmek bir amaç haline gelmiştir. Kesintisiz, dilediğimiz kadar ve olabildiğince uzaklarla haberleşebilmek bir zenginlikse bu haberleşmenin altyapısı ve içeriğindeki bilgi bir hazinedir.

Kaynakça

(1) Anton A. Huurdeman (2003). Chronology. Worldwide History of Telecommunications. John Wiley & Sons. ISBN 978-0-471-20505-0

(2) Poe, Marshall T. A History of Communications: Media and Society From the Evolution of Speech to the Internet (Cambridge University Press; 2011), ISBN 978-1-107-00435-1

(3) 'https://dpworkshop.org/dpm-eng/timeline/timeline', Cornell University Library (2003), Digital Preservation and Technology Timeline, Digital Preservation Management

(4) 'https://www.pcworld.com/article/130207/article.html', Christopher Null (April 2, 2007), The 50 Best Tech Products of All Time, PC World.

Milli Ağ Cihazları
Vizyonu ve Yol Haritası

Hazırlayan
Mehmet Uçak
HBT SMD Bilgi Teknolojileri
Sistem Mühendisliği Müdürlüğü

Günümüzde kalkınmanın kilit unsurları teknoloji alanında milli ve yerli çözümler üretebilmek, ilgili çözümlerle ihracat gerçekleştirebilmek ve böylece hem ihracatı arttırarak hem de ithalatı azaltarak cari açığı azaltabilmek ve hatta pozitife döndürebilmektir.

Herşeyden önce, kalkınmanın anlamlı ve katma değer üretebilmesi için sürdürülebilir olması gerekmektedir.

Bu nedenle yerli ve milli teknolojilerle sürdürülebilir bir kalkınma için teknolojik altyapılarda söz sahibi olmak ve çözümler üretebilmek son derece önemlidir.

Kalkınma kavramının tarih içerisinde tanımı değişmiş ve gelişmiş olmakla birlikte günümüzde bu kavram sürdürülebilir kalkınma olarak ele alınmaktadır.

Sürdürülebilir kalkınmanın ekonomik unsuru da şöyle tanımlanmaktadır:

Ekonomik olarak sürdürülebilir bir sistem, mal ve hizmetleri süregelen esaslara dayanarak üretebilmeli, hükümetin ve dış borçların yönetilebilirliğini sürdürebilmeli, tarımsal ve endüstriyel üretime zarar veren sektörel dengesizliklerden sakınmalıdır. (Holmberg, J. ve Sandbrook, R. (1992). Sustainable Development: What Is to Be Done? Making Development Sustainable: Redefining Institutions, Policy, and Economics. (Ed. J. Holmberg). International Institute for Environment and Development, p. 19-38, Island Press, Washington, D. C.)

Bu tanım, aslında içinde, kalkınma için temel parametreleri barındırıyor ki bunlar planlama, altyapı oluşturma, üretim ve istihdam olarak sıralanabilir. Öyleyse eğer bir sektörde kalkınmayı hedefliyorsak o sektörde gerekli planlamaları yapmalıyız, altyapıyı kurmalıyız ve altyapıda yer almalıyız, üretmeliyiz ve böylece istihdam yaratmalıyız.

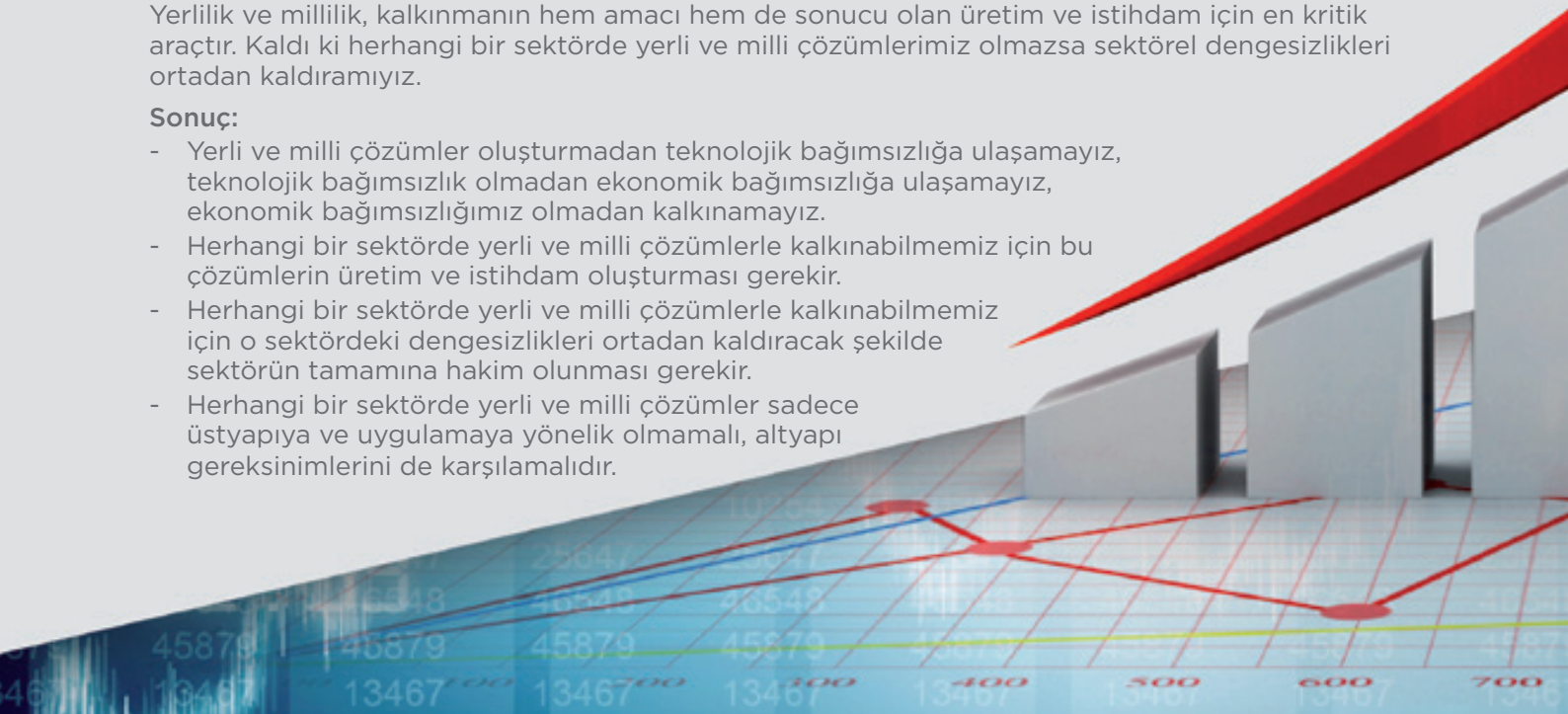
Bağımsızlığın kaçınılmaz dayanağı ekonomik bağımsızlıktır ki ekonomik bağımsızlık için de teknolojik bağımsızlığın gerektiğine sanırım kimsenin şüphesi yoktur.

Yine sürdürülebilir kalkınmanın tanımından yola çıkarsak, teknolojik bağımsızlık için de teknolojide üretim yapmalıyız, istihdam sağlamalıyız ve sektörel dengesizlikleri ortadan kaldıracak şekilde girişimler içinde olmalıyız.

Yerlilik ve millilik, kalkınmanın hem amacı hem de sonucu olan üretim ve istihdam için en kritik araçtır. Kaldı ki herhangi bir sektörde yerli ve milli çözümlerimiz olmazsa sektörel dengesizlikleri ortadan kaldıramıyız.

Sonuç:

- Yerli ve milli çözümler oluşturmadan teknolojik bağımsızlığa ulaşamayız, teknolojik bağımsızlık olmadan ekonomik bağımsızlığa ulaşamayız, ekonomik bağımsızlığımız olmadan kalkınamayız.
- Herhangi bir sektörde yerli ve milli çözümlerle kalkınabilmemiz için bu çözümlerin üretim ve istihdam oluşturması gerekir.
- Herhangi bir sektörde yerli ve milli çözümlerle kalkınabilmemiz için o sektördeki dengesizlikleri ortadan kaldıracak şekilde sektörün tamamına hakim olunması gerekir.
- Herhangi bir sektörde yerli ve milli çözümler sadece üstyapıya ve uygulamaya yönelik olmamalı, altyapı gereksinimlerini de karşılamalıdır.




800
900
1000
1100
1200
1300
1400
1500

Herhangi bir sektörde yerli ve milli faaliyetlerin, ilgili sektörün bir ucundan tutulmasıyla değil tamamına hakim olunarak gerçekleştirilmesi gerekir. Çünkü yerli ve milli bir faaliyetin hem bir ürün ortaya koyması, hem üretim ekonomisine katkı sağlaması, hem de hammadde olarak yerli ve milli bileşenlerden oluşması gerekir. Ülkemizde, özellikle teknolojik konularda yerli ve milli bir çıktı elde edilirken bu bileşenlerin tümüyle hedeflenemediğini ve çoğu zaman sadece uygulamaya yönelik faydalar elde edildiğini görüyoruz.

Örneğin, bilgi teknolojileri konusunda sektörün röntgenini çektiğimizde, çalışmalar ve ilgi ekseriyetle verinin işlenmesine ve kullanılmasına yoğunlaşıyor. Milyonlarca sensörden toplanan verileri işleyecek büyük veri, veri madenciliği vb. faaliyetler son derece önemli ve sahip olmamız gereken teknolojiler. Peki veriler kaynağından hedefine nasıl iletiliyor, nasıl taşınıyor ve nerelerde nasıl depolanıyor? Sektörün bu kısmıyla yeterince ilgili miyiz? Başka bir deyişle evimizdeki elektriği kullanıyoruz; ev cihazlarımızı evimize kadar gelen elektrikle çalıştırıp işimizi görüyoruz; ama elektrik evimize kadar nasıl geliyor, nasıl üretiliyor, nasıl dağıtılıyor gibi konuları pek düşünmüyoruz. Benzer şekilde musluğu açınca suyumuz akıyor ama su musluğa kadar nasıl geliyor sorusunu pek aklımıza getirmiyoruz. Ama ne zaman elektrikler kesilirse, ne zaman su kesilirse hayatımız felce uğruyor...

Bu yaklaşımla milli ağ cihazları vizyonunun amacı, ağ altyapılarında bulunmak ve bunun için milli ağ cihazları ve çözümleri oluşturmak olarak belirlenmiştir. Bu vizyon ile,

- ağ hiyerarşisinde katman 1'de, katman 2'de, katman 3'te ve katman 4-katman 7'de ihtiyaç duyulan çözümler sağlanacaktır,
- ağ hiyerarşisinde hem erişim seviyesinde, hem dağıtım seviyesinde, hem de omurga seviyesinde ihtiyaç duyulan çözümler sağlanacaktır,
- tüm çözümler hem askeri versiyonlar hem de ticari/endüstriyel versiyonlar şeklinde tasarlanıp geliştirilecektir,
- çözümlerin millilik oranının arttırılmasına yönelik çalışmalar yapılacaktır,
- geniş bir ekosistem oluşturularak ülke ekonomisine ve kalkınmaya doğrudan ve dolaylı katkılar sağlanacaktır.

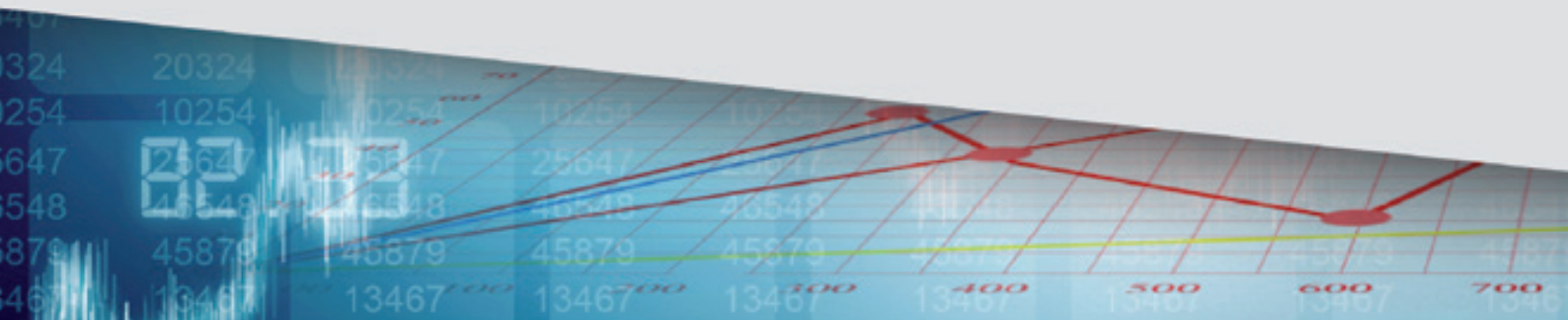
Buna göre ağ hiyerarşisinde katman 1'den katman 7'ye kadar tüm seviyelerde çözümler sunabilmek için milli ve yerli,

- IP yönlendiriciler,
- Ethernet anahtarlar,
- Kablosuz ağ cihazları (Erişim noktası cihazları ve terminal cihazları),
- Transmisyon cihazları ve medya çeviriciler,
- Güvenlik cihazları,
- IP santral ve VoIP (Voice over IP) uygulamaları,
- Ağ yönetim yazılımı,

tasarlanıp geliştirilmesi hedeflenmiştir.

Bu planlama kapsamında tasarlanacak tüm cihazlar zaman içerisinde daha da geliştirilerek SDN (Software Defined Network)/NFV (Network Function Virtualization) uyumlu ağ cihazları haline getirilecektir.

Böylelikle tüm IP tabanlı ağlarda hem erişim seviyesinde, hem dağıtım seviyesinde ve hem de omurga seviyesinde askeri tipte ve ticari/endüstriyel tipte cihazlar ve çözümler oluşturulacak ve Türkiye ekonomisinin her yıl milyarlarca dolar ithalat yaparak tedarik ettiği bilgi teknolojileri ürünleri için yerli ve milli alternatifler sunulmuş olacaktır. Ayrıca ilgili ürünlerin ciddi bir ihracat potansiyeli olacağı da kaçınılmaz bir gerçektir.



Söz konusu faaliyetlerde, çalışmalar belirli bir olgunluğa erişince tasarımda ve üretimde kullanılan hammaddelerin de yerli ve milli olarak tedarik edilebilmesini sağlamak için milli switch fabric entegresi ve milli SFP (Small Form Pluggable) modülü entegresi tasarımı ve geliştirilmesi hedeflenmektedir. Bu sayede de ilgili ürünlerin üretiminde yaşanabilecek tedarik kısıtları için önlem alınmış ve yerlilik ve millilik oranı yükseltilmiş olacaktır. Benzer şekilde bir milli yönlendirme protokolünün ve milli VPN (Virtual Private Network) protokolünün tasarlanıp geliştirilmesiyle de kritik ağlar için her koşulda güvenilir ve idame ettirilebilir bir altyapı sağlanabilecektir.

Söz konusu tüm bileşenlerin hayata geçirilebilmesi için yol haritası kapsamında geniş bir ekosistem oluşturulması hedeflenmektedir. İlgili faaliyetlerin üretimi, kalifikasyonu, satış sonrası hizmetleri de ülkemizde gerçekleştirilerek önemli bir istihdam yaratılmış olacaktır. Özellikle satış sonrası hizmetler ve teknik destek faaliyetleri için ihtiyaç duyulacak işgücünün sağlanması amacıyla gençlerimiz artık ithal üreticilerin eğitimlerine katılıp sertifikalar almak yerine, yerli ve milli ürünlerin eğitimlerine katılacak ve bunlarla ilgili operasyonel sertifikaları ve diğer uzmanlık belgelerini alacaklardır. Bu sayede oluşturulacak ekosistemin, ülke ekonomisine çok ciddi katkılar sağlayacağı öngörülmektedir.

Milli ağ cihazları vizyonu kapsamında yürütülen ve yürütülecek çalışmaların özeti Tablo 1'de gösterilmiştir.

Tablo 1: Milli Ağ Cihazları ve Çözümleri-Vizyon ve Yol Haritası

Proje	2014 2019	2020	2021	2022	2023	Seviye
Ethernet Anahtar Ailesi (240 GBit/s)						1
IP Yönlendirici (TURKAY) Ailesi (240 GBit/s)						1
Kriptolu IP Yönlendirici (Kriptolu TURKAY)						1
Ağ Yönetim Yazılımı (SNMP, NETCONF)						1
Kriptolu Wi-Fi Cihazları						1
SDN/NFV Uyumlu Ağ Cihazları, SDWAN, vCPE						2
Milli Switch Fabric						2
Milli Yönlendirme Protokolü						2
Milli SFP Modülü						2
Transmisyon Cihazları ve Medya Çeviriciler						2
Gömülü IP Santral						2
Gömülü VoIP Uygulamaları						2
Ethernet Anahtar Ailesi (6 TBit/s)						3
IP Yönlendirici Ailesi (6 TBit/s)						3
Wi-Fi Erişim Noktası Özellikli IP Yönlendirici Ailesi						3
Milli BRAS						3
Yük Dengeleyici						3
Milli DNS Güvenlik Cihazı						3
Milli VPN Protokolü						3
Milli Ağ Cihazları Laboratuvar Yazılımı (aMACLAB)						3
Sertifikalı Ağ Personeli (aSAP) / Certified Network Personnel (aCNP)						3

TAMAMLANAN veya DEVAM EDEN ÇALIŞMALAR

HENÜZ BAŞLAMAYAN ÇALIŞMALAR

Tablo 1'de detaylandırılan bileşenler seviye 1, seviye 2 ve seviye 3 olarak sınıflandırılmışlardır. Seviye 1 olarak listelenen bileşenlerin tasarımı ve geliştirilmesi için halihazırda çalışmalar başlamıştır ve devam etmektedir ki bunlar için oluşturulan tasarım kütüphaneleri ve modüler mimariler ile hızlı ve verimli bir şekilde hedeflere ulaşılmaktadır. Seviye 2 ve seviye 3 olarak listelenen çözümlerle ilgili tasarım ve geliştirme henüz başlamamıştır.

Milli ağ cihazları vizyonunda gelinen nokta ve yapılacak çalışmalar aşağıda ağ hiyerarşisindeki katmanlara göre detaylandırılmıştır.

Katman 1 Çözümleri

Her ne kadar doğrudan bir katman 1 çözümü olarak değerlendirilmese de IP ağlarının genişletilmesi ve kablosuz haberleşme ile desteklenmesi için kullanıldığı için Wi-Fi cihazları, katman 1 çözümü kapsamında ele alınabilmektedir.

Bu kapsamda KKAC (Kriptolu Kablosuz Ağ Cihazı) ile bir erişim noktası cihazı çözümü ve TKABC (Terminal Kablosuz Ağ Bağlantı Cihazı) ile bir terminal cihazı çözümü elde edilmiştir.

Bu cihazların geliştirilmesi için Mini KAC (Mini Kablosuz Ağ Cihazı) Tasarımı Projesi başlatılmıştır ve bu proje kapsamında cihazın daha küçük boyutlara ve düşük ağırlığa sahip, kullanımı ve montajı daha kolay, katman 3 özelliklerini de içeren, özellikle gemi platformlarındaki zorlayıcı koşullarda da çalışabilecek ve ticari uygulamalar için de kullanılabilecek yeni versiyonlarının geliştirilmesi amaçlanmaktadır.

Mini KAC, hem askeri tipte hem de ticari/endüstriyel tipte tasarlanıp geliştirilmektedir. Bu kapsamda hedeflenen ürünler Kriptolu Askeri Mini KAC, Ticari/Endüstriyel Mini KAC ve Kriptolu Ticari/Endüstriyel Mini KAC olacaktır.

Katman 1 Çözümleri kapsamında hedeflenen temel çözüm, IP ağların fiber optik iletim altyapısındaki eksikliklerini giderecek transmisyon cihazlarıdır.

Başta cep telefonu operatörlerinin ve internet servis sağlayıcılarının ağları olmak üzere TAFICS vb. ağlarda fiber optik iletim altyapısında önemli eksiklikler vardır. Nitekim bugün ülkemizdeki 15 milyondan fazla mekana hala fiber optik iletim altyapısı ulaştırılamamıştır. Özellikle cep telefonu operatörleri ve internet servis sağlayıcıları bu alanda tek başına yatırım yapmaya cesaret edememektedir. Böyle bir altyapının bağımsız bir otorite tarafından ve tek bir kaynaktan sağlanması halinde hem yatırım giderleri azalacak hem de ilgili otorite çok ciddi bir pazara hükmedebilecektir.

İnternet servis sağlayıcıların DSL (Digital Subscriber Line) şebekelerini fiber optik altyapılara dönüştürmesi sebebiyle dünyada yeni çalışılan bir konu da OLT (Optical Line Terminal)/ONT (Optical Network Terminal) GPON (Gigabit Passive Optical Network) cihazlarıdır. Özellikle açık kaynak kodlu yazılımların kullanıldığı GPON altyapıları gelecekte popüler haberleşme konusu olacaktır. Bu kapsamda desteklenmesi durumunda dünya ile aynı anda bir ürün geliştirilmesi ve pazara çıkılması sağlanabilecektir. Katman 1 Çözümleri kapsamında OLT/ONT GPON cihazlarının tasarımı ve geliştirilmesi de hedeflenmektedir.

Benzer şekilde katman 1 çözümleri kapsamında, konvensiyonel ve idame ettirilmesi gereken eski ağ altyapıları için medya çeviriciler tasarlanıp geliştirilmesi ile bu altyapıların da milli ağ cihazları ile entegrasyonu hedeflenmektedir.

Katman 2 Çözümleri

Katman 2 Çözümleri olarak

- 5.6 GBit/s'den 240 GBit/s'ye kadar anahtarlama yeteneği olan,
- 8/12/16/24/48 portlu konfigürasyonlar şeklinde ve
- Askeri tip ve ticari/endüstriyel tip,

ethernet anahtarlar tasarlanıp geliştirilmektedir.

Mevcut katman 2 çözümlerinin anahtarlama yeteneğinin 240 GBit/s'den 6 TBit/s'ye yükseltilmesi ve bu sayede başta cep telefonu operatörlerinin ve internet servis sağlayıcılarının ağları olmak üzere tüm ağlardaki millileştirme oranının maksimum seviyeye çıkartılması hedeflenmektedir.

Ayrıca ethernet anahtar ailesi ürünlerinin tümü SDN/NFV uyumlu ağ cihazları haline getirilerek SDWAN (Software Defined Wide Area Network) ve vCPE (Virtual Customer Premises Equipment) çözümleri de sağlanmış olacaktır.

Katman 3 Çözümleri

Katman 3 çözümü olarak TURKAY Milli Yönlendiriciler tasarlanıp geliştirilmiştir. TURKAY Milli Yönlendiriciler, askeri tipte 48 GBit/s'lik ve 32 GBit/s'lik iki versiyon olarak çözüm sunmaktadırlar. 2020 yılının sonunda IP yönlendiriciler için hedeflenen olgunluğa tam olarak ulaşılması hedeflenmektedir.

TURKAY Milli Yönlendiricilerin geliştirilmesi için Milli Yönlendirici Ailesi Tasarımı Projesi başlatılmıştır ve bu projeyle

- 240 GBit/s'ye kadar yönlendirme yeteneği olan,
- 8/16/24/48 portlu konfigürasyonlar şeklinde ve
- Askeri tip ve ticari/endüstriyel tip,

IP yönlendiriciler tasarlanıp geliştirilmektedir. Bu sayede IP yönlendiriciler için de milli ve modüler donanım tasarım kütüphaneleri, yazılım tasarım kütüphaneleri ve mekanik tasarım kütüphaneleri elde edilecektir ki aynı çalışma kapsamında mevcut TURKAY milli yönlendiriciler de bu milli ve modüler tasarım kütüphaneleri ile entegre edilecek ve IP yönlendiriciler ile ilgili çözümlerin ethernet anahtarlar ile ilgili çözümlerle özellikle kod uyumluluğu ve bütünlüğü de sağlanacaktır. Yine bu proje kapsamında bir de kriptolu TURKAY Milli Yönlendirici tasarlanıp geliştirilecektir.

Mevcut katman 3 çözümlerinin yönlendirme yeteneğinin 240 GBit/s'den 6 TBit/s'ye yükseltilmesi ve bu sayede başta cep telefonu operatörlerinin ve internet servis sağlayıcılarının ağları olmak üzere tüm ağlardaki millileştirme oranının maksimum seviyeye çıkartılması hedeflenmektedir.

Ayrıca milli yönlendirici ailesi ürünlerinin tümü SDN/NFV uyumlu ağ cihazları haline getirilerek SDWAN ve vCPE çözümleri de sağlanmış olacaktır.

Bunlara ilaveten mevcut IP yönlendirici ailesi çözümleri içerisine, Wi-Fi erişim noktası cihazı çözümlerinin entegrasyonu da hedeflenmektedir. Bu sayede Wi-Fi erişim noktası özellikli IP yönlendirici çözümü de vizyona kazandırılmış olacaktır.

Özellikle internet servis sağlayıcılar tarafından genişband şebekelerde kullanılan, SSG (Service Selection Gateway) veya daha genel adıyla BRAS (Broadband Remote Access Server) olarak adlandırılan cihaz literatürde artık service router olarak adlandırılmaya başlamıştır. Bu cihazlar ile internet servis sağlayıcılar, müşterilerine internet kotası bazlı faturalama servisi sunmaktadır. Bu cihazlar aynı zamanda LI (Lawful Interception), diğer bir adıyla yasal dinleme amacıyla da kullanıldığından kritik derecede önemlidir.

Katman 4 - Katman 7 Çözümleri

Katman 4-katman 7 çözümü olarak tüm milli ağ cihazları için bir ağ yönetim yazılımının tasarlanıp geliştirilmesi için çalışmalar başlatılmıştır.

Bu kapsamdaki ağ yönetim yazılımı tasarımı projesi ile

- hem ethernet anahtarlar hem IP yönlendiriciler ile birlikte kullanılacak,
- Wi-Fi cihazları ile birlikte kullanılacak kablosuz ağ yönetim yazılımı ile entegre olacak,
- SNMP (Simple Network Management Protocol) tabanlı olacak,
- NETCONF tabanlı olacak,
- sektördeki ağ cihazları ile birlikte kullanılabilecek ve
- IP tabanlı ağların kontrolü, konfigürasyonu ve monitör edilmesi işlevlerini yerine getirecek

bir ağ yönetim yazılımı (NMS: Network Management Software) çözümü elde edilmiş olacaktır.

Mevcut katman 3 çözümlerinin yeteneklerinin IP tabanlı uygulamalar ile zenginleştirilmesi için

- Gömülü IP santral
- Gömülü VoIP uygulamaları
- Yük dengeleyici
- Milli DNS (Domain Name System) güvenlik cihazı

çözümlerinin sağlanması hedeflenmektedir.

Mikro Çözümler

Milli ağ cihazları vizyonu ile arzu edilen olgunluk seviyesine ulaşılıp ağ hiyerarşisindeki tüm ihtiyaçların adreslenmesi sağlandıktan sonraki en önemli adım olarak çözümlerin millileştirilme oranının arttırılması ve bu sayede IP ağlarında oluşabilecek güvenlik risklerinin minimum düzeye indirgenmesinin sağlanması görülmektedir. Bu kapsamda adreslenen çözümler ise

- Milli switch fabric,
- Milli yönlendirme protokolü,
- Milli VPN protokolü ve
- Milli SFP modülüdür.

Milli switch fabric ve milli SFP modülü ile, milli ağ cihazlarının donanım seviyesinde maksimum düzeyde millileştirilmesi sağlanabilecek ve ayrıca olası malzeme tedariği kısıtları ve engelleri için çözüm üretilmiş olacaktır.

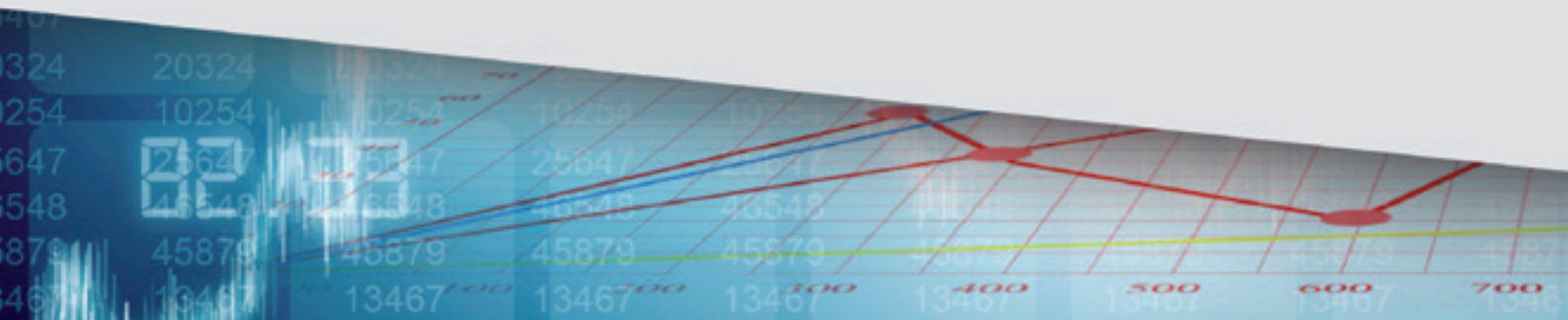
SFP modülleri, ethernet anahtar ve IP yönlendirici ekipmanı kullanılan her ağda bu ekipmanların ilgili port sayıları adedinde ithalatı yapılan ürünlerdir. Fiber optik kablonun ethernet anahtar veya IP yönlendirici ekipmanına sonlandırılabilmesi için kullanılan bu ürünler adet olarak en çok ithal edilen haberleşme ürünüdür. SFP, SFP+, XFP, QSFP/QSFP+, CFP ve QSFP28 vb. onlarca modeli bulunmakla birlikte her modelin mesafe, dalga boyu, hız, fiber/bakır destek durumlarına göre düşünüldüğünde yüzlerce alt modeli mevcuttur. Bu modüllerinin yerli olarak üretilmesi bilgi güvenliği anlamında önemli görülmektedir çünkü üzerinden geçen paketlerin manipüle edilmesi teknik olarak mümkün olmaktadır.

Milli yönlendirme protokolü sayesinde de milli ağ cihazlarının yazılım seviyesinde maksimum düzeyde millileştirilmesi sağlanabilecektir. Öngörülen söz konusu protokol ile savaş zamanı ve kriz zamanı durumlarında ağlarda güvenilir komşuluk ilişkileri kurulabilecek, bu güvenilir komşuluk ilişkileri ile ağların idamesi sağlanabilecek ve de ilgili güvenilir komşuluk ilişkilerini kuramayacak ağ cihazlarının ağdan izole edilmesi (ve böylece ağı manipüle etmelerinin önlenmesi) sağlanabilecektir. Milli yönlendirme protokolü, istenirse ithal ürünler için de kullanma zorunluluğu getirilmesi şartıyla, sektördeki ithal ürünlerin de bir seviyeye kadar güvenli olarak kullanımını sağlamaya yarayabilecektir.

VPN protokolleri iki nokta arasında güvenli veri iletimi sağlamak üzere tasarlanmış servislerdir. Böylece herhangi ilave bir fiziksel donanım kullanmadan, VPN desteği olan mevcut donanımlarla güvenli iletişim sağlamak üzere kullanılmakta olup kullanım kolaylığından dolayı özellikle sivil haberleşme sektöründe yaygın olarak tercih edilmektedir. Bu nedenle bilgi güvenliği kapsamında bir milli VPN protokolü tasarlanması önem arz etmektedir.

Satış ve Pazarlama Çözümleri

Milli ağ cihazları vizyonunun ticari faydalarının maksimum düzeye getirilebilmesi için ilgili sektörün dinamiklerine uygun bir satış ve pazarlama ağı oluşturulması gerekmektedir. Halihazırda bu konudaki çalışmalar ve girişimler devam etmektedir.



Satış Sonrası Hizmetler için Çözümler

Milli ağ cihazları ve çözümlerinin garanti süresi boyunca ve garanti süresi sonrasındaki bakım onarım faaliyetleri için satış sonrası hizmetler ile ilgili çözümler ile desteklenmesi, sektördeki faaliyetler açısından en az tasarım, geliştirme ve üretim kadar önemlidir. Bu kapsamda satış ve pazarlama ağı olarak kullanılacak altyapı kullanılabileceği gibi farklı bir ekosistem oluşturulması da mümkündür.

İlgili bakım, onarım ve teknik destek altyapısında kullanılacak kalifiye personelin yetiştirilmesi için de aSAP (ASELSAN Sertifikalı Ağ Personeli) / aCNP (ASELSAN Certified Network Personel) şeklinde isimlendirilebilecek bir program dahilinde eğitim ve sertifikasyon sağlanması öngörülmektedir.

Bahsedilen eğitim ve sertifikasyon kapsamında kullanılmak üzere talep edenlere ücretsiz olarak sağlanabilecek bir uygulama yazılımına ihtiyaç olacaktır. Bu amaçla tasarlanıp geliştirilecek aMACLAB (ASELSAN Milli Ağ Cihazları Laboratuar Yazılımı) hem öğrencilerin, hem akademisyenlerin, hem de kullanıcıların operasyonel işler için ve ağ tasarımı ve geliştirmesi için kullanabileceği bir araç olacaktır. Söz konusu uygulama yazılımı, bu sayede satış sonrası hizmetler için önemli bir araç olmasının yanı sıra üniversitelerde ilgili alanlarda çalışacak öğrenciler ve akademisyenler için de faydalı olacak ve ilgili ürünlerin benimsenmesini sağlayacaktır. Nitekim sektördeki bazı markaların ülkemizdeki üniversitelerde benzer uygulamalar ile kurslar ve hatta akademisyenler aracılığıyla dersler açarak dolaylı bir pazarlama ve satış kanalı açtığı bilinmektedir.

Bunlara ilaveten bakım, onarım ve teknik destek altyapısının, sesli mesajları ve e-posta mesajlarını karşılayacak bir çağrı merkezi ile ve web üzerinden mesajlaşma (chat) için kullanılacak servisler ile desteklenmesi gerekecektir.

IP Yönlendirici Teknolojileri

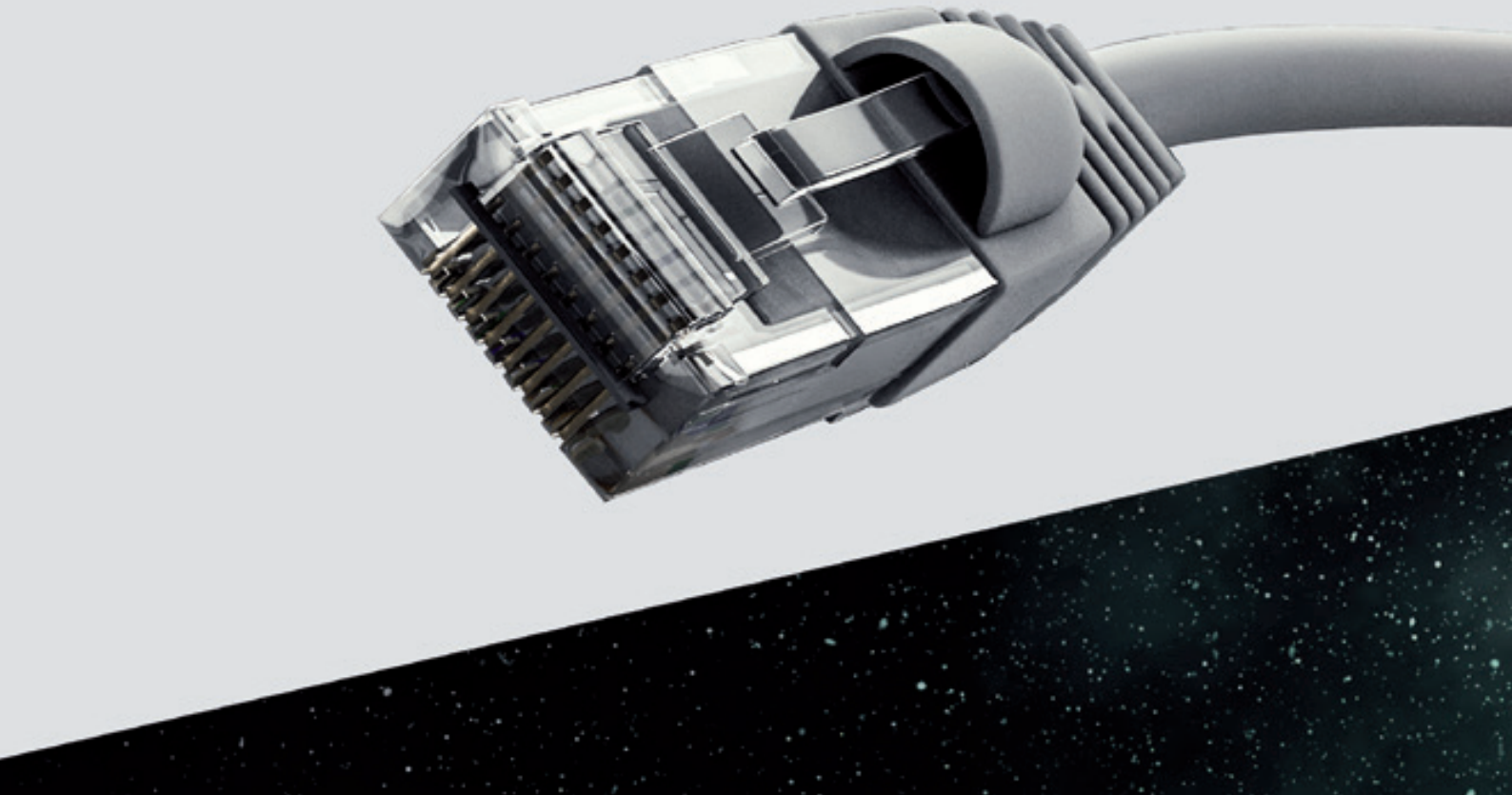
Hazırlayanlar
Mehmet Emre Berk, Ceren Yaren Erer, Fatma Aysu Köksal
HBT SMD Bilgi Teknolojileri Sistem Mühendisliği Müdürlüğü

Giriş

1966 yılında ARPANET ve Uluslararası Ağ Çalışma Grubu (INWG) tarafından çalışmalarına başlanmış olan ve o dönemlerde ağ geçidi olarak adlandırılan yönlendirici cihazları günümüzde IP tabanlı bir çözüme erişerek gelişimini sürdürmekle birlikte yaklaşık 15 milyar $'lık bir pazar hacmine ulaşmış bulunmaktadır.[1] Dijitalleşme süreci ile bilgi teknolojilerinde artan haberleşme ihtiyacı ve buna karşılık artan hız, kapasite, cihaz sayısı ve farklı bağlantı arayüzleri ihtiyacı doğrultusunda IP yönlendiriciler ağ sistemlerinin temel bileşeni haline gelmiştir. Buna ek olarak, haberleşme trafiğinin çoğunu üzerinden geçiren IP yönlendiricilerin stratejik önemi her geçen gün artmaktadır. ASELSAN, Türkiye ve dünya pazarında yer alan askeri ve ticari/endüstriyel alanlardaki haberleşme ihtiyaçlarını karşılamaya yönelik 2014 yılında başladığı faaliyetleriyle özgün tasarıma sahip yerli ve milli IP yönlendirici çözümleri sunmaktadır.

IP Yönlendirici Nedir?

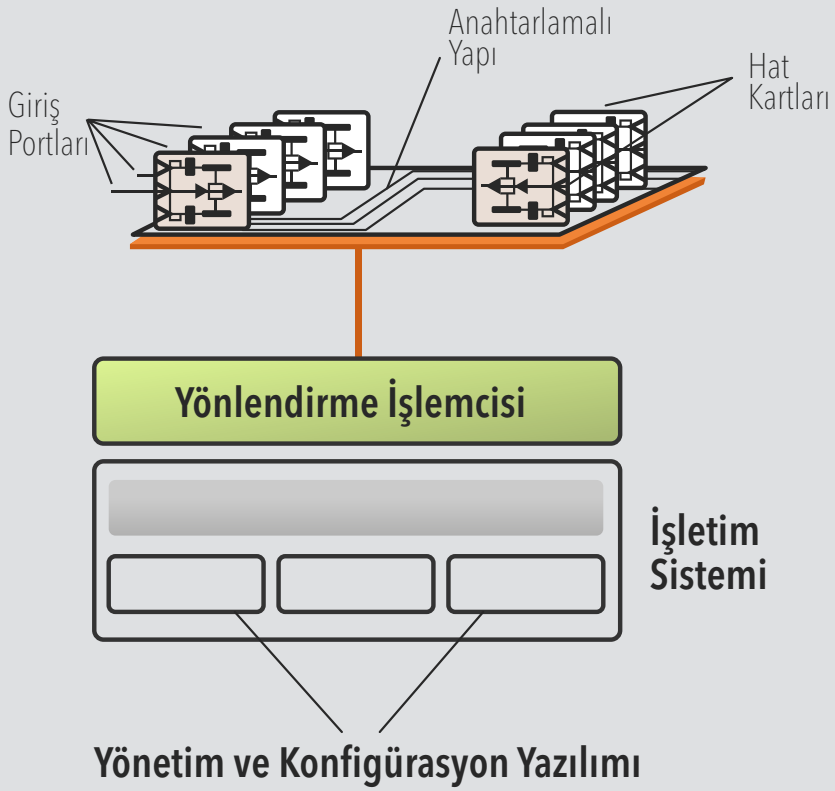
Bilgisayar ağlarındaki genel amaç bilgisayarlar arasında veri akışının sağlanmasıdır. Veri akışının sağlanması için büyüyen internet dünyasında farklı ağlara ihtiyaç duyulmaktadır. Farklı ağlar arasındaki paketlerin iletilme (forwarding) süreci olan yönlendirme (routing) işlemi, haberleşmenin sağlanması için gereklidir. Yönlendirme işleminin temelinde IP yönlendiriciler bulunmaktadır. IP yönlendiriciler, OSI (Open Systems Interconnection) modelinde katman 3 olan ağ katmanında çalışmaktadır ve trafik paketlerini ağ üzerinde iletmek ve hedef ağa yönlendirmek için mantıksal adres olan IP adreslerini kullanmaktadır.



