Akıllı Şebekeler Yolunda Akıllı Sayaçlar
Smart Meters on the Path Leading to Smart Grid

Muhammet Öztemür[1], Betül Soysal[1]

[1]Siber Güvenlik Enstitüsü Bilgi Teknolojileri Ürün Güvenliği Laboratuvarı
TÜBİTAK BİLGEM
muhammet.oztemur@tubitak.gov.tr, betul.soysal@tubitak.gov.tr

Özet

Akıllı şebekelerin kullanımı, sağladığı avantajlar nedeniyle tüm dünyada hızla artmaktadır. Ülkemizde de bu konuda oluşan bilinçle bağlantılı olarak bu kapsamda çalışmalar yapılmaktadır. OSOS projesi ile bu çalışmalar için bir temel oluşturulmuştur. Gerek dünya genelinde yapılan akıllı şebeke uygulamalarında, gerekse ülkemizde uygulamaya konulan OSOS projesi kapsamında akıllı sayaçlar kritik bir öneme sahiptir. Ülkemizde kaçak elektrik kullanımı gerçeğinden haraketle bu sayaçların güvenli bir şekilde tasarlanması ve yapılan tasarımların kontrol edilmesi gerekir. Bu çalışmaların uluslararası bir güvenlik standardına dayandırılması başarıya ulaşılması açısından önem taşımaktadır. Hâlihazırda birçok BT ürün güvenliği değerlendirmeleri için uluslararası geçerliliği ve güvenilirliği olan tek standart ISO 15408 - BT Ürün Güvenliği için Ortak Kriterler standardıdır. Dolayısıyla, ülkemizde güvenli sayaç üretimi ve kullanımı için temel Ortak Kriterler standardının kullanımını öneriyoruz.
Anahtar kelimeler: Akıllı sayaçlar, ortak kriterler, akıllı sayaçların güvenliği

1. Giriş

Tüm dünyada ve ülkemizde gün geçtikçe yükselen yaşam standardı ve buna bağlı olarak artan üretim miktarı, beraberinde enerji ihtiyacını da artırmaktadır. Uluslararası Enerji Ajansı tarafından 2012 yılı verileri esas alınarak yayınlanan WEO2012 raporuna göre elektrik enerjisine olan ihtiyaç önümüzdeki yıllarda hızla artış gösterecek ve 2035 yılında şu anki ihtiyaç miktarına göre %70 artış göstererek 32.000 Tws miktarına ulaşacaktır. Yine aynı rapora ait analize göre şu anki kurulu sistemin bu ihtiyacı karşılaması söz konusu değildir [1]. Artan enerji talebini karşılamak için şu an kurulu olan klasik üretim ve dağıtım sistemlerini artırmak doğrudan bir çözüm gibi görünse de, bu yöntem pek çok dezavantajı beraberinde getirecektir. Üretim miktarına paralel olarak artan hammadde ihtiyacı, dağıtım sistemlerinde meydana gelen teknik kayıpların devamı, sistemin sürdürülebilmesi için ihtiyaç duyulan insan kaynağının maliyete etkisi ve çevre kirliliğinin ulaştığı tehlike sınırlarının zorlanması bunların ilk akla gelenleridir. Tüm bu nedenlerden dolayı, klasik enerji sistemlerinde yatırımların artırılması yerine, her anlamda verimliliğin artırılması esasına dayanan çalışmaların yapılması gereği ortaya çıkmıştır. Bu da akıllı şebekelerin ortaya çıkmasına zemin oluşturmuştur.

2. Akıllı şebekeler ve avantajları

Akıllı şebekeler için birçok tanımlamalar yapılmaktadır. Bu tanımlamaların bazıları şunlardır. "Verimli, güvenilir ve birbirleriyle eşgüdümlü olarak çalışan, her biri otomasyona tabi birçok iletim ve dağıtım sisteminden oluşan bir güç sistemidir." "Acil durumlarda kendi kendini iyileştirme özellikleri olan ve üretim/iletim/dağıtım şirketi ile enerji pazarının ihtiyaçlarına karşılık veren bir güç sistemidir. "Kimi tanımcılar ise akıllı şebekeyi enernet (enerji interneti) olarak tanımlamaktadır [2]. Akıllı şebeke kavramının esnekliği nedeniyle bu tanımların tamamının doğru olduğu kabul edilebilir.

