AKILLI ŞEBEKELERDE AĞ GÜVENLİĞİ
NETWORK SECURITY IN SMART GRIDS

Gökhan Bölük
Siemens San. Tic. A.Ş Altyapı & Şehirler Akıllı Şebekeler Enerji Otomasyonu Ar-Ge Grubu
gokhan.boluk@siemens.com

ÖZETÇE

Akıllı şebekeler, elektrik enerjisinin kesintisiz ve en az maliyetle kullanıcıya arz edilmesini mümkün kılmakta ve elektrik enerjisi dağıtım şebekelerinin özelleşmesi ile birlikte enerji otomasyonu çözümlerinde daha fazla önem kazanmaktadır. Enerji otomasyonu çözümlerinde siber güvenlik, uzaktan erişilebilir ve kontrol edilebilir sistemlerde teknolojinin hızla gelişmesi ile daha da önemli olmaktadır. Bir enerji şebekesinin siber güvenliğinin sağlanması için, Siemens bünyesindeki Spectrum Power çözümlerine entegre olarak siber güvenlik çözümleri geliştirilmektedir. Bu çözümlerle temel olarak ağ üzerinde kurulan tüm bağlantı oturumları analiz edilerek her bir oturumun güvenilir olup olmadığı tespit edilebilmekte, ayrıca tüm oturumlar loglanabilmekte ve güvenli olmayan oturumlar sonlandırılabilmektedir. Böylece enerjinin kesintisiz ve güvenilir bir şekilde en uçtaki kullanıcıya ulaşması sağlanabilmektedir.

ABSTRACT

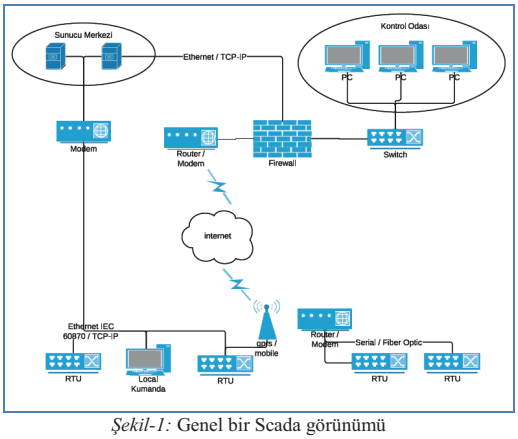
Smart grids enable providing electrical energy to the consumer uninterruptedly and with the least cost and they become more of an issue in energy automation solutions along with the privatization of electricity distribution networks. Cyber security in energy automation solutions becomes even more important when the system can be accessed and controlled remotely with the rapid development of technology. To ensure cyber security of an energy grid,cyber security solutions integrated with Siemens Spectrum Power solutions are developed. With these solutions, basically, all the established connections on the network are analyzed to check whether each connection session is reliable or not. Furthermore, all sessions can be logged and non-secure sessions can be terminated. Thus, the continuous and reliable transmission of the energy to the end-user can be ensured.

1. GİRİŞ

Ağ güvenliği yazılımları, internet kullanımının artması ve özellikle Supervisory Control And Data Acquisition (SCADA) şebekelerinin internete bağlanması ile bu şebekelere yapılabilecek saldırılar sonucu ihtiyaç duyulan en önemli konulardan biri haline gelmiştir. Bununla birlikte kurum ya da kuruluşların sahip oldukları ve tüm dünyaya açık tuttukları mail, DNS, veritabanı gibi sunucularının saldırılara maruz kalabilecekleri ihtimali yine ağ güvenliği yazılımlarına ihtiyaç duyulmasına sebep olmaktadır. Kurumların sahip oldukları çalışan sayısı ve bu çalışanların kendi kurumlarındaki kritik değer taşıyan yapılara saldırabilme ihtimalleri de iç networkün ya da tek tek kritik sunucuların kontrol altında tutulma gerekliliğini beraberinde getirir.

2. SCADA

SCADA, genel olarak kritik altyapıdaki datanın üretilmesinin, işlenmesinin ve denetlenmesinin izlenmesi gibi işlemlerin bilgisayarlar, sensörler ve haberleşme cihazları kullanarak adım adım takibini oluşturulan bir sistemdir. Enerji sektöründe Elektrik-Su-Doğalgaz altyapılarında veya bir üretim faaliyetinde SCADA isminin duyulması artık kaçınılmazdır. Son teknolojik gelişmeler esas alındığında SCADA sistemlerinde kullanılan haberleşme cihazlarının, işçi maliyetine gore daha uygun olması, bu sistemlerin kullanımının teknik olmasının yanı sıra ekonomik olmasını da sağlamaktadır. Örneğin, elektriğin üretilmesinde/dağıtılmasında, şebekenin uzaktanizlenebilmesi, hızlı ve etkin bir biçimde müdahale edilebilmesi, bu sistemleri tartışmasız daha güvenilir, daha kaliteli ve kesintisiz veya minimum kesintili duruma getirir. Üstelik, bu sistemdeki bilgilerin arşivlenebilmesi, istatistiksel olarak incelenmesi açısından muazzam kolaylıklar sağlar. Örnek bir SCADA şeması Şekil-1 de gösterilmiştir.



