TÜRK BİLİM ARAŞTIRMA VAKFI
TÜBAV
1995
TURKISH SCIENCE-RESEARCH FOUNDATION
TUBAV BILIM DERGISI

Yıl: 2008, Cilt:1, Sayı:2, Sayfa:72-78

DAĞITIK DENETİM SİSTEMLERİNE YÖNELİK ELEKTRONİK TEHDİTLER

Şeref SAĞIROĞLU[1], İlhami ÇOLAK[2], Ramazan BAYINDIR[3], Alper ÖZBİLEN[4]

GEMEC-Gazi Elektrik Makineleri ve Enerji Kontrol Grubu
Gazi Üniversitesi, Teknik Eğitim Fakültesi, Elektrik Eğitimi Bölümü,
06500 Beşevler Ankara

Özet

Bu çalışmada, Dağıtık Denetim Sistemlerine (DDS) yönelik elektronik tehditler ve sistem güvenlik açıkları incelenmiş, tanımlanan güvenlik açıklarının giderilmesine yönelik düzeltmeler ve iyileştirmeler üzerinde durulmuştur. Çok fazla sayıda kenar birim içermesi nedeniyle elektrik dağıtım sistemlerinde kullanılan DDS'ler esas alınmakla birlikte güvenlik risklerinin azaltılmasına yönelik olarak sunulan öneriler tüm dağıtık denetim sistemleri için geçerliliğini korumaktadır.

Anahtar Kelimeler: Dağıtık Denetim Sistemleri, Güvenlik, Elektronik Saldırı, Kritik Altyapı Sistemleri

CYBER THREAD AGAINST DISTRIBUTED CONTROL SYSTEMS

Abstract

In this work, cyber thread against distributed control systems and system security vulnerabilities were investigated, the improvement and remedy methods in order to avoid security vulnerabilities were also considered. Although electricity distribution system is used as base system in many terminals, suggestions for reducing security risks were applicable for all distributed control systems.

Key Words: Distributed Control System, Security, Cyber Attack, Critical Infrastructure

[1] ss@gazi.edu.tr
[2] icolak@gazi.edu.tr
[3] bayindir@gazi.edu.tr
[4] alper.ozbilen@tib.gov.tr

1.Giriş

Elektrik, gaz, petrol, su ve telekomünikasyon sistemleri toplum yaşantısında sürekli hizmet vermesi gereken sistemler arasında olduğundan kritik altyapı sistemleri olarak değerlendirilirler. Bu sistemler arasında, özellikle elektrik üretim ve dağıtım sistemleri diğer kritik altyapılarının da işletilmesinde kullanıldığından daha kritik altyapı sistemi olarak düşünülebilir.

Amerika Birleşik Devletleri Kritik Altyapılar hakkındaki Başkanlık Raporunun 63. Başkanlık Direktifinde, kritik altyapı sistemlerinin sürekli işletiminin hayati önemi kabul edilmiş ve kullanılan dağıtık denetim sistemlerinin fiziki ve elektronik saldırılara karşı dayanıksızlığı vurgulanmıştır [1].

Elektrik enerji sistemleri, üretim, iletim ve dağıtım birimi olmak üzere üç temel altyapı bileşeninden oluşur. Özellikle elektrik dağıtım şebekesi, coğrafi olarak dağıtık binlerce birimi içeren dinamik bir sistemdir. NIST (National Institute of Standards and Technology) ve Amerikan Hükümetince yapılan araştırma ve çalışmalarda elektrik enerji sistemlerine yönelik tehditler, doğal, sosyo ekonomik ve politik olarak sınıflandırılmıştır. Doğal tehditler, doğal afet ve kazalar sonucu oluşan fiziki hasarlar olarak; sosyoekonomik tehditler, piyasa regülasyonu, rekabeti ve personel ihmal, hata, işten çıkarmalar olarak; politik tehditler, terörizm, sabotaj ve endüstriyel casusluklar olarak tanımlanmaktadır [2-5].

