Endüstriyel Otomasyon Sistemlerinde Network Güvenliği

İlhami Muharrem ORAK [1], Uğur ÖZDEMİR [2]

[1] Karabük Üniversitesi, Bilgisayar Mühendisliği Bölümü, Karabük
[2] Kastamonu Üniversitesi, Bilgi İşlem Daire Başkanlığı, Kastamonu
imorak@karabuk.edu.tr, ugurozdemir@kastamonu.edu.tr

Özet: Endüstriyel otomasyon sistemleri için network ve haberleşme büyük bir öneme sahiptir. Sistemin işleyişi bu yapının sürekli ve güvenilir bir şekilde çalışmasına bağlıdır. Haberleşme sisteminde oluşacak aksaklıklar işlerin yavaşlamasına hatta durmasına kadar gidebilir. Ayrıca internetin hayatımızda zorunlu bir ihtiyaç haline geldiği bu günlerde sisteme içeriden ve dışarıdan gelebilecek tehlike riski de artmıştır. Bu çalışmada örnek bir otomasyon sisteminde network yapısının nasıl tasarlanacağı, güvenliğinin ne şekilde sağlanacağı ve nasıl bir yol izleneceği üzerinde durulmaktadır.

Anahtar Sözcükler: Endüstriyel Otomasyon Sistemleri, Network Güvenliği

Network Security in Industrial Automation Systems

Abstract: Network and communication have great importance for industrial automation systems. Functioning of the system depends on continuous and reliable operation of this structure. Deficiencies of the network system cause slowing down or even stopping works. In addition, the Internet has become a necessity in our lives these days also increased the risk of danger to the system from within and from outside. In this study; these are emphasized that how to design the network structure and what security will be provided to in a model automation system.

Keywords: Industrial Automation Systems, Network Security

1. Giriş

Endüstriyel otomasyon sistemleri; kaliteli ve hızlı bir üretim için proseslerin sistematik ve kontrollü olarak gerçekleştirildiği, insan gücü kullanımının en aza indirgendiği sistemlerdir. Bu sistemlerin işleyişinde haberleşme temel bileşendir. Çünkü sistemin başlangıç noktası olan mekanik sistemlerinin kontrolünden en üst seviyedeki karar destek sistemlerinin çalışmasına kadar bütün sistem; networkün sürekli ve güvenli haberleşmesi esasına bağlı olarak çalışır.

Haberleşme sistemlerindeki gözle görülür gelişmeler (özellikle internetteki gelişmeler-3G gibi) bilgiye istenilen yer ve zamanda ulaşma imkânı sunmaktadır. Endüstriyel otomasyon sistemlerinde de bu gelişmeler ışığında web tabanlı yazılım uygulamaları ve uzaktan yönetim uygulamaları kullanımı hızla artmaktadır. İnternetin sağladığı faydaların yanında eğer gerekli güvenlik tedbirleri alınmazsa sisteme dışarıdan gelebilecek saldırılarda kaçınılmaz olur.

Çalışmamızın ilk bölümünde yaygın olarak görülen network saldırı yöntemleri ele alınacaktır. İkinci bölümünde ise endüstriyel otomasyon sistemlerinin bölümleri, çalışması ve network protokolleri üzerinde durulacak, network saldırılarının endüstriyel otomasyon sistemlerini nasıl etkileyeceği ve ne gibi sonuçlar doğuracağı anlatılacaktır.

2. Network Saldırı Yöntemleri

Güvenlik önlemleri alınmadığı zaman networke ve üzerinden geçen verilere yönelik değişik saldırılar yapılabilir.

Man-in-the-Middle Saldırıları: Bu tür saldırılarda saldırgan kurban ile kurbanın gitmek istediği hedef noktası arasına girerek bütün iletişimi istediği gibi kontrol eder. Bu saldırılar birçok değişik şekilde karşımıza çıkabilir.(ARP Zehirlenmesi, DNS Ön Bellek Zehirlenmesi vb.)