Şekil-1: Genel bir Scada görünümü

3. AĞ GÜVENLİĞİ

Özel eşyaların çalınma riskine karşı, bir evin veya işyerinin güvenliğine nasıl önem veriliyorsa network dünyasındaki özel bilgilerinizin çalınma riskine karşı da bilgisayar ağının güvenliğine o derece önem verilmesi gerekir. Ağınızı hırsızlıktan, gizli bilgilerinizin yayılmasından, internet dünyasında çok sık karşılaşılan trojan veya virüs gibi

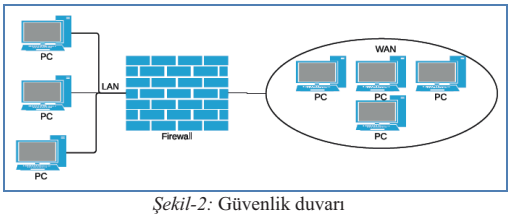
tehlikelerden korumak için ağ güvenliği teknolojisi kullanmak bir zorunluluk haline gelmiştir. Bu teknolojilerin kullanılmadığı ağlara, yetkisiz sızma, network paketleri ile ağa zarar verme, bant genişliğini şişirme, hatta adınıza yapılmış saldırılar yüzünden yasal işleme maruz kalma gibi problemlerle karşılaşılabilir.

Ağ güvenliği teknolojisinden; bir ağın normal trafiğinden yola çıkarak, içeriden ve dışarıdan gelebilecek bir saldırı olduğu taktirde olağanüstü durumu algılayıp, bilinen bir saldırı ise önlem alabilmesi ve loglama yapabilmesi veya yeni bir saldırı tipi ise loglayarak anormal durumu kullanıcıya bildirmesi beklenmektedir. Bir ağ trafiğinin saldırı olup olmadığına karar verilmesi için saldırı tespit sistemleri, (Intrusion detection system IDS), eğer bir saldırı tespit edilmişse bu saldırıdan korunması için ise saldırı koruma sistemleri (Intrusion prevention system IPS + FIREWALL) gerekmektedir.

Akıllı şebeke uygulamalarında; kullanılacak olan sistemler ve çözümler, bazı dünya standartlarını da kapsamalıdır. Bu sebeple bu yazılımlar gerçekleştirilirken müşteri isterleri göz önüne alındığı gibi bu standartların kısıtları da göz önüne alınmıştır.[1][2]

3.1. Güvenlik Duvarı (Firewall)

Sunucunun bağlı olduğu lokal network ile internete açılan dış network arasında gelen giden trafiğin geçişinden sorumlu olan yazılım veya cihazlardır. Bir networke güvenlik duvarı kurulduğunda kurallar tablosu ile trafik üzerinde etkin rol oynanabilir. Güvenlik duvarının arkasındaki networke kimlerin girip giremeyeceği, girenlerin neler yapabilip yapamayacağı güvenlik duvarı sayesinde kontrol edilir[3]. Ayrıca lokal ağdan dışarıya bağlanmak isteyen bir IP adresini maskeleyerek (Ağ adresi dönüştürme) dış ağda lokal ağa ait topoloji yapısını ve lokal IP adres bilgilerini saklamış olur. Gelişmiş bir güvenlik duvarı, olup biteni kaydedebilme ve gerektiği durumlarda alarm üretebilme yeteneğine sahiptir.



Şekil-2: Güvenlik duvarı

Güvenlik duvarları, gelen giden paketlerin içeriği ile ilgilenmezler. Dolayısıyla bu tarz bir açığı kapatmak isteyenler için başka güvenlik sistemleri ile entegre çalışabilmektedirler. Örneğin; bir bilgisayara büyük boyutlu ICMP (Internet Control Message Protocol) paketleri çok sık gönderilirse firewall bu paketlerin geçişine izin verir. Ancak bu paketlerin güvenlik duvarları ile entegre çalışan başka bir sisteme yönlendirildiği taktirde bunun bir saldırı olduğu tespit edilir ve güvenlik duvarına bu paketin geçişine izin vermemesi konusunda bilgi gönderilir.