Doğal tehditler dışındaki diğer tüm etmenler birbirinin nedeni veya sonucu olabilecek etmenler olarak sayılabilir. Örneğin terörist bir saldırı hazırlığında, hedef görülen enerji sistemine ilişkin bilgi toplama eylemi, piyasadaki rekabet koşulları nedeniyle işten kovulan bir personel üzerinden yapılabilir.

Herhangi bir nedenle Dağıtık Denetim Sistemlerinde (DDS) oluşabilecek kesinti ve hata, üretimin veya hizmetin durmasına, altyapı elemanlarının zarar görmesine, hatta çalışan veya hizmet alan insanlarının zarar görmesine neden olabilecek boyutlara varabilmektedir.

IEEE (Institute of Electrical and Electronics Engineers) 1402-2000 sayılı standardında belirtildiği gibi, enerji santrallerindeki röle koruma, denetim ve bilgi toplama sistemlerine bilgisayarlar yardımıyla uzaktan erişilmesi, kullanılan bilgisayar sistemlerinin sahip olduğu tüm zafiyetlerden enerji sisteminin de etkilenmesi sonucunu doğurmaktadır [6]. Bu nedenle, elektrik enerji sistemlerine yönelik yukarıdaki tehditlere, bilgisayar sistemlerin tabi olduğu elektronik tehditler de ilave olmuştur.

2.Dağıtık Denetim Sisteminin Temel Bileşenleri

Dağıtık Denetim Sistemleri temel olarak üç bileşenden oluşurlar. Bunlar, *Merkez Birim* (Master Station), *Kenar Birim* (Remote Terminal Unit) ve *İletişim Birimleridir* [7].

Kenar birim, DDS'nin izlenmesi ve kumanda edilmesi gereken tüm birimlerine yerleştirilen bileşenler olup karar verme mekanizmalarına sahip değildirler. Donanımsal ve yazılımsal bileşenleri kısıtlı olup gerçek zamanlı ve önceden tanımlı işlemleri yürütmek üzere tasarlanmışlardır.

Merkez birim, işlemci, belek, disk ve ağ ara yüzlerinden oluşan bilgisayar donanımları ile genel veya özel amaçlı bir işletim sistemi ve onun üzerinde koşan DDS yazılımlarından oluşur [7].

DDS merkezi birim yazılımı genel olarak şu iki fonksiyonu yerine getirmek üzere tasarlanır. Birincisi, kenar birimlerden alarm ve verileri toplayıp işlemek ve bunları raporlamak üzere saklamaktır. Diğer temel fonksiyonu ise, kenarlardan toplanan veriler değerlendirerek tekrar kenar birimlere gönderilmek üzere uygun komutlar üretmektir [7]. Farklı kenar birim ve merkez birim üreticilerinin ürünlerinin birlikte çalışabilirliğini sağlamak amacıyla çeşitli DDS standartları yayınlanmıştır [8].

İletişim birimleri, merkez ve kenar birimler arasındaki haberleşmeyi sağlayan erişim ortamlarını ve haberleşme protokollerini kapsar. DDS'ler için iletişim birimlerinin gerçek zamanlı ve kesintisiz aktarım yapabilme şartlarını her durumda sağlamaları beklenir. İletişim birimleri için alınacak her türlü güvenlik tedbirlerinin bu iki şartı sağlaması önemlidir.

Takip eden bölümlerde merkez, kenar ve iletişim birimlerinin karşı karşıya olduğu elektronik tehditler ve bu tehditlere yönelik temel tedbirler açıklanmıştır.

3.DDS'lere Yönelik Elektronik Tehditler ve Temel Tedbirler

Birçok DDS ağı, başlangıçta DDS işletmecisine ait diğer bilgisayar ağlarından ayrı ve izole olarak kurulmuşken, DDS merkez ve kenar birimlerine uzaktan erişim ihtiyacının ortaya çıkmasıyla her iki ağ birlikte kullanılır hale gelmişlerdir [8]. DDS mimarileri, internet ve mobil erişim tekniklerinin yaygınlaşmasında ile bu erişim kolaylığı ve çeşitliliğinden daha fazla etkilenmeye başlamışlardır [9].