IP yönlendiriciler, topolojideki ağlar hakkındaki bilgiyi komşu yönlendiriciler ile haberleşerek veya ağ yöneticisinin tanımlamasıyla elde etmektedir. Bu bilgi yönlendirme tablosunu (routing table) oluşturmak için kullanılmaktadır. Böylece IP yönlendiricide oluşan yönlendirme tablosu, ağ topolojisinde yer alan bütün hedef IP adreslerini komşu yönlendirici ve portlar ile eşlemekte ve ağ topolojisinin haritası çıkarılmaktadır. Aynı hedefe giden birden çok rota yönlendirme tablosunda yer alabilmektedir. Ağ yöneticisinin manuel olarak rota tanımlaması statik yönlendirmeyi ifade etmektedir. IP yönlendirici üzerinde çalıştırılan belirli bir yönlendirme algoritmasını (Routing Algorithm) kullanan protokol ile rotaların otomatik öğrenilmesi ve belirli aralıklarla rota bilgilerinin güncellenmesi ise dinamik yönlendirmeyi ifade etmektedir.

Tipik bir IP yönlendiricide giriş portları, çıkış portları, switching fabric ve işlemci olmak üzere dört temel bileşen bulunmaktadır. Giriş portları, fiziksel bağlantı noktaları olmakla beraber gelen paketler için giriş noktalarıdır. Portlar genellikle 4, 8 veya 16 bağlantı noktasını destekleyen çevrim içi kartlardır. Switching fabric, gerekli anahtarlama işlemlerini yaparak giriş portlarını ve çıkış portlarını birbirleri ile ilişkilendirmektedir. Çıkış portları paketleri depolayarak bir çıkış bağlantısında hizmet için zamanlamaktadır. İşlemci, yönlendirme protokollerini kullanarak paket iletmede kullanılan yönlendirme tablosunu meydana getirmektedir. Temel IP yönlendirici mimarisi şekil 1'de gösterilmektedir.

Şekil 1: Temel IP Yönlendirici Mimarisi[2]



IP Yönlendiriciler kullanım amaçlarına göre üç temel sınıfa ayrılmaktadır:

- **Omurga yönlendiriciler:** Ağ hiyerarşisinde omurga seviyesinde konumlandırılan, çok sayıda LAN (Local Area Network) arayüzlerinin ve WAN (Wide Area Network) arayüzlerinin anahtarlama işlemini yapabilen yüksek performansa sahip IP yönlendiricilerdir. İnternet servis sağlayıcılar arasındaki bağlantıyı kurmaktadırlar. Genellikle modüler yapıya sahip olan bu cihazlar; 10/40/100 GBit/s'lik yüksek hızlarda çok sayıda porta sahip olmakla birlikte fiber optik bağlantı özelliğini de desteklemektedir.
- **Kurumsal yönlendiriciler:** Kurumsal veya kampüs ağlarında uç istasyonlarını birbirine bağlamayı amaçlamaktadır. Omurga yönlendiricilerin aksine düşük maliyetle mümkün olduğunca çok sayıda uç noktaya bağlantı sağlamak hedeflenmektedir. Farklı seviyede hizmet kalitelerine (QoS: Quality of Service) destek sunmaktadır.
- **Erişim yönlendiricileri:** Temel amaç, ev tüketicileri ve küçük şirketler gibi uç istasyonlarını internet servis sağlayıcısına bağlamaktır. Omurga yönlendiricilere ve kurumsal yönlendiricilere göre daha düşük maliyete, daha düşük performansa, 10/100 MBit/s gibi daha düşük hıza ve daha az sayıda porta sahiptir.

IP Yönlendiriciler ile ilgili ASELSAN Çözümleri

ASELSAN Milli Yönlendirici Ailesi, askeri platformlar ve endüstriyel uygulamalar için tasarlanmış OSI katman 3'te çalışan TURKAY IP yönlendiricilerden oluşmaktadır. Bu ailenin ürünleri, üst katmanlardaki bazı protokolleri de tam/kısmi olarak destekleyecek, sabit port sayılı ve tam yönetilebilir şekilde tasarlanmıştır. Bu cihazlar, port sayıları ve anahtarlama kapasitelerine göre orta/geniş ölçekli işletme kampüs ağlarında erişim kısmında, küçük/orta ölçekli işletme kampüs ağlarında dağıtım kısmında, küçük ölçekli ağ sistemlerinde ise omurga kısmında kullanılabilmektedir.

TURKAY Milli Yönlendirici Ailesinin tüm cihazları toplam 27 farklı model ve konfigürasyon olarak tablo 1'de sunulmuştur. Değişen port sayılarında ve port hızlarında bağlantı yeteneklerine sahip cihaz modelleri farklı fiziksel özelliklere sahiptir. Her konfigürasyonun hem askeri şartlara uygun olarak tasarlanmış modeli hem de ticari/endüstriyel ortamlara uygun tasarlanmış modeli bulunmaktadır. Askeri cihazlar, zorlu askeri koşullara dayanıklı ve hem çevre koşulları hem de elektromanyetik uyumluluk anlamında MIL-STD askeri standartları destekleyecek şekilde yapılmıştır. Ticari/endüstriyel cihazlar ise endüstriyel ortamlara uygun, uluslararası geçerli IEC (International Electrotechnical Commission) standartlarına ve CE (European Conformity) kriterlerine uyumlu şekilde tasarlanmıştır.

Cihazlarda, AC/DC güç kaynağı dahili olarak konumlandırılmıştır. Buna ilişkin olarak cihazlar, hem DC olarak 19 V-32 V değer aralığında, hem de AC olarak 110 V/220 V değerlerinde beslenebilmektedir. AC/DC geçiş herhangi bir performans kaybı yaşanmadan yapılabilmektedir. Yüksek akım, yüksek voltaj, düşük voltaj ve termal koruma önlemleri alınmıştır.

Tablo 1: TURKAY Milli Yönlendirici Ailesi Konfigürasyonları

Askeri Model Konfigürasyonları	Ticari/Endüstriyel Model Konfigürasyonları
8x10/100/1000Base-T + 2x1GE SFP/Combo; 8xPoE+	8x10/100/1000Base-T + 2x1GE SFP/Combo; 8xPoE+
8x10/100/1000Base-T + 4x10GE SFP+/Combo; 8xPoE+	8x10/100/1000Base-T + 4x10GE SFP+/Combo; 8xPoE+
16x10/100/1000Base-T + 4x1GE SFP/Combo; 16xPoE+	16x10/100/1000Base-T + 4x1GE SFP/Combo; 16xPoE+
16x10/100/1000Base-T + 4x10GE SFP+/Combo; 16xPoE+	16x10/100/1000Base-T + 4x10GE SFP+/Combo; 16xPoE+
24x10/100/1000Base-T + 4x1GE SFP/Combo; 24xPoE+	24x10/100/1000Base-T + 4x1GE SFP/Combo; 24xPoE+
24x10/100/1000Base-T + 4x10GE SFP+/Combo; 24xPoE+	24x10/100/1000Base-T + 4x10GE SFP+/Combo; 24xPoE+
24xSFP + 4x10GE SFP+/Combo	24xSFP + 4x10GE SFP+/Combo
44x10/100/1000Base-T + 4x1GE SFP/Combo	44x10/100/1000Base-T + 4x1GE SFP/Combo
44x10/100/1000Base-T + 4x10GE SFP+/Combo	44x10/100/1000Base-T + 4x10GE SFP+/Combo
46x10/100/1000Base-T + 2x10GE SFP+/ Combo (WAN Stacking: 4x10GE SFP+)	46x10/100/1000Base-T + 2x10GE SFP+/ Combo (WAN Stacking: 4x10GE SFP+)
48x10/100/1000Base-T + 4x1GE SFP/Combo	48x10/100/1000Base-T + 4x1GE SFP/Combo
48x10/100/1000Base-T + 4x10GE SFP+/Combo	48x10/100/1000Base-T + 4x10GE SFP+/Combo
TURKAY Dağıtım Milli Yönlendirici 16x10/100/1000Base-T + 2x1GE SFP/Combo; 3xPoE+	
TURKAY Omurga Milli Yönlendirici 24x10/100/1000Base-T + 2x1GE SFP/Combo; 3xPoE+	

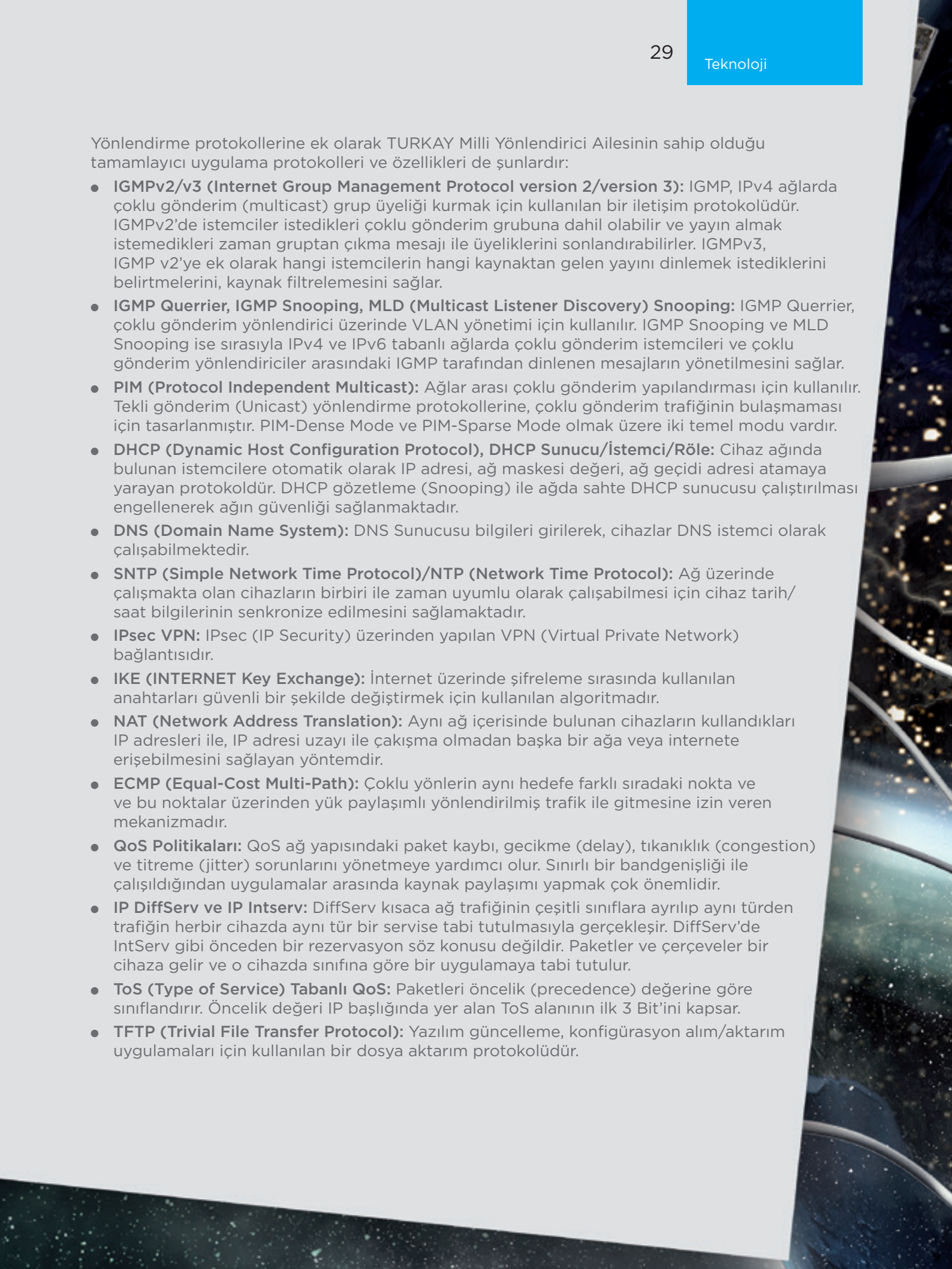
Cihazlar IPv4 ve IPv6 uyumlu çalışmakla beraber, performans özelliklerine ilişkin olarak 8 ayrı öncelik kuyruğuna sahiptir, 16K MAC (Media Access Control) adres tablosu bulundurmaktadır ve 10 KByte büyüklüğündeki jumbo paketleri desteklemektedir.

TURKAY Milli Yönlendirici Ailesi aşağıdaki yönlendirme protokollerini desteklemektedir:

- **Statik yönlendirme:** IP yönlendiricinin yol seçimi yapılandırmasında kullanılacak yolların ağ yöneticisi tarafından sabit olarak IP yönlendiriciye girilmesini sağlayan bir iletişim yöntemidir.
- **RIP (Routing Information Protocol):** Rotaları hesaplamak için Bellman-Ford algoritmasını kullanan bir yönlendirme protokolüdür.
- **OSPFv2 (Open Shortest Path First version 2):** IPv4 tabanlı, SPF (Shortest Path First) algoritmasını kullanan açık standart bir yönlendirme protokolüdür.
- **OSPFv3 (Open Shortest Path First version 3):** IPv6 tabanlı, SPF (Shortest Path First) algoritmasını kullanan açık standart bir yönlendirme protokolüdür.
- **BGP (Border Gateway Protocol):** İnternet üzerindeki otonom sistemler arasında geniş bilgi paylaşımı ve yönlendirmeye imkan sağlayan bir yönlendirme protokolüdür.
- **BGP Route Reflector:** Otonom ağlardaki tüm IBGP konuşan IP yönlendiricilerin döngü oluşmasını engelleyerek mevcut rotalar hakkında bilgi edinmesini sağlar.
- **IS-IS (Intermediate System to Intermediate System):** Genellikle büyük ağlarda kullanılan, hızlı yakınsama ve geniş ölçekleme sağlayan bir yönlendirme protokolüdür.

Yönlendirme protokollerine ek olarak TURKAY Milli Yönlendirici Ailesinin sahip olduğu tamamlayıcı uygulama protokolleri ve özellikleri de şunlardır:

- **IGMPv2/v3 (Internet Group Management Protocol version 2/version 3):** IGMP, IPv4 ağlarda çoklu gönderim (multicast) grup üyeliği kurmak için kullanılan bir iletişim protokolüdür. IGMPv2'de istemciler istedikleri çoklu gönderim grubuna dahil olabilir ve yayın almak istemedikleri zaman gruptan çıkma mesajı ile üyeliklerini sonlandırabilirler. IGMPv3, IGMP v2'ye ek olarak hangi istemcilerin hangi kaynaktan gelen yayını dinlemek istediklerini belirtmelerini, kaynak filtrelemesini sağlar.
- **IGMP Querrier, IGMP Snooping, MLD (Multicast Listener Discovery) Snooping:** IGMP Querrier, çoklu gönderim yönlendirici üzerinde VLAN yönetimi için kullanılır. IGMP Snooping ve MLD Snooping ise sırasıyla IPv4 ve IPv6 tabanlı ağlarda çoklu gönderim istemcileri ve çoklu gönderim yönlendiriciler arasındaki IGMP tarafından dinlenen mesajların yönetilmesini sağlar.
- **PIM (Protocol Independent Multicast):** Ağlar arası çoklu gönderim yapılandırması için kullanılır. Tekli gönderim (Unicast) yönlendirme protokollerine, çoklu gönderim trafiğinin bulaşmaması için tasarlanmıştır. PIM-Dense Mode ve PIM-Sparse Mode olmak üzere iki temel modu vardır.
- **DHCP (Dynamic Host Configuration Protocol), DHCP Sunucu/İstemci/Röle:** Cihaz ağında bulunan istemcilere otomatik olarak IP adresi, ağ maskesi değeri, ağ geçidi adresi atamaya yarayan protokoldür. DHCP gözetleme (Snooping) ile ağda sahte DHCP sunucusu çalıştırılması engellenerek ağın güvenliği sağlanmaktadır.
- **DNS (Domain Name System):** DNS Sunucusu bilgileri girilerek, cihazlar DNS istemci olarak çalışabilmektedir.
- **SNTP (Simple Network Time Protocol)/NTP (Network Time Protocol):** Ağ üzerinde çalışmakta olan cihazların birbiri ile zaman uyumlu olarak çalışabilmesi için cihaz tarih/saat bilgilerinin senkronize edilmesini sağlamaktadır.
- **IPsec VPN:** IPsec (IP Security) üzerinden yapılan VPN (Virtual Private Network) bağlantısıdır.
- **IKE (INTERNET Key Exchange):** İnternet üzerinde şifreleme sırasında kullanılan anahtarları güvenli bir şekilde değiştirmek için kullanılan algoritmadır.
- **NAT (Network Address Translation):** Aynı ağ içerisinde bulunan cihazların kullandıkları IP adresleri ile, IP adresi uzayı ile çakışma olmadan başka bir ağa veya internete erişebilmesini sağlayan yöntemdir.
- **ECMP (Equal-Cost Multi-Path):** Çoklu yönlerin aynı hedefe farklı sıradaki nokta ve ve bu noktalar üzerinden yük paylaşımlı yönlendirilmiş trafik ile gitmesine izin veren mekanizmadır.
- **QoS Politikaları:** QoS ağ yapısındaki paket kaybı, gecikme (delay), tıkanıklık (congestion) ve titreme (jitter) sorunlarını yönetmeye yardımcı olur. Sınırlı bir bandgenişliği ile çalışıldığından uygulamalar arasında kaynak paylaşımı yapmak çok önemlidir.
- **IP DiffServ ve IP Intserv:** DiffServ kısaca ağ trafiğinin çeşitli sınıflara ayrılıp aynı türden trafiğin herbir cihazda aynı tür bir servise tabi tutulmasıyla gerçekleşir. DiffServ'de IntServ gibi önceden bir rezervasyon söz konusu değildir. Paketler ve çerçeveler bir cihaza gelir ve o cihazda sınıfına göre bir uygulamaya tabi tutulur.
- **ToS (Type of Service) Tabanlı QoS:** Paketleri öncelik (precedence) değerine göre sınıflandırır. Öncelik değeri IP başlığında yer alan ToS alanının ilk 3 Bit'ini kapsar.
- **TFTP (Trivial File Transfer Protocol):** Yazılım güncelleme, konfigürasyon alım/aktarım uygulamaları için kullanılan bir dosya aktarım protokolüdür.



TURKAY Milli Yönlendirici Ailesi yönetilebilirlik anlamında birer adet konsol, CLI (Command Line Interface) ve USB (Universal Serial Bus) arayüzüne sahip olmakla beraber desteklediği yönetimsel özellikler aşağıda sunulmuştur:

- **SNMPv1/v2/v3 (Simple Network Management Protocol version 1/version 2/version 3):** Cihazların uzaktan izlenmesi, konfigüre edilmesi ve yönetilmesi için yönetim bilgi birimleri (MIB: Management Information Base) adı verilen daha önce tanımlanmış parametre bilgilerini kullanan yönetim protokolüdür.
- **TELNET:** Cihaza IP adresi ile uzaktan erişim sağlanması için kullanılan protokoldür.
- **SSHv1/v2 (Secure Shell version 1/version 2):** IP adresi ile uzaktan erişimi güvenli (şifrelenmiş) olarak gerçekleştiren protokoldür.
- Web arayüzü üzerinden yönetim sağlanabilmektedir.
- TFTP ile yazılım güncelleme, sistem raporu alınması, uzaktan konfigürasyon yedeklemesi ve yüklemesi sağlar.
- **Cihaz içi test:** Cihazın yazılımsal ve donanımsal bileşenlerinin sürdürülebilir kontrolü sağlanmaktadır.
- **Modbus TCP:** Sunucu/istemci mimarisinde çalışan, daha çok endüstriyel otomasyon uygulamalarında kullanılan bir yönetim protokolüdür.
- **Syslog:** Cihaz içinde oluşan bilgi, uyarı, hata mesaj kayıtlarının tutulmasını sağlamaktadır.
- Ağ yönetim yazılımı tarafından izlenme ve yönetilme özelliği bulunmaktadır.

TURKAY Milli Yönlendirici Ailesinin öne çıkan ve fark yaratan özellikleri aşağıda sıralanmıştır.

- **Hat hızında (wirespeed) çalışma:** Cihazlar tüm portlarında, aynı anda, portların desteklediği en yüksek hızda, paket kaybetmeden anahtarlama yapabilmektedir. Bu sayede 8/12/16/24 portlu cihazların anahtarlama kapasitesi 140 GBit/s'e, 48 portlu cihazların ve SFP (Small Form Pluggable) portlarından oluşan 24 portlu cihazın anahtarlama kapasitesi 240 GBit/s'e kadar çıkabilmektedir.
- **Fansız soğutma tasarımı:** Tüm modellerde gerçekleştirilen fansız tasarım özelliği sayesinde, güç tüketim değeri azalmış ve fan kaynaklı yaşanan donanımsal sorunların önüne geçilmiştir.
- **Lisans:** Yazılım yığınında bulunan protokollerin ve uygulamaların tamamı ayrı lisanslama yetkisine ihtiyaç duyulmadan sınırsız kullanıma açıktır.
- **AVB (Audio Video Bridging) desteği:** Audio/video yayınlarının ethernet üzerinden tam senkronize ve düşük gecikmeli olarak iletilmesine olanak sağlanmaktadır.

Sonuç

21. yüzyıl ile birlikte yaşanan bilimsel ve teknolojik gelişmeler sonucunda haberleşme imkanları artmıştır. Küresel olarak artan dijitalleşme süreci ile birlikte bilgi teknoloji altyapısının temel birimi olan ağ cihazları toplum ve kamu güvenliği açısından stratejik önem kazanmıştır. Bu stratejik ihtiyacın giderilmesi noktasında TURKAY Milli Yönlendirici Ailesi yerli ve milli bir ürün ailesi olarak ortaya çıkmaktadır. Geliştirilen bu ürünler ASELSAN'da gerçekleştirilen bir çok sistem içerisinde aktif olarak kullanılmaktadır. HBT Sektör Başkanlığı tarafından yürütülen TASMUS-II Projesi'nde ve AZRA Projesi'nde konumlandırılmıştır. SST Sektör Başkanlığı tarafından yürütülen SİPER Projesi ve HBT Sektör Başkanlığı tarafından yürütülen Barbaros Yarı Ömür Modernizasyonu Projesi kapsamında kullanılması planlanmaktadır.

ASELSAN'ın TURKAY Milli Yönlendirici Ailesine ilişkin gelecek vizyonunda, cihaz ailesini 6 TBit/s'lik hıza sahip yeni aile üyeleriyle genişletmek, cihazlara SDN (Software Defined Network)/NFV (Network Function Virtualization) yetenekleri kazandırılmak ve cihazları her büyüklükteki bilgisayar ağlarında ve internet servis sağlayıcı ağlarında konumlandırma hedefleri bulunmaktadır. Planlanan bu çalışmalarla, yerli ve milli teknoloji kullanımı ile ülke çapında ihtiyaç duyulan güvenli bilgi teknolojileri altyapısı sağlanmış olacaktır.

Kaynakça

(1) International Data Corporation, 'https://bit.ly/308zppu'

(2) Keshav, S., & Sharma, R.(1998). Issues and trends in router design. IEEE Communications Magazine, 1998, 36.5:144-151.

Ethernet Anahtar Teknolojileri

Hazırlayan
Cem Karabakal, Emre Sönmez
HBT SMD Bilgi Teknolojileri Sistem Mühendisliği Müdürlüğü

Giriş

İlk standardı yaklaşık kırk yıl önce yayınlanan ethernet teknolojisi, günümüze kadarki süreçte onlarca standart ile zenginleşerek; maliyet, ölçeklenebilirlik, güvenilirlik ve yönetilebilirlik faktörlerinde yarattığı avantaj ile en yaygın kullanım alanı bulan ağ teknolojisi olarak ön plana çıkmaktadır. Bu gelişime paralel olarak bilgi teknolojilerinde artan cihaz sayısı ve buna karşılık artan hız, kapasite, port ihtiyacı doğrultusunda ethernet anahtarlar, ağ sistemlerinin vazgeçilmez bileşenleri haline gelmiştir. Bunun sonucunda ethernet anahtar pazarı günümüzde dünya çapında yıllık %2.3 büyüme oranıyla yaklaşık 30 milyar $'lık bir hacme ulaşmıştır.[1] ASELSAN, hem dünyadaki bu pazarın, hem de ülkemizin savunma sanayi alanındaki haberleşme ihtiyaçlarını karşılama amacıyla 2014 yılında başlanan faaliyetlerle yerli ve milli ethernet anahtar çözümleri sunmaktadır.

Ethernet Anahtar Nedir?

Bilgisayar ağlarındaki temel amaç bilgisayarlar arasında veri akışının sağlanmasıdır. Veri akışının sağlanması, günümüzün en yaygın kablolu ağ teknolojisi olan ethernetin kullanılması ve bilginin sıralı olarak dizilmiş olduğu ethernet çerçevelerinin bilgisayarlar arasında taşınması ile mümkündür.

Farklı üreticilere ait bilgisayarların ve ağ cihazlarının birbirleriyle sorunsuz ve verimli çalışması, söz konusu teknolojinin belirli standartlara göre tanımlanması ve üreticilerin bu standartlara uygun tasarım yapması ile temin edilmektedir. Bu konudaki öncü kurum olan IEEE (Institute of Electrical and Electronics Engineers), yerel alan ağ (LAN: Local Area Network) ve geniş alan ağ (WAN: Wide Area Network) teknolojisini standartlaştırarak IEEE 802 adı altında toplamıştır. Bunlar arasında günümüzde en yaygın kullanım alanı bulanı IEEE 802.3 (ethernet) ve IEEE 802.11 (Kablosuz LAN / Wi-Fi)'dir. IEEE 802.3, ethernetin fiziksel katmanına ilişkin standartlarını tanımlarken, IEEE 802.1 başlığı altında ise veri bağlantı katmanındaki işletimine ve yönetimine ilişkin standartlar belirlenmiştir.

Ethernetin fiziksel katmandaki gelişiminin tarihçesine bakacak olursak, 1980'li yıllarda ethernet, 10 MBit/s hızında (IEEE 802.3a-IEEE 802.3e) koaksiyel kablolar ile kullanım alanı bulmuştur. Koaksiyel kablolar, kurulum zorluğu ve maliyetleri neticesinde yerini 1990'lı yılların başında çift bükümlü (twisted pair) kablolara ve fiber optik kablolara bırakmıştır (IEEE 802.3i: 10Base-T, IEEE 802.3j: 10Base-F). Artan hız ihtiyacına karşılık çift bükümlü ethernet hatlarının önce 100 MBit/s hızında çalışmasıyla fast ethernet (IEEE 802.3u: 100Base-TX); sonrasında 1 GBit/s desteği ile Gigabit ethernet (IEEE 802.3ab: 1000Base-T); fiber optik hatlarda 1 GBit/s hız desteği ile 1000Base-X (IEEE 802.3z) ortaya çıkmıştır. 2000'li yıllarda bağlantılar fiber optik kablolar üzerinde 10GBase-SR/LR/ER (IEEE 802.3ae) etiketiyle, çift bükümlü kablolar üzerinde ise 10GBase-T (IEEE 802.3an) etiketiyle 10 GBit/s hızında desteklenmiştir. 2010 yılının başından günümüze kadarki süreçte çift bükümlü kablolardaki veri kapasitesi 25/40 GBit/s (IEEE 802.3bq: 25G/40GBase-T) hızlarına ulaşmıştır; Fiber optik kablolarda ise 25/40 GBit/s hızları 25Base-SR/LR/ER (IEEE 802.3by, IEEE802.3cc) ve 40Base-SR4/LR4/ER4 (IEEE 802.3ba) olarak standartlaştırılmıştır. Sonraki zamanlarda fiber arayüzlerdeki veri hızları 50/100/200/400 GBit/s değerlerini[2] sağlayacak şekilde geliştirilerek muhtelif standartlarla ve etiketlerle yayınlanmıştır.

ethernet anahtar, birden fazla anahtarlama portuna sahip olan bir ağ cihazıdır. Portlarına bağlı ethernet tabanlı cihazların birbirleriyle haberleşmesine olanak sağlamaktadır. Portları arasındaki bağlantıyı köprüleme (bridging) yaparak oluşturmaktadır ve OSI (Open Systems Interconnection) modelinde katman 2 olan veri bağlantı katmanında çalışmaktadır. Kendisine bağlı bir kaynak cihazdan aldığı ethernet çerçevesini, kendisine bağlı hedef cihaza ya da cihazlara iletimini (forwarding), çerçevenin MAC (Media Access Control) adreslerini kullanarak gerçekleştirmektedir. Ethernet anahtarların adres öğrenme kabiliyetleri olduğundan çerçevenin iletimi, bağlantı bulunan tüm portlarına değil, sadece hedef adresin ilişkili olduğu portuna yapılmaktadır. Köprülemeye ve iletime ilişkin standart IEEE 802.1d olarak tanımlanmıştır. Bu standartla, bir ağ tasarımı içerisinde farklı üreticilere ait ethernet anahtarların birbirlerine çerçeve iletimi mümkün kılınmaktadır.

İçerisinde birçok ethernet anahtar barındıran ağ sistemlerinde, cihazlar arasında yapılacak bağlantılar neticesinde, cihazlar arasında birden çok aktif yol bulunabileceği örgü (mesh) tipi ağ topolojileri oluşabilmektedir. Döngüler içeren bu topolojilerde, ethernet anahtarlar broadcast mesajları bağlantı bulunan tüm portlarına ilettiğinden, broadcast mesajlar yayın fırtınalarına (broadcast storm) sebep olabilmektedir. Bunun önüne geçilmesi için IEEE 802.1d altında tanımlanan STP (Spanning Tree Protocol), yayın fırtınalarını engellemek amacıyla, sadece tek bir aktif bağlantı olması için bazı portların iletişime kapatılmasını sağlamaktadır. Kapatılan port, aktif bağlantının kopması durumunda tekrar aktif hale gelerek örgü topoloji üzerinde hat yedekliliği de sağlanabilmektedir. STP'nin ağ topolojilerindeki değişikliklere hızlı yanıt verilmesi için hızlandırılmış hali RSTP (Rapid Spanning Tree Protocol) (IEEE 802.1w), sanal yerel alan ağlar (VLAN: Virtual LAN)'ın yapılandırıldığı ağlar üzerinde çalışabilmesi için de birden çok ağaç yapısının oluşturulabildiği MSTP (Multiple Spanning Tree Protocol) (IEEE 802.1s) tanımlanmıştır.

VLAN (IEEE 802.1q), bir yerel alan ağı üzerindeki kullanıcıların ve kaynakların mantıksal olarak gruplandırılması ve bu grupların ethernet anahtarın portlarına atanmasıyla yapılandırılmaktadır. Farklı gruplara ait portlar, birbirlerinden bağımsız ethernet anahtarlar gibi çalışmaktadır. Böylelikle bir ethernet anahtar üzerindeki çarpışma etki alanı azaltılarak bandgenişliğinin etkin kullanımı ve farklı kullanıcı gruplarının ayrılmasıyla güvenlik önlemleri sağlanmaktadır. Portların VLAN tanımı erişim (access) ya da demet (trunk) olarak tanımlanmaktadır. Demet tanımlı portlarda, VLAN kimlik bilgisi, çerçevenin katman 2 başlığı içinde 802.1q için ayrılmış alandaki 12 Bit'lik haneye yazılmaktadır. Böylece toplamda en fazla 4096 adet VLAN tanımı yapılabilmektedir.

Ethernet çerçevesi formatının IEEE 802.1q için ayrılmış alanı içerisinde VLAN kimlik bilgisininin yanı sıra 3 Bit'lik hane, verilerin sınıflandırılması için ayrılmıştır. Bu sınıflandırma ile verilere bir öncelik değeri atanarak, ethernet anahtarlar bu öncelik sırasına göre verinin iletimini yapmaktadır. Bir QoS (Quality of Service) yöntemi olan ve katman 2'de gerçekleştirilen bu yöntem CoS (Class of Service) (IEEE 802.1p) olarak adlandırılmaktadır. CoS etiketiyle önceliklendirilmiş çerçeveler ethernet anahtarların port kuyruklarında beklemektedir. Farklı önceliklere sahip çerçevelerin hangi sırada iletileceklerine ilişkin farklı kuyruk işleme yöntemleri vardır. Bunlar arasında önceliklendirilmiş çerçevelerin, her koşulda yüksek önceklikli paketlerin ilk önce gönderilmesini sağlayan Strict Priority ve önceliklendirme sırasına göre uygun katsayılarla, daha adil iletimini sağlayan kuyruk yönetimi Weighted Fair Queueing ön plana çıkmaktadır.

Sürekli hizmet veren ethernet yerel alan ağlarında kullanılan cihazların sayısının ve ağ karmaşıklığının zamanla artmasıyla, bu ağlarda performans arttırımına ve ağ yönetimine ilişkin olarak etkin yöntemler ortaya çıkmıştır.

Bunların öne çıkanları aşağıda sıralanmıştır:

- **LACP (Link Aggregation Control Protocol) (IEEE 802.1ad):** Cihazlar arasındaki birden fazla fiziksel hattı tek bağlantı olarak göstererek, veri hızında artış ve hat yedekliliği sağlamaktadır.
- **LLDP (Link Layer Discovery Protocol) (IEEE 802.1ab):** Ağ topolojilerinde, komşu cihazların kimlik bilgilerini ve yeteneklerini keşfetmeye olanak sağlamaktadır.
- **MAC Adres Yetkilendirmesi (IEEE 802.1x):** Bir kimlik doğrulama sunucusuna (örneğin, RADIUS (Remote Authentication Dial-In User Service) Sunucusu'na) bağlanarak, port bazında kimlik doğrulama işlemlerini gerçekleştirmektedir.
- **Port Aynalama (Mirroring):** Cihazın bir portundan ya da portlarından akan verinin, başka bir portuna kopyalanarak, hata ayıklama ve arıza giderme amaçlı izlenebilmesidir.

Ethernet anahtarlar fiziksel yapılarına, yönetilebilirlik özelliklerine ve ağ topolojisindeki konumlarına göre farklı sınıflarda yer alabilmektedir.

Fiziksel yapılarına göre sınıflandırıldığında, aşağıdaki üç ana başlık karşımıza çıkmaktadır:

- **Sabit port sayılı:** Üzerinde port arayüzlerinin ve port sayılarının sabit olduğu maliyet etkin cihazlardır.
- **Yığınlanabilir:** Sabit port sayılı cihazlara benzer görünüme sahip olup birden fazla cihazın özel yığın arayüzleri ya da WAN/Uplink portları ile yığınlanabildiği ve yığına ait tüm cihazların tek cihaz gibi yönetilebildiği cihazlardır.
- **Modüler:** Şase formunda olup şasesine takılıp çıkarılan genişleme modülleri ile port sayısı ve port arayüzleri değiştirilebilen cihazlardır.

Yönetilebilirlik özelliklerine göre sınıflandırıldığında, aşağıdaki üç ana başlık karşımıza çıkmaktadır:

- **Yönetilemeyen:** Konfigürasyon ihtiyacı bulunmayan, tak-çalıştır olarak ve daha çok masaüstü ortamlarda çalışan cihazlardır.
- **Kısmi yönetilebilir:** Yönetim işlemlerini kısmi olarak gerçekleştirebilen ve basit konfigürasyon girdileri oluşturulabilen cihazlardır.
- **Tam yönetilebilir:** Yönetim uygulamalarında CLI (Command Line Interface), web, TELNET, SSH (Secure Shell), SNMP (Simple Network Management Protocol), RADIUS, TACACS+ (Terminal Access Controller Access-Control System +), Syslog vb. protokolleri destekleyen, katman 2 özelliklerinde tam konfigürasyon yönetimi sağlayan ve bununla beraber desteklemesi durumunda daha üst katmandaki bazı protokollere (IGMP-Internet Group Management Protocol, ACL-Access Control List, Statik Yönlendirme vb.) ilişkin konfigürasyon girdileri oluşturulabilen cihazlardır.

Ağ topolojisindeki konumlarına (3 aşamalı ağ modeline) göre sınıflandırıldığında, aşağıdaki üç ana başlık karşımıza çıkmaktadır:

- **Erişim:** Uç istasyonların ve istemcilerin bağlandığı, 10/100/1000 MBit/s hızları destekleyen portlara sahip ve genellikle katman 3 özelliklerin kullanılmadığı kısımda çalışan cihazlardır.
- **Dağıtım:** Erişim ethernet anahtarların bağlandığı, 1/10 GBit/s hızları destekleyen portalara sahip ve genellikle katman 3 özelliklerin de kullanıldığı kısımda çalışan cihazlardır.
- **Omurga:** Dağıtım ethernet anahtarların bağlandığı, 10/40/100 GBit/s gibi yüksek hızları destekleyen portlara sahip, genellikle modüler yapıya sahip cihazlardır.

Ethernet Anahtarlar ile ilgili ASELSAN Çözümleri

ASELSAN ethernet Anahtar Ailesi, askeri platformlar ve ticari/endüstriyel uygulamalar için tasarlanmış, katman 2'de çalışan anahtarlama cihazlarından oluşmaktadır. Bu ailenin ürünleri, üst katmanlardaki bazı protokolleri de tam/kısmi olarak destekleyecek, sabit port sayılı ve tam yönetilebilir şekilde tasarlanmıştır. Bu cihazlar, port sayıları ve anahtarlama kapasitelerine göre orta/geniş ölçekli işletme kampüs ağlarının erişim kısmında, küçük/orta ölçekli işletme kampüs ağlarının dağıtım kısmında, küçük ölçekli ağ sistemlerinin ise omurga kısmında kullanılabilmektedir.

Ethernet anahtar ailesinin tüm cihazları toplam 42 farklı model ve konfigürasyon olarak tablo 1'de sunulmuştur. Cihaz konfigürasyonları ve bağlantı yetenekleri, cihazın sahip olduğu port sayısı ve bu portların desteklediği veri akış hızına göre değişmektedir. Her konfigürasyonun hem askeri şartlara uygun olarak tasarlanmış modeli hem de ticari/endüstriyel ortamlara uygun tasarlanmış modeli bulunmaktadır. Askeri cihazlar, zorlu askeri koşullara dayanıklı ve hem çevre koşulları hem de elektromanyetik uyumluluk anlamında MIL-STD askeri standartları destekleyecek şekilde yapılmıştır. Ticari/endüstriyel cihazlar ise endüstriyel ortamlara uygun, uluslararası geçerli IEC (International Electrotechnical Commission) standartlarına ve CE (European Conformity) kriterlerine uyumlu şekilde tasarlanmıştır.

Konfigürasyonların tamamında combo portu özelliği bulunduğundan, cihazların WAN portları ister fiber optik arayüzü isterse de bakır arayüzü olarak kullanılmaktadır. Cihazların tüm konfigürasyonlarının LAN portları, bakır arayüzü olarak ve buna alternatif oluşturacak şekilde ETHS-M-24SE4XG-N ve ETHS-I-24SE4XG-N modellerinin LAN arayüzleri, fiber optik arayüzü olarak tanımlanmıştır. Ethernet anahtar ailesinin 8/12/16/24 portlu konfigürasyonları için PoE+ opsiyon olarak sunulmaktadır. Böylelikle bakır LAN portlarına bağlanacak PoE+ (Power over ETHERHET +) beslenebilen cihazlara 25.5 Watt'a kadar güç beslemesi sağlanabilmektedir. Cihazlar, yüksek kapasiteli güç kaynakları ile tüm portlarından aynı anda PoE+ beslemesi yapabilecek şekilde planlanmıştır.

Cihazlarda, AC/DC güç kaynağı dahili olarak konumlandırılmıştır. Buna ilişkin olarak cihazlar, hem DC olarak 19 V-32 V değer aralığında, hem de AC olarak 110 V/220 V değerlerinde beslenebilmektedir. AC/DC geçiş herhangi performans kaybı yaşanmadan yapılabilmektedir. Yüksek akım, yüksek voltaj, düşük voltaj ve termal koruma önlemleri alınmıştır.

