Elektrik Altyapılarında Bilgi Güvenliği Riskleri ve Çözümler
Information Security Risks and Controls in Electricity Infrastructures

Mustafa Fikret Ottekin

TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü
fikret.ottekin@tubitak.gov.tr

Özet

Bu makalede akıllı şebekeler de dâhil olmak üzere elektrik iletim ve dağıtım sistemlerinde karşılaşılan başlıca bilgi güvenliği riskleri ve bu risklerin kontrol altında tutulması için alınması gereken önlemler incelenecektir. Bilgi güvenliği kapsamında risk, bilgi varlıklarında bulunan açıklıkların tehditler tarafından kullanılması sonucunda bilgi varlığının gizlilik, bütünlük veya sürekliliğinin kaybolmasıdır. Makalede enerji altyapılarında bulunan en büyük bilgi güvenliği risklerinin hangileri olduğunu belirlemek için öncelikle riski oluşturan unsurlar değerlendirilecektir. Bu kapsamda etki alanı, derinliği ve olasılık ölçekleri geliştirilecek ve risk değerlendirme tablosu oluşturulacaktır. Bunun ardından elektrik altyapılarında bulunan belli başlı bilgi güvenliği riskleri ve bunları işlemek için alınabilecek önlemlere değinilecektir. Son bölümde akıllı şebekelerde bulunabilecek belli başlı bilgi güvenliği riskleri ve bu risklerin işlenmesi için atılması gereken adımlar hakkında düşünceler geliştirilecektir.

Anahtar Kelimeler: Bilgi Güvenliği, Elektrik Altyapısı, SCADA, Akıllı Şebeke.

1. Giriş

Elektrik enerjisinin iletim ve dağıtımını denetlemek için kullanılan SCADA sistemlerinin devre dışı kalması veya ele geçirilmesi halinde enerjinin tüketiciye ulaştırılamaması söz konusu olabileceği gibi elektrik sistemlerinde kalıcı hasar da meydana gelebilir. Bu gerçek, elektrik iletim ve dağıtım altyapılarını denetleyen SCADA sistemlerinin bilgi güvenliği bakış açısı ile yönetilmesi gerektiğini ortaya koymaktadır.

Bilgi güvenliği kapsamında riski oluşturan üç bileşen vardır: Varlık, varlıkta bulunan açıklık ve bu açıklığı kullanacak tehdit. Bu üç faktörün bir araya gelmesi ile bilginin gizliliğinin, bütünlüğünün veya sürekliliğinin kaybolması söz konusu olmakta, böylece ortaya çıkması beklenen olumsuz etki risk olarak adlandırılmaktadır [1]. Risk, aşağıdaki formülle ifade edilebilir:

$$\text{Risk} = \text{Etki (Alan x Derinlik x Süre)} \times \text{Olasılık} \quad (1)$$

Elektrik altyapılarında gerçekleşebilecek bilgi güvenliği risklerinin belirlenebilmesi için önce sistemlerin, sonra riski oluşturan bileşenlerin nesnel kriterler uyarınca değerlendirilmesi gerekir.

2. Elektrik Altyapılarında Risk Analizi

2.1. Sistemlerin Değerlendirilmesi

Elektrik iletim ve dağıtım sistemlerinin devre dışı kalması ile oluşacak etki, bu sistemlerin taşıdıkları enerjinin hacmi göz önünde bulundurularak değerlendirilebilir.

Enerji Bakanlığı verilerine göre elektrik enerjisi Türkiye'nin tükettiği toplam enerji içinde % 18.4'lük paya sahiptir [2]. Otoprodüktörler tarafından üretilen enerjiden arta kalan %17,33'lük pay Türkiye Elektrik İletim A.Ş. Milli Yük Tevzi SCADA/EMS sistemi tarafından izlenen ve denetlenen iletim altyapısı aracılığı ile dağıtım şirketlerine aktarılmaktadır. Çoğu SCADA sistemleri tarafından yönetilen veya yönetilme arifesinde olan dağıtım sistemleri, elektrik enerjisini tüketicilere ulaştırmaktadır [3].

Üretim ise yüzlerce santral tarafından gerçekleştirildiği için [4] elektrik santralleri iletim ve dağıtım sistemleri kadar kritik değildir.