Akılı şebekeler Tesla'dan bu yana kullanılan klasik elektrik üretim ve dağıtım şebekelerine göre birçok avantaj sağlamaktadır. Bunların en temel olanları aşağıda listelendiği gibidir [2]:

- Akıllı şebekeler, enerji tüketiminin uzaktan ve anlık olarak izlenebilmesine ve kontrol edilebilmesine olanak sağlar. Bu sayede, klasik şebekelerde kullanıcı verilerinin temini için söz konusu olan insan kaynağı ihtiyacı ortadan kalkmış olur. Bununla bağlantılı olarak insan eli ile yönetilen sistemin doğasından ortaya çıkacak hatalar bertaraf edilmiş olur. Ayrıca anlık alınan enerji verileri analiz edilerek daha sağlıklı ve verimli enerji üretim politikasının geliştirilmesine imkân sağlar.
- Akıllı şebekeler, şebekedeki problemlerin daha hızlı ve doğru bir şekilde tespit edilmesine imkân sağlar. Bu sayede, problemlerin düzeltilmesi sağlanır ve elektriğin kullanılamadığı zamandan kaynaklanan maliyet kaybının önüne geçilir.
- Akıllı şebekeler, elektik üretim ve dağıtım yapısının dağıtık hale getirilmesine olanak sağlar. Bu sayede klasik şebekelerde olduğu gibi, şebekenin üretim ve dağıtım ile ilgili herhangi bir noktasında ortaya çıkacak bir problemin genel olarak tüm kullanıcıları etkilemesinin önüne geçilmiş olur.
- Akıllı şebekeler, yakın gelecekte kullanımı öngörülen akıllı cihazların (buzdolabı, klima vb.) etkin bir şekilde uzaktan kontrolü için altyapı sağlar.
- Akıllı şebekeler, yenilenebilir enerji kaynaklarının dağıtık olarak üretime etkin bir şekilde katılımını sağlar.

Bu sayede, başta fosil yakıtların kullanımı olmak üzere, çevre kirliliğine neden olan yöntemlerle enerji üretiminin önüne geçilmiş olur. Ayrıca, bu yenilenebilir eneji yöntemleriyle kullanıcıların kendi elektriklerini kendilerinin üretmesi hatta ürettiği fazla enerjiyi şebekeye satması mümkün olabilir.

Akıllı şebekelerin yukarıda sayılan avantajlarını ve klasik şebeke yapısına göre üstünlüklerini destekler nitelikte birçok örnek mevcuttur. Akıllı şebekelerin kullanımı ile sağlanan kazanımlar ve klasik şebekelerin kullanımına devam edilmesi halinde ortaya çıkabilecek riskler için somut birer örnek vermek, konunun öneminin anlaşılması açısından kolaylık sağlayacaktır.

Örneğin 2000-2006 yılları arasında İtalya'nın tamamında uygulanan Telegestore projesinde yaklaşık 30 milyon akıllı sayaç 2.1 milyar Euro harcanarak tüm abonelere sağlanmıştır. Bu projenin en büyük amacı faturalandırma, müşteri takip, arıza tespit gibi özellikleri ile birlikte talep yönetimini sağlamaktır. Nitekim bu sayede, İtalyan elektrik dağıtım sektörü yılda 500 milyon Euro gelir elde etmektedir [3].

Klasik şebeke yapısının kullanılmasındaki riske örnek olarak ise, 2003 yılında ABD'de meydana gelen elektrik kesintisi problemi verilebilir. 2003 yılının Ağustos ayında ABD'de yaşanan enerji kesintisi, aşırı ısınma ve sistem çökmelerinin birbirini takip etmesi sonucu oluşmuştur. Bu arıza sonucu enterkonnekte lokal şebekelerin çökmesi, 50 milyon kişinin enerjisiz kalmasına neden olmuştur. Anderson Ekonomik Grubu'na göre bu da yaklaşık 8.2 milyar dolar bir zararın ortaya çıkmasına neden olmuştur. Bu enerji kesintisinde eğer ABD'nin Cleveland bölgesi arızayı hemen açabilmiş olsaydı, yaşanılan enerji kesintisinin 50 milyon kişiyi değil, sadece 1-2 milyon kişiyi etkilemiş olacağı belirtilmiştir [4].

*Şekil 1.*ABD'de 2003 yılında meydana gelen kesintiden etkilenen bölgeler [2].

3. Türkiye'de akıllı şebekeler

Akıllı şebekelerin yaygın olarak kullanımı ilk defa Malta'da uygulanmıştır [5]. Bununla beraber başta ABD olmak üzere, gelişmiş ülkelerde akıllı şebekeler üzerine yoğun şekilde yatırımlar yapılmakta ve akıllı şebekelere geçiş süreci tamamlanmaya çalışılmaktadır.