Tablo 1: ASELSAN Ethernet Anahtar Ailesi Konfigürasyonları

Askeri Modeller	Ticari /Endüstriyel Modeller	Konfigürasyon / Port Sayıları
ET-HS-M-08FE-2GE-P	ETHS-I-08FE2GE-P	8 adet 10/100Base-T Fast Ethernet, 2 adet 1 Gigabit Ethernet/SFP Combo, 8 adet PoE+ Besleme
ETHS-M-12FE-2GE-N	ETHS-I-12FE2GE-N	12 adet 10/100Base-T Fast Ethernet, 2 adet 1 Gigabit Ethernet/SFP Combo
ETHS-M-12FE-2GE-P	ETHS-I-12FE2GE-P	12 adet 10/100Base-T Fast Ethernet, 2 adet 1 Gigabit Ethernet/SFP Combo, 12 adet PoE+ Besleme
ETHS-M-16FE-4GE-N	ETHS-I-16FE4GE-N	16 adet 10/100Base-T Fast Ethernet, 4 adet 1 Gigabit Ethernet/SFP Combo
ETHS-M-16FE-4GE-P	ETHS-I-16FE4GE-P	16 adet 10/100Base-T Fast Ethernet, 4 adet 1 Gigabit Ethernet/SFP Combo, 16 adet PoE+ Besleme
ET-HS-M-24FE-4GE-N	ETHS-I-24FE4GE-N	24 adet 10/100Base-T Fast Ethernet, 4 adet 1 Gigabit Ethernet/SFP Combo
ET-HS-M-24FE-4GE-P	ETHS-I-24FE4GE-P	24 adet 10/100Base-T Fast Ethernet, 4 adet 1 Gigabit Ethernet/SFP Combo, 24 adet PoE+ Besleme
ET-HS-M-08GE-2GE-P	ETHS-I-08GE2GE-P	8 adet 10/100/1000Base-T Ethernet, 2 adet 1 Gigabit Ethernet/SFP Combo, 8 adet PoE+ Besleme
ETHS-M-08GE2XG-P	ETHS-I-08GE2XG-P	8 adet 10/100/1000Base-T Ethernet, 2 adet 10 Gigabit Ethernet/SFP+ Combo, 8 adet PoE+ Besleme
ETHS-M-12GE-2GE-N	ETHS-I-12GE2GE-N	12 adet 10/100/1000Base-T Ethernet, 2 adet 1 Gigabit Ethernet/SFP Combo
ETHS-M-12GE-2GE-P	ETHS-I-12GE2GE-P	12 adet 10/100/1000Base-T Ethernet, 2 adet 1 Gigabit Ethernet/SFP Combo, 12 adet PoE+ Besleme
ETHS-M-16GE-4GE-N	ETHS-I-16GE4GE-N	16 adet 10/100/1000Base-T Ethernet, 4 adet 1 Gigabit Ethernet/SFP Combo
ETHS-M-16GE-4GE-P	ETHS-I-16GE4GE-P	16 adet 10/100/1000Base-T Ethernet, 4 adet 1 Gigabit Ethernet/SFP Combo, 16 adet PoE+ Besleme
ET-HS-M-24GE-4GE-N	ETHS-I-24GE4GE-N	24 adet 10/100/1000Base-T Ethernet, 4 adet 1 Gigabit Ethernet/SFP Combo
ET-HS-M-24GE-4GE-P	ETHS-I-24GE4GE-P	24 adet 10/100/1000Base-T Ethernet, 4 adet 1 Gigabit Ethernet/SFP Combo, 24 adet PoE+ Besleme
ET-HS-M-48GE-4GE-N	ETHS-I-48GE4GE-N	48 adet 10/100/1000Base-T Ethernet, 4 adet 1 Gigabit Ethernet/SFP Combo
ETHS-M-48GE4XG-N	ETHS-I-48GE4XG-N	48 adet 10/100/1000Base-T Ethernet, 4 adet 10 Gigabit Ethernet/SFP+ Combo
ETHS-M-48GE2XG-N	ETHS-I-48GE2XG-N	48 adet 10/100/1000Base-T Ethernet, 2 adet 10 Gigabit Ethernet/SFP+ Combo (WAN Stacking: 4 adet 10 Gigabit Ethernet/SFP+)
ET-HS-M-48GE-2GE-N	ETHS-I-48GE2GE-N	48 adet 10/100/1000Base-T Ethernet, 2 adet 1 Gigabit Ethernet/SFP Combo
ETHS-M-24SE4XG-N	ETHS-I-24SE4XG-N	24 adet 1000Base-LX/SX/ZX SFP, 4 adet 10 Gigabit SFP+ Combo
ET-HS3-M-4GE-2GE-N	ETHS3-I-4GE2GE-N	4 adet 10/100/1000Base-T Ethernet, 2 adet 1 Gigabit Ethernet/SFP Combo Katman 3 Anahtar

Cihazlar IPv4 ve IPv6 uyumlu çalışmakla beraber, performans özelliklerine ilişkin olarak sekiz ayrı öncelik kuyruğuna sahiptir, 16K MAC adres tablosu bulundurmaktadır ve 10 KByte büyüklüğündeki jumbo paketleri desteklemektedir.

ASELSAN ethernet anahtar ailesi, veri bağlantı katmanında aşağıdaki protokolleri ve özellikleri desteklemektedir.

- STP, RSTP, MSTP
- 802.1q VLAN, Port Tabanlı VLAN, Voice VLAN
- QoS Politikaları, CoS Tabanlı QoS
- Strict Priority ve Weighted Fair Queueing kuyruk özellikleri
- LACP
- LLDP
- MAC adres yetkilendirmesi
- Port aynalama

Cihazlar, internet katmanında aşağıdaki protokolleri ve özellikleri desteklemektedir:

- **IGMPv2/v3, IGMP Sorgulayıcı (Querrier), IGMP Gözetleme (Snooping), MLD (Multicast Listener Discovery) Gözetleme:** IGMP, TCP/IP'de çoklu dağıtım (multicast) üyelerini yönetmek için kullanılan bir iletişim protokolüdür. IGMP gözetleme ile ağdaki IGMP trafiği dinlenerek, sadece IGMP grubuna üye portlara çoklu dağıtım yapılarak ağ trafiği performansı arttırılmaktadır. IPv6 tabanlı ağlarda MLD gözetleme kullanılmaktadır.
- **IP Access Security:** Erişim kontrol listeleri (ACL) oluşturarak, gelen/giden trafiği kaynak/hedef IP adresi bazında filtrelemeyi sağlamaktadır.
- **Login Security:** Cihaza web arayüzü ya da CLI ile erişimi, kullanıcı adı ve şifre ile güvenli olarak sağlamaktadır.
- **QoS politikaları, IP DiffServ (Differentiated Services) ve ToS (Type of Service) Tabanlı QoS:** Ethernet paketlerinin katman 3 başlığındaki DSCP (Differentiated Services Code Point) alanına 6 Bit'lik öncelik değeri atanarak, QoS Önceliklendirme gerçekleştirilmektedir.
- **Statik yönlendirme:** Farklı ağlar arasında IP bazlı yönlendirme yapılabilmesi için statik rotaların yazılabilmesidir. Katman 3 anahtarda gerçeklenmiş olup toplam 32 adet rota yazılabilmektedir.
- **TWAMP (Two Way Active Measurement Protocol):** Sunucu/istemci mimarisinde çalışan iki cihaz arasındaki ağ performansını hız, gecikme, seğirme değerleri bazında ölçüp gösteren protokoldür. Katman 3 anahtarda gerçeklenmiştir.

Cihazlar, uygulama katmanında aşağıdaki protokolleri ve özellikleri desteklemektedir:

- **DHCP (Dynamic Host Configuration Protocol), DHCP sunucu/istemci/röle, DHCP gözetleme:** Cihaz ağında bulunan istemcilere otomatik olarak IP adresi, ağ maskesi değeri, ağ geçidi adresi atamaya yarayan protokoldür. DHCP gözetleme ile ağda sahte DHCP sunucusu çalıştırılması engellenerek ağın güvenliği sağlanmaktadır.
- **RMON (Remote Network Monitoring):** Merkezi bir lokasyondan, hatların monitör ve analiz edilmesi ve bu hatlarla ilgili sorun giderme işlemlerinin yapılabilmesi için SNMP'nin uzantısı olarak geliştirilmiş bir protokoldür. Trafik tıkanıklığı, paket çarpışmaları ve paket düşürmeye ilişkin istatistiklerin izlenmesine olanak sağlamaktadır.
- **DNS (Domain Name System):** DNS sunucusu bilgileri girilerek, cihazlar DNS istemci olarak çalışabilmektedir.
- **SNTP (Simple Network Time Protocol):** Ağ üzerinde çalışmakta olan cihazların birbiri ile zaman uyumlu olarak çalışabilmesi için cihaz tarih/saat bilgilerinin senkronize edilmesini sağlamaktadır.
- **PTP (Precision Time Protocol):** Senkronizasyon mesajlarına zaman damgası da vurarak SNTP'den daha hassas tarih/saat bilgilerinin paylaşılmasını sağlamaktadır.
- **TFTP (Trivial File Transfer Protocol):** Yazılım güncelleme, konfigürasyon alım/aktarım uygulamaları için kullanılan bir dosya aktarım protokolüdür.

ASELSAN Ethernet Anahtarlar tam yönetilebilirlik anlamında birer adet CLI, konsol ve USB arayüzüne sahiptir. Bu arayüzlerle komut satırından yönetim, web arayüzü üzerinden yönetim, TFTP ile yazılım güncelleme ve sistem raporu alma, cihaz içi test işlemleri gerçekleştirilmektedir. Merkezi yapıda çalışan ağ yönetim yazılımı tarafından uzaktan izleme ve yönetilme işleri yapılabilmektedir. Bunların yanı sıra yönetimsel özelliklere ilişkin aşağıdaki protokoller desteklenmektedir:

- **SNMPv1/v2/v3:** Cihazların uzaktan izlenmesi, konfigüre edilmesi ve yönetilmesi için yönetim bilgi birimleri (MIB: Management Information Base) adı verilen daha önce tanımlanmış parametre bilgilerini kullanan yönetim protokolüdür.
- **TELNET:** Cihaza IP adresi ile uzaktan erişim sağlanması için kullanılan protokoldür.
- SSHv1/v2: IP adresi ile uzaktan erişimi, güvenli (şifrelenmiş) olarak gerçekleştiren protokoldür.
- **TACACS+:** Kimlik doğrulama ve yetkilendirme protokolüdür.
- **Modbus TCP:** Sunucu/istemci mimarisinde çalışan, daha çok endüstriyel otomasyon uygulamalarında kullanılan bir yönetim protokolüdür.
- **Syslog:** Cihaz içinde oluşan bilgi, uyarı, hata mesaj kayıtlarının tutulmasını sağlamaktadır.

ASELSAN Ethernet Anahtar Ailesinin öne çıkan ve fark yaratan özellikleri aşağıda sıralanmıştır:

- **Hat hızında (wirespeed) çalışma:** Cihazlar tüm portlarında, aynı anda, portların desteklediği en yüksek hızda, paket kaybetmeden anahtarlama yapabilmektedir. Böylelikle 8/24 portlu cihazların anahtarlama kapasitesi 56 GBit/s'e, 48 portlu cihazların anahtarlama kapasitesi 240 GBit/s'e kadar çıkabilmektedir.
- **Trafik şekillendirme:** Ticari/endüstriyel cihazlarda bulunan trafik şekillendirme özelliği sayesinde, internet servis sağlayıcıların sunduğu haberleşme altyapısının imkan verdiği trafik hızından daha yüksek hızda gelen paketlerin bir tampon (buffer) mekanizması sayesinde paket kaybı yaşanmadan iletimine imkan sağlanmaktadır.
- **SyncE (Synchronous Ethernet) (ITU-T G.8261):** Bir ITU standardıdır. Cihazların bakır arayüzlerinde ethernet üzerinden, frekans ve faz senkronizasyonunu yüksek çözünürlükte sağlayan bu teknoloji, hücresel ve mobil sistemlerde kullanılmaktadır.
- **AVB (Audio Video Bridging) (IEEE 802.1qav-at):** Audio/video yayınlarının ethernet üzerinden tam senkronize ve düşük gecikmeli olarak iletilmesine olanak sağlamaktadır.
- **ERPS (Ethernet Ring Protection Switching) (ITU-T G.8032):** Halka topolojilerde döngülerin oluşmasını engellemektedir. Aktif bağlantının kopması durumunda veri akışının ters yönlü yapılmasını sağlamaktadır. STP, RSTP ve MSTP'ye göre daha hızlı geçiş süreleri ile hizmet sağlamaktadır.

ASELSAN Ethernet Anahtar Ailesine gelecekte kazandırılması planlanan özellikler şöyle sıralanmıştır:

- **Statik yönlendirme:** Halihazırda ETHS3-M-4GE2GE-N ve ETHS3-I-4GE2GE-N model numaralı katman 3 anahtarda gerçeklenmiş olan statik yönlendirmenin tüm cihaz ailesine kazandırılması planlanmaktadır.
- **TWAMP:** Halihazırda ETHS3-M-4GE2GE-N ve ETHS3-I-4GE2GE-N model numaralı katman 3 anahtarda gerçeklenmiş olan TWAMP'ın tüm cihaz ailesine kazandırılması planlanmaktadır.
- **Yığınlama:** WAN arayüzleri ile bağlanarak birden çok cihaz yığınlanabilecek ve cihaz topluluğu tek bir ethernet anahtar gibi çalışıp yönetilebilecektir.
- **RADIUS AAA:** Halihazırda RADIUS kapsamında gerçeklenmiş kimlik doğrulama (authentication) fonksiyonunun yanında, yetkilendirme (authorization) ve aktivite izlenmesi (accounting) fonksiyonlarının geliştirilmesi planlanmaktadır.

ASELSAN 3U VPX Ethernet Anahtar Kartı

3U VPX (Versatile Performance Switching) formu; boyut, ağırlık ve güç (SWaP) parametrelerinde öne çıkan avantajları ve getirdiği dayanıklılık neticesinde gömülü askeri ve havacılık/uzay uygulamalarında tercih edilmektedir. Bu tür görev kritik uygulamalarda ethernet teknolojisine ilişkin ihtiyaçların karşılanması için ASELSAN 3U VPX Ethernet Anahtar Kartı çözümü oluşturulmuştur.

ASELSAN 3U VPX Ethernet Anahtar Kartı, 16 portlu olarak 3U VPX formuna ve MOD3-SWH-16T profiline uygun olarak tasarlanmıştır. Bağlantı konnektörleri, VITA (VME Bus International Trade Association) 46 standardını desteklemektedir. Ethernet anahtar ailesindeki cihazların desteklediği tüm katmanlara ilişkin uygulama özelliklerine ve yönetim arayüzlerine sahiptir. ASELSAN 3U VPX Ethernet Anahtar Kartı zorlu çevre koşullarında çalışacak şekilde tasarlanmıştır.

Sonuç

Ülkemiz, Kıbrıs Barış Harekatında edindiği acı tecrübeler sonucu kendi telsizlerini üretme gayesi ile ASELSAN'ı kurmuş, günümüzde hem askeri hem de profesyonel tip telsizlerini yerli/milli imkanlarla üretebilir hale gelmiştir. Aynı acı tecrübeleri ağ teknolojilerinde edinmeden, yerlilik/millilik anlamında benzer hedefleri ağ cihazları alanında da gerçekleştirmenin ilk adımı olarak ASELSAN Ethernet Anahtar Ailesi ürünleri ortaya çıkmıştır. Gelinen nokta itibarıyla bu ürünler ASELSAN'da gerçekleştirilen birçok sistem içinde kullanılmaya başlanmıştır. Askeri Cihazlar, HBT Sektör Başkanlığı tarafından yürütülen AZRA projesinde, REHİS Sektör Başkanlığı tarafından yürütülen Silah Tespit Radarı projesinde; Ticari/endüstriyel cihazlar ise HBT Sektör Başkanlığı tarafından yürütülen İstanbul Büyükşehir Belediyesi Geniş Alan Telsiz sisteminde, Emniyet Genel Müdürlüğü Sayısal Haberleşme şebekesinde, Deniz Kuvvetleri Komutanlığı ÇBSTM Kurulum Bütünleştirme projesinde, TVEG Entegre Muhabere Sistemi projesinde kullanılmaktadır. UGES Sektör Başkanlığı tarafından yürütülen Kent Güvenlik Yönetim Sistemi Projesi kapsamında teslim/sipariş edilen ticari/endüstriyel cihaz sayısı 18541 adede ulaşmıştır. 3U VPX Ethernet Anahtar Kartının, REHİS Sektör Başkanlığı bünyesinde yürütülen Radar Sistemlerinde konumlandırılan sinyal işleme birimlerinde kullanılması planlanmaktadır.

ASELSAN'ın ethernet anahtarlara ilişkin gelecek vizyonu, cihaz ailesini 6 TBit/s mertebesinde anahtarlama kapasitesine sahip yeni aile üyeleriyle genişletmeyi ve cihazları SDN (Software Defined Network)/NFV (Network Function Virtualization) teknolojileri ile uyumlu hale getirmeyi hedeflemektedir. Böylelikle mevcut ve gelecekte çıkacak cihazların, her büyüklükteki bilgisayar ve servis sağlayıcı ağlarının her kısmında konumlandırması sağlanacaktır. Bunun sonucunda normal, acil, afet ve savaş durumlarında yerli ve milli teknolojiden elde edilen fayda ülke genelinde arttırılacaktır.

Kaynakça

(1) IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Weakness in Fourth Quarter of 2019

(2) IEEE 802.3 Ethernet Working Group, Archive of Completed Work: 'http://www.ieee802.org/3/archive.html'

Wi-Fi Teknolojileri

Hazırlayan
Cem Karabakal, Ozan Yüksel, Gülçin Sinem Akçakoyunlu
HBT SMD Bilgi Teknolojileri Sistem Mühendisliği Müdürlüğü

Giriş

Son otuz yılda haberleşme alanında artan hareket edilebilirlik ihtiyacına karşılık, kablosuz yerel alan ağı (WLAN: Wireless Local Area Network) teknolojilerinde öne çıkan Wi-Fi (IEEE 802.11) teknolojisi, 1997 yılında ilk standardının yayınlanmasından günümüze kadarki süreçte internet ekosistemindeki kullanım oranını her geçen gün artırmaktadır. Wi-Fi'ın avantajları; lisanssız bantta kullanılması, kullanıcıya kazandırdığı hareket kabiliyeti, her geçen yıl artan hız desteği, birlikte çalışabilirlik ve ağın ölçeklendirilmesinde yarattığı esneklik olarak sıralanmaktadır. Bu avantajlarla Wi-Fi, sadece ticari/endüstriyel alanda değil aynı zamanda askeri alanda da emniyet önlemleri alınarak kullanımı rağbet görmektedir. ASELSAN, TAYAS (Taktik Yerel Alan Ağı) Projesi kapsamında, Wi-Fi tabanlı yeni ve özgün ürünler çıkarmış ve Kriptolu Kablosuz Ağ Cihazı (KKAC) ve Terminal Kablosuz Ağ Bağlantı Cihazı (TKABC) ile kablosuz özgürlüğü emniyetli hale getirmiştir.

Wi-Fi Teknolojisi Nedir?

Wi-Fi ismiyle bilinen teknoloji sayesinde bilgisayarlar, ağ cihazları ve bu teknolojiyi destekleyen nesneler birbirleriyle hava arayüzü ile bağlanarak kablosuz yerel alan ağı oluşturabilmektedir. Bu ağdaki cihazlar, Wi-Fi teknolojisi esaslarına göre veri iletimi gerçekleştirerek, geniş alan ağına ya da internete erişebilmektedir. Wi-Fi tanımına ilişkin marka hakları, kar amacı gütmeyen bir sertifikalandırma kuruluşu olan Wi-Fi Alliance'a ait olmakla beraber bugün günümüzde yaygınca bilinen bu teknolojiye ilişkin standartlar IEEE tarafından 802.11 başlığı altında tanımlanmaktadır. İlk kez 1997 yılında, IEEE tarafından kablosuz yerel alan ağı standardı olarak tanıtılan IEEE 802.11 ile, 2.4 GHz bandında 1 MBit/s-2 MBit/s veri hızında en çok 75 metrelik mesafeye ulaşabilecek şekilde veri aktarımı yapılabilmiştir. Günümüze kadarki süreçte, kullanıcıların artan taleplerine karşılık IEEE 802.11 standardının çeşitli versiyonları geliştirilmiştir.

1999 yılında ortaya çıkan ve 802.11'in geliştirilmiş sürümü olan 802.11a ile daha fazla kanal seçebilme, daha fazla bandgenişliği kullanma ve bunun sonucunda daha hızlı veri iletimi avantajları sunulmuştur. 802.11a standardı, OFDM (Orthogonal Frequency-Division Multiplexing) ile verinin birden çok alt taşıyıcı ile kodlanmasına ve birbirine karışmayacak şekilde aynı kanalda paralel olarak iletilmesine imkan sağlayarak, 5 GHz frekansında 54 MBit/s veri aktarım hızı sağlamıştır. Aynı yıl yayınlanan 802.11b ile veri hızından feragat edilerek, 2.4 GHz bandında daha geniş kapsama alanına erişilebildiği görülmüştür.

2003 yılında IEEE tarafından, 2.4 GHz frekansında 54 MBit/s veri aktarım hızına çıkabilen 802.11g standardı tasarlanmıştır. O zamana kadar ki en popüler WLAN standardı olan 802.11b ile uyumlu çalışan bu standart, kısa mesafede veri aktarım ihtiyaçlarını önemli ölçüde karşılamıştır. Ancak artan Wi-Fi kullanıcı sayısı ve kullanılan uygulamalarda artan hız ihtiyacı daha farklı yöntemlerin ortaya çıkmasına sebep olmuştur. 2003 yılında 802.11n protokolüne ilişkin çalışmalar yapılmıştır. Bu çalışmalar kapsamında çoklu giriş / çoklu çıkış (MIMO: Multiple Input / Multiple Output) adı verilen yeni bir yöntemin desteklenmesiyle hem 2.4 GHz hem de 5 GHz bandında alınan sinyal başarımında arttırım elde edilmiştir. Kablosuz ağlarda gönderilen veriler açık veya kapalı alanda cisimlere çarpıp yansıyarak ve farklı rotaları takip ederek alıcı antenlere farklı zamanlarda birden fazla kez ulaşmaktadır. Bununla ilişkili olarak MIMO'nun çalışma prensibi, farklı antenlerden aynı sinyal ya da farklı sinyaller gönderilerek, alıcı tarafta farklı rotalarda gelen sinyalleri farklı antenler üzerinde alarak birleştirmektir. Bunun sayesinde, 250 metre gibi uzun mesafelerde iletim sağlayan bu teknoloji 600 MBit/s'e kadar veri iletim hızı sağlamıştır.

2014 yılında ise günümüzde çok yaygın olarak kullanılan 802.11ac teknolojisi ya da bilinen diğer adıyla Wi-Fi 5 dünyaya tanıtılmıştır. 802.11ac standardı, 5 GHz bandında 1.8 GBit/s hızına erişen veri aktarımı sağlamıştır.

802.11ac teknolojisinin, 802.11n protokolüne göre veri aktarım hızında yarattığı faydaya ilişkin olarak getirdiği fark özellikler aşağıda sıralanmıştır:

- **Geniş frekans bandları:** 802.11'in ilk standartlarından bu yana 20 MHz'lik kanallar kullanılmaktadır. Bu kanalların yanı sıra 802.11n standartı ile 40 MHz'lik kanallar, 802.11ac'de ise 80 MHz'lik ve 160 MHz'lik kanallar kullanılabilmektedir. 160 MHz'lik kanallar komşu iki 80 MHz'lik kanalın oluşturduğu bandgenişliği olarak tanımlanan opsiyonel bir kanal olarak sunulmuştur. Çip üreticileri, hava radarlarının 5 GHz bandını kullanması ve diğer regülatif sınırlamaları gerekçe göstererek 160 MHz'lik kanalları kullanabilen ürünler yerine, 80 MHz bandgenişliklerini kullanan ürünlere yer vermiştir. 802.11ac standardı gereği, DFS (Dynamic Frequency Selection) desteği sağlanarak boş kanallar otomatik olarak seçilmektedir.
- **Uzaysal yayılım sayısı:** Teorik olarak, 802.11n standardında 4x4 uzaysal yayılım, 802.11ac'de 8x8 uzaysal yayılım desteklenmektedir. Pratikte ise, Wi-Fi çip endüstrisinde fiyat, boyut ve güç kısıtları altında 802.11n'de 2x2 MIMO, 802.11ac'de ise 3x3 MIMO ya da 4x4 MIMO destekli çipler ön plana çıkmıştır. MIMO, aynı anda birden fazla alıcı anten ve verici anten kullanmaya dayalı aktarım tekniğidir ve en temel faydası, yayılım sayısına paralel oranda veri aktarım hızında artış sağlamasıdır. 802.11ac haberleşmesi yapabilen cihazlar, 3x3/4x4 MIMO'yu desteklemesiyle beraber alış sinyal seviyelerindeki iyileşme ile hız performanslarında artış sağlamaktadır.
- **Çok-kullanıcılı (multi-user) MIMO:** Aynı 802.11n tabanlı Wi-Fi ağında, kullanıcı sayısının artmasıyla ve/veya kullanıcıların fazla bandgenişliği harcayan uygulamalar kullanmasıyla beraber, diğer kullanıcılara sunulan hizmet kalitesinin düştüğü gözlenmektedir. 802.11ac standardı ise çok-kullanıcılı MIMO teknolojisi sayesinde, SDMA (Space Division Multiple Access) yöntemini kullanarak uzaysal yayılımı kullanıcılar arasında bölerek mevcut bandgenişliğinin daha adil ve verimli kullanılmasına olanak sağlamaktadır.
- **Modülasyon ve kodlama:** 802.11n standardında kullanılan en hızlı modülasyon yöntemi 64-QAM iken 802.11ac'de 256-QAM kullanılabilmektedir. Böylelikle sembol başına taşınan bit sayısı 6'dan 8'e yükselmiştir. Daha önceki standartlarda 1/2 ve 2/3 kodlama oranlarında güvenilir haberleşme yapabilirken, 802.11ac'de bu değerler 3/4 ve 5/6 kodlama seviyesine çıkmıştır. Kodlama verimliliğindeki %20-%33 seviyesinde artış, veri hızına doğrusal olarak yansımıştır.
- **Koruma aralığı (guard interval):** OFDM sembollerinin birbirine karışımını önlemek amacıyla, iki sembol arası zamansal olarak koruma aralığı bırakılmaktadır. 802.11n'deki koruma aralığı 800 ns iken, 802.11ac'de bu aralık 400 ns'ye düşürülerek veri hızında %10'luk artış sağlanmıştır.
- **Çerçeve bütünleştirme (frame aggregation):** Gönderilecek çerçeveleri kümeleyip tek iletim döngüsünde aktarıp, tek alındı bildirimi ile tüm küme adına cevap alma esasına dayanmaktadır. Gönderilen çerçevelere alınacak cevapların oluşturacağı trafiği azaltmaya yönelik bir uygulamadır. 802.11n standardıyla beraber yayınlanan Aggregation MAC Service Data Unit (A-MSDU) sayesinde tek başına gönderilecek çerçevelerin oluşturacağı overheadler, bir gönderim zamanı ile sınırlandırılmaktadır. Bu protokolün üzerine geliştirilmiş ve 802.11ac'de yayınlanmış olan Aggregation MAC Service Data Unit (A-MPDU), aynı prensipte gönderilen birimler arasına bir ayırıcı başlığı koyarak, çerçeve kaybının yüksek olabileceği ortamlarda, tüm küme yerine sadece ilgili çerçevenin tekrar iletimini sağlayan yöntemdir.

802.11ac teknolojisi, 802.11s standardıyla ön plana çıkmış önemli bir özelliği de beraberinde getirmektedir. Bu özellik, kablosuz erişim noktalarının ad-hoc modeline uygun olarak kablosuz örgü ağı (wireless mesh network) topolojisi kurabilmesidir. Ad-hoc merkezi olmayan, istemcilerin kendi aralarında kablosuz olarak haberleşmesini sağlayan bir ağ yapısıdır. Böylelikle cihazlar ağdaki diğer cihazlarla eş zamanlı birden fazla bağlantı kurabilmektedir. Ağdaki herhangi bir cihaz ya da örgü noktası (mesh point) çalışmaz hale gelirse, örgü ağındaki haberleşmenin devamlılığı, rotaların çalışan örgü noktalarının üzerinden tekrar çizilmesi ile sağlanmaktadır. Bu sayede yedekli, kendini onarabilir ve kullanışlı bir yapı sunulmaktadır. 802.11s'de tanımlı iki çalışma modu bulunmaktadır. Örgü noktalarının birbirleri arasında bir merkezi cihaza yani erişim noktası (AP: Access Point) ihtiyaç duymadan haberleşmesinde Ad-Hoc modu kullanılırken, erişim noktasına ihtiyaç duyulan durumlarda ise infrastructure modu kullanılır.

802.11s'de kablosuz çerçeve yapısı, katman 2 başlığına örgü ağa ilişkin metrik bilgilerinin eklenmesi ile değiştirilmiştir. Bu bilgiler ve katman 2'de tanımlı kaynak/hedef MAC (Media Access Control) adresleri kullanılarak örgü noktaları üzerinde verinin iletimi yol seçim (path selection) yöntemleriyle yapılmaktadır. İki tip yol seçim yöntemini içeren HWMP (Hybrid Wireless Mesh Protocol), 802.11s'de ve 802.11ac'de varsayılan olarak yapılandırılmıştır.

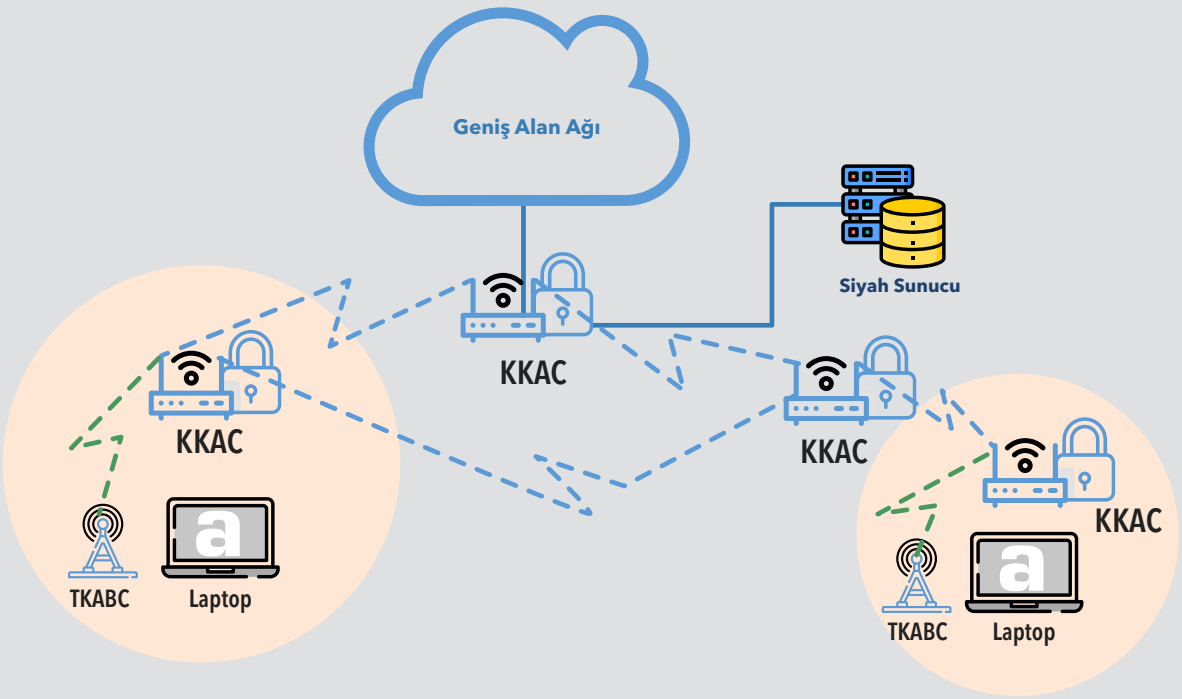
HWMP, hem reaktif (reactive) hem de proaktif (proactive) yol seçim yöntemlerini destekleyen, bu özelliğinden dolayı da hibrit ismini almış protokoldür. Hibrit çalışmanın doğası gereği bu iki yöntem birlikte ya da ayrı ayrı kullanılmaktadır. Reaktif yöntemde bir örgü ağında bir noktadan diğer noktaya veri aktarmak istenildiğinde yönlendirme tablosunda herhangi bir rota olup olmadığına bakılmaktadır. Eğer tabloda kayıtlı rota yoksa hedefe doğru çeşitli mesajlar gönderilmekte ve tespit edilen rotaların metrik hesabı yapılmaktadır. Belirlenen rotalardan en iyi metrik değerine sahip olanı yönledirme tablosuna kaydedilmektedir. Bu protokolün literatürdeki adı Radio Aware Metric - Ad-Hoc On Demand Distance Vector (RMAODV)'dür. İhtiyaç halinde iki nokta arasındaki rotayı ve bu rotaya ait metrikleri hesaplamaya dayalı bu yöntem ile veri aktarım gecikmeleri oluşsa da yol tablosu her veri akış isteğinde güncellenmekte ve böylelikle ağdaki değişikliklere dinamik bir şekilde cevap verilmesi sağlanmaktadır. Proaktif yöntemde ise ağaç tabanlı (tree-based) protokol üzerinden yönlendirme işlemleri yapılmaktadır. Kök (root) cihaz tarafından güncel rota bilgilerini tutmak için periyodik olarak örgü ağına mesajlar gönderilmektedir. Her örgü noktası ağın topolojisine ilişkin metrik değerlerini kendi tablosunda tutmaktadır. Bellekte sürekli tutulan ve ihtiyaç hali olmadığında dahi güncellenen bu bilgiler, veri aktarım gecikmelerini önlediği gibi sistem kaynaklarını sürekli kullanmaktadır. Proaktif yöntemde uygun rotalar sürekli hesaplanırken, reaktif yöntemde iki nokta arası veri aktarım isteği olduğunda hesaplanmaktadır.

En güncel Wi-Fi teknolojisi olan ve henüz geniş ölçekte yaygınlaşma fırsatı bulamayan 802.11ax, bir diğer adıyla Wi-Fi 6, 2.4 GHz bandında ve 5 GHz bandında çalışmaktadır. 802.11ac'den temel farkı 2.4 GHz bandında da çalışabilmesi, uzaysal yayılım sayısını arttırması (12x12 MIMO) ve STR (Simultaneous Transmit/Receive), Downlink/Uplink OFDMA (Orthogonal Frequency-Division Multiple Access), Uplink MU-MIMO, Dynamic CCA (Clear Channel Assesment) gibi teknolojileri kullanabilmesidir. Bu geliştirmelerle 802.11ac'ye göre yaklaşık beş kat daha fazla cihaza hizmet verebilecek kapasiteye sahip olan 802.11ax, 5 GHz bandında 10.53 GBit/s veri iletim hızına ulaşmaktadır.

ASELSAN'ın Wi-Fi Çözümleri

ASELSAN'ın Wi-Fi çözümleri, kablosuz hattın emniyetli hale getirilmesi için hem erişim noktasında hem de istemci tarafında oluşturulmuştur ve TAYAS Projesi kapsamında Kara Kuvvetleri Komutanlığının taktik sahadaki kriptolu kablosuz haberleşme ihtiyaçlarını karşılamaya yönelik tasarlanmıştır. Kriptolu Kablosuz Ağ Cihazı (KKAC) kriptolu kablosuz erişim noktası olarak, TKABC (Terminal Kablosuz Ağ Bağlantı Cihazı) ise kriptolu kablosuz istemci olarak sistemde yer almaktadır. Cihazlar birbirleri arasındaki bağlantıyı, aldıkları en iyi sinyal seviyelerine göre otomatik olarak yaptığından ve kablo bağlantıları gerektirmediğinden, taktik sahada kullanıcıya hızlı kurulum imkanı sağlamaktadır. Cihazlar kapsama alanlarının sağladığı ölçekte, ağa bağlanan istemciler arasında, katman 2'de haberleşme yeteneği sunmaktadır.

TKABC, dizüstü bilgisayarlara USB (Universal Serial Bus) arayüzünden bağlanmakta ve kablosuz arayüzü üzerinden KKAC'lere kayıtlanmaktadır. KKAC'ler, TKABC'lerden aldıkları kriptolu paketleri ya ağ topolojisinde bulunan diğer KKAC'lere ve TKABC'lere anahtarlamaktadır ya da kriptosunu çözerek kablolu arayüzüne taşımaktadır. KKAC'ler, kendi aralarında örgü (mesh) ağ kurabilmektedir. Böylelikle KKAC'lerden hizmet alan TKABC'ler, kayıtlı olduğu KKAC'nin kapsama alanı dışına çıkıp örgü ağ içindeki başka KKAC'nin kapsama alanına girdiğinde otomatik kayıtlanarak aynı ağdan hizmet almaya devam etmektedir. Örnek ağ topolojisi şekil 1'de verilmiştir. Burada kök KKAC, USB arayüzünden bağlı olduğu sunucu üzerinde kurulu KAYY'den (Kablosuz Ağ Yönetim Yazılımı) aldığı istekleri örgü ağa dağıtarak, tüm KKAC'lerin kablosuz arayüzüne ilişkin parametrelerinin izlenmesini ve konfigüre edilmesini sağlamaktadır.



Şekil 1: KKAC-TKABC için Örnek Ağ Topolojisi

KKAC, 19” rafa monte edilebilir ve 220 V AC’den beslenebilir yapıdadır. Cihazın tasarımı, çevresel koşullar ve elektromanyetik uyumluluk için MIL-STD askeri standartları sağlayacak şekilde yapılmıştır. Cihazda, örgü ağı ve erişim ağı için ayrı Wi-Fi modülleri kullanılarak, frekans yalıtımı ve trafik optimizasyonu yaratılmıştır.

KKAC, aşağıdaki özellikleri sağlayacak şekilde IEEE 802.11ac uyumlu haberleşme yeteneklerine sahiptir:

- Örgü ağındaki ve erişim ağındaki arayüzleri üçer adet uzaysal yayılımı desteklemektedir. Böylelikle KKAC’de altı adet anten bulunmaktadır.
- Örgü ağda, cihazlardan birinin devre dışı kalması durumunda geri kalan KKAC’ler, kök cihaza doğru olan kablosuz ağ yollarını otomatik olarak güncelleyerek kablosuz ağı onarabilmektedir.
- 20 MHz’lik, 40 MHz’lik ve 80 MHz’lik kanalları dinamik frekans seçimi yaparak kullanmaktadır.
- Örgü ağında havadaki anlık toplam kriptolu veri akışı katman 2’de 300 MBit/s hızı sağlayacak şekilde tasarlanmıştır.
- Kablosuz erişim ağında MAC adres filtrelemesi sağlamaktadır.

TKABC, taşınabilir bilgisayarların şarj eden USB arayüzünden beslenebilir yapıdadır.

TKABC, aşağıdaki özellikleri sağlayacak şekilde IEEE 802.11ac uyumlu haberleşme yeteneklerine sahiptir:

- İki uzaysal yayılımı sağlayacak şekilde iki adet anten bulundurmaktadır.
- 20 MHz’lik, 40 MHz’lik ve 80 MHz’lik kanalları dinamik frekans seçimi yaparak kullanmaktadır.
- Erişim ağında havadaki anlık toplam kriptolu veri akışı katman 2’de 80 MBit/s hızı sağlayacak şekilde tasarlanmıştır.
- Herhangi bir erişim noktası seçmeden ve erişim şifresi girmeden ağa otomatik dahil olacak şekilde yapılandırılmıştır.

Cihazların kriptografik tasarımı kırmızı-siyah ayrımını gözeterek TEMPEST ve COMSEC uyumlu olarak yapılmıştır. Cihaz üzerinde kullanıcı yetkilendirmesi Elektronik Kimlik Modülü (EKIM) ile yapılmaktadır. Yetkisiz cihazların ağa dahil olmaması için cihazlar arasında üç yönlü kimlik doğrulaması çalışmaktadır. Milli gizli kripto algoritması ile kriptolanarak cihazların havaya çıkardığı veriler başkaları tarafından dinlenememektedir. Kripto anahtarları, ASELSAN 2070 Fill Gun Cihazı vasıtasıyla yüklenmektedir.

ASELSAN, Wi-Fi çözümlerine ilişkin cihaz ailesini genişletmek amacıyla tasarım ve geliştirme faaliyetleri devam eden Mini KAC (Mini Kablosuz Ağ Cihazı) ürünlerini kullanıcılara sunmayı planlamaktadır. Mini KAC kapsamında üç farklı ürün ortaya çıkacaktır. Bunlar Askeri Mini KAC, Kriptolu Ticari/Endüstriyel Mini KAC ve Ticari/Endüstriyel Mini KAC olacaktır.

- **Askeri Mini KAC:** KKAC'nin geliştirilmiş, boy ve ende yaklaşık yarı oranda küçültülmüş, katman 3'te çalışan yönlendirme protokolleri (HWMP, AODV, OLSR, BATMAN) ile donatılmış versiyonu ve TKABC'ler ile de kriptolu IEEE 802.11ac uyumlu Wi-Fi iletişimi kurabilen cihazlar olarak planlanmıştır.
- **Kriptolu Ticari/Endüstriyel Mini KAC:** Askeri Mini KAC'den farklı olarak çevresel koşullar ve elektromanyetik uyumluluk için IEC standartları sağlayacak şekilde tasarlanacaktır. Kripto algoritması olarak 256 Bit AES kullanılabilecektir.
- **Ticari/Endüstriyel Mini KAC:** Kriptosuz, endüstriyel ortamlar dahil piyasadaki tüm kullanıcıların ihtiyaçlarını karşılamaya yönelik maliyet etkin cihazlar olarak tasarlanacaktır.

Kablosuz Ağ Yönetim Yazılımı (KAYY), ağda bulunan KKAC'leri ve TKABC'leri izlemek ve konfigüre etmek, topoloji gözlemi ve yönetimi yapmak ve ağa ait bilgi, uyarı ve hata gibi kayıtları göstermek amacıyla tasarlanmış olan ve kullanıcılara web arayüzü üzerinden hizmet sunan bir yazılım uygulamasıdır.