Elektrik altyapısı işleten kurumlar öncelikle ulusal enerji tüketiminde kontrol ettikleri payı göz önünde bulundurarak kurumsal risk yönetimi sürecinin gerekliliğini değerlendirmelidir. Risk yönetimi yapılacaksa ilk iş olarak önemli sistem bileşenlerini içeren varlık envanterinin ve ağ topolojisinin hazırlanması gerekir.

2.2. Sistem Bileşenleri ve Etkilenen Alan

Elektrik altyapı sistemlerinin topolojisi ile ilgili yayınlar [5] ve TEİAŞ verileri [6] göz önünde bulundurulduğunda sistemlerin tam olarak olmasa da ağaç topolojisine yakın olduğu anlaşılmaktadır.

SCADA kontrol sunucusunun devre dışı kalması halinde sistemin tamamı etkileneceğinden, elektrik iletim ve dağıtım sistemlerindeki en önemli bilgi varlıkları, ağacın tepesinde yer alan kontrol sunucularıdır. Kontrol sunucusunu sistemin geri kalanına bağlayan yönlendirici, modem vb. ağ bileşenleri de sunucunun kendisi kadar değerlidir.

Diğer sistem bileşenleri ile ilgili olarak, bileşenlerin değerinin sistem merkezine uzaklıkla ters orantılı olduğu söylenebilir. Bileşenleri değerlendirmek için Çizelge 1 kullanılabilir:

Çizelge 1. Etki alanının değerlendirilmesi

Sistem Bileşeni	Etki Alanı	Değer
Sistem merkezinde yer alan sunucu, yönlendirici, iletişim hattı vb. bileşenler.	Sistemin tamamı	100
Bölgesel kontrol merkezlerindeki bileşenler veya bunları merkeze bağlayan hatlar.	Bölgesel	10
Uzak istasyonlarda bulunan bileşenler veya bunları kontrol merkezine bağlayan hatlar.	Sınırlı	1

2.3. Farklı Tehditler ve Etki Derinlikleri

Sistem bileşenlerinde gerçekleşecek riskler değerlendirilirken, tehdidin ortaya koyabileceği etkinin şeklinin, daha doğrusu derinliğinin de göz önünde bulundurulması gerekir. Etki derinliği, bilginin güvenlikle ilgili özellikleri göz önünde bulundurularak Çizelge 2'deki gibi sınıflandırılabilir:

Çizelge 2. Etki derinliğinin değerlendirilmesi

Etki Derinliği	Açıklama	Değer
Ele geçirme (BÜTÜNLÜK kaybı)	Veri akışının veya kontrol mesajlarının kötü niyetle şekillendirilmesi veya tekrarlanması sistemin saldırıya uğradığı anlamına gelir.	3
İletişimin kesilmesi (SÜREKLİLİK kaybı)	Kontrol mesajlarının veya veri akışının kesilmesi, sistemin kontrolsüz kalması anlamına gelir.	2
İletişimin dinlenmesi (GİZLİLİK kaybı)	Kontrol mesajlarının veya veri akışının dinlenmesi, orta vadede sistemin ele geçirilmesine neden olabilir.	1

Çizelge 1 ve 2'de yapılan tespitler bir araya getirilerek farklı sistem bileşenlerinde gerçekleşebilecek belli başlı risklerin etkileri değerlendirilebilir:

Çizelge 3. Etki değerlendirmesi

	Ele Geçirme	Kesinti	Dinleme
Sistem merkezi	300	200	100
Bölgesel Kontrol Merkezi	30	20	10
Uzak İstasyon	3	2	1

(1) numaralı formülde etkiyi oluşturan bileşenlerden biri olarak gösterilen "Süre" için de yukarıdakilere benzer bir çizelge oluşturulabilir ve süre etki değerlendirmesine çarpan olarak eklenebilir.

2.4. Olasılık, Açıklık ve Tehdit

Riskin belirlenmesi için değerlendirilmesi gereken son parametre, tehdidin ve tehdidin kullanacağı açıklığın varlığı ile orantılı olan olasılıktır. Olasılık değerlendirmesi, aşağıdaki gibi yapılabilir:

Çizelge 4. Olasılık değerlendirmesi

Açıklık	Tehdit	Olasılık	Değer
Var	Var	Yüksek	10
Var	Yok	Orta	3
Yok	Yok	Düşük	1

Bu kapsamda tehditler üç kategoriye ayrılabilir [7]. Bunlar:

1. Fiziksel tehditler
2. Çevresel tehditler ve
3. Siber tehditlerdir.

Açıklıklar ise, kabaca, altı kategoride değerlendirilebilir [8]. Bunlar:

1. Donanım açıklıkları
2. Yapılandırma açıklıkları,
3. Yazılım açıklıkları
4. İletişim açıklıkları,
5. İnsan kaynakları açıklıkları ve
6. Politika ve prosedür açıklıklarıdır.

