SCADA DMS/OMS SİSTEMİ YENİLEME TEKNİK ŞARTNAMESİ

1. İşin Adı ve Tanımı

SCADA/DMS/OMS Renovasyon Projesi, Merkezi Kontrol ve Veri İzleme (SCADA) Sistemi, Dağıtım Yönetim Sistemi (DMS) ve Kesinti Yönetim Sistemi'nin (OMS) temini ve kurulumlarının gerçekleştirilmesi, mevcut izleme ve kontrol sistemlerinde yer alan izleme noktalarının (RTU, DCU ve EKK) temin edilecek yeni Sisteme dahil edilmesi ve Sistemin BT entegrasyonlarının (GIS, OMS, WFM, EDVARS, SAP, CRM, SENTİNEL, OSOS, TEİAŞ ICCP, TEDAŞ TALEP TAKİP vb. mevcut SCADA sistemine entegrasyonu olan sistemlerin) yapılmasıdır.

2. Amaç

Bu proje ile, Kontrol Merkezi'nin iyileştirilmesinin yanı sıra, işletme verimliğini arttırılması hedeflenmektedir. Kurulacak SCADA/DMS/OMS sistemleri tam merkezi yönetimi ve EPDK, TEDAŞ vb. meri mevzuat hükümlerini destekler bir mimariye sahip olacak, BT sistemleri ve üçüncü parti yazılımlar ile entegre çalışabilecek, sistem mimarisi güvenilirliği yeni kapsamın tamamı için iyileştirilmiş olacaktır.

3. İşin Kapsamı

Bu Şartnamedeki ana kapsam, Yönetimsel Kontrol ve Veri Toplama Sistemi (SCADA) ve Dağıtım Yönetim ve Arıza Yönetim Sistemleri (DMS/OMS) tesisi, yedekli bir Acil Durum Kontrol Merkezi (ADKM) sisteminin kurulumu, ŞİRKET'in diğer kurumsal BT sistemleriyle entegrasyonun sağlanmasıdır. Proje kapsamı 8 ana başlık altında tanımlanmaktadır.

- Şartnamede belirtilen tüm özellikleri ile SCADA/DMS/OMS Sisteminin; AKM ve ADKM kapsamlarına ait yazılımlarının, uygulamalarının tesisi ve devreye alınmaları,
- Mevcut İzleme ve Kontrol Sistemlerinin yeni SCADA/DMS/OMS Sistemine Aktarılması,
- Kapsam içerisindeki iş, ürün ve sistemlerin 6 Haziran 2023 Tarih ve 32213 sayılı Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği kapsamında 1.2.3.seviye göre detayları tarif edilen isterlere tam uygunluğunun sağlanması,

  Kapsam ve uyulması istenen kontroller ve yöntemi için detaylar 10.5 Siber Güvenlik başlığında verilmiştir.
- ŞİRKET'e ait GIS, WFM, SAP, CRM, OSOS, TEAİŞ ICCP, EDVARS vb. mevcut ADMS sistemine doğrudan entegrasyonu olan sistemler ile TEDAŞ TALEP TAKİP vb. mevcut ADMS sistemine dolaylı entegrasyonu olan sistemlerin, yeni kurulacak sisteme entegrasyonunun tüm ilgili paydaşlarıyla çalışılarak sağlanması ve hava durumu takip sistemi, araç takip sisteminin entegrasyon akışları ve tipleri karşılıklı çalıştaylarla netleştikten sonra, entegrasyonların ADMS tarafı YÜKLENİCİ, diğer birimlerin entegrasyon uçları sorumlulukları ŞİRKETE ait olacaktır.
- GIS Elektrik Şebeke Modelinin ADMS Sistemine aktarılması,
- İnceleme ve Testler
- Eğitimlerin ücretsiz olarak verilmesi

- Sistem üzerinde şebekeye ait çalışmaların, ADMS modülleri üzerinde isterlere uygun revizyonların/güncellemelerinin yapılması

4. Tanımlar

ŞİRKET: SAKARYA ELEKTRİK DAĞITIM A.Ş (SEDAŞ)

YÜKLENİCİ: İhaleyi Kazanıp Sözleşme İmzalayan Firma

SIEMENS SPECTRUM POWER 4.7: ŞİRKET tarafından aktif olarak kullanılan, IEC 60870-5-104 haberleşme standartları ile 407 RTU/DCU noktasının izlenmesini ve kontrolünü sağlayan Siemens firmasına ait SCADA yazılımıdır.

ADMS: Yönetimsel Kontrol ve Veri Toplama Sistemi / Dağıtım Yönetim Sistemi/ Kesinti Yönetim Sistemi

SCADA: Yönetimsel Kontrol ve Veri Toplama Sistemi

DMS: Dağıtım Yönetim Sistemi

OMS: Kesinti Yönetim Sistemi

ŞEBEKE MODELİ: OG ve AG, canlı (SCADA kapsamında) ve cansız istasyonları ve bağlantısallıklarını içeren elektrik ağının bütüncül modeli

CBS/GIS: Coğrafi Bilgi Sistemi

OSOS: Sayaç verilerinin otomatik olarak uzaktan okunabilmesi, verilerin merkezi bir sisteme aktarılması, doğrulanması amacıyla İşveren tarafından kurulmuş olan gerekli yazılım, donanım ve iletişim altyapısını kapsayan sistem.

WFM: İş Gücü Yönetimi Sistemi

CRM: Müşteri İlişkileri Yönetimi Sistemi

SENTİNEL: İş Gücü Yönetimi Sistem Arayüzü

ÇAĞRI MERKEZİ: ŞİRKET'in müşteri arıza bildirimlerinin gerçekleştirildiği merkez

EDVARS: Elektrik Dağıtım ŞİRKETleri veri ambarı sistemi

PRISM: ŞİRKET tarafından aktif olarak kullanılan, raporlama yazılımıdır. Mevcut sistemin alarmları, haberleşme takipleri ve raporlamaları bu yazılım üzerinden takip edilmektedir.

TEİAŞ ENTEGRASYONU (ICCP): Türkiye Elektrik İletim A.Ş. Sistemine ICCP (IEC 60870-6) protokolü ile veri aktarımının yapıldığı entegrasyon sistemidir.

TEDAŞ TALEP TAKİP: Kesinti bilgilerinin TEDAŞ'a iletildiği sistemdir.

SUNUCU: Sanal veya fiziksel sunucuları tanımlar.

FAIL-OVER: Online sunucudan otomatik yedekleme sunucusuna geçiş yapmayı tanımlar.

FAIL-BACK: Fail-Over durumunun sona erip sistemin orijinal durumuna geri yüklenmesini tanımlar.

AKM: Ana Kontrol Merkezi. Birincil öncelikli kullanılacak SCADA/DMS/OMS Sistemini tanımlar.

ADKM: Acil Durum Kontrol Merkezi. Afet, durumlarında AKM'nin yerine kullanılacak ve AKM'nin fonksiyonel olarak tüm özelliklerine sahip yedek SCADA/DMS/OMS Sistemidir.

ADMS TEST SİSTEMLERİ: SCADA/DMS/OMS yazılımının; ekran çizimi ve veri girişi yapılabileceği, diğer sistemlerle entegrasyon çalışmalarının denenebileceği, SCADA/DMS/OMS Sistemine uygulanabilecek her türlü hotfix, bugfix, güncelleme vb. süreçlerin yürütülebileceği test versiyonudur.

DAĞITIK ÜRETİM SANTRALLERİ İZLEME: Dağıtım şebekesine gömülü dağıtık üretim santrallerinin, şarj istasyonlarının, GES uygulamalarının vb. izlenip kontrol edileceği ve ister verilerin raporlanacağı SCADA/DMS/OMS yazılımı entegrasyonunu tanımlar.

İM/DM: İndirici Merkez ve Dağıtım Merkezleri, Dağıtım şebekesine bulunan bina tipi dağıtım transformatörleri ile büyük anahtarlama istasyonlarıdır.

KÖK: Özellikle kırsal bölgelerde bulunan bina küçük anahtarlama istasyonlarıdır.

FAU: Özellikle şehir merkezlerinde bulunan SEDAŞ elektrik dağıtım şebekesindeki bina tipi dağıtım transformatörleri ile diğer küçük anahtarlama merkezleridir. (Fider Otomasyon Noktası)

5. İş Yeri

ŞİRKET'in Ana Kontrol merkezi, Acil Durum Kontrol Merkezi ve Sakarya EDAŞ Genel Müdürlüğü çalışma ofisleri ile dağıtım şebekesi sahasında çalışmalar gerçekleştirilecektir. Ayrıca YÜKLENİCİ, çalışmanın mahiyetine göre kendisine tahsis edilen uzak bağlantı ile kendi belirleyeceği çalışma ofisinde ŞİRKET onayı ile çalışabilecektir.

6. İşin süresi

Sözleşme taslağında belirtildiği gibidir.

7. Bildirimler ve Kalite Parametreleri

İlgili Standartlar

ANSI/IEEE (Amerikan Ulusal Standartlar Enstitüsü, Elektrik Ve Elektronik Mühendisleri Enstitüsü)

- ANSI X3.28-1976: Belirli Veri İletişim Bağlantılarında Bilgi Değişimleri için Amerikan Ulusal Standart Kodu İletişim Kontrol Karakterleri Kullanımına Yönelik Prosedürler.
- ANSI/IEEE C37.1-2007: SCADA Ve Otomasyon Sistemleri için IEEE Standartları.
- IEEE Std. 610.12-1990: Yazılım Mühendisliği Terimler Sözlüğü.
- IEEE Std. 802.3-2008: Çarpışma Algılayıcıyla Çoklu Erişimde Çakışma Saptamalı Taşıyıcı Sezme Mantığı (CSMA/CD). Erişim yöntemi Ve Fiziksel Katman Özellikleri.
- ANSI/IEEE Std. 730-2002: Yazılım Kalite güvence Planları
- IEEE Std. 830-1998: Yazılım Gereklilikleri Özellikleri İçin IEEE Tarafından Önerilen Uygulamalar
- IEEE Std. 1815TM-2012: Elektrik Güç Sistemleri Haberleşmesi – Dağıtık Ağ Protokolü (DNP3)

IEC (Uluslararası Elektroteknik Komisyonu)

- IEC 60870: Telekontrol Ekipmanları ve Sistemleri
- IEC 60870-5: Tele Kontrol ve Güç Sistemleri Otomasyon Uygulamaları için standartlar bütünü.
- IEC 60870-6: ICCP (Inter Control Center Protocol) tele kontrol standardı.
- IEC 61850: Elektrik otomasyon sistemleri, akıllı elektronik cihazların konfigürasyonu için standart.
- IEC 61968 Uygulamaların Elektrik İdarelerinde Entegrasyonu - Dağıtım yönetimi için sistem ara yüzleri
- IEC 61970 Enerji yönetim sistemi uygulama programı ara yüzü (EMS-API)
- EC 62351 Güç Kontrol Sistemi ve İlgili İletişimler - Veri ve İletişim Güvenliği

8. İşin İfası ile İlgili Şartlar

8.1 YÜKLENİCİ Sorumlulukları

SCADA/DMS/OMS Sisteminin ve SCADA Test Sistemlerinin tüm altyapı ve donanımları ile tanımlandığı şekilde tasarım, test, tedarik, teslim, kurulum, kurulum denetimi, devreye alma ve garanti süreçleri ile bunlara ek olarak ŞİRKET'in personel eğitimlerinin verilmesi vb. olarak belirtilen ve aşağıda ifade edilen işler ;

1) Tüm altyapı/donanım gereklilikleri ŞİRKET in onayı doğrultusunda temini, tesisi, devreye alınması vb YÜKLENİCİ sorumluluğunda olacaktır.

2) Proje başlangıcında Şartnamede tarif edilen özelliklerde SCADA Test Sisteminin, AKM ve ADKM devreye alınıncaya kadar operasyonel ve ön test amacıyla sonrasında ise SCADA/DMS/OMS Sistemi üzerinden uygulanacak her türlü güncelleme, geliştirme, hotfix, bugfix vb. süreçlerin canlı sistemden önce tatbik edilmesi amacıyla kullanımı için kurulumu ve devreye alınması YÜKLENCİ sorumluluğunda olup, test sisteminde devreye almadığı hiçbir işlemi canlı sistemde uygulamaya geçmeyecektir. Tüm işlemler test sisteminde yapıldıktan sonra ŞİRKET onayına müteakip canlı sisteme alınacaktır.

3) Proje başlangıcı itibariyle ŞİRKET ile , ŞİRKET isterlerinin belirleneceği KAVRAMSAL çalışması yapılacak olup bu isterlere tam uyum sağlanacaktır.

4) Şartname kapsamında oluşturulacak tüm entegrasyon, kurulum, konfigrasyon vb yapılar için topoloji ve kavramsal tasarım dokümanları YÜKLENİCİ tarafından hazırlanacak ve ŞİRKETE teslim edilecektir.

5) Pilot Saha Kabul Testleri (PSAT)' kısmında detayları verilen ve tüm sistem kurulumlarının gerçekleşmesi öncesinde en temel donanım/yazılım kurulumları ile ŞİRKET tarafından belirlenen merkezlerin teklif edilen ADMS yazılımı üzerinde gösterilmesi,
6) ŞİRKET bünyesinde mevcut SCADA sistemi ve yeni yapılacak kumanda merkezi aynı anda devrede kalacaktır. YÜKLENİCİ yeni sistemin bağlantı ve devreye alınmasından sorumludur. Eski sistem ve saha ekipmanları tarafında yapılması gereken işlemler ŞİRKET sorumluluğunda olacaktır.
7) SCADA kabinlerinin yeniden çizilmesi, sinyallerin eklenmesi ve haberleşme linklemesi yapılması ŞİRKET sorumluluğunda olup, çalışma sürecinde alınan hataların gün içerisinde müdahalesi YÜKLENİCİ sorumluluğunda olacaktır.
8) SCADA kabinlerinin çizilmesi sonrasında tüm SCADA Kabinlerinde PTP ŞİRKET tarafından yapılacaktır. Testler esnasında sorun oluşması durumunda hataların gün içerisinde müdahalesi YÜKLENİCİ sorumluluğunda olacaktır. 5 istasyon için PTP sürecinde uzaktan anlık destek YÜKLENİCİ tarafından sağlanacaktır.
9) YÜKLENİCİ, mevcut sistemdeki ŞİRKET tarafından dışa aktarılan Oracle veri tabanındaki verilerini yeni sistemin veri tabanına taşıyacaktır. YÜKLENİCİ aktarımlar esnasında yapılması gereken tüm migrasyon planlarını ŞİRKET ile paylaşacaktır.
10) AKM'nin şartnamede belirtilen tüm uygulamaları/yazılımları ile temini, tesisi, altyapı kurulumu, devreye alınması ve güncellemelerinin yapılması sağlanacaktır.
11) ADKM'nin şartnamede belirtilen tüm uygulamaları/yazılımları ile temini, tesisi, altyapı kurulumu, devreye alınması ve güncellemelerinin yapılması sağlanacaktır.
12) Proje boyunca temin edilen her türlü lisansın mevcuttaki donanım, entegrasyon ve yazılım lisanları ile sistem mimarisi içerisinde bir bütün olarak uyumlu çalışması sağlanacaktır.
13) Bu Şartname ve Sözleşme şartlarına uygun olarak, SCADA/DMS/OMS Sisteminin kendinden beklendiği şekilde tam olarak çalıştırılması için gerekli olacak tüm kurulumların ve devreye alınmaların tamamlanması,
14) Şartnamenin Testler ve Kabuller başlığı altında bulunan tüm testlerin gerçekleştirilmesi,
15) Sistemin performans testlerinin yapılması,
16) Bu Şartnamede belirtilen tüm eğitimlerin verilmesi,
17) Bu Şartnamede istenen tüm dokümantasyonların teslim edilmesi,
18) Proje ilerleme raporlarının haftalık ve günlük periyodik olarak hazırlanıp ŞİRKET'e iletilmesi,
19) Proje başlangıcında GANTT diyagramı ile bir zaman planı hazırlanarak ŞİRKET onayının alınması. İlerleyen süreçte revizyon gerekirse, gerekli güncellemelerin yapılarak revize zaman planının ŞİRKET'e iletilerek onay alınması.
20) ŞİRKET tarafından proje yürütümünde SCADA/DMS/OMS ve kontrol merkezi sistemlerinde talep edilecek özelleştirme ve konfigürasyonların uygulanması.