DDS'ler için en temel elektronik tehditler aşağıda sıralanmıştır:

- Uzaktan yetkisiz erişim,
- Güvensiz iletim ortamlarında komut ve verilerin şifresiz aktarımı,
- Kullanılan yazılımların (işletim sistemleri ve uygulama programlarının) açıkları.

Yukarıda sayılan elektronik tehditlerin kaynağı olan güvenlik açıkları ve bu açıkların giderilmesine yönelik tedbirler, *iletim ve erişim güvenliği*, *işletim sistemi ve yazılım güvenliği*, *iletişim protokolü güvenliği* olmak üzere üç başlık altında incelenmiştir.

3.1.İletim ve Erişim Güvenliği

İlk DDS'lerde, farklı birimler arasında haberleşme için *RS-232 (Recommended Standard 232)*, *RS-422* ve *RS-485* seri haberleşme standartları kullanılmıştır. Bu sayede, her birim bağlı olduğu diğer birimle özel bir hat üzerinden haberleşiştir [10]. Günümüz DDS sistemlerinde ise, farklı uçlar arasındaki iletişim kablolu veya kablosuz ethernet bağlantısı, kiralık hatlar veya mevcut internet bağlantıları üzerinden yapılmaktadır [11]. Ancak kullanımına devam edilen geçmiş DDS kenar birim cihazları ile haberleşmek için seri haberleşme standartları günümüzde de kullanılmaktadır.

Seri haberleşme biçiminde, her birim iletişime geçeceği diğer bir birime tahsisli hatlar üzerinden bağlıdır [10]. Her bir haberleşme hattının fiziksel olarak diğerlerinden izole olması bir anlamda iletişim güvenliğine katkı sağlar. Ancak seri haberleşme ara yüzleri için tanımlanmış ilave bir güvenlik fonksiyonu bulunmamaktadır. Örneğin uçlar arasındaki mesajlar şifresiz olarak gönderilir ve birimlerin birbirlerine gönderdiği komutlar herhangi bir yetkilendirme mekanizmasına tabii tutulmadan kabul edilirler [11]. Ayrıca seri haberleşme standartlarının desteklediği kanal kapasitesi ve erişim fonksiyonları da oldukça kısıtlıdır.

DDS bileşenlerine yapılabilecek yetkisiz erişimlerin önlenmesi, sistem güvenliği açısından anahtar rol oynamaktadır [9]. Hem geçmiş seri haberleşme birimleri için hem de günümüz ethernet ağ ara yüzleri için erişim denetimi ayrı bir mekanizma üzerinden gerçekleştirilebilmektedir.

DDS'lerde yetkilendirme mekanizmasının eksikliklerinden ötürü ortaya çıkan güvenlik zafiyetlerine birçok güncel çalışmada değinilmektedir [11-16]. Bu çalışmalarda genel olarak sunulan önlemler aşağıda özetlenmiştir.

Her Birime Ait Şifre: DDS birimlerine ortak ve kolay şifre verilmemesi ve verilen şifrelerin önceden belirlenmiş politikalara uygun olarak düzenli olarak değiştirilmesi.