2.5. Risklerin Değerlendirilmesi

Varlık envanteri, ağ topolojisi ve yukarıdaki çizelgeler kullanılarak sistem bileşenlerindeki açıklıklar, bunları kullanabilecek tehditler ve ilgili riskler belirlenir (Çizelge 5). Büyük riskler öncelikli olmak üzere risklerin işlenmesi için görevlendirme ve planlama yapılır.

Çizelge 5. Risk Değerlendirme Tablosu

Varlık	Açıklık	Etki	Olasılık	Risk	Açıklama
SCADA Sunucusu					
Güvenlik Duvarı					
Operatör Terminali					
Bölgesel Kontrol Merkezi Sunucusu					
…					

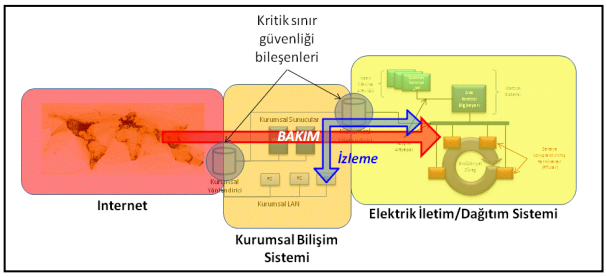
3. Başlıca Riskler ve Güvenlik Önlemleri

Bu bölümde elektrik altyapılarında karşılaşılan en büyük bilgi güvenliği riskleri ve bu risklerin işlenmesi için alınabilecek önlemler kısaca açıklanacaktır.

3.1. Ağlar Üstünden Yetkisiz Erişim

3.1.1 Açıklık

Elektrik iletim ve dağıtım sistemlerinin hemen hepsinin kısıtlı da olsa kurumsal bilişim ağı ile ve Internet'le bağlantısı mevcuttur. Güvenlik açığı arz ettikleri bilinmekle birlikte pratik gereksinimler dolayısı ile bu bağlantılar kullanılmaktadır. Kurumsal bilişim sistemi ile bağlantı kurum yöneticilerinin iletim/dağıtım sürecine ilişkin parametreleri izlemesi, Internet ile bağlantı ise SCADA'nın bakım ve güncellemelerinin üretici firma tarafından uzaktan yapılabilmesi gereksiniminden kaynaklanmaktadır (Şekil 1).



Şekil 1. Elektrik altyapısının kurumsal ağ ve Internet'le bağlantısı.

3.1.2 Güvenlik Önlemi

Bu bağlantılardan kaynaklanan risklerin asgari düzeye indirilmesi için sınır güvenliği sistemlerinin teknik boyutta ve politika boyutunda doğru yapılandırılması gerekir. Bu kapsamda genellikle kontrol ağı ile kurumsal ağ arasında bir DMZ oluşturulması, ağlar arasında bilgi paylaşımı için kullanılacak kayıt sunucusu vb. sistemlerin bu bölgede konuşlandırılması ve DMZ'e erişimin mümkünse birden çok güvenlik duvarı ile korunması önerilmektedir [8], [9]
İdari boyutta ise sistem merkezine uzaktan erişim politikasının oluşturulması ve üretici firmaya sözleşme ile dikte edilmesi gerekir. Bu önlemlerin alınması halinde SCADA'ya yönelen tehditlerin sadece yetkili kullanıcılardan kaynaklanması beklenmektedir.