Kablosuz ağ yönetim yazılımının kullanıcılara sunabileceği hizmetler aşağıda verilmiştir:

- Kök KKAC'nin içinde bulunduğu tüm ağdaki KKAC'lerin ve TKABC'lerin, MAC adresi, seri numarası ve yazılım versiyon bilgileri izlenebilmektedir.
- KKAC'ler arası örgüsel yapıya ait metrikler ve ağ topolojisi görüntülenmektedir.
- KKAC'lere ve TKABC'lere ait haberleşme frekans kanalları, seri numaraları, SSID (Service Set Identifier) ve parola bilgileri değiştirilebilmektedir.
- KKAC'lerin ve TKABC'lerin RF güç ayarları değiştirilebilmektedir.
- MAC adres filtrelemesi yapılarak, ağ üzerindeki KKAC'lere bağlanması istenen/istenmeyen istemciler için erişim kontrol listesi (ACL) hazırlanabilmektedir. Bu listeler dışarıya veya hazırlanmış listeler içeriye aktarılabilmektedir.
- Ağdaki tüm KKAC'lerin yazılımları, sunucu üzerinde bulunan yazılım dosyasının havadan paylaşılmasıyla güncellenebilmektedir.
- Yönetici, okuma/yazma ve okuma yetkilerine sahip kullanıcı tipleriyle, Kablosuz Ağ Yönetim Yazılımı üzerinde farklı kullanım yetkileri tanımlanabilmektedir.
- Ağ içerisindeki KKAC'lere ve TKABC'lere ait bilgi, uyarı, hata gibi tüm işlemlerin kayıtları tutulmaktadır.
- Kayıtları tutulan işlemlere ait çıktılar, belirlenen kişilere e-posta yolu ile iletilebilmektedir.

Sonuç

Wi-Fi teknolojisini destekleyen nesnelerin yaygınlaşmasıyla, bu teknolojinin internetteki tüm veri akışına hizmet oranı, diğer teknolojiler ile karşılaştırıldığında, her geçen sene artmaktadır.[1] İçinde bulunduğumuz pandemi sürecinde ise rekor seviyelere ulaşmıştır.[2] Önümüzdeki senelerde yaygınlaşacak Wi-Fi 6'nın, 5G teknolojisi ile birlikte kullanımı sonucunda; sadece ev/ofis uygulamalarında değil, sağlık, üretim, otomotiv sektörlerindeki haberleşme platformlarında da öncü rollerden birini oynayacağı değerlendirilmektedir.[3] Bu gelişmelere paralel olarak Wi-Fi Teknolojisinin askeri alanlarda kullanımı da kaçınılmazdır. ASELSAN, teknoloji yol haritasında Wi-Fi tabanlı cihazları konumlandırarak, hem ticari/endüstriyel hem de askeri tipteki özgün ve emniyetli ürünleri kullanıcılara sunmaktadır.

Kaynakça

Cisco Annual Internet Report, (2018-2023) http://wififorward.org/2020/04/02/covid19updates/

Wireless Broadband Alliance Annual Industry Report 2020

Ağ Yönetim Teknolojileri

Hazırlayan
Emre Sönmez
HBT SMD Bilgi Teknolojileri Sistem Mühendisliği Müdürlüğü

Giriş

1980'li yıllarla birlikte, ethernet teknolojisi gelişmiş, kişisel bilgisayarlar ve ofisler bilgisayar ağlarına kavuşmuştur. Bildiğimiz en büyük bilgisayar ağı internet başta olmak üzere, bilgisayar ağlarının ölçeğindeki büyüme ve ağdaki bileşenlerin sayısındaki sürekli artış, ağın yönetimini zorlu ama üzerinde durulması gereken konulardan biri haline getirmiştir. Ağ yöneticisinin, otomatize edilmiş uygulamalardan yararlanmadan bu ihtiyacı karşılaması mümkün değildir; dolayısıyla o yıllardan itibaren ağ yönetim teknolojileri üzerine çalışmalar hız kazanmış olup günümüzde de devam etmektedir. Haberleşme teknolojileri, ağ cihazlarının yetenekleri ve veriye dayalı sonuç çıkarma teknolojileri (makine öğrenmesi, derin öğrenme vb.) gelişim gösterdikçe ağın daha etkin izlenip yönetilmesi ile ilgili çalışmalar elzem biçimde devam edecektir. Araştırmalar ağ yönetim uygulamalarının 2024 yılına gelindiğinde 11 milyar $ pazar hacmine erişeceğini belirtiyor.[1]

ASELSAN, çağın ihtiyaçlarına yanıt veren yerli ve milli bilgi teknoloji ürün ailesi oluşturma hedefiyle bir yol haritası oluşturmuş, aileye ağ yönetim yazılımını da ekleme kararı almıştır. 2018 yılında başlayan projede sona yaklaşılmış olup tüm askeri, endüstriyel ve ticari ağlarda yönetim ihtiyacını karşılayacak olgunluktaki ürün 2020 yılında hayata geçecektir.

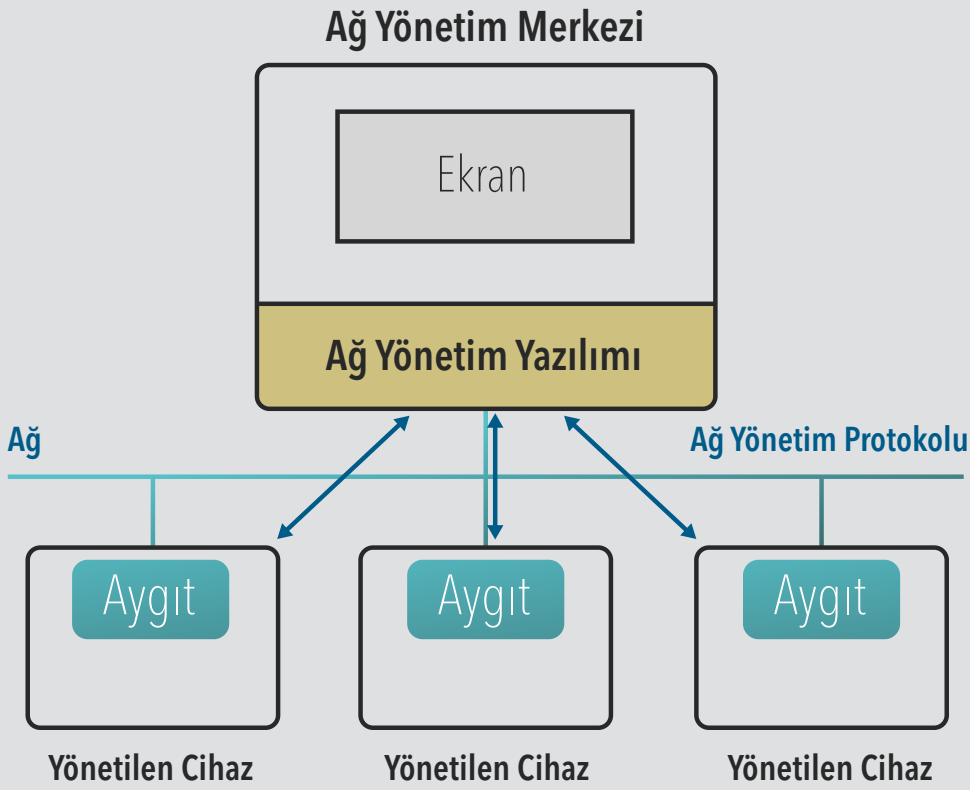
Ağ Yönetimi Nedir?

Karmaşık bir ağda, neyin yanlış gittiğine dair net bir bilgi olmadan sorun çözmeye çalışmak, karanlıkta arıza bulmaya çalışmakla eşdeğerdir. Ağ yönetimi, çeşitli protokollerin, araçların, uygulamaların birlikte çalışarak ağ yöneticisine ağdaki bileşenlerin izlenmesi ve kontrol edilmesi imkanı sunan bir servistir. İlk ağ yönetim araçları, 1987 yılında SGMP (Simple Gateway Monitoring Protocol) ile beraber oluşturulmuştur. 1988'de IAB (Internet Architecture Board) tarafından SNMP'nin (Simple Network Management Protocol) ağ yönetiminde geçerli bir çözüm olarak onaylanması standardizasyon sağlamış, yenilikçi çözümlere de zemin hazırlamıştır.

Ağ yönetim sistemi, bir ağ içerisindeki bağımsız bileşenleri izlemeye ve kontrol etmeye yarayan uygulamalar bütünüdür. Yönetilen ağ cihazları, ağ yönetim yazılımı, kullanıcı arayüzleri ve veri toplama mekanizması sistemin parçalarıdır. Şekil 1'de ağ yönetim sistemi için temel bir mimari yer almaktadır. Ağ yönetim merkezi, ağ yöneticisi ile olan kullanıcı arayüzünü, ağdaki cihazlarla haberleşecek yazılımı ve üzerinde koşacağı sunucuyu içerir. Yönetilen ağ cihazları, merkezden gelen taleplere yanıt verir. Ağdaki cihaz çeşitliliği (IP yönlendiriciler, ethernet anahtarlar, yük dengeleyiciler, bilgisayarlar vb.) ve herbirinin işletim sistemi, arayüz çeşitliliği göz önünde bulundurulduğunda; merkez ile cihazlar arasında iletişim sağlayacak ağ yönetim protokolü kritik öneme sahiptir. SNMP ve CMIP (Common Management Information Protocol) yaygın iki protokol olarak karşımıza çıkmaktadır; CMIP daha gelişmiş olmasına karşın SNMP kolay ve ihtiyacı karşılar olmasıyla daha fazla benimsenmiştir.

ISO (International Organization for Standardization) tarafından geliştirilen OSI (Open Systems Interconnection) Modeli, ağ farkındalığına sahip cihazlarda çalışan uygulamaların birbirleriyle nasıl iletişim kuracaklarını tanımlayan referans modeldir; ağ yönetimi için de bir model tanımlanmıştır ve ağ yönetim sistemleri de bu referansa uygun tasarlanmaktadır. OSI ağ yönetim modeli, dört alt modelden oluşur:

- **Organizasyon modeli:** Yöneticiyi, aygıtı ve yönetilen bileşeni tanımlar. Ağ yönetim sisteminin bileşenlerinin işlevleri ve altyapısı hakkında bilgi verir.
- **Bilgi modeli:** Ağdaki cihazlardan toplanan bilginin yapısı ve depolanması ile ilgili kıstaslar yer alır. SMI (Structure of Management Interface), MIB'de (Management Information Base) saklanan bilginin sözdizimini ve anlamını tanımlar. MIB, hem yönetici hem aygıt tarafındaki işlemlerde bilginin depolanması ve alıverişi için kullanılır.
- **İletişim modeli:** Bilgi alışverişinin aygıt ve yönetici arasında nasıl olacağını tanımlar. Bu modelde belirtilmesi gereken üç anahtar unsur taşıma protokolü, uygulama protokolü ve iletilen mesajdır.
- **Fonksiyonel model:** Ağ yönetiminin kullanıcı odaklı gereksinimleri yer alır ve işlevsel uygulama alanları (hata analizi, konfigürasyon yönetimi, kullanıcı yönetimi, performans takibi, güvenlik yönetimi) tanımlanır.



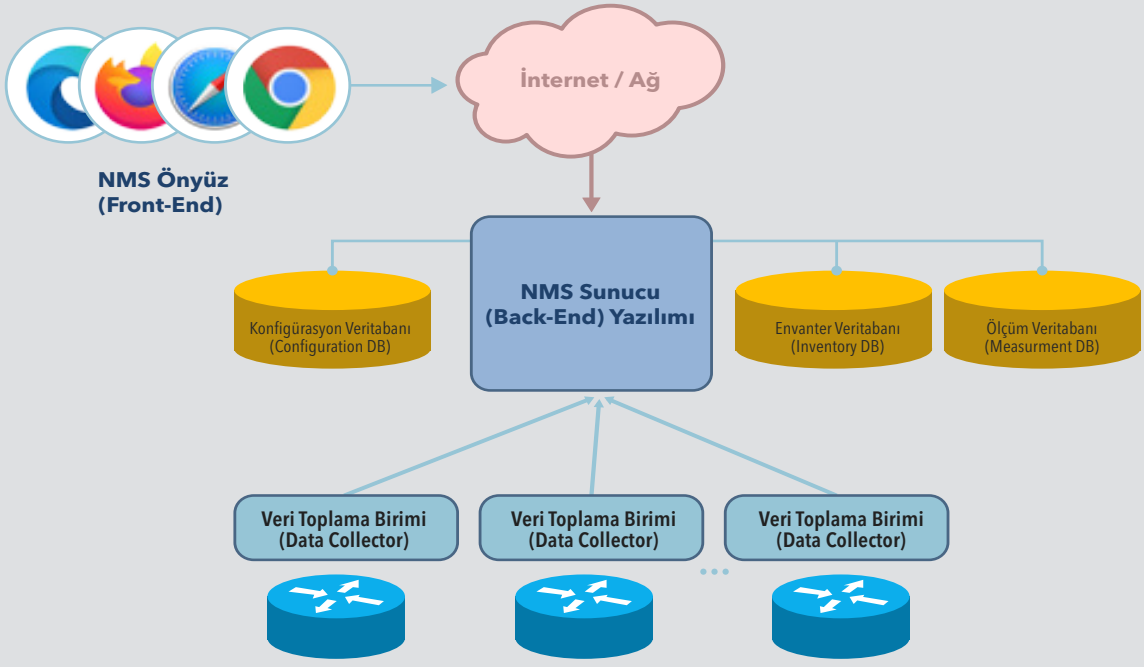
Şekil 1: Ağ Yönetim Sistemi Mimarisi

Fonksiyonel modelin kapsamındaki uygulama alanları, FCAPS (Fault, Configuration, Accounting, Performance, and Security) kısaltma adıyla da literatürde yer almaktadır ve beş ana başlıkta gruplandırılmıştır:

- **Arıza yönetimi (fault):** Ağdaki anormalliklerin tespit edilmesi ve düzeltilmesi bu alan kapsamındadır. Arıza yönetiminin amacı, ağdaki arızayı hızlıca gidermek ve sistemi her zaman canlı tutmaktır. Örneğin iki ağ bileşeni arasındaki fiziksel iletişim hattının kopması bir arızadır, ağın sürekli izlenmesi bunun tespitini ve çözüm süresini hızlandırır.
- **Konfigürasyon yönetimi (configuration):** Ağın başlangıç durumuna getirilmesi, kontrol edilip izlenmesi ve ağdaki bileşenlerin yapılandırılması bu alan kapsamındadır. Ağdaki bileşenlerin arasındaki ilişkinin kurulması, sürdürülmesi ve güncellenmesi konfigürasyon yönetiminin görevleridir.
- **Hesap yönetimi (accounting):** Ağdaki kaynakların kullanıcılar arasında en uygun ve adil şekilde dağıtılması, ağı kullanan abonelerin faturalandırılması bu alan kapsamındadır. Optimal ve adil kullanımla ağdaki işlem maliyetinin azaltılması hedeflenmektedir.
- **Performans yönetimi (performance):** Yönetilen ağ cihazlarının davranışlarını ve etkinliğini değerlendirmek bu alan kapsamındadır. Ağdan toplanan trafik hacmi, cihazların yanıt süresi, gelen/giden paket miktarı vb. veriler yardımıyla performans ölçülmektedir.
- **Güvenlik yönetimi (security):** Ağın ve sistemin yetkisiz erişimden uzak tutulup siber saldırılardan korunması bu alan kapsamındadır. Kimlik doğrulama, yetkilendirme ve kriptolama güvenlik yönetimi mekanizmalarıdır. Güvenlik duvarı ve saldırı tespit sistemleri gibi cihazların ağda bulunması, olayların gerçek zamanlı takibinin yapılmasını ve kaydının tutulmasını sağlar, güvenlik yönetimi için gereklidir.

Ağ Yönetimi ile ilgili ASELSAN Çözümleri

ASELSAN markalı bir ürün olarak piyasaya çıkacak olan ağ yönetim yazılımı, ağ yöneticilerinin herhangi bir ağ içerisindeki bağımsız bileşenleri monitör edebilmelerini, kontrol ve konfigüre edebilmelerini, yönetebilmelerini ve gerekli raporlama faaliyetlerini gerçekleştirebilmelerini sağlayan web tabanlı bir uygulamadır. Yazılım, şekil 2'de görüldüğü gibi dört ana bölümden oluşmaktadır.

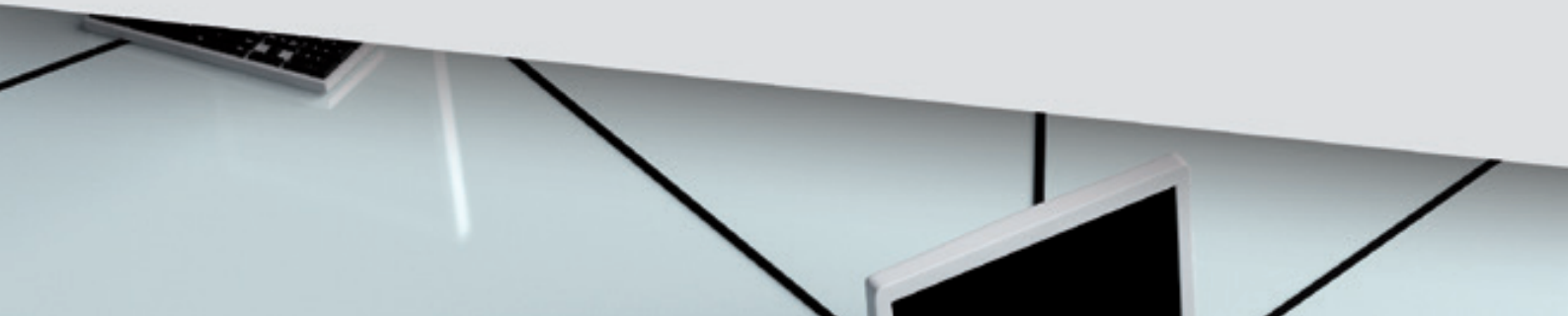


Şekil 2: Ağ Yönetim Yazılımı Üst Seviye Mimarisi

- **Ön yüz yazılımı:** Kullanıcı etkileşimini sağlayarak sistemin çalışmasında gerekli ayarların yapılabilmesini sağlar.
- **Sunucu yazılımı:** Yazılımın temel görevlerini yerine getiren yapıdır ve mikro servis mimarisi kullanır. Çalışan mikro servisler gelen trafiği işlemekte yetersiz kalırsa ilgili mikro servislerden yeteri kadar kopya daha çalıştırılarak sistemin artan trafiği işleyebilmesi sağlanır. Bu sayede cihaz sayısının yüksek olduğu ağlar içerisinde de yüksek performansla çalışabilmektedir.
- **Veritabanları:** Sistemde oluşacak verinin saklanmasında görev almaktadır. Verilerin kullanılma amaçlarına göre ayrılmış üç veritabanı bulunmaktadır. Zamana bağlı olarak değişen veriler ölçüm veritabanında saklanır. İlişkisel olarak saklanması gereken cihaz bilgileri, kullanıcılar gibi veriler konfigürasyon veritabanında saklanır. Döküman bazlı olarak saklanacak olan raporlar, güncellemeler ve konfigürasyon dosyaları sistem içerisinde envanter veritabanında saklanır.
- **Veri toplama birimleri:** Ağ içerisindeki cihazlar ile farklı protokoller (SNMP, NETCONF, OpenFlow, NetFlow, soket bağlantısı) üzerinden iletişim kurup verilerin ağ yönetim yazılımına iletilmesinden sorumludur. Veri toplama işlemleri senkron ve asenkron olarak iki türde yapılmaktadır. Sistem toplanan veriyi veri türüne göre ilgili veritabanlarına sunucu yazılımı üzerindeki farklı mikro servisler aracılığıyla iletmektedir.

Ürünün genel özellikleri aşağıdaki şekildedir:

- Sanal makine üzerinde çalışabilmektedir.
- SNMP, NETCONF/RESTCONF, OpenFlow ve NetFlow veya özel soket bağlantısı ile Ağ Cihazları'ndan gerçek zamanlı veri toplanabilmektedir.
- İkibin ve üzeri sayıda Ağ Cihazı'ndan veri toplanabilmektedir.
- FCAPS modeli ile uyumludur.
- Ağ üzerindeki cihazların envanteri (marka, model, seri numarası, yazılım ve işletim sistemi) çıkarılabilmektedir.
- Ağ üzerinde bulunan cihazların konfigürasyon yönetimi yapılabilmektedir.
- Sistem içerisinde tanımlı veya özel olarak kullanıcının seçtiği veriler kullanılarak grafiksel analiz yapılabilmektedir.
- LLDP (Link Layer Discovery Protocol), ICMP (Internet Control Message Protocol) ve TWAMP (Two-Way Active Measurement Protocol) gibi protokoller kullanarak ağdaki cihazları keşfetme ve haritalandırma sağlanmaktadır.
- Ağdaki trafik akışı izlenebilmektedir.
- Ağ özelinde oluşan problemler görüntülenip raporlanabilmektedir.
- Ağ içerisinde bulunan cihazlar ve servisler ile ilgili alarm, olay ve SLA (Service Level Agreement) tanımlamaları yapılabilmektedir ve önemine göre derecelendirilip oluşması durumunda SMS (Short Message Service), e-posta ya da bir HTTP (Hyper Text Transfer Protocol) servisi aracılığıyla ilgili noktaya bilgi gönderilebilmektedir.
- Statik/dinamik yönlendirme, mirroring ve ACL (Access Control List) özellikleri yönetilebilmektedir.
- QoS (Quality of Service) Yönetimi sağlanmaktadır.
- Ağdaki cihazların web arayüzüne ve komut satırına erişilebilmektedir.
- Ağdaki cihazlara farklı erişim kontrol yöntemleri (SSH-Secure Shell, TELNET vb.) sağlanmaktadır.
- Ağdaki cihazlar üzerindeki konfigürasyonlar karşılaştırılabilmektedir.
- Ağdaki cihazlara sürüm güncelleme yapılabilmektedir.



- Kullanıcının tanımladığı periyotlara göre performans verisi toplanabilmektedir.
- Kullanıcılar farklı seviyelerde yetkilendirilebilmektedir.
- LDAP (Lightweight Directory Access Protocol), AD (Active Directory), TACACS (Terminal Access Controller Access-Control System) ve RADIUS (Remote Authentication Dial-In User Service) sistemleri ile entegre çalışabilmektedir ve ağa bağlanmaya çalışan kullanıcılar ile ilgili başarılı/başarısız IEEE 802.1x kayıtları görüntülenebilmektedir.
- Ağdaki cihazlardan toplanan kayıtların görüntülenebilmesi ve geçmişe dönük aranabilmesi sağlanmaktadır.

Ürünün öne çıkan ve fark yaratan özellikleri aşağıdaki şekildedir:

- Sanal makine veya konteyner üzerinde çalışabilme, uygulamanın kurulum ve devreye alınması açısından kolaylık sağlar. Müşterinin ağına hızlıca entegre olarak ağı keşfeder ve yönetir.
- Ağa yönelik saldırıların arttığı ve bu yöndeki çözümlerin kıymetlendiği günümüz teknolojisinde LDAP, AD, TACACS ve RADIUS sistemleri ile entegre çalışabilme ve IEEE 802.1x kayıtları görüntüleyebilme özellikleri güvenlik yönetimi açısından önemlidir.
- NETCONF ve RESTCONF protokolleri SNMP'ye kıyasla daha güncel, NFV (Network Function Virtualization) mimarisi ile sanallaşmış ağlarda yönetim için tercih edilmektedir. Bu protokollerin desteği, gelecekte daha da yaygın hale gelecek olan bu mimaride, ağ yönetimi için ASELSAN Ağ Yönetim Yazılımını ayrıcalıklı kılmaktadır.

Ürüne gelecekte kazandırılması planlanan özellikler aşağıdaki şekildedir:

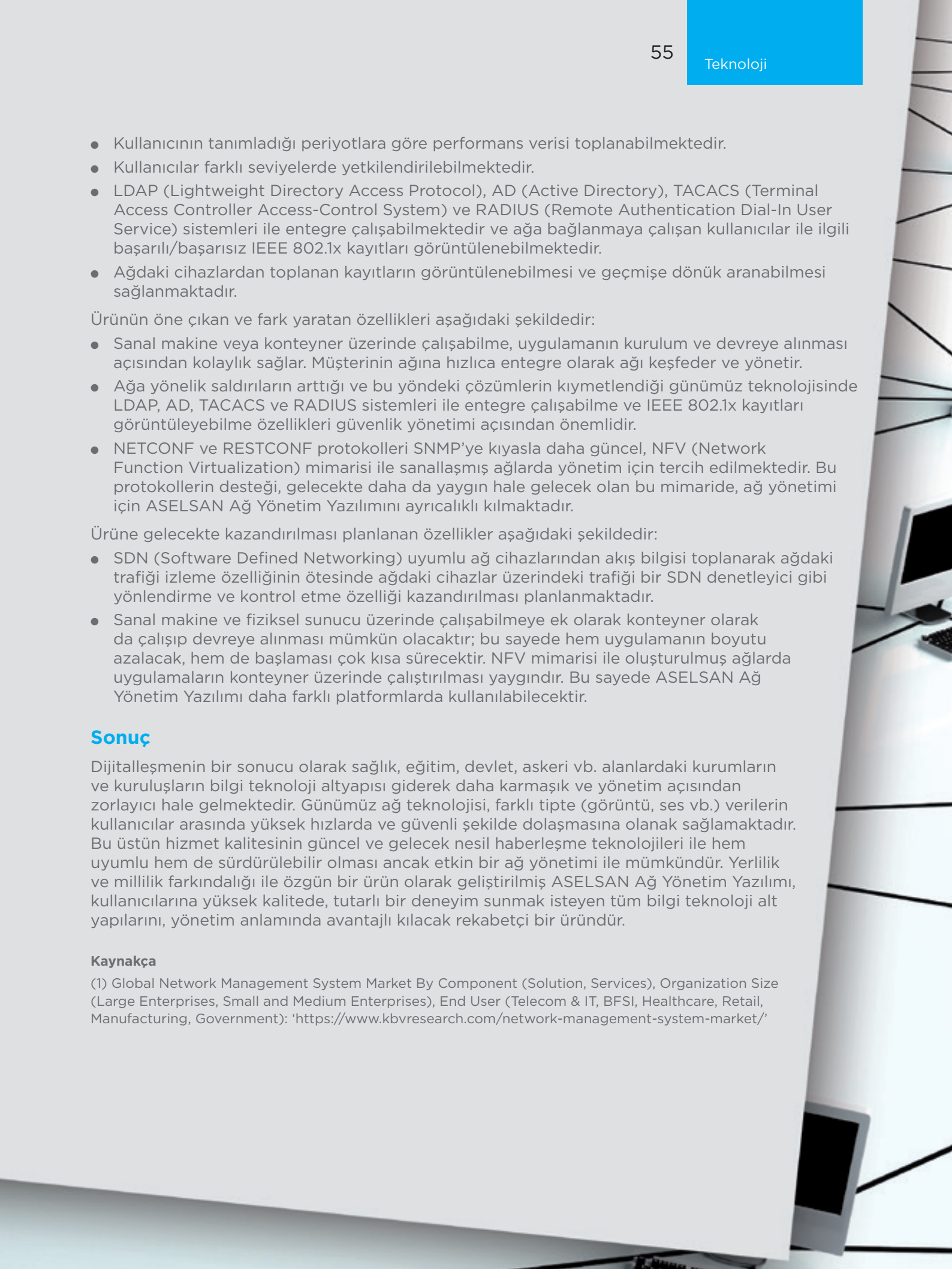
- SDN (Software Defined Networking) uyumlu ağ cihazlarından akış bilgisi toplanarak ağdaki trafiği izleme özelliğinin ötesinde ağdaki cihazlar üzerindeki trafiği bir SDN denetleyici gibi yönlendirme ve kontrol etme özelliği kazandırılması planlanmaktadır.
- Sanal makine ve fiziksel sunucu üzerinde çalışabilmeye ek olarak konteyner olarak da çalışıp devreye alınması mümkün olacaktır; bu sayede hem uygulamanın boyutu azalacak, hem de başlaması çok kısa sürecektir. NFV mimarisi ile oluşturulmuş ağlarda uygulamaların konteyner üzerinde çalıştırılması yaygındır. Bu sayede ASELSAN Ağ Yönetim Yazılımı daha farklı platformlarda kullanılabilecektir.

Sonuç

Dijitalleşmenin bir sonucu olarak sağlık, eğitim, devlet, askeri vb. alanlardaki kurumların ve kuruluşların bilgi teknoloji altyapısı giderek daha karmaşık ve yönetim açısından zorlayıcı hale gelmektedir. Günümüz ağ teknolojisi, farklı tipte (görüntü, ses vb.) verilerin kullanıcılar arasında yüksek hızlarda ve güvenli şekilde dolaşmasına olanak sağlamaktadır. Bu üstün hizmet kalitesinin güncel ve gelecek nesil haberleşme teknolojileri ile hem uyumlu hem de sürdürülebilir olması ancak etkin bir ağ yönetimi ile mümkündür. Yerlilik ve millilik farkındalığı ile özgün bir ürün olarak geliştirilmiş ASELSAN Ağ Yönetim Yazılımı, kullanıcılarına yüksek kalitede, tutarlı bir deneyim sunmak isteyen tüm bilgi teknoloji alt yapılarını, yönetim anlamında avantajlı kılacak rekabetçi bir üründür.

Kaynakça

(1) Global Network Management System Market By Component (Solution, Services), Organization Size (Large Enterprises, Small and Medium Enterprises), End User (Telecom & IT, BFSI, Healthcare, Retail, Manufacturing, Government): 'https://www.kbvresearch.com/network-management-system-market/'



SDN/NFV Teknolojileri

Hazırlayan
Semih Kaya
Haberleşme ve Bilgi Teknolojileri (HBT) Sektör Başkanlığı - Sistem Mühendisliği Direktörlüğü (SMD) - Bilgi Teknolojileri Sistem Mühendisliği Müdürlüğü

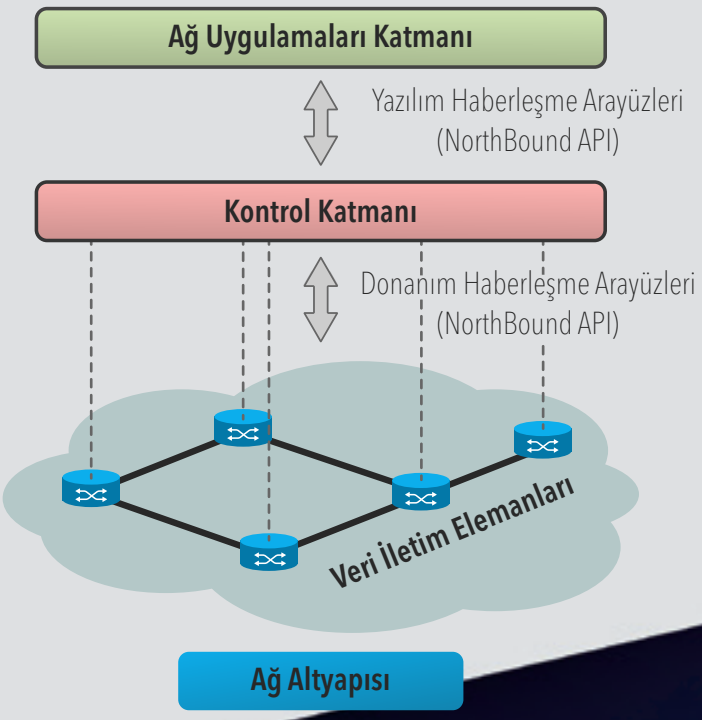
Giriş

Konvansiyonel bilgisayar ağları, belirli fonksiyonları yerine getirecek özelleşmiş donanımların birlikte çalışması ile oluşturulmaktadır. Bu fonksiyonlar ağ içerisinde verinin anahtarlanması ya da yönlendirilmesi, veri yönlendirme güzergahlarının düzenlenmesi, veri paketlerinin önceliklendirilmesi gibi işlemleri yerine getirir. Bu fonksiyonların ortak özelliği paket üzerinde önceden belirlenmiş kuralların uygulanarak, ağ yöneticileri tarafından belirlenen işlemlerin yerine getirilmesini, diğer bir deyişle veri üzerinde kontrolü sağlayabilmektir. Konvansiyonel ağ donanımlarının ve yazılımlarının çalışma şekli, ağ üzerindeki veri işleme yetenekleri ve donanım davranışları, donanımın ve yazılımın yetenekleri ile sınırlanmaktadır.

İnternet kullanımının servislerdeki hızlı artışa bağlı olarak artması, veri paketlerinin ve veri trafiğinin esnek bir şekilde işlenebilmesinin bir gereksinim olarak hissedilmesine neden olmuştur. Önceleri donanımlar üzerinde programlanabilir ağ fonksiyonları ile karşılanmaya çalışılan bu gereksinim, bilgisayar ağlarındaki kontrol katmanının ve veri katmanının ayrılmasını hedefleyen açık kaynak arayüzlerin geliştirilmesi ile bugün kullandığımız SDN (Software Defined Networking) ve NFV (Network Function Virtualization) mimarilerinin ortaya çıkmasını sağlamıştır.

SDN ve NFV Nedir?

SDN, bilgisayar ağlarının kapasite, trafik kontrol, değişim ve davranış açılarından açık arayüz katmanları aracılığı ile programlanabilmesini ifade etmektedir. SDN mimarisinin sadeleştirilmiş bir görseli şekil 1'de gösterilmiştir.

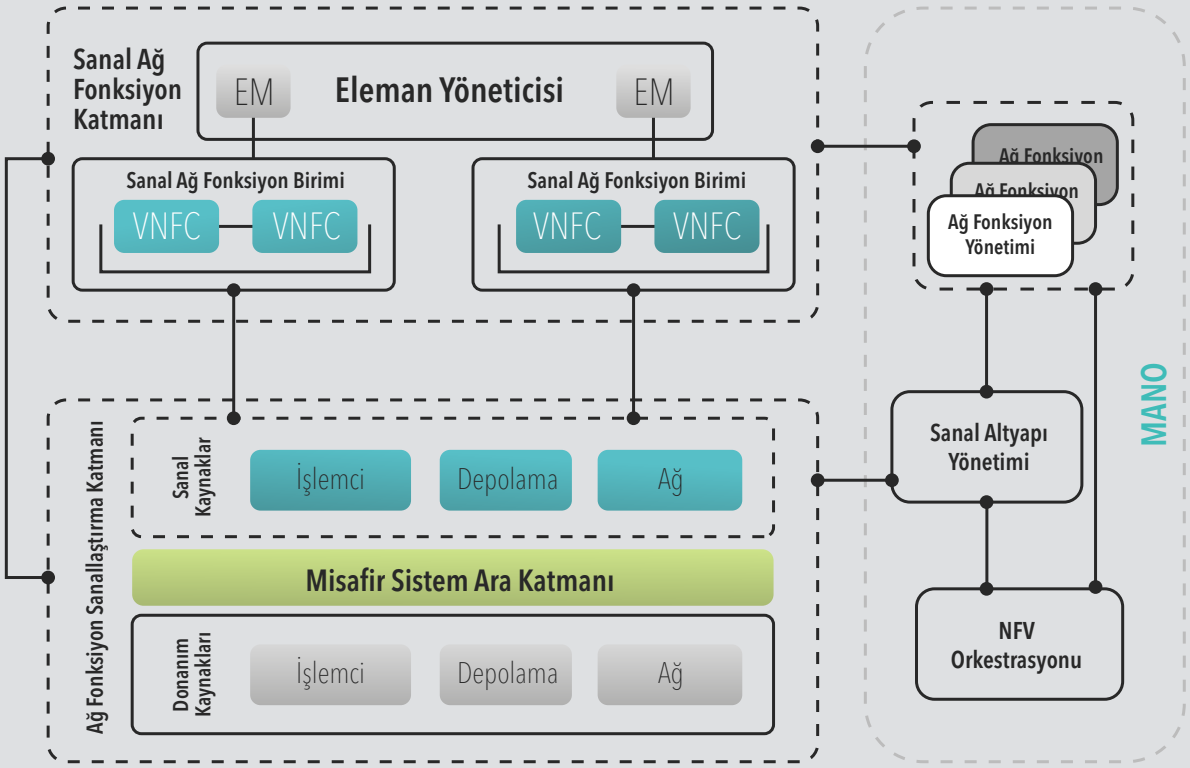


Şekil 1: SDN Mimarisi: Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76.

SDN mimarisinin donanımlarla haberleşmesini sağlayan donanım haberleşme arayüzleri (SouthBound API) mimarinin temelini oluşturmaktadır. Bu API (Application Programming Interface)'ler arasında en çok tanınanı olan OpenFlow protokolünün ilk çalışmaları 2009 yılında Open Networking Foundation tarafından yayınlanmıştır. Bu standartlaşma çalışması Alcatel-Lucent, Big Switch, Brocade ve Radisys gibi pazar payı yüksek firmalar tarafından desteklenmiş ve halen devam etmektedir. OpenFlow'un yanında 2004 yılında IETF (Internet Engineering Task Force) tarafından tanımlanan ForCES (Forwarding & Control Element Seperation) ya da OpenState, POF (Protocol Oblivious Forwarding) gibi protokoller ağ donanımlarını programlamada kullanılabilecek haberleşme arayüzleri ve yaklaşımlar için farklı alternatifler sunmakta ve bu alanda gelişmelerin devam ettiğini göstermektedir.

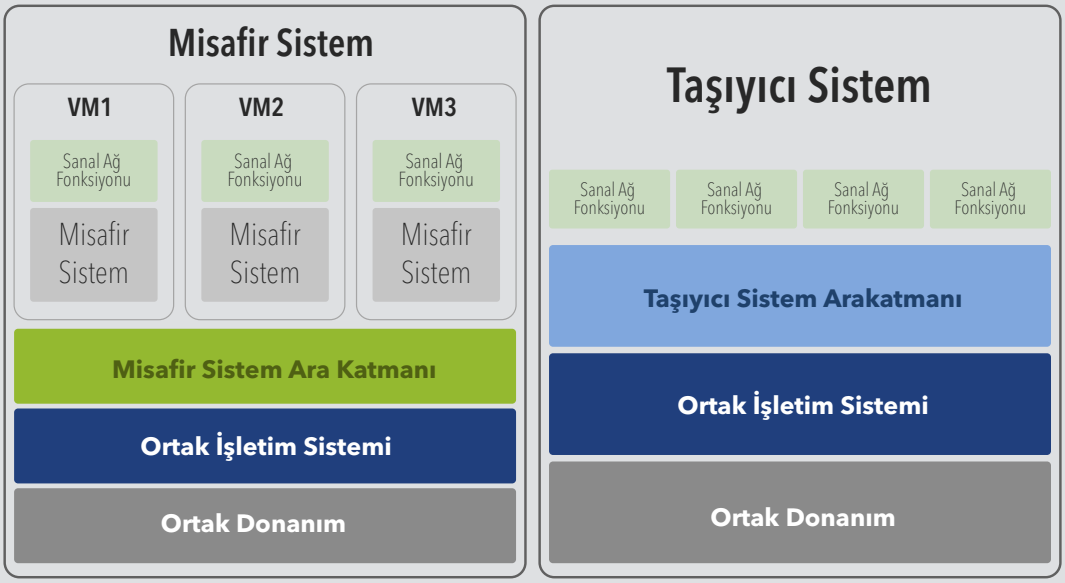
SDN gibi NFV de ağ yöneticilerinin esneklik ihtiyacına cevap vermeyi amaçlayan bir mimaridir. SDN'den farklı olarak NFV'de amaç konvansiyonel ağ cihazlarında kullanılan fonksiyonları, sanallaştırma teknolojilerinden yararlanarak donanımdan bağımsız hale getirebilmektir.

Genel olarak NFV mimarisi sanallaştırılmış ağ fonksiyonlarının, birbirleri ile olan haberleşmelerini ve ortak Sunucu kaynaklarının kullanımını düzenleyecek orkestrasyon birimlerinden oluşur. NFV mimarisinin bir görseli şekil 2'de gösterilmiştir.



Şekil 2: NFV Mimari Gösterimi: Yi, B., Wang, X., Li, K., & Huang, M. (2018).
A comprehensive survey of network function virtualization. Computer Networks, 133, 212-262.

Misafir sistem ara katmanına alternatif olarak, giderek yaygınlaşan taşıyıcı (container) yapısı da NFV sanallaştırmaları için kaynak gereksinimlerini azaltarak uygun altyapı çözümleri sunmaktadır. Sanallaştırma ara katmanı ve taşıyıcı mimarilerinin kullanılması arasındaki farklar şekil 3'te gösterilmiştir.

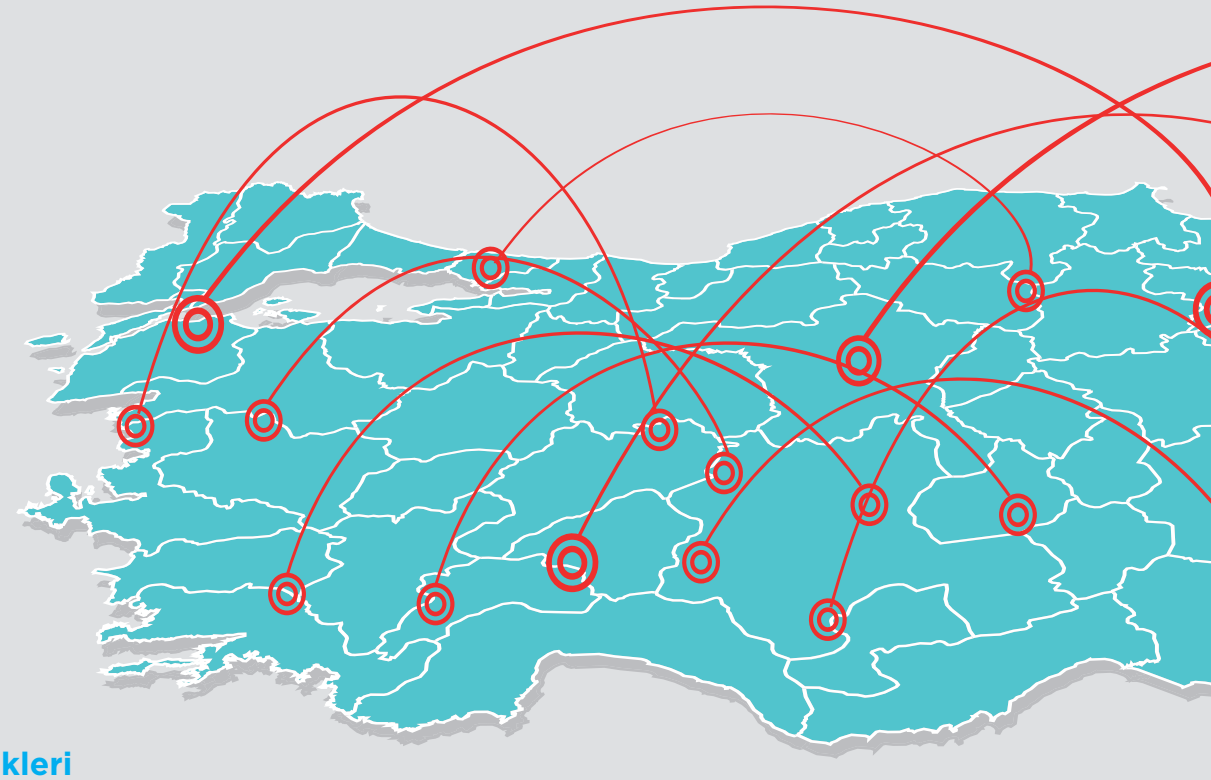


Şekil 3: NFV Hypervisor ve Container Yapıları: Yi, B., Wang, X., Li, K., & Huang, M. (2018). A comprehensive survey of network function virtualization. Computer Networks, 133, 212-262.

