NIST SP 800-53, Test etme ve güvenliği değerlendirme, bilgi sistemi veya organizasyonu için güvenlik ihtiyaçlarını karşılama konusunda beklenen çıktıları üretebilmeyi ve planlanan süreçleri ve hangi kontrollerin doğru olarak uygulandığını kontrol eder .[100]

Standart, güvenlik değerlendirmeleri konusundaki ayrı bir güvenlik kontrolleri, yani CA ailesi: Güvenlik Değerlendirme ve Yetkilendirmeyi [100] tahsis eder. Bu kontroller, diğerleri arasında, kurumların daha önce tanımlanmış olan güvenlik değerlendirme planlarına dayanarak bilgi sistemlerinde (CA-2) uygulanan güvenlik kontrollerini periyodik olarak değerlendirmeleri gerektiğini belirtir. Bu, sistem için belirtilen güvenlik gerekliliklerine atıfta bulunulmalı ve sonuçların bir güvenlik değerlendirme raporunda belgelenmesi gerekir. Bunun yanında, güvenlik kontrolleri sürekli olarak izlenmelidir [100].

Örgütler resmi, belgelenmiş güvenlik değerlendirme ve yetkilendirme politika ve prosedürlerini geliştirmeli, yaymalı ve periyodik olarak gözden geçirmeli / güncellemelidir (CA-1). Değerlendirmeler sırasında tespit edilen zayıflıkları veya eksiklikleri gidermek için düzeltici eylemleri tanımlamalı ve belgelendirmelidir [100].

Güvenlik değerlendirmeleri yazılım ve ürün yazılımı geliştirme aşamasında (SA ailesi) yapılmalıdır. Bunun için güvenlik değerlendirme planları tanımlanmalıdır. Control SA11, güvenlik değerlendirme planlarının, geliştiricilerin analiz etme, test etme ,değerlendirme veya yazılım incelemeleri gibi gerçekleştirmeyi planladığı belirli faaliyetleri tanımladığını belirtir. Tanımlar analiz türlerini, bunların derinliğini, doğruluğunu ve kapsamını ayrıca bu işlemler sırasında üretilen yapay doku türlerini (yan ürünler) kapsar.

Güvenlik değerlendirme planları için kabul kriterleri, kusur giderme işlemleri ve planların / işlemlerin uygun şekilde uygulandığına dair kanıtlar sözleşmelere dahil edilmelidir. Değerlendirme planlarını, kanıtlarını ve belgelerini inceleme ve koruma yöntemleri, bilgi sisteminin güvenlik kategorisine veya sınıflandırma seviyesine uygun olmalıdır [100].

Yüksek kritiklikte sistemler için (aksi takdirde isteğe bağlı) kavrama testi yapılması gerekir (CA-8). Belgeye göre kavrama testi için yaygın bir yöntem şunları içerir:

* Hedef sistemin tam bilgisine dayalı ön analiz,
* Ön analize dayalı potansiyel açıkların belirlenmesi,
* Belirlenen güvenlik açıklarından ne ölçüde yararlanılabileceğini belirlemek için tasarlanmış testler.

Güvenlik değerlendirme konularının açıklamaları NIST SP 800-53'te ayrıntılı olarak verilmiştir ve önerilen kontrollerin geliştirilmesini içermektedir. Dahası, (ilgi sıralarına göre listelenmiştir) [100] için başka yayınlara referanslar verilmiştir:

* NIST SP 800-115, Bilgi Güvenliği Test ve Değerlendirme Teknik Rehberi [123],
* NIST SP 800-137, Federal Bilgi Sistemleri ve Organizasyonları İçin Bilgi Güvenliği Sürekli İzleme (ISCM),
* NIST SP 800-53A, Federal Bilgi Sistemleri ve Organizasyonlarında Güvenlik ve Gizlilik Kontrollerini Değerlendirme: Etkili Değerlendirme Planları Oluşturma [108],
* NIST SP 800-37 Risk Yönetim Çerçevesini Federal Bilgi Sistemlerine Uygulama Kılavuzu: Bir Güvenlik Yaşam Döngüsü Yaklaşımı [104].

Nist in 4.revizyonu mütekabiliyet kavramını tanıtıyor olduğunu belirtmek değerlidir. O kavram şöyle tanımlanır: Bilgi paylaşımı için birbirlerinin değerlendirilmiş güvenlik duruşlarını kabul etmek veya sistem kaynakları bilgilerini yeniden kullanmak amacıyla birbirlerinin güvenlik değerlendirmelerini kabul etmek için katılımcı organizasyonlar arasındaki ortak anlaşmadır. [100].

**6.9. NIST SP 800-82**

NIST SP 800-82 “Endüstriyel Kontrol Sistemleri (ICS) Güvenliği Rehberi”, Endüstriyel Kontrol Sistemleri güvenliğine adanmış NIST birincil yayınıdır. Diğer NIST yayınları gibi, dünya çapında yaygın olarak tanınmakta ve kabul edilmektedir.

Standart, NIST SP 800-53'e benzer şekilde, güvenlik değerlendirmeleri konusuna ayrı bir güvenlik kontrolleri ailesi, yani - CA ailesi: Güvenlik Değerlendirme ve Yetkilendirmede belirtilen güvenlik kontrollerinin doğru bir şekilde uygulandığını doğrulamak ve onaylamak için bir temel oluşturan, istenildiği gibi ve istenen sonucu üretmektedir. [132]. NIST SP 800-82, NIST SP 800-53'ten [132] taşınan güvenlik değerlendirmeleri ile ilgili güvenlik kontrolleri hakkında ICS'ye özel rehberlik sunar.

Güvenlik açığı ve sızma testi araçlarına ilişkin özel önerilerde bulunulmuştur. Bu araçların bir ICS'nin çalışması üzerindeki etkilerini dikkatlice değerlendirmek önerilir, çünkü aktif güvenlik açığı ve sızma testi sırasında kullanılan ek trafik ve istismarların, ICS'nin sınırlı kaynakları ile birlikte kullanılmasına neden olduğu durumlar olmuştur (örnekler verilmiştir). Bu nedenle, ICS için önerilen güvenlik açığı ve sızma testi tekniklerinin bir listesi Sandia National Laboratories (SNL) tarafından geliştirilmiştir [35]. Listedeki yöntemler aktif değil, pasif, daha az müdahalecidir.