Sonuç olarak güvenlik duvarları, ağ için olmazsa olmazlardandır, fakat tek başına tam bir güvenlik için yeterli değildir.

3.2. Saldırı Tespit Sistemleri (IDS)

Saldırı tespit sistemleri, sunucu tabanlı ve ağ tabanlı olarak iki farklı yöntemde uygulanabilir.

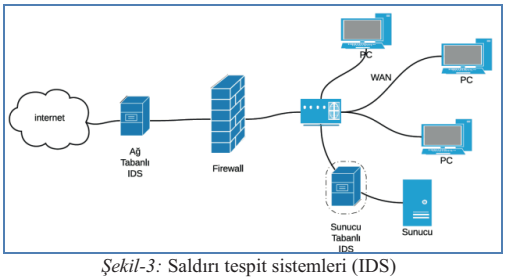
3.2.1. Ağ tabanlı IDS

Ağ tabanlı IDS, bir ağa ait tüm trafiği algılayarak, bu ağ üzerinden geçen her bir data paketini analiz eder. Bu paketin güvenli olup olmadığına karar vererek ağ güvenlik uzmanını bilgilendirir. Ayrıca arşiv kayıtları ve raporlar oluşturur. IDS bir data paketinin saldırı amaçlı olup olmadığını, kendi saldırı veritabanında bulunan saldırı türleriyle karşılaştırarak anlar.[4]

3.2.2. Sunucu tabanlı IDS

Ağ tabanlı IDS in yaptığı tüm işlemleri, üzerinde kurulu olduğu tek bir sunucu için yapar. İlgilendiği paketler, sadece o sunucuya gelen paketlerdir.

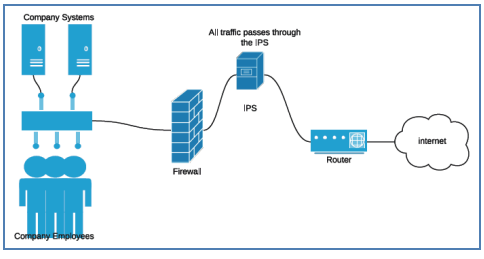
Şekil-3'te,ağ tabanlı IDS'e bir örnek gösterilmektedir. IDS, sunucu-switch arasına konumlandırıldığı taktirde sunucu tabalı bir koruma yöntemi olacaktır.



Şekil-3: Saldırı tespit sistemleri (IDS)

3.3. Saldırı Koruma Sistemleri (IPS)

Sadece güvenlik duvarı ile bir sisteme yapılan saldırıları tespit etmek veya engellemek mümkün değildir. Çünkü güvenlik duvarı, üzerinden geçen paketleri incelemez. Sadece tablosundaki kurallar yardımıyla bir paketin geçip geçmeyeceği ile ilgilenir. İşte bu noktada kendisine gelen paketi inceleyebilecek, gerektiği zaman önceki paketler ile bu paketi kıyaslayabilecek, şüpheli bir durum varsa geçişine izin vermeyerek sistemi koruyacak ikinci bir güvenlik uygulamasına ihtiyaç duyulacaktır.Network dünyasında bu işleri yapan uygulamalara Saldırı Koruma Sistemleri (IPS) denilmektedir.



Şekil-4: Saldırı koruma sistemleri (IPS)

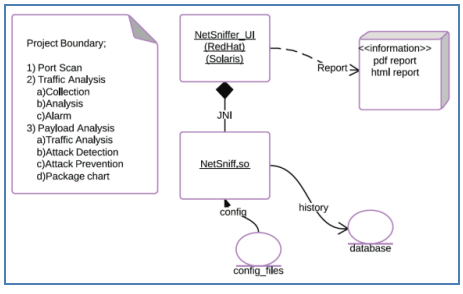
4. AKILLI ŞEBEKELERDE AĞ GÜVENLİĞİ UYGULAMALARI

Yukarıda saldırı tespit ve koruma sistemlerinin temel özelliklerinden bahsedilmiştir. Bir güvenlik yöneticisi, sorumlu olduğu ağı korumak için bu temel özellikleri kapsayan farklı yöntemler kullanabilir. Siemens olarak geliştirmekte olduğumuz iki farklı uygulama bu temel özellikleri kapsamaktadır. Alt bölümlerde bu uygulama deneyimlerinden bahsedilecektir.