ARP Zehirlenmesi: ARP saldırısı yerel ağlarda gerçekleştirilebilen bir saldırıdır. Bu saldırı, üç şekilde gerçekleştirilmektedir. Birincisi; hedef bilgisayarın ARP tablosunun yanlış bilgilerle dolmasını sağlayarak hedef bilgisayarın göndereceği paketlerin saldırganın istediği adreslere gitmesini sağlamak. İkincisi; hedef bilgisayarın göndereceği tüm paketlerin, saldırganın bilgisayarı üzerinden geçmesini sağlamak (Man in the Middle). Üçüncüsü de; hedef bilgisayarın, paketlerini bir başka bilgisayara göndermesini sağlayarak bu bilgisayara servis dışı bırakma (Denial of Service) saldırısı yapmak şeklindedir. IP-MAC eşleştirmelerini switchler üzerinde port bazlı tutarak sorunu çözebiliriz[1].

DNS Ön Bellek Zehirlenmesi: Bu saldırılarda, bir DNS sunucusuna yetkisiz bir kaynaktan veri yüklenmesi ile kullanıcıların istediği alan adlarına gittiğini zannedip önemli bilgilerini elde etmeye çalışmak veya mağdur etmek için kullanılır. Açıklık kapatılması için yaygın yazılım üreticileri tarafından çıkartılan yamaların uygulanması tavsiye edilmektedir. Yamalar uygulanamıyorsa veya yama mevcut değilse bu sunuculara erişimin kısıtlanması, yerel (internetten doğrudan ulaşılamayan) DNS önbelleğinin kullanılması, DNS sunucuları önüne saldırıyı kesebilecek Linux Iptables veya OpenBSD PF yerleştirilmesi veya tüm trafiğin yamanmış, açıklığı olmayan bir sunucuya yönlendirilmesi tavsiye edilmektedir[2].

DHCP Snooping: Bu saldırı yönteminde saldırı yapan bilgisayar ağ üzerindeki DHCP sunucusunun yerine geçiyor ve IP bilgilerini isteyen istemcilere kendi istediği bilgileri veriyor. Bu bilgilerden en önemlisi DNS sunucusu ve varsayılan ağ geçidinin IP adresi. Saldırgan bu bilgileri

değiştirerek istemcilerin bağlanmak istedikleri web sitelerinin yerine kendi istediği yere ulaşmalarını sağlıyor. Sonuçta internet bankacılığı gibi uygulamalarda kullanıcı farkına varmadan sahte bir siteye yönlendirilip şifresi çalınabiliyor[3]. Çözüm güvenilen dhcp sunucusu tanımlarının switchlere girilmesidir.

DOS (Denial of Service) Saldırıları: Bu tür saldırılarda amaç değişik hizmetler veren ağ cihazlarının (e-posta sunucusu, web sunucusu vb.) servis dışı bırakarak kullanıcılarını mağdur etmektir.

Ping of Death Saldırısı: ICMP protokolünün içerisinde bulunan ping işlemi kullanılarak varsayılan aralıktan çok daha büyük veri gönderip alınmaya çalışıldığında kurbanın bilgisayarı bu duruma cevap veremeyip hizmet dışı kalacaktır. Güvenlik duvarı üzerinden ping portunu kapatarak saldırı engellenebilir.

Ping Flooding: Bu saldırı kurbanın bilgisayarına çok fazla ping paketi gönderilerek gerçekleştirilir. Bilgisayar bir süre sonra bu isteklere cevap veremeyip hizmet dışı kalır. Bu saldırıda güvenlik duvarından ping portunu kapatarak engellenebilir.