Güvenlik açığı ve sızma testi yapan değerlendiricilerin ICS sahipleri tarafından ICS'nin sürekli çalışmasının önemi ve testlerin gerçekleştirilmesindeki riskler hakkında bilgilendirilmesi gerekir. Bir diğer olası risk azaltma stratejisi, testleri endüstriyel proseslerde uygulananlarla aynı ICS bileşenlerini kullanarak bir laboratuar ortamında gerçekleştirmektir. Bununla birlikte, laboratuar sisteminin temsili olduğundan emin olmak için çok iyi bir yapılandırma yönetimiyle bile, gerçek sistem üzerinde yapılan testlerin, laboratuarda temsil edilmeyen kusurları ortaya çıkarması muhtemeldir. Kuşkusuz, laboratuar testleri, operasyonel sisteme potansiyel olarak zararlı test prosedürlerini ortadan kaldırmak için uygulanabilir [132].

İç Güvenlik Bakanlığı (DHS) ve Samurai Projeleri Hizmet Programları için Güvenlik Test Çerçevesi (SamuraiSTFU) tarafından geliştirilen Siber Güvenlik Değerlendirme Aracı (CSET) olarak iki değerlendirme aracı sunulmuştur. CSET, kontrol listesi temelli değerlendirmeler için sistematik ve tekrarlanabilir bir yaklaşım sunarak kuruluşların kilit ulusal siber varlıklarını korumalarına yardımcı olmayı amaçlamaktadır. SamuraiSTFU geleneksel bir ağ kavrama testi araç kutusudur. Tipik test uygulamalarının yanı sıra, kapsamlı laboratuar testleri yapmak için kullanılabilecek ICS için emülatörleri, akıllı sayaçları ve diğer enerji sektörü sistemlerini de içerir [132].

NIST SP 800-115, NIST SP 800-53A, NIST SP 800–37 (bakınız Bölüm 6.8) ve NIST SP 800 100 “Bilgi Güvenliği El Kitabı: Yöneticiler İçin Rehber” e daha fazla rehberlik referansı verilmiştir. Fiili standart, IACS kullanan akıllı şebeke mimarisinin tüm bileşenlerine uygulanabilir (bkz. Şekil 1).

**6.10. ISO / IEC 15408 ve 18045 (Ortak Kriterler ve CEM)**

ISO / IEC 15408 “Bilgi teknolojisi - Güvenlik teknikleri - BT güvenliği için değerlendirme kriterleri” olan üç standarttan oluşan bir set [74,75,77], BT ürünlerinin (donanım ve yazılım) güvenlik değerlendirmesi için kriterleri açıklamaktadır. Standartlar, sistematik, tanınabilir ürün doğrulamaları ve sertifikalandırmayı amaçlayan Ortak Kriterler projesinde geliştirilmiştir. Proje üyeleri, ortak kriterlerini kullanmak için ISO / IEC'ye özel olmayan lisans vermişlerdir.

  ISO / IEC 15408 geliştirme şartnamesinde. Şu anda mevcut olan ISO / IEC 15408 standartları 2008 ve 2009’dan, en yeni, serbestçe erişilebilir olan Ortak Kriterler (v3.1 Sürüm 4) [2-4] 2012 sonunda yayınlanmıştır. Bu standartlar tamamen Güvenlik ürünleri ile ilgili olarak güvenlik değerlendirme konusudur. Değerlendirmeler test laboratuarlarında yapılmaktadır.

433 sayfadaki “Bilgi Teknolojisi Güvenliği Değerlendirmesi için Ortak Metodoloji” (CEM) [5] adlı ayrı bir belge, değerlendirmelerin standartlaştırılmış, sistematik bir metodolojisini açıklamaktadır. Belge çok ayrıntılı ve tekniktir. Açıkça akıllı şebekeden söz etmese de, yazılım / donanım bileşenlerinin güvenlik değerlendirmesine uygulanabilir. Bu belgenin daha önceki bir sürümü ISO / IEC 18045 “Bilgi teknolojisi - Güvenlik teknikleri - BT güvenliği değerlendirmesi için Metodoloji” standardı [76] olarak kabul edildi ve 2008 yılında yayınlandı. : //standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

**6.11. IEC 61850**

IEC 61850 “Elektrik şebekesi otomasyonu için iletişim ağları ve sistemleri - Bölüm 10: Uygunluk testi” [61], güvenlik değerlendirmeleri veya güvenlik değerlendirme metodolojisi açıklamalarını veya referanslarını içermez.

**6.12. DHS kataloğu**

İç Güvenlik Bakanlığı (DHS) “Kontrol Sistemleri Güvenliği Katalogu: Standart Geliştiriciler için Tavsiyeler”, çeşitli endüstriyel kuruluşların, Endüstriyel Kontrol Sistemlerinin (ICS) güvenliğini arttırmak için önerdikleri uygulamaları sunmaktadır. 19 kategoride toplanmış olan öneriler, bireysel güvenlik gereksinimlerine özgü sağlam siber güvenlik standartlarının geliştirilmesine olanak sağlayan bir esneklik düzeyi sağlamak için kapsam açısından geniştir.

DHS, faaliyetlerine başlamadan önce ve bundan sonra - periyodik olarak veya önemli herhangi bir değişikliğin ardından ICS'nin işlem için yetkilendirilmesinin yapılması önerilmektedir. Kılavuza göre, her yetkiye, uygulanan güvenlik önlemlerinin (sertifikasyon) değerlendirilmesi eşlik etmelidir. Güvenlik sertifikaları yıllık olarak yenilenmelidir. Sertifikalardan önce güvenlik değerlendirmeleri de yapılmalıdır [30].