4.1. NetSniffer

Ağ güvenliği uygulamalarında, asıl amaç paketlerin 5-TUPLE (kaynak ip-kaynak port- hedef ip-hedef port- protokol) [5] yöntemi ile oturum bütünlüğü sağlamak ve bu yöntem üzerinden her oturuma ait ağ paketlerini bir bütünlük içerisinde analiz ederek bir anormallik tespit edildiğinde gerekli önlemleri almaktır. NetSniffer uygulaması ile;

- Her bir oturuma ait ip-port, protokol, gelen giden paket sayısı gibi bilgiler kullanıcıya sunulur.
- Kurulan her oturum önceden tanımlanmış kuralları baz alarak "bilinen" ve "bilinmeyen" olarak sınıflandırılır.
- Daha önceden belirlenen kurallar göz önüne alınarak incelenen oturumun bir saldırı olduğu anlaşıldığında o oturuma ait paketler engellenir.
- Kullanıcılar arayüz üzerinden engellenen oturumları görüntüleyebilir, mevcut engelleri kaldırabilirler.
- Ağda bulunan bir bilgisayarın portlarını kontrol ederek açık port bilgisi kullanıcı arayüzünde gösterilir.
- İncelenen oturumlara ait bilgiler HTML veya PDF formatında kaydedilebilir.



Şekil-5: NetSniffer

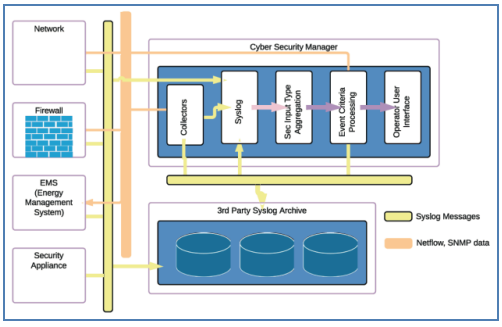
NetSniffer bu özellikleri sunarken, ICMP, TCP, UDP protokollerini inceleyerek; DDOS, PINGFLOOD, PINGOFDEATH ve ARPSPOOFING saldırılarını önceden belirlenen kurallar çerçevesinde yakalar ve bu saldırı kaynağını engelleyerek sistemi koruma altına alır. PORTSCAN adı verilen port taramalarına maruz kalındığında aynı şekilde tepki verir. Şekil 5'te proje cerçevesinde tanımlanan uygulama, bir IPS'in sahip olması gereken özellikleri kapsamaktadır.

4.2. Cyber Security Manager

Siemens'in akıllı şebekeler ağ güvenliği yönetimi için geliştirdiği Cyber Security Manager (CSM)[6], ağ yöneticisinin ağ güvenliği ile ilgili daha çok bilgi sahibi olmasını sağlar. Yönetici, kullanıcı dostu bir arayüz ile tüm güvenlik altyapısını yönetebilir. Şekil 6'da CSM'nin genel yapısı gösterilmiştir. Bu uygulama ile;

- Ağ üzerinde bulunan tüm ağ cihazlarına ait loglar tek bir merkezde toplanır.
- Loglar analiz edilip ağ üzerinde gerçekleşen tüm haberleşme kullanıcı arayüzü ile ağ yöneticisine sunulur.
- Analiz sonucunda herhangi bir anormallik farkedildiğinde alarm üretilerek acil önlem alması için ilgili kişi uyarılır.
- Ağ üzerindeki tüm cihazların; işlemci, disk kullanımı gibi Simple Network Management Protocol (SNMP) bilgileri kullanıcıya sunulur.
- Ağ üzerindeki kurulmuş olan bağlantılar, "bilinen" veya "bilinmeyen" şeklinde sınıflandırılır.
- VPN, SSL gibi güvenli bağlantılarda kullanılan dijital sertifikalara ait bazı bilgiler kullanıcıya sunulur. Örneğin, geçerlilik süresi, sertifika sahibi, onaylama kurumu gibi.
- TCP protokolünün analizi yapabildiği gibi UDP, ICMP gibi protokollerin analizi de yapılabilir.
- Bir ağ üzerinde bulunması gereken her bileşen (firewall, router, switch, bilgisayarlar, yazıcı) kullanılarak TCP/IP, SSL ve SSH bağlantısı simüle edebilen bir simulatör ortamı sunabilmektedir.

Bu uygulama bir IDS olarak sınıflandırılabilir.



Şekil-6: Cyber Security Manager

5. KAYNAKÇA

1. http://www.subnet.com/solutions/nerc-cip/cip-003-security-management-controls.aspx
2. http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39612

3. http://tools.ietf.org/pdf/rfc2196.pdf
4. Yasinsac A., Goregaoker S. "An Intrusion Detection System for Security Protocol Traffic"
5. http://www.techopedia.com/definition/28190/5-tuple
6. http://w3.usa.siemens.com/smartgrid/us/en/distribution-grid/products/distribution-management-system-components/distribution-management-system-components-tab/Documents/CyberSecurity_Whitepaper.pdf

ÖZET (SUMMARY)

Acronym for Supervisory Control and Data Acquisition, SCADA is a computer system for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation

Using network security systems is mandatory in order to keep network system safe from any attack, virus, trojan or stealing special data from SCADA systems.