21) YÜKLENİCİ, proje kapsamında temin ve tesis edeceği donanımların PR (Product Release) ve EOL (End of Life) tarihleri belirtilecektir.
22) Acil durum haberleşme kesme ve acil durum polis çağrı butonlarının temini ve tesisi sağlanacaktır. Detayları KAVRAMSALda ŞİRKET ile belirlenecektir.
23) YÜKLENİCİ, proje süresince son geçici kabul tarihine kadar temin ve tesis edeceği donanım/yazılım ve altyapının güncelliğinden proje ve garanti süresince sorumlu olacaktır. Güncel bir sürüm gelmesi durumunda son güncellemeleri temin ve tesis edecektir.
24) SCADA/DMS/OMS sistemi için gerekli (server odası, operatör odası vs.) tüm data, ekstra ihtiyaç duyulacak enerji vs. kablajının işçiliği, montajı ve malzemesine yönelik ihtiyaçların belirlenerek ŞİRKET'e bildirilmesinden YÜKLENİCİ sorumlu olacaktır. Kontrol merkezi iç işlerinin yapılması süresince, ŞİRKET ile koordineli çalışma çerçevesinde, sistem için gerekli şaftların, rezervasyonların ve mekân hacimlerinin ölçüleri, şekilleri ve cihazların yerleşimi için mimari ve inşaat gereksinimler ile bilgileri ŞİRKET'e verecektir. İşin yapılması ŞİRKET sorumluluğundadır.
25) Kontrol Merkezi'nde, SCADA/DMS/OMS Sistemi için gerekli tüm konektörler ve donanımlara sahip UPS Sistemlerinin tüm kablolama ve irtibatları dahil olmak üzere, tasarımı, tedariki ve kurulumuna yönelik gereksinimlerin belirlenmesinde ŞİRKET ile koordineli çalışma çerçevesinde işi yürütecektir. İşin yapılması ŞİRKET sorumluluğundadır.
26) Kontrol Merkezi Haberleşme Ağı sistemlerinin uygulanması, (Örneğin: tasarım, yapılandırma, veri mühendisliği, kurulum ve devreye alma, kablaj hariç)
27) Haberleşme alt yapısının uçtan uca temini ve kurulumu,
28) Gerekli tüm haberleşmelerin sağlanması için kontrol merkezi telekomünikasyon ekipmanlarının (Örneğin, ön-uç işlemciler, LAN switch, vb. kablaj hariç) ve ilgili hizmetlerin uygulanması,
29) YÜKLENİCİ, ŞİRKET kaynaklarına yapacağı tüm erişimler için, ŞİRKET'in belirleyeceği yöntemleri/teknolojileri (PAM,2FA,VPN vb.) kullanacaktır.
30) Şartname kapsamında YÜKLENİCİ tarafından sağlanan yazılım ve donanım kapasiteleri belirlenirken, ilave olarak hali hazırda ŞİRKET tarafından kullanılmakta olan sistemlerde göz önünde bulundurulmalıdır. Bu sistemler için kapasite ihtiyacı ve yazılım lisansları (yedekleme, antivirüs, monitoring vb. lisansları) YÜKLENİCİ tarafından kurulacak olan yeni sunucu platformu içerisinde karşılanacaktır. YÜKLENİCİ tarafından bu ilave ihtiyaç için sağlanan Microsoft lisanları için sahiplik ŞİRKET, Microsoft Enterprise Agreement sözleşmesi dahilinde yapılacaktır.
31) Yapılacak tüm çalışmalar için EK-2.4. EPDK Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Referans Topolojisi baz alınacaktır ve tam uyum sağlanacaktır.
32) SCADA/DMS/OMS Sistemi haricinde ŞİRKET tarafından ihtiyaç duyulan donanım altyapısı aşağıda belirtilmiştir. YÜKLENİCİ kendi kuracağı sistemler için gerekli donanım altyapısını belirtecek, aşağıda bulanan donanımı da kapsayacak şekilde bir sunucu parkuru oluşturarak temin ve tesis edecektir. Aşağıda bulunan donanımlar ŞİRKET tarafından SCADA/DMS/OMS harici(Siber Güvenlik vb) sistemler için kullanılacaktır.

Sanal sunucuların kapasite ve lisans bilgileri şu şekildedir;

Ana Veri Merkezi;

400 GB RAM
150 V-Core CPU
15 TB Disk Kapasitesi
15 adet Windows Server işletim sistemli sanal sunucu
7 adet Linux işletim sistemli sanal sunucu

Acil Durum Kontrol Merkezi;
200 GB RAM
50 V-Core CPU
5 TB Disk Kapasitesi
5 adet Windows Server işletim sistemli sanal sunucu
3 adet Linux işletim sistemli sanal sunucu

8.2 ŞİRKET Sorumlulukları

ŞİRKET, YÜKLENİCİNİN talep ettiği ve iş kalemlerinin gerektirdiği aşağıda belirtilen teknik bilgileri tedarik edecektir,

1) Proje yönetimi ve koordinasyonu,
2) SCADA/DMS/OMS Sisteminin kurulması için gereksinimleri YÜKLENİCİ tarafından belirlenen tüm donanım / yazılımın onayı ŞİRKET tarafından yapılacaktır.
3) SCADA kabinlerinin yeniden çizilmesi, sinyallerin eklenmesi ve haberleşme linklemesinin yapılması ŞİRKET sorumluluğunda olacaktır.
4) SCADA/DMS/OMS Sisteminin kurularak işletileceği lokasyonlarda YÜKLENİCİ personelinin çalışabileceği ortamın tahsis edilmesi,
5) YÜKLENİCİ personelinin uzaktan yürütebileceği süreçleri için gerekli uzak bağlantı hesaplarının oluşturulması,
6) Şartname gerekliliklerinden dolayı kurulacak olan altyapı (işletim sistemi, veri tabanı vb.) yönetimi ve idamesi ŞİRKET tarafından yapılacak olmakla beraber bu kapsamda dolabilecek ihtiyaçlar konusunda YÜKLENİCİ gerekli desteği sağlayacaktır.

9. Mevcut Sistem ve Entegrasyonlar

Bu başlıklar altında tanımlanan fonksiyonların ve entegrasyonların tamamı (DMS Fonksiyonlarından sadece Şartnamede ister olarak belirtilenler) ve Şartnamede istenen diğer koşullar ile işbu SCADA/DMS/OMS Projesi kapsamında temin edilecek yeni SCADA/DMS/OMS Sisteminde çalışır durumda ŞİRKET'e teslim edilecektir.

9.1 Mevcut Sistem Mimarisi

SEDAŞ SCADA/DMS/OMS projesi kapsamında yapılan sistem SCADA, DMS ve OMS fonksiyonlarını ihtiva eder.

Bütün sunucular ve operatör bilgisayarları yedekli LAN ile birbirlerine bağlıdır.

Mevcutta Gebze'de Ana Kontrol Merkezi ve Sakarya'da Acil Durum Kontrol Merkezi bulunmaktadır.

Ana kontrol merkezinde 10 iş istasyonu ve acil kontrol merkezinde 2 iş istasyonu bulunmaktadır.

9.2 Raporlama Sistemi (PRISM)

Raporlama sistemi, enerji verilerini görselleştirmek ve tüm kurum içinde erişilebilir hale getirmek için kullanılan bir yazılım platformudur. Raporlama, SCADA/DMS/OMS sisteminden veri toplayan ve ardından bu verileri kendi zaman serisi veri tabanında depolayan harici bir çözümdür ve BT sistemi üzerinde konumlandırılmıştır. SCADA /DMS/OMS den, raporlama sisteminin zaman bazlı veri tabanına tek yönlü veri aktarımı yapılmaktadır. SCADA analog ve dijital verileri otomatik olarak raporlama sistemine akmaktadır. Analog ve dijital verilerde sahadan SCADA'ya gelen tüm değişimler sistem üzerinde saklanmaktadır. SCADA/DMS/OMS Projesi kapsamında temin edilecek yeni SCADA/DMS/OMS den Raporlama Sistemine anlık veri akışı sağlanması beklenmektedir.

9.3 Dashboard Sistemi

İndirici Trafo Merkezi ve Üreticilere ait anlık yüklenme ve Sistem Kullanım anlaşması limit değerlerine göre verileri gösterir.

9.4 GIS Verileri Importu

ŞİRKET GIS uygulaması olarak Başarsoft'un PowerNetMaestro yazılımını kullanmaktadır. Mevcut GIS import süreci ŞİRKETin csv ve dxf olarak export aldığı verileri aylık olarak SCADA sistemine hata ayıklama süreciyle birlikte gerçekleşmektedir.

9.5 Üretici Verilerinin Importu

Üretim Tesislerinin GIS koordinat bilgilerine istinaden SCADA GIS haritasına ikon ile manuel girişleri yapılmaktadır.

AG Panolardan, OG hücrelerden ve/veya kabinden gelen analog ve dijital sinyaller sahada tesis edilen RTU'ya aktarılmaktadır. RTU ile IEC 60870-5-104 haberleşme protokolü kullanılarak SEDAŞ SCADA Kontrol Merkezinde bulunan SCADA yazılımına iletilmektedir. Ayrıca sahada tesis edilmiş olan Enerji Kalite Kaydedicisinin verileri, SEDAŞ ağında bulunan Teknik Kalite İzleme Yazılımına aktarılmaktadır.

9.6 Müşteri Verileri Importu

ŞİRKET Kesinti Yönetim Sistemi'nde kullanılması için müşteri verilerini aylık periyotta SAP ISU sisteminde export alarak ve hata ayıklaması yaparak SCADA sistemine csv formatında yüklemektedir.

9.7 DMS Fonksiyonları

SPM: Switching Procudure Management

Operatörün, anahtarlama prosedürleri oluşturmasını, düzenlemesini, daha önce hazırlanmış bir prosedürü seçmesini, sıralamasını, çıktı almasını, yürütmesini ve kaydetmesini sağlar. Anahtarlama Prosedür Yönetimi, planlı bakım çalışmaları gibi operasyonları yürütmek için kullanılmaktadır.

PF: Power Flow

Dağıtım Sistemi Güç Akışı fonksiyonu, sahadan gelen ölçümleri, kullanıcı tarafından belirlenmiş ve atanmış yük tiplerini ve anlık topoloji verilerini kullanarak sistemin her noktasındaki akım, voltaj, aktif/reaktif güç ve diğer güç verilerini, teknik kayıplarını hesaplar.

OFR: Optimum Feeder Reconfiguration

Hattaki veya transformatördeki aşırı yük gibi olumsuz çalışma koşullarını ortadan kaldırmak için gerekli olan optimal şebeke yapılandırmasını belirler. Bu işlev operatörlere, sistem kayıplarını azaltan ve indirici Trafo Merkezlerin/Dağıtım Merkezlerinin yükünü dengeleyen, dağıtım fiderlerinin yeniden yapılandırılmasını uygulayan bir dizi anahtarlama etkinliği önerir.

FISR: Fault Isolation Service and Restoration

Arıza izolasyonu ve enerjilendirme fonksiyonu herhangi bir nedenle izole edilmesi gereken bir bölgenin, enerjisinin kesilmesi için gerekli manevraları belirler. Ayrıca bu manevraların, izole edilecek bölge dışında kalan ekipmanlar üzerindeki etkilerini de minimize eder.

FLOC: Fault Location

Arıza Yeri Bulma (Fault Location), SCADA dan ve Kesinti Yönetimi Sistemi (OMS) alınan verilere göre, arıza yerinin anahtarlarla ve/veya arıza akım göstergeleriyle olası en küçük arızalı bölümü tespit eder.

SCC: Short Circuit Calculation

Kısa devre akımı hesaplaması fonksiyonu, bir bölgede meydana gelebilecek herhangi bir arıza durumunda, kaynaktan arızalı bölgeye doğru oluşacak kısa devre akımlarını hesaplar.

VVAR: Volt/VAr CONTROL

Volt-VAr Kontrolü, sistem gerilim seviyesini ve reaktif güç akışını düzenlemek için kullanılır. Volt-VAr, düzenleme işlemi transformatör tap seviyelerini (gerilim regülatörlerini) ve kapasitör anahtarlarını kullanarak gerçekleştirir.

9.8 BT Entegrasyonları

SCADA sistemiyle entegre mevcut sistemler:

OSOS: Otomatik sayaç okuma sistemi ile, ilgili sistemde bulunan sayaçlardan enerji var/yok bilgisi alınarak kesinti yönetimi sistemine bu bilgilerin aktarılması sağlanır.

CRM: Müşteri ilişkileri yönetimi sistemi ile, Müşterilerden gelen kesinti çağrı kayıtlarının, kesinti yönetimi sistemine aktarılması sağlanır. İlişkilendirilen kesintiye ait bilgilerin de tekrar bu sistemdeki çağrı kaydı verilerini güncellemesi sağlanır.

SAP-WFM/SENTİNEL: Kesinti yönetimi sistemi ile entegre olan operasyonel süreçlerin yönetimine ait verileri işler ve veri akışını sağlar. Kesinti yönetimine ait kesinti kayıtları SAP-WFM'e iletilerek bir sipariş oluşturulması sağlanır. İşgücü yönetimi ve kesinti yönetimi ile entegrasyonu ile, siparişlere ait verilerin trafiği ve işlenmesi sağlanır.

İş gücü yönetimi sistemi (Sentinel) ile, iş havuzuna aktarılan kesinti kayıtlarının saha ekip tabletlerine atama yapılması sağlanır. Ekip tarafından tablet üzerinde girilen değerler ve aşamalar kesinti yönetimi sistemine aktarılır.

EDVARS: Elektrik Dağıtım ŞİRKETlerine ait kesinti kaydı verilerinin toplandığı yerdir. İlgili entegrasyon sistemi ile günlük olarak ŞİRKET'e ait kesinti yönetimi sistemi verilerinin aktarılması sağlanır.

TEDAŞ TALEP TAKİP: Elektrik Dağıtım ŞİRKETlerine ait kesinti kaydı verilerinin toplandığı yerdir. İlgili entegrasyon sistemi ile anlık olarak ŞİRKET'e ait kesinti yönetimi sistemi verilerinin aktarılması sağlanır.

TEİAŞ MERKEZLERİ İZLEME: ŞİRKET**,** TEİAŞ indirici Trafo Merkezlerinden enerji aldığı fiderlerin pozisyon bilgilerini ve bu fiderlerin analog verilerini SCADA Sisteminde izler.

9.9 Kesinti Yönetimi Sistemi (OMS)

Kesinti kayıtlarının oluşmasından kapatılmasına kadar olan sürecin yürütüldüğü sistemdir.

Kesintiler planlı ve plansız olmak üzere iki ana başlıkta yürütülür.

Planlı Kesintiler:

Bakım çalışmaları için, planlı kesintiler yönetim sürecine uygun olarak 48 saat önceden SPM ve OMS de ilişkili olarak oluşturulan kesintilerdir.

Plansız Kesintiler Oluş Türleri;

- SCADA
- OSOS
- Çağrı Kaydı
- Manuel Tetikleme

SCADA Açmaları Nedeni ile Oluşan Kesintiler;

SCADA (Telemetrili) kabinlerde meydana gelen kesici açmalarında sistem otomatik bir kesinti kaydı oluşturur. Bu kesinti kaydında kesintiden etkilenen tüm trafolar, müşteriler ve akıllı sayaçlar otomatik olarak listelenir. Kesinti yaşanan bölgeden gelen OSOS enerji yok sinyalleri ve çağrı kayıtları otomatik olarak kesinti ile ilişkilendirilir ve yeni kesinti kaydı oluşturmaz. Oluşan kesinti saha ekibinin müdahalesini gerektiriyor ise WFM sistemine senkron edilir ve SAP sisteminde bir sipariş oluşur. SAP sisteminde oluşan kesinti saha ekibinin tabletine gönderilir ve ekibin arıza noktasına yönlendirilmesi sağlanır. Saha ekibinin bu sipariş ile ilgili yaptığı işlemler OMS ekranından takip edilir. Sipariş atanan ekip tabletinden işi yürütürken OMS ekranına gelen WFM aşamaları şunlardır.

- **Ekip Atama Onay:** Henüz tablete ulaşmamış.
- **Alındı:** Ekibin tabletine ulaştı.
- **Ön kabul:** Ekip işi gördü.
- **Yola çıktım:** Ekip işi kabul edip yola çıktı.
- **Adresteyim:** Ekip adrese ulaştı kesinti noktasını tespit edecek.
- **İşe başla :** Bu aşama ekibin kesinti noktasını onayladığı ve açık anahtarlama yaptığı aşamadır. Ayrıca tahmini enerji verme zamanını günceller.
- **Manevra Tamamlandı:** Ekip tüm fidere enerji vermiş ve son anahtarlama yapmıştır. Bu aşama kesinti bitmiş anlamına gelir. İşe başla ve manevra tamamlandı arasında ekibin yaptığı tüm anahtarlamalar kesinti kaydı içerisine otomatik olarak düşer.
- **Tamamlandı:** Ekip bölgedeki son kontrollerini ve kullandığı malzemelerin düşümünü yapıp işi kapatır.