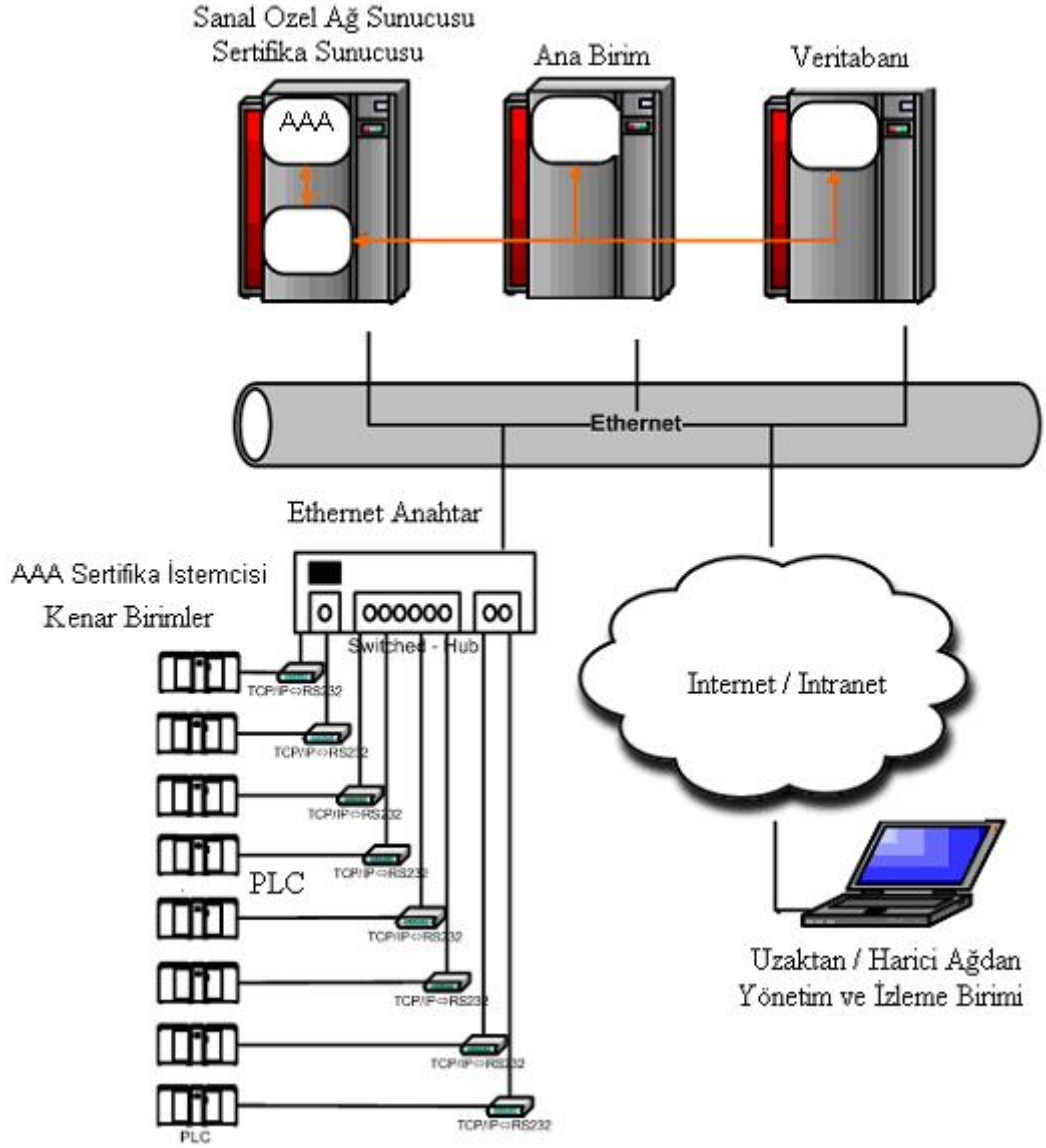
Erişim Kayıt Defteri: Merkez ve kenar birimlere yapılan her türlü bağlantı denemesinin ve erişiminin kayıt altına alınması ve bu kayıtların belirli bir süre için saklanması. Ayrıca, tutulan bu kayıtların incelenerek anormallik durumlarının raporlanması.

Sanal Özel Ağ: Tahsisli veya paylaşımlı her türlü erişim ve iletim ortamı için, verilerin şifrelenerek gönderilmesine imkan tanıyan *Sanal Özel Ağların* (Virtual Private Networks) kullanılması.

Güvenli Çevirmeli Modemler: Günümüzde erişim yedekliği için kullanılan çevirmeli modem erişimleri için numara kısıtlama, güçlü şifre sorma vb. tekniklerin kullanılması.

Açık Anahtar Altyapısı (AAA): Bilginin gizliliği ve bütünlüğünün sağlanması, alıcı tarafından inkâr edilememesi ve her türlü erişimin yetkilendirilmesini sağlamakta kullanılan teknoloji ve politikalar bütünü olan AAA'nın, DDS'lerde kenar ve merkez birimlere seviyelendirilmiş ve yetkilendirilmiş erişim imkânı sağlamakta kullanılması.