SYN Flooding: Bu saldırıda saldırgan kullanılmayan IP adreslerini aldatma amaçlı kaynak adresi olarak kullanarak birçok SYN paketini kurbanın bilgisayarına yollar. Alınan her SYN paketi için kurbanın bilgisayarı kaynak ayırır ve onay paketini SYN paketinin yollandığı kaynak ip adresine yollar. Kurban saldırgandan yanıt alamayacağından, SYN-ACK paketini 5 kez daha göndermeyi deneyecektir. Bu işlemler her SYN paketi için gerçekleşeceğinden belirli bir süre sonra kaynaklar tükenip sistem cevap veremez hale gelecektir. Bu saldırı güvenlik duvarından SYN paketleri daha çabuk zaman aşımına uğratılarak engellenebilir.

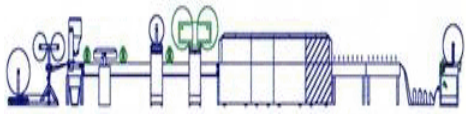
3. Endüstriyel Otomasyon Sistemleri

3.1 Bölümleri ve Genel Çalışması

Endüstriyel otomasyon sistemleri genel olarak altı bölümden oluşur.

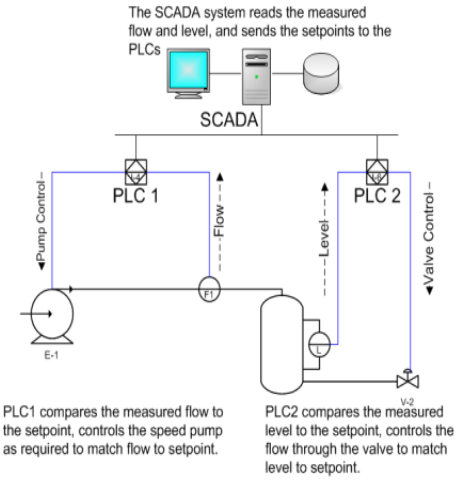
1. Mekanik Sistemler
2. Otomasyon Sistemleri
3. Proses Kontrol Sistemleri
4. Üretim Kontrol Sistemleri
5. Kaynak Planlama Sistemleri
6. Karar Destek Sistemleri

Mekanik Sistemler: Üretimin yapılabilmesi gerekli makinelerin ve mekanik elemanların (Motor, valf, pompa, yürüyen bant vb.) bulunduğu bölümdür. Sistemin çekirdeğini oluşturur. Bütün sistem bu yapıya göre şekillendirilir.



Şekil-1: Örnek Bir Mekanik Sistem

Otomasyon Sistemleri: Otomasyon sistemlerinde kullanılan PLC (Programmable Logic Controller), DCS (Distributed Control System) vb. sistemler genel olarak scada (Supervisory Control and Data Acquisition) sistemleri olarak bilinirler. Sistemin uzaktan izlenmesini ve sistem parametrelerinin kontrolünü mümkün kılan scada sisteminin temelleri 1932 yılında Automatic Electric Company'nin uzaktan kontrol ürünlerinden yola çıkarak atıldı. 1960'ların sonlarında bilgisayar tabanlı sistemlerin kullanılmaya başlanması ve 1971 yılında Intel 4004 serisi mikroişlemcilerin çıkmasıyla birlikte bilgisayar tabanlı scada sistemlerinin gelişimi devam etmiş günümüzde de hala devam etmektedir[4].



Şekil-2: Örnek Bir Scada Sistemi

Scada sistemi; mekanik sistemlerden sensörler, transducerlar vb. elektronik devre elemanları yardımıyla bilgi toplar ve bu bilgiler ışığında kontrol programları yardımıyla mekanik sistemlerin hedeflendiği gibi çalışmasını sağlar. HMI (Human-Machine Interface) kullanıcı ara yüzleri yardımıyla sistem sürekli olarak uzaktan izlenir.