Özellikle, önerilen kontrol 2.18.4: Güvenlik Değerlendirmeleri, kontrollerin doğru uygulanmasının derecesini, amaçlanan operasyonunu ve tespitini belirlemek için güvenlik kontrollerinin kuruluş tarafından tanımlanmış bir sıklıkta (yılda - en az - en az) tekrar tekrar değerlendirilmesi gerektiğini , sistemin güvenlik gereksinimlerini karşılamak için istenen sonucu üretip üretmedikleri belirtir. Değerlendirmenin sonuçları bir güvenlik değerlendirme raporuna kaydedilmelidir. Değerlendirmeler periyodik, habersiz, derinlemesine izleme, kavrama testi ve kırmızı takım egzersizlerini içerebilir [30].

Yıllık değerlendirme gerekliliğini yerine getirmek için kuruluşlar - aşağıdaki kaynaklardan herhangi birinin sonuçlarını kullanabilirler [30]:

* Bir sistem yetkilendirme veya yeniden yetkilendirme sürecinin parçası olarak gerçekleştirilen güvenlik değerlendirmeleri,
* Sürekli izleme veya
* Devam eden sistem geliştirme yaşam döngüsü sürecinin bir parçası olarak sistemin test edilmesi ve değerlendirilmesi.

Mevcut güvenlik değerlendirme sonuçları geçerliyse, yeniden kullanılabilir ve gerektiğinde ek değerlendirmelerle desteklenebilir [30].

Değerlendirme için güvenlik kontrollerinin seçimi [30] 'a göre yapılmalıdır:

* Sistemin güvenlik sınıflandırması (sistemin kritikliği),
* Kurum tarafından seçilen ve istihdam edilen belirli güvenlik kontrolleri ve
* Kuruluşun güvenlik kontrollerinin etkinliğini belirlemede sahip olması gereken güvence seviyesi.

Kritik kontroller yıllık olarak, diğer güvenlik kontrolleri en az üç yılda bir değerlendirilir. Değerlendirmeler, organizasyonda uygulanan bilgi güvenliği politikalarını ve prosedürlerini ve belirli bir tesis ve / veya süreçle ilgili riskleri anlayan nitelikli ve yetkili değerlendiriciler tarafından yapılmalı ve belgelenmelidir. Kuruluşlar, değerlendirmelerin ICS işlevlerini engellemediğinden emin olmalıdır. Bazı durumlarda, bir ICS'nin değerlendirmeyi sağlamak için çoğaltılması veya çevrimdışı moda geçirilmesi gerekebilir. Bir ICS'nin canlı değerlendirmesi yapılamazsa, kuruluş, çoğaltılmış bir sistem sağlama gibi telafi edici kontroller kullanmalıdır [30].

Kuruluşlar, sistemdeki güvenlik kontrollerinin tarafsız bir değerlendirmesini yapmak için bağımsız bir değerlendirici veya sertifikalandırma ajanı veya bir değerlendirme ekibi / sertifikalandırma acentesi kullanabilir. Tarafsızlık, değerlendiricilerin, kontrol sistemiyle ilişkili gelişimsel, operasyonel ve / veya yönetim komuta zinciri veya güvenlik kontrol etkinliğinin belirlenmesi ile ilgili herhangi bir çıkar çatışmasına karışmadığını belirtir.

Bazı durumlarda, örneğin bir kuruluş küçükse, değerlendirme bağımsız uzmanlar tarafından yapılamaz. Bu durumda, sonuçların bütünlüğünü, tutarlılığını ve doğruluğunu onaylamak için değerlendirme sonuçlarını bağımsız bir uzmanlar ekibi tarafından dikkatlice inceleyerek ve analiz ederek değerlendirmenin bağımsızlığı sağlanabilir [30].

DHS tarafından önerilen kontrol - 2.18.3: Sertifikalandırma, Akreditasyon ve Güvenlik Değerlendirme Politikaları, kuruluşların resmi ve dokümante edilmiş dokümanları geliştirmelerini, yaymalarını ve periyodik olarak gözden geçirmelerini ve güncellemelerini gerektirir:

* Amaç, kapsam, roller, sorumluluklar, yönetim taahhüdü, kuruluşlar arasında koordinasyon ve uygunluğu belirleyen güvenlik değerlendirme ve belgelendirme ve akreditasyon politikaları,
* •Güvenlik değerlendirmeleri ve belgelendirme ve akreditasyon politikalarının uygulanmasını kolaylaştıran prosedürler ve ilgili değerlendirme, belgelendirme ve akreditasyon kontrolleri [30].

Fiilen standart, akıllı şebeke mimarisinin tüm bileşenlerine uygulanabilir (bkz. Şekil 1).

**6.13. IEC 62056-5-3**

IEC 62056-5-3 “Elektrik ölçümü veri değişimi - DLMS / COSEM paketi - Bölüm 5-3: DLMS / COSEM uygulama katmanı” [63] güvenlik değerlendirmeleri veya güvenlik değerlendirme metodolojisi açıklamalarını veya referanslarını içermez.

**6.14. ISO 15118**

Üç parçalı uluslararası standart ISO 15118 “Karayolu taşıtları şebekeye haberleşme arabirimine araç” [73] güvenlik değerlendirme rehberi sağlamaz. Güvenlik dahil olmak üzere ağ ve uygulama protokolü gereksinimlerini tanımlayan Bölüm 2, elektrikli araçlar ve Elektrikli Araç Tedarik Ekipmanları arasındaki ara yüzlerin uygunluk kontrolüne dayalı değerlendirmelerine uygulanabilir [73].

**6.15. ISO / IEC 27019**

ISO / IEC 27019 [82] “Bilgi teknolojisi - Güvenlik teknikleri - Enerji hizmet endüstrisine özgü proses kontrol sistemleri için ISO / IEC 27002'ye dayalı bilgi güvenliği yönetim kuralları”, enerji hizmet sektöründeki kuruluşlara ISO / IEC'yi yorumlama ve uygulama konusunda yardımcı olmayı amaçlamaktadır. Endüstriyel Kontrol Sistemlerini (ICS) korumak için 27002. Standart ISO / IEC 27002'ye dayanmaktadır.