Ülkemizde akıllı şebekeler konusunda yapılan çalışmaların temelini Otomatik Sayaç Okuma Sistemi (OSOS) çalışmaları oluşturmaktadır. Enerji Piyasasını Denetleme Kurulu (EPDK) tarafından, Nisan 2011 tarihinde yayınlanan "Otomatik Sayaç Okuma Sistemlerinin Kapsamına ve Sayaç Değerlerinin Belirlenmesine İlişkin Usul ve Esaslar" kapsamında dağıtım şirketleri tarafından OSOS uygulaması için gerekli altyapı tasarımlarının ivedi olarak EPDK'ya iletilmesi gerektiği belirtilmiştir. Ayrıca en üst sınır 800 MWh/yıl olmak üzere, dağıtım şirketlerinin ne kadarlık tüketim kapasitesi üzerindeki abonelerini OSOS kapsamına alacakları bilgisi istenmiştir. Bu kapsamda dağıtım şirketleri tarafından OSOS kapsamına alınacak abone limitleri belirlenmiştir. Söz konusu limitler Çizelge 1'de görülmektedir.

Çizelge 1. Dağıtım şirketleri tarafından OSOS kapsamına alınacak aboneler için belirlenen limitler [6]

Dağıtım Şirketi	OSOS Tüketim Limiti (MWh/yıl)
Akdeniz Elektrik Dağıtım A.Ş.	30
Akedaş Elektrik Dağıtım A.Ş.	800
Aras Elektrik Dağıtım A.Ş.	100
Aydem Elektrik Dağıtım A.Ş.	200
Boğaziçi Elektrik Dağıtım A.Ş.	200
Çamlıbel Elektrik Dağıtım A.Ş.	800
Çoruh Elektrik Dağıtım A.Ş.	200
Dicle Elektrik Dağıtım A.Ş.	800
Enerjisa Başkent Elektrik Dağıtım A.Ş.	800
Fırat Elektrik Dağıtım A.Ş.	200
Gediz Elektrik Dağıtım A.Ş.	100
İstanbul Anadolu Yakası Elektrik Dağıtım A.Ş.	130
Kayseri ve Civarı Elektrik Dağıtım A.Ş.	12
Meram Elektrik Dağıtım A.Ş.	100
Osmangazi Elektrik Dağıtım A.Ş.	800
Sakarya Elektrik Dağıtım A.Ş.	30
Toroslar Elektrik Dağıtım A.Ş.	150
Trakya Elektrik Dağıtım A.Ş.	800
Uludağ Elektrik Dağıtım A.Ş.	90
Vangölü Elektrik Dağıtım A.Ş.	800
Yeşilırmak Elektrik Dağıtım A.Ş.	800

Bu çizelge, dağıtım şirketlerinin büyük çoğunluğunun sadece EPDK'nın koyduğu en üst sınırın üzerinde tüketim yapan aboneler için OSOS uygulamasını gerçekleştirmeyi planladıklarını göstermektedir. Örneğin, 21 dağıtım şirketinden 9 tanesi sadece 800 MWh/yıl üzerinde tüketim yapan aboneler için OSOS altyapısı kuracağını belirtmiştir. Bu durumun dağıtım şirketlerinin başlangıçta oluşacak sistem kurulumu maliyetlerinden kaçınmak istemelerinden kaynaklandığı düşünülmektedir. Belirlenen bu limitler uygulamanın yaygınlaşma düzeyinin şimdilik düşük sayılabilecek düzeyde kaldığını göstermektedir.

OSOS uygulaması ile ilgili diğer bir konu, ülkemizde uygulanan sistemin kapsamıdır. Bu konuda temel olarak EPDK tarafından [7] kapsamında belirtilen asgari özellikler dikkate alınmaktadır. Bu özelliklere göre, OSOS ile istenen tam olarak gelişmiş bir akıllı şebeke yapısı olmayıp isminden de anlaşılacağı gibi, bir "otomatik sayaç okuma sistemi" dir. Henüz mekanik sayaçların kullanımda olduğu ülkemizde, akıllı şebekeye geçiş sürecinde bu şekilde sınırlı isterlerle yola çıkmak ta bir bakıma doğru bir yaklaşım olabilir. Belirtilen noktalara rağmen, akıllı şebekelerin ülkemizde gelişmesine temel oluşturması anlamında OSOS süreci büyük önem taşımaktadır.

Nitekim OSOS faliyetlerinin ortaya çıkması bu konuda sistem kurulumu gerçekleştiren birçok yerli ve yabancı firmanın ülkemizde çalışma yapmasına neden olmuştur. Oluşan bu iş yeteneğinin, ileriki yıllarda geniş kapsamlı akıllı şebeke çalışmalarının sonuca ulaşması için ülkemize kazanç sağlayacağı düşünülmektedir.