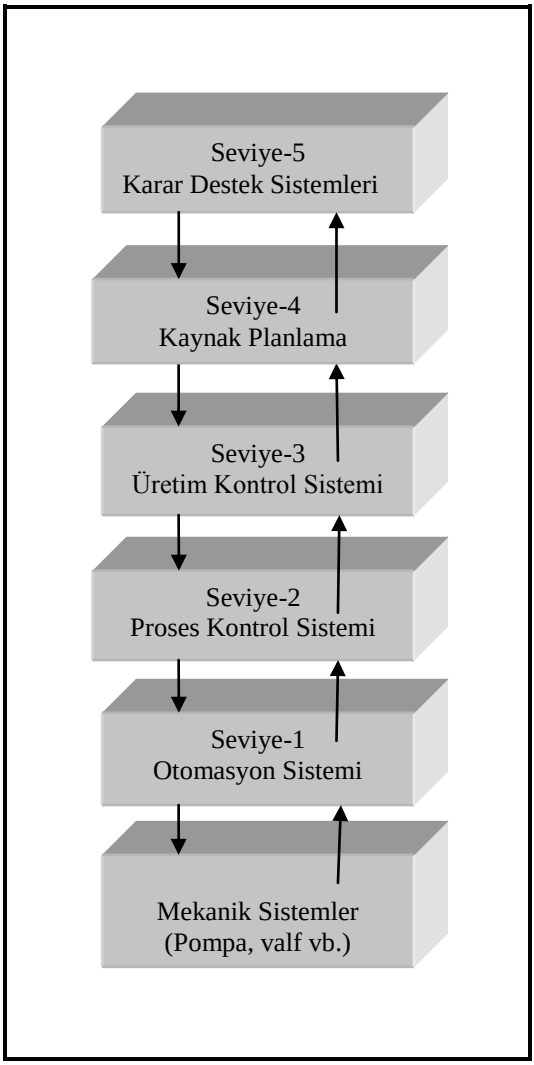
Proses Kontrol Sistemleri: Otomasyon sisteminde verilen görevlerin denetimini yapar. Bunu yaparken ileri programlama teknikleri ve veri tabanı uygulamaları kullanılır. Otomasyon sisteminin yöneticisi sürekli olarak HMI ekranından sistemi takip eder.

Üretim Kontrol Sistemleri (MES): Veri tabanı uygulamaları kullanılarak üretime yönelik raporlar alınır, bu raporlar neticesinde üretim planlaması yapılır ve sistemin optimizasyonu sağlanır. Burada da yine HMI ekranından sistem sürekli kontrol edilir.

Kaynak Planlama Sistemleri (ERP): Kümelenmiş sistemlerin ve veri tabanı uygulamalarının kullanıldığı ve üretim sonrası satış, stok kontrol, sipariş vb. işlemlerin gerçekleştirildiği bölümdür.

Karar Destek Sistemleri (DSS): Bilgilerin hızlı bir şekilde tüm sistem içerisinden aktarıldığı ve verilerin analiz edilip karar vericinin sistem üzerindeki kararlarına destek olması için kullanılan sistemlerdir.

Şekil-3'de Endüstriyel otomasyon sistemlerinin bölümleri gösterilmiştir.



Şekil-3

3.2 Endüstriyel Networkler

3.2.1 Protokoller

Endüstriyel otomasyon sistemleri ModBus/TCP, Ethernet/IP, DNP3 gibi endüstriyel network protokollerini kullanılıyor. Modbus protokolü OSI modelinin 7. Seviyesinde bulunan uygulama katmanı mesajlaşma protokolüdür. Farklı networklerde bulunan cihazlar arasında İstemci/Sunucu iletişimini sağlar. DNP3 ve ProfiBus protokolleride herhangi bir yetkilendirme veya güvenlik sorgusuna bakılmaksızın uzaktaki aygıtların kontrolüne imkan sunuyor. İnternet tabanlı endüstriyel otomasyon sistemlerinde bunlara TCP/IP protokolüde eklendi. Bu protokollerin TCP/IP protokolü ile birlikte kullanılması sisteme bir saldırgan tarafından kolay bir şekilde zarar verme fırsatı sundu[5]. Honeywell (USA), Emerson (USA), ve Siemens (German) gibi scada sistem üreticileri bu eksiklikleri kendi ürünlerinde ortadan kaldırmak için güvenlik çözümleri geliştirmeye ve aynı zamanda geleneksel IT şirketleride (CISIO, IBM, Symantec vb.) bu kritik güvenlik altyapısını sağlayabilecek ürünler sunmak için kendi güvenlik duvarı, sunucu ve güvenlik yazılımlarında yoğun çalışmalar yapmaya başladı[6].