NFV mimarisinde orkestrasyon birimi (MANO), sanal birimlerin kaynak ihtiyaçlarının düzenlenmesinden ve yaşam döngülerinden sorumludur. Avrupa Telekomünikasyon Standartları Komitesi, Orkestrasyon Biriminin özelliklerini genel olarak belirlemektedir. OpenMANO, ZOOM ve OpenSource MANO (OSM) bu standartlara uyularak hazırlanmış ürünlerin bazı örnekleridir.

Sanallaştırma Katmanı ve orkestrasyon katmanı, sanal ağ fonksiyonlarının (VNF) gerçekleştirimini sağlar. Sanal ağ fonsiyonlarına örnek olarak yönlendiriciler, adres dönüştürme fonksiyonları, trafik hızlandırma ve yük dağıtım fonksiyonları gösterilebilir. NFV mimarisinin hedefi temel olarak bu fonksiyonların, sunucular üzerinde de özerk donanımlarda gösterdiği davranışları göstermesidir.

SDN ve NFV, bilgisayar ağlarının yazılım tabanlı mimariye dönüşümlerinde iki ana akımı oluşturmaktadır. SDN, ağ cihazlarının programlanması ve esnek bir işleme ortamı sunmayı hedeflerken NFV, bilgisayar ağlarının hızlı ve donanımdan bağımsız olarak hizmete sunulmasını hedeflemektedir. İki mimarinin de ortak özelliği OPEX ve CAPEX giderlerinin düşürülmesi ve yeni servis mimarilerinin kolayca oluşturularak kullanıcılara sunulmasıdır.



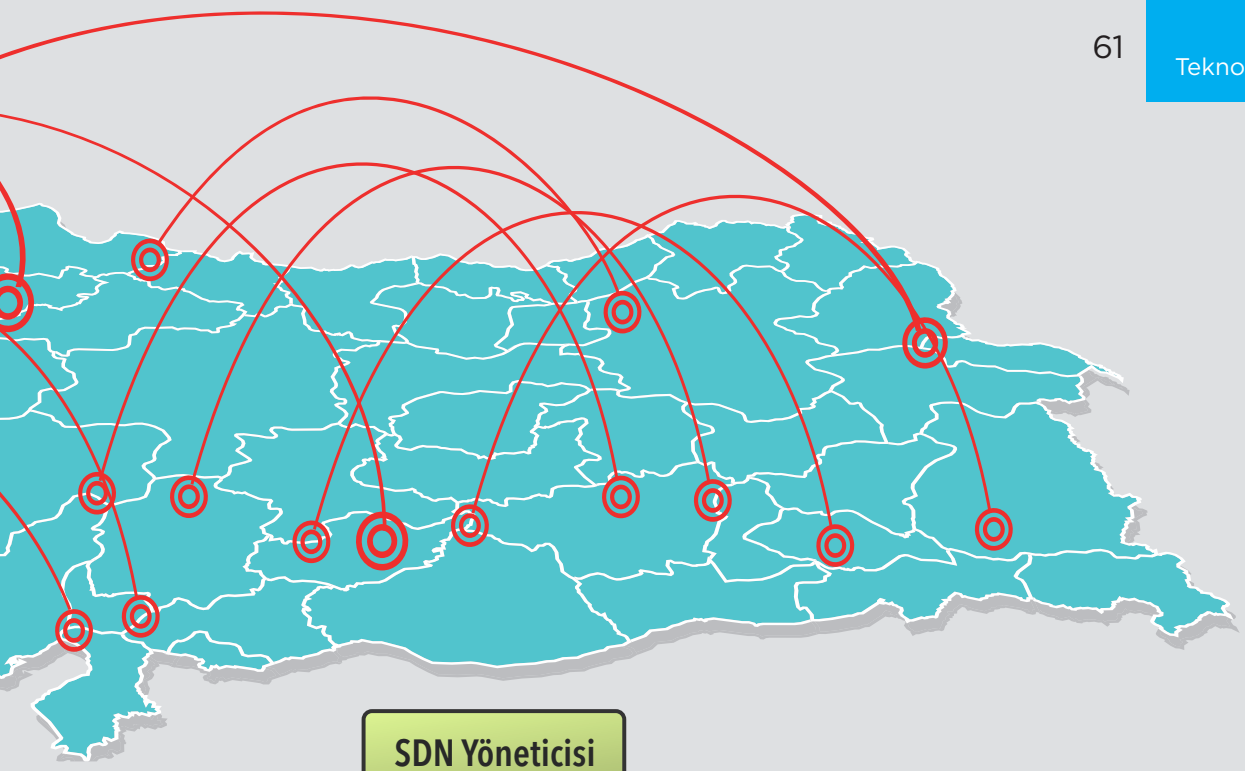
SDN'nin Yenilikleri

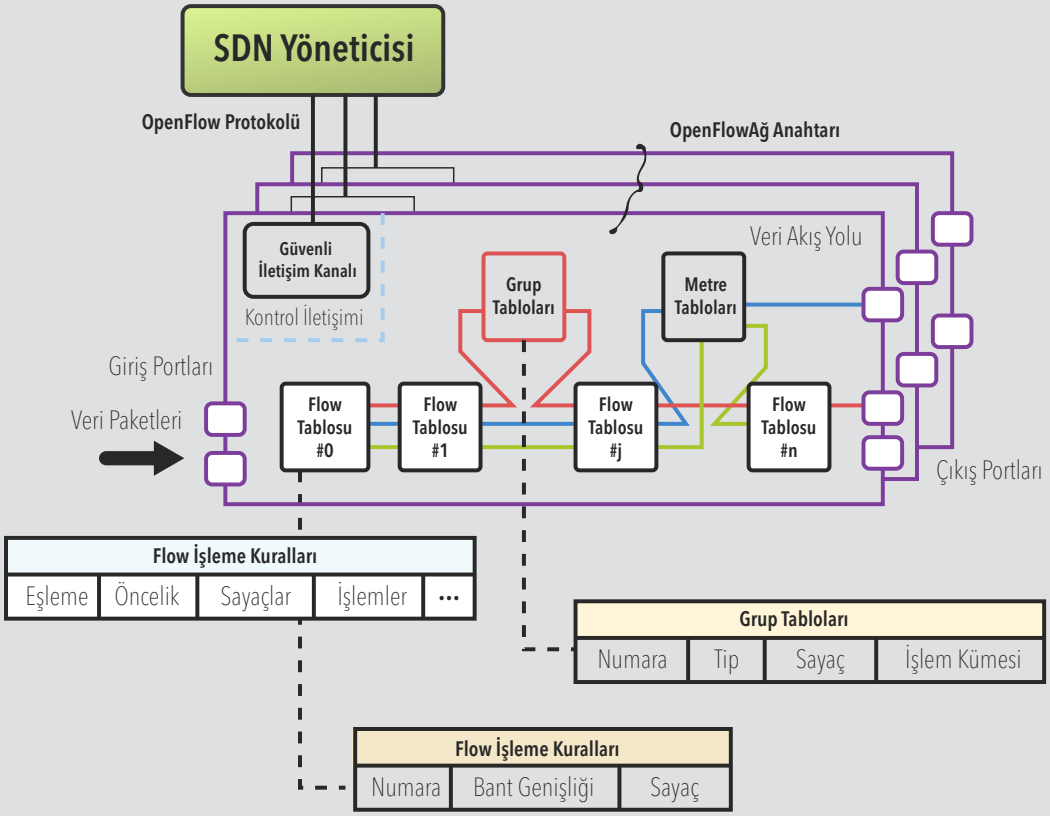
SDN, mimari olarak konvansiyonel bilgisayar ağlarından ayrıldığı gibi, donanımlarının çalışma şekli olarak da farklılık göstermektedir. Konvansiyonel bilgisayar ağlarında, OSI (Open Systems Interconnection) ağ modeline bağlı kalınarak anahtarlama işlemleri veri bağlantı katmanında, yönlendirme işlemleri ağ katmanında, güvenlik duvarı ve yük dağılımı işlemleri ulaştırma katmanında ve üzerindeki katmanlarda yapılır. Bu yapı, mimari olarak düzenleme getirmesine karşın, düzenlemenin uygulamadaki karşılığı, yapılacak işlem için farklılaşmış donanımlar ya da birden fazla işlemin bir araya geldiği donanımlardır. OSI mimarisine bağlı kalınarak ağ oluşturmak yüksek maliyete, birleştirilmiş donanımların kullanılması ise yazılımlara bağlı entegrasyon sorunlarına neden olur. SDN mimarisi ile bu işlemler anahtarlama donanımına indirgenebilir.

OpenFlow anahtarlama standardı, anahtarlar için aşağıdaki eşleştirme alanlarını tanımlamaktadır:

- Geliş portu
- VLAN (Virtual Local Area Network) numarası ve öncelik değeri
- Ethernet kaynak adresi
- Ethernet hedef adresi
- Ethernet çerçevesi tipi
- IP kaynak adresi
- IP hedef adresi
- IP
- IP ToS (Type of Service) değeri
- TCP/UDP kaynak portu
- TCP/UDP hedef portu

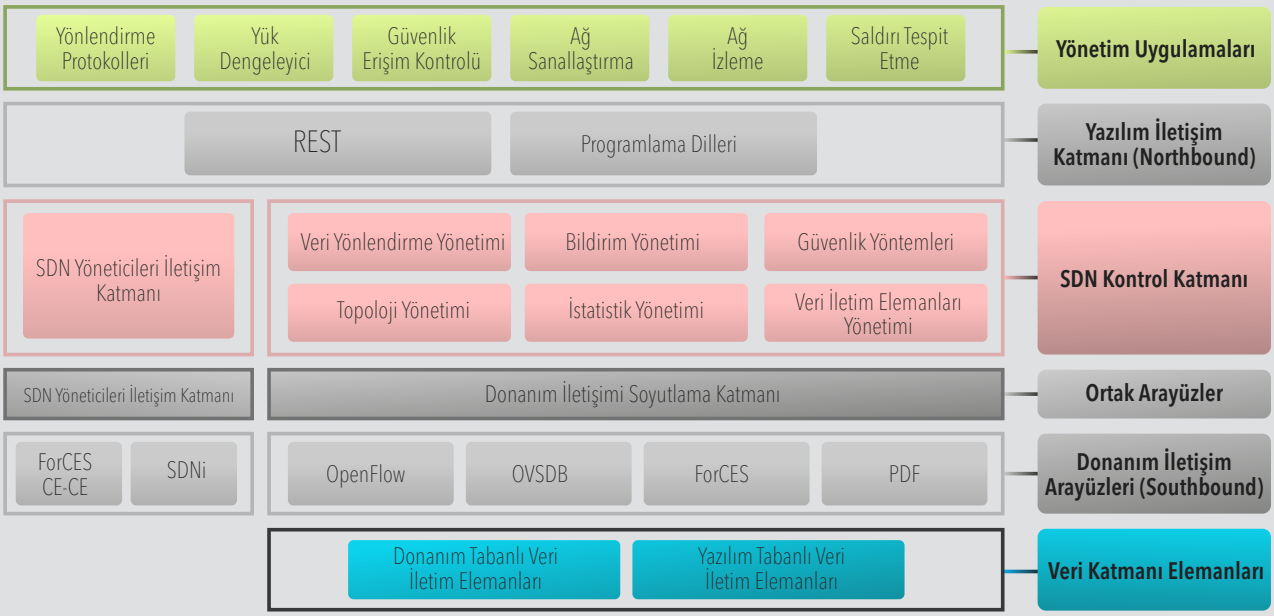
Veri paketleri, SDN anahtarlara ulaştığında, donanım tarafından yapılacak yönlendirme için bu alanlar istenilen kombinasyonda kullanılabilir. Ek olarak OpenFlow 1.3'te, birden fazla kural kümesinin tablolar halinde işleme konulabilmesi için gereksinimler tanımlanmıştır. OpenFlow temelli bir anahtarlama donanımındaki iş akışlarını gösteren bir görsel şekil 4'te gösterilmiştir.





Şekil 4: OFSwitch İşlem Akışı: Challa, R., Jeon, S., Kim, D. S., & Choo, H. (2017). CentFlow: centrality-based flow balancing and traffic distribution for higher network utilization. IEEE Access, 5, 17045-17058.

SDN mimarisi ağ kontrolünde de farklılıklar ve esneklikler sunmaktadır. SDN mimarisinde kullanılabilecek bazı kontrol programları farklı programlama dili destekleri ve kullanıcı arayüzleri ile sunulmaktadır. Çoğunluğu açık kaynak olan bu programların akdemik çalışmalarda yoğunlukla kullanılan örnekleri Floodlight, OpenDaylight, Ryu, NOX ve POX olarak sıralanabilir. Kontrol programlarının ortak mimarisinin görseli şekil 5'te gösterilmiştir. Bu şekilden de anlaşılacağı üzere yönetim uygulamaları katmanı, yazılımsal olarak mümkün olan tüm veri işleme yöntemlerinin ağ üzerinde de yapılmasına imkan vermektedir.



Şekil 5: SDN Denetleyici Yazılım Mimarisi: Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76.

SDN'nin Endüstri Uygulamaları

Bilişim sektöründeki öncü firmalardan Google, 2012 yılında, dünya geneline yayılmış veri merkezlerini genel internet trafiğinden ayrı bir şekilde birleştirmek için, kendi tasarımları olan SDN yönlendiriciler kullanarak B4 ağını oluşturdu. B4 ağı sayesinde, servis kalitesinde bir düşüş yaşamadan Veri Merkezleri'nde uygulama seviyesinde trafik kontrolü ve veri hatlarında %100'e yakın kullanım oranlarına ulaşmayı başardı. B4 ağı ilk kurulduğu gün dünya internet trafiğinin %1'ine eşdeğer trafik taşırken, takip eden dört yıl içerisinde taşıdığı trafik miktarı on kat arttı.

Organizasyonlar tarafından yoğun bir şekilde kullanılan MPLS çözümlerinden, internet servis sağlayıcılardan ve bağlantı için kullanılan veri hattı altyapısından bağımsız bir şekilde trafik yönlendirmeyi ve özerk trafik işleme kabiliyetlerini kazandıran bu çözüm, benzer şekilde uzak lokasyonlarını birleştirerek veri merkezi servislerini sunan organizasyonlarda da ilgi oluşturdu.

Sektörde oluşan bu ilgi, bilgi teknolojileri alanında ürün geliştiren firmaların SD-WAN (Software Defined Wide Area Network) ve çeşitli tünel teknolojileri üzerinde çalışan kaplama SDN (overlay SDN) çözümlerinin oluşmasını sağladı.

IDC (International Data Corparation), SD-WAN alanında pazar için 4.5 milyar $'lık bir derinlik ve yıllık %40 büyüme oranı tahmin etmektedir.

Networkworld; internet of things, big data ve 5G gibi teknolojilerin yaygınlaşması ile SDN pazarının ve ürün çeşitliliğinin artacağını belirtmektedir.

SDN/NFV ile ilgili ASELSAN Çözümleri

ASELSAN olarak, SDN ve NFV alanındaki gelişmeleri yakından takip ederek ürettiğimiz milli ağ cihazlarında bu mimarilerin gereksinimlerini uygulamak ve ürünlerimizi bu mimari içersinde konumlandırmak için çalışmalarımız devam etmektedir. Bunun yanında mevcut geliştirme çalışmalarımızın kontrol katmanında konumlandırılabilmesi ve mimarinin ihtiyaçlarını karşılayacak desteği sunması için geliştirme faaliyetlerimiz bulunmaktadır.

Sonuç

Dünyamız, veri işlemeye bağlı teknolojilerin yaygınlaşması ve kolay ulaşılır hale gelmesiyle hızlı bir değişim sürecine girmiştir. Bu değişimin en önemli sağlayıcılarından olan bilgi teknolojileri alanında değişim ve gelişim sürmektedir. ASELSAN donanım ve yazılım seviyesinde, yeni ağ teknolojilerini ve öne çıkan gelişmeleri, sektörün sivil ve askeri ihtiyaçlarını da göz önüne alarak, yakından takip etmektedir. ASELSAN'ın devam eden bu gelişime bilgi birikimi, tecrübe ve yetenek olarak katkı sunması, mimari yapıların sivil ve askeri alanda kabul edilmesini hızlandırmanın yanında, bu alanlarda yerli ve milli teknolojilerin üretilmesini de hızlandıracaktır. Bu da, bağımsızlığımızın önemli unsurları olan üretim ve teknoloji alanlarında, şirketimiz ve ülkemiz adına yeni fırsatların doğmasını sağlayacaktır.

Kaynakça

(1) Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76.

(2) Yi, B., Wang, X., Li, K., & Huang, M. (2018). A comprehensive survey of network function virtualization. Computer Networks, 133, 212-262.

(3) Challa, R., Jeon, S., Kim, D. S., & Choo, H. (2017). CentFlow: centrality-based flow balancing and traffic distribution for higher network utilization. IEEE Access, 5, 17045-17058.

(4) Jain, S., Kumar, A., Mandal, S., Ong, J., Poutievski, L., Singh, A., ... & Zolla, J. (2013). B4: Experience with a globally-deployed software defined WAN. ACM SIGCOMM Computer Communication Review, 43(4), 3-14.

(5) Specification, OpenFlow Switch Sepcification 1.5.1, Open Networking Foundation

4G/4.5G/5G CPE Teknolojileri

Hazırlayan
Mehmet Uçak
HBT SMD Bilgi Teknolojileri Sistem Mühendisliği Müdürlüğü

Son yıllarda 4G/4.5G/5G ile ilgili teknolojik gelişmeler özellikle cep telefonu operatörlerine ve internet servis sağlayıcılarına müşterilerine ulaşmak için önemli açılım sağlamış ve CPE (Customer Premises Equipment) pazarında ilgili teknolojilerin kullanımı yaygınlaşmıştır.

Günümüzde hem ülkemizde hem de tüm dünyada insanlar için her zaman, her yerde ve yüksek veri hızında kesintisiz haberleşme bir ihtiyaç olmaktan çıkıp bir zorunluluk haline gelmiştir. Nitekim cep telefonu operatörleri ve internet servis sağlayıcıları için daha fazla aboneye ulaşmanın yolu bu beklentiyi sağlamaktan geçmektedir.

Bu beklentiyi karşılamadaki en büyük zorluk ise tüm hanelere veya binalara ilgili hizmeti götürmek için altyapıdaki eksiklikler ve zorluklardır. Cep telefonu operatörleri ve internet servis sağlayıcıları, abonelerine istenilen hizmetleri sunabilmek için fiber optik altyapıya ihtiyaç duymaktadırlar. Ancak ülkemizde hala 15 milyondan fazla haneye fiber optik altyapı ile ulaşılamadığı değerlendirilmektedir. Bunda fiber optik altyapı kurulumunun yüksek maliyetinin yanı sıra coğrafi koşulların ortaya çıkardığı zorluklar da önemli bir rol oynamaktadır. Benzer şekilde dünyanın pek çok coğrafyasında fiber optik altyapının yok denecek kadar az olduğu birçok ülke olduğu da bir gerçektir.

İşte bu noktada 4G/4.5G/5G ile ilgili gelişmeler cep telefonu operatörleri ve internet servis sağlayıcıları için bir çıkış noktası olmuş ve her haneye fiber optik hat ulaştırmak yerine 4G/4.5G/5G tabanlı CPE'ler ile çözüm sağlamaya başlamışlardır.

Söz konusu çözümler ile abonelerin 4G/4.5G/5G üzerinden WAN (Wide Area Network) erişimi sağlanırken, lokalde yani LAN (Local Area Network) düzeyinde haberleşmeleri Wi-Fi ve/veya ethernet anahtar çözümleri ile sağlanabilmektedir. Bu sayede kablolu haberleşme bir binanın ve hanenin içinde sınırlı kalacak şekilde birçok aboneye internet hizmeti sunulabilmektedir.

4G/4.5G/5G CPE'ler; bina içi çözümler, bina dışı çözümler ve çatı çözümleri olarak üç genel tipte tasarlanıp üretilmektedir.

Bina içi çözümler, 4G/4.5G/5G sinyal seviyesinin yeterli olduğu ve propagasyon etkileri nedeniyle haberleşmede sıkıntılar yaşanmayan noktalarda çözüm olabilmektedir. Nitekim sinyal seviyesinin yeterli olmadığı ve/veya propagasyon sorunlarının haberleşmeyi zorlaştırdığı noktalar için de bina dışı çözümler kullanılmaktadır. Çatı çözümleri ise her iki durum için de iyi bir optimizasyon sağlayarak özellikli çok haneli binalarda çatılarda kullanılmakta ve çatılardan hanelere ethernet anahtar tabanlı bir LAN ile dağıtım sağlanmaktadır.

Şu anda ülkemizdeki cep telefonu operatörleri ve internet servis sağlayıcıları ilgili ürünler için tamamen dışa bağımlıdırlar. Bu ürünlerin yerli ve milli olanaklarla tasarlanıp üretilebilmesi için ASELSAN, 2019 yılından itibaren bir dizi çalışmalar başlatmıştır. 2021 yılında tasarımı, geliştirmesi ve kalifikasyonları tamamlanması hedeflenen 4G/4.5G/5G CPE'ler ile cep telefonu operatörleri ve internet servis sağlayıcıları için yerli ve milli çözümler oluşturulması hedeflenmektedir.

4G/4.5G/5G ile ilgili teknolojik gelişmelere bağlı olarak yakın geleceğin vazgeçilmez konusu olan otonom sürüşün merkezinde yer alacak olan TCU (Telemetry Control Unit), CPE pazarında öne çıkan bir diğer üründür.

Geleceğin otomobillerinin en kritik parçalarından biri olacak 5G TCU ürünleri, hem otomobil içerisindeki tüm telemetri bilgilerini toplayıp kontrol edecek, hem otomobil dışındaki sensörlerden verilerek toplayıp bunları işleyebilecek, hem de 5G üzerinden bu verileri bir merkez ile paylaşabilecektir.

ASELSAN tarafından 5G TCU ile ilgili araştırmalara başlanmış olup Türkiye'nin Otomobili Girişimi Grubunun da gereksinim duyduğu bu ürün için yerli ve milli bir çözüm oluşturulması hedeflenmektedir.

Kripto Cihazları ile Güvenli Ağ Mimarisi

Hazırlayan
Ayça Bahar Yıldırımoğlu,
Kaan Sergen Arslan,
Fırat Rozkan Kılıç
HBT KBTPD Kripto ve Bilgi Güvenliği Sistem Mühendisliği Müdürlüğü

Günümüz dünyasında verinin değerliliği tartışılmaz bir konu haline gelmiştir. Sadece kritik kurumlar değil tüm devlet kurumları, kuruluşlar, özel şirketler, okullar, bankalar sahip oldukları verinin korunması üzerine önlemler almaya çalışmaktadır. Verinin güvenliğini korumak bireysel ortamlarda da gündemimizdedir.

Değerli ve kritik verinin bulunduğu ortamlarda korunmasının yanı sıra veri akışında da alınabilecek her türlü güvenlik önlemi alınmalıdır. Bu önlemlerin başında haberleşme ağlarında güvenli mimariler oluşturmak gelmektedir. Güvenli ağ mimarileri tasarlanırken hem verinin erişilebilirliği hem de verinin gizliliği ve bütünlüğü korunması hedeflenmelidir. Kripto cihazı kullanımı güvenli ağ mimarilerinde hedeflenen güvenlik seviyelerini sağlamak amacıyla yer almalıdır.

ASELSAN, güvenli ağ mimarisi tasarımlarında ağ kripto cihazlarını konumlandırarak haberleşme ağlarında güçlü korumalar sağlamaktadır. Cihazların gizlilik (confidentiality), bütünlük (integrity) ve doğrulama (authentication) özellikleri yer aldıkları ağlarda kullanıcıların verilerini ve veri trafiğini yüksek güvenlik seviyelerinde korumaktadırlar. Kripto cihazlarında yer alan algoritmalar, talep edilmesi durumunda ASELSAN bünyesinde tasarlanmakta ve donanımsal olarak yine ASELSAN Mühendisleri tarafından gerçeklenmektedir. Algoritma tasarımı ve gerçeklemelerin özgün olması, haberleşmenin bilinmeyen algoritmalarla kriptolanmasını sağlayarak, anahtarın gizliliği ile birlikte, saldırganların veri elde etme ihtimalini ortadan kaldırmaktadır. ASELSAN Ağ Kripto Cihazları uçtan uca kriptolama, güçlü kimlik doğrulama ve veri bütünlüğü mekanizmaları ile tüm haberleşme akışını çeşitli ağ mimarilerinde (star, mesh vb.) korumaktadır.

ASELSAN tarafından geliştirilmiş link kripto cihazı ve IP kripto cihazı ürünleri yurt içi ve yurt dışı pek çok kurumda ve kuruluşta güvenli ağ mimarilerinin temel parçası olarak kullanılmaktadır. Cihazlar, IP ağlarında iletilen tüm verilerin Gizli gizlilik seviyesinde korunmasını sağlamaktadır. Kripto cihazları, TÜBİTAK BİLGEM bünyesindeki milli laboratuvarlarda kripto analizi testine, TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) testine ve COMSEC (Communications Security) testine tabi tutulmaktadır. Link kripto cihazı, link seviyesinde kriptolama işlemi gerçekleştirirken, IP kripto cihazı ağ seviyesinde kriptolama işlemi gerçekleştirmektedir. Tasarlanan topolojilerde yüksek hız gereksinim olan, tahsis edilmiş linklerin kullanıldığı, veri linklerinin kullanıldığı, link seviyesinde alt yapının sağlandığı sistemlerde link kripto cihazı kullanımı tercih edilmektedir. Güvensiz ağlarda yönlendirme işlemi gerektiren, IP adreslerine göre politikalar belirlenen sistemlerde IP kripto cihazı kullanımı tercih edilmektedir. IP ağlarının mantıksal ayrım yapması nedeniyle kullanıcılar fiziksel konumdan bağımsız olarak güvenli iletişim kurabilmektedir.

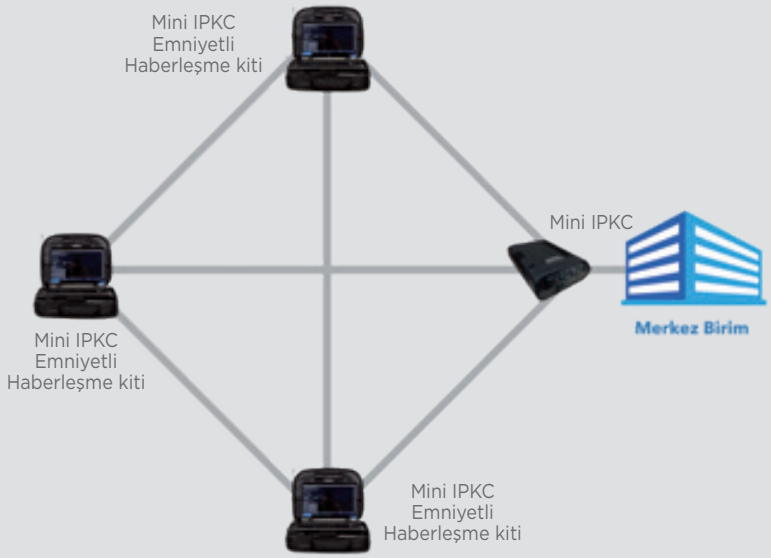
Haberleşme ağları, kurumların kullanım şekillerine, yöntemlerine ve alt yapılarına göre oluşturulmaktadır. Kurulacak olan ağ yapısına göre link kripto cihazı ve/veya IP kripto cihazı kullanılmaktadır. IP kripto cihazları ile sistem konfigürasyonuna göre politikalar girilerek yıldız ve örgü (mesh) topolojiler kurulabilmektedir. IP kripto cihazı ve link kripto cihazı içeren örnek bir mimaride merkez birim ile merkeze bağlı alt birimlerin yıldız topoloji üzerinden güvenli haberleşme trafiği sağlama amacıyla IP kripto cihazı konumlandırılabilir. Merkezde yer alan kripto cihazının tüm birimlere hizmet verebilmesi için yüksek hızlı veri geçirme özellikli olması tercih edilmelidir. Uç birimlerin cihaz tercihleri fiziksel koşullara göre tercih edilebilir. Merkez birimi ile veri yedekleme amaçlı kullandığı felaket kurtarma birimi arasındaki haberleşme, tahsis edilmiş hatlar üzerinden link kripto cihazı kullanılarak güvenli hale getirilebilir.

Güvenli Ağ Mimarisi'nde Kripto Cihazı Kullanımı

Geniş alan ağında IP kripto cihazı ile güvenli hatlar kurulması politika yapılandırması gerçekleştirilerek merkez ile güvenli haberleşebilen bir yıldız topoloji kurmak mümkündür. Ağ kripto cihazı ailesinin hız ve çevre koşulu gereksinimlerine göre geliştirilmiş farklı modelleri mevcuttur. Geniş alan ağı üzerinde IPsec (IP Security) benzeri tüneller kurularak güvenli iletişim kurulmaktadır. Örnek topolojide merkez birimi için yüksek trafik gereksinimi ihtiyacı öngörülerek çift yönlü 18 GBitps veri aktarım hızına sahip 10G kripto cihazı, uç birimlerin daha düşük trafik gereksinimi ihtiyacı öngörülerek çift yönlü 350 MBitps veri aktarım hızına sahip 2064 Mini IPKC Cihazları konumlandırılmıştır. Topolojiye ayrıca taktik sahadaki bulunan askeri standartlara uygun IPKC-v2 Cihazı ile güvenli iletişim hattı eklenmiştir. Ayrıca genel merkezde bulunan değerli veriler çift yönlü 800 MBitps veri aktarım hızına sahip Mini LKC Cihazları ile metro ethernet hattı üzerinden güvenli olarak felaket kurtarma merkezine yedeklenmektedir.

ASELSAN tarafından geliştirilmiş Emniyetli Haberleşme Kiti (EHAK) mobil kullanıcıları olan topolojilerde yer alabilmektedir. EHAK sisteminde, 3G/4G MODEM, 2064 Mini IPKC Cihazı, güç kaynağı bulunmaktadır. Kullanıcılar, taşınabilir EHAK sistemi ile 3G/4G altyapısının desteklendiği herhangi bir konumdan geniş alan ağı üzerinde güvenli haberleşebilmektedir. Böylece kurumlar saha kullanıcıları ile konumdan bağımsız güvenli haberleşme gerçekleştirebilmekte, güvenli ağlarına bu kullanıcılarının dahil olmasını sağlayabilmektedir. Merkez biriminde oluşturulacak kripto yönetim merkezi ile cihazların uzaktan konfigürasyon, kriptografik yönetim ve anahtar

yükleme işlemlerini gerçekleştirilebilmektedir. EHAK, 3G/4G ağları üzerinden güvenli haberleşme imkanı sağlamaktadır. Benzer bir topoloji uydu sistemlerinde uydu modem birimleri ile kripto cihazları kullanılarak uydu ağlarında güvenli haberleşme imkanı sağlamakta kullanılabilir. ASELSAN IP Kripto Cihazları yurt içi ve yurt dışı birçok uydu sisteminde haberleşme güvenliği sağlayan unsur olarak konumlandırılmıştır.



EHAK Birimi ile Güvenli Ağ Mimarisi

Mantıksal olarak aynı yerel alan ağda bulunan fakat fiziksel olarak farklı konumlarda yer alan birimlere sahip ağ topolojilerinde kripto cihazlarının yer alması için Mini IP Kripto Cihazının LAN (Local Area Network)-WAN (Wide Area Network) yeteneğine sahip çalışma modu kullanılabilir. Bu çalışma modu ile geniş alan ağı üzerinde güvenli linkler oluşturulabilmektedir. Cihazlar geniş alan ağının ucundaki iki farklı noktayı yerel alan ağı gibi birbirine bağlayarak güvenli bir iletişim altyapısı oluşturmaktadır.

Geniş Alan Ağı Üzerinde Güvenli Yerel Alan Ağı Mimarisi

Örnek verilen topolojilerde kripto cihazlarının kullanımı haberleşme trafiğine güçlü güvenlik önlemleri kazandırmaktadır. ASELSAN'ın milli özgün ve farklı konfigürasyonlara uyumlu çözümleri birçok mimariyi destekleyecek yapıda geliştirilmekte, yurt içinde ve yurt dışında ilgili kurumlara hizmet vermektedir. Güvenli ağ mimarisi tasarımlarında kripto cihazlarının kullanımı sistemlerin vazgeçilmez tercihi olmalıdır. ASELSAN, güncel ağ teknolojisinin yüksek hız gereksinimlerine uygun ve güçlü kripto çözümleri içeren cihazlar gerçekleştirmekte ve güvenli ağ mimarilerinde kullanılacak ürün ailesini genişletmeyi hedeflemektedir.

Kuantum Sonrası
Kriptografi Çözümleri

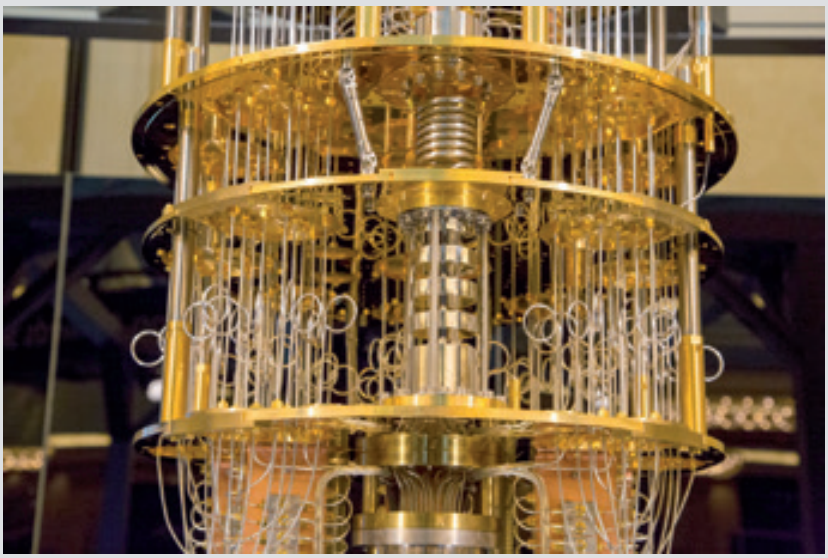
Hazırlayan
Murat Burhan İlter, Uzman Algoritma Tasarımcısı
HBT KBTPD Kripto ve Bilgi Güvenliği
Sistem Mühendisliği Müdürlüğü

Hazırlayan
Sevgi Babacan Çetin, Müdür
HBT KBTPD Kripto ve Bilgi Güvenliği
Sistem Mühendisliği Müdürlüğü

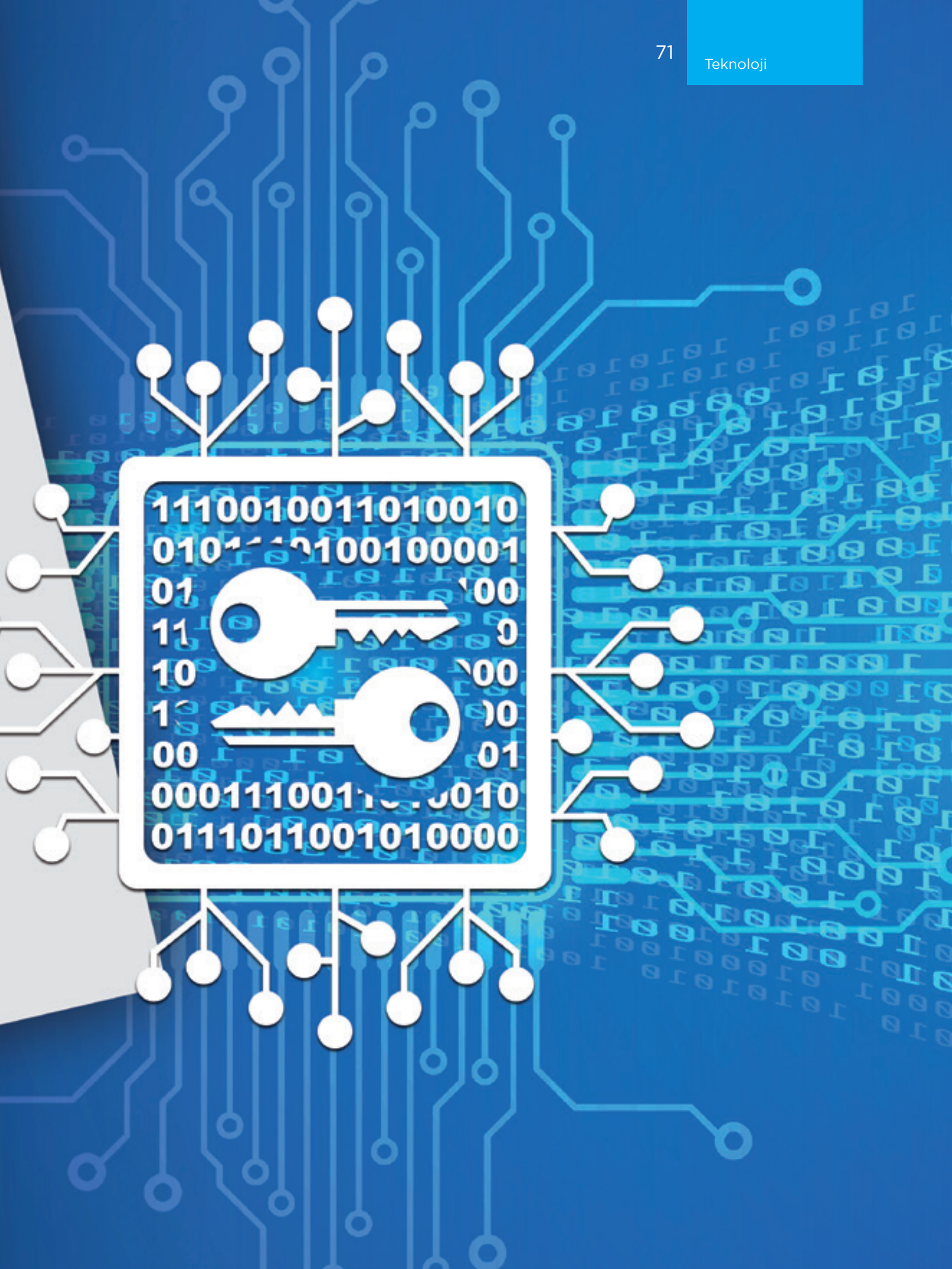
Şifreleme Algoritmaları, simetrik ve asimetrik olarak ikiye ayrılmaktadır. Simetrik sistemler genellikle şifreleme işlemlerinde kullanılırken asimetrik sistemler genellikle imzalama, kimlik doğrulama ve anahtar paylaşım protokollerinde kullanılmaktadır. Kripto algoritmalarının güvenliği gizli anahtarların makul sürelerde ele geçirilememesine dayanmaktadır.

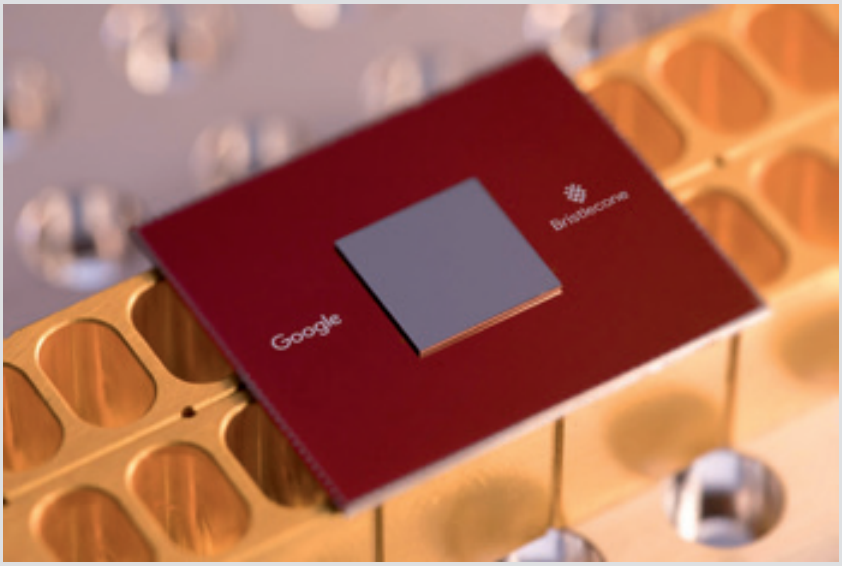
Günümüzde kullanılan asimetrik sistemlerin güvenliği üzerinde yıllarca çalışılmış matematiksel olarak zor olduğu düşünülen problemlere dayanmaktadır. Örneğin, RSA (Rivest-Shamir-Adleman) algoritmasının güvenliği çarpanlara ayırma problemine, sayısal imza algoritmasının ve Diffie-Hellman anahtar değişiminin güvenliği modüler ve eliptik eğriler üzerinde tanımlanan ayrık logaritma problemine dayanmaktadır. İşlemci gücünün artmasıyla daha uzun anahtarların kullanılması ihtiyacı doğmaktadır. Klasik bilgisayarlar kullanarak şu an güvenli olarak kabul edilen sistemlerin anahtarlarının makul sürelerde elde edilmesi mümkün değildir.