Daha sonra Operatör kaydın anahtarlamalarını kontrol edip kaydı teftişe hazır aşamasına alır. Kontroller sonunda kayıt arşivlenir.

OSOS Sinyalleri ile Oluşan Kesintiler;

Trafolarda ve müşterilerde mevcut olan akıllı sayaçlardan gelen enerji yok sinyalleri ile oluşan kesinti tipidir. Aynı anda gelen OSOS sinyalleri sistem tarafından otomatik olarak tek bir kesintide toplanır ve tahmini bir kesinti noktası ile bir kesinti kaydı oluşturur.

Çağrı Kaydı ile Oluşan Kesintiler;

Çağrı merkezinden alınan müşteri kesinti bildirimleri CRM entegrasyonu ile kesinti yönetimi sistemine ulaşmaktadır ve ilişkili kesintiler ile ilgili bilgiler CRM tarafını güncellemektedir. Çağrı merkezi sisteminden kesinti bildirimleri normal ya da fuzzy (kesinti noktasına ait elektriksel adres tam olarak belli değil) olarak gelmektedir. Gelen bildirimler mevcut kesintiler ile ilişkilendirilemiyorsa sistem otomatik olarak tek abonenin etkilendiği tahmini bir kesinti kaydı oluşturur. Aynı bina, aynı SDK veya aynı trafoya tanımlı farklı bir bildirim gelirse otomatik olarak bu kesinti ile ilişkilenip kesinti noktasını bir üst seviyeye çıkartır. Bu kesinti noktaları aşağıdaki sıra ile en üst şebeke unsuruna kadar ulaştırılır;

- Abone Tesisi
- AG Bina

- AG SDK
- AG Fider
- Trafo Ana Şalteri

Manuel Tetikleme ile Oluşan Kesintiler;

Diğer üç durumun gerçekleşmediği fakat saha ekibi tarafından tespit edilen emniyet amaçlı, acil kesinti yapılması gerektiğinde oluşan kesintilerdir. Sistem yapılan manuel tetikleme ile yeni bir kesinti kaydı oluşturur.

Yukarıdaki kesinti aşamaları tüm kesinti tipleri için geçerlidir. Sadece SCADA anahtarlamalarının saha tarafından yapılması gerekmez. Diğer anahtarlamalar tabletten yapılmalı ve kesinti kaydında anahtarlama olarak görünmesi gerekmektedir.

9.10 Alarm Yönetimi

SCADA kapsamındaki telemetrili istasyonlardan gelen alarmlar izlenmekte ve alarm türüne ve Sinyal Yönetim Planına göre Operatör tarafından aksiyon alınmaktadır. SCADA kabinlerinden gelen alarm Genel ve Sistem alarmları olarak iki kategoriye ayrılmaktadır.

a) Genel Alarmlar, kendi içinde Şebeke, Saha, Limit ve Test alarmları olarak dört farklı tabloda izlenebilmekte, alarmın türüne göre SENTİNEL sisteminden iş emri açılıp saha ekipleri yönlendirilmektedir. Alarmlara ve kabinlere alınan aksiyon ile ilgili not yazılabilmektedir.
b) Scadalı binalarda röle açma sinyali alıp kesici pozisyonu değişmeyen objeler raporlanabilir olacaktır. İlgili şebeke unsuru için SAP otomatik siparişi açılacaktır.
c) Sistem Alarmları, kendi içinde sistem, RTU, iletişim olmak üzere üç farklı tabloda izlenebilmekte alarmın türüne göre SENTİNEL sisteminden iş emri açılıp ekipler kabinlere yönlendirilmektedir. Alarmlara ve kabinlere alınan aksiyon ile ilgili not yazılabilmektedir.
d) Acil durum alarmlarının listelendiği farklı bir acil alarm tablosu listelenebilmektedir.

9.11 Uç Nokta SCADA Haberleşme Yapısı

Mevcut Sistemde, Dağıtım Merkezleri, TEİAŞ İndirici Merkezleri ve 3.Şahıslara ait üretim tesislerine ait RTU ve DCU lar IEC 60870-5-104 protokolü, Enerji kalite analizörleri ise Modbus TCP/IP protokolü ile haberleşmektedir.

Mevcutta 480 RTU/DCU ve 2859 Fider ile yaklaşık 150000 sinyal SCADA sistemine aktarılmaktadır.

Uç noktalardan alınan analog değer ve sinyaller Şartname Eki EK-2.1 olarak verilmiştir.

Ayrıca

Uç noktalarda RTU lara veriler farklı haberleşme protokolleri (IEC 61850, MODBUS TCP/IP, MODBUS RTU, IEC 60870-5-104) ve Hard Wired olarak aktarılmaktadır.

10. Yeni ADMS Teknik Özellikleri ve İsterleri

10.1 SCADA/DMS/OMS Genel Sistem Mimarisi

1) SCADA/DMS/OMS Sistemi, Ana Kontrol Merkezi (AKM), Acil Durum Kontrol Merkezi'nden (ADKM) ve Mühendislik Veri Kontrol Merkezi'nden oluşacaktır.
2) AKM Sistem Mimarisi ise SCADA/DMS/OMS, Test Sistemi ve Operatör Eğitim Sistemi bileşenlerinden oluşacaktır.
3) AKM'de, tüm sunucu donanımları ve üzerlerinde çalışacak uygulama yazılımları tam yedeklilik sağlanacak şekilde kurulacak ve konfigüre edileceklerdir. AKM'ni işlevsiz hale getirecek herhangi bir durum meydana geldiğinde, SCADA/DMS/OMS sistem fonksiyonları ve şebeke operasyonları ADKM tarafından yürütülecektir. ADKM' nin sistem yönetimini devralması, kullanıcı ekranlarına geçiş sebebi ile alarm olarak gösterilecektir.
4) Saha ekipmanları ile AKM arasındaki iletişim, ADKM sistem yönetimini devraldığında otomatik olarak ADKM'e yönlendirilecektir. ADKM iletişimin yeniden yönlendirilmesi için tüm saha iletişim cihazlarını tetikleyecektir. İletişim yolunun dinamik olarak geçişi herhangi bir iletişim ve veri kaybına neden olmayacaktır. İletişim esnasında oluşacak hatalar raporlanabilir olacaktır.
5) Tüm iş istasyonları AKM ve ADKM ile iletişim kurma özelliğine sahip olacaktır. AKM Yönetimdeyken tüm iş istasyonları AKM ile, ADKM sistem yönetimini devraldığında ise tüm iş istasyonları otomatik olarak ADKM sunucuları ile iletişim kuracaktır.
6) İş istasyonlarının yetkileri, erişim hakları, kullanıcı tanımlamaları ve kontrol alanları tamamen kullanıcı (Sistem Yöneticisi) tarafından tanımlanabilir olacaktır.
7) İş istasyonları için 6 Haziran 2023 Tarih ve 32213 sayılı Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği kapsamında 1.2.3.seviye isterlere uygun kontrol merkezi kapsamında sağlanması gereken koruma (yazılımsal ve/veya donanımsal) YÜKLENİCİ tarafından sağlanacaktır.
8) İşbu sözleşme kapsamında SCADA network haricinde yapılacak olan bağlantılar için web üzerinden erişim imkanı verilecek olup, en az Kesinti bilgileri, Şebeke anlık topolojisi, ekip konumu, etkilenen abone, çağrı detayları vb(Detayları kavramsalda ŞİRKET tarafından belirlenecektir) verileri görecek web erişim platformu YÜKLENİCİ tarafından sağlanacaktır. Sağlanacak olan web platformu için yetkilendirme özelliği olmalı (görülecek veriler, bölgesel ayrım, şebeke topolojisi, kesinti bilgileri, ihbar giriş ekranları, planlı kesinti giriş ekranı). Bağlantılar için anlık en az 300 kullanıcı bağlantı imkanı vermelidir.
9) İş istasyonlarının yetkileri, erişim hakları, kullanıcı tanımlamaları ve kontrol alanları kavramsal tasarım sürecinde YÜKLENİCİ tarafından ŞİRKET'in onayına sunulacaktır. Bu yetkiler ve kullanıcı grupları ŞİRKET tarafından yönetilebilir olacaktır. İstenen kriterlere uygun güncellenebilir olmalıdır.

10) Ana Kontrol Merkezi

SCADA/DMS/OMS sistemi; dağıtım şebekesinin yönetilmesi, işletilmesi ve kontrol edilebilmesi için gerçek zamanlı kontrol modunda olan;

a) Şebeke Kontrol İş İstasyonlarının bağlanmasına izin verecektir ve eş zamanlı olarak 19 adet Şebeke Kontrol İş İstasyonunun herhangi bir performans kaybı yaşanmadan bağlanmasına imkan sağlayacaktır.
b) Ana Kontrol Merkezi Sakarya'da konumlanacaktır. Gebze lokasyonunda 5 adet Mühendislik Veri Kontrol Uzak İş İstasyonları kullanılacak şekilde altyapı planlaması ,temini ve tesisi yapılacaktır.

11) Acil Durum Kontrol Merkezi

a) Acil Durumu Kontrol Merkezi, AKM devre dışı kaldığında ya da aktif edildiğinde iki (2) dakika içerisinde SCADA/DMS/OMS sistemi aktif kullanılabilir hale gelecektir.
b) Proje esnasında ŞİRKET tarafından belirlenen lokasyonda Şebeke Kontrol İş İstasyonlarının kurulumu sağlanacaktır. Acil Durum Kontrol Merkezi dört (4) iş istasyonuna sahip olacaktır.

10.2 Genel Sistem Gereklilikleri

1) SCADA/DMS/OMS Sistemi 'haberleşme sunucuları' saniyede en az 10.000 (10 bin) protokol mesajı (IEC60870-5-104, NTP, TCP, UDP vb.) işleyebilecek ve 'gerçek zamanlı SCADA sunucuları' ise, saniyede en az 10.000 (on bin) IEC-60870-5-104 protokol paketini (veri, onaylama vb.) sorunsuz ve herhangi bir performans kaybı olmaksızın işleyebilecek yeterlilikte olacaktır.
2) SCADA/DMS/OMS Sistemine min. 6000 sayıda sınır yönetim cihazı (RTU, PLC, Gateway, FCD, FID, Recloser, Sectionalizer vb.) tanımlanabilecektir. SCADA/DMS/OMS Sistemi, en az 800.000 I/O tagi ile belirtilen performans kriterlerini sağlayacak şekilde çalışabilecektir.
3) SCADA/DMS/OMS Sistemi sunucuları ve iş istasyonları Şartnamenin gerekliliklerini karşılamak üzere boyutlandırılmış RAM kapasitesine sahip olacaktır. SCADA/DMS/OMS Sistemi sunucularının/iş istasyonlarının ortalama CPU kullanımı, ağır yük koşulları altında (Stres testlerinde kriterler ŞİRKET tarafından belirlenmiştir.) dahi yüzde yetmiş beş (%75) geçmeyecektir. SCADA/DMS/OMS Sistemi depolama kapasitesi, bu Şartnamenin şartlarını karşılayacak şekilde boyutlandırılacak ve genişletilebilir olacaktır. Garanti Süresini de kapsayacak şekilde sistem depolama kapasitesi için gerekli olacak genişleme gereklikleri ilk fiyata dahilinde olacaktır
4) Sahada gerçekleşen zaman etiketli bir değişimin SCADA sunucularına erişmesi ile değişimin operatör iş istasyonları alarm/olay, grafik ara yüzleri vb. üzerinde gösterilmesi arasında geçen süre ortalama bir (1) saniyeyi geçmeyecektir.
5) Belirtilen performans kriterleri, Ana ve Acil Durum Kontrol Merkezleri kabul testleri ve saha kabul testlerinde belirleyici olacaktır. YÜKLENİCİ sistemin yazılım tasarımını istenilen performans değerlerini sağlayacak şekilde yapmakla, donanım gereksinimlerini belirlemekle, temin ve tesis etmekle sorumlu olacaktır. Performans testlerinin sağlanmaması durumunda gerekli donanım/yazılım iyileştirmeleri YÜKLENİCİ sorumluluğundadır.
6) Herhangi bir uygulama sunucusunun soğuk başlangıç (POST – Power On Self Test) ile çalışır duruma gelme süresi on beş (15) dakikayı geçmeyecektir.
7) Sıcak Yedekli sunucuların 'Fail-Over' süresi on (10) saniyeyi geçmeyecektir.
8) AKM ile ADKM arasındaki 'Fail-Over' süresi iki (2) dakikayı geçmeyecektir.

9) Tüm dağıtım şebekesi üzerinde tanımlanmış yük akışı uygulamasının çalıştırılması en fazla on (10) dakika sürecektir.
10) Tüm dağıtım şebekesi üzerinde tanımlanmış topoloji analiz/işletim uygulamasının çalıştırılması en fazla on (10) dakika sürecektir.
11) Bir arıza lokasyonu için Arıza yeri izolasyonu ve servis restorasyonu uygulamasının çalıştırılması en fazla bir (1) dakika sürecektir.

10.3 Donanımlar

YÜKLENİCİ, SCADA/DMS/OMS Sisteminin yedeklilik ve Şartnamede istenen sistem gerekliliklerini karşılamak için gerekli sayıda sunucu, veri depolama, switch ve iş istasyonunu temin ve tesis edecektir. Seçilecek donanımın 5 yıl boyunca herhangi bir ilave olmadan kabul esnasındaki performans koşullarını sağlayarak kullanılabilecek şekilde tasarlanması gerekmektedir.

Ana Kontrol Merkezi on iki (12) iş istasyonuna, Gebze lokasyonunda 5 adet Mühendislik Veri Kontrol Uzak İş İstasyonuna, Acil Durum Kontrol Merkezi ise dört (4) iş istasyonuna sahip olacaktır.

Her bir iş istasyonu başına 4 adet monitör, kablosuz klavye mouse, kulaklık, tüm donanımları ve lisansları ve gerekli mühendislik işleri dahil olacak şekilde YÜKLENİCİ tarafından sağlanacaktır. Donanım özelliklerinin detayları aşağıdaki maddelerde belirtilmiştir.

10.3.1 Sunucular

Sunucularda aşağıdaki donanımlar minimum olarak karşılanmalıdır.

a) En az 2 adet CPU ve en az Intel Xeon-Gold 6348 serisi işlemci kullanılacaktır.
b) DDR4 3200 MT/s RAM ve RAM slotlarının en fazla yüzde sekseni (%80) kullanılacaktır.
c) Local depolama için minimum 2 adet SSD veya NVME sürücü kullanılacaktır.
d) En az 2 adet 4 port 1Gb BASE-T ve 2 adet 2 port 10Gb SFP+ Ağ Adaptörlerine sahip olacaktır.
e) En az 2 adet 16Gb Çift Port Fiber Depolama Ağ Adaptörüne sahip olacaktır.
f) Teklif edilecek sunucular “Rack” tipi olacaktır.
g) Sunucuların güç kaynakları yedekli yapıda olacaktır.
h) Teklif edilecek sunucular, üreticinin EOL (End of Life) duyurusu yapılmamış olacaktır.
i) Üretici firma tarafından sağlanacak Garanti Süresi sonuna kadar Firmware Lisansı
j) Üretici firma tarafından sağlanacak Garanti Süresi sonuna kadar yerinde destek

10.3.2 Veri Depolama

Veri depolama amaçlı kullanılacak aşağıdaki özellikleri karşılamalıdır.

a) Veri depolama sistemi birbirini donanımsal hatalara karşı yedekleyen AKM ve ADKM için aktif/aktif çalışan en az iki (2) kontrol ünitesi bulunacaktır. Kontrol ünitesinin birinin arızası durumunda hizmet kesintisi ve veri kaybı yaşanmayacaktır
b) Harici veri depolama sistemi, birden fazla veri depolama sisteminin kümeleme veya benzeri yöntemlerle birleştirilmesinden oluşmuş olmamalıdır.