Şekil-1'de erişim kayıt defteri, AAA ve sanal özel ağ kullanan ethernet tabanlı DDS ağı gösterilmiştir. Oman ve arkadaşlarının [17-18] belirttiği gibi, uzaktan erişilebilen enerji istasyonları için, DDS sistemlerin güvenlik açıkları



Şekil 1. AAA ve Sanal Özel Ağ Kullanan DDS ağı

daha da önem kazanan bir konudur. Uzaktan erişimin güçlü denetimi, DDS'lere ait birçok açığın dış kaynaklarca kullanımını engelleyecek en etkin tedbirler arasındadır.

3.2.İşletim Sistemi ve Yazılım Güvenliği

DDS kenar birimlerinde çoğunlukla gömülü işletim sistemine ve gerçek zamanlı denetim fonksiyonlarına sahip cihazlar kullanılmaktadır [19]. Bu cihazlar, genel maksatlı işletim sistemlerine kıyasla daha az güvenlik fonksiyonuna sahip olmakla birlikte, mikro çekirdek mimariye sahip olduklarından daha az sistem açığı barındırırlar.

DDS ana birimler, çoğunlukla üzerinde UNIX veya Microsoft Windows gibi genel amaçlı işletim sistemi bulunan standart bilgisayarlar üzerinde koşmaktadır. Geleneksel DDS ana birim makinelerinde çoklu görev yeteneğine sahip UNIX işletim sistemleri kullanılırken, günümüzde daha çok Microsoft Windows işletim sistemleri tercih edilmektedir. Ayrıca, maliyet avantajı sağlayan ve UNIX tipi özelliklere sahip olan LINUX işletim sistemi de ciddi bir alternatif olmaya başlamıştır [20].

UNIX ve UNIX tipi işletim sistemi olan LINUX işletim sistemleri, çok işlemli ve çok kullanıcılı işletim sistemleridir. Ancak, yürüttükleri her bir süreç için sistem kaynaklarını zamana göre paylaştırdıklarından ötürü gerçek zamanlı işletim sistemi sınıfına girmemektedirler. UNIX ve LINUX türü işletim sistemlerinin zaman paylaşımlı süreç yönetimi, DDS uygulamaları için engel olarak görülmektedir [21]. Ancak günümüzde farklı UNIX türleri ve LINUX dağıtımları için gerçek zamanlı süreç yönetimi fonksiyonları eklenmektedir.

Bilgisayar donanım maliyetlerinin düşmesiyle birlikte, günümüz DDS kenar birimlerinde geçmişe oranla yüksek işlem kapasitesine sahip donanımlar üzerinde Microsoft Windows veya LINUX gibi genel amaçlı işletim sistemleri kullanılmaya başlanmıştır. Gömülü işletim sistemlerine göre çok daha fazla çekirdek kodu ve servis içeren bu işletim sistemleri, DDS'ler için ciddi tehdit oluşturmaktadır [22].

Genel amaçlı işletim sistemleri ve onların açıkları hakkında internet ortamında birçok bilgi ve dokuman bulunmaktadır. Ayrıca bu tür işletim sistemlerine yönelik olarak hazırlanan virüs, solucan, truva atı ve zararlı kodların fazla ve yaygın oluşu, genel amaçlı işletim sistemlerinin DDS'lerde kullanımının ciddi risk oluşturabileceği göstermektedir.

Tıpkı kurumsal bilgisayar ağlarında olduğu gibi, DDS'lerde kullanılan genel veya özel amaçlı işletim sistemlerinin güvenlik yamalarının düzenli olarak yapılması ve kullanılan anti-virüs sisteminin virüs imzalarının sürekli güncellenmesi, sistem güvenliği açısından mutlaka gereklidir [23- 24].