Kriptografi, disiplinler arası bir bilim dalı olmakla birlikte temel bilim ve mühendislik alanında yapılan çalışmalar doğrultusunda şekillenmektedir. Örneğin, kuantum fiziğinin kriptografi alanında önemli etkileri olmuştur. Kuantum mekaniğine ait (belirsizlik ilkesi, foton polarizasyonu, dolanıklık vb.) teknikler kullanılarak oluşturulan çözümlere Kuantum Kriptografi adı verilmiştir. Uygulama alanları arasında kuantum anahtar dağıtımı ve kuantum rassal sayı üreteçleri bulunmaktadır. Ayrıca IBM ve Google firmalarının üretmiş oldukları kuantum bilgisayar ve kuantum çip, sırasıyla, şekil 1'de ve şekil 2'de verilmiştir.



Şekil 1: IBM Kuantum Bilgisayarı


11100100110100100
01011100100100001
01 00
11 0
10 00
1 0
00 01
000111001 0010
01110110010100000



Şekil 2: Google Bristlecone Kuantum Çipi

Kuantum bilgisayarların çalışma prensipleri kullanılarak yapılan analiz çalışmaları literatürde bulunmaktadır. 1994 yılında Shor'un ve 1996 yılında Grover'in önermiş olduğu algoritmalarla asimetrik ve simetrik kriptosistemlerin güvenlikleri önemli ölçüde etkilenmiştir (1, 2). Shor, yapmış olduğu çalışma ile günümüzde birçok alanda kullanılan asimetrik sistemlerin yeterli büyüklükte kuantum bilgisayarlar inşa edildiği takdirde güvensiz olacağını göstermiştir. Grover, yapmış olduğu çalışmada ise yeterli seviyede kuantum bilgisayarlar kullanılarak simetrik sistemlerin güvenliğinin anahtar uzunluğunun yarısı kadar güvenlik seviyesi sağlayabileceğini göstermiştir. Bu çalışmalar sonucunda simetrik sistemlerin anahtar uzunluğunu iki katına çıkarmak yeterli olurken RSA, eliptik eğri kriptografisi, Diffie-Hellman anahtar değişimi ve sayısal imza gibi asimetrik sistemlerin güvensiz olduğu sonucu çıkmaktadır.

Çarpanlara ayırma ve ayrık logaritma problemlerinin kuantum bilgisayarlara karşı dayanıksız olduğu anlaşıldıktan sonra matematiksel olarak zor olan diğer problemler incelenmeye başlanmıştır. Kuantum sonrası kriptografi (post quantum cryptography), kuantum bilgisayarlara karşı dayanıklı olduğu düşünülen zor matematiksel problemler kullanılarak oluşturulan kriptosistemlerdir.

Bu kriptosistemleri beş ana alt başlıkta incelemek mümkündür:

- Latis (kafes) tabanlı kriptosistemler
- Kod tabanlı kriptosistemler
- Özet tabanlı kriptosistemler
- İzojeni tabanlı kriptosistemler
- Çok değişkenli kriptosistemler

2016 yılında NIST (National Institute of Standards and Technology) tarafından kuantum sonrası kriptografi alanında standart olabilecek algoritma belirlemek amacıyla bir süreç başlatılmıştır. Bu süreç kapsamında aday algoritmaların hem klasik hem de kuantum ataklara karşı dayanıklı olması, performans ve gerçeklendiği platform üzerinde kapladığı alan kıstaslarına göre değerlenme yapılmaktadır. 2019 yılında ikinci tur aday algoritmalar açıklanmıştır. Aday algoritmalar arasında anahtar kapsülleme, şifreleme ve imzalama algoritmaları bulunmaktadır. 2022-2024 yılları arasında kuantum sonrası taslak standardının yayınlanması hedeflenmektedir.

NATO tarafından 2019 yılında kuantum tehdidi yüksek risk olarak belirlenmiştir. Anahtar paylaşımı, haberleşme gizliliği ve haberleşmede kaynak doğrulama ve inkar edememe mekanizmaları kuantum dayanıklılık çalışmalarını önümüzdeki yıllarda gerçekleştirmeyi ve sistemlere kazandırmayı hedeflenmektedir.

ASELSAN, kripto cihazı tasarımında öncü gerçeklemeler sunmak amacıyla kuantum ataklarına dayanıklı anahtar paylaşımı, kimlik doğrulama ve sayısal imza algoritması geliştirme çalışmalarına başlamıştır. Bu doğrultuda yurt içinde ve yurt dışında kuantum sonrası kriptografi alanında yapılan çalışmalar ve NIST'in süreci yakından takip edilmektedir. Üniversiteler ile ortak projeler yapılmakta ve bu alanda çalışan akademik personellerin tecrübelerinden faydalanılmaktadır.

ASELSAN ile TÜBİTAK BİLGEM, kuantum sonrası kriptografi alanında ortak çalışmalar yürütmektedir. Bu kapsamda düzenlenen Kuantum Sonrası Kriptografi Çalıştayı, 5 Aralık 2019 tarihinde yapılmıştır. 29 Şubat - 1 Mart 2020 tarihleri arasında gerçekleşen ASELSAN-TÜBİTAK BİLGEM İş Birliği Çalıştayında alınan kararlar doğrultusunda projelendirilmesi muhtemel Milli Savunma Bakanlığı ve Savunma Sanayii Başkanlığı projelerinde ortak çalışma kararı alınmıştır.

Klasik kriptografi ile kuantum sonrası kriptografi çözümlerinin birlikte kullanıldığı yöntemler hibrit yöntemler olarak adlandırılmakta ve bu sistemlerin kullanılması önerilmektedir. ASELSAN tarafından tasarlanan güvenli ağ mimarisi çözümlerinde kullanılacak kripto cihazlarında hibrit yöntemlerin uygulanması için çalışmalar devam etmektedir. Bu alandaki çalışmalar ile ASELSAN bünyesinde tasarlanan güvenli ağ mimari çözümlerinin, yeterli büyüklükte kuantum bilgisayarlar inşa edilse bile, sistemlerin güvenli olması hedeflenmektedir.

Kaynakça

(1) Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.

(2) Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

ASELSAN Siber Güvenlik Çalışmaları

Hazırlayan
Dr. Sinan Şenol
HBT KBTPD Kripto ve Bilgi Güvenliği Sistem Mühendisliği Müdürlüğü

Siber Güvenlik Hayatımıza Nasıl Girdi?

1900'lü yılların başında da Nikola Tesla'nın kablosuz dünya sistemi hayali ile başlayan internet düşüncesi, 1960'larda Amerikan Savunma Bakanlığının ilk çalışan prototip ARPANET'inin kurulmasıyla gerçekleşmeye başladı. 1 Ocak 1983'te ARPANET'in TCP/IP protokol yığınını uyarlamasıyla modern internet ağların ağı fikri somutlaştı. 1994 yılında bilgisayar uzmanı Tim Berners-Lee'nin World Wide Web'in (WWW) temellerini atmasıyla bildiğimiz internet daha yaygın bir hal aldı.

Peki siber güvenlik ne zaman başladı? Her ne kadar son yıllarda siber güvenlik kulaklarımızı çokça doldursa da, siber güvenliğin tarihi internetin tarihi kadar, hatta çok daha eski. Elektronik bileşenlerin gelişmediği zamanlarda farklı yöntemlerle siber güvenliğin gizlilik bileşeni farklı yöntemlerle kullanılıyordu. Örneğin Romalıların ünlü hükümdarı Sezar, mesajlarının gizliliğini korumak için her mesajının harflerini sonraki beşinci harf ile değiştiriyordu. Tabii, elektroniğin gelişmesi ile siber dünyadaki saldırılar da oldukça teknolojik bir şekil aldı.

Her ne kadar internet evlerimize geç girse de ilk bilgisayar zararlı yazılımı 1971 yılında Bob Thomas'ın yarattığı bilgisayar solucanıydı. Çok zararlı bir yazılım değildi, sadece bilgisayar ekranına beklenmedik bir mesaj gösteriyordu. 1989'da Robert Morris'in yazdığı ağın büyüklüğünü hesaplama yazılımı bir bilgisayar solucanına dönüştü ve ilk servis dışı bırakma saldırısına neden oldu. Morris, zararlı bir yazılım yaratma amacıyla yapmamıştı ama sonuç ekonomik maliyet olarak ciddi bir durum oluşturdu.

İnternetin ilk çıkması ile dikkat toplayan siber güvenlik konuları, günümüzde hayatımızın bir parçası haline geldi. Bugün mobil teknolojiler insanlara ailesinden bile daha yakın bir hale gelmiş durumda. Bilgi teknolojilerinin hayatımızın her noktasına girmiş olması, hayatımızın her noktasında siber güvenliğin de bir eylem maddesi olduğunu gösteriyor.

Siber güvenlik her türlü saldırıya karşı hazırlıklı olmayı gerektiriyor. Bu saldırılar uygulama şekline göre birçok farklı biçim alabiliyor. Örneğin iki iletişim kuran sistem arasına girmeye dönük ortadaki adam saldırıları. Bilgi işlem sistemlerinin yazılımlarının içine sızan zararlı yazılımlar (virüs, solucan, trojan vb.). Bilgisayarların kontrolünü eline alan botnetler. Web uygulamalarının içine sızmaya neden olan saldırılar (SQL injection, cross-site scripting vb.). Daha ileri gidip ülkelerin ve kurumların üzerinde odaklanan APT'ler yani ileri hedefli saldırılar. Kurumların içinden ortaya çıkan içteki saldırganlar (insiders). Birçok ülke kurumlarının oldukça başını ağrıtan bilgi işlem verilerini şifreleyen fidye isteyen zararlı yazılımlar (ransomware). Görüldüğü gibi siber saldırılar her noktadan ortaya çıkabildiği için, siber güvenlik hayatımızın bir parçası durumunda.

Siber saldırılar dünyanın üstünde bu kadar büyük bir maliyet ve kişisel yaşamları tehdit eder bir duruma düşünce siber güvenlik de bu duruma yanıt verme yönünde aynı hızla gelişti. Siber güvenliğin ana kavramları modellendiğinde üç kavram oldukça kapsayıcıdır. Bunlar gizlilik, bütünlük ve erişilebilirliktir. Siber güvenlikte bu üç kavramın bir bilgi sisteminde doğru bir şekilde gerçeklenmesi, güvenliğin en temel gereksinimi olarak görülmektedir.


aselsan

Bir bilgisayar sisteminin ve ağının, gizlilik, bütünlük ve erişilebilirliğini sağlamak için birçok teknoloji, prosedür ve yönetim mekanizması işin içinde olmalıdır. Bu anlamda siber güvenlik tek bir unsurla sağlanacak bir koruma değildir. Bütüncül bir yaklaşım gerektirir. İnsanların farkındalığı da bu anlamda çok önemlidir. Sosyal mühendislik saldırıları insanların kişisel zaaflarından faydalanarak siber saldırı gerçekleştirme yöntemidir.

Teknolojik siber güvenliği sağlama yöntemleri çok çeşitli. Bilgisayar sisteminin ağ çıkışının önünde konumlandırılan güvenlik duvarları, saldırı tespit/önleme sistemleri, DDoS zayıflatıcılar, ağ güvenli geçit sistemleri bunlar arasında sayılabilir. Bilgisayar sistemlerinin içinde konumlandırdığımız antivirüs ve internet güvenlik bileşenleri de bunlarından bazıları.

Bir bilgi teknolojisi sisteminin siber güvenliğinin sağlanması sadece siber güvenlik cihazları ile sağlanması mümkün değildir. Tamamen kurumsal organizasyon gerektirmektedir. Bu noktada her kurumun en tepe noktasının desteğini gerektirmektedir. Bu hususta standartlaşma dünya genelinde katılımla belirgin bir ilerleme katetmiştir. ISO:27000 standartları serisi bu noktada sağlam bir temel oluşturmaktadır. NIST 800 doküman serisi de siber güvenliğin daha çok devlet kurumlarına dönük bir siber güvenlik temeli oluşturmaktadır.

Ülkemizde de bu durum ciddi bir şekilde ele alınmaktadır. Tüm kurumlar siber güvenliğin ne kadar öncelikli olduğunun farkındadır. Bu noktada T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığının Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2016 – 2019), her Türkiye Cumhuriyeti kurumu mensubunun farkında olması gereken bir rehberdir. Ülkemizdeki siber güvenlik ekosistemini daha iyi algılamak için bu eylem planı mutlaka incelenmelidir.

Ülkemizde özellikle Savunma Sanayii Başkanlığının öncülük ettiği Siber Güvenlik Kümelenmesi bu süreçte ulusal sinerjiyi artıracak etkiyi yaratmaktadır. Kümelenmenin, üretilecek ürünlerin kalitesini ciddi oranda geliştirmesi kaçınılmazdır.

ASELSAN da siber güvenliğin önemini yeterli düzeyde algılamış ve bu konuda çok yönlü yaklaşımlar geliştirmiştir. Bundan sonraki bölümde, ASELSAN'ın siber güvenlik yaklaşımına değineceğim.

Sanal Hava Boşluğu

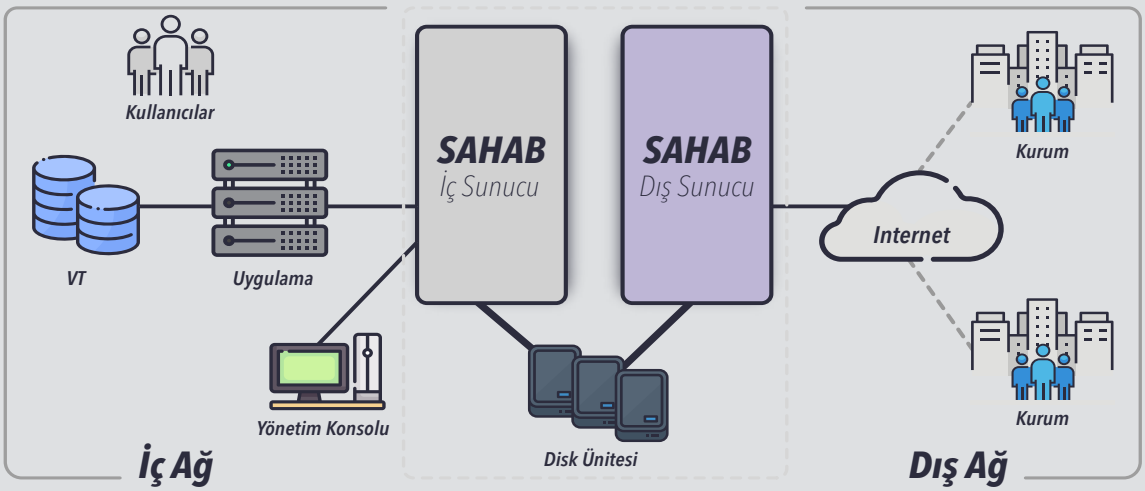
AGİT

AGİT Projesi, Türk Silahlı Kuvvetlerinin görev kritik kullanım ihtiyacını karşılamak üzere 2017 senesinde teslim edildi. Bir önceki SAHAB versiyonundan eklenen beş yeni protokol ile daha geniş bir bağlantı ihtiyacını karşıladı. Arttırılan güvenlik özellikleri ile ortak kriter EAL 4+ düzeyinde sertifika sahibidir. Bu aşamadan sonra kullanımı birçok kamu kurumunda yaygınlaştı.

SAHAB'ın konfigürasyonu iki yüksek işleme kapasitesine sahip sunucu ve bunların arasında bilgi paylaşımını sağlayan disk ünitesinin biraraya gelmesi ile oluşmuştur. Sunucularda bulunan yazılımlar sıkılaştırılmış işletim sistemi üzerinde yerli ve milli olarak tasarlanmıştır.

Farklı güvenlik seviyesindeki ağların bağlantısını hedefleyen SAHAB, yüksek güvenlik ihtiyacı olan ağı koruyucu yüksek güvenlik özellikleri ile güvenli bilgi alış verişi sağlamaktadır. AGİT Projesinin ana ürünü olan SAHAB şu an yedi protokol desteklemektedir. Bunlar sırasıyla HTTP/S, FTP/S, SMTP, TLS ve VoIP iletişim protokolleridir. Kurumsal ağın SAHAB üzerinden güvenli ağ çıkışı ile kurumsal ağın güvenlik seviyesine zarar vermeden çift yönlü iletişimi mümkün kılmaktadır.

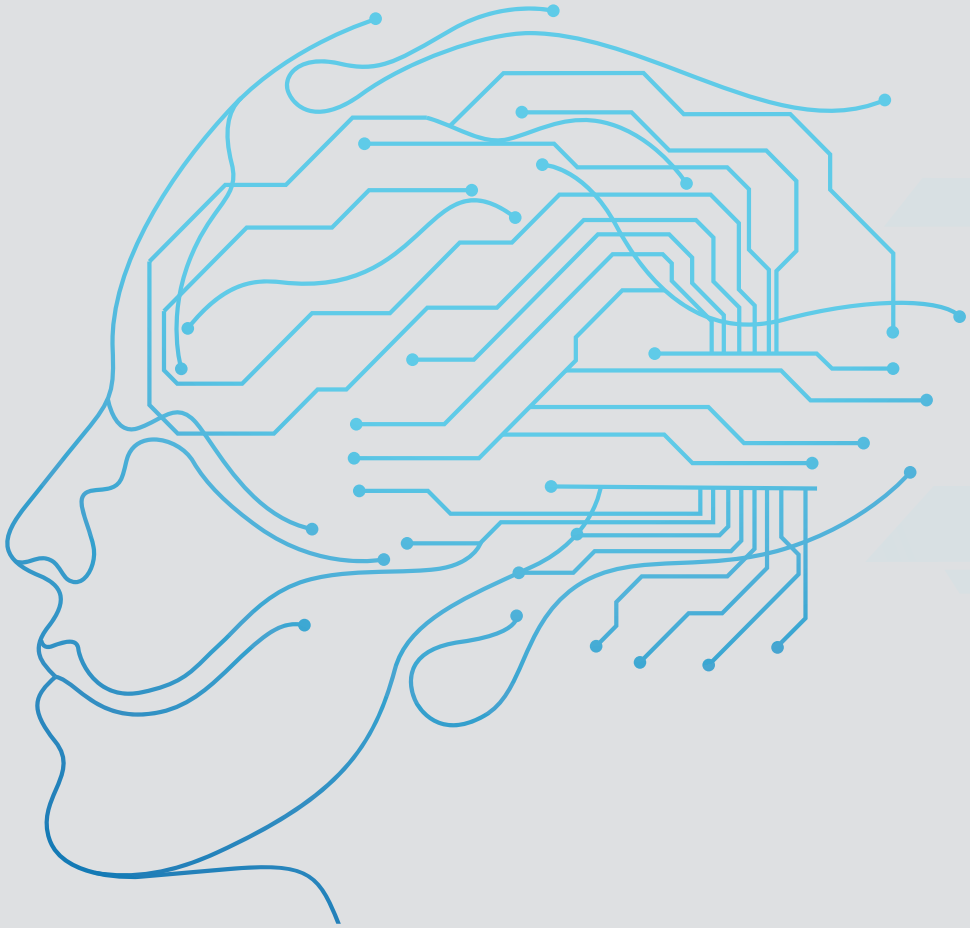
SAHAB, bu bağlantı ihtiyacını karşılarken, birçok güvenlik bileşenini sistemine entegre etmiştir. Bunlar arasında olan IDS/IPS, WAF, dosya bütünlük aracı, firewall, antivirüs yazılımı güvenliği sağlam tutmayı sağlamaktadır.



Versiyon 3.0

SAHAB şu an yeni yazılımı ile yepyeni özellikler destekleyecek ve performansını arttıracaktır. Hız için çok tatmin edici değerleri vadeden SAHAB'ın yeni yazılımı da güvenliği arttırılmış olarak sunulacaktır. SAHAB'ın mimari yapısına yapılacak güncelleme ile daha önce görülmemiş hızlara çıkması beklenmektedir.

SAHAB yeni yazılımı güçlü bilgi etiketleme ve kontrol becerileri ile NATO ADatP-4774 ve 4778 destekleyecektir. Güvenliğin ön planda olduğu yeni yazılımda kullanıcı ihtiyaçları ön planda tutulmaktadır.



Ortak Kriter Sertifikası

SAHAB bilgi teknolojisi alanının en çok kabul gören güvenlik sertifikası olan ortak kriter sertifikasına sahiptir. SAHAB'ın güvenlik sertifika düzeyi EAL 4+ düzeyindedir. Bu sertifika ile SAHAB metodik olarak tasarlandığını, test edildiğini ve değerlendirildiğini ispatlamıştır. EAL 4 seviyesine ek güvenlik özellikleri ile EAL 4+ düzeyine ulaşmıştır.

Yapay Zeka ve Siber Güvenlik

Projelere Yapay Zeka İyileştirme Entegrasyonları

Siber güvenlikte yapay zeka teknolojileri oldukça olgunlaştı. Yapay zeka teknolojilerinin sunduğu fırsatlar projelerin her safhasında kullanılmak için bekliyor. Yapay zeka teknolojileri, müşteriye sunulan ürünün bir bileşeni olabileceği gibi, ürünün son hale gelmesinde yürütülen sürecin bir parçası da olabilir. Bu sayede müşterinin memnuniyeti ileri noktalara taşınabilir.

Biz de projelerimizin özellikle her safhasında daha iyi tasarım ve performansa kapı açacak yapay zeka teknolojileri entegrasyonları üzerinde çalışıyoruz. Projelerin özellikle analitik modellemesi zor veya mümkün olmayan aşamalarında yapay zeka algoritmaları iyi çözüme ulaşmayı sağlıyor.

Yapay Zeka Siber Güvenlik Platformu

Üzerinde çalıştığımız projelerin özellikle fizibilitesi açısından uygun olanlarına yapay zeka iyileştirmesi üzerinde çalışıyoruz.

Siber güvenlik konusunda da modellemenin kolay olmadığı durumlar oldukça fazla. Bir açıdan bakıldığında, siber saldırıların ana merkezi insan zekasının davranış biçimlerine dayandığı için, çözümün de yine benzer biçimde çalışan algoritmalar ile sağlanması en kuvvetli aday.

Buradan hareketle, özellikle yeni ürünlerimizden saldırı tespit özelliği bulunan cihazların ilk sürümlerini yapay zeka bileşenleri ile müşterimize sunmak için çalışıyoruz. Bu ürünlerin yerli ve milli kaynaklar ile hazırlanması güvenliklerini katlayacak bir faktördür.

Yapay zeka çözümlerimiz için tasarladığımız platform, sadece yazılım değil donanım ile desteklenenen bir genel çözüm olma yolunda ilerliyor. Bu platformun hızlı tasarlanması ve hızlı entegrasyonu projelerimizin sürecinin en önemli hedefi.

Yapay zeka teknolojileri bazı problemler için şu an için tek çözüm olma niteliğinde. Örneğin, büyük veri ve bulut bilişimin yaygınlaşmasıyla işlenecek veri ciddi derecede artıyor. Bunu işletecek insanın bütün veri işlemesine gücü yetse dahi hata yapmaması ve konsantrasyonunu kaybetmemesi lazım. Güvenlik amaçlı yapılacak analizler için de aynı durum sözkonusu. İnsan görevlilere güvenilerek yapılan çalışmalarda en geçerli kural en zayıf halkanın insan olduğu prensibidir. Dünyada yapay zekaya yapılan yatırım çok yüksek durumda. Şu an için herkesin cebindeki telefonların insanın her işin yapabilmesindeki potansiyeli farkeden üreticiler bunu yönetmek için yapay zeka teknolojilerinden yararlanıyor. Apple için Siri, Google için Google Asistan, Amazon için Alexa ve Samsung için Bixby her geçen gün daha etkili ve yetenekli hale geliyor. Bu noktada da bu yapay zekalar kendi içinde yarışıyor. Bu yarış insan için etkili bir dost mu yaman bir düşman mı olacak? Buna yapay zeka konusunda ülke olarak atacağımız adımlar belirleyici olacak.

Yapay zeka çalışmaları devamlı gelişen, evrimleşen uzun soluklu bir faaliyet olacaktır. Burada atılacak milli yapay zeka merkezi temeli, siber güvenlik açısından önemli bir kazanç olacaktır. Milli yapay zekanın en performanslı çözüm olması açısından hibrit bir yaklaşımla kural tabanlı çözümleri ve makine öğrenmesini adapte etmesi iyi bir başlangıç olarak görünüyor.

ABD'nin bir çok devlet kurumu güvenliği için yapay zeka merkezli güvenlik çözümleri kullandığını biliyoruz. Ülkemizin de yapay zeka merkezi ile siber güvenliğine etkili bir yardımcıya ihtiyacı tartışmasızdır.

Siber Güvenlikte Yeni Teknolojiler

Web Uygulama Güvenlik Duvarı

Siber dünyada saldırılar gitgide daha sofistike yaklaşımlarla gelişiyor. Buna karşılık siber güvenliğin de bu trende cevap vermesi gerekiyor.

Bu noktadan hareketle, özellikle uygulama düzeyindeki saldırı tespit ve önleme sistemlerinin önemi ön plana çıkıyor.

İnternet dünyasının en geniş uygulama platformu olan web uygulamaları da güvenliğin en ihtiyaç duyulduğu uygulama seviyesi alan olma noktasında. Biz de web uygulama güvenlik duvarı çözümünü kısa zaman içerisinde ürünlerimizin arasına katmayı planlıyoruz.

Web uygulama güvenlik duvarı saldırı tespit ve önleme çözümlerinin çokça zorluk içeren alanlarından birisi. Bu noktada, özellikle yapay zeka teknolojisinin sağlayacağı faydaları ürünün içerisine dahil etme yönünde ilerliyoruz. Ürünün hem yazılımsal hem de donanımsal seçeneklerle sunulması planlanmaktadır.

Veri Diyodu

Özellikle yüksek güvenlik ihtiyacı olan kurumlarda, güvenlik yaklaşımlarını sadece güvenilir yazılım ve donanım tasarımlarına dayandırma konusunda tartışma olabiliyor. Bu yüzden güvenli yazılım ve donanım tasarımı yanında, güvenli güvenlik mimarisi de güvenliği arttıran önemli bir faktör. Bu yaklaşımla ortaya çıkan veri diyodu mimarisi, hassas bilgi işleyen kurumların, bilgilerinin bağlı oldukları güvenlik riski bulunan ağa bilgi sızmasını engelleyecek mimari çözüm adayıdır.

Ürünlerimizin arasına katmayı planladığımız veri diyodu çözümümüzün en önemli kriteri yüksek güvenlik ve yüksek performans olarak belirlenmiştir. Yüksek hızlara ulaşarak ulusal kurumların kesintisiz bilgi paylaşımını garanti altına almak önemli bir tasarım kriterimiz. Askeri alanlarda ihtiyaç duyulacak özel çevresel koşulları destekleyecek donanımsal tasarım ürünümüzün bir seçeneği olacaktır.

DLP Sistemi

En az web uygulama güvenlik duvarı ve veri diyodu kadar önemli gördüğümüz bir ürün de veri sızıntısını güçlü algoritmik yapısıyla engelleyen DLP çözümleridir. Biz de özellikle bu alandaki ürünleşme çalışmalarımızı bu çerçevede devam ettiriyoruz.

DLP çözümleri bölgesel ve kültürel özelleştirmeleri gerektiren bir çözüm. Bu yüzden, DLP çözümlerinde yerli ve milli tasarımlar, müşteriyi daha çok tatmin edecek potansiyele sahiptir. En son teknolojilerin ve algoritmaların zenginleştirdiği DLP ürünü çalışmalarımız da yapay zeka desteği ile birlikte sunma yolunda ilerlemektedir. Ürünün hem yazılımsal hem de donanımsal seçeneklerle sunulması planlanmaktadır.

Siber Güvenlik Mühendisliği

NIST 800-115 Testleri

ASELSAN projeleri hassas nitelikteki operasyonlarda kullanılmaktadır. Bu yüzden biz de ASELSAN projelerinin müşteriye ulaşmadan olası tüm siber güvenlik testlerinden geçerek ve tespit edilen bulguların düzeltilerek tamamlanması yönünde faaliyet gösteriyoruz.

Özellikle ASELSAN Sektör Başkanlıkları ile yürüttüğümüz, uluslararası kabul görmüş olan NIST 800-115 standardına uygun olarak siber güvenlik testlerini projelerimizde gerçekleştiriyoruz. Projelerin başarısını katlayan bu testler ile kötü amaçlı müdahalelerden ürünlerin uzak tutulmasını hedefliyoruz.

NIST 800-115 testleri birçok başlıkta yapılıyor. Bunlar arasında aşağıdaki yaklaşımları sayabiliriz:

- Oturum yönetimi testleri
- Girdi doğrulama testleri
- Kimlik doğrulama testleri
- Girdi-Çıktı yönetimi testleri
- Kullanıcı parola kırma testleri
- Yetkilendirme mekanizmalarını devre dışı bırakma testleri
- Hizmet dışı bırakma testleri
- Erişime açık olmayan bilgi ve dokümanın erişilebilirlik testleri
- Uygulama sunucusu servisleri denetimi
- Bellek taşma testleri
- Güvenlik cihazları devre dışı bırakma testleri
- Güvenlik cihazları yapılandırma testleri
- İşletim sistemi yapılandırma testleri
- Sunucular/istemciler üzerindeki erişilebilir servis testleri
- Hesapların ele geçirilebilirlik testleri
- Yetki yükseltme testleri

Test sonucunda çıkan zafiyetlere NIST 800-53 özel yayınının da kontrolleri içeren düzeltmeler uygulanıyor.

Sistem Güvenlik Mühendisliği Desteği

ASELSAN projeleri artık tüm sistemlerin tasarım süreçlerinde zorunlu hale gelen sistem güvenlik mühendisliği yaklaşımlarının bir parçası olmuştur. Siber güvenlik sürecinin bir parçası olarak bu süreçte projelerin siber güvenlik gereksinimlerini belirliyor ve projelerin güvenlik gereksinimlerini doğruluyoruz. Bu sayede her proje ön tasarım aşamasından itibaren siber güvenlik kriterleri önde tutularak yürütülmektedir.

Sistem güvenlik mühendisliği süreci ile her projedeki değerli varlıklar, muhtemel zafiyet noktaları, potansiyel tehditler belirleniyor ve muhtemel kötü amaçlı müdahaleler projenin en başından itibaren etkisiz hale getiriliyor.

Sistem güvenlik mühendisliği güvenli donanım geliştirme ve güvenli yazılım geliştirme başlıklarının yanında tüm ürün sistemine bütünsel bakış açısıyla sistemin tasarım, devreye alma, operasyonel ve ömür sonu süreçlerini de kapsıyor. Bu konudaki NIST 800-160 özel yayımı sistem güvenlik mühendisliği temelleri açısından önemli bir başvuru kaynağıdır. Disiplinler arası iş birliğini gerektiren sistem güvenliği güvenlik konusundaki uzmanlık ile ürünün uygulama alanındaki uzmanlığı biraraya getiriyor.

BT Ürünleri için
Pazar Değerlendirmesi

Hazırlayan
Mustafa Çelikkaya, Sadık Burak Bişkin, Beyza Tuğçe Bilgiç
HBT KBTPD Bilgi Teknolojileri Program Müdürlüğü

Bilgi teknolojileri, geçmişten günümüze dünya ekonomisine yön veren, tüm sektörler ile etkileşimde olup ülkelerin gelişmesinde ve kalkınmasında büyük rol üstlenen bir sektör haline gelmiştir.

Sektördeki küresel eğilimler göz önüne alındığında nesnelerin interneti, robotik otomasyon, siber güvenlik, bilgi ve veri güvenliği, askeri teknoloji, akıllı sistemler, yapay zeka, haberleşme gibi bilişim tabanlı uygulamalar özellikle son yıllarda dünya genelinde çalışmaların en çok yapıldığı, gelişmelerin öngörülemez bir hızda ilerlediği alanlar arasında yer almaktadır. Bu teknolojilerin etkin bir şekilde kullanıldıkları durumlarda, tüm sektörlerde verimlilik artışı ve ekonomi alanında da rekabet avantajı sağladığı görülmektedir.

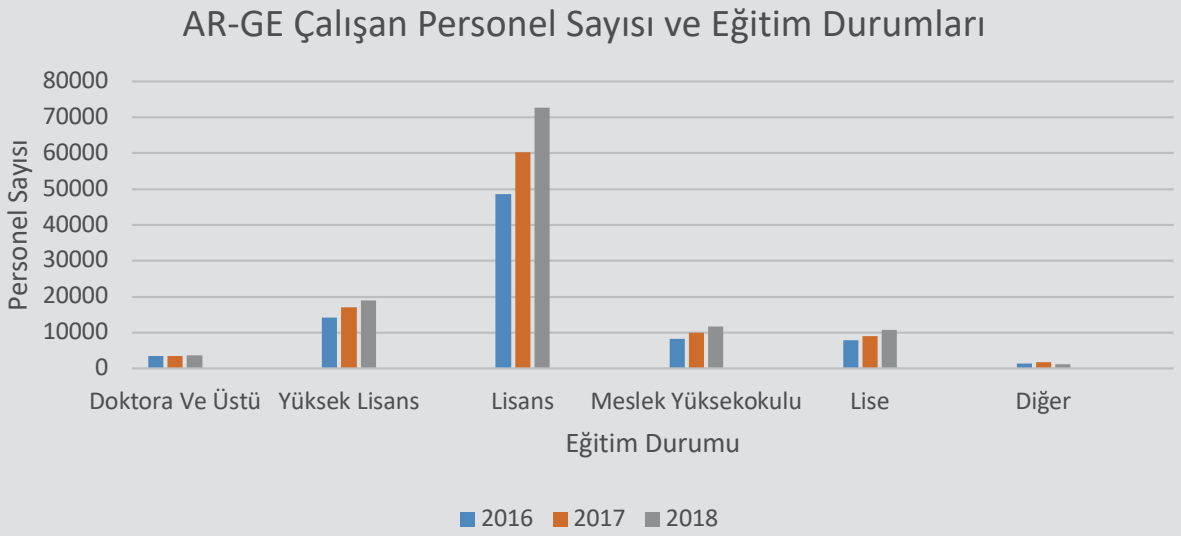
Gartner analiz raporlarına göre dünya genelinde, bilgi ve iletişim teknolojilerinin pazar hacmi 2019 yılında 3.7 trilyon $'lık bir değere ulaşmıştır. Bu değerin 2018 yılında kaydedilen değerden %0.4 daha fazla olduğu görülmüştür. 2020 sonunda ise %3.7 oranında bir büyüme ile tamamlanacağı öngörülmekteyken pandemi olarak ilan edilen COVID-19 salgını tüm dünya genelinde ciddi olumsuz etkiler yaratmıştır. COVID-19 salgını sebebi ile tüm sektörlerde, iş süreçlerindeki verimliliği devam ettirebilmek adına yeni teknolojilerin kullanımı hususunda daha fazla odaklanılarak çalışma düzenlerinde bazı değişiklikler yapılması gerektiğinin farkına varılmıştır[1].

Şekil 1: Bilgi ve İletişim Teknolojileri Pazar Verileri[2]


IoT
CPU
DISK
GPU
79%

COVID-19 salgını sürecinde, dijital altyapıların olası benzeri krizlerin etkilerini azaltacak şekilde geliştirilmesinin, yapay zeka teknolojilerinin ve büyük veri analizlerinin de sürece entegre edilerek kullanılmasının kritik öneme sahip olduğu görülmektedir. Bununla birlikte operasyonların, üretim ve bakım faaliyetlerinin uzaktan yönetimine, kamu sağlığı ve güvenliğinin daha etkili bir şekilde sürdürülebilirliğine imkan veren akıllı sistem uygulamalarının hayatımızdaki önemi daha açık bir şekilde anlaşılarak nesnelerin interneti teknolojilerinin bu sistemlerin geliştirilebilmesi için kritik bir role sahip olduğu gözlenmektedir. COVID-19 ile mücadelede Türkiye yüksek eğitim kalitesi ve her geçen gün artan teknoloji yatırımları ile yeni teknoloji çözümleri üzerinde çok sayıda çalışmayı devam ettirmektedir. Pandemi sürecinde T.C. Sağlık Bakanlığı tarafından insanların bilgilendirilmesi, yönlendirilmesi, uyarılması ve virüsün takip edilebilmesi amacıyla geliştirilen Hayat Eve Sığar (HES) Uygulaması, akıllı uygulamaların faydalarının sadece kriz dönemlerinde değil, normal süreçlerde de etkili olacağını açık bir şekilde göstermektedir. Bu doğrultuda bilgi teknolojileri sektörüne ait değişen küresel eğilimlere karşı, ülkemizin konum alması ve uluslararası faaliyetlere hız vermesi önem arz etmektedir. Bilginin üretilmesi, patent, tasarım ve marka gibi fikri ürüne dönüştürülmesi ve ticarileştirilmesi günümüz ekonomisinde büyümenin ve ülke kalkınmasının temelini oluşturmaktadır. TÜBİSAD (Türkiye Bilişim Sanayicileri Derneği) Bilgi ve İletişim Teknolojileri Sektörü Pazar Verileri 2019 raporuna göre ülkemizin bu sektörde devam ettirdiği önemli faaliyetler neticesinde, sektördeki pazar büyüklüğünde her geçen yıl belirgin bir artış ve süreklilik gözlenmektedir.

Türkiye, jeostratejik konumu sayesinde bilgi ve iletişim teknolojileri alanında yerli ve milli ürünlerin dünyaya ulaştırılmasında elde ettiği avantajlardan yararlanarak AB, Orta Doğu ve Kuzey Afrika ile Asya ve Kuzey Amerika bölgelerine yapılan 1 milyar $'ı aşan bir ihracat değerine ulaşmıştır. T.C. Cumhurbaşkanlığı Yatırım Ofisi verilerine göre ülke genelinde 1200'den fazla Ar-Ge merkezinde, yaklaşık olarak 60 bin çalışan personel bulunmaktadır. Ar-Ge merkezlerinin %23'ü yazılım, bilgi teknolojileri ile elektronik sektörlerinde faaliyet göstermektedir. Ayrıca bu çalışan sayısının %70'inin 35 yaşın altında olmasıyla beraber eğitim düzeyi olarak doktora ve yüksek lisans derecesine sahip araştırmacı insan kaynağı oranı son yıllarda sürekli bir artış göstermektedir[3][4]. Türkiye İstatistik Kurumu verilerine ait Türkiye'deki Ar-Ge personellerine ait eğitim durumu şekil 2'de verilmiştir.



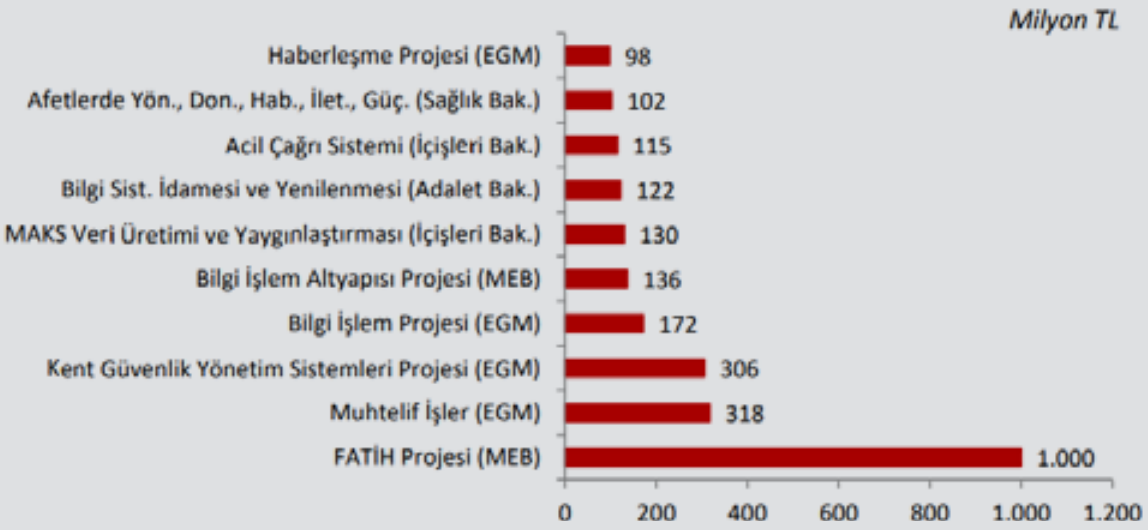
Şekil 2: Türkiye'de AR-GE Çalışan Sayısı ve Eğitim Düzeyleri[5]

4.794 Ar-Ge personeli ile ASELSAN, bilgi teknolojilerinin yerli ve milli imkanlar ile geliştirilmesi amacıyla yıllık cirosunun %7'sini Ar-Ge harcamalarına ayırarak bu sektördeki gelişime yön veren firmalardandır.