c) Harici veri depolama sisteminde tek noktadan hata durumuna karşı önlemler alınmış olmalı ve herhangi bir parçanın arızasında yedek birim veri depolama sisteminin durmadan çalışmasını sağlamalıdır.
d) Harici veri depolama sisteminde herhangi bir sorun çıkması durumunda sistem içerisindeki herhangi bir parçanın (disk, güç kaynağı, fanlar, vs.) değiştirilmesi, sistem çalışırken herhangi bir sistem kapanması gerektirmeden yapılabilmelidir.
e) Harici veri depolama sistemi üzerinde en az 2 adet denetleme birimi bulunmalıdır
f) Harici veri depolama ünitesi üzerinde en az 2 (iki) adet birbirini yedekleme ve aktif-aktif çalışma özelliğine sahip denetleme birimi bulunmalıdır. Veri depolama sistemi FC ve iSCSI protokollerini aynı disk denetleme birimi üzerinden ek donanım veya lisans gereksinimi olmadan desteklemelidir. Gateway ya da benzeri çözümler kabul edilmeyecektir.
g) Teklif edilen veri depolama ünitesi Linux, Microsoft Windows işletim sistemleri ve VMware, Hyper-V sanallaştırma çözümleriyle uyumlu olmalıdır."
h) Harici veri depolama sistemi en az RAID 6 veya RAID-DP koruma seviyesini desteklemelidir
i) Harici veri depolama sistemi senkron ve asenkron replikasyon metotlarını desteklemelidir. Bu özellik için gerekli lisanslar teklife dahil edilmelidir.
j) Harici veri depolama sistemi asenkron replikasyonda bir den fazla (one-to-many) noktaya replike yapabilmelidir.
k) Harici veri depolama sistemi inline sıkıştırma ve tekilleştirme özelliğine sahip olmalıdır. Bu özellik için gerekli lisanslar teklife dahil edilmelidir.
l) Harici veri depolama sistemi snapshot (anlık kopya) alabilmeli ve bu kopyalardan geri dönebilmelidir. Anlık kopyalar "Delayed-Copy-on-Write" tekniği kullanılarak alınmamalı, performansa olumsuz etkisi olmaması bakımından "Redirect-on-Write" tekniği kullanılmalıdır. Bu işlemler için gerekli lisanslar teklife dahil edilmelidir.
m) Harici veri depolama sistemi thin provisioning özelliğine sahip olacaktır. Bu özellik için gerekli olan lisanslar teklife dahil edilmelidir.
n) Harici veri depolama sistemiyle birlikte grafik ara yüzlü yönetim yazılımı sağlanacaktır. Yönetim yazılımı ile sistem alarmları, boş alan, kapasite bilgileri, donanım durumları, LUN yapılandırmaları vb. durum bilgileri gözlemlenebilecektir.
o) Harici veri depolama sistemi, üzerinde oluşan bir arıza durumunda sistem yöneticisini e-posta ile uyarma özelliğine sahip olacaktır.
p) Teklif edilecek veri depolama sisteminin EOL (End of Life) duyurusu yapılmamış olacaktır.
q) Üretici firma tarafından sağlanacak Garanti Süresi sonuna kadar Firmware Lisansı verilecektir.
r) Üretici firma tarafından sağlanacak Garanti Süresi sonuna kadar yerinde destek verilecektir.
s) Teklif edilen veri depolama sistemi kabin içi güç ve bağlantı kabloları ile teklif edilecektir.

10.3.3 Zaman Servisi (NTP)

a) SCADA/DMS/OMS Sisteminin zaman senkronizasyonu, GPS saatine (GPS Clock) dayalı NTP sunucular üzerinden gerçekleştirilecektir. Kullanılacak GPS saati aşağıdaki özellikleri sağlaması gerekmektedir. 100 - 240V AC - (standart teslimatta güç kaynağı)
b) 2 adet 10/100/1000 Mbit/s otomatik algılama özelliğine sahip Ethernet arayüzü,
c) Network Time Protocol version 4 (RFC5905),
d) IRIG-B (modüle / modüle edilmemiş)

e) DCF77 (modüle / modüle edilmemiş)
f) Döngüsel Darbeler (PPS, PPM, vb.)
g) Alarmlar
h) SNMPv2c / SNMPv3
i) E-Posta bildirimi
j) SYSLOG
k) IEEE 802.1Q'ya göre VLAN desteği
l) IEEE 802.3ad trunks desteği ile Port aggregation (NIC Bonding/Teaming)
m) IEC 62439-3'e göre Parallel Redundancy Protocol (PRP)
n) IEEE 1588-2008'e göre Precision Time Protocol (PTP)
o) IEEE Std C37.238-2011'e göre IEEE 1588 Precision Time Protocol kullanımı için IEEE Standart Profili (Power Profile)
p) SINEC H1 zaman datagramı

10.3.4 Monitör

a) 54 adet monitör olacaktır. Özellikleri aşağıdaki gibi olacaktır.
   I. Ekran Panel Tipi: 23.8 inç IPS, Micro edge LED arka ışık
   II. Çözünürlük: 1920 x 1080, 60 Hz
   III. En-boy Oranı: 16:9
   IV. Parlaklık: 250 nit
b) Haricen yukarıdaki aynı özelliklere sahip sadece ekran panel boyutu 27 inç olan 5 adet ve 32 inç olan 7 adet ekran temin edilecektir.

10.3.5 Firewall – Tip1

1) Cihaz, mimari açıdan stateful inspection, IP Paket Filtreleme ve Uygulama Tanıma özelliklerini bünyesinde bulundurmalı ve aşağıdaki güvenlik servislerine sahip olmalıdır. Anti-Virus, DNS Security, URL Filtreleme ve Sıfırıncı Gün Koruma tarafında gelişmiş özelliklerin tümünün kullanılabilmesi için gerekli tüm lisanslar teklife eklenmelidir.

- Firewall
- IPSEC VPN, SSL VPN
- Uygulama kontrolü (Application Control)
- Endüstriyel güvenlik ve görünürlük servisi (Operasyonel teknoloji ağları için)
- Atak Engelleme (IPS)
- Anti-Virus
- Anti-Spyware
- URL Filtreleme

- DNS Security
- Kullanıcı kimliği entegrasyon
- SSL Inspection
- Sıfırıncı gün koruma (Anlık hash sorgusu + on-prem/cloud sandbox desteği)

2) Teklif edilecek olan her iki sistem port ve performans anlamında birbiriyle aynı marka model

3) Ürün, yüksek performans ve düşük gecikme ihtiyacı nedeniyle ASIC veya FPGA işlemci mimarisine sahip olmalıdır. Bu sayede özellikle SSL Deep Inspection gibi yüksek performans gereksinimi duyulan durumlarda performans sorunu yaşanmamalıdır.

4) Ürün, aşağıda detayları belirtilen OSI mimarisine uygun çok katmanlı güvenlik modeline sahip olmalıdır.

- Güvenlik politikaları özelinde OSI L4 ve L7 katmanları arasında çalışabilmelidir. Bu sayede istenen trafikler L4 (kaynak ip/kullanıcı, hedef ip, hedef port) istenen trafikler L7 uygulama seviyesinde analiz edilebilmelidir.
- 7. katmanda uygulama seviyesinde analiz edilmesi gerekmeyen trafikler tipleri için (yedekleme trafiği, database senkronizasyonu v.b.) sistemin gereksiz yere performans tüketmesi engellenebilmeli ve sistem verimliliği arttırılabilmelidir.
- Ürün, L4 seviyesinde 1518 byte UDP paketleri ile en az 75 Gbps, 64 byte UDP paketleri ile en az 70 Gbps throughput desteklemelidir.

5) Politika özelinde L7 güvenlik servisleri aktif edilebilmelidir. Bu kapsamda aşağıda listelenen güvenlik servisleri tercihe bağlı olarak seçilebilmelidir.

- Uygulama Kontrolü
- Atak Engelleme (IPS)
- AntiVirus, AntiMalware, AntiSpyware
- URL/Web Filtreleme
- DNS Security
- Dosya Filtreleme
- SSL Inspection

6) Teklif edilen güvenlik duvarının L7 seviyesinde firewall throughput değeri (Uygulama Kontrolü açıkken) 64 KB HTTP paketler ile 28 Gbps performansını desteklemelidir. Üreticinin herkese açık dökümanlarında bu değer açıkça belirtilmemiş ise IPS ve Application Control açıkken throughput değeri en az 10 Gbps olmalıdır.

7) Ürün, en az 9 Gbps tehdit engelleme (Firewall, Uygulama Kontrol, IPS, AntiMalware servisleri aktif) performans (throughput) değerine sahip olmalıdır. Üreticinin resmi web sayfasında ilgili değerin herkese açık bir şekilde yayınlanmış olması gerekmektedir.

8) Önerilen donanımın IPS ve SSL Deep Inspection özellikleri aktifken sağlayabileceği throughput değeri üreticinin resmi web sayfasında herkese açık bir şekilde yayınlanmış olması tercih sebebi olacaktır. Bu değer resmi olarak belirtilmemiş ise proje kapsamında üretici kuruma ilgili değeri beyan etmelidir.

9) Ürün 512 byte paketler ile en az 55 Gbps IPSEC VPN performans değerine sahip olmalıdır.

10) Ürün, aynı anda en az 7.8 milyon oturumu desteklemelidir.

11) Ürün, saniyede en az 500.000 yeni oturum açabilme kapasitesine sahip olmalıdır.

12) Cihaz 960 GB disk alanına sahip olmalıdır.

13) Teklif edilecek çözümün DoS/DDoS ataklarına karşı ASIC veya FPGA tabanlı koruma yeteneği olmalıdır. Bu sayede yüksek seviyeli saldırıların sistemin performansına etkisi minimum olmalıdır.

14) Ürün, aynı anda en az 8 adet 10GE SFP+ fiber, 16 adet 1GE RJ45 bakır ve 8 adet 1GE SFP bağlantı desteğine sahip olmalıdır.

15) Şartnamede istenen performans ve port değerleri tek bir donanım ile karşılanamaması durumunda üretici firma birebir aynı özelliklere sahip donanım veya şase ürününden birden fazla teklif ederek isterleri kümeleme (clustering) ile sağlayabilecektir. Bu durumda cihazların isterlere uygun çalışabilmesi için gerekli cihaz ve yazılımlar da teklife dahil edilecektir. Kümeleme (clustering) yapılacak cihazların hepsi port ve performans anlamında birbiriyle aynı marka model ve kapasitede olmalıdır.

16) Kurum kaynaklarına uzaktan güvenli erişiminin sağlanabilmesi için cihaz üzerinde aşağıda detayları belirtilen SSL-VPN özelliği olmalıdır.

17) Cihaz aynı anda en az 5.000 kullanıcının SSL VPN ile bağlantısına izin verebilecek kapasitede olmalıdır ve gerekli lisanslar teklife eklenmelidir.

18)SSL VPN istemcisi en az aşağıdaki işletim sistemlerini desteklemelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.

- Windows
- Mac OS
- Linux
- IOS
- Android

19) Farklı kullanıcılara farklı ip adresleri atanmasını desteklemelidir.

20) SSL VPN üzerinden erişen kullanıcıların lokal kullanıcı veritabanı, RADIUS, LDAP veya Microsoft AD üzerinden kimlikleri doğrulanabilmelidir.

21) SSL VPN tüneli içerisinden gelen trafiklerde IPS, Uygulama Kontrolü, AntiMalware, URL Filtreleme özellikleri uygulanabilir olmalıdır.

22) SSL-VPN ile bağlantı yapacak adresler belirtilebilmeli, belirtilen adresler dışından SSL-VPN erişimleri engellenebilmelidir.

23) Split tunnelling özelliği ile sadece belirtilen hedef adresler için trafiğin tünele yönlendirilmesi sağlanabilmelidir.

24) DNS servisi için ayrıca split tunneling'i desteklemelidir. Bu sayede sadece spesifik domain sorguları için merkezdeki DNS sunucularının kullanımı sağlanabilmelidir.

25) SSL-VPN ile bağlanacak kullanıcılar için two factor authentication (2FA) özelliği desteklenmelidir.

26) SSL-VPN ile yapılan aktif bağlantılar monitör edilmelidir. Bağlı olan kullanıcı ve ne zaman login olduğu bilgilerine web arayüzü üzerinden erişilebilmelidir.

27) 2FA amacıyla üreticinin kendisine ait soft-token uygulaması tercih sebebidir. Kullanıcıların akıllı telefonlarında push notification desteklenmeli, kullanıcılar SMS sistemlerinde olduğu gibi tek kullanımlık şifreyi şifre ekranına yazmak zorunda kalmadan sadece telefon ekranındaki notification'ı onaylayarak erişim yapabilmelidir.

28) SSL-VPN portal özelliği ile son kullanıcı bilgisayarlarına yazılım (vpn agent) kurmadan portal üzerinden SSL VPN yapılabilmelidir. Portal üzerinden aşağıdaki uygulama ve protokol erişimleri desteklenmelidir.

- HTTP(S)
- FTP
- Telnet
- SMB/CIFS
- VNC
- RDP
- SSH

29)Firewall üzerinde en az 10 adet sanal firewall oluşturulabilecek lisans ile teklif verilecektir.

30)Güvenlik Duvarı sistemi yedekli mimaride iki adet teklif edilecektir.

31)Ürün, aktif-aktif ve aktif-pasif yedeklilik senaryolarını desteklemelidir.

32)Kümeleme yapılan donanımlarda oturumlar donanımın herhangi birisinin arızalanması durumunda oturum kaybı olmadan otomatik olarak diğer güvenlik duvarı cihazı üzerinde devam edebilmelidir.

33) Network arayüzlerinin herbiri LAN, WAN, DMZ veya kullanıcı tanımlı bir segment olarak konfigüre edilebilmelidir. İlgili arayüzler 802.1q protokolünü desteklemelidir. Her bir interface için Alias tanımı girilebilmelidir.

34)Saat, gün bazında erişim kontrolü yapabilmelidir.

35)Yerel ağdaki bir ya da birden fazla adres aralığındaki birçok IP'yi istenirse tek bir adres arkasında, istenirse her bir aralığı başka bir tek adres arkasında saklayabilmeli ya da bire bir adres çevrim özelliği (NAT) olmalıdır.

36) NAT kuralları, Güvenlik kurallarından bağımsız ayrı kural seti olarak tanımlanabilecektir.

37) Tek bir NAT kuralı ile hem internete çıkış hem de internet geliş yönünde bire bir adres çevrimi için Statik NAT özelliği (NAT) olmalıdır.

38) DHCP server ve IPv4/v6 DHCP Relay olarak yapılandırabilecektir.

39)Güvenlik Duvarı 802.3 ad LACP desteklemelidir.

40)Güvenlik Duvarı SNMP v3 desteklemelidir.

41)Güvenlik Duvarının Netflow desteği olmalıdır. Fiziksel port bazında netflow profili tanımlanabilmelidir.

42)Sistem IPv4/v6 Statik ve Dinamik (OSPFv2/v3, BGPv4, RIPv2) Yönlendirme protokollerini desteklemelidir, lisans gerekiyorsa teklife dâhil edilmelidir.

43)Yönetim arayüzü veya CLI üzerinden her bir fiziksel, sanal interface ve interface grubuna ait (LACP) trafik kullanım değerleri gerçek zamanlı ve geçmişe dönük görüntülenebilmelidir. Bu sayede hangi interface üzerinde o an için ne kadar trafik kullanımı olduğu bilgisi (throughput) IN ve OUT yönlü analiz edilebilmelidir.

44)Cihazın MAC adres bazlı güvenlik politikaları oluşturma desteği olmalıdır. Trafiği yaratan cihazlar hardware adresine göre gruplanabilmeli aynı zamanda MAC adres aralığı bazında da bloklama yapılabilmelidir.

45)Sistemin SPI (Stateful Packet Inspection) özelliği olmalıdır.

46)RIP, OSPF, BGP, static ve kaynak tabanlı (policy based) yönlendirme özelliklerine sahip olmalıdır. Multicast routing'i desteklemelidir.

47)Sistem IPv4/v6 Statik ve Dinamik (OSPFv2/v3, BGPv4, RIPv2) Yönlendirme protokollerini desteklemelidir, lisans gerekiyorsa teklife dâhil edilmelidir.

48)Path monitoring vb özelliği cihaz üzerinde tanımlanan statik route tanımları bağdaştırılabilecektir. Böylece tanımlanan statik yönlendirmeler üzerinden sağlanan erişimlerin çalışıp çalışmadığını kontrol edebilecektir. Erişim olmadığı durumlarda statik yönlendirme satırını yönlendirme tablosundan otomatik olarak kaldırarak alternatif yoldan erişim imkânı sağlanacaktır.

49)Cihazın Multicast yönlendirme desteği olmalı ve PIM-SM, PIM-SSM, IGMP v1, v2, v3 desteklemelidir.

50)Site to site ve client to site IPSEC VPN desteği olmalıdır.

51)Cihaz, IPSec VPN standardını desteklemelidir. IKE şifreleme şemalarını desteklemelidir. 3DES, AES algoritmaları ile paket şifreleme yapabilmelidir. Veri bütünlüğü için MD5 ve SHA1 algoritmalarını desteklemelidir. Diffie-Hellman groups 1, 2 ve 5 (Perfect forward secrecy) desteği olmalıdır.

52)Cihaz GRE tunnel destekleyecektir.

53)Cihaz IPv6 IPsec destekleyecektir.