Kontrol 15.2 Güvenlik politikaları ve standartlarına uygunluk ve ISO / IEC 27002 kavrama testleri ve güvenlik açığı değerlendirmelerinde belirtilen teknik uygunluk (ISO / IEC 27001 ve 27002 bölümüne bakınız), asıl belgeye doğrudan referans içermektedir. Ayrıca, Ek B “Güvenli Kontrol Sistemleri için Gereksinimler” bölümünde, üretim sistemlerinden ayrılmış ortamlarda sistem testlerinin, güncellemelerin, iyileştirmelerin ve güvenlik yamalarının test edilmesi önerilmektedir.

Ek B'de belirtilen tüm gereksinimler, IACS kullanan akıllı şebeke mimarisinin tüm bileşenlerinde (bkz. Şekil 1) ICS'ye uygunluk kontrolü için kullanılabilir.

**6.16. Gelişmiş Ölçüm Altyapısı için Güvenlik Profili**

Gelişmiş Ölçüm Altyapısı için Güvenlik Profili [9] Gelişmiş Ölçüm Altyapısı Güvenliği (AMI-SEC) Görev Gücü tarafından geliştirilen ve Haziran 2010'da yayımlanan bir kılavuzdur. Belgenin amacı, güvenlik önlemlerinin içeri alınması ve AMI altyapısıdır. Standartta sunulan güvenlik kontrollerinin çoğu DHS Kontrol Sistemleri Güvenliği Katalogundan uyarlanmıştır (bkz. Bölüm DHS Katalogu).

Kontrol DHS-2.10.3 Sistem İzleme ve Değerlendirme, AMI sisteminin tüm bileşenlerinin güvenlik açıkları ve bakım ve güvenlik politikalarına uyum için düzenli olarak değerlendirilmesini önerir. Değerlendirmelerin sıklığı, kuruluşun risk yönetimi stratejisine bağlı olmalıdır. Analizler sırasında belirlenen güvenlik açıklarıyla ilgili tüm güvenlik açıkları veya uyumsuzluklar, ilgili AMI sistem bileşenlerinin güncellenmesine veya değiştirilmesine neden olmaktadır. [9].

Kılavuz, AMI sisteminde uygulanan tüm şifreleme modüllerinin FIPS 140-2'nin gereklerine göre güvenlik analizini tavsiye etmektedir. (Federal Bilgi İşleme Standardı “Şifreleme Modülleri için Güvenlik Gereklilikleri”). En çok tavsiye edilen çözüm, Kriptografik Modül Doğrulama Programı [110] tarafından doğrulanan kriptografik modüllerin kullanılmasıdır.

**6.17. NRC RG 5.71**

ABD Nükleer Düzenleme Komisyonu (NRC) Düzenleme Rehberi 5.71 “Nükleer Tesisler İçin Siber Güvenlik Programları” [113] nükleer altyapıların korunmasına ilişkin ulusal düzenlemeleri ele alan bir dizi güvenlik kontrolü ve kullanımıyla ilgili kılavuz sunar. Standarttaki kontroller NIST SP 800-53 ve NIST SP 800-82'den kaynaklanmaktadır, ancak bunlar nükleer enerji sektörünün özelliklerine uyarlanmıştır. Bunlar Ek A'da sunulan bir siber güvenlik programı şablonu halinde gruplandırılmıştır. Standart, güvenlik ve güvenlik açısından önemli olan ve zorunlu olarak korunması gereken Kritik Dijital Varlıklar (CDA) kavramını ortaya koyar [113].

Belgeye göre, güvenlik değerlendirmeleri politikaları ve uygulama prosedürleri siber güvenlik programının ayrılmaz bir parçası olmalıdır. Her yıl gözden geçirilmeleri gerekir [113].

Sürekli izleme sürecinin bir parçası olarak gerçekleştirilen güvenlik kontrollerinin periyodik olarak, en azından yıllık değerlendirmeleri CDA'yı korumak için gerekli güvenlik kontrollerinin varlığını, doğru işleyişini ve etkinliğini doğrulamayı amaçlamaktadır. Güvenlik kontrollerinin etkinliği, geçici tehdit ortamı ve sistem ortamı nedeniyle sürekli değişikliklere maruz kalmaktadır. Tespit edilen boşluklar siber güvenlik programında değişikliklerle sonuçlanmalıdır. Bileşen kusurları ve arızalar giderilmelidir [113].

Ek olarak, her CDA en az 3 ayda bir veya güvenlik kontrollerindeki zayıflıklar tespit edildiğinde güvenlik açıkları açısından taranmalıdır. Güvenlik açığı yönetimi sürecinin öğelerini otomatikleştiren birlikte çalışabilir araçlar ve teknikler kullanılmalıdır [113].

Standart akıllı şebeke mimarisinin tüm bileşenlerine uygulanabilir (bkz. Şekil 1). ABD nükleer santralleri için siber güvenlik öz değerlendirme yöntemi (NUREG / CR-6847) [49] ile ilgili düzenleyici bir kılavuza atıfta bulunur, ancak belge halka açık değildir [113].

**6.18. NIST SP 800-64**

NIST SP 800-64 “Sistem Geliştirme Yaşam Döngüsünde Güvenlikle İlgili Hususlar” [86] ABD federal kurumlarına adanmış bir kılavuz olup, iyi güvenlik uygulamalarının BT sistemi geliştirme yaşam döngüsüne nasıl dahil edileceğini açıklamaktadır.

Standarda göre, sistem geliştirmenin uygulama / değerlendirme aşamasında yapılan ana faaliyetlerden biri sistem güvenliği değerlendirmesidir (faaliyet 3.3.3.3). Yeni geliştirilen sistemler veya mevcut yazılım / donanıma yapılan değişiklikler, operasyon için yetkilendirilmeden önce resmi olarak değerlendirilmelidir. Değerlendirme, işlevsel ve güvenlik gereklilikleri ile uyumluluk kontrolüne dayanır ve NIST SP 800-53A “Federal Bilgi Sistemlerinde Güvenlik Kontrollerini Değerlendirme Kılavuzu” nda açıklanan değerlendirme prosedürlerini izlemelidir. [108]. Tüm güvenlik kontrollerinin, işlevsel ve etkin bir şekilde çalışıp çalışmadıklarının doğrulanması gerekir.