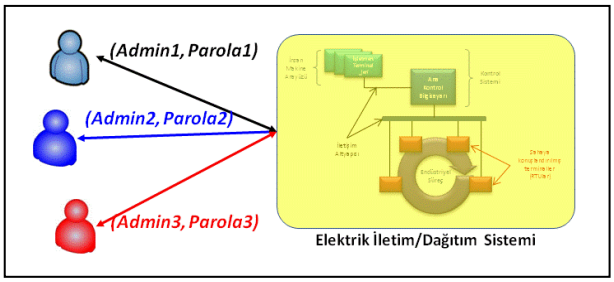
3.2. Yetkili personelin izlenmemesi

3.2.1 Açıklık

Elektrik altyapı sistemlerinin önemli bölümünde sistem yöneticisi, operatör ve benzeri yetkili kullanıcıların sistemde işlem yapmadan önce, kendilerine özgü kullanıcı isimleri ve parolalarla kimlik tespitine zorlanmadığı görülmemektedir. Bu sistemlerin bir bölümünde uygulama yazılımında güvenli oturum açma işlevi yoktur. Bu durum kayıt yönetimi sistemleri eksiksiz olarak çalışsa bile herhangi bir tarihte yetkili kullanıcılardan biri tarafından yapılan işlemin hangi kullanıcı tarafından yapıldığını belirlemeyi olanaksız hale getirmektedir.
Bu kapsamda diğer bir açıklık, elektrik altyapı sistemlerinin hemen hepsinde sistem yöneticilerinin yaptıkları işlemlerle ilgili kayıtları silme hakkına sahip olmasıdır. Bir sistem yöneticisinin sisteme yaptığı saldırı veya yaptığı hata ile ilgili kaydı silmesi, gerçekleşen olayla ilgili delillerin yok olması, dolayısı ile hukuki sürecin devreye sokulamaması anlamına geleceğinden kabul edilemez.

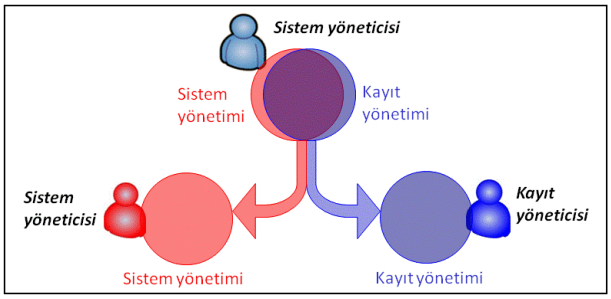
3.2.2 Güvenlik Önlemi

Bu açıklıklardan kaynaklanan risklerin asgari düzeye indirilmesi için öncelikle SCADA'ya erişim yetkisine sahip (sistem yöneticisi, operatör, vb.) personele tekil kullanıcı ismi atayacak kurumsal süreç oluşturulmalı, aynı süreç kapsamında yetkili personel, sistem tarafından karmaşık parolalar seçmeye ve parolalarını düzenli aralıklarla değiştirmeye zorlanmalıdır. Yetkili personel, bilişim sistemine erişmeden önce kimliğini kullanıcı kimliği ve parolası ile bilişim sistemine ispatlamalı, bu özellik uygulama yazılımında bulunmuyorsa, geliştirici firma ile görüşülmeli ve güvenli oturum açma işlevi uygulama yazılımına eklenmelidir (Şekil 2).



Şekil 2. Yetkili kullanıcıların sisteme erişimi

SCADA'da yetkili personel tarafından yerel olarak yapılan işlemlere ek olarak Internet ve kurum bilişim sistemi üstünden yapılan işlemler de kayıt altına alınmalıdır.
Sistemler, yetkili personelin yaptığı işlemlerle ilgili kayıtları silme olasılığını ortadan kaldıracak şekilde yapılandırılmalıdır. Bu bağlamda "Kayıt Yöneticisi" rolü tanımlanmalı, kayıtlar kayıt yöneticisi rolüne sahip bir sistem yöneticisi tarafından düzenli aralıklarla gözden geçirilmeli ve gerekli durumlarda yönetime bilgi verilmelidir. Kayıt yöneticisi sistem üstünde herhangi bir işlem yapma hakkına sahip olmamalıdır (Şekil 3).



Şekil 3. Sistem yönetiminde görevler ayrılığı

3.3. Kritik Sistem Bileşenlerinin Yedeksiz Çalışması

3.3.1 Açıklık

Bu makalenin 2.2 bölümünde de belirtildiği gibi, farklı sistem bileşenlerinin devre dışı kalması halinde farklı büyüklükte alanlarda olumsuz etkiler oluşabilmektedir. Bu olumsuz etkilerin makul bir süre içinde giderilememesi zararın artarak devam etmesine neden olabilir. Sistem merkezleri başta olmak üzere elektrik altyapılarının kritik bileşenlerinin iş sürekliliği bakış açısı ve kurumsal bir süreç çerçevesinde şekillendirilmemesi durumunda geniş alanlarda uzun süreli olumsuz etkilerin ortaya çıkması sürpriz olmayacaktır.