Firewall has responsibility only for allowing or blocking network packets between local network and out-world network. It has a table which consists of rules. Thanks to these rules, the firewall can terminate a connection by blocking network packets that belong to the same session or give permission by passing network packets. Meanwhile, these rules can be managed by a a network security software or device such as IDS.

All network packets that pass through IDS are examined. If a suspecious packet is found, it generates an alarm and save that packet. Also IDS runs with Firewall in order to block connections. Thus, it can be said that the network system is more secure. There is another security mechanism which is called IPS. IPS can do both detecting and preventing. All network packets that pass through IPS are examined and in case of an attack, all packets which belong to a suspecious connection are blocked. Thus, it can be said that the network system is more secure.

NETSNIFFER

NETSNIFFER is running on computers which have Siemens Spectrum Power components. It behaves as an IDS and generates rules for firewall in order to manage network packets. It can identify the sessions to which each network packet belongs, thanks to 5-tuple (source ip-source port-destination ip-destination port- protocol). It can extract some details belonging to the connection, Such as sender ip- port, receiver ip-port, sending-received packet count and protocol. It can also cut a connection once any suspicious situation is detected. It allows the user to remove blocks, because it is known that it would block again in case of that the attack continuous. By using NETSNIFFER, it is so easy to find out whether own ports or any computer's ports are open or not. Ultimately, it generates a log files which format is either pdf or html.

CSM

All devices or programs on the network have logging mechanism. These logs are collected in one center, then analyzed and reported via a very useful user-interface. This process is provided by CSM which is the abbreviation of Cyber Security Manager. CSM can also generate an alarm by sending an e-mail in case of a suspicious situation. Also CSM provides information from the SNMP agent such as CPU usage, disk space. By using the rules which were defined before, CSM can classify all connections as "secure" or "unsecure". In addition, it can extract some details (issued name, subject name, validation ...) that belongs to the digital certificate which is used in an encrypted connection like SSL, VPN. CSM is also able to analyse UDP, ICMP messages. Ultimately, CSM has an advanced simulator which has all network elements like router, switch, printer,firewall. It provides services in order to simulate SSL, SSH or TCP connections.

6. TEŞEKKÜR:

Bu bildirinin oluşturulması ve NetSniffer projesinin tasarım ve gerçeklenmesi aşamasında destek olan değerli meslektaşım Seydi Mihmanlı'ya teşekkürlerimi iletirim.

CONSTRUCTION OF A 200-kV HVDC REFERENCE DIVIDER MODULE

200 kV REFERANS HVDC GERİLİM BÖLÜCÜSÜ YAPIMI

Ahmet Merev[1], Anders Bergman[2], Serkan Dedeoğlu[1], Alf-Peter Elg[2], Jari Hällström[3], Ernest Houtzager[4], Wolfgang Lucas[5], Johann Meisner[5], Matthias Schmidt[5], Esa-Pekka Suomalainen[3], Christian Weber[6]

[1] *TÜBİTAK National Metrology Institute (UME), Gebze, Turkey (ahmet.merev@tubitak.gov.tr)*
[2] *Technical Research Institute of Sweden (SP), Borås, Sweden.*
[3] *Centre for Metrology and Accreditation (MIKES), Espoo, Finland*
[4] *Dutch Metrology Institute (VSL), Delft, The Netherlands.*
[5] *Physikalisch-Technische Bundesanstalt (PTB), Braunschweig, Germany.*
[6] *Trench Switzerland&France, Saint Louis, France.*

This work is funded by the European Union on the basis of Decision No 912/2009/EC, and identified in the European Metrology Research Programme (EMRP) as Joint Research Project (JRP) ENG07 HVDC, Metrology for High Voltage Direct Current. The Project was led by SP, and the work described here was coordinated by MIKES.

ABSTRACT

Increasing transmission voltages in high-voltage direct current (HVDC), and incipient introduction of dc grids creates the need for traceable calibrations of dc line voltage at levels above a few hundreds of kilovolts. Although control and protection requires accurate measurement, even more important requirements are needed to ensure correct metering.

This paper describes the design and includes uncertainty estimate related to some performance test results of a wideband HVDC reference divider module. The nominal voltage of module is 200 kV, and the module has been designed so that a number of modules can be stacked to extend voltages up to 1000 kV. The module, or a stack of modules, will be used for traceable calibration of HVDC measuring systems in customers' laboratories. The first priority in the design was the accuracy of HVDC measurements. In addition, the divider was designed to have wide bandwidth, both to enable measurement of ripple voltages and to prevent damage during possible flashovers.