NIST SP 800-64, süreçten beklenen teslimatları: bir güvenlik değerlendirme raporu, eylem planı ve kilometre taşları ve güncellenmiş sistem güvenlik planını belirtir. Bazı uygulama önerileri verilmektedir [86].

**6.19. IEEE 1402**

IEEE 1402 “Elektrik Trafo Merkezi Fiziksel ve Elektronik Güvenlik Kılavuzu” [69], elektrik trafo merkezlerinin kurulması ve işletilmesine ilişkin güvenlik hususlarını açıklamaktadır. Standardın 8.5. Kısmı güvenlik değerlendirmelerini ifade eder ancak fiziksel güvenliğe adanmıştır. Sunulan örnek güvenlik değerlendirme formu, diğer kontrol listesi temelli değerlendirme türlerinde referans olarak yararlı olabilir [69].

**6.20. IEEE C37.240**

IEEE C37.240 “Trafo Merkezi Otomasyonu, Koruma ve Kontrol Sistemleri için Standart Siber Güvenlik Gereklilikleri” [68], elektrik trafo merkezlerinin iletişim sistemlerine (otomasyon, koruma ve kontrol) yönelik temel siber güvenlik gereksinimlerini sunmaktadır. İhtiyaçlar orta derecede tekniktir (ayrıntılı teknik özellikler olmadan fakat mevcut teknik çözümler).

Gereksinim 6.8, bir trafo merkezi siber güvenlik stratejisinin ayrılmaz bir parçası olarak güvenlik testini uygular. Test etmenin amacı, uygulanan güvenlik kontrollerinin bilinen saldırılara karşı ve aynı zamanda henüz tespit edilmemiş saldırılara karşı savunmada etkinliğini doğrulamaktır. Belirtilen test yöntemleri şunları : güvenlik politikaları ve prosedürlerinin incelemeleri, sızma testi, fiziksel güvenlik denetimleri, güvenlik açığı taraması ve güvenlik duvarı kurallarının incelenmesini içerir. Bu işlemler periyodik olarak yapılmalıdır.

**6.21. ISO/IEC 27005**

ISO / IEC 27005 “Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği risk yönetimi” [78] en popüler ISO / IEC 27000 serisinden bir başka önemli belgedir. Özellikle ISO / IEC 27001 ile uyumlu kuruluşlar için uygun olan risk yönetimi sürecini açıklar. Standart risk merkezli olmasına rağmen, güvenlik açıklarının tanımlanmasında kılavuz (risk analizinin bir parçası) herhangi bir güvenlik değerlendirmesinde yararlı olabilir. Ek D, “Güvenlik açığı değerlendirmesi için güvenlik açıkları ve yöntemleri”, kontrol listesinde değerlendirmelerde kullanılabilecek bir güvenlik açığı listesi ile birlikte güvenlik açığı değerlendirme yöntemlerini: otomatik güvenlik açığı taraması, güvenlik testi ve değerlendirmesi, sızma testi ve kod incelemesi önerir ve açıklar [78]. Standart akıllı şebeke mimarisinin tüm bileşenlerine uygulanabilir (bkz. Şekil 1).

**6.22. NIST SP 800-115**

NIST SP 800-115 “Bilgi Güvenliği Test ve Değerlendirme Teknik Kılavuzu” [123], üç zorunlu aşamayı kapsayan güvenlik değerlendirmelerini gerçekleştirmek için sistematik ve tekrarlanabilir bir metodoloji sunmaktadır: planlama, yürütme ve yürütme sonrası. Belge, kapsamlı, ayrıntılı açıklamalar ve diğer destekleyici belgelere çok sayıda referans içermektedir. Bu nedenle, bu belge akıllı şebeke bilgi sistemlerinde siber güvenlik değerlendirmeleri konusunda rehberlik ararken ilk seçenek olabilir [123].

Standart, teknik açıkları tespit etmek, doğrulamak ve değerlendirmek ve kurumların sistemlerinin ve ağlarının güvenlik duruşlarını anlama ve iyileştirmelerine yardımcı olmak için kullanılabilecek teknik test ve inceleme tekniklerini tanımlar. Ek A'da [123] dahil olmak üzere diğer güvenlik değerlendirme metodolojilerine referanslar verilmiştir:

* Bilgi Tasarım Güvencesi Kırmızı Ekibi (IDART) [122],
* Ulusal Güvenlik Ajansı (NSA) Bilgi Değerlendirme Metodolojisi (IAM) [83],
* NIST SP 800-53A [108] 'de açıklanan NIST güvenlik değerlendirme metodolojisi,
* Açık Kaynak Güvenlik Test Metodolojisi El Kitabı (OSSTMM) [55],
* Açık Web Uygulama Güvenliği Projesi (OWASP) Test Projesi [99].

Fiili standart, akıllı şebeke mimarisinin tüm bileşenlerine uygulanabilir (bkz. Şekil 1).

**6.23. Akıllı şebeke siber güvenlik değerlendirmesine ilişkin diğer uygunluk standartları**

AMI Sistem Güvenliği Gereklilikleri [20], tedarik endüstrisinde ve tedarikçilerine, tedarik sürecinde kullanılacak Gelişmiş Ölçüm Altyapısı (AMI) için bir dizi güvenlik gereksinimi sağlar. DHS Siber Güvenlik Tedarik Dili Kontrol Sistemleri için [29] benzer tedarik güvenliği gereksinimlerini tanımlamaktadır, ancak Endüstriyel Kontrol Sistemleri için.