Ayrıca, OSOS faliyetlerine ek olarak ülkemizde akıllı şebekelere yönelik gelişmiş Ar-Ge çalışmalarının da yapıldığı bilinmektedir. Örneğin TÜBİTAK Enerji Enstitüsü tarafından yurtdışında, yalnız uzaktan okuma ve kontrol işlemlerinin değil aynı zamanda abonelerin yenilenebilir yöntemlerle enerji üreterek ihtiyaç fazlasını şebekeye satabildiği bir sistem kurulumu projesi gerçekleştirilmektedir [8].

4. Akıllı sayaçlar ve güvenliklerinin sağlanması

Oluşturulan şebekenin sağlaması gereken özellikler, sistem oluşturulurken uygulanabilecek teknolojik imkânlar ve başka parametrelere bağlı olarak klasik şebeke ve farklı akıllı şebeke topolojilerinin çizilmesi ve uygulanması mümkündür. Ancak bu uygulamalarda daima varlığı değişmeyen ve en yüksek öneme sahip olan bileşen sayaçtır. Güvenilir bir sayaç altyapısının olmadığı bir sistemin güvenilirliğinden söz edilemez. Ayrıca sayaçların sistem içerisindeki önemi, akıllı şebekelerin uygulamasının da öncesine dayanmaktadır. Akıllı şebeke uygulamalarında da sayaçların önemini koruyacağı bir gerçektir.

Enerji şebekelerinde olduğu gibi sayaçlar da tüm dünyada ve ülkemizde zaman içinde değişim göstermiştir. 2001 yılına kadar mekanik sayaçlar kullanılırken, bu tarihten sonra daha doğru ölçüm özelliğine ve tarife uygulaması yeteneğine sahip elektronik sayaçlara geçiş sağlanmıştır. Yakın gelecekte mekanik sayaçların tamamen kullanımdan kalkması beklenmektedir.

OSOS faliyetlerinin başlamasından sonra ise, uzak erişimlere imkân sağlayan daha gelişmiş sayaçlar üretilmeye ve kullanılmaya başlamıştır. Bu sayaçların sağlaması gereken asgari teknik özellikler EPDK tarafından belirtilmiştir [7].

4.1. Sayaç güvenliğinin önemi

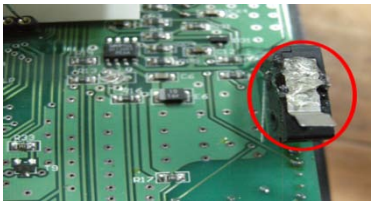
Enerji şebekeleri oluşturulurken Dünya üzerinde yapılan uygulamaların yanı sıra ülkelere özel şartlarında dikkate alınması gerekmektedir. Buna en güzel örneklerden biri ülkemizin kaçak elekrik kullanımı gerçeğidir. Yapılan denetimlerle bu seviye düşürülmeye çalışılsa da, kaçak kullanım ülkemiz ekonomisi üzerine bir yük olmaya devam etmektedir.

Kaçak kullanım nedeniyle;

- Tüketicinin ödediği faturalara fazladan yansıyan miktarla, tüketici bedel ödemektedir.
- Kamu ve özel sektöre ait dağıtım şirketleri, sattıkları enerjiyi tamamen faturalandıramadıkları için zarara uğramaktadır.
- Kaçak kullanımın yüksek olduğu bölgelerde, zarar etme korkusu nedeniyle özelleştirme çağrılarına özel sektör tarafından rağbet gösterilmemektedir. Bu durum özelleştirme sürecinin aksamasına neden olmaktadır.

Zarara uğrayan taraf kim olursa olsun, kaybolan milli servettir. Bu kaybın bir an önce telafi edilmesi gerekmektedir.

Kaçak elektik kullanımı için en yaygın yöntemin sayaçlara müdahale etmek olduğu bilinmektedir. Kaçak kullanım konusunun ele alındığı platformlarda bu konu dile getirilmektedir [9,10].