3.3.2 Güvenlik Önlemi

Başlıca sistem bileşenlerinin ve bu bileşenlerin iletişimi için kullanılan hatların yedeklenmesi gerekir. İş sürekliliği analizi kapsamında belirlenmesi gereken başlıca parametre olan RTO ("Recovery Time Objective"), asıl sistem bileşeni devreden çıktıktan ne kadar zaman sonra yedeğin devreye girmesi gerektiğini belirtir. Bu parametre uyarınca planlanan ve kurulan yedek sistem bileşeni, asıl sistem bileşeni devreden çıktıktan bir süre sonra devreye girerek etkilenen alanda normal çalışma şartlarına dönülmesini sağlar. Yedek sistem bileşenleri planlanırken aşağıdaki çizelgeler kullanılabilir [10]:

Çizelge 6. Sistem Bileşenlerinin Yedeklenmesi

Sistem Bileşeni	RTO	Yedekleme / Kurtarma Stratejisi
Sistem merkezi	Çok kısa	Disk replikasyonu, Canlı yedek sistemler, "Sıcak" site
Bölgesel kontrol merkezi	Kısa-orta	Optik yedekleme, WAN/VLAN replikasyonu, "Ilık" site
Uzak istasyon	Orta-uzun	Teyplere yedekleme, Taşınma veya "Soğuk" site

Çizelge 7. Yedek site kategorileri

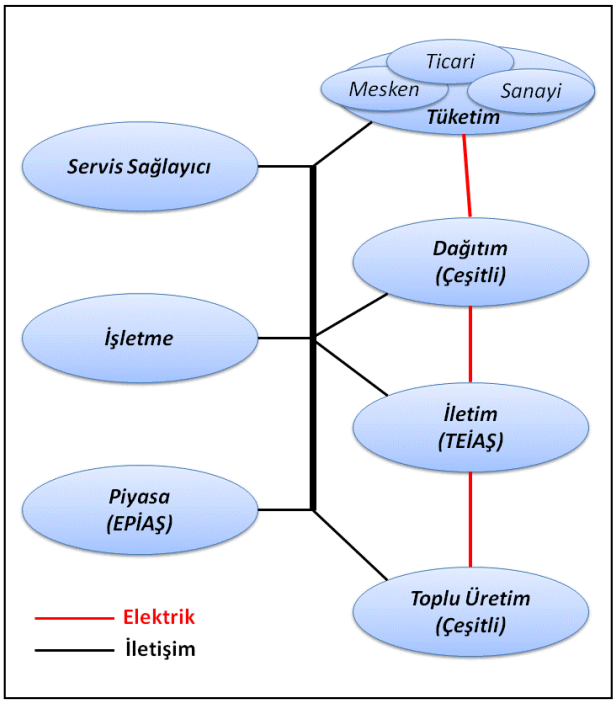
	Bütçe ihtiyacı	Donanım sistemleri	İletişim sistemleri	Devreye girme süresi
Soğuk	Düşük	Yok	Yok	Uzun
Ilık	Orta	Kısmi	Kısmi	Orta
Sıcak	Yüksek	Tam	Tam	Kısa

Sistem merkezi ile hizmet verilen bölge arasında ilave katman veya katmanlar oluşturulması ise sistemin daha dağıtık bir yapıya kavuşmasını ve sistem bileşenleri devre dışı kaldığında etkilenecek bölgenin küçülmesini sağlar. Uzun vadede sistemlerde yapılacak değişiklikler planlanırken bu prensip de göz önünde bulundurulabilir.
İş sürekliliğini sağlamak için kurulan sistemlerin işlerliğini güvence altına almak için gerekli prosedürlerin hazırlanması, görevlendirmenin yapılması, ilgili insan kaynağının eğitimi ve tüm bu önlemlerin periyodik tatbikatlarla test edilmesi gerekir.