Sanz ve Arzen'e göre [9], DDS sistemlerde kullanılan işletim sistemlerinin ve işletim sistemleri üzerinden koşan süreç yönetimine ilişkin denetim uygulamalarının sahip olması gereken özellikler şunlardır:

Zaman Kritik Süreç Yönetimi: Yazılımlar yüksek performanslı olmalı ve gerçek zamanlı süreçlere göre tasarlanmalıdır.

Gömülülük: Yazılımlar, kısıtlı işlem kaynağına sahip platformlar üzerinde çalıştırılabilmeli ve harici çevre birimleriyle etkileşime geçebilmelidir.

Hata Toleransı: Yazılımlar, sistemde bir hatanın meydana gelmesi durumunda da belirli bir performansta çalışmaya devam edebilmelidir.

Dağıtıklık: Yazılım bileşenleri dağıtık olmalı ve farklı bileşenler farklı bilgisayarlar üzerinde ortak bir işlemi yürütebilme özelliği sahip olmalıdır.

Açıklık: Yazılımlar, kapalı olmamalı ve farklı uygulamalarla birlikte kullanılabilmelidir.

Heterojenlik: Yazılımlar, farklı işletim ortamlarında çalıştırılabilmelidir.

Yukarıda verilen özellikler, DDS sistemlerinin güvenilir işletimi açısından önemlidir.

3.3.İletişim Protokolü Güvenliği

DDS'lere ait denetim birimlerinin birbirleriyle haberleşmesinde, Tablo-1'de verilen protokoller kullanılmaktadır.

DDS'ler gerçek zamanlı işlemler yürüttüğünden ötürü verilerin kaybolması ve gecikmesine karşı toleransı olmayan sistemlerdir. Bu nedenle, denetim birimlerinin birbirleriyle haberleşmesinde Tablo-1'de verilen ve DDS'lere özgü tasarlanan iletişim protokollerden biri veya birkaçı kullanılır. Ancak bu protokollerin tasarımında, DDS güvenlik gereksinimleri yeterince dikkate alınmamıştır [9, 24-25]. Bu nedenle, iletişim kanalarına sızılması durumunda, DDS iletişim protokollerinin taşıdıkları veri ve komutların elde edilmesi veya değiştirilmesi mümkün olabilmektedir.

Tablo-1'de verilen iletişim protokollerinin içerdikleri güvenlik açıkları kullanılarak DDS'lere yapılacak saldırılara karşı koymak için kullanılan güvenlik duvarları ve saldırı tespit sistemleri, aynı zamanda verinin zamanında ulaşmasını geciktiren unsurlardır. Bu nedenle güvenlik duvarı ve saldırı tespit sistemleri zaman kritik süreçler yöneten DDS'ler için ayrıca bir risk oluşturabilmektedir [24].

Tablo 1. DDS İletişim Protokolleri [9]

DDS İletişim Protokolü	**Organizasyon / Standartlar**
Ethernet /IP	Open DeviceNet Vendors Association www.odva.org
ControlNet	ControlNet International www.controlnet.org
PROFIBUS	IEC Standard11674 ve 61158 www.profibus.org
MODBUS TCP/IP	MODBUS-IDA www.modbus.org
DNP3	IEC Technical Committee 57 Working Group 03 Standard
Foundation Fieldbus	The Fieldbus Foundation Open Standart Protocol www.fieldbus.org

Stamp ve arkadaşlarının [26] da belirttiği gibi DDS iletişim protokollerini tanıyan az sayıda ticari güvenlik duvarları ve saldırı tespit sistemleri bulunmaktadır. Günümüzde Tablo-1'deki iletişim protokollerinden bir veya birkaçını tanıyan güvenlik duvarı tasarımları da devam etmektedir. DDS iletişim protokollerinin açıklarına yönelik imza desteği veren saldırı tespit sistemlerinin geliştirilmesi DDS sistemlere yönelik elektronik tehditlerin indirgenmesi açısından her geçen gün daha fazla önem kazanmaktadır.