Bilgi teknolojilerinin gelişmesinde önemli bir etkisi olan dijitalleşme sürecinde rekabet edebilir bir pozisyonda olabilmek için kullanılan yapay zeka, nesnelerin interneti, büyük veri ve siber güvenlik gibi teknolojilerin etkili ve verimli bir şekilde kullanılması gerekmektedir. İnsan gücüyle geleneksel yöntemlerle yapılan çok fazla işte otonom yöntemlerin kullanılmasının önemine karşı toplum bilincinin oluşmasıyla, dünya genelinde akıllı sistemlerin geliştirilmesi ve hayatımızda uygulanabilirliğini artırabilmek adına önemli yatırımlar ve çalışmalar sürdürülmektedir. Özellikle son yıllarda yaygınlaşan 5G teknolojisi ile beraber sürdürülebilir bir etkileşime sahip olması beklenen kablosuz ağ bağlantısına sahip çok sayıda cihazın internet bağlantısı ile birbiriyle bağlantıda olabileceği düşünülmektedir. Bu gelişmeler doğrultusunda, birçok ülke dijital dönüşüm stratejileri geliştirerek dijital yol haritalarını hazırlamışlardır. Böylece otonom sistemlerin altyapısını oluşturan nesnelerin interneti uygulamalarında daha verimli sonuçlar almak mümkün olacak ve dijital dönüşüm sürecinde önemli adımlar atılmaya başlanacaktır. Bu süreçte dijital ortama taşınan her veri, siber saldırılara karşı yeni ve ciddi riskler oluşturma potansiyeline sahiptir. Kritik altyapıların olası siber saldırılara karşı korunması ve oluşabilecek zararların en aza indirilmesi amacıyla kurumsal dijital dönüşüm süreçlerinin, siber güvenlik risklerinin yönetimine entegre olarak yürütülmesi gerekmektedir. Yerli ve millî yenilikçi teknolojilerin geliştirilmesi, milli yazılımların desteklenmesi ve kritik altyapıların korunması amacıyla kurulan T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, yapay zeka, büyük veri ve siber güvenlik gibi alanlarda ülke genelinde eğitimler vererek ve projeler yürüterek ülkemizin dijital dönüşümünü gerçekleştirmeyi ve ulusal güvenliği sağlamayı hedeflemektedir.

Türkiye'nin dijital dönüşümü kapsamında planlanan değişimlerle birlikte işgücünde de değişim beklenmektedir. Bu aşamada ise nitelikli işgücünün yetiştirilmesi önem kazanmaktadır. Bu amaçla atılması düşünülen başlıca adımlar sürekli eğitim merkezlerinde ve tematik teknik kolejlerde dijital teknoloji kullanıcıların yetiştirilmesi, üniversitelerimizde dijital teknoloji geliştiricileri yetiştiren programların çoğaltılması, eğitimin her kademesinde eğitimcilere dijital yetkinliklerin kazandırılması, özel teşvikler ve desteklerle dijital yetkinliklere sahip işgücünün sanayi ile buluşturulması, dijital dönüşüm farkındalığının artırılması, yaygınlaştırılması ve dijital dönüşüm paydaşları arasında iş birliğinin geliştirilmesidir. T.C. Sanayi ve Teknoloji Bakanlığının dijital teknolojilerinin üretim sürecindeki etki potansiyeli verilerine göre nitelikli iş gücüne sahip olmak, iş gücü verimliliğini %80-%85, kalite yönetimi verimliliğini %10-%20 ve süreç ve kaynak verimliliğini de %3-%5 arttırmaktadır.

Türkiye'de dijital dönüşümde e-Devlet, e-Fatura, e-İmza, e-Bilet, e-Nabız gibi uygulamalar aktif olarak kullanılmaktadır. Dijital dönüşümde lokomotif firmaların başında gelen ASELSAN, kamunun ihtiyacını karşılamak için önemli projelere imza atmıştır. Kent Güvenlik Yönetim Sistemleri (KGYS) Projesi, Mekansal Adres Kayıs Sistemi (MAKS) Veri Üretimi ve Yaygınlaştırılması Projesi ve Acil Çağrı Sistemi (112) Projesi başta olmak üzere son yıllarda en fazla ödenek ayrılan ilk on bilgi ve iletişim teknolojileri projelerinde üç proje ile yer alan ASELSAN, Türkiye'de hedeflenen yüksek verimliliğe ulaşılmasında katkı sağlamaktadır.

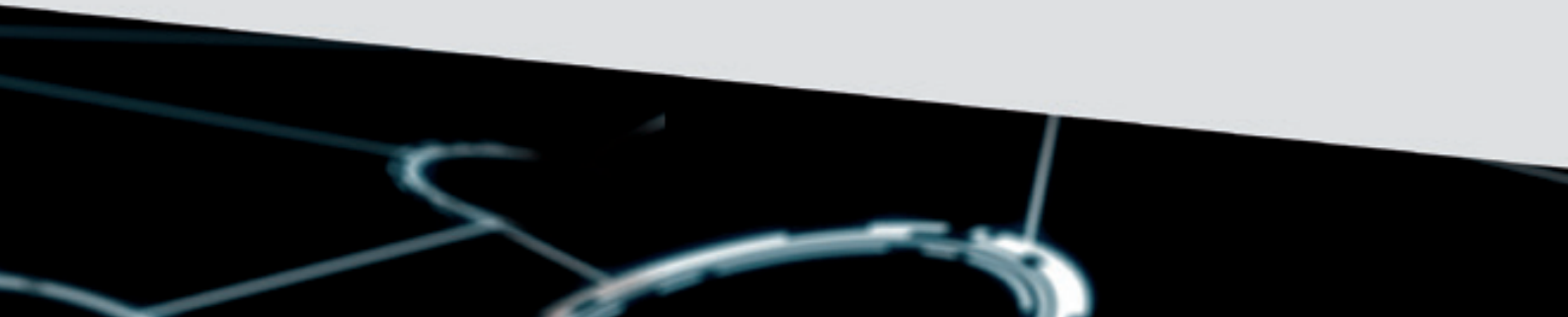


Şekil 3: 2018 Yılında En Fazla Ödenek Ayrılan İlk 10 Bilgi ve İletişim Teknolojileri Projesi[6]

Bilgi teknolojilerindeki gelişmeler dünya devletlerinin arasında küresel teknoloji rekabeti yaratmaktadır. ABD'nin, Çin Halk Cumhuriyetinde bulunan telekomünikasyon firmalarına yaptırımlar getirmesi ve aynı zamanda kritik veri akışı olan yerlerde Çin üretimi olan donanım kullanmaması rekabetin en önemli göstergesidir. Bu ve benzeri durumlar dünyadaki askeri ve ekonomik savaşların artık teknoloji savaşlarına döndüğünü göstermektedir. Türkiye olarak kendi yetişmiş insan kaynaklarımız ile milli ürünlerimizin oluşturulması milli ekonomi, milli güvenlik ve milli kalkınma konularında önem arz etmektedir. Özkaynaklı projeleri ile Türkiye'de öncü bir firma olan ASELSAN, son teknolojileri yakından takip ederek ortaya koyduğu ürünler ve çalışmalar sonucunda Technology Fast 50 Turkey 2019 Big Star Ödülüne layık görülmüştür.

ASELSAN tarafından özkaynakları kullanılarak yerli ve milli imkanlar ile üretilen milli ağ cihazları ailesi özel sektörün, kamu kurumlarının ve kuruluşların ihtiyaçları ile gelişen teknoloji doğrultusunda çalışmalarına devam etmektedir. Bu doğrultuda, güvenli haberleşme altyapısını sağlama hususunda pek çok sistemde imzası bulunan ASELSAN, askeri alanda TASMUS, AZRA (Azerbaycan Radyolink Haberleşme Projesi) ve REHİS Silah Tespit Radarı projelerinde ve bununla birlikte endüstriyel alanda İstanbul Büyükşehir Belediyesi Geniş Alan Telsiz Sistemi, Emniyet Genel Müdürlüğü Sayısal Haberleşme Şebekesi ve KGYS (Kent Güvenlik ve Yönetim Sitemi) projelerinde milli ağ cihazlarını aktif olarak konumlandırmıştır.

Bilgi ve iletişim teknolojileri sektörü her geçen yıl pazar hacmi ve çalışan personel sayısı ile ciddi olarak artış göstermektedir. Bu sektör kapsamında özellikle savunma sanayii, haberleşme, bilgi ve veri güvenliğine ait ürünlerin yerli ve milli olarak geliştirilmesi, üretilmesi ve ihraç edilmesi ülkemizin bu sektörde sahip olduğu konumu koruması ve daha da ileri taşıması amacıyla ciddi öneme sahiptir. ASELSAN, özgün ürün ve sistem tasarımlarıyla bilgi teknolojileri çözümlerini müşteri ihtiyaçları doğrultusunda üretmeye ve geliştirmeye devam etmektedir. Üretim ve tasarım faaliyetleri ile bilgi teknolojileri sektöründe iç pazardaki sürekliliği sağlamakla beraber küresel pazarda da aktif bir rol almayı hedeflemektedir.



Kaynakça

(1) Gartner Says Global IT Spending to Grow 3.7% in 2020. Gartner, 2020, 'www.gartner.com/en/newsroom/press-releases/2019-10-23-gartner-says-global-it-spending-to-grow-3point7-percent-in-2020#:~:text=Worldwide%20IT%20spending%20is%20projected,latest%20forecast%20by%20Gartner%2C%20Inc'.

(2) Bilgi Ve İletişim Teknolojileri Sektörü 2019 Pazar Verileri. 2019, 'www.tubisad.org.tr/tr/images/pdf/tubisad-bit-2019.pdf'.

(3) IDC Directions 2020. IDC, 2020, 'www.idc.com/mea/events/66527-idc-directions-2020'.

(4) BİLGİ & İLETİŞİM TEKNOLOJİLERİ. Bilgi & İletişim Teknolojileri - Invest in Turkey, 2020, 'www.invest.gov.tr/tr/sectors/sayfalar/ict.aspx'.

(5) TUİK, 2019, 'biruni.tuik.gov.tr/medas/?kn=124&locale=tr'.

(6) Kamu BIT Yatırımları 2018. 2019, 'www.bilgitoplumu.gov.tr/wp-content/uploads/2018/06/Kamu_BIT_Yatirimlari_2018.pdf'.

aselsan

GÜNCEL HABERLER


INTERNET
PASSWORD
CODE
DATA
INTERNET
SECURE

ASELSAN'da İstihdam Aynı Hızla Devam Ediyor

ASELSAN, 2020 yılı 0cak ayı itibarıyla 541 kişi daha istihdam ederek toplamda 8.106 kişiye ulaştı. Hedef yıl sonunda 1.300 yeteneği ailesine katmak olacak.

Türkiye'nin en büyük savunma elektroniği kuruluşu olan ASELSAN, haberleşme ve bilgi teknolojileri, radar ve elektronik harp, elektro-optik, aviyonik, insansız sistemler, kara, deniz ve silah sistemleri, hava savunma ve füze sistemleri, komuta kontrol sistemleri, ulaştırma, güvenlik, trafik, otomasyon ve sağlık teknolojilerine yönelik ihtiyaçlarını karşılayabilecek çok geniş bir ürün yelpazesini geliştirmekte ve üretmektedir. ASELSAN, bu gurur dolu yolculuğuna 8.106 ASELSAN'lı ile devam ediyor.

2020 Ocak ayından bu yana 201 mühendis, 307 teknisyen ve 33 uzman ile yollarını birleştiren ASELSAN, güçlü kurum değerlerinin de bir yansıması olarak insan kaynağına her geçen gün daha çok yatırım yapıyor. Bünyesine kattığı mühendis kadrosunun %59'u tasarım ve arge , %12'si program yönetimi alanlarında çalışırken, %29 ise lojistik, üretim, yönetim destek, kalite ve iş geliştirme alanlarında çalışmak üzere imza attılar.

ASELSAN Yönetim Kurulu Başkanı ve Genel Müdürü Prof. Dr. Haluk GÖRGÜN, "Geliştirdiğimiz her ürünümüz çalışanlarımızın hayalinin, emeğinin, tasarımının eseridir. 2020 gibi çok zorlu ve belirsiz bir yılda bile Devletimizin gösterdiği kararlılık ve verdiği güveni referans alarak büyümeye devam ediyoruz. Sürdürülebilir iş planlarımızı kesintisiz bir şekilde uygulamaya devam edebiliyorsak bunu yüreğini ortaya koyarak çalışan kıymetli ASELSAN'lılara atfederim. Ailemize katılan her yeni çalışma arkadaşımızla birlikte, en ileri teknolojiyi en güçlü takım olarak geliştirerek ülkemiz için, milletimiz için, milli menfaatlerimizin en büyük savunucularından biri olmaya devam edeceğiz." diyerek insan kaynaklarına ve kurum kültürüne verdikleri önemi bir kez daha vurguladı.

ASELSAN tüm zorlu koşullara rağmen büyümeye devam edecek. 2019 yılında yaklaşık 1200 yeteneği ailesine katan ASELSAN, 2020 istihdam planlarında herhangi bir değişikliğe gitmeyerek 1300'ün üzerinde yeni çalışma arkadaşına ulaşarak yılı kapatmayı hedefliyor.

Kent Güvenlik Yönetim Sistemi ve Plaka Tanıma Sistemi Projesi Yaygınlaştırılıyor

Emniyet Genel Müdürlüğü ihtiyacına binaen, terörle mücadele, asayiş ve güvenliğe katkı sağlamak amacıyla Türkiye'nin tüm il ve ilçelerinde Kent Güvenlik Yönetim Sistemleri ve Plaka Tanıma Sistemlerinin kurulumları gerçekleştirilmekte ve okullarda güvenli eğitim ortamının tesis edilmesi amacıyla çevre görüntüleme sistemlerinin kurulumları yapılmaktadır. Bununla birlikte milli olarak geliştirilen yazılımlar ile tüm sistemlerin tek bir merkezden yönetilmesi yeteneği Emniyet Genel Müdürlüğü'ne kazandırılmış durumdadır.

Sistemlerin ülke çapında yaygınlaştırılması kapsamında, **Emniyet Genel Müdürlüğü'nün ilave ihtiyaçlarına istinaden ek paketler için tedarik işlemleri Başkanlığımızca gerçekleştirilmekte olup mevcut durumda yaklaşık 44.000 kamera ve 9.000 adet plaka tanıma sistemi Emniyet Genel Müdürlüğü'ne teslim edilmiştir. Ayrıca Türkiye Cumhuriyeti Hükümeti ile Kuzey Kıbrıs Türk Cumhuriyeti Hükümeti arasında imzalanan protokol kapsamında Kuzey Kıbrıs Türk Cumhuriyeti Makamlarınca ihtiyaç bildirilen noktalar için güvenlik sistemleri ve plaka tanıma sistemleri tedarik edilmesi proje kapsamına alınmıştır.**

SSB ile Aselsan arasında imzalanan Ek Talep Paketi-4 kapsamında 1523 adet sabit kamera, 514 adet hareketli kamera ve 11 adet lazer PTZ kamera ile 139 adet Plaka Tanıma Sistemi ve 200 adet Mobil Plaka Tanıma Sistemi tedarik edilecektir. Bununla birlikte KGYS sistemleri üzerinde hatalı park yapan araçların tespitine yönelik ilave yetenekler de sisteme kazandırılacaktır. Sistemlerden alınan verimin artırılması ve Emniyet Genel Müdürlüğü personelinin saha işlerinin kolaylaştırılması kapsamında sahada görevli personel tarafından kullanılabilecek yaka kameraları tasarlanmış olup ihtiyaca yönelik geliştirmeler devam etmektedir. Sözleşmesi imzalanan bu paket ile birlikte, tedarik edilen ürün ailesi akıllı ürün ailelerine dönüştürülmüş olup artık sahada sabotaj tespiti, yönlü çizgi geçişi, yönlü hareket tespiti, şüpheli nesne tespiti, kişi/trafik analizi ve hedef takibi yapabilen kameralar kullanılacaktır.

Proje ile birlikte; yüksek çözünürlüklü kameraların kullanımı ile terör ve güvenlik olaylarının hızlı ve etkin bir şekilde çözümlenmesi, plaka tanıma ve ikiz plaka tespit başarı oranlarının artırılması, tek bir çatı yazılım ile tüm sistemlerin tek bir merkezden yönetilebilmesi konularında önemli kazanımlar edinilmiştir.

Aynı zamanda Kent Güvenlik Yönetim Sistemlerinden elde edilen video görüntülerinden anlamlı sonuçlar çıkaracak ve emniyet güçlerinin olayları daha hızlı çözmelerine katkı sağlayacak video analiz sistemi geliştirilme çalışmaları devam etmekte olup sistemin envantere alınması ile birlikte KGYS sistemlerinin asayiş ve güvenliğe olan katkısının artırılması hedeflenmektedir.

Cumhurbaşkanımız Sayın Recep Tayyip Erdoğan'ın önderliğinde yürütülen 180 Günlük İcraat Programı içerisinde yer almakta olan sistem kurulumları Başkanlığımızca başarı ile sürdürülmektedir.

Savunma Sanayii Başkanlığımız asayiş ve güvenliğe katkı sağlanması amacıyla ihtiyaç bildirilen tüm noktalar için sistem kurulumlarının yapılması, sistemlerin sorunsuz ve yüksek performans ile çalışmasını teminen her türlü tedbirin alınması hususlarında çalışmalarına devam etmektedir.

Jandarma Plaka Tanıma Sistemi Ağı ASELSAN'la Genişliyor

Jandarma Genel Komutanlığı ihtiyacı olan Plaka Tanıma Sistemleri, ASELSAN A.Ş. ile Savunma Sanayii Başkanlığı arasında 30 Mart 2020 tarihinde imzalanan Jandarma Entegre Muhabere ve Bilgi Sistemi (JEMUS) 5-İl Projesi kapsamında Ulaşım, Güvenlik, Enerji, Otomasyon ve Sağlık Sistemleri (UGES) Sektör Başkanlığı tarafından teslim edilecek.

İmzalanan sözleşme ile Jandarma Plaka Tanıma sistemleri ağına, 100 noktada 650 adet Sabit Plaka Tanıma Sistemi (S-PTS) ve 100 adet Mobil Plaka Tanıma Sistemi (M-PTS) ilave edilecektir.

JEMUS-3 projesinden beri Jandarma Genel Komutanlığı ile beraber çalışan ASELSAN, bugüne kadar Türkiye'de 70 ilde 321 noktaya sabit PTS ve 81 ilde 364 adet mobil PTS teslim etti. Yeni gelecek sistemler ile mevcut ağın genişlemesi, iller arası araç geçişlerin denetim altına alınması hedefleniyor.

Tek kameralı, yüksek çözünürlüklü plaka tanıma sistemlerinin, yapay zekâ algoritmalarının ve büyük veri analizlerinin kullanılacağı bu yeni sözleşme ile mevcut Jandarma Plaka Tanıma sistemleri ağı bir sonraki versiyona geçerek, asayiş, trafik, kaçakçılık ve organize şubelerine daha efektif karar destek bulguları sunacak. Geliştirilen merkezi yazılım ile Jandarma Envanterine UGES Güvenlik yazılımı olan MIRSAD yazılımı dâhil edilecek.

Teslimatların 2023 yılına kadar tamamlanması hedefleniyor.

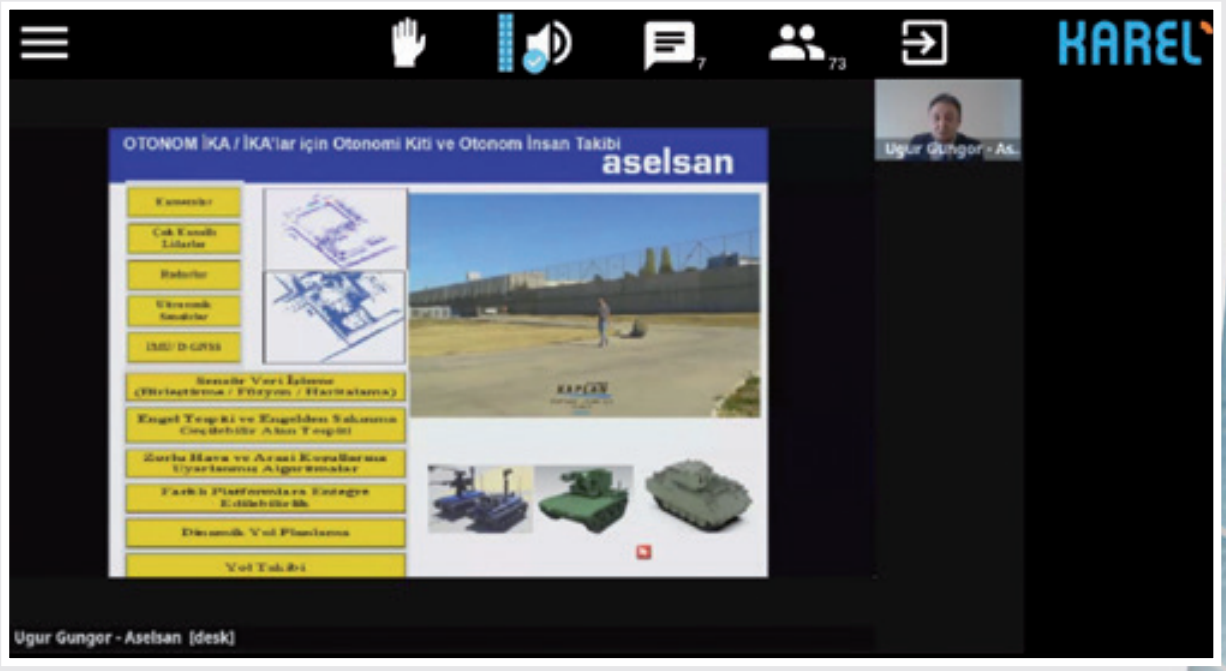
Sürü Zekası Odak Teknoloji Ağı Lansmanı

Sürü Zekası Odak Teknoloji Ağı Lansmanı, Savunma Sanayii Başkanlığı (SSB) AR-GE ve Teknoloji Yönetimi Daire Başkanlığı tarafından yapıldı.

İhtiyaç makamları, birçok kurum ve akademisyenin katıldığı çalışmada, ASELSAN lider kurum olarak görevlendirildi.

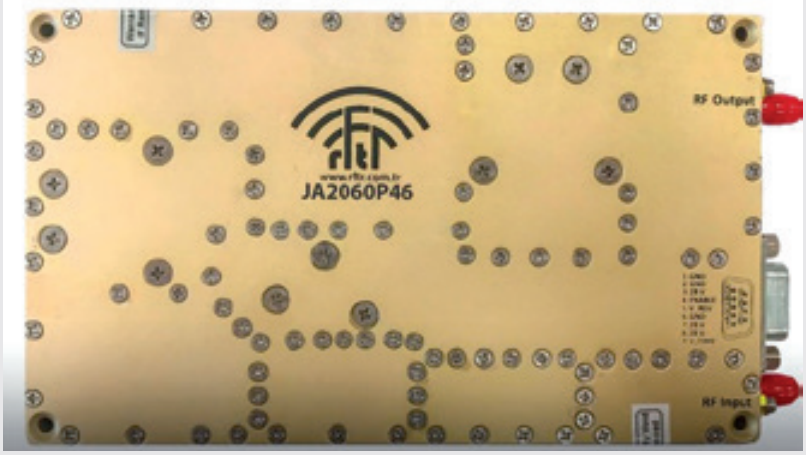
Savunma Sanayii Başkan Yardımcısı Dr. Celal Sami Tüfekçi'nin açılış konuşması ile başlayan lansmanda, SSB Bilgi Teknolojileri Müdürü Ahmet Bahadır Bülbül ve ASELSAN İnsansız Sistemler Sistem Mühendisliği Müdürü Uğur Güngör sunumlarını gerçekleştirdi.

2020 yılı boyunca sürecek olan çalışma kapsamında, Sürü Zekası Teknolojisi alanında savunma sanayii yol haritasının oluşturulması hedefleniyor.



Milli ve Yerli Malzeme

ASELSAN ürünlerinde kullanılan malzemelerin, milli ve yerli olarak yurt içinde üretilmesine yönelik faaliyetlerimiz devam ediyor. Yurt dışından alınan 2.5-6 GHZ_30W, 2-6 GHZ_ 45W, 500-2500 MHz_120W ve 2.5-6GHz_20W Güç Yükselteç tanımlı ürünler, RFTR Elektronik A.Ş. üzerinden yerlileştirildi.



ASELSAN Orta Asya'daki Faaliyetlerini Artırıyor

Faaliyet yürüttüğü pazarlarda yerelleşme çalışmalarını da hızla sürdüren ASELSAN, Kazakistan'ın ihtiyacı kapsamında SARP DUAL uzaktan komutalı silah sistemine yönelik yeni bir sözleşme imzaladı.

ASELSAN'ın, çeşitli kara ve deniz platformlarında kullanılabilen farklı konfigürasyon ve kalibrelerde geliştirdiği uzaktan komutalı silah sistemleri halen 20 farklı ülkenin envanterinde yer alıyor.

ASELSAN ve Kazakistan'daki iştiraki Kazakhstan ASELSAN Engineering (KAE), Kazakistan'ın askeri ve sivil alanlardaki ihtiyaçlarını azami düzeyde karşılayabilmek için üretim kapasitelerini artırmayı hedefliyor.

Ürünler Millileştirildi, Kaynaklar Türkiye'de Kaldı

ASELSAN'ın ürün yelpazesinde kullanılan malzemelerdeki dışa bağımlılığı azaltmak, tedarik sürecinde zorluklar yaşanan ürünleri milli/yerli olarak üretmek, tedarik maliyetlerini ve sürelerini düşürmek, teknolojik yetkinlik kazanmak amacıyla 2018 başında kurulan Milli ve Yerli Ürün Geliştirme Kurulu bünyesinde millileştirme çalışmalarına hız verildi.

Sektör Başkanlıkları, Teknoloji ve Strateji Yönetimi Genel Müdür Yardımcılığı ve Sanayileşme ve Tedarik Direktörlüğü temsilcilerinden oluşan kurul, ithal edilen tüm ürünleri gözden geçirerek, teknolojinin önemi, ihraç kısıtları, maliyet etkisi ve temin süresi gibi kriterleri göz önüne alarak öncelikle milli ve yerli olarak temin edilmesi gereken ürünleri belirliyor.

Kurul bünyesinde bugüne kadar yaklaşık 20 bin ürün için detaylı inceleme ve çalışma başlatıldı. İlk aşamada 300 ürünün yerli olanaklarla geliştirilmesi ve üretimi kararlaştırılırken, daha sonra bu sayı 450'ye yükseltildi.

Kurul nezdinde öncelikle millileştirilmesi uygun görülen malzemeler için hazırlanan broşürler, birçok yeteneğe aynı anda ulaşılmasını sağlayan ve karmaşık savunma projelerine çözüm üretebilecek yetkin firmaların bir arada bulunduğu savunma sanayisi kümeleri, organize sanayi bölgeleri ile portföyünde farklı yetkinliklerde birçok firma barındıran sanayi ve ticaret odalarının bilgisine sunuluyor.

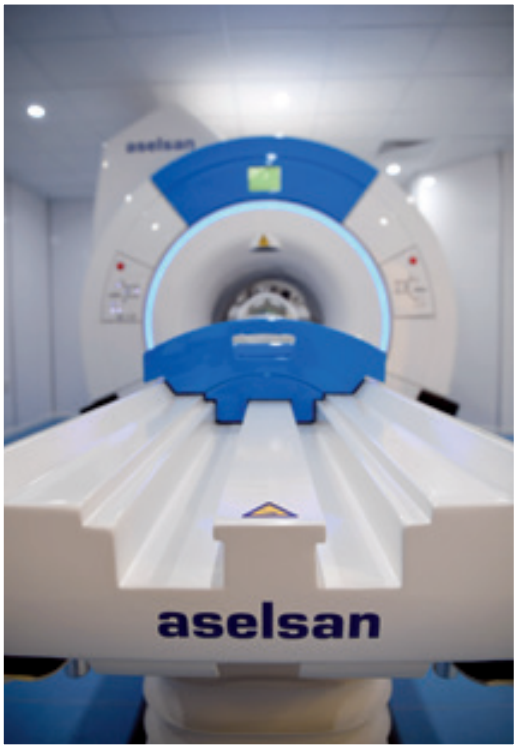
Ürünler millileşti, yenileri yolda

Bu kapsamda 350-400 ürün karşılığı yayınlanan 100'ün üzerinde broşür için son 1-1,5 yılda yaklaşık 400 başvuru alındı. Şu anda 100'e yakın ürün için görüşmeler ve üretim süreci devam ediyor. 10 ürün için de doğrulama ve onay aşaması sürüyor.

Bugüne kadar 17 firma ile 29 farklı ürün gamının millileştirilmesi kapsamında çalışmalar tamamlanarak 24 ürün için yurt içi siparişler açıldı. Gelecek 3 yıllık alım öngörülerine göre millileştirilen 24 ürün özelinde yurt dışından yurt içine döndürülen tutar 25 milyon dolar seviyesine ulaştı.

ASELSAN, millileştirme çalışmalarını kurum ihtiyaçları, savunma sanayisi projelerinin gereksinimleri ve ülke menfaatlerini ön planda tutarak sürdürecek.

İlk Yerli MR Cihazı Çalışması Sürüyor



Cumhurbaşkanlığı Savunma Sanayii Başkanı Prof. Dr. İsmail Demir, ASELSAN ve Bilkent UMRAM tarafından prototipi geliştirilen ilk yerli MR cihazını inceledi. Savunma sanayiinin sağlık sektörüne katkılarına ilişkin açıklama yapan Demir, "ASELSAN bu MR cihazının yanında suni solunum cihazı, kalp-akciğer pompası, mobil X-Ray cihazı ve taşınabilir defibrilatör üzerinde çalışmalarını sürdürüyor. Ayrıca savunma sanayii olarak hasta bakımı, tanı kiti, veri ve görüntü işleme üzerine ARGE çalışmalarımız devam ediyor" şeklinde konuştu.

Cumhurbaşkanlığı Savunma Sanayii Başkanı Prof. Dr. İsmail Demir, beraberinde ASELSAN Yönetim Kurulu Başkanı ve Genel Müdürü Haluk Görgün ile Bilkent Üniversitesi UMRAM'ı (Ulusal Manyetik Rezonans Araştırma Merkezi) ziyaret etti. Bilkent Üniversitesi Rektörü Prof. Dr. Abdullah Ataları'ın da bulunduğu ziyarette, yapılan çalışmalar hakkında bilgi alan Başkan Demir, ASELSAN ve Bilkent UMRAM'ın birlikte ilk prototipini geliştirdiği yerli MR cihazını inceledi.

SSB Başkanı Demir, ziyareti ve savunma sanayiinin sağlık teknolojilerine yönelik çalışmaları hakkında bir açıklamada bulundu. Demir açıklamasında şunları söyledi:

"Savunma sanayiinde geliştirilen teknolojilerin çoklu kullanımı açısından çeşitli projelerimiz devam etmekteydi. Bugünlerde gündem olan pandemi ile beraber sağlık sektöründeki çalışmalar öne çıkmış durumda. Bunun ilk örneği de solunum cihazının gündeme gelmesi oldu. Sanayi ve Teknoloji Bakanlığımızın da öncülüğüyle yapılan girişimle, bir KOBİ şirketimizle iki büyük savunma sanayii şirketimiz bir araya gelerek bir solunum cihazı ürettiler ve bunun başarısı şu anda görülüyor. Ama çalışmalar sadece bundan ibaret değil."

"ASELSAN'ın zaten çalışmakta olduğu 5 adet daha cihaz vardı. ASELSAN bu MR cihazının yanında suni solunum cihazı, kalp-akciğer pompası, mobil X-Ray cihazı, ve taşınabilir defibrilatör üzerinde çalışmalarını sürdürüyor. Yine Başkanlığımız bünyesinde ultraviyole dezenfektan konularında, hem maske hem diğer ürünlerin geliştirilmesi konusunda çalışmalar hızla devam ediyor."

“Bunun yanında AR-GE başlığı olarak savunma sanayiinin tetiklediği birkaç başlık daha var. Bunların başında hasta bakımı ve monitör edilmesi ile ilgili teknolojilerin geliştirildiği çalışmalarımız var. Yine hasta tanı ve veri kiti oluşturmayla ilgili çalışma var. Diğer taraftan veri işleme, görüntü işleme, bunların akıllı sistemlerle, derin öğrenmeyle geliştirilecek yöntemlerle yaklaşımların ortaya çıkarıldığı teknolojiler var. Bunların çoklu olarak devam ettirildiğini söylemek mümkün.

“Çünkü burada uygulanan teknolojiler aynı zamanda savunma sanayiinde geliştirilen bazı temel teknolojilerin uygulanmasını içerdiği gibi geliştirilen teknolojilerin savunmaya doğrudan etkileri de var. Gerek savunma alanında askerlerimizin, güvenlik güçlerimizin sorunları gerekse öğrenilen elektronik, veri işleme, görüntü işleme ve programlama teknikleriyle ilgili sağlık sektöründe ortak çalışmanın oluşturulacağı bir alan görmüş durumdayız. Sağlık bu çoklu kullanım alanlarının başlangıcı olarak düşünülebilir ve şu anda gündeme gelmesi hasebiyle kamuoyunun gündemine taşınan konular. Ancak bunun yanında enerji, çeşitli hassas tesis ve sistem koruma çalışmaları, çeşitli dağıtım sistemlerinin monitör edilmesi ve otomatik kontrolünün sağlanması, iletişim sistemleri ve buna ilaveten oluşacak siber güvenlik alanı, iletişim alanı, çeşitli alanlarda oluşan teknolojilerin çoklu kullanımı ile ilgili de devletin de çeşitli birimleriyle temas halinde çalışmalarımız devam ediyor.

“Sağlık konusunda bu beş ürünle yola çıkan ASELSAN’ın yanında gerek yazılım sistemleri gerek çeşitli veri işleme ve görüntü işleme sitemleriyle ilgili diğer şirketlerimizle çalışmalarının sonuçlarını yakında görmüş olacağız. Burada mühim olan bir Millî Teknoloji Hamlesi konusunun ülkenin gündeminde daha sıcak tutulması ve ülkede geliştirilen her alandaki teknolojilerin çoklu kullanımının ve hızlı bir yol almanın sağlanması olarak görüyoruz. İnşallah bunu savunma sanayii olduğu gibi diğer sanayi alanları ile de yakın işbirliği ile sürdüreceğiz.”

“Bunun temel unsurlarından birisi de aslında bilim ve teknolojiyi buluşturmak, bir arada yürütmek ve bunu uygulamaya geçirmek. Bunun da tabii yuvası malumunuz araştırma kurumları, üniversiteler. Şu anda çatısı altında bulunduğumuz Bilkent Üniversitesi UMRAM ve çeşitli araştırma merkezleri de yine yakından işbirliği yaptığımız yapılar arasında. Çeşitli üniversitelerle bu anlamda çalışmalarımız da sürmekte. Yani bilgi ve teknoloji gelecek. Biz bu geleceği gençlerimizle beraber yatırım yapmaya devam ediyoruz. Savunma sanayii de inşallah bunun öncülüğünü yapmaya devam edecek.”

Mehmetçiğe Robot Yardımcı

Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (SSB) ve ASELSAN arasında Orta Sınıf 2. Seviye İnsansız Kara Aracı Projesi Sözleşmesi imzalandı.

Cumhurbaşkanlığı Savunma Sanayii Başkanı Prof. Dr. İsmail Demir: "Mehmetçiğe robot yardımcılar geliyor! Hafif ve orta sınıf 1.seviye insansız kara araçları prototiplerinden sonra orta sınıf 2.seviye için Aselsan ile sözleşme imzaladık. Katmerciler'in de platform üreticisi olacağı projeyle silahlı insansız kara araçları KKK'ya teslim edilecek.

İnsansız Sistemlerin savunma ve güvenlik alanındaki yeri gün geçtikçe artıyor. Özellikle asimetrik savaş koşullarında, keşif-gözetleme-istihbarat, savunma, lojistik destek ve benzeri faaliyetleri hızlı ve etkin bir şekilde ve personel kaybı vermeden yürütmek üzere kara, deniz veya havada çalışabilen ve kendi kendine karar verebilen insansız sistemlere ihtiyaç duyuluyor.

ASELSAN geleceğin savaş alanlarında yaygın bir şekilde kullanılacak olan;

- Uzaktan kontrol edilebilen,
- Kendi başına karar verme ve uygulama yeteneğine sahip,
- Her türlü koşulda görev yapabilen, değişik boyutlara sahip

İnsansız Sistemlerin geliştirilmesi ve üretilmesine yönelik çalışmalarına devam ediyor.

Bu amaç doğrultusunda bu alandaki kritik yapı taşlarını oluşturan, otonomi, insansız sistemlerin silahlandırılması, birden fazla insansız sistemin koordinasyonu ve komuta kontrol sistemlerine entegrasyonu konularında bilgi ve tecrübe biriktirmek üzere konsept platformları geliştirildi. ASELSAN, 14 yıl önce gerçekleştirilen IDEF 2007 Uluslar arası Savunma Fuarında ilk insansız kara aracı olan İZCİ'yi ve hemen ardından GEZGİN'i tanıttı. ASELSAN, yıllar içinde insansız sistemler alanındaki teknolojik altyapısını mükemmelleştirdi ve yerli/yabancı platform üreticileri ile ortaklıklar geliştirdi.

ASELSAN, TSK'nın envanterine insansız sistemler alanında duyacağı ihtiyaçlara cevap verecek milli ve yüksek teknolojiye sahip benzer ürünler kazandırdı. Güvenlik Kuvvetlerimizin envanterinde ASELSAN ürünü insansız hava, deniz ve kara araçları (Bomba İmha Robotları) uzun yıllardır görev yapıyor.

TSK ÇBSMT Kara Kuvvetleri Komutanlığı Telsiz Teslimatları

Türk Silahlı Kuvvetleri (TSK) Çok Bantlı Sayısal Müşterek Telsiz (ÇBSMT) Projesi kapsamında geliştirilen **Milli Kriptolu, Elektronik Harp Korumalı, Yazılım Tabanlı** araç, sırt ve sabit merkez telsizinin fabrika kabul testleri, Savunma Sanayii Başkanlığı ve Kara Kuvvetleri Komutanlığı katılımı ile tamamlandı.
Gerçekleştirilen teslimat ile Kara Kuvvetleri Komutanlığının taktik sahada ihtiyaç duyduğu 9661 V/UHF ve 9661 HF yazılımlı tabanlı telsizler TSK envanterine kazandırıldı.

Emniyet Genel Müdürlüğü Kriptolu Sayısal Telsiz Ağını Yeni Teknolojiler ile Genişletiyoruz

Sayısal Haberleşme Şebekesi Projesi Ankara ve İstanbul illerinden sonra Adana ve İzmir illerinde de boy göstermeye başladı.

Savunma Sanayii Başkanlığı ile ASELSAN arasında Emniyet Genel Müdürlüğü'nün kullanımı için 22.04.2020 tarihinde **Sayısal Haberleşme Şebekesi (Adana ve İzmir, DMR + LTE) Projesi (Kamu Güvenliği ve Acil Haberleşme Sistemi) Sözleşmesi** imzalandı. Proje kapsamında İzmir İl Emniyet Müdürlüğü için DMR Sisteminin, Adana İl Emniyet Müdürlüğü için ise DMR + LTE Kamu Güvenliği ve Acil Haberleşme Sistemlerinin kurulumu yapılacak.

Adana ve İzmir illeri ile birlikte Emniyet Genel Müdürlüğü için toplamda 26 ilde Kriptolu Milli DMR Sayısal Telsiz Sistemi kurulumu tamamlanmış olacak. Adana'da DMR + LTE Kamu Güvenliği ve Acil Haberleşme Sistemlerinin kurulması ile birlikte, Türkiye'de ilk defa bir Kamu Güvenliği Haberleşme Projesinde Dar Bant + Geniş-Bant Hibrit sistem kurulumu gerçekleştirilmiş olacak. Ayrıca, projede Adana İli için tasarımı ve üretimi tamamen ASELSAN öz kaynakları ile gerçekleştirilecek olan 3810 Hibrit El Terminali teslimatı da yapılacak. Teslimatların 2021-2023 yılları içerisinde tamamlanması planlanıyor.

Adana İl Sistemi pilot sistem olacak, Dar Bant + Geniş-Bant Hibrit sistemin tüm illere yaygınlaştırılması için yol haritası belirlenecek.

Kurulacak Dar Bant + Geniş Bant Hibrit Sistem ile terör, kriz ve doğal afet durumlarında muhabere kesintisiz yapılabilecek, olaya müdahale süresi azaltılarak hızlı, güvenilir, esnek, mobil ve ekonomik haberleşme yapılabilecek ve geniş-bant video ile görüntülü olay yeri takip ve müdahale etkinliği artırılacak.

X-BANT Görev Yükü Fabrika Kabul Testleri

Türk Silahlı Kuvvetleri (TSK) X-Bant Uydu Haberleşme Sistemi (TUMSİS) Projesi kapsamında geliştirilen ve TÜRKSAT-6A uydusunda kullanılacak X-Bant Görev Yükünün fabrika kabul testleri tamamlandı.

Başarı ile sonuçlanan testlere ait doküman ve sertifikasyon işlemlerinin tamamlanması, Savunma Sanayii Başkanlığı/TSK ile doküman incelemelerinin sonlandırılması ve yapılan toplantı ile X-Bant Görev Yükü kabulü tamamlandı.

Sağlık tedbirlerinin çok önem taşıdığı bu günlerde, emeği geçen tüm çalışma arkadaşlarımıza teşekkür ederiz.