3.2.2 Sistemin Tasarlanması ve Genel Network Mimarisi

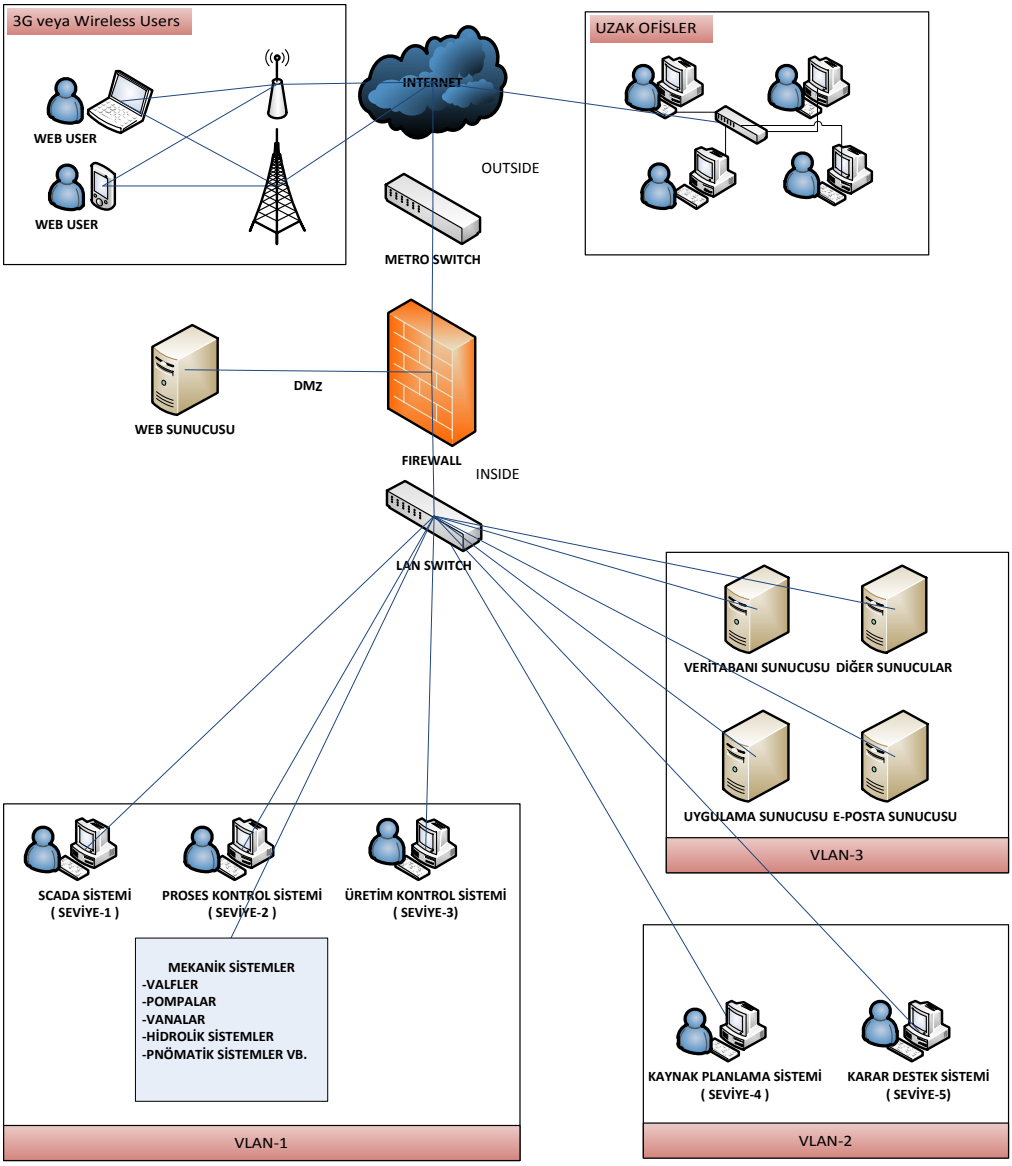
Networkte Inside, Outside ve DMZ olmak üzere üç ana bölge oluşturuldu(Şekil-4). Inside; üretim ve diğer işlerin yapıldığı güvenli bölgedir. Inside (LAN) içerisine güvenlik, broadcast kontrol ve esneklik gibi avantajlar sağladığından üç ana bölüm için ayrı birer vlan tanımlandı. Outside; İnternet üzerinden sisteme dahil olacak kullanıcıların ve uzak ofislerin bulunduğu bölgedir. DMZ; web sunucusunun bulunduğu bölgedir. Genellikle internet üzerinden yapılan saldırılar öncelikle web sunucularına oluyor. Bu yüzden farklı bir bölgede tutulması gereklidir.