4.Sonuçlar

Bu çalışmada, sürekli ve doğru işletilmesi gereken, kesinti veya hata durumunda üretimin veya dağıtım hizmetlerinin durmasına, hatta ciddi hata veya kasıt durumunda işleten ve hizmet alan insanların fiziki zarar görmesine neden olabilecek kritik altyapı şebekelerinde kullanılan dağıtık denetim sistemlerine yönelik elektronik tehditler incelenmiştir.

DDS'lerin tüm bileşenleri dikkate alındığında en önemli tehdit, sistemin tümünü izleyen ve kontrol eden merkezi birimin açıklarından kaynaklanan risklerin giderilmemesidir. Merkezi birimin çalışmasının aksatılması veya yetkisizce yönetilmesi tüm sistemin durmasına veya zarar görmesine neden olabilir. Diğer yandan bir veya birkaç kenar birime yönelik yetkisiz müdahale sistemin bir kısmının durması veya zarar görmesiyle sonuçlanacaktır. Ancak bu çalışma kapsamında, bileşenler arasında bir önem sıralamasına gidilmeden sistem bir bütün olarak ele alınmış ve güvenlik tedbirleri sistemin bütününe yönelik riskleri azaltmak üzere önerilmiştir. Yeni bir DDS tasarlanırken veya mevcut bir sistem güncellenirken, bu çalışma kapsamında sıralanan elektronik risklerin göz önünde bulundurulmasında ve önerilen güvenlik tedbirlerinin alınarak birçok tehdidin en baştan engellenmesinde fayda olacaktır.

İletişim, erişim ve yazılım güvenliğine ilişkin fonksiyonları içermeyen ürünlerden oluşan DDS'ler için güvenlikten bahsetmek mümkün değildir. Ancak güncel ürünlerin büyük bir kısmında bu çalışmada bahsedilen güvenlik fonksiyonlarının bir kısmının veya tamamının desteklendiği görülmektedir. Bu fonksiyonların etkin biçimde kullanılması ise kurulum, güncelleme ve kullanıma ilişkin güvenlik politikalarının önceden belirlenmesiyle mümkün olacaktır.

Gelişen ve ucuzlayan bilgisayar teknolojisi sayesinde, DDS merkez ve kenar birimlerinde standart bilgisayar donanımı ve yazılımı kullanılmaya başlanmış ve bu durum DSS sistemler için daha önce var olmayan yeni elektronik tehditlerin ortaya çıkmasına neden olmuştur. Ayrıca, internetin ve mobil erişim tekniklerinin yaygın kullanımı ile DDS mimarileri bu erişim kolaylığı ve çeşitliliğinden daha fazla etkilenmeye başlamıştır.

Günümüz DDS'lerinin maruz kalabileceği elektronik tehditler, bilgisayar sistemlerin tabi olduğu elektronik tehditlerden farklı değildir. Ancak kritik altyapılarda kullanılan DDS'deki kesinti veya hataların maliyetleri çok daha ağır olabileceği kolaylıkla öngörülebilir.

Başta Amerika Birleşik Devletleri olmak üzere, birçok batılı ülkede DDS'lerin karşı karşıya olduğu tehditler ve bu tehditlerin giderilmesine yönelik önlemler üzerine çeşitli kamu kurumları ve enstitülerce sürekli araştırmalar yapılmaktadır. Ülkemizde DDS'lere yönelik elektronik tehditler konusunda farkındalığın geliştirilmesi ve bu çalışmada sunulan çözüm önerilerinin ülkemizdeki kritik altyapı denetim sistemlerinde uygulanması gereklidir.