54)DHCP Server ve DHCP Relay özelliği bulunmalıdır.

55)NAT64 ve Jumbo frame desteği olmalıdır.

56)Cihaz üzerindeki portlar Layer3 (routing mod) ve Layer2 (bridge mod) ve Monitoring (TAP mod) katmanlarında çalışabilecektir.

57)Cihazın yeniden başlatılmasına gerek kalmadan üzerindeki portların çalışma seviyesi (L2, L3, monitoring) istendiği gibi değiştirilebilmelidir.

58)Ağ arayüzü veya zone bazlı kural yazılmasını desteklemelidir.

59)Saat, gün, tarih bazında erişim kontrolü yapabilmelidir.

60)MS Active Directory ile entegre olarak kişi ve grup bazında kural yazılabilecektir. Kullanıcıya göre kural yazma sadece kimlik bilgisi gönderen uygulamalarla sınırlı olmayacaktır. Tutulan kayıtlarda kullanıcı ismi de yer alacaktır.

61)Kullanıcı entegrasyonu için yönetici (administrator) hesabına ve Active Directory yapısında herhangi bir değişikliğe ihtiyaç olmayacaktır.

62)Cihaz kendisine kullanıcı doğrulaması yapan sistemlerin gönderdiği syslog veya benzeri mesajları çözerek User-IP mapping işlemini gerçekleştirebilecektir.

63)Cihaz aynı anda farklı yöntemleri kullanarak farklı kaynaklardan IP-Kullanıcı eşleşmesini sağlayabilecektir.

64)Kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS, LDAP ve AD üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.

65)Sistemin aşağıda detayları belirtilen SD-WAN özellikleri olmalıdır.

66)Ürün, birden fazla geniş alan ağı (WAN) bağlantısının (örneğin Metro Ethernet, MPLS, Radyolink, xDSL, LTE v.b.) trafik paylaşımı amacıyla aktif/aktif mimaride kullanımını için sanal interface altında gruplanmasını desteklenmelidir.

67)Birden fazla SDWAN sanal interface grubu tanımlanabilmelidir.

68)Sanal hatları kullanarak güvenlik kuralı (policy) ve rota (route) yazılabilmelidir.

69)SD-WAN hatlarının bağlantı kalitesi aşağıdaki protokoller aracılığıyla gecikme (latency), paket kaybı (packet loss) ve sapma (jitter) yöntemleriyle takip edilebilmelidir.

- http
- ping
- tcp-echo
- udp-echo
- twamp
- dns

70)Hat durum kontrollerine ait geçmişe yönelik bilgiler grafik üzerinden gösterilebilmelidir. Bu sayede ilgili hat üzerinde yakın geçmişe ait paket kayıp seviyesi, gecikme ve sapma değerleri görüntülenebilmelidir.

71)Trafik, SD-WAN hatları arasında aşağıdaki yöntemlere göre dağıtılabilmelidir:

- Kaynak IP'ye göre dağılım
- Kaynak ve hedef IP'ye göre dağılım
- Oturum sayısı (session) bazında oransal dağılım
- Hat bazında eşik değer belirleyerek (Spillover) dağılım
- Trafik oranı bazında (volumetric) oransal dağılım

72) Özelleştirilmiş SD-WAN kuralları tanımlanabilmelidir. Böylece belirli kullanıcı/kullanıcı grubu, kaynak ip, hedef ip ve uygulama/uygulama kategorisi tanımına göre trafiğin;

73)Öncelikli hattan gönderilmesi sağlanabilmelidir. Örneğin kritik uygulamalar MPLS'ten, mail ve internet gibi bulk uygulamaların ADSL'den gitmesi sağlanabilmelidir. Burada belirli SLA değerleri tanımlanabilmelidir. Örneğin kritik uygulamalar MPLS'ten giderken gecikme/paket kaybı/jitter değeri belirli bir threshold'u geçerse trafik otomatik olarak hat kalite değerleri daha iyi olan ADSL hattına yönlenebilmelidir. MPLS hattı düzeldiği zaman trafik otomatik olarak MPLS'e dönebilmelidir.

74)Hat kalite testlerine (latency, packet loss ve jitter) göre daha yüksek kaliteye sahip hattan gönderilmesi sağlanabilmelidir.

75)Sadece belirli bir SLA kriterini (latency, packet loss ve jitter) sağlayan hatlara trafik load-balance edilebilmelidir.

76)Spesifik bir hattan gönderilmesi sağlanabilmelidir.

77)Uygulama/uygulama kategorisi bazında spesifik SD-WAN kuralları tanımlanabilmelidir. Bu sayede örneğin Youtube/Voice/Video/Outlook/Windows Update gibi uygulama trafiklerinin belirli hat üzerinden yönlendirilmesi sağlanabilmelidir.

78) SD-WAN kuralı içinde anlık olarak trafiğin hangi hattan yönlendiği bilgisi işaretli olmalı ve kolayca anlaşılabilmelidir.

79) Paket kayıplarını azaltmak ve bantgenişliğini daha iyi kullanmak için FEC (Forward Error Correction) teknolojisini desteklemelidir.

80)Cihazın asimetrik trafikleri engellemek için route cache özelliği olmalıdır.

81) Cihazın özel durumlarda geri dönüş trafiğinin başka bir hattan yönlendirilmesine izin verilmesi için auxiliary session desteği olmalıdır.

82) Özellikle dinamik routing senaryolarında route tablosunda devamlı değişiklikler olduğu durumda session başladığı andaki route'un session bitimine kadar kullanımının garanti edilebilmesi amacıyla route-preserve özelliği olmalıdır.

83) Sistem IPv6 trafikleri için de SD-WAN özeliğine sahip olmalıdır.

84) SD-WAN bağlantıları üzerinde istenirse otomatik IPSEC VPN tünel oluşturma yeteneğine sahip olmalıdır. SD-WAN konfigürasyonu esnasında hangi hatlar üzerinde VPN tünel yapılacağı seçilebilmeli ve bu sayede birden fazla SD-WAN hatları üzerinden tek bir hedefe otomatik VPN tanımlaması yapılabilmelidir.

85) Kullanıcı/kullanıcı grubu, kaynak ip/ağ, hedef ip/ağ ve uygulama bazlı bantgenişliği yönetim (QoS) desteği olmalıdır. Grup bazlı ya da uç nokta bazlı QoS yapılabilmelidir. QoS interface tabanlı, inbound/outbound yönünde ve zamana bağlı olarak hat kapasitesinin yüzdesel oranında tanımlanabilmelidir. Ses/video gibi kritik uygulamalara öncelik (priority) ve garanti bantgenişliği yazılabilmelidir. Belirlenen trafik için maksimum bantgenişliği tanımlama imkanı olmalıdır.

86) SSL inspection (https trafiğinin açılması) desteği olmalıdır. Bu sayede ssl trafiklerini açarak, uygulama detaylarına göre; SD-WAN, QoS, uygulama kuralları yazılabilmelidir.

87) Sistem üzerinde detayları aşağıda belirtilen uygulama kontrol özelliği bulunmalıdır.

88) Sistemin uygulama kütüphanesinde en az 4000 (dört bin) adet uygulama yer almalıdır.

89) Uygulama kütüphanesinde yer alan tüm uygulamalar aşağıda belirtilen parametrelere göre kategorize edilmiş olmalıdır.

90) Uygulama davranışına göre (botnet, tünelleme amaçlı, bulut uygulaması, bandwith tüketim odaklı v.b.)

- Risk seviyesine göre (Critical, High, Medium, Low v.b.)
- Dünya genelindeki kullanım yoğunluğu, popülerlik seviyesine göre,
- Kullanılan protokole göre (HTTP, DNS, FTP, SIP, H323 gibi)
- Üreticiye göre (Google, Microsoft, Apple gibi)
- Erişim yöntemine göre (Client-server, browser tabanlı, P2P gibi)

91) Uygulama kontrol özelliği active directory ile entegre çalışabilecek bu sayede active directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında uygulama kontrol kuralları tanımlanabilecektir.

92) Veri tabanında yer alan uygulamaların listesi, ilgili uygulamanın yer aldığı ana ve alt kategoriler, ilgili uygulamanın risk seviyesi bilgileri yönetim ekranında görüntülenebilecektir.

93) Kuruma özel uygulamaların sisteme tanıtılması özel imza oluşturmak suretiyle mümkün olmalıdır.

94) Standart portları dışında çalışan uygulamaları otomatik raporlayabilecektir.

95) Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir, sistem yöneticileri tarafında istenirse manuel olarak da güncellenebilir olmalıdır.

96) İstenmeyen uygulamaları kullandığı tespit edilen ip adresleri süreli veya süresiz olarak karantinaya alınabilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

97) Uygulama kontrol veritabanında yer alan tüm uygulamaların listesi, hangi kategoride yer aldıkları ve risk seviyesi bilgisine üreticinin resmi web sitesi üzerinden erişilebilmeli bu bilgiler herkese açık şekilde yayınlanmış olmalıdır.

98) Sistem yöneticileri tarafından özel uygulama imzaları tanımlamaya izin vermelidir.

99) Default portlar üzerinden yapılmayan uygulamaların bloklanması sağlanabilmelidir (örneğin 53 portu dışında başka portlardan yapılan DNS trafiği gibi).

100) Sistem üzerinde detayları aşağıda belirtilen endüstriyel (OT) ağların güvenliği için gerekli yetenekler desteklenmeli ve ilgili lisanslar teklife eklenmelidir.

101) Sistem kütüphanesinde endüstriyel ağ protokolleri (DNP3, IEC104, Bacnet, S7, S7plus gibi) ile ilişkili en az 2200 adet uygulama imzasına sahip olmalıdır.

102) Sistem kütüphanesinde OT sistemlerindeki zaafiyetleri engellemek üzere en az 600 adet OT spesifik IPS imzasına sahip olmalıdır.

103)Sistem OT envanterini purdue modelini referans alarak harita üzerinde işaretlemeye imkanı sunmalıdır.

104) Sistem OT protokolleri komut setleri için gerekli imzaların ait olduğu endüstriyel bir uygulama kontrolü kategorisine sahip olmalıdır.

105) Cihaz üzerinde 'rota arama' (route searching) özelliği olmalıdır. Bu sayede spesifik bir adres için trafiğin hangi rota (route) üzerinden gideceği web arayüzü üzerinden kolaylıkla tespit edilebilmelidir.

106) Sistemin güncel saldırıların engellenmesi amacıyla aşağıda detayları belirtilen atak engelleme (IPS) özelliği olmalıdır.

- IPS sistemi aşağıda belirtilen saldırı tiplerini engelleyebilmelidir.
- Trafik Anomaly
- Protocol Anomaly
- Oran (rate) bazlı saldırılar (brute force gibi)
- Sızma temelli (evasive) saldırılar

107) IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak da yapılabilmelidir.

108) Her bir IPS imzası için aşağıdaki aksiyonlar alınabilmelidir.

- İzin ver (pass)
- İzin ver ve olay kaydı al (monitor)
- Paketi düşür (block)
- Paketi düşür ve session'ı sonlandır (Reset)
- Saldırıyı yapanı karantinaya al

109) Tanımlı saldırı tiplerine göre saldırı yapan ip adresleri süreli veya süresiz olarak karantinaya alınabilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

110) Veri tabanında yer alan imzalar aşağıdaki tanımlara göre filtrelenebilmelidir.

- Kullanılan uygulamaya göre (IIS, Oracle, SQL, Apache gibi)
- İşletim sistemine göre (Windows, Linux, Solaris gibi)
- Protokole göre (HTTP, HTTPS, FTP, DNS gibi)
- CVE koduna göre
- Risk seviyesine göre (Kritik, Yüksek Risk, Orta Risk, Düşük Risk gibi)
- Hedef işletim sistemine göre (client ve/veya server)

111) Rate tabanlı saldırı tanımları içerisinde ne kadar sürede kaç adet istekte bulunulabileceği tanımlanabilmelidir. Örneğin OWA'ya 5 sn içerisinde 3'ten fazla login isteğinde bulunulmasın gibi.

112) IPS sistemi aşağıda belirtilen detaylı sızma tekniklerine karşı koruma sağlayabilmelidir.

- IP Packet Fragmentation,
- TCP Stream Fragmentation
- TCP Stream Segmentation,
- RPC Fragmentation,
- URL & HTML Obfuscation,

113) IPS sistemi Botnet aktivitelerini tespit edebilmeli ve engelleyebilmelidir.

114) IPS imzası özelinde kaynak ve hedef adres bilgisine dayalı istisna adresler (exception) tanımlanabilmelidir.

115) IPS sistemi zararlı URL adreslerine yapılan erişim isteklerini engelleyebilmelidir.

116) Sistem IPS loglarında saldırının yönünü gösterebilmelidir (client to server veya server to client)

118) Farklı kullanıcı veya kullanıcı grupları için farklı IPS politikaları oluşturulabilmelidir.

119) Cihaz üzerindeki IPS imzaları CVE id lerine, kritiklik seviyelerine ve host (client/server) tipine göre aranabilecektir.

120) IPS sisteminin saldırıları karşılama biçimi, sistem yöneticisi tarafından her bir imza için ayrı ayrı ayarlanabilmelidir.

121) IPS özelliğinde saldırılara karşı kullanılan filtreler, güncelleme dosyasından ya da internet üzerinden güncellenebilmelidir. Ayrıca eğer istenirse, imza güncellemeleri kullanıcı müdahalesi olmadan otomatik olarak da yapılabilmelidir.

122) Sistem spoof saldırılarını tespit edebilmelidir.

123) Sistem üzerinde detayları aşağıda iletilen URL Filtreleme özelliği bulunmalıdır.

124) Karaliste ve beyazliste özelliği olmalıdır. Bu sayede direk url adresi, regex ve wildcard formatında tanımlı adreslere erişime izin verebilmeli veya engelleme yapabilmelidir.

125) Site içeriği taraması yapabilmelidir. Regex veya wildcard formatında belirtilen metni içeren sitelere erişim engellenebilmeli ya da izin verebilmelidir.

126) USOM gibi harici karaliste kaynakları engellenebilmeli ve otomatik olarak güncellenebilmelidir.

127) Sadece URI bazında değil, erişilen ip bazında da kontrol yapabilmelidir.

128) URL bloklama ekranı özelleştirilebilmelidir.

129) Farklı kullanıcı ve kullanıcı gruplarına farklı URL filtreleme profilleri uygulanabilmelidir.

130) Riskli kategorideki web sayfalarında kullanıcının AD kullanıcı ve şifresi ile giriş yapması engellenebilmelidir. Bu sayede özellikle kimlik bilgilerini ele geçirme amaçlı phishing saldırıları engellenebilmelidir.

131) URL filtreleme özelliği Active Directory ile entegre çalışabilecek bu sayede Active Directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında URL filtreleme kuralları tanımlanabilecektir.

132) URL bloklama ve uyarı portalı değiştirilebilecektir.

133) Güncel zararlı yazılımların eriştiği C&C (Command and Control) ve Malware Download URL listelerini dinamik olarak güncelleyebilmelidir.

134) URL filtreleme özelliğinde XFF (X-forwarded-for) özelliği bulunmalıdır.

135) Gerçek zamanlı analiz yaparak kimlik hırsızlığına karşı phishing sitelerini ve Java script tabanlı atakları engelleyebilecektir.

136) Cihazın detayları aşağıda belirtilen sanal güvenlik duvarı özelliği olmalıdır:

- Cihaz üzerinden birbirinden izole sanal güvenlik duvarları oluşturulabilmelidir.
- Cihaz üzerindeki arayüzler veya sanal arayüzler (vlan) sanal güvenlik duvarları arasında paylaştırılabilmelidir.

137) Her bir sanal güvenlik duvarı için dedike bir sistem yöneticisi atanabilmeli, sistem yöneticilerinin yetkileri olmayan sanal güvenlik duvarlarına erişimleri engellenebilmelidir.

138) Sanal güvenlik duvarı oluşturulması işlemi web arayüzünden kolayca yapılabilmeli 139) Her bir sanal güvenlik duvarı üzerinde açılabilecek maksimum oturum (session) sayısı limitlenebilmelidir.

140) Cihazın detayları aşağıda belirtilen servis dışı bırakma saldırılarını (DoS) engelleme özelliği olmalıdır.

141) DoS politikaları ile internetten erişilebilir sistemlere (web server, dns server gbi) yönelik trafikler için eşik değer (threshold) bazlı sınırlandırma yapılabilmelidir.

142) L3 seviyesinde kaynak ve hedef ip bazında açılabilecek toplam oturum sayısı (session) limitlenebilmelidir.

143) L4 seviyesinde kaynak ve hedef ip bazında açılabilecek oturum sayısı limitlenebilmelidir.

144) Sistem portscan ve udpscan saldırılarını tespit edip engelleyebilmelidir.