LAN'ın Yapılandırılması:

- Network veri hattı ve cihazlarının fiziksel güvenliği sağlanmalı.
- Veri kaybını engellemek için veri kablo boyları standartlara uygun yapılandırılmalı.
- Networkte kullanılacak bütün cihazlar kayıt altına alınmalı.
- Cihazlar switchlerin hangi portuna bağlanacaklarsa port bazlı MAC güvenliği sağlanmalı.
- Switchlerin kullanılmayan portları yönetimsel olarak kapatılmalı.
- Switchlerde arp zehirlenmesine karşı IP-MAC listeleri oluşturulmalı.
- Switchlerde DHCP snooping saldırılarına karşı güvenilir DHCP portu tanımlanmalıdır.
- Veri tabanı ve ip tabanlı uygulamalar olacağından vlan-2 gibi alanlarda sabit ip kullanımı gereklidir.

Güvenlik Duvarı Yapılandırılması:

- Sistemde her yerden erişimin olacağı sunucuların ilgili portları (80, 110, 25 vb.) açılmalıdır.
- Dışarıdan içeriye doğru tüm portlar öncelikle kapalı olmalıdır. İhtiyaçlar doğrultusunda içeriyle (uzak ofislere ve uzak kullanıcılara) ilgili portlar sabit IP tanımlaması yapılarak açılmalı. Böylelikle dışarıdan gelen yetkisiz isteklerin filtrelenmesi sağlanır.
- Dmz üzerinden içeri gelebilecek olan scada sistemini uzaktan yönetim için gerekli portlar açılmalıdır.



Şekil-4: Endüstriyel Otomasyon Sistemlerinin Genel Network Mimarisi

3.3.4 Meydana Gelen Kazalar, Saldırılar ve Sonuçları

- Amerikada 2003 yılında nükleer düzenleme kurulu; Ohio DavisBesse nükleer santralinde operatörleri kazalar hakkında uyaran iki önemli monitör sisteminin saatler boyunca hizmet dışı kalmasına Slammer bilgisayar wormunun networke sızmasının sebep olduğunu resmi olarak duyurdu.

- 2000 yılında Maroochy Shire'da iş başvurusu reddedilen Avustralyalı bir adam atık su kontrol sistemine dizüstü bilgisayar ve kablosuz bir radio kullanarak girip intikam aldı. Milyonlarca litre atık su yerel parklara, nehirlere ve Majör otelin arazisine boşaldı.