Kaynaklar

[1] Critical Foundations Protecting America's Infrastructures, "*Report of the President's Commission on Critical Infrastructure Protection*", (1997), (http://www.fas.org/sgp/library/pccip.pdf).
[2] Fraser, R., "*Process Measurement and Control - Introduction to Sensors, Communication, Adjustment, and Control"*, Prentice-Hall, Inc., (2001).
[3] National Security Telecommunications Advisory Committee Information Assurance Task Force, *"Electric Power Risk Assessment"*, (1997), (http://www.ncs.gov/n5_hp/Reports/EPRA/electric.html).
[4] The White House Office of the Press Secretary, *"White House Communications on Critical Infrastructure Protection"*, (1997), (http://www.julieryan.com/Infrastructure/IPdoc.html).
[5] U.S. National Institute of Standards and Technology, *"Introduction to Computer Security: The NIST Handbook"*, NIST, Dept. of Commerce, (1994).
[6] IEEE Power Engineering Society, "*IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security*", IEEE, New York, NY, (2000).
[7] McDonald, J.D., "*Developing and Defining Basic SCADA System Concepts*", 37th Annual Rural Electric Power Conference, (1993).
[8] Amanullah, M.,Kalam, A., Zayegh, A., "*Network Security Vulnerabilities in SCADA and EMS*", Transmission and Distribution Conference and Exhibition: Asia and Pacific, IEEE/PES 2005,1 – 6, (2005).
[9] Sanz, R., Arzen, K., "*Trends in Software and Control*", Control Systems Magazine, IEEE Volume 23, Issue 3, Page(s):12 – 15, (2003)
[10] Brown T., "*Security in SCADA systems: How to Handle The Growing Menace to Process Automation*", Computing and Control Engineering, (2005).
[11] Ralston,P.A.S., Graham,J.H.,Hieb J.L., "*Cyber security risk assessment for SCADA and DCS networks ISA Transactions*", Volume 46, Issue 4, Pages 583-594, (2007).
[12] Fernandez J., Fernandez A., "*SCADA systems: Vulnerabilities and Remediation*", Journal of Computing Sciences in Colleges, 20(4):160–8, (2005).
[13] Igure V., Laughter S., Williams R., "*Security Issues in SCADA Networks*", Computers & Security, 25(7):1–9, (2006).
[14] Kropp T., "*System Threats and Vulnerabilities*", Power and Energy Magazine, 4(2):46–50, (2006).
[15] Smith C., "*Connection to Public Communications Increases Danger of Cyberattacks"*, Pipeline and Gas Journal, 230(2):20–4, (2003).
[16] Watts D., "*Security & Vulnerability in Electric Power Systems*", 35th North American Power Symposium, Page(s): 559–66, (2003).
[17] Oman, P., Schweitzer, E., Frincke, D., "*Concerns about Intrusions into Remotely Accessible Substation Controllers and SCADA systems*", Proceedings of the Twenty-Seventh Annual Western Protective Relay Conference, (2000).
[18] Oman, P., Schweitzer, E., Roberts, J., "*Protecting the Frid From Cyber Attack – Part 1: Recognizing Our Vulnerabilities*", Utility Automation & Engineering T&D, vol. 6(7), pp. 16–22, (2001).
[19] Igure, V., Laughter S., Williams R., "*Security Issues in SCADA Networks*", Computers & Security, 498-506, (2006).
[20] Chikuni, E., Dondo, M., "*Investigating the Security of Electrical Power Systems SCADA*", AFRICON 2007, Page(s):1, (2007).
[21] Qizhi, C., Qinquan, Q., "*The research of UNIX platform for SCADA*", Power Engineering Society Winter Meeting, 2000. IEEE Volume 3, Page(s):2041 - 2045 vol.3, (2000).
[22] Hentea, M., "*Improving Security for SCADA Control Systems*", Interdisciplinary Journal of Information, Knowledge, and Management Volume 3, (2008).
[23] Tanenbaum, A., Herder, J., Bos, H., "*Can we make operating systems reliable and secure*", IEEE Computer, 39(5), 44-51, (2006).
[24] Haji, F., Lindsay, L., Song., S., "*Practical Security Strategy for SCADA Automation Systems and Networks*", Electrical and Computer Engineering Canadian Conference, Page(s):172 – 178, (2005).
[25] Kropp, T., "*System Threats and Vulnerabilities: an EMS and SCADA Security System Overview"*, IEEE Power & Energy Magazine, pp.46-50, (2006).
[26] Stamp J., Campbell P., Depoy J., Dillinger J., Young W., "*Sustainable Security for Infrastructure SCADA*", Sandia National Laboratories Report SAND2003-4670, Power Systems Conference I -179, (2003).