ASELSAN İhracat İvmesini Koruyor

ASELSAN, Bahreyn Krallığı'nın deniz platformu kullanımına yönelik olarak, uzaktan komutalı silah sistemlerinin ihracatına ilişkin yeni bir satış sözleşmesi daha imzaladı.

2019 yılında yakalamış olduğu satış ve üretim rekoruna ilişkin performansını 2020 yılında da sürdürmeyi hedefleyen ASELSAN, Körfez ülkelerine gerçekleştirdiği son uzaktan komutalı silah sistemi ihracatının yanı sıra, 10 yıldan fazla süredir Körfez pazarında varlık göstererek; bölge ülkelerine doğrudan satış, teknoloji transferi programları, yerel üretim ve ortak girişim şirketleri aracılığıyla savunma ve teknoloji çözümleri sunuyor.

Körfez İş Birliği Konseyi üyesi ülkelere ve özellikle Bahreyn Krallığı'na yönelik olarak önümüzdeki dönemde yatırım ve iş birliği alanlarını geliştirmeyi hedefleyen ASELSAN, sürdürülebilir büyüme stratejisinin bir sonucu olarak, çeşitli kara ve deniz platformlarında kullanılabilen farklı konfigürasyonlarda geliştirdiği uzaktan komutalı silah sistemlerini 20 farklı ülkenin kullanımına başarıyla sundu.

45’inci Olağan Genel Kurul Toplantısı

ASELSAN 45’nci Olağan Genel Kurul Toplantısı, 19 Haziran 2020 Cuma günü Akyurt tesislerinde, Savunma Sanayii Başkanı Prof. Dr. İsmail Demir’in başkanlığında, Yönetim Kurulu Üyeleri ve pay sahiplerinin katılımıyla, tüm sağlık önlemleri gözetilerek gerçekleştirildi.

ASELSAN Yönetim Kurulu Başkanı ve Genel Müdürü Prof. Dr. Haluk Görgün’ün açılış konuşması ile başlayan 45’nci Olağan Genel Kurul Toplantısında aşağıdaki kararlar alındı:

2019 yılı hesap dönemine ait finansal tabloları onaylandı.

Yönetim Kurulu Üyelerinin, 2019 yılı hesap dönemine ait faaliyetlerinden ve hesaplarından dolayı ibra edilmeleri onaylandı.

2019 yılı hesap dönemine ait kârın kullanım şeklinin ve dağıtılacak kâr payı oranına ilişkin olarak; 2019 yılı faaliyetlerinden elde edilmiş net dönem kârından; brüt 335.000.000,- TL'lik (1 TL'lik pay başına 29,38596 Kuruş) kısmının, (net 284.750.000,- TL'nin, 1 TL'lik pay başına 24,97807 Kuruş) nakit kâr payı olarak ve çıkarılmış sermaye üzerinden %100 oranına tekabül eden 1.140.000.000,- TL'lik kâr payının ise bedelsiz pay olarak ortaklara dağıtılmasına ve pay sahiplerine dağıtılacak nakit kâr payının 17 Temmuz 2020, 16 Ekim 2020 ve 18 Aralık 2020 tarihlerinde olmak üzere 3 eşit taksitte, bedelsiz payların ise yasal sürecin tamamlanmasını takiben dağıtılması hususunda karar verildi.

Görev süresi dolan Yönetim Kurulu Üyelerinin ve Bağımsız Yönetim Kurulu Üyelerinin seçimi ve görev sürelerinin tespiti ile ilgili olarak; Prof. Dr. Haluk Görgün, Dr. Celal Sami Tüfekci, Yavuz Çelik, Mehmet Fatih Kacır, Alpaslan Kavaklıoğlu ve Salih Kul'un bir sonraki olağan genel kurul toplantısına kadar görev yapmak üzere gerçek kişi olarak Yönetim Kurulu Üyeliğine seçilmelerine karar verildi. Bağımsız Yönetim Kurulu üyesi olarak ise Prof. Dr. Ercümend Arvas, Prof. Dr. Turan Erol ve Prof. Dr. İbrahim Özkol'un seçilmelerine karar verildi.

Yönetim Kurulu Üyelerine, 2020 yılı faaliyetlerinin görüşüleceği 2021 yılındaki Olağan Genel Kurul Toplantısına kadar aylık net 4.000,-TL (Dört Bin Türk Lirası) ücret ödenmesine karar verildi.

2020 yılı faaliyet döneminde bağımsız denetimini yapmak üzere, Bağımsız Dış Denetim Şirketi olarak Yeditepe Bağımsız Denetim ve Yeminli Mali Müşavirlik A.Ş. seçildi.

2020 yılı hesap döneminde yapılacak bağış ve yardımların üst limiti 15.000.000 TL olarak belirlendi.

2020 yılı hesap döneminde yapılacak sponsorlukların üst limiti 9.000.000 TL olarak belirlendi.

ASELSAN Bir Kez Daha İklim Lideri


CDP
DISCLOSURE INSIGHT ACTION

CDP TURKEY 2019 CLIMATE LEADERSHIP AWARD

is hereby granted to the

ASELSAN ELEKTRONİK SANAYİ VE TİCARET A.Ş.

Paul Dickinson (Executive Chairman)
24 March 2020

ASELSAN, dünyanın en güvenilir derecelendirme metodolojisine sahip çevre projesi CDP'de (Carbon Disclosure Project) bir kez daha İklim Lideri ödülü aldı.

ASELSAN, 2019 Yılı CDP Türkiye raporlamasında İklim Değişikliği başlığı altında cevap veren 54 firma arasında A- puan seviyesinde yer alan ve İklim Lideri ödülü almaya hak kazanan beş firmadan biri oldu.

ASELSAN, dünyadaki önemli savunma sanayi liderlerinin Karbon Saydamlık Projesi (Carbon Disclosure Project – CDP) skorunu bir alt seviyeye düşürdüğü 2019 yılında, ilk defa 2018 yılında yer aldığı A- puan seviyesindeki yerini koruyarak sürdürülebilir bir çevreye verdiği önemi bir kere daha göstermiş oldu.

2019 Yılı CDP Türkiye İklim Lideri ödülleri, COVID-19 salgını nedeniyle online webinar şeklinde düzenlenen ödül töreniyle 9 Haziran 2020 tarihinde sahiplerini buldu. İlk olarak 2010 yılında gerçekleştirilen CDP Türkiye raporlaması, şirketlere sera gazı emisyonlarını şeffaf bir şekilde raporlama ve iklim stratejilerinde performans iyileştirmesi yapma imkânı veriyor. Tüm dünyada marka değeri, yatırımcı ilişkileri çalışmaları ve sürdürülebilirlik raporu için önem arz eden CDP raporuna, gönüllü olarak Türkiye'den BİST-100 şirketleri ve diğer firmalar katılım sağlıyor.

2012 yılında yaptığı ilk raporlama ile CDP Türkiye Programına dahil olan ve her yıl başarısını artırarak üst üste iki yıl İklim Lideri ödülü alan ASELSAN, çevreyi gelecek nesillere aktarılacak bir emanet olarak görme taahhüdü doğrultusunda, iklim değişikliği konusunda çözüm olabilecek yenilenebilir enerji sistemleri, ulaşım sistemleri, akıllı şebeke sistemleri gibi Ar-Ge ve üretim faaliyetlerini, sürdürülebilir büyümenin bilincinde olarak yürütmek için çaba sarf etmeye devam ediyor.

Savunma Sanayii Başkanlığı ve ASELSAN arasında imzalanan 35 mm Hava Savunma Sistemi ve Parçacıklı Mühimmat Tedariki Projesi Kapsamında

AİC ve MÇT Sistemlerinin İlk Kafile Teslimatı

Ateş İdare Cihazı (AİC) ve Modernize Çekili Top (MÇT) sistemlerinin ilk kafile kabulü kapsamında bir adet AİC ve iki adet MÇT için kabul testleri 29 Mayıs 2020 tarihinde başarı ile tamamlandı. Sistemler 01 Haziran 2020 tarihinde kullanıcı birliğine teslim edildi.

AİC ve MÇT sistemleri kabul testleri süresince fabrika testlerinin yanı sıra helikopter ve F-16 uçuşunu içeren testler ve hedef uçağa karşı yapılan atışlı testler ile yeteneklerini tekrar kanıtladılar.

AİC takımı, kritik tesisler ile sabit askeri birliklerin hava savunmasının etkin şekilde gerçekleştirilmesi amacıyla en güncel teknolojiye dayalı bir alçak irtifa hava savunma çözümü sunmaktadır. AİC sistemi aynı anda üç adete kadar Modernize Çekili Topun (MÇT) yanı sıra bir adet HİSAR-A Füze Fırlatma Sisteminin (FFS) kontrolünü üstlenebilmektedir. Tipik AİC takımı, bir adet AİC, iki adet 35mm MÇT ve bir adet Alçak İrtifa Hava Savunma Füze Fırlatma Sisteminden (HİSAR-A FFS) oluşmaktadır.

2020 Verimlilik Yılında MGEO Kalibrasyon Laboratuvarı Hizmetlerini Artırıyor

Mikroelektronik Güdüm ve Elektro-Optik (MGEO) Sektör Başkanlığı Kalite Yönetim Direktörlüğü, 2020 verimlilik yılı uygulamaları kapsamında, Ulaşım, Güvenlik, Enerji, Otomasyon ve Sağlık Sistemleri (UGES) ve Savunma Sistem Teknolojileri (SST) Sektör Başkanlıklarına kalibrasyon hizmeti vermeye başladı.

ISO 17025 standardına akredite olan MGEO Ölçüm ve Kalibrasyon Laboratuvarında yapılan kalibrasyonlar daha önce dışarıdan alınan hizmete kıyasla çok daha kısa sürede gerçekleştirildi.

Laboratuvarımızın diğer sektör başkanlıklarına vermiş olduğu hizmetlerin yaygınlaştırılarak sürdürülmesi hedefleniyor.

aselsan
MGEO
Ölçüm ve Kalibrasyon Laboratuvarı

ASELSAN ELEKTRONİK SAN. VE TİC. A.Ş.
MİKROELEKTRONİK, GÜDÜM VE ELEKTRO-OPTİK
SEKTÖR BAŞKANLIĞI
ÖLÇÜM VE KALİBRASYON LABORATUVARI

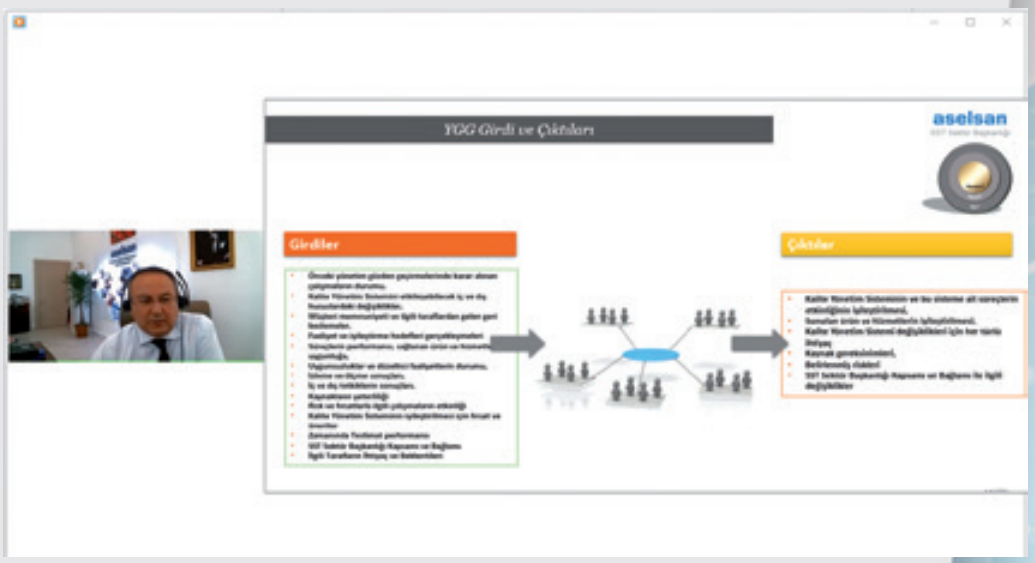
Kalibrasyon Sertifikası
Calibration Certificate

İmalatçı *Manufacturer*	: Mitutoyo	Dosya No *Folder No*	: UG-1
Model *Model*	: 500-181-30	Talep Eden *Issued For*	: UGES
Seri No *Serial Number*	: 15111027	Adres *Adress*	: Mehmet Akif Ersoy Mah. 296.Cad. No:16 Yenimahalle/ ANKARA
Tanım *Description*	: Sayısal Kumpas	Ölçüm Lab.'a Kabul Tarihi *Calibration Item Receipt Date*	: 06.03.2020
Opsiyonlar *Options*	: -	Kalibrasyon Tarihi *Date of Calibration*	: 10.03.2020
Teknik Detaylar *Technical Details*	: 150mm	Toplam Sayfa Sayısı *Total Number of Pages*	: 4

Kalibrasyonu Yapan *Performed By*	Kontrol Eden *Checked By*	Onaylayan *Approved By*	Mühür *Seal*
İsim-Unvan-İmza	İsim-Unvan-İmza	İsim-Unvan-İmza	
Emre AKKAYA Uzman Teknisyen	Barış UMUL Uzman Mühendis	Nurettin BAKMAZOĞLU Lider Mühendis	
		Sertifika Onay ve Yayın Tarihi 11 Mart 2020	

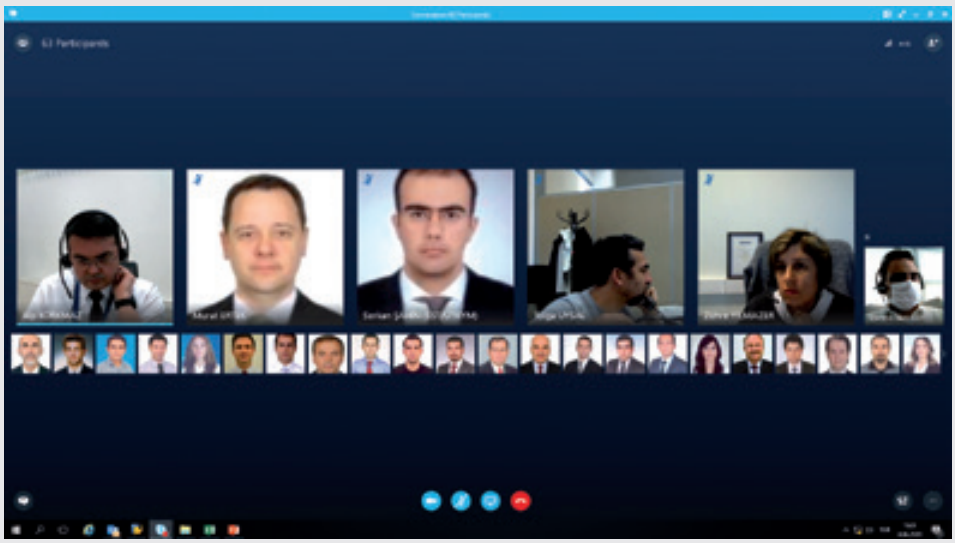
MG-2952 G

SST Sektör Başkanlığı Kalite Yönetim Sistemi Yönetim Gözden Geçirme Toplantısı



05 Mart 2020 tarihinde Yönetim Kurulu Başkanı ve Genel Müdür Prof. Dr. Haluk Görgün ve Kurumsal Yönetim Genel Müdür Yardımcısı Doç. Dr. Hakan Karataş'ın da katılımları ile gerçekleştirilen Savunma Sistem Teknolojileri (SST) Yönetim Gözden Geçirme Toplantısının devamı niteliğinde olan Kalite Yönetim Sistemi Yönetim Gözden Geçirme Toplantısı, 04-05 Haziran 2020 tarihlerinde Sektör Başkanı Mustafa Kaval'ın başkanlığında, iki oturum halinde gerçekleştirildi.

SST Kalite Yönetim Direktörü Alp Korkmaz'ın açılış konuşması ile başlayan toplantıda; ISO 9001, AS9100, AQAP 2110, AQAP 2210 standartlarının gereği olan girdiler temelinde sunumlar gerçekleştirildi. Toplantı, COVID 19 salgını nedeni ile kurum için video konferans sistemi üzerinden gerçekleştirildi.



SST yöneticileri, süreç sahipleri ve proje yöneticilerinin yer aldığı ilk oturuma 93 kişi; SST yöneticilerinin yer aldığı ikinci oturuma ise 63 kişi katılım sağladı.

Sunumlar "hatasız, en düşük maliyetle ve en hızlı tasarım, üretim ve lojistik destek ile müşteri memnuniyeti sağlamak" amacı doğrultusunda kurgulanan girdiler çerçevesinde gerçekleştirildi ve SST Yönetim Sistemini bu amaca taşıyacak kararlar toplantı çıktısı olarak tanımlandı.

SST'de Görünür Liderlik

"İş sağlığı ve güvenliği hedefleri doğrultusunda,
Üst yönetimin liderliği ve çalışanların katılımı ile
yönetim sistemi performansının sürekliliğini sağlamayı taahhüt ederiz."

ASELSAN Entegre Yönetim Sistemleri Politikası

Çalışmalarını ISO 45001 standardının gerekliliklerine ve yasal şartlara uygun olarak sürekli iyileştirme prensibi ile yürüten ASELSAN; ilgili tarafların ihtiyaç ve beklentilerini dikkate alan, tüm çalışanların uygulama ve gelişimine katkı sağladığı, üst yönetimin liderliğinde güçlü bir iş sağlığı ve güvenliği kültürü oluşturmayı hedefliyor.

Bu hedeften yola çıkılarak, Savunma Sistem Teknolojileri (SST) Sektör Başkanı ve Genel Müdür Yardımcısı Mustafa Kaval'ın katılımıyla Görünür Liderlik Etkinliği gerçekleştirildi. Saha turu sırasında Kaval'a iş güvenliği ve çevre uygulamaları konusunda detaylı bilgi verildi ve kendisinin görüşleri alındı.

İş güvenliği ilkelerinin uygulanmasında büyük bir özen gösteren, sürdürülebilir ve değer katan bir sistem oluşturmak için katkı sağlayan tüm SST Sektör Başkanlığı çalışanlarına teşekkür ederiz.

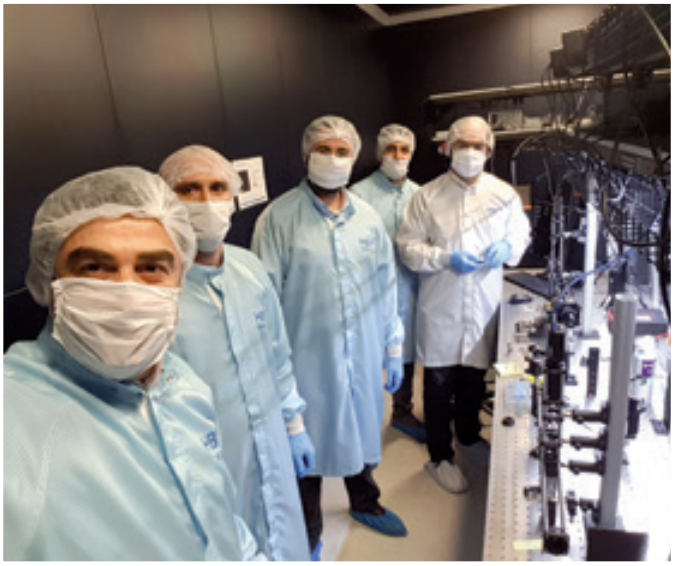
Ailemiz “A-Yetenek”lerle Büyüyor

Mayıs ayında gerçekleşen A Yetenek Programı kapanış süreci kapsamında toplam 202 adayımız, projelerine ve ASELSAN deneyimlerine ilişkin sunum videolarını hazırlanan portal üzerinden giriş yaparak sürece özel olarak tasarladığımız sisteme yükledi.

Adaylarımızın hazırladıkları videolar, Sektör Başkanlıklarımız ve Genel Müdür Yardımcılıklarımız bazında oluşturulan değerlendirme komisyonları tarafından birliktelik, gelişim, mükemmellik ve yenilik değerlerimiz dikkate alınarak puanlandı. Program mentorlerinin daha önceden iletmiş oldukları puanlamaların da ilgili değerlendirmelere eklenmesiyle birlikte adaylarımızın kadroya geçiş aşamasında önemli bir dönemeç aşılmış oldu.

Araştırma Merkezinde Tıbbi Tanı için Optik Tabanlı Biyosensör Geliştiriliyor

Biyosavunma Araştırma Program Birimi (BAPB) bünyesinde biyolojik ajanların tespiti yönünde optik tabanlı tıbbi tanı kiti biyosensör geliştirilmesi için ASELSAN öz kaynakları ile Ar-Ge faaliyetleri devam ediyor. Geliştirilmekte olan biyosensör, algılama molekülü olarak antikorları kullanılıyor. Şu ana kadar Hepatit B, H1N1 ve HSV1 virüs tanıları başarıyla gerçekleştirildi. Tanı çalışmalarına SARS-CoV-2 virüsünün de eklenmesi planlanıyor. Proje kapsamında Yeditepe Üniversitesi ve KOBİ'ler ile işbirliğine gidilerek bu alanda yerli bir ekosistem geliştirilmesine katkı sağlanması da hedefleniyor. Geliştirme faaliyetleri devam eden biyosensör, laboratuvar tipi ve sahada kullanıma uygun milli ve yerli bir ürün olacak.



Kıbrıs İleri Teknolojiler Araştırma Program Müdürlüğünden Özgün Metamalzeme Tabanlı Ürünler

ASELSAN Kıbrıs İleri Teknolojiler Araştırma Program Müdürlüğü ve ODTÜ Kuzey Kıbrıs Kampusu iş birliği ile antenlerde kullanılacak altı adet özgün meta malzeme, yedi adet yeni nesil meta malzeme tabanlı anten ve beş adet ileri teknoloji frekansı ayarlanabilir meta malzeme tabanlı rezonatörü geliştirildi. Tasarım, modelleme, simülasyon, prototip üretim ve laboratuvar ortamında doğrulama faaliyetleri tamamlanan ürünler seri üretime hazır hale getirildi. Bu çalışma ile iletişim sistemleri boyutlarında önemli ölçüde küçülmeler olabileceği ve maliyetlerin azabileceği değerlendiriliyor. Özgün meta malzeme tabanlı anten çalışmaları ile düşük profile sahip yüksek kazançlı anten ve minyatür anten aileleri oluşturuldu. Yüksek kazançlı antenler ile elde edilen sinyal kuvvetindeki artış, kapsama alanında iki kat artış sağlandı. Aynı özellikteki geleneksel antene kıyasla boyutlar beş kat küçültüldü.

ASELSAN Akademi 3'üncü Yılını Uzaktan Eğitim ile Tamamladı

2017-2018 eğitim öğretim döneminde Yüksek Öğretim Kurulu (YÖK) ile ASELSAN arasında imzalanan protokol kapsamında faaliyetlerine başlayan ASELSAN Akademi, araştırma üniversiteleri olan Gazi Üniversitesi, Gebze Teknik Üniversitesi, İstanbul Teknik Üniversitesi ve Orta Doğu Teknik Üniversitesi ile lisansüstü eğitim faaliyetlerine devam ediyor. ASELSAN Akademi kapsamında 471 yüksek lisans, 51 doktora olmak üzere toplam 522 öğrenci bulunuyor.

2019-2020 bahar döneminde ASELSAN Akademi kapsamında, açılan toplam 64 ders, sosyal mesafe önlemleri sebebiyle uzaktan eğitim ile tamamlandı. Üniversitelerin uzaktan eğitim altyapılarının kullanıldığı ders döneminde, Akademi öğrencileri, ASELSAN yerleşkelerinden derslere ve sınavlara katılım sağladı.

ASELSAN'da İnovasyon Yönetim Sistemi Kuruluyor

İnovasyon Yönetim Sisteminin (İYS) kurulması faaliyetleri kapsamında, sektörler ve genel yönetim bölümlerinden inovasyon elçilerinden oluşan bir İYS Çalışma Ekibi oluşturuldu. Haziran ayı içerisinde ilgili ekip ve tüm sektörlerimizden katılımcılardan oluşan toplam 61 personel İnovasyon Yönetim Standartları eğitimi aldı. ISO-56000:2020, ISO-56002:2019, ISO-56003:2019 ve ISO/TR-56004:2019 standart eğitimlerini alan ilgili İYS çalışma ekibi ile açık inovasyon konusunda altyapı oluşturma çalışmaları devam edecek.

Grafen ve İki Boyutlu Malzeme Odak Teknoloji Ağı

Yüksek teknolojiye sahip savunma sistemlerinin millileştirilmesi, mevcut durum analizlerinin gerçekleştirilmesi için, Savunma Sanayii Başkanlığı (SSB) himayelerinde Grafen ve İki Boyutlu Malzeme Odak Teknoloji Ağı başlığı altında yol haritası çalışmaları başlatıldı. Birbirini bütünleyen çalışmalar; Elektronik/Optoelektronik, Kompozitler, Kaplamalar ve Boyalar ile Enerji odak çalışma grupları vasıtasıyla ele alınıyor. Mart 2020 tarihinde 200 katılımcı ile lansman gerçekleştirildi; ardından 130 katılımcı ile 13-14-15 Mayıs 2020 ve 1-2-3 Temmuz 2020 tarihlerinde düzenlenen video konferanslarla sırasıyla Odak Grup Konu Öneri Çalıştayları ve GZTF (Güçlü, Zayıf, Tehdit, Fırsat) analizleri yapıldı. ASELSAN İleri Malzemeler Araştırma Program Biriminin hem lider kuruluş temsilciliği hem de Elektronik/Optoelektronik Odak Grup Liderliğini üstlendiği çalışma devam ediyor.

Taşların Bilimi
Mineroloji

Jeolojinin bir alt dalı olan mineroloji, yerkabuğunda oluşan ve içerdikleri çeşitli minerallerden dolayı farklılaşan taşların fiziksel ve kimyasal özelliklerini inceler.

ASELSAN Kurumsal İletişim Müdürlüğünde uzman teknisyen olarak görev yapan Halil İbrahim Muştucu, minerolojiye ilgisini hayatının odağına taşımış durumda. Muştucu, her biri ayrı bir evren olan taşları bir araya getiriyor. Dağ tepe araştırıp kazarak ülkemize özgü taş ve minerali buluyor, katalogluyor ve sergiliyor. Çalışma arkadaşımız Muştucu'nun evi, gökkuşağının tüm renklerini taşıyan birbirinden ilginç taşlarla dolmuş durumda.

Halil İbrahim Muştucu, mineroloji ile ilgili şunları söyledi:

Taşlar milyonlarca yıl önce toprağın altında ısı ve basınç etkisiyle oluşmuş. Tıpkı insanlar gibi belli titreşime sahip ve bunu sürekli çevrelerine yayıyorlar. Bu da demek oluyor ki bu titreşimlerden bize uygun olanı alıp enerjimize uyumlayabiliriz. Enerjinizi yükseltmenin en kolay ve kısa yollarından birisi enerjinize uygun bir taşa dokunmak veya yanınızda taşımaktır.

Bir taşın size uygun olup olmadığını anlamanın en kestirme yollarından birisi o taşı gördüğünüzde ne hissettiğinizdir. Çoğunlukla ilk gördüğünüzde bayıldığınız taş sizin taşınızdır.

Yine de kararsızlık hissediyorsanız şunlara dikkat edin. Rengini sevdiniz mi, elinize aldığınızda taşta bir ısınma oldu mu? Nasıl bir duygu hissettirdi size. Bunlar çok önemli. Çünkü her taşın herkes üzerinde etkisi başkadır. Birinin çok fayda gördüğünü söylediği taşla sizin frekansınız asla uyuşmayabilir.

Bir taş kullanmanın amacı nedir?

- Fiziksel ve zihinsel problemlerinizde şifa almak.
- Evinizde ve üzerinizdeki negatif enerjiyi temizlemek ve arındırmak.

Dolayısıyla taşı kullanmadan önce mutlaka enerjisinin temizlenmesi gerekir. Siz kullanmaya başladıktan sonrada belli aralıklarla temizlenmesi gerekir. Çünkü taşlar size pozitif enerji verdikleri gibi etraftaki negatif enerjileri absorbe ettikleri için belli bir doygunluğa ulaştıktan bir süre sonra o negatif enerjiyi geri yaymaya başlarlar.

Taşları arındırmak çok kolaydır. Ben genellikle deniz tuzu koyduğum suda bir gece bekletiyorum. Güneş altında 1 saat kadar bekletebilirsiniz. Toprağa gömüp bir gece bekletebilir sonra suyla yıkayıp kullanabilirsiniz.

Taşların bazısı huzur sakinlik verirken bazısı enerji verir canlandırır. Kimi ağrı dindirir şifa verir, kimisi stresi dağıtır, romantik duygularınızı artırır, kimi bilgiyi kolay hatırlamanıza yardımcı olur, karşıdan size gelebilecek negatif enerjiyi pozitife çevirir.”

6098 Sayılı Türk Borçlar Kanunu'na Göre Konut ve Çatılı İşyerinde Güvence Bedeli ve Kira Bedelinin Ödenmemesi Halinde

Tahliye Hakkı

Hazırlayan
Elif Şahin Taşkın
ASELSAN Hukuk Müşavirliği

İnsanlar en temel ihtiyaçlarından biri olan 'barınma ihtiyacını'giderebilmek için sürekli arayış ve iletişim içerisinde olmuş, çağlara göre farklı çözümler bulmuş ve uygulamışlardır. Geçen zaman, gelişen teknoloji ve değişen ihtiyaçlar bu konuda çok sayıda ve farklı sorunların doğmasına neden olmuş, buna bağlı olarak da yazılı düzenlemeler yapılması gereği doğmuştur. Günümüzde barınma ihtiyacı, genel olarak konut veya işyeri satın alarak değil; kira ilişkisi kurarak giderilmektedir. Bu da Kira Hukuku'nun gelişmesine neden olmuş; kira sözleşmesinin bir türü olarak konut ve çatılı işyeri kiralarına yönelik ayrı düzenlemelerin yapılmasını gerekli kılmıştır. Bu yazımızda günlük yaşantıda sıkça karşılaşıldığını düşündüğümüz "Konut ve Çatılı İş Yeri Kiralarında Güvence Bedeli ve Kira Bedelinin Ödenmemesi Nedeni ile Tahliye" hallerinden kısaca bahsedeceğiz.

Kira sözleşmesine ilişkin düzenlemeler 6098 sayılı Türk Borçlar Kanunu'nda (TBK) yer almaktadır. Buna göre kira sözleşmesi, kiraya verenin bir şeyin kullanılmasını ya da kullanmayla birlikte ondan yararlanılmasını kiracıya bırakmayı, kiracının da buna karşılık kararlaştırılan kira bedelini ödemeyi üstlendiği sözleşmedir. Tanımdan da anlaşıldığı gibi kira sözleşmesi, iki tarafa da borç yükleyen, sinallagmatik bir akittir. TBK'da kiraya konu eşyanın taşınır olup olmadığına, kira sözleşmesinin süresine, kiracıya tanınan yetkiye ya da kira konusunun ürün getirip getirmediğine göre farklı tiplerde kira sözleşmeleri düzenlenmiştir. Hangi kira sözleşmesi olursa olsun sözleşme taraflarının borçları ve buna bağlı olarak hakları bulunmaktadır.

Bir kira sözleşmesinde kiraya verenin borçları genel olarak; kiralananı sözleşmede öngörülen kullanmaya elverişli teslim ve bu halde bulundurma borcu, kiralananı ayıpsız olarak teslim etme ve sözleşme süresince de ayıpsız olarak tutma borcu (ayıba karşı tekeffül borcu), kiralananın yan giderlerine katılma borcu, kiraya verenin vergi ve benzeri yükümlülüklere katlanma borcu olarak ifade edilebilir. Kiraya verenin bu borçlarına karşılık kiracının borçları ise genel itibariyle Kiralananı sözleşmeye uygun özenle kullanma ve komşulara saygı gösterme borcu, kiralanandaki ayıpların giderilmesine ve kiralananın gezilip görülmesine katlanma yükümlülüğü, kiralananı geri verme borcu ve kira bedelini ödeme borcudur.

Tarafların bu temel borçlarını belirttikten sonra; uygulamada sıkça karşılaşılan ve bu nedenle bu yazıda değinilmesinde fayda gördüğümüz konut ve çatılı işyerlerinde "güvence bedeli" ve "kira bedelinin ödenmemesi halinde tahliye " başlıkları detaylandırılacaktır.

Kira ilişkilerinde kira bedellerinin geç ödenmesi ya da ödenmemesi, yan giderlere katılma yükümlülüğün ihlali, erken tahliye, kiralananın amaca aykırı ve özensiz kullanımı gibi durumlarla karşılaşılmaktadır. Bu riskler nedeniyle kiraya verenler, kira sözleşmesinin başında teminat verilmesini talep etmektedir. Bu teminat yasal olarak "güvence", uygulamada ise "depozito" adı ile karşımıza çıkmaktadır. TBK öncesinde kira sözleşmelerinde "güvence" ile ilgili bir düzenleme bulunmazken; TBK bu konuda bir kısım düzenlemeler yapmış ve konuyu taraflar açısından açıklığa kavuşturmuştur. Güvence bedeline ilişkin yapılan bu düzenlemeler konut ve çatılı işyerleri için getirilmiştir.

Buna göre konut ve çatılı işyeri kiralarında üç aylık kira bedelinden daha fazla güvence bedeli talep edilemez. Güvence para olabileceği gibi, kıymetli evrak (çek, bono vb.) de olabilir. Güvence para olarak kararlaştırılmışsa kiracı, kiraya verenin onayı olmaksızın çekilmemek üzere, parayı vadeli bir tasarruf hesabına yatırır; kıymetli evrak olarak kararlaştırılmışsa bankaya depo eder. Kiraya veren, kira sözleşmesinin sona ermesini izleyen üç ay içinde kiracıya karşı kira sözleşmesiyle ilgili bir dava açtığını veya icra ya da iflas yoluyla takibe giriştiğini bankaya yazılı olarak bildirmemişse banka, kiracının istemi üzerine güvenceyi geri vermekle yükümlüdür.

Uygulamaya ilişkin değinilmesi gereken bir diğer konu da kira bedeli ve bu bedelin ödenmemesi durumunda kiraya veren tarafından başvurulacak hukuki yollardır. Konut ve çatılı işyeri kirasında kira bedeli asli unsurlardan biridir. Bu nedenle kira borcunun ödenmemesi ve buna bağlı tahliye halleri kanunda ayrıca düzenlenmiştir. Buna göre kira bedelini tahsil edemeyen bir kiraya veren kiracısını tahliye etmek için üç ayrı şekilde davranabilir.

Bu kapsamda başvurulabilecek yollardan birincisi, TBK'nın 352. maddesine göre açılacak tahliye davasıdır. Bu yöntem uygulamada " iki haklı ihtar nedeni ile tahliye" olarak ifade edilmektedir. Kiraya veren, kiracısına kira bedelini ödemediği için yazılı olarak iki ayrı haklı ihtar gönderir. Burada önemli olan gönderilecek ihtarın aynı kira döneminde ödenmemiş kira bedellerine ilişkin olması ve içeriğinde de "bedelin ödenmemesi halinde tahliye yoluna başvurulacağı" ihtarının açıkça yer almasıdır. Bu şartlara uygun olarak gönderilmiş iki haklı ihtara rağmen kiracı, kira bedelini ödemezse kiraya veren Sulh Hukuk Mahkemesinde kiracısı aleyhinde tahliye davası açabilecektir. Sözü edilen tahliye davasının iki haklı ihtarın çekildiği kira döneminin bitimini takip eden bir ay içerisinde açılması gerekmektedir. Aksi halde yasal süreye uyulmadığından davanın reddedilmesi ihtimali söz konusu olacaktır.

İkinci yöntem, TBK'nın 315. maddesi uyarınca kira bedeli ve yan giderleri zamanında ödememiş kiracıya 30 gün süre verilmesi, bu süre içerisinde borcun ödenmemesi halinde sözleşmenin feshedileceği ve tahliye yoluna gidileceği hususlarının ihtar edilmesi ve koşulların oluşması halinde tahliye davası açılmasıdır. Bu yöntem uygulamada "temerrüt nedeni ile tahliye" olarak bilinmektedir. Kiracı kendisine verilen 30 günün sonunda kira bedelini ödemez ve yeri de tahliye etmezse kiraya veren, kiracısı aleyhinde tahliye davası açar. Burada önemli olan, gönderilecek ihtarda en az 30 gün süre verilmesi, kiracıya ödeme yapması için yeterli bir sürenin tanınmış olmasıdır.

Üçüncü yöntem ise, kirasını ödemeyen kiracı hakkında dava açmadan doğrudan icra takibi başlatılmasıdır. Bu yöntemde kiraya veren icra dairesi nezdinde başlatacağı icra takibinde, hem borcun ödenmesini hem de tahliyeyi talep edecektir. Sadece borcun ödenmesinin talep edilmesi, tahliye talebinde bulunmaya engeldir. Tahliye talepli icra takibi, Sulh Hukuk Mahkemesi'nde açılacak tahliye davasından daha pratik ve hızlı bir yöntemdir. Tahliye talepli icra takibinde, kiracı (borçlu), ödeme emrini tebliğ aldıktan sonra 7 gün içinde borca itiraz edebilir; etmezse de 30 gün içinde kira bedelini ödemek durumundadır. 30 gün içerisinde kira bedelinin icra dairesine ödenmesi durumunda icra takibi sona erer; haciz ya da tahliye talep edilemez. Kiracının, ödeme süresi içinde kira borcunu ödemiş olması yeterlidir; kiradan sayılmayan faiz, icra giderleri ve avukatlık ücretinin ödenmemesi nedeniyle tahliye kararı verilemez.

Ödeme emrine itiraz edilmemiş ve borç ödenmemişse kiraya veren alacaklı, cebri icra yolu ile borçlunun mallarının haczedilmesini talep edebileceği gibi; 30 günlük ödeme süresinin bitim tarihinden itibaren altı ay içerisinde icra mahkemesinden kiracının tahliyesine karar verilmesini isteyebilir. Bu durumda icra mahkemesinin yapacağı inceleme sadece, 7 günlük süre içerisinde itiraz edilip edilmediği; edilmemiş ise 30 günlük süre içerisinde ödeme yapılıp yapılmadığı ile sınırlı olacaktır. Borçlu kiracının kira bedelini ödediği iddiaları bu mahkeme tarafından dinlenmez; mahkeme yedi gün içerisinde itiraz edilmediğini, 30 gün içerisinde de ödeme yapılmadığını gördüğü anda tahliye kararı verir. Bu anlamda ilamsız tahliye takibi başlatılarak icra mahkemesinden tahliye istenmesi, genel mahkemede iki haklı ihtara dayanılarak tahliye istenmesinden daha kısa ve pratik bir yöntemdir.

Borçlu kiracının 7 günlük süre içerisinde ödeme ermine itiraz etmesi durumunda ise ilamsız tahliye takibi durur. Takibe devam edilebilmesi için alacaklı kiraya veren tarafından icra mahkemesine başvurularak itirazın kaldırılmasına ve taşınmazın tahliyesine karar verilmesi talep edilmelidir. Alacaklı itirazın kendisine tebliğinden itibaren altı ay içerisinde bu yönde bir talepte bulunmazsa aynı kira alacağından dolayı tekrar tahliye takibi yapamaz. Mahkeme itiraz sebepleri ile bağlı olduğundan, borçlu kiracıların itiraz dilekçelerinde tüm gerekçelerini belirtmesi önem arz etmektedir.

Kira hukukunun geniş ve kapsamlı bir hukuk alanı olması nedeni ile uygulamada çok sayıda ve somut olaya göre farklılık gösteren uyuşmazlıklar yaşanabilmektedir. Bu nedenle kira sözleşmelerinin ihtiyaçlar göz önüne alınarak detaylı şekilde hazırlanmasını ve uyuşmazlık söz konusu olduğunda ise konu ile ilgili yetkin kişilerle çalışılmasını öneriyoruz.

BÜYÜK TÜRK MİLLETİNİN VAKFI

TÜRK SİLAHLI KUVVETLERİNİ GÜÇLENDİRME VAKFI

YÜCE TÜRK MİLLETİNİN BAĞIŞLARIYLA
1987 YILINDA KURULAN TSK GÜÇLENDİRME VAKFI
BÜYÜK TÜRK MİLLETİNDEN ALDIĞI BAĞIŞLARIN
TEK BİR KURUŞUNU DAHİ HEBA ETMEDEN
TÜRK SİLAHLI KUVVETLERİMİZİN
SAVAŞ GÜCÜNÜ ARTIRMAYA YÖNELİK ÇALIŞMALARINA
BUGÜN OLDUĞU GİBİ YARIN DA
AZİM VE KARARLILIKLA DEVAM EDECEKTİR.

EL BİRLİĞİ İLE GÜÇ BİRLİĞİNE

aselsan TÜRKHAVACILIK UZAYSANAYİİ roketsan HAVELSAN İSBİR ASPİLSAN

Yapacağınız bağışlar ile
geleceğe umut, hayata değer katıyoruz.

Bağış Hesap Numaralarımız
YAPI VE KREDİ BANKASI OSTİM ŞUBESİ

Şube Kodu: 602
Hesap No: 59468139
Para Cinsi: TL
Iban No: TR13 0006 7010 0000 0059 4681 39

Şube Kodu: 602
Hesap No: 59430336
Para Cinsi: USD
Iban No: TR60 0006 7010 0000 0059 4303 36

Şube Kodu: 602
Hesap No: 59451723
Para Cinsi: EUR
Iban No: TR52 0006 7010 0000 0059 4517 23

asil
Geleceğe Umut Hayata Değer
ASELSAN SOSYAL İNOVASYON LİDERLERİ YARDIMLAŞMA DERNEĞİ