145) TCP synflood ve UDP flood saldırılarına karşı aynı kaynaktan aynı anda gelebilecek syn istek sayısı limitlenebilmelidir.

146) Sistem IPv6 adresleri için de yukarıda belirtilen anti-DoS özelliklerini desteklemelidir.

147) Belirtilen tüm DoS politika konfigürasyonları cihazın web arayüzünden yapılabilmelidir.

148) Cihazın detayları aşağıda listelenen "SSL Deep Inspection" özelliği olmalıdır.

149) Cihazın SSL Inspection özelliği sadece secure HTTP (HTTPS) trafiği için desteklenmemeli, aşağıdaki protokoller için de araya girerek tarama yapabilmelidir.

- SMTPS
- POP3S
- IMAPS
- FTPS

150) SSL tabanlı botnet iletişiminin engellenmesi amacıyla sertifika karaliste özelliği olmalıdır.

151) İstenen web adresleri, kategorileri ve domain'ler için SSL Inspection istisnası uygulanabilmelidir. Wildcard FQDN istisna objeleri desteklenmelidir.

152) SSL anomaly'lerini ve yazılan istisnai SSL erişimlerini loglayabilmelidir.

153) Bağlantıyı daha güçlü SSL-cipher algoritmaları kullanımına zorlama özelliği olmalıdır.

154) Bağlantıyı TLS 1.2 ve 1.3 protokollerine zorlama özelliği olmalıdır.

155) Güvenilir olmayan CA'ler tarafından imzalanmış sertifika kullanan sitelere erişimler engellenebilmelidir.

156) Süresi geçmiş (expired) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.

157) Doğrulama süresi geçmiş (validation timeout) ya da doğrulanamayan (validation failed) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.

158) Client hello mesajı içerisinde SNI kontrolü yapabilmelidir.

159) Ön tanımlı gelen ve devamlı güncellenen bilindik güvenilir site veritabanı olmalı, ilgili siteler için SSL Deep Inspection istisnası tanımlanabilmelidir.

160) Cihazın SSL Offloading özelliği olmalıdır. Internetten gelen HTTPS trafiğini decrypt ettikten sonra arka taraftaki web server'lara HTTP olarak dağıtabilmelidir.

161) Sistemin grafik arayüzü veya CLI aracılığıyla aşağıda belirtilen detaylı trafik analiz işlemleri yapılabilecektir. Grafik arayüzünde gerçek zamanlı olarak bu bilgilerin alınabilmelidir.

- Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafik yaratan ve en fazla bağlantı (session) isteğinde bulunan kullanıcıların listesi,
- Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafik yapılan ve en fazla bağlantı (session) isteğinde bulunulan hedef sunucuların listesi,
- Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafik yaratan ve en fazla bağlantı (session) açılan uygulamaların listesi,
- Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafiğin yapıldığı network arayüzleri (interface'ler),
- Geçmiş döneme ait tehditlerin risk puanlarına ve bağlantı (oturum) sayılarına göre listesi,

162) Yukarıda belirtilen trafik bilgilerinin detay analizi yapılabilmelidir. Örneğin son 24 saatte en fazla oturum açan (session) kullanıcı tespit edildikten sonra bu oturumların detaylarına (hangi uygulamaları kullanarak hangi hedef sunuculara ve web adreslerine doğru bu bağlantıların açıldığı bilgisine) ulaşılabilmelidir.

163) Cihazın yönetim arayüzü üzerinden sistemle ilgili aşağıdaki detay bilgilere ulaşılabilmelidir.

- Seri no, Firmware versiyonu ve Uptime bilgisi,
- Saniyede oluşan log miktarı (eps),
- Saniyede oluşan bağlantı isteği sayısı (connection per second),
- Mevcut oturum (session) sayısı,
- CPU, Memory ve Disk kullanım değeri (yüzdesel),
- Lisans durumu,
- WAN interface'inin ip adresi ve karalisteye alınmış ise bilgisi,
- Sisteme bağlı olan admin'lerin bilgisi,

164) Teklif edilen sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama, Ping6, IPv6 captive portal, IPv6 FQDN adresleri desteklenmelidir.

165) SNMPv3'ü desteklemelidir.

166) İşletim sistemi ve yazılım güncellemelerini web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.

167) Sistemin detayları aşağıda belirtilen AntiMalware özelliği olacaktır;

168) Sistem aşağıda belirtilen protokoller aracılığıyla yapılan malware trafiklerini tespit edip engelleyebilmelidir.

- HTTP(S)
- POP3(S)

- IMAP(S)
- FTP
- CIFS/SMB

169) Farklı kullanıcı veya kullanıcı grupları için farklı anti-virüs politikaları oluşturulabilmelidir.

170) Bilinen virüsler için imza temelli bloklama yapabilmelidir.

171) Anti-virüs imzaları payload tabanlı olmalıdır, hash tabanlı olmamalıdır.

172) Akan dosya trafiğini tarayabilmelidir.

173) Sistem, yukarıda belirtilen protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir.

174) AntiMalware sistemi internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmeli, gerekmesi durumunda antivirüs veritabanı manuel olarak güncellenebilmelidir.

175) AntiMalware sistemi, akıllı telefonlara yönelik mobil malware'leri tespit edebilme ve engelleme yeteneğine sahip olmalıdır.

176) Arşiv dosyalarının detay analizini yapabilmeli ve bozuk (corrupted), şifreli (encrypted), içiçe geçirilmiş (nested) arşiv dosyaları engellenebilmelidir.

177) Malware içerdiği tespit edilen kaynak adresler otomatik olarak karantinaya alınabilmelidir.

178) Sistem, henüz lokal veritabanında yer almayan virüslere karşı anlık, gerçek zamanlı istihbarat servis sorgulaması (real-time query) yapabilmelidir. Bunu yaparken dosyanın kendisi paylaşımlı bulut servisine gönderilmemelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.

179) AntiMalware sistemi dış kaynaklardan alınan malware hash (feed) bilgilerine göre kontrol ve engelleme özelliği olmalıdır. Sistem dış kaynaklardan aldığı hash verisini otomatik olarak güncelleyebilmeli, sistem yöneticilerinin manuel işlem yapmasına ihtiyaç olmamalıdır. Sistem sadece lokal virüs veritabanına bağlı kontrol yapmamalı, lokal veritabanında yer almayan hash'leri siber istihbarat servisi üzerinden gerçek zamanlı olarak sorgulayabilmelidir.

180) Sistem, henüz lokal veritabanında yer almayan virüslere karşı anlık, gerçek zamanlı istihbarat servis sorgulaması (real-time query) yapabilmelidir. Bunu yaparken dosyanın kendisi paylaşımlı bulut servisine gönderilmemelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.

181) Çok yeni tespit edilen ancak cihaz üzerindeki lokal AntiVirus veritabanında henüz yer almayan virüslere karşı gerçek zamanlı koruma sağlayabilmelidir

182) Üreticinin Sandbox sensörleri ve Sandbox teknolojisini kullanan diğer kurumların Sandbox ürünleri tarafından tespit edilmiş zararlı veritabanından eş zamanlı faydalanması mümkün olmalıdır. Bu özelliğin kullanımı için dosyanın kendisinin buluta gönderimi gerekmemelidir.

183) Üretici Cyber Threat Alliance (CTA) üyesi olmalıdır. CTA'nın üyesi olan diğer üreticilere ait malware veritabanından eş zamanlı faydalanabilmeli, kendi AV veritabanında olmayan ama CTA üyesi başka bir üreticiye ait malware veritabanında yer alan hash bilgisi aracılığıyla zararlının anında engellenmesi mümkün olabilmelidir.

184) Zero-Day Ataklarına karşı NGFW çözümünün on-Prem Sandbox entegrasyon desteği olmalıdır. Dosyanın kendisi cloud'a gönderilmemelidir.

185) Sistem üzerinde detayları aşağıda belirtilen DNS Security özelliği bulunmalıdır.

186) Lokal veya internet DNS sunucularına doğru yapılan DNS sorguları kontrol edilerek istenmeyen domain'ler için yapılan sorgulara sistem yöneticileri tarafından belirlenen ip adresinin döndürülmesi veya istenen DNS trafiğinin bloklanması sağlanabilmelidir.

187) Karaliste ve beyazliste özelliği olmalıdır. Bu sayede direk domain adresi, regex ve wildcard formatında tanımlı adreslere DNS sorgusu yapılmasına izin verebilmeli ya da bloklama yapabilmelidir.

188) URL veritabanı aynı zamanda DNS isteklerinin kontrolü amacıyla domain kategori veritabanı olarak kullanılabilmelidir.

189) USOM gibi harici karaliste kaynakları spesifik DNS kategorisi olarak eklenebilmeli ve otomatik olarak güncellenebilmelidir. Bu listede yer alan domain adreslerine yapılan DNS sorgularında sistem yöneticileri tarafından belirlenen ip adresinin döndürülmesi sağlanabilmelidir.

190) DNS sorguları sonrası DNS server'ın bildirdiği ip adresi bazında da harici karaliste sorgulaması yapabilmelidir. Böylece sadece domain sorgu aşamasında değil, sorgu sonucu gelen cevaba göre analiz yapabilmelidir.

191) Kurumun internetten sorgulara açık olan DNS sunucularına doğru sadece kurum domain'i için yapılan DNS sorgulamalarına izin verilmesi, diğer tüm alan adları için yapılan DNS isteklerinin bloklanabilmelidir.

192) Sistemin DNS translation özelliği olmalıdır.

193) Sistem üzerindeki DNS Security özelliği ile Lokal veya internet DNS sunucularına doğru yapılan DNS sorguları kontrol edilerek DGA, Phishing, Botnet, C2C, Malware, Newly Registered, Newly Observed gibi istenmeyen domain'ler için yapılan DNS sorguları, tehdit istihbarat servisindeki Yapay Zeka, Makine Öğrenmesi algoritmaları veya imza veritabanı da kullanılarak engellenebilmelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.

194) Cihazın farklı ürünlerle entegrasyonu amacıyla aşağıdaki protokolleri desteklemesi tercih sebebidir.

- WCCP client
- ICAP client
- RADIUS client

195) Cihazın detayları aşağıda belirtilen bant genişliği yönetim özelliği olmalıdır.

196) Kaynak ip/ağ, kullanıcı/kullanıcı grubu, hedef ip/ağ ve servis bazında bant genişliği politikası yazılabilmelidir.

197) Spesifik uygulama (örneğin Youtube) ve uygulama kategorisi (öneğin Update) bazında bant genişliği politikası yazılabilmelidir.

198) Zaman aralığı bazında bant genişliği politikası yazılabilmelidir (örneğin mesai saatleri içerisinde gibi.).

199) Aynı session içerisinde trafiğin yönüne göre (IN ve OUT yönünde) bant genişliği politikası yazılabilmelidir.

200) Sistemdeki tüm kullanıcılar için tanımlı bant genişliği kuralı içerisinde ip başına limitasyon yapılabilmelidir. (örneğin tüm kullanıcıları 10 mbps ile limitle gibi..)

201) Firewall kuralları bazında bant genişliği politikası yazılabilmelidir. Böylece ilgili kuralla eşleşen trafiklerin limitlenmesi sağlanabilmelidir.

202) Cihazın proaktif mimaride otomatik aksiyon alabilme özelliği olmalıdır. Bu özellik sayesinde aşağıdaki olaylardan birisi gerçekleştiğinde otomatik olarak eposta gönderimi veya herhangi bir web servisini tetikleme aksiyonlarını otomatik olarak alabilmelidir. Bu özellik için gereken lisanslar ve/veya ürünler teklife eklenmelidir.

- Konfigürasyon değişikliği yapıldığında,
- Cihaz kapanıp açıldığında,
- Lisans süresi bittiğinde,
- Yedekli (cluster) cihazlar arasında geçiş yaşandığında,
- AV veya IPS database'i güncellendiğinde,
- Sistemde önceden tanımlı herhangi bir olay gerçekleştiğinde (örneğin güncelleme işlemi başarısız olduğunda, AD entegrasyonunda sorun olduğunda, IPSec bağlantısı koptuğunda v.b.)

203) Cihazın aşağıda belirtilen SDN (private cloud) ve bulut (public cloud) temelli çözümlerle API entegrasyonu olması tercih sebebidir.

- Cisco ACI
- Amazon Web Service
- Microsoft Azure
- VMware NSX-T
- VMware ESXi
- Google Cloud Platform (GCP)

204) Cihaz üzerinde detayları aşağıda belirtilen servis veritabanı özelliği olmalıdır.

205) İlgili internet servis veritabanı çok bilinen sistem, ağ ve güvenlik üreticilerinin hizmet amaçlı kullandıkları Web, DNS, FTP v.b. sunucularının ip, port, protokol ve coğrafya bilgilerini içermelidir.

206) Bu veri tabanında yer alan üreticilerin hizmetlerine erişimler için veritabanında yer alan objeler kolayca politikalar içerisinde kaynak veya hedef olarak seçilebilmelidir. Örneğin Microsoft sunucularına veya güncelleme için X antivirüs üreticisine doğru erişim kuralı kolayca tanımlanabilmelidir.

207) Internet servis veri tabanı sistem tarafından otomatik olarak güncellenmelidir.

208) Birden fazla internet hattının olması durumunda internet servis veritabanı kullanılarak spesifik üretici ve uygulama trafiklerinin belirtilen internet hattı üzerinden yönlendirilmesi sağlanabilmelidir. Örneğin Amazon, Dropbox, Facebook sunucularına giden trafiği A hattından, diğer trafikleri B hattından yönlendir gibi.

209) Internet servis veritabanı sistem yöneticileri tarafından gerekirse özelleştirilebilmelidir.

210) Internet servis veritabanında yer alan hizmetlerin hangi ülke ve hangi şehirden yapıldığı bilgisine ulaşılabilmelidir. Örneğin Microsoft update sunucularının ip, port, protokol bilgileri ile Türkiye'den hangi lokasyonlardan hizmet verildiği bilgisi görüntülenebilmelidir.

211) Önerilecek güvenlik duvarı üreticisi, güncel "Gartner Magic Quadrant Enterprise Network Firewalls" raporunda "Leaders" kategorisinde yer almalıdır.

212) Teklif edilecek tüm ürünler üreticinin global destek merkezi tarafından 7x24 destek hizmeti dahil şekilde tekliflendirilecektir. Kurum, üreticinin global destek merkezine 7x24 case açabilecektir.

213) Güvenlik Duvarı sisteminin 5 yıl süre ile yazılım/işletim sistemi güncellemelerini ve 5 yıl süre için Güvenlik Duvarı (Firewall), IPSec VPN, SSL VPN, Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Kontrol (Application Control), Virüs/Zararlı İçerik Kontrolü (AV), URL (Web) Filtreleme, DNS Güvenlik Sistemi, SSL-TLS Tarama (Inspection), Bulutta Sıfırıncı Gün Tarama (Cloud Sandbox) lisanslarının default + gelişmiş özelliklerin tümünün kullanımı için gereken bütün lisanslar teklife eklenmelidir.

214) Teklif edilecek donanım ve lisanslar Demo, Lab, Spare tipinde olmamalıdır.

215) Cihaz üzerindeki tüm güç kaynağı yuvaları tamamen dolu olarak teklif edilecektir.

216) Güvenlik duvarı yönetimi windows, macos, linux işletim sistemleri ile erişilebilmelidir.

217) Cihazlar kendi üzerindeki Web tabanlı ara yüzü üzerinden yönetilebilecektir. Web tabanlı yönetim arayüzünden firewall güvenlik politikaları, url filtering, application control, ips, antivirüs, dns güvenliği gibi yapılandırmalar gerçekleştirilebilmelidir.

218) Teklif edilecek merkezi yönetim sisteminin arızalanması durumunda güvenlik duvarı cihazlarının web arayüzünden tüm fonksiyonların yönetimi mümkün olmalıdır.

10.3.6 Firewall – Tip2

1)Teklif edilecek ürün aşağıda belirtilen özellikleri desteklemelidir.

- Güvenlik Duvarı (Firewall)
- IPSec VPN Sonlandırma Sistemi
- SSL VPN Sonlandırma Sistemi
- Saldırı Tespit ve Engelleme Sistemi (IPS)
- Uygulama Kontrol (Application Control) Sistemi
- Endüstriyel altyapılar için güvenlik servisi (Industrial security service)
- HTTPS Tarama (Inspection)
- SDWAN (Çoklu WAN Hatlarının A/A Kullanımı)

2)Ürün, yüksek performans ve düşük gecikme ihtiyacı nedeniyle ASIC işlemci mimarisine sahip olmalıdır. Bu sayede özellikle SSL Deep Inspection gibi yüksek performans gereksinimi duyulan durumlarda performans sorunu yaşanmamalıdır.