4. Akıllı Şebekelerde Bilgi Güvenliği

4.1. Genel Sistem Güvenliği

Akıllı şebekelerden elde edilmesi beklenen sonuçlar, bu şebekelere katkı yapacak taraflar arasında etkin ve güvenli veri iletişiminin sağlanmasına bağlıdır. Akıllı şebekelerin güvenliği, ağırlıklı olarak iletişim kanallarının güvenliğinin sağlanması olarak değerlendirilebilir. Diğer sistem bileşenlerinin güvenliği ile ilgili olarak mevcut bilgi güvenliği süreç ve önlemleri geçerlidir.
Akıllı şebekelerde yer alacak tarafların yedi alanda toplanabileceği belirtilmektedir [11]. Hemen hepsi birbiriyle iletişim halinde olan bu yedi alan Şekil 4'de görülmektedir. Bu yedi alan arasında yer alan ara yüzlerin her birinde bilginin gizliliği, bütünlüğü ve sürekliliği açısından farklı güvenlik gereksinimleri olduğu bildirilmektedir [12].
İlk iş olarak bu ara yüzlerin sahiplerinin belirlenmesi ve her bir ara yüzde alınacak güvenlik önlemlerinin kararlaştırılması gerekir.



Şekil 4. Akıllı şebekelerde yer alan taraf ve kurumlar

Hali hazırda çalışır durumda bulunan ara yüzler TEİAŞ ile üreticiler ve dağıtım şirketleri arasındaki ara yüzdür. İlave olarak, EPİAŞ'ın bilgi sistemi faal durumdadır. Bu iki kurumun kendi ara yüzleri ile ilgili güvenlik önlemlerini paydaşları ile birlikte gözden geçirmeleri ve standartlaştırmaları beklenebilir. Diğer ara yüzlerle ilgili olarak çalışma yapılması gerekmektedir. Yol haritasının şu şekilde olacağı söylenebilir:

- Ara yüzleri belirle.
- Ara yüzlerin sahiplerini belirle.
- Ara yüzlerde bulunması gereken güvenlik önlemlerini belirle.
- Standartları oluşturur.
- Standartlara uygun bileşenlerin geliştirilmesini sağla.
- Bileşenlerin güvenlik gereksinimlerini sağladığını doğrula.
- Tedarik, kurulum ve operasyon.

Bu adımların genel koordinasyonun EPDK gibi yetkili kamu kurumlarından biri tarafından yapılması gerektiği söylenebilir.

4.2. Tüketici Ara Yüzünde Beklenebilecek Sorunlar

Akıllı şebekelerle birlikte tüketici katmanında devreye girmesi beklenen yeni sistem bileşenleri mevcuttur. Bunlardan ilki, tüketim verilerinin gerçek zamanda dağıtım sistemi merkezine akmasını sağlayacak akıllı sayaçlardır. İkincisi ise, tüketicilerin güneş panelleri ve rüzgâr türbinleri aracılığıyla ürettikleri enerjiye ilişkin veriyi dağıtım sistemi merkezine iletecek invertör vb. bileşenlerdir.

Bu tablonun bilgi güvenliği bakış açısı ile değerlendirilmesi sonucunda iki riskin gerçekleşmesi beklenebilir:

- Son kullanıcıların sayaç verilerine müdahale ederek tüketim verilerini değiştirmesi
- Tüketicinin kişisel mahremiyetinin kaybolması
- Son kullanıcıların invertör verilerine müdahale ederek üretim verilerini değiştirmesi.

İlk risk göz önünde bulundurulduğunda akıllı sayaçlarla dağıtım sistemi arasındaki ara yüzde veri bütünlüğünün sağlanması gerektiği görülmektedir. Uçtan uca kriptolama ile sağlanabilecek bu gereksinim kripto algoritmasının akıllı sayaç üstünde gerçeklenmesi gereğini ortaya çıkarmaktadır. İlave olarak, milyonlarca akıllı sayacın katılacağı anahtar yönetimi sürecinin etkin bir şekilde çalıştırılabilmesi gerekmektedir. Özellikle mesken tipi akıllı sayaçların belli bir bedelin altında kalması gereği yüzünden bu gereksinimlerin sağlanması güçtür.. Uçtan uca kriptolamaya ilave olarak, sistem merkezinde toplanan verinin "normalliğini" sınayarak saldırıların belirlenmesinin de gerekli olduğu belirtilmektedir [13]. Bu gereksinimlerin sağlaması için ilave Ar-Ge çalışması gerektiği kaydedilmektedir [14].