TR / T 20279 Bilgi Güvenliği Teknolojisi - Ağ ve Terminal Ayrıştırma Ürünlerinin Güvenlik Teknik Gereklilikleri [6], güvenlik duvarları ve benzeri cihazlar için teknik güvenlik gereksinimlerini sunan ulusal bir standarttır. “Gelişmiş Ölçüm Altyapısının Gizliliği ve Güvenliği” adlı ISO 27001 tabanlı güvenlik ve gizlilik gereksinimlerini Hollanda kılavuzu [101], AMI için sunmaktadır. Risk analizine dayalı güvenlik politikalarının periyodik değerlendirmelerini yapar. VGB Standardı “Tesis Üretmek İçin BT Güvenliği” [16] enerji santralleri için güvenlik gereksinimlerini belirtir.

IEC TR 62541-2: 2016 “OPC birleşik mimarisi - Bölüm 2: Güvenlik Modeli” [64], OPC Birleştirilmiş Mimarisine (UA) olası tehditlerin tanımını ve bunları hafifletmeyi amaçlayan güvenlik işlevlerini içeren tüm güvenlik modelini açıklar. Belgenin önemli bir kısmı, OPC-UA güvenlik fonksiyonlarının güvenlik hedeflerini nasıl karşıladığını ve tehditlere karşı nasıl koruduklarının analizine adanmıştır.

ISO / IEC 19790: 2012 “Bilgi teknolojisi - Güvenlik teknikleri - Kriptografik modüller için güvenlik gereksinimleri” [79], bilgisayar ve telekomünikasyon sistemlerinde hassas bilgileri koruyan güvenlik sistemlerinde kullanılan kriptografik modüller için güvenlik ön koşullarını tanımlar.

RFC 6272 “Akıllı şebeke için internet protokolleri” [13] akıllı şebekede kullanılacak anahtar İnternet protokollerini tanımlar. TCP ve IP protokollerinin güvenlik değerlendirme belgelerine referanslar içerir.

NIST SP 800–124 “İşletmelerdeki Mobil Cihazların Güvenliğini Yönetme Rehberi” [129], güvenlik değerlendirme rehberliği için NIST SP 800–115'e işaret etmektedir. Pasif (ör. Günlükleri gözden geçirme) veya aktif (ör. Güvenlik açığı taramaları veya sızma testi) periyodik doğrulamaları önerir.

IEEE Std 2030.2-2015 “Elektrik Enerjisi Altyapısına Entegre Enerji Depolama Sistemlerinin Birlikte Çalışabilirliği İçin Rehber” [71], 8. Bölümünü enerji depolama sistemlerinde güvenlik ve güvenlik konusuna adamıştır. Sistemlerde veya cihazlarda uygulanan teknoloji analizlerini, güvenlik özelliklerini ve yeteneklerini ve ayrıca kavrama testlerini yaparak tüm güvenlik kontrollerinin, mekanizmalarının ve prosedürlerinin periyodik testlerini önerir. Sonuncusunun, endüstriyel süreçler üzerinde muhtemelen en düşük etkiye sahip olduğu durumlarda, bir zaman diliminde gerçekleştirilmesi önerilir.

**6.24. Akıllı şebeke siber güvenliği ile ilgili diğer standartlar**

ABD Enerji Bakanlığı (DoE) “Küçük ve Orta Ölçekli Enerji Tesisleri için Enerji Altyapısı Risk Yönetimi Kontrol Listeleri” [32], belediye ve bağımsız kuruluşlar gibi küçük ve orta ölçekli enerji tesisleri veya kırsal kooperatifler için risk yönetimine eksiksiz bir kontrol listesi sunmaktadır.

Elektrik sektörüne adanmış bir risk yönetimi metodolojisi, ABD DoE, NIST ve NERC tarafından ortaklaşa geliştirilen “Elektrik Alt Sektör Siber Güvenlik Risk Yönetimi Süreci” [33] bölümünde açıklanmaktadır. Metodoloji, NIST SP 800-39 “Bilgi Güvenliği Riskini Yönetme” de açıklanan “genel amaçlı” risk yönetimi sürecine dayanmaktadır [105].

**6.25. Standartların özeti ve karşılaştırılması**

Tablo 5-8, Bölüm 5'te açıklanan kriterlere göre standartların ana özelliklerini göstermektedir.

tablolar gelecek.

**7. Endüstri standartlarının benimsenmesi**

Tanımlanan standartlara ilişkin ilginç bir soru, sektör tarafından gerçek uygulamalarının statüsüdür. Bu, gibi faktörleri standartların benimsenme seviyeleri uygulama süreçlerinin süresi maliyetleri ve beklenen faydaları olarak değerlendir ayni zamanda hangi standartlar uygulanır veya organizasyonlar tarafından uygulama süreçlerindeki hangi kısıtlama ile karşılaşılır.Bu soruları cevaplamak için en uygun 13 standart için literatür analizi yapılmıştır (bkz. Tablo 5 ve 6). Anketin ana bölümündeki aynı bilimsel veri tabanları (bkz. Tablo 1) ve İnternet kamu kaynakları, “NISTIR 7628 uygulaması”, “NISTIR 7628 benimseme”, “NIST SP 800-82 uygulaması” anahtar kelimeleri için araştırılmıştır. “akıllı şebeke standartlarının uygulanması” ve “akıllı şebeke standartlarının benimsenmesi”. Sonuçlar, bu konudaki mevcut verilerin çok az olduğunu göstermektedir.

NERC CIP standartları, ABD'deki Federal Enerji Düzenleme Komisyonu (FERC) tarafından uygulanan yasal zorunluluk nedeniyle ABD'deki elektrik hizmetleri kuruluşları tarafından uygulanmaktadır .[14,44,87]. Das ve diğ. [27], ancak, FERC'in elektrik sektörünün diğer katılımcılarını düzenleme yetkisine sahip olmadığı için, bu sürecin yalnızca toplu enerji sistemini (elektrik üretimi ve iletimi) ilgilendirdiğini belirtmektedir. Sonuç olarak, diğerleri sistemlerinin siber güvenliğini arttırma zorunluluğu hissetmezler.