3)Ürün, aşağıda detayları belirtilen OSI mimarisine uygun çok katmanlı güvenlik modeline sahip olmalıdır.

4)Güvenlik politikaları özelinde OSI L4 ve L7 katmanları arasında çalışabilmelidir. Bu sayede istenen trafikler L4 (kaynak ip/kullanıcı, hedef ip, hedef port) istenen trafikler L7 uygulama seviyesinde analiz edilebilmelidir.

5)Yedinci katmanda uygulama seviyesinde analiz edilmesi gerekmeyen trafikler tipleri için (yedekleme trafiği, database senkronizasyonu v.b.) sistemin gereksiz yere performans tüketmesi engellenebilmeli ve sistem verimliliği arttırılabilmelidir.

6)Politika özelinde L7 güvenlik servisleri aktif edilebilmelidir. Bu kapsamda aşağıda listelenen güvenlik servisleri tercihe bağlı olarak seçilebilmelidir.

- Uygulama Kontrolü
- Atak Engelleme (IPS)
- Dosya Filtreleme
- SSL Inspection (Tarama)

7)Ürün en az 5.95 (beş nokta doksanbeş) gbps L4 güvenlik duvarı performans (throughput) değerine sahip olmalıdır. Üreticinin resmi web sayfasında ilgili değerin herkese açık bir şekilde yayınlanmış olması gerekmektedir.

8)Ürün, en az 1.3 (bir nokta üç) gbps L7 güvenlik duvarı (uygulama kontrol) performans (throughput) değerine sahip olmalıdır. Üreticinin resmi web sayfasında ilgili değerin herkese açık bir şekilde yayınlanmış olması gerekmektedir.

9)Ürün, en az 500 (beşyüz) mbps tehdit engelleme (Firewall, Uygulama Kontrol, IPS, AntiMalware servisleri aktif) performans (throughput) değerine sahip olmalıdır. Üreticinin resmi web sayfasında ilgili değerin herkese açık bir şekilde yayınlanmış olması gerekmektedir.

10)Ürün, HTTPS uygulamalarına erişimler için IPS + HTTPS Inspection servisi açıldığında 460 (dörtyüzaltmış) mbps performans (throughput) değerine sahip olmalıdır.

11)Ürünün trafikte yaratacağı gecikme en fazla 3.10 mikrosaniye olmalıdır. Üreticinin resmi web sayfasında ilgili değerin herkese açık bir şekilde yayınlanmış olması gerekmektedir.

12)Ürün en az 3.5 (üç nokta beş) gpbs IPSEC VPN performans değerine sahip olmalıdır.

13) Ürün, aynı anda en az 600,000 (altıyüzbin) oturumu desteklemelidir.

14)Ürün, saniyede en az 19,000 (ondokuzbin) yeni oturum açabilme kapasitesine sahip olmalıdır.

15)Ürün, aynı anda en az 4 adet GE bakır, 1 çift bypass yetenekli GE bakır ve

16) 2 adet SFP bağlantı desteğine sahip olmalıdır.

17)Teşekkül kaynaklarına uzaktan güvenli erişiminin sağlanabilmesi için cihaz üzerinde aşağıda detayları belirtilen SSL-VPN özelliği olmalıdır.

18)Cihaz aynı anda en az 100 (yüz) kullanıcının SSL VPN ile bağlantısına izin verebilecek kapasitede olmalıdır.

19)SSL VPN istemcisi en az aşağıdaki işletim sistemlerini desteklemelidir.

- Windows
- Mac OS
- Linux
- IOS
- Android

20)Farklı kullanıcılara farklı ip adresleri atanmasını desteklemelidir.

21)SSL VPN üzerinden erişen kullanıcıların lokal kullanıcı veritabanı, RADIUS, LDAP veya Microsoft AD üzerinden kimlikleri doğrulanabilmelidir.

22) SSL VPN tüneli içerisinden gelen trafiklerde IPS, Uygulama Kontrolü özellikleri uygulanabilir olmalıdır.

23)SSL-VPN ile bağlantı yapacak adresler belirtilebilmeli, belirtilen adresler dışından SSL-VPN erişimleri engellenebilmelidir.

24)Split tunelling özelliği ile sadece belirtilen hedef adresler için trafiğin tünele yönlendirilmesi sağlanabilmelidir.

25)DNS servisi için ayrıca split tunneling'i desteklemelidir. Bu sayede sadece spesifik domain sorguları için merkezdeki DNS sunucularının kullanımı sağlanabilmelidir.

26)SSL-VPN ile bağlanacak kullanıcılar için two factor authentication (2FA) özelliği desteklenmelidir.

27)2FA amacıyla üreticinin kendisine ait soft-token uygulaması olmalıdır. Böylece kullanıcıların akıllı telefonlarında push notification desteklenmeli, kullanıcılar SMS sistemlerinde olduğu gibi tek kullanımlık şifreyi şifre ekranına yazmak zorunda kalmadan sadece telefon ekranındaki notification'ı onaylayarak erişim yapabilmelidir.

28)SSL-VPN ile yapılan aktif bağlantılar monitör edilmelidir. Bağlı olan kullanıcı ve ne zaman login olduğu bilgilerine web arayüzü üzerinden erişilebilmelidir.

29)SSL-VPN portal özelliği ile son kullanıcı bilgisayarlarına yazılım (vpn agent) kurmadan portal üzerinden SSL VPN yapılabilmelidir. Portal üzerinden aşağıdaki uygulama ve protokol erişimleri desteklenmelidir.

- HTTP(S)
- FTP
- Telnet
- SMB/CIFS
- VNC
- RDP
- SSH

30)Cihaz üzerinde aynı anda 10 (on) adet sanal güvenlik duvarı oluşturulabilmelidir.

31)Ürün, aşağıda belirtilen yedeklilik ve yük paylaşım senaryolarını desteklemelidir.

- Dört adet cihaza kadar aktif-aktif yedekli mimari (A/A cluster)
- Dört adet cihaza kadar aktif-pasif yedekli mimari (A/P cluster)
- Dört adet cihaza kadar sanal firewall özelinde aktif-aktif yedekli mimari (A/A virtual cluster)

16 adet cihaza kadar detayları aşağıda iletilen yük paylaşım mimarisi;

32)Load balancer, router, switch v.b. cihazlar aracılığıyla aynı topolojiye sahip çoklu güvenlik duvarları arasında oturum (session) dağıtımı yapılabilmelidir. Bu model sayesinde Teşekkül alt yapısının büyümesi paralelinde üçüncü, dördüncü, beşinci vb. güvenlik duvarının sisteme eklenmesi durumunda güvenlik duvarı ürünleri arasında load balancer cihazı ile trafik

eşit oranda paylaştırılabilmeli, ilgili cihazlar kendi aralarında oturum (session) senkronizasyonu yapabilmelidir.

33)Bu model A/A ya da A/P yedekli (cluster) mimaride çalışan güvenlik duvarı cihazları arasında da desteklenmelidir.

34) Bu model asimetrik trafiği desteklemelidir (X cihazından geçen syn isteğine ait syn-ack paketinin Y cihazından geri gelmesi gibi)

35) Farklı lokasyonlar arası coğrafi yük paylaşımı senaryoları desteklenmelidir.

36)Yukarıda belirtilen tüm senaryolarda hangi protokole ait trafiklerin cihazlar arasında sync edileceği sistem yöneticileri tarafından belirlenebilmelidir (sadece TCP, UDP, ICMP, connectionless, NAT session'ları gibi)

37) Ağ arayüzlerinin herbiri LAN, WAN, DMZ veya kullanıcı tanımlı bir segment olarak konfigüre edilebilmelidir. İlgili arayüzler 802.1q protokolünü desteklemelidir. Her bir interface için Alias tanımı girilebilmelidir.

38)Cihaz üzerinde soft-switch desteği olmalıdır. İstenen interface'ler switch grubu oluşturularak aynı L2 grubunda toplanabilmelidir.

39) L2 interface grubunda (soft-switch) yer alan herhangi bir interface'in trafiği aynı gruptaki başka bir interface'e mirror'lanabilmelidir.

40)Yönetim arayüzü üzerinden her bir fiziksel, sanal interface ve interface grubuna ait (LACP) trafik kullanım değerleri gerçek zamanlı ve geçmişe dönük görüntülenebilmelidir. Bu sayede hangi interface üzerinde o an için ne kadar trafik kullanımı olduğu bilgisi (throughput) IN ve OUT yönlü analiz edilebilmelidir.

41) Cihazın MAC adres bazlı güvenlik politikaları oluşturma desteği olmalıdır. Trafiği yaratan cihazlar hardware adresine göre gruplanabilmeli aynı zamanda MAC adres aralığı bazında da bloklama yapılabilmelidir.

42)Sistemin SPI (Stateful Packet Inspection) özelliği olmalıdır.

43) RIP, OSPF, BGP, static ve kaynak tabanlı (policy based) yönlendirme özelliklerine sahip olmalıdır. Multicast routing'i desteklemelidir.

44)DHCP Server ve DHCP Relay özelliği bulunmalıdır.

45)NAT64 ve Jumbo frame desteği olmalıdır.

46)Ağ arayüzü veya zone bazlı kural yazılmasını desteklemelidir.

47) Saat, gün, tarih bazında erişim kontrolü yapabilmelidir.

48)MS Active Directory ile entegre olarak kişi ve grup bazında kural yazılmasına olanak tanımalı, tutulan kayıtlarda kullanıcı ismi yer alabilmelidir. Bu sayede trafiği yaratan kaynağın isim ile takibinin yapılabilmesine olanak sağlamalıdır.

49)Kullanıcıları ve kullanıcı gruplarını otomatik olarak Active Directory'den okuyabilmelidir.

50) Kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS, LDAP ve AD üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.

51) Sistem yöneticilerinin otomatik üretilen tek seferlik şifre (OTP) ile cihaza bağlantı yapmasını desteklemelidir. Bu özellik en az iki sistem yöneticisi için desteklenmeli, sistem yöneticilerinin akıllı telefonlarına yüklenen uygulama ile tek seferlik şifre üretimi sağlanabilmelidir.

52)Sistemin aşağıda detayları belirtilen SD-WAN özellikleri olmalıdır.

53) Ürün, birden fazla geniş alan ağı (WAN) bağlantısının (örneğin Metro Ethernet, MPLS, Radyolink, xDSL, LTE v.b.) trafik paylaşımı amacıyla aktif/aktif mimaride kullanımını için sanal interface altında gruplanmasını desteklenmelidir.

54)Birden fazla SDWAN sanal interface grubu tanımlanabilmelidir.

55)Sanal hatları kullanarak güvenlik kuralı (policy) ve rota (route) yazılabilmelidir.

56) SD-WAN hatlarının bağlantı kalitesi aşağıdaki protokoller aracılığıyla gecikme (latency), paket kaybı (packet loss) ve sapma (jitter) yöntemleriyle takip edilebilmelidir.

- http
- ping
- tcp-echo
- udp-echo
- twamp
- dns

57) Hat durum kontrollerine ait geçmişe yönelik bilgiler grafik üzerinden gösterilebilmelidir. Bu sayede ilgili hat üzerinde yakın geçmişe ait paket kayıp seviyesi, gecikme ve sapma değerleri görüntülenebilmelidir.

58)Trafik, SD-WAN hatları arasında aşağıdaki yöntemlere göre dağıtılabilmelidir:

59)Kaynak IP'ye göre dağılım

60)Kaynak ve hedef IP'ye göre dağılım

61)Oturum sayısı (session) bazında oransal dağılım

62)Hat bazında eşik değer belirleyerek (Spillover) dağılım

63)Trafik oranı bazında (volumetric) oransal dağılım

64)Özelleştirilmiş SD-WAN kuralları tanımlanabilmelidir. Böylece belirli kullanıcı/kullanıcı grubu, kaynak ip, hedef ip ve uygulama/uygulama kategorisi tanımına göre trafiğin;

65)Öncelikli hattan gönderilmesi sağlanabilmelidir. Örneğin kritik uygulamalar MPLS'ten, mail ve internet gibi bulk uygulamaların ADSL'den gitmesi sağlanabilmelidir. Burada belirli SLA değerleri tanımlanabilmelidir. Örneğin kritik uygulamalar MPLS'ten giderken gecikme/paket kaybı/jitter değeri belirli bir threshold'u geçerse trafik otomatik olarak hat kalite değerleri daha iyi olan ADSL hattına yönlenebilmelidir. MPLS hattı düzeldiği zaman trafik otomatik olarak MPLS'e dönebilmelidir.

66) Hat kalite testlerine (latency, packet loss ve jitter) göre daha yüksek kaliteye sahip hattan gönderilmesi sağlanabilmelidir.

67)Sadece belirli bir SLA kriterini (latency, packet loss ve jitter) sağlayan hatlara trafik load-balance edilebilmelidir.

68)Spesifik bir hattan gönderilmesi sağlanabilmelidir.

69)Uygulama/uygulama kategorisi bazında spesifik SD-WAN kuralları tanımlanabilmelidir. Bu sayede örneğin Voice/Video/Outlook/Windows Update gibi uygulama trafiklerinin belirli hat üzerinden yönlendirilmesi sağlanabilmelidir.

70)SD-WAN kuralı içinde anlık olarak trafiğin hangi hattan yönlendiği bilgisi işaretli olmalı ve kolayca anlaşılabilmelidir.

71)Paket kayıplarını azaltmak ve bantgenişliğini daha iyi kullanmak için FEC (Forward Error Correction) teknolojisini desteklemelidir.

72)Cihazın asimetrik trafikleri engellemek için route cache özelliği olmalıdır.

73)Cihazın özel durumlarda geri dönüş trafiğinin başka bir hattan yönlendirilmesine izin verilmesi için auxiliary session desteği olmalıdır.

74)Özellikle dinamik routing senaryolarında route tablosunda devamlı değişiklikler olduğu durumda session başladığı andaki route'un session bitimine kadar kullanımının garanti edilebilmesi amacıyla route-preserve özelliği olmalıdır.

75)Sistem IPv6 trafikleri için de SD-WAN özeliğine sahip olmalıdır.

76)SD-WAN bağlantıları üzerinde istenirse otomatik IPSEC VPN tünel oluşturma yeteneğine sahip olmalıdır. SD-WAN konfigürasyonu esnasında hangi hatlar üzerinde VPN tünel yapılacağı seçilebilmeli ve bu sayede birden fazla SD-WAN hatları üzerinden tek bir hedefe otomatik VPN tanımlaması yapılabilmelidir.

77)Kullanıcı/kullanıcı grubu, kaynak ip/ağ, hedef ip/ağ ve uygulama bazlı bantgenişliği yönetim (QoS) desteği olmalıdır. Grup bazlı ya da uç nokta bazlı QoS yapılabilmelidir. QoS interface tabanlı, inbound/outbound yönünde ve zamana bağlı olarak hat kapasitesinin yüzdesel oranında tanımlanabilmelidir. Ses/video gibi kritik uygulamalara öncelik (priority) ve garanti bantgenişliği yazılabilmelidir. Belirlenen trafik için maksimum bantgenişliği tanımlama imkanı olmalıdır.

78)SSL inspection (https trafiğinin açılması) desteği olmalıdır. Bu sayede ssl trafiklerini açarak, uygulama detaylarına göre; SD-WAN, QoS, uygulama kuralları yazılabilmelidir.

79)Sistem üzerinde detayları aşağıda belirtilen uygulama kontrol özelliği bulunmalıdır.

- Sistemin uygulama kütüphanesinde en az 2500 (ikibinbeşyüz) adet uygulama yer almalıdır.
- Sistemin uygulama kütüphanesinde en az 18 (onsekiz) farklı uygulama kategorisi tanımlı olmalıdır.

80)Uygulama kütüphanesinde yer alan tüm uygulamalar aşağıda belirtilen parametrelere göre kategorize edilmiş olmalıdır.

- Uygulama davranışına göre (botnet, tünelleme amaçlı, bulut uygulaması, bandwith tüketim odaklı v.b.),
- Risk seviyesine göre (Critical, High, Medium, Low v.b.)
- Dünya genelindeki kullanım yoğunluğu, popülerlik seviyesine göre,
- Kullanılan protokole göre (HTTP, DNS, FTP, SIP, H323 gibi)
- Üreticiye göre (Google, Microsoft, Apple gibi)
- Erişim yöntemine göre (Client-server, browser tabanlı, P2P gibi)

81)Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir, sistem yöneticileri tarafında istenirse manuel olarak da güncellenebilir olmalıdır.