Şekil 2. İçindeki güvenlik anahtarı (Switch) devre dışı bırakılmış bir sayaç [9]

Çünkü sayaçlar, bir enerji şebekesine ait kıymetli verilerin ilk üretildiği noktadır. Bir bilginin korunmasına ilişkin temel ilkelerden bir tanesi, verinin mümkün olduğu kadar ilk kaynağına yakın bir nokatada koruma altına alınmasıdır. Bilginin ilk noktada koruma altına alınması (kriptografik olarak şifreleme, imzalama vb.) daha ileri noktada bilgiye yönelik birçok saldırının önüne geçebilir. Bunun tersi bakış açısıyla, ilk noktada koruma altına alınmayan bilginin ileri noktalarda koruma altına alınması veya bu korumanın güvenilirliğinin sağlanması daha zor olacaktır. Örneğin, gelişmiş bir akıllı şebeke yapısını ele alalım. Kullanıcı tüketim bilgilerinin sayaçlar üzerinde korunmadığını, ancak iletim hatlarındaki siber tehditlere karşı güçlü önlemlerle korunduğunu düşünelim. Eğer saldırgan (bu saldırgan sayaç kullanıcısı da olabilir) sayaca erişip tüketim bilgilerinin doğruluğuna müdahale ederse, veri iletim hatları ne kadar güçlü önlemelerle korunursa korunsun merkeze üzerinde müdahale yapılmış yanlış veri ulaşacaktır. Bu örnek akıllı şebekelerdeki iletim hatlarında siber güvenliğin önemli olmadığı anlamına gelmemekte, sayaçların sistem güvenliği içerisindeki yerini vurgulamaktadır. Bağlı olduğu merkez ile uçtan uca güvenliği sağlama kapasitesine sahip sayaçların sisteme entegresyonundan sonra, yapılan analize göre network güvenliği alanında açıkta kalan noktaları kapatarak tam güvenlik sağlanabilir.

4.2. Sayaç güvenliğini sağlamada izlenecek yol

Şu an ülkemizde kullanılan sayaçların güvenliği ile ilgili olarak TEDAŞ tarafından [11] kapsamında yayınlanan asgari teknik özellikler tebliğinde bazı maddeler yer almaktadır. Buna ek olarak, OSOS kapsamında kullanılacak sayaçların asgari teknik özellikleri için EPDK tarafından yayınlanan tebliğ içerisinde de, sayaçların güvenliği ile isterler yer almaktadır [7].

Her iki dokümanda yer alan güvenlik isterleri, şüphesiz belli bir tecrübenin ürünü olup büyük önem taşımaktadır. Bununla beraber özellikle ülkemiz gibi kaçak kullanım sorununun olduğu bir yerde, güvenlik konusu fonksiyonel özelliklerden ayrı bir şekilde kapsamlı olarak ele alınması gereken bir parametredir.

Güvenlik konusunun aşağıdaki adımlarla ele alınması gerektiği düşünülmektedir.

- Enerji piyasası içinde aktif olan tüm tarafların önerileri dikkate alınarak; sistemde korunması gereken varlıklar, sisteme yönelik tehditler, düzenleyici kuruluşlar tarafında belirlenen politikalar ve sayacın şebekeden beklentileri (varsayımla) belirlenmelidir.
- Yukarıda belirlenen parametreler dikkate alınarak, kullanılacak sayaçların güvenlik esaslarına ilişkin bir teknik kılavuz hazırlanmalıdır.
- Üretilen sayaçarın, güvenlik esaslarına uygunluğu test edilmelidir.
- Sayaçların kullanımında manipülasyon yapacak saldırgan bakış açısıyla, sayaçlar üzerine sızma yapılmaya çalışılarak güvenlik yönünden dayanıklılıkları teyit edilmelidir.

Tüm bu adımları atarken yeni ve yerel bir süreç tanımlamak yerine uluslararası kabul görmüş bir güvenlik standardını takip etmek birçok avantajı beraberinde getirecektir. Bu sayede; BT ürünlerinin güvenliğinin değerlendirilmesi konusunda

uygulanabilirliği kabul görmüş bir birikimden farydalanılması, yurt dışında getirilen ürünlerin yerli piyasaya uyum sağlaması ve yerli piyasada üretilen ürünlerin yurt dışı piyasasına kolaylıkla çıkabilmesi sağlanacaktır. Bu kapsamda ISO15408/Common Criteria metodolisinin iyi bir kılavuz olacağı düşünülmektedir.