ÖZETÇE

Yüksek gerilim doğru akım (HVDC) iletim sistemlerinin kullanımının yaygınlaşması ve dc şebekelerinin kullanılmaya başlanmış olması, dc enerji iletim hatlarının gerilim seviyeleri birkaç yüz kilovolt üzerindeki düzeylerde izlenebilir şekilde kalibrasyon gereksinimini ortaya çıkarmaktadır. Kontrol ve koruma için hassas ölçümler yapmak gerekli olmakla birlikte, doğru ölçümler yapılmasını sağlamak için de çeşitli gerekliliklere ihtiyaç duyulmaktadır.

Bu makalede geniş bant bir HVDC referans bölücü modülünün tasarımı anlatılmakta ve bazı performans testi sonuçlarıyla ilgili belirsizlik kestirimine yer verilmektedir. Modülün nominal gerilimi 200 kV'dur ve benzer modüllerin seri olarak bağlanması durumunda gerilimi 1000 kV değerine kadar yükseltilebilen bir gerilim bölücüsüne dönüşebilecek şekilde tasarlanmıştır. Bu modül veya bir modül serisi, HVDC ölçme sistemlerinin izlenebilirliğini kullanıcıların tesislerinde veya laboratuvarlarında gerçekleştirilen kalibrasyonlarla sağlanmaktadır. Tasarımdaki birinci öncelik HVDC ölçümlerinin hassaslığı olmuştur. Ayrıca, hem dalgalı gerilimlerin ölçülebilmesine olanak tanımakta hem de muhtemel kısa devre olayları sırasında oluşabilecek cihaz hasarlarına karşı koruma sağlayacak şekilde tasarlanmıştır.

1. INTRODUCTION

The main application for this reference divider [1, 6] is the calibration of HVDC dividers up to the highest transmission voltages in use world-wide. For accuracy class 0.2 %, the reference system should have an uncertainty less than 0.02 %. A secondary aim is to create a basis for future determination of loss in converter stations by direct measurement of ac and dc power [2], which necessitates a performance of at least 0.01 %.

HVDC dividers used in precise applications are traditionally based on a resistive design [3-4], whereas high voltage ac (HVAC) dividers used at 50 Hz and above typically rely on a capacitive or a transformer design. Owing to high resistance inherent in the dc dividers, going from dc to even very low frequency (VLF) ac will usually lead to problems related to stray capacitances.

2. DESIGN

The accuracy requirement for dc was set to target of 0.01 % at the nominal voltage. These goals required a design with very good dc performance that is ensured by use of very stable high-voltage resistors run with low current to minimize heating effects. The nominal current through the divider is 100 µA at full voltage in a 200 kV module.

To ensure good bandwidth, a concentric, parallel divider chain was used featuring capacitors as the main ratio elements. Bleeder resistors were added to capacitors to ensure that the dc

ratio stays the same on both divider chains. The two divider chains were carefully separated to ensure that the performance of the dc divider was not compromised.

All high voltage components are placed in a fiberglass tube with an inner diameter of 400 mm. The tube is filled with pressurized (about 150 kPa) SF_6 gas for good insulation. The sealed structure will ensure that the internal insulation surfaces remain clean, and the pressure is low enough to provide increased dielectric strength without ruling out the possibility for air transport.

Additionally, this divider can be used for calibration or characterization of ripple measurement capabilities besides calibration of direct voltage measuring systems.

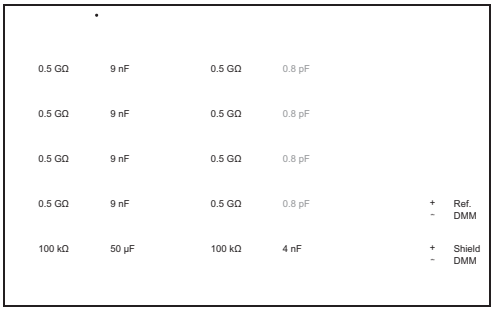


Figure 1. Simplified circuit diagram of the 200 kV divider

3. MAIN CIRCUIT

The system consists of two parallel dividers as shown in Figure 1. A capacitive shield divider surrounds the resistive reference divider. The fast capacitive divider, made of dry polypropylene capacitors, has parallel bleeding resistors to ensure good dc behavior. The bandwidth of the shield divider extends to tens of kilohertz. Care has been taken to minimize the inductance of the high capacitance low voltage part of the shield divider to ensure that the self-resonance frequency is substantially higher than required by the application. The shield divider is composed of three parallel branches, which surround the reference divider.