Bartnes Line ve ark. [15] küçük ve büyük Norveç dağıtım sistemi operatörlerinde (DSO'lar) siber güvenlik yönetimi uygulamalarının durumunu analiz etmişlerdir. Görüşme temelli ankete göre, operatörler arasında siber güvenlik riskinin algılanması ve hazırlık durumu düşüktür. Bu, özellikle, siber güvenlik olayları yaşarken tedarikçilerine büyük ölçüde bağımlı olmasına rağmen, en kötü siber tehdit senaryolarına dayanma kabiliyetini ilan eden küçük elektrik dağıtım sistemi operatörleri ile ilgilidir. Kendilerini bir saldırının olası hedefi olarak algılamıyorlar, çünkü onların görüşüne göre, daha büyük operatörler saldırganlar için daha çekicidir. Çalışma, standartların kendi başına benimseme seviyesini araştırmamasına rağmen, onu etkileyebilecek faktörleri göstermektedir.

Wiander [19], 4 kurumda ISO / IEC 17799'un (ISO / IEC 27002'nin öncüsü) 4 kuruluşta (profilde belirtilmemiş) uygulama deneyimlerini belirlemek üzere yarı yapılandırılmış görüşmelere dayanan bir çalışma yürütmüştür. Bulgulardan biri, çalışanların kişisel olarak değişiklik yapmadığı sürece bilgi güvenliği yönetim sistemini uygulamaya yönelik olumlu bir tutum sergilemesiydi. O andan itibaren tutumları, çalışmaya göre belirsizlik ve bilgi eksikliğinden kaynaklanan isteksizliğe dönüşmüştür. Benzer şekilde, Sussy ve diğ. [134]de Peru kamu kuruluşlarında ISO / IEC 27001 uygulamasının durumunu tanımladılar ve kritik başarı faktörlerini belirlediler. Sonuçlar 5 kuruluştaki vaka çalışmaları ile doğrulanmıştır. Ancak bu çalışmalar elektrik sektörüne yönelik değildir.

Elektrik sektörüne özgü olmayan bazı anketler mevcuttur [119,136]. ABD'deki 338 BT ve güvenlik uzmanını kapsayan Tenable Network Security anketine göre [136], tüm kuruluşların% 84'ü bir siber güvenlik çerçevesi benimsiyor. En popüler çerçeveler ISO / IEC 27001/27002 ve Kritik Altyapı Siber Güvenliğinin Geliştirilmesi İçin NIST Çerçevesini içerir. Kamu hizmetleri sektörü söz konusu olduğunda, katılımcıların sadece% 5'i siber güvenlik çerçevesinin kullanıldığını ilan etmiştir. İngiltere’de yapılan benzer bir anket (243 katılımcı) [119] yine en yaygın kabul gören standart olarak ISO / IEC 27001’i (≈% 22) göstermektedir. Ayrıca, bilimsel literatürde, ISO / IEC 27001'in “geniş kapsamlı bir standart” olduğu ortak bir görüş paylaşılmaktadır [87,93,143].

Analiz, konunun tartışmasız önemine rağmen, mevcut literatürde yeterince ayrıntılı olmadığını göstermektedir. Daha fazla araştırmaya ihtiyaç olduğu açıktır.

**8. İlgili iş**

Bölüm 4'te belirtildiği gibi, literatür araştırması sırasında siber güvenlikle ilgili mevcut standartları belirten akıllı şebeke standardizasyonu girişimleri belirlenmiştir. Çalışmalar uzman bilgisine dayanmaktadır ve analizlerin bilimsel bütünlüğünü amaçlamamaktadır. Böylece, bu amaca hizmet edecek sistematik bir metot belirlenmiyor. Sonuç olarak çeşitli standartlar oluşturuyorlar ve konuyu çeşitli açılardan ele alıyorlar.

Ayrıca, akıllı şebeke siber güvenlik standartlarını belirlemeye odaklanan 8 bilimsel makale tanımlanmıştır (bkz. Bölüm 4) [40,52,53,85,120,121,142,143].

Ruland ve diğ. [121] genel bakış IEC 62351, IEC 62443, IEC 62541-2, ISO / IEC 27019, NISTIR 7628, NERC CIP ve CEN-CENELEC-ETSI Akıllı Şebeke Koordinasyon Grubu'nun Akıllı Şebeke Bilgi Güvenliği'ni inceleyin ve odaklarını ve uygulama kapsamlarını karşılaştırın.

Griffin ve Langer [53] akıllı bir şebeke güvenlik mimarisi geliştirmeyi açıklar. Bu yaklaşım, NISTIR 7628, Akıllı Şebeke Koordinasyon Grubu’nun Akıllı Şebeke Mimarisi Modeli (SGAM) ve Sandia’nın geniş kapsamlı olarak açıklanan Mikro Şebeke Güvenlik Referans Mimarisi'ne (MSRA) dayanıyor. Ek olarak birkaç IEC ve IEEE standardı belirtilmiştir. Her ne kadar makale standartların tanımlanmasına veya değerlendirilmesine adanmamış olsa da, sağladığı referanslar ve açıklamalar yararlı olabilir.

Rosinger ve Uslar [120], beş standart setini (IEC 62351, IEC 62443 / ISA 99, NERC CIP ve ISO / IEC 27000) ve iki ulusal (Almanca) standart (BDEW Beyaz Bülteni [17] , Ağ Geçidi için Koruma Profili) , Akıllı Ölçüm Sistemi (Smart Meter Gateway PP) [89])sunmaktadır. Standartlar, akıllı bir şebekeye (üretme, ticaret, perakende satış, iletim, depolama, ölçüm, uygulama) belirli bir alana ekledikleri değere bağlı olarak kategorize edilir.

Kanabar ve diğ. [85] çeşitli güç iletim ve dağıtım ağlarındaki koruma, kontrol ve izleme uygulamaları için akıllı şebeke standartlarını kısaca açıklamaktadır. Güvenlik konusunda - IEC 62351 , IEEE 1686 ve NERC CIP, NIST SP 800–53 ve NIST SP 800–82 kısaca açıklanmıştır .