5. Ortak Kriterler Standardı

Ortak Kriterler ismi ISO15408/Common Criteria standardının dilimizdeki karşılığı olarak kullanılmaktadır.
Avrupa, Kanada ve Amerika Birleşik Devletleri'nde üretilen yazılım/donanım ve sistemlerin farklı farklı standartlara göre güvenlik değerlendirmelerinin gerçekleştirilmesi, uluslararası satılan ürünlere uygulanmış testlerin diğer ülkelerde anlaşılmamasına, yazılım/donanım ve sistem güvenliği konusundaki çalışmaların farklı ülkeler arasında farklı şekilde geliştirilmeye çalışılması sorunlara sebep olmuştur. Bu sorunların önüne geçilebilmesi için; Kanada, Fransa, Almanya, İngiltere, Avustralya, Yeni Zelanda ve Amerika Birleşik Devletleri 1996 yılında bir araya gelerek Ortak Kriterler (Common Criteria) sürüm 1.0 dokümanını yayınlamışlardır. Haziran 1999'da Ortak Kriterler ISO/IEC 15408 standardı olarak kabul edilmiştir.
Ortak Kriterler standardı dünyada gün geçtikçe yaygın hale gelmektedir. Hâlihazırda dünyada CCRA'yi (Common Criteria Recognition Arrangement) sertifika tüketicisi olarak 10 ülke, sertifika üreticisi olarak Türkiye'nin de aralarında bulunduğu 16 ülke imzalamıştır.
Ortak Kriterler kapsamında aşağıda listelenen ürün grupları değerlendirilmektedir.

- Erişim Kontrol Cihazları ve Sistemleri
- Biyometrik Sistemler ve Cihazlar
- Sınır Koruma Cihazları ve Sistemleri
- Veri Koruma
- Veritabanları
- Tespit Cihazları ve Sistemleri
- Akıllı Kartlar-Entegre Devre
- Akıllı Kart İşletim Sistemleri
- Akıllı Kart Okuyucuları
- Anahtar Yönetim Sistemleri
- Ağ ve Ağla ilgili Cihazlar ve Sistemler
- İşletim Sistemleri
- Sayısal İmzalı Ürünler
- Güvenilir Hesaplama

5.1. Ülkemizde Ortak Kriterler

2003 yılında Türkiye, uluslararası Ortak Kriterler tanınırlık anlaşması olan CCRA'a imza atarak ortak kriterler alanında dünyada yapılan çalışmaları takip eder ve diğer ülkelerin sertifikalandırdığı ürünleri tanır pozisyona gelmiştir. Türkiye başlangıç sürecinde sadece üretilen sertifikaları tanıyan ülke pozisyonunda iken, 2010 yılında girdiği denetimlerde başarılı olarak sertifika üreticisi ülke olmuştur. Dolayısıyla bir ürün için, Türkiye'deki akredite laboratuarlar tarafından yapılan testler sonunda sertifika makamı tarafından üretilen sertifikalar 26 ülkede tanınmaktadır.
Ortak Kriterler için Türkiye'de sertifika makamı TSE Ortak Kiterler Belgelendirme Sistemi (TSE OKBS)'dir. Şu an için Türkiye'de Ortak Kriterler testlerini yapmak için akredite olan tek laboratuvar TÜBİTAK-BİLGEM OKTEM labotatuvarıdır. Bununla beraber Ortak Kriterler sertifikası almak isteyen üreticiler Türkiye dışında sertifika üreticisi olan 15 ülkeden birine bağlı olan laboratuvarlara ürünlerini analiz ettirerek onay alabilirler.

5.2. Ortak Kriterler çalışma metodolojisi

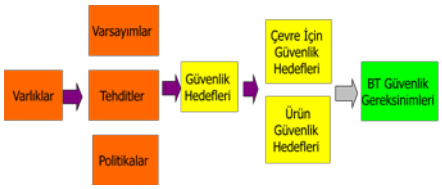
Ortak Kriterler süreci yalnız tamamlanmış bir ürünün güvenlik analizinden ibaret değildir. Ürüne ait; tasarım, üretim, değerledirme, test, analiz ve son kullanıcıya kadar düzgün ulaştırılma süreci dahil olmak üzere yaşam döngüsünü kontrol altına alır. Yaptığı kontrollerle, geliştiriciyi üründeki ve sistemdeki olası güvenlik zayıflıklarını minimuma düşürecek bir metodolojiye uymaya zorlar. Yukarıdaki süreçlerin kontrolü ile beraber, fonksiyonel ve sızma testleri (açıklık analizi çalışması) yaparak ürün için uygun garanti seviyesi verir.
Ortak Kriterler, Değerlendirme Garanti Seviyesi (EAL: Evaluation Assurance Level) olarak bilinen yedi adet garanti paketi tanımlamaktadır.
En düşük seviye olan EAL-1 seviyesinden en yüksek seviye olan EAL-7 seviyesine doğru gidildikçe değerlendirme kapsamı genişlemektedir. Her bir EAL düzeyi için yapılan analizlerin kapsamı Ortak Kriterler standartlarında metrik olarak tanımlanmıştır.