Akıllı sayaçlar aracılığı ile bir meskende veya ticari tesiste gerçekleşen tüketimin izlenmesi ile, bu alanlarda yürütülen faaliyetler veya yaşayan bireylerin alışkanlıkları ile ilgili bilgiler üretilebilir [15]. Bu durum kişisel mahremiyet haklarının ihlalini gündeme getirmekte olup, "bilmesi gereken" prensibi uyarınca kurumsal bilgi sistemlerinde korunması gereken gizli bilgiden daha ciddi düzeyde erişim kontrolü gerektirmektedir. Bu gereksinimin karşılanması için öncelikle gereksiz verinin toplanmaması, ikinci olarak sistem merkezinde toplanan veriye erişimin en ciddi şekilde yönetilmesi gerekir.

Üretim verilerinin bütünlüğüne ilişkin güvenlik gereksiniminin, akıllı sayaçlarda olduğu gibi uçtan uca kriptolama ile çözülebileceği, kripto algoritmasının gerçekleneceği bileşenle ilgili bütçe kısıtının akıllı sayaç kadar zorlu olmayacağı, ancak "kurcalamaya" dayanıklı yapılar konusunda Ar-Ge gereksinimi bulunduğu kaydedilmektedir [14].

5. Sonuç

Bilişim sistemlerine bağımlılığı üst düzeyde olan Akıllı Şebeke uygulamalarının devreye girmesi ile mevcut elektrik iletim ve dağıtım sistemlerine dönük bilgi güvenliği tehditlerinin çeşitlenmesi ve daha geniş bir saldırı yüzeyinden sistem merkezlerine ulaşması beklenmelidir. Bu nedenle, akıllı şebekelerin başarılı olması için bilgi güvenliği boyutunda ilave çözümlerin üretilmesi gerekmektedir. Gereksinimlerin bir kısmı ara yüz standardizasyonu kapsamında olup kurumlar arası koordinasyon ve iş birliği ile gerçekleştirilebilir. Gereksinimlerin diğer bir kısmı için ise etkin ve ekonomik ürünlerin geliştirilmesi gerekmektedir. Bu kapsamda akla gelen ilk ürün akıllı sayaçtır. Akıllı sayaçla ilgili gereksinimlerin belirlenmesi, ürün standardizasyonu, tedarik ve testi kapsamında dağıtım şirketlerinin dayanışma içinde hareket etmesinin çözüme yardımcı olacağı değerlendirilmektedir. Hem ara yüz standardizasyonu, hem de akıllı sayaç standardizasyonu kapsamında yapılacak çalışmaların yetkili bir kamu kurumu liderliğinde gerçekleştirilmesinin çözüme katkı sağlayacağı da söylenebilir.

6. Kaynaklar

[1] International Standard *ISO/IEC 13335-1 Information technology-Security techniques–Management of information and communications technology security Part 1*, Geneva, 2004

[2] Enerji ve T.K. Bakanlığı, 2011 Yılı Genel Enerji Dengesi - http://www.enerji.gov.tr/EKLENTI_VIEW/index.php/raporlar/raporVeriGir/71073/2

[3] 2010 Türkiye Elektrik Tüketim ve Dağıtım İstatistikleri - http://www.tedas.gov.tr/29,Istatistiki_Bilgiler.html

[4] *EÜAŞ Elektrik Üretim Sektör Raporu 2011* - http://www.euas.gov.tr/apk%20daire%20baskanligi%20kitapligi/Sektor%20Raporu/Sektor_Raporu_2011.pdf

[5] Hines P., Blumsack S., Sanchez E. C., Barrows C., "The Topological and Electrical Structure of Power Grids", *43rd Hawaii International Conference on System Sciences*, s1-10, 2010

[6] Uçan B., Koçak S., Aksakallı H. M., "TEİAŞ Milli Yük Tevzi SCADA/EMS Sistemi", *Türkiye 11. Enerji Kongresi*, İzmir, 2009

[7] *National Infrastructure Protection Plan*, Department of Homeland Security, 2009

[8] Stouffer K., Falco J., Scarfone K., *NIST (National Institute of Science and Technology) Special Publication 800-82 - Guide to Industrial Control Systems (ICS) Security*, Gaithersburg, 2011

[9] Byres E., Savage K., *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, CPNI, London, 2005

[10] Swanson M., Bowen P.., *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34, Gaithersburg, 2010

[11] *NIST Special Publication 1108R2, NIST Framework and Roadmap for Smart Grid Interoperability Standards*, 2012

[12] *NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, 2010

[13] Cardenas A. A., Moreno R., "Cyber-Physical Systems Security for the Smart Grid", *NISTIR 7916 Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop*, 2012

[14] *NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References*, 2010

[15] *NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, 2010