The response of the divider will closely follow the wide-band response of the shield divider. The output of the shield divider, which is adjusted to closely match with reference divider output, is used for cancellation of the effect of the cable capacitance on the reference signal branch. The voltage difference between the centre conductor and the inner shield of the cable is very close to zero, which effectively cancels the respective capacitance. Only the stray capacitance parallel with the reference high voltage resistors needs to be compensated in the low voltage part.

The resistive current at nominal voltage is 100 µA for both shield and reference dividers, which leads to total power dissipation of 40 W for one 200 kV module.

4. HIGH VOLTAGE PART

The outer diameter of the module is 480 mm, it is 1500 mm high, and it weighs about 150 kg. The module and its internal structure are shown in Figure 2.

The components are enclosed in an SF_6 filled fibreglass tube. The top endplate houses a gas valve, pressure gauge and a feed-through for the reference divider signal. The bottom plate has a mating feed-through, so that the modules can be directly stacked and mounted on top of each other.

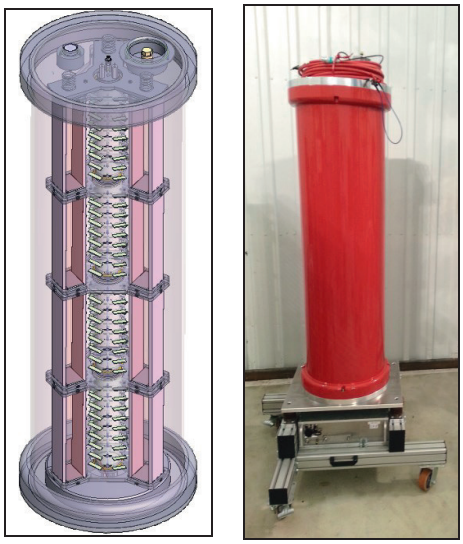


Figure 2. The appearance of 200 kV module

A 200 kV module consists of four 50 kV submodules. Each submodule has 51 selected 10 MΩ precision film resistors with an average temperature coefficient (TC) of (+1.1 ± 0.2) µΩ/Ω/K., and a voltage coefficient (VC) of (−10 ± 4) µΩ/Ω/kV [5]. The low TC will reduce the effect of self heating and the known VC can be compensated numerically.

The submodule structure is shown in Figure **Hata! Başvuru kaynağı bulunamadı.**. The resistors (1) are mounted on a ceramic glass (Macor) support (2). Macor was selected because of its high dielectric constant ($\varepsilon_r \approx 6$) and low dielectric absorption properties; it will provide a good quality parallel capacitor for the reference resistor chain. The resistor support is insulated from the shield divider electrodes (4) by silicon o-rings. Each submodule has three dry polypropylene capacitor modules (3) around the reference resistor chain. These capacitors will provide both field grading for the divider and mechanical rigidity for the internal structure of the module.

5. LOW VOLTAGE PART

The fixed 100 kΩ resistor in the low voltage part of the reference branch is a metal foil high precision resistor with TC of (−0.1 ± 0.5) μΩ/Ω/K.

The three other components in the low voltage arm (see Figure 1) have to be adjusted to their correct values for optimal ac performance. The low voltage part adjustments are performed in binary steps using latching relays.

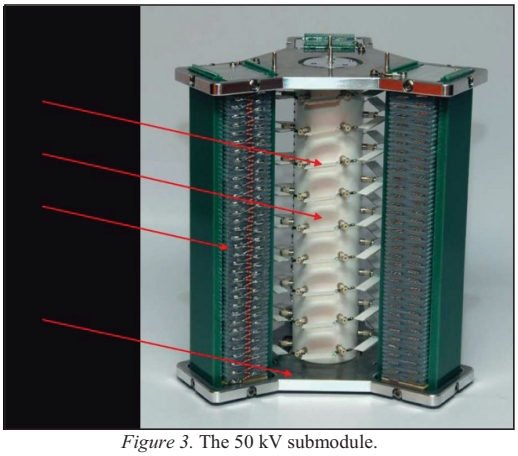


Figure 3. The 50 kV submodule.

The capacitance of the low voltage part of the shield divider is adjustable from 43 to 52 μF. Its design was critical for ensuring a wide bandwidth. Special care was taken to minimize the inductance of the 50 μF low voltage part to ensure that the self-resonant frequency is high enough. Figure 4 shows the shield divider's low voltage part during the assembly process. This capacitor bank, made of dry polypropylene capacitors, lies between two PCBs of 420 mm x 420 mm. The estimated inductance of this capacitor bank is approximately 4 nH. These values lead to a resonant frequency of about 350 kHz.