Goraj ve diğ. [52] genel bakış NERC CIP, IEEE 1686, IEC 62351, NISTIR 7628, CIGRE siber güvenlik ve bazı Avrupa siber güvenlik girişimleriyle ilgili teknik broşürler - elektrik trafo merkezlerine güvenli uzaktan erişim bağlamındadır.

Falk ve Fries [40], NERC CIP, Alman BDEW, NIST SGIP ve Avrupa Akıllı Şebeke Ortak Çalışma Grubu, standartlar ve kılavuzlar dahil olmak üzere akıllı şebeke güvenliği standardizasyon ve düzenleme girişimlerini, ayrıca standartlar ve yönergeleri özetlemektedir: NIST SP 1108, NISTIR 7628, ISO / IEC 62351, IEC 61850, ISO / IEC 15118, ISA99, IEEE 1686 ve RFC 6272.

Wang ve diğerleri Sekiz standart veya standart kümesini (NISTIR 7628, IEC 61850, GB / T 22239, IEC 62351, ISO / IEC 15408, GB18336, ISO 27001, GB / T 22080) ve dört standardizasyon kuruluşunu (IEC SG3, IEEE PES, NIST ve SGCC) [142]tanımlamaktadır.

Değerlendirmeler arasında, Wang ve ark. [143] en sistematiktir. İlk adımda, yazarlar şeffaf kriterlere dayanan bir literatür taraması yaparlar (standart kaynak, akıllı şebeke siber güvenliği ile ilgililik ve temsil edilebilirlik). NISTIR 7628, IEEE 1686- 2007, NERC CIP, NIST SP 800-53 ve SP 800-82 veya DHS Kataloğu gibi tanınmış standartları içeren 17 yayını belirtirler.

Tüm bu çalışmalar farklı seviyelerde tamamlanma göstermekte ve sıklıkla konuyu belirli bir açıdan ele almaktadır. [143] dışında, değerlendirmede kullanılan sistematik bir yöntemin ne de seçim / değerlendirme kriterlerinin ayrıntılarını sunmazlar. Bunların çoğu, aslında akıllı şebeke güvenliği ile ilgili standartlara ve kılavuzlara genel bir bakış niteliğindedir. Çalışmaların hiçbiri akıllı şebeke bileşenlerinin siber güvenlik değerlendirmesine konu edilmemiştir.

Bu yazıda sunulan araştırma aşağıdaki ayırt edici özellikleri sunar:

* Siber güvenlik değerlendirmesine adanmıştır - yazarın bildiği kadarıyla, konusuna ve gerçekliğine rağmen bu konuyu ele alan başka yayın yoktur.
* Açıkça tanımlanmış seçim ve değerlendirme kriterleri ile arama ve analiz yöntemi (bkz. Bölüm 5). tekrarlanabilir, sistematik ve titiz bir literatür uygulamasına bağlı olarak yüksek eksiksizlik güvencesi sağlar.
* Araştırma yönteminin detayları verilmiştir (bkz. Bölüm 4).
* Akıllı şebeke standartlarındaki güvenlik değerlendirmeleri hakkında kapsamlı rehberlik sağlar - 35 standart ve kılavuz, güvenlik değerlendirmesi perspektifinden tanımlanır, birbirlerine atıfta bulunur ve değerlendirme kriterleri ile ilgilidir.
* Tüm standartlar IEC akıllı şebeke mimarisine referansta bulunur (bkz. Şekil 1).

9. Sonuçlar

Çalışma, siber güvenlik değerlendirmelerinde akıllı bir şebeke standardının şu ana kadar belirtilmediğini gösteriyor. Akıllı şebeke için siber güvenlikle ilgili standartlar konuyu çeşitli boyutlarda ve farklı şekillerde ele almaktadır.

IACS'ye, trafo merkezlerine veya tüm akıllı şebeke bileşenlerine uygulanabilecek güvenlik değerlendirme süreçleri hakkında daha fazla bilgi sağlayan 6 akıllı şebeke veya güç sistemi standardı vardır (bkz. Tablo 5). Standartlar teknik özellikler olmadan oldukça genel rehberlik sağlar. Güvenlik değerlendirme politikalarının çıkarılması, sorumluluk atama veya güvenlik değerlendirme faaliyetlerinin zamanlanması gibi daha üst düzey faaliyetler için referans noktası olarak kullanılabilirler. Bunlardan dördü uygunluk testinde kullanılabilir. Refere SET, Samuray ve [124]

Daha ayrıntılı, genel ve teknik bilgiler, özellikle akıllı şebekelere yönelik olmayan 7 geniş uygulanabilirlik standardında (işletmeler, BT ürünleri) verilmektedir (bkz. Tablo 6). Bu standartlar akıllı şebeke işletme seviyesinin yanı sıra iletişim teknolojilerini ve işlem bilgilerini kullanan tüm bileşenlerine uygulanabilir. Standartlarda verilen rehberliğin yanı sıra, ilave yöntemleri ve araçları tanımlayan ileri literatüre birden fazla atıfta bulunulmuştur. Bunlar arasında NIST SP 800-115, en kapsamlı güvenlik değerlendirme rehberliği kaynağı olarak öne çıkıyor. Üç aşamalı bir güvenlik değerlendirme metodolojisini tanımlar, çeşitli değerlendirme tekniklerini tanımlar ve daha fazla literatüre ve yaklaşımlara referanslar sağlar [55,83,99,108,122]. Akıllı şebeke bilgi sistemlerinde siber güvenlik değerlendirmeleri konusunda rehberlik ararken bu belge ilk tercih olabilir.

Güvenlik değerlendirmelerine daha az ya da daha çok atıfta bulunan kalan 21 yayın, bu konuda ayrıntılı bilgi vermemektedir. Bunlar yine , örneğin değerlendirmelerin türü veya sıklığı ile ilgili üst düzey kararlar için kullanılabilir. Bunların çoğu uyumluluk testinde kullanılabilir.