5.3. Koruma Profili

Ortak Kriterler'in çalışma metodolojisinde önemli olan kavramlardan biri de Koruma Profili (PP: Protection Profile)'dir. PP, Ortak Kriterler kapsamında analiz edilecek ürün grupları için hazırlanan teknik şartname olarak tanımlanabilir. Ortak Kriterler kapsamında, 14 farklı ürün grubu içi 237 adet PP yayınlanmıştır [12].
Bir PP oluşturulurken aşağıdaki adımlar dikkate alınır.

- Ürün üzerinde, korunması gereken tüm varlıklar tespit edilerek listelenir. Bir akıllı sayaç için, kullanıcı tüketim verisi bir varlık örneği olabilir.
- Ürünün kullanımına ilişkin düzenleyici kuruluşun politikaları belirlenir. Sayaçlardan gelen verilerin depolandığı merkezlerin güvenli ortamda olması bir politika örneği olabilir.
- Ürünün kullanımı ile ilgili varsayımlar dikkate alınır. Bir akıllı sayaç için, sayacın doğru ölçüm yaparak kullanıcı verilerini oluşturması bir varsayım olabilir.
- Varlıklara yönelik tehditler tespit edilir. Bir akıllı sayaç için, kullanıcı tüketim verisinin değiştirilmesi bir tehdit örneği olabilir.
- Varlıklara yönelik tehditlerin karşılanması için ürün veya ürün çevresine ait güvenlik hedefleri belirlenir. Bir akıllı sayacın verileri şifreli saklaması ürüne ait bir güvenlik özelliğidir. Sayaçların fiziksel olarak güvenli ortamda saklanması ürün çevresine ait bir güvenlik özelliğidir.
- Ürünün sağlaması gereken hedefler için gerekli teknik

özellikler belirlenir. Bir akıllı sayaç için, üzerinde güçlü kriptografik algoritmaların yer alması buna bir örnek olabilir.



Şekil 3. Koruma profili yapısı

5.4. Ortak Kriterler ve Akıllı Sayaçlar

Sayaçların güvenliği, ülkemizde ve dünyada akıllı şebekelerden daha önce enerji piyasası gündemine gelmiş bir konudur. Akıllı şebekeler ile beraber, enerji sistemlerinin üzerinde yapılan çalışmalar akıllı sayaçların güvenliğini tekrar ön plana çıkarmıştır. Bu güvenliğin garanti altına alınması için, sayaçların üretiminde dikkate alınması gereken belli bir standardın sağlanması gerekmektedir. Ortak Kriterler, uluslararası kabul görme yaygınlığı ve aynı kapsam içinde yer alan BT ürünlerinin güvenlik değerlendirmesinde kullanım yaygınlığı ile sayaç güvenliğinin sağlanması için de uygun bir platformdur.

Düzenleme ve standartlar konusunda Avrupa'nın önde gelen ülkesi konumunda olan Almanya'da hâlihazırda bu konuda çalışmalar başlamıştır. Federal Bilgi Güvenliği Merkezi (BSI: Bundesamt für Sicherheit in der Informationstechnik) iki PP dokümanı hazırlamıştır. Bu PP dokümanlarından bir tanesi; basit ölçme cihazları, akıllı ev bileşenleri (akıllı cihazlar, güneş panelleri vb.) ve yönetim merkezi arasında bağlantıyı sağlayan "smart meter gateway" modülü için yazılmıştır [13]. Diğeri ise, bu gateway içinde sadece güvenlik fonksiyonlarını yerine getirmeye odaklı "güvenlik modülü" için yazılmıştır [14].

İçinde bulunduğumuz yıl içerisinde yapılacak düzenlemelerle, üretilen akıllı sayaçların söz konusu PP'lere uyumluluk sağlaması beklenmektedir.

Bu durum, Almanya'ya yönelik üretim yapan sayaç üreticileri tarafından hâlihazırda dikkate alınmıştır. Elster ve Itron gibi büyük firmalar yeni çıkardıkları ürünlerinde bu teknik kılavuzlara uyumluluğa dikkat etmekte ve ürün ilanlarında bunu belirtmektedirler [15,16].