The resistive part of the shield divider low voltage side is adjustable from 93 to 102 kΩ to enable balancing for the same ratio as the precision divider. It lies on a separate PCB beside the capacitor bank.

A third board was made to house both the fixed reference resistor (100 kΩ) and the capacitor bank for compensating the stray capacitance parallel with the high voltage part resistors. This NP0 type capacitor bank is adjustable from 3.3 to 5.5 nF.

6. MEASUREMENTS AND UNCERTAINTY

The reference divider has been characterized with different methods: linearity effect, temperature dependence, self-heating, voltage dependence, frequency response, step response. As a result of performance tests mentioned above, uncertainty analysis has been done.

Table 1 shows estimates for different contributions to the overall uncertainty, if the divider module is used for measurement of 200 kV dc voltage. This budget assumes that the divider will be calibrated by supplying 1 kV from a dc calibrator on the divider output and measuring the respective output voltage. The temperature is assumed to be (21 ± 3) ºC. Several of the estimates are intended to be conservative, e.g. the leakage current related non-linearity estimated to be 5 μV/V, whereas indications so far indicate that this effect is negligible. As the first manufactured divider module was disassembled for modification soon after the characterization measurements in autumn 2013, no contribution for long term stability can be added onto this uncertainty budget.

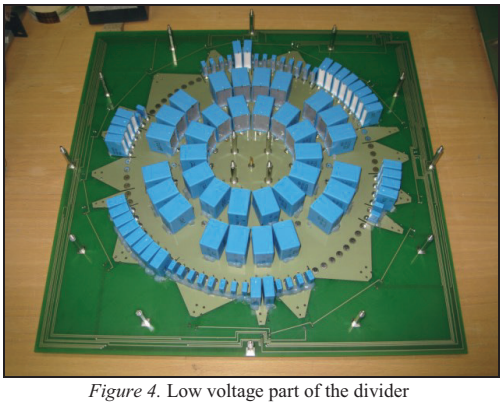


Figure 4. Low voltage part of the divider

Table 1. Uncertainty budget for 200 kV measurements

Contributions	**Uncertainty in μV/V**
Statistical spread	1
Determination of scale factor	10
Uncertainty of voltage coefficient correction	4
Uncertainty for (21±3)ºC temperature range	5
Non-linearity due to leakage currents	5
Self-heating effect	2
Uncertainty of multimeter reading	2
Overall uncertainty	**13**

7. CONCLUSION

It is presented the design of a divider module for high accuracy dc measurements. The film resistors selected for the design have a TC of (+1.1 ± 0.2) μΩ/Ω/K and a voltage coefficient of (−10 ± 4) μΩ/Ω/kV. The estimated overall uncertainty for the measurement of stable 200 kV dc voltage using the divider module is about 13 μV/V (k=2).

Some simulations suggest that with careful design the bandwidth of the planned 1000 kV divider can be in the range of tens of kilohertz, while maintaining precision of dc voltage measurement below than 100 μV/V. The capacitive proximity effects on the divider limit its usability for most demanding ac calibrations. Nine modules for five European National Metrology Institutes have been built in spring 2013, and results of their characterization measurements reaching up to 1000 kV level, will be published later.

8. REFERENCES

[1] J. Hällström et al., “Design of a wideband HVDC reference divider”, *Conference on Precision Electromagnetic Measurements*, Washington, USA, 2012. Pages: 207 – 208.

[2] A. Bergman, “Analysis of metrological requirements for electrical measurement of HVDC station losses”, *IEEE Transactions on Instrumentation and Measurement*, Vol. 61, Issue: 10, 2012.

[3] A. Merev, Ö. Kalenderli, "The construction of a DC high voltage precision divider", *Journal of Electrostatics*, Vol. 67 No. 5 (Sept. 2009) 741-745.

[4] D. Peier and V. Graetch, “A 300 kV dc measuring device with high accuracy”, *8th International Symposium on High Voltage Engineering*, paper 43.08, Milan, Italy, 1979.

[5] E. Houtzager, G. Rietveld, J. Hällström, A.-P. Elg and J.H.N. van der Beek, “Selection and characterization of 10 MΩ, 1 kV resistors for HVDC divider,” *Conference on Precision Electromagnetic Measurements*, Washington, USA, 2012. Pages: 197 – 198.

[6] J. Hällström et al., “Performance of a wideband 200 kV HVDC reference divider module”, *IEEE Transactions on Instrumentation and Measurement*, to be published. doi: 10.1109/TIM.2014.2304857