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

-1997 yılında Beyaz Rusya da virüs araştırma şirketi olarak kurulan, **VirusBlokAda** tarafından **Temmuz 2010** da keşfedilen **Stuxnet kurtçuğu** (worm), İran-Buşehr nükleer santralindeki **SCADA** sistemlerini etkilemek için, özel amaçlar gözetilerek santralin **PLC** sistemlerini farklı frekanslarda ve motor hızlarında çalıştıracak şekilde işlevsiz hale getirmek amacıyla, **ABD Savunma Bakanlığı (DARPA) desteğiyle,** bir grup gönüllü siber savaş yazılımcısı tarafından Alman-Siemens PLC sistemlerine ait bilgi birikimi ve İsrail'in lojistiğiyle USB bellekler-diskler ile yayılacak şekilde siber silah olarak hazırlandığı tahmin ediliyor.**İran istihbarat kurumu başkanı Haydar Moslehi;** kamuya ait 30 bin kadar bilgisayarın etkilendiği bu saldırıyı, "Batılı güçlerin planladığını" İngiliz The Guardian gazetesine ifade etti.[7]

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

- 7 Nisan 1992'de Texas Branham'daki gaz boru hattında scada kontrolörü yanlış bir şekilde işlemeye başladı. Scada izleme sistemide hayli uçucu olan sıvının anormal sızıntısını algılayamadı. Bunun sonucunda ateş alan madde 3 kişinin ölümüne, 21 kişinin yaralanmasına ve 9 milyon dolar zarara sebep oldu.

- 22 Haziran 2009'da iki DC Metro treni çarpıştı. NTSB araştırması scada tabanlı otomatik tren koruma sisteminin rölantide olan bir treni algılayamamasından kaynaklandığını saptadı. Bunun sonucunda 9 kişi öldü ve 52 kişi yaralandı[8].

4.Sonuç

Endüstriyel otomasyon sistemlerinde internet tabanlı uygulamaların kullanılmaya başlanması ile klasik network sistemlerinden daha farklı bir network yapısına sahip olan bu sistemlere eksiklikleri nedeniyle içeriden ve dışarıdan yapılabilecek network saldırı riski de artmıştır. Bu sistemlere yapılacak network saldırıları üretimi yavaşlatabilir, durdurabilir ve hatta can ve mal kaybına yol açabilir. Bu sebeplerden ötürü network güvenliğini sağlamak çok önemlidir. Bunu yaparken öncelikle network iyi analiz edilmeli, güvenlik açıklarını kapatacak şekilde yapılandırılmalı ve internet tabanlı uygulamalara kontrollü bir geçiş yapılmalıdır.

KAYNAKLAR

[1] http://www.bilgiguvenligi.gov.tr/aktif-cihaz-guvenligi/ikinci-katman-saldirilari-5.html

[2] http://www.hakanuzuner.com/index.php/tag/dns-onbellek-zehirlenmesi

[3] http://www.chip.com.tr/konu/Guvenli-aglara-giden-yol-DHCP-Snooping_12045_4.html

[4] Daniel E. Nordell, P.E., Senior Member, IEEE "Communication Systems for Distribution Automation" Transmission and Distribution Conference and Exposition, 2008.

[5] I. Nai Fovino, A. Carcano, M. Masera, "A Secure and Survivable Architecture for SCADA Systems", Second International Conference on Dependability, 2009.

[6] Ning Cai, Jidong Wang, Xinghuo Yu, "SCADA System Security: Complexity, History and New Developments" , Industrial Informatics, 2008, 6th IEEE International Conference.

[7] http://www.bilgiguvenligi.gov.tr/siber-savunma/siber-savasta-yeni-cephe-iran-busehr-nukleer-santrali-ve-scada-plc-sistemler.html

[8] Robert E. Johnson, "Survey of SCADA Security Challenges and Potential Attack Vectors", Internet Technology and Secured Transactions (ICITST), 2010.