6. Sonuç

Sayaçlar üzerinde yasa dışı müdahaleler yaparak kaçak enerji kullanımı, kaçak kullanımın yaygın olduğu ülkemizde çözülmesi gereken önemli bir problemdir. Öte yandan ülkemizde, mekanik sayaçlardan elektronik sayaçlara geçiş aşamasını tamamlanmak üzeredir. OSOS faliyetleri ile beraber uzaktan erişimli sayaç modellerine geçiş başlamıştır. Önümüzdeki yıllarda, tüm dünyayı etkileyen enerji konjonktürürünün de etksiyle akıllı şebekelere yönelik çalışmalar yoğunlaşacaktır. Bu kapsamda yine sayaç modellerinde yeni değişimler olacaktır. Tüm bu gelişmeler, ülkemizin enerji sistemleri ve bu sistemlerin kalbi konumunda olan sayaçlar konusunda bir eşik noktasında olduğunu göstermektedir. Bir sayacın tüketim ömrünün 10 yıl olduğu düşünülmektedir. Bu nedenle önümüzdeki geçiş sürecinde sayaçların tekrardan bir değişime ihtiyaç olmayacak şekilde ürettirilmesi gerekmektedir. Aksi durumda, sonradan tespit edilen güvenlik problemleri nedeniyle ortaya çıkacak değiştirme ihtiyaçları büyük miktarda milli servet kaybına neden olacaktır. Şu an bulunduğumuz noktada; güvenlik konusunu hafife almak veya sadece uzaktan okuma sisteminin varlığı ile sorunların tamamen çözüleceğini düşünmek doğru bir düşünce tarzı olmayacaktır. Yine benzer şekilde, güvenlik ile ilgili olarak sadece klasik şebekelerdeki durumlara odaklanmak, problemin eksik olarak ele alınmasına neden olacaktır. Önümüzde kaçınılmaz bir yol olan akıllı şebekelere doğru gidildikçe, dikkate alınmayan bu problemler kendini gösterecektir.

Sonuç olarak, akıllı sayaçlarda güvenlik konusunun kapsamlı olarak ele alınması gerekmektedir. Metodoji olarak ISO15408/Ortak Kriterler metodolojisi ile hareket edilmesi önerilmektedir. Bu kapsamda, üretilecek sayaçların güvenlik özelliklerini belirleyen bir PP dokümanı oluşturulması, bu dokümanda tanımlanan özelliklere göre ürünlerin değerlendirilmesi önerilmektedir.

7. Kaynakça

[1] International Energy Agency, World Energy Outlok 2012.

[2] Tanrıöven, K., Yararbaş S. ve Cengiz H., "Geleceğin Elektrik Dağıtım Şebekesi Smart Grid", *Elektrik-Elektronik ve Bilgisayar Sempozyumu*, Fırat Üniversitesi, 2011

[3] Nadar A., "Akıllı Şebekeler", *Mimar ve Mühendis*, Sayı-67, Sayfa: 60-63, 2012

[4] Can M., "Akıllı Şebekeler", Selçuk Üniversitesi Fen Bilimleri Enstitüsü Tezsiz Yüksek Lisans Programı, 2012

[5] http://www.ibm.com/smarterplanet/ie/en/smart_grid/examples/index.html

[6] Alıcı O., "OSOS Usül Esasları Düzenlemesi", *Elektrik Sayaçları Çalıştayı*, Antalya, 2012

[7] 2012 Enerji Piyasası Denetleme Kurulu, "OSOS kapsamına dahil edilecek sayaçların, haberleşme donanımının ve ilave teçhizat ve altyapının asgari teknik özellikleri", Resmi Gazete Sayı: 28105.

[8] Şahin C., Kahraman Ö., Temiz A., Smiai M. S., Alramadan F. Y., Almutairi S. S., ve Alshahrani S.,"A Smart Control System for PV Generation in LV Distribution", *Saudi Arabia Smart Grid*, Cidde, Suudi Arabistan,

[9] Kara A.N., "BEDAŞ Sunumu", *Elektrik Sayaçları Çalıştayı*, Antalya, 2012

[10] Şimşek H., ""AYEDAŞ Sunumu", *Elektrik Sayaçları Çalıştayı*, Antalya, 2012"

[11] Türkiye Elektrik Dağıtım A.Ş., "Elektronik Sayaçlarda TEDAŞ Tarafından İstenen Asgari Şartlar", http://www.tedas.gov.tr/BilgiBankasi/KitaplikMevzuatlar/Elektronik Sayaçlarda Tedaş Tarafından İstenilen Asgari Şartlar.doc

[12] http://www.commoncriteriaportal.org/pps/stats/

[13] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Protection Profile for the Gateway of a Smart Metering System", 2011.

[14] Bundesamt für Sicherheit in der Informationstechnik (BSI), " Protection Profile for the Security Module of a Smart Metering System (Security Module PP)", 2011.

[15] http://www.elster.com/en/press-releases/2012/1656430

[16] http://www.insys-icom.com/icom/en/energy/smart-metering