82)İstenmeyen uygulamaları kullandığı tespit edilen ip adresleri süreli veya süresiz olarak karantinaya alınabilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

83)Uygulama kontrol veritabanında yer alan tüm uygulamaların listesi, hangi kategoride yer aldıkları ve risk seviyesi bilgisine üreticinin resmi web sitesi üzerinden erişilebilmeli bu bilgiler herkese açık şekilde yayınlanmış olmalıdır.

84)Sistem yöneticileri tarafından özel uygulama imzaları tanımlamaya izin vermelidir.

85)Default portlar üzerinden yapılmayan uygulamaların bloklanması sağlanabilmelidir (örneğin 53 portu dışında başka portlardan yapılan DNS trafiği gibi).

86)Cihaz üzerinde 'rota arama' (route searching) özelliği olmalıdır. Bu sayede spesifik bir adres için trafiğin hangi rota (route) üzerinden gideceği web arayüzü üzerinden kolaylıkla tespit edilebilmelidir.

87)Sistemin güncel saldırıların engellenmesi amacıyla aşağıda detayları belirtilen atak engelleme (IPS) özelliği olmalıdır.

- IPS sistemi aşağıda belirtilen saldırı tiplerini engelleyebilmelidir.
- Trafik Anomaly
- Protocol Anomaly
- Oran (rate) bazlı saldırılar (brute force gibi)
- Sızma temelli (evasive) saldırılar

88)IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak da yapılabilmelidir.

89)Her bir IPS imzası için aşağıdaki aksiyonlar alınabilmelidir.

- İzin ver (pass)
- İzin ver ve olay kaydı al (monitor)
- Paketi düşür (block)
- Paketi düşür ve session'ı sonlandır (Reset)
- Saldırıyı yapanı karantinaya al

90)Tanımlı saldırı tiplerine göre saldırı yapan ip adresleri süreli veya süresiz olarak karantinaya alınabilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

91)Veri tabanında yer alan imzalar aşağıdaki tanımlara göre filtrelenebilmelidir.

- Kullanılan uygulamaya göre (IIS, Oracle, SQL, Apache gibi)
- İşletim sistemine göre (Windows, Linux, Solaris gibi)
- Protokole göre (HTTP, HTTPS, FTP, DNS gibi)
- CVE koduna göre
- Risk seviyesine göre (Kritik, Yüksek Risk, Orta Risk, Düşük Risk gibi)

- Hedef işletim sistemine göre (client ve/veya server)

92)Rate tabanlı saldırı tanımları içerisinde ne kadar sürede kaç adet istekte bulunulabileceği tanımlanabilmelidir. Örneğin OWA'ya 5 sn içerisinde 3'ten fazla login isteğinde bulunulmasın gibi.

93)IPS sistemi aşağıda belirtilen detaylı sızma tekniklerine karşı koruma sağlayabilmelidir.

- IP Packet Fragmentation,
- TCP Stream Fragmentation
- TCP Stream Segmentation,
- RPC Fragmentation,
- URL & HTML Obfuscation,

94)IPS sistemi Botnet aktivitelerini tespit edebilmeli ve engelleyebilmelidir.

95)IPS imzası özelinde kaynak ve hedef adres bilgisine dayalı istisna adresler (exception) tanımlanabilmelidir.

96)IPS sistemi zararlı URL adreslerine yapılan erişim isteklerini engelleyebilmelidir.

97)Sistem IPS loglarında saldırının yönünü gösterebilmelidir (client to server veya server to client)

98)Sistem spoof saldırılarını tespit edebilmelidir.

99)Sistemin 'Risk Puanlama' (Threat Score) özelliği olmalıdır. Bu sayede sistem tarafından tespit edilen malware trafiklerine (virüs, botnet v.b.), kullanılan uygulamaların kategorilerine (P2P, Proxy v.b.) ve erişim yapılan web adreslerinin kategorilerine (Phishing, Hacking v.b.) göre ilgili olaya atanacak risk seviyesi ve risk puanı belirlenebilmelidir. Örneğin yapılan her bir Proxy uygulamasının risk seviyesi 'Critical' ve risk puanı 50 olsun. Erişim yapılmak istenen her bir adult içerikli site için risk seviyesi 'Medium' ve risk puanı 40 olsun gibi.

100)Cihazın detayları aşağıda belirtilen sanal güvenlik duvarı özelliği olmalıdır:

- Cihaz üzerinden birbirinden izole sanal güvenlik duvarları oluşturulabilmelidir.
- Cihaz üzerindeki arayüzler veya sanal arayüzler (vlan) sanal güvenlik duvarları arasında paylaştırılabilmelidir.

101)Her bir sanal güvenlik duvarı için dedike bir sistem yöneticisi atanabilmeli, sistem yöneticilerinin yetkileri olmayan sanal güvenlik duvarlarına erişimleri engellenebilmelidir.

102)Sanal güvenlik duvarı oluşturulması işlemi web arayüzünden kolayca yapılabilmeli ve çalışan mevcut sistemin reboot edilmesine ihtiyaç olmamalıdır.

103)Her bir sanal güvenlik duvarı üzerinde açılabilecek maksiumum oturum (session) sayısı limitlenebilmelidir.

104)Cihazın detayları aşağıda belirtilen servis dışı bırakma saldırılarını (DoS) engelleme özelliği olmalıdır.

105)DoS politikaları ile internetten erişilebilir sistemlere (web server, dns server gbi) yönelik trafikler için eşik değer (threshold) bazlı sınırlandırma yapılabilmelidir.

106)L3 seviyesinde kaynak ve hedef ip bazında açılabilecek toplam oturum sayısı (session) limitlenebilmelidir.

107)L4 seviyesinde kaynak ve hedef ip bazında açılabilecek oturum sayısı limitlenebilmelidir.

108)Sistem portscan ve udpscan saldırılarını tespit edip engelleyebilmelidir.

109)TCP synflood ve UDP flood saldırılarına karşı aynı kaynaktan aynı anda gelebilecek syn istek sayısı limitlenebilmelidir.

110)Sistem IPv6 adresleri için de yukarıda belirtilen anti-DoS özelliklerini desteklemelidir.

111)Belirtilen tüm DoS politika konfigürasyonları cihazın web arayüzünden yapılabilmelidir.

112)Cihazın detayları aşağıda listelenen "SSL Deep Inspection" özelliği olmalıdır.

113)Cihazın SSL Inspection özelliği sadece secure HTTP (HTTPS) trafiği için desteklenmemeli, aşağıdaki protokoller için de araya girerek tarama yapabilmelidir.

- SMTPS
- POP3S
- IMAPS
- FTPS

114)SSL tabanlı botnet iletişiminin engellenmesi amacıyla sertifika karaliste özelliği olmalıdır.

115)İstenen web adresleri, kategorileri ve domain'ler için SSL Inspection istisnası uygulanabilmelidir. Wildcard FQDN istisna objeleri desteklenmelidir.

116)SSL anomaly'lerini ve yazılan istisnai SSL erişimlerini loglayabilmelidir.

117)Bağlantıyı daha güçlü SSL-cipher algoritmaları kullanımına zorlama özelliği olmalıdır.

118)Bağlantıyı TLS 1.2 ve 1.3 protokollerine zorlama özelliği olmalıdır.

119)Güvenilir olmayan CA'ler tarafından imzalanmış sertifika kullanan sitelere erişimler engellenebilmelidir.

120)Süresi geçmiş (expired) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.

121)Doğrulama süresi geçmiş (validation timeout) ya da doğrulanamayan (validation failed) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.

122)Client hello mesajı içerisinde SNI kontrolü yapabilmelidir.

123)Ön tanımlı gelen ve devamlı güncellenen bilindik güvenilir site veritabanı olmalı, ilgili siteler için SSL Deep Inspection istisnası tanımlanabilmelidir.

124)Cihazın SSL Offloading özelliği olmalıdır. Internetten gelen HTTPS trafiğini decrypt ettikten sonra arka taraftaki web server'lara HTTP olarak dağıtabilmelidir.

125)Sistemin grafik arayüzü aracılığıyla aşağıda belirtilen detaylı trafik analiz işlemleri yapılabilecektir.

126)Gerçek zamanlı (anlık) ve geçmişe dönük en fazla trafik yaratan ve en fazla bağlantı (session) isteğinde bulunan kullanıcıların listesi,

127)Gerçek zamanlı (anlık) ve geçmişe dönük en fazla trafik yapılan ve en fazla bağlantı (session) isteğinde bulunulan hedef sunucuların listesi,

128)Gerçek zamanlı (anlık) ve geçmişe dönük en fazla trafik yaratan ve en fazla bağlantı (session) açılan uygulamaların listesi,

129)Gerçek zamanlı (anlık) ve geçmişe dönük en fazla trafiğin yapıldığı ağ arayüzleri (interface'ler),

130)Geçmiş döneme ait tehditlerin risk puanlarına ve bağlantı (oturum) sayılarına göre listesi,

131)Yukarıda belirtilen trafik bilgilerinin detay analizi yapılabilmelidir. Örneğin son 24 saatte en fazla oturum açan (session) kullanıcı tespit edildikten sonra bu oturumların detaylarına (hangi uygulamaları kullanarak hangi hedef sunuculara ve web adreslerine doğru bu bağlantıların açıldığı bilgisine) ulaşılabilmelidir.

132)Cihazın adminler tarafından yapılan tüm trafikleri (webUI, ssh v.b.) kullanıcı trafiklerinden öncelikli işleme özelliği olmalıdır. Bu sayede cihaz üzerinde kaynak dedike etmeye gerek kalmadan admin trafiğinin her koşulda öncelikli işlenmesi garanti edilmeli ve bu özellik sistem yöneticileri tarafından istense de değiştirilememelidir.

133)Cihazın yönetim arayüzü üzerinden sistemle ilgili aşağıdaki detay bilgilere ulaşılabilmelidir.

- Seri no, Firmware versiyonu ve Uptime bilgisi,
- Saniyede oluşan log miktarı (eps),
- Saniyede oluşan bağlantı isteği sayısı (connection per second),
- Mevcut oturum (session) sayısı,
- CPU, Memory ve Disk kullanım değeri (yüzdesel),
- Lisans durumu,
- WAN interface'inin ip adresi ve karalisteye alınmış ise bilgisi,
- Sisteme bağlı olan admin'lerin bilgisi,

134)Sistemin web arayüzü üzerinde grafiksel topoloji görünümü olmalıdır. Bu sayede her bir fiziksel ve/veya sub-interface ile aynı ağ içerisinde yer alan bağlı aktif cihaz sayısı, ilgili cihazların anlık olarak yarattığı trafik miktarı, açık session sayıları, mevcut session'lar içerisinden ne kadar data oluşturdukları, işletim sistemi bilgisine ulaşılabilmelidir.

135)Sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama, Ping6, IPv6 captive portal, IPv6 FQDN adresleri desteklenmelidir.

136)SNMPv3'ü desteklemelidir.

137)İşletim sistemi ve yazılım güncellemelerini web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.

138)Cihazın farklı ürünlerle entegrasyonu amacıyla aşağıdaki protokolleri desteklemesi gerekmektedir;

- WCCP client
- ICAP client

- RADIUS client

Cihazın detayları aşağıda belirtilen bant genişliği yönetim özelliği olmalıdır.

139)Kaynak ip/ağ, kullanıcı/kullanıcı grubu, hedef ip/ağ ve servis bazında bant genişliği politikası yazılabilmelidir.

140)Spesifik uygulama ve uygulama kategorisi (öneğin Update) bazında bant genişliği politikası yazılabilmelidir.

141)Zaman aralığı bazında bant genişliği politikası yazılabilmelidir (örneğin mesai saatleri içerisinde gibi.).

142)Aynı session içerisinde trafiğin yönüne göre (IN ve OUT yönünde) bant genişliği politikası yazılabilmelidir.

143)Sistemdeki tüm kullanıcılar için tanımlı bant genişliği kuralı içerisinde ip başına limitasyon yapılabilmelidir. (örneğin tüm kullanıcıları 10 mbps ile limitle gibi..)

144)Firewall kuralları bazında bant genişliği politikası yazılabilmelidir. Böylece ilgili kuralla eşleşen trafiklerin limitlenmesi sağlanabilmelidir.

145)Cihazın proaktif mimaride otomatik aksiyon alabilme özelliği olmalıdır. Bu özellik sayesinde aşağıdaki olaylardan birisi gerçekleştiğinde otomatik olarak eposta gönderimi, register edilmiş olan IPhone'a push notifikasyon gönderimi ve herhangi bir web servisini tetikleme aksiyonlarını otomatik olarak alabilmelidir.

- Konfigürasyon değişikliği yapıldığında,
- Cihaz kapanıp açıldığında,
- Lisans süresi bittiğinde,
- Yedekli (cluster) cihazlar arasında geçiş yaşandığında,
- AV veya IPS database'i güncellendiğinde,

146)Sistemde önceden tanımlı herhangi bir olay gerçekleştiğinde (örneğin güncelleme işlemi başarısız olduğunda, AD entegrasyonunda sorun olduğunda, IPSec bağlantısı koptuğunda v.b.)

147)Cihazın aşağıda belirtilen SDN (private cloud) ve bulut (public cloud) temelli çözümlerle API entegrasyonu olmalıdır. Entegrasyon yapılan ürünlere ait tanımlanan dinamik objeler bazında güvenlik politikaları tanımlanabilmelidir.

- Cisco ACI
- Amazon Web Service
- Microsoft Azure
- VMware NSX-T
- VMware ESXi
- Nuage Virtulized Service Platform
- Oracle OCI
- OpenStack (Horizon)

- Google Cloud Platform (GCP)
- IBM Cloud
- AliCloud
- Kubernetes

Cihaz üzerinde detayları aşağıda belirtilen servis veri tabanı özelliği olmalıdır.

148)İlgili internet servis veritabanı çok bilinen sistem, ağ ve güvenlik üreticilerinin hizmet amaçlı kullandıkları Web, DNS, FTP v.b. sunucularının ip, port, protokol ve coğrafya bilgilerini içermelidir.

149)Bu veritabanında yer alan üreticilerin hizmetlerine erişimler için veritabanında yer alan objeler kolayca politikalar içerisinde kaynak veya hedef olarak seçilebilmelidir. Örneğin Microsoft sunucularına veya güncelleme için X antivirüs üreticisine doğru erişim kuralı kolayca tanımlanabilmelidir.

150)Internet servis veritabanı sistem tarafından otomatik olarak güncellenmelidir.

151)Birden fazla internet hattının olması durumunda internet servis veritabanı kullanılarak spesifik üretici ve uygulama trafiklerinin belirtilen internet hattı üzerinden yönlendirilmesi sağlanabilmelidir.

152)Internet servis veritabanı sistem yöneticileri tarafından gerekirse özelleştirilebilmelidir.

153)Internet servis veritabanında yer alan hizmetlerin hangi ülke ve hangi şehirden yapıldığı bilgisine ulaşılabilmelidir. Örneğin Microsoft update sunucularının ip, port, protokol bilgileri ile Türkiye'den hangi lokasyonlardan hizmet verildiği bilgisi görüntülenebilmelidir.

154)Güvenlik duvarı üreticisi, güncel "Gartner Magic Quadrant Enterprise Network Firewalls" raporunda "Leaders" kategorisinde yer almalıdır.

155)Ürünler herhangi bir donanım arızası durumunda arızanın bildirilmesinden sonraki iş günü (next business day) değişim garantisiyle teklif edilecektir.

10.3.7 Switch -Tip 1

1) Switchin en az 24 (yirmi dört) adet 10/100/1000BaseT ethernet portu ve en az 4 adet 10G SFP+ fiber yuvası bulunacaktır.
2) Switch aynı anda 28 adet portu aktif olarak kullanabilecektir.
3) Switch hem web üzerinden hem de SSH protokolleri aracılığı ile komut arayüzü üzerinden yönetilebilecektir.
4) Switchnın anahtarlama kapasitesi en az 128Gbps olmalıdır.
5) Switchnın paket işleme kapasitesi 204Mpps olmalıdır.
6) Switch 16.000 Mac adresi tutma kapasitesine sahip olmalıdır.
7) Switch üzerinde en az 4.000 adet vlan tanımlanabilecektir.
8) Switch 802.1s,802.1d ve 802.1w spanning tree protokollerini desteklemelidir.
9) Switchnın Private VLAN desteği olmalıdır.
10) Switch statik yönlendirme desteklemeli ve üzerinde en az 1000 adet rota bilgisi tutabilecektir.
11) Switch MAC ve Port tabanlı 802.1x erişim yetkilendirme protokolünü desteklemelidir.

12) Switchnı yönetecek yöneticiler merkezi Radius sunucusu kullanılarak yetkilendirilebilecektir.

13) Switch http REST API metodu ile yönetilebilmesi ve izlenebilmesi tercih sebebidir.

14) Switch SNMP v1, v2 ve v3 protokolleri ile izlenebilecektir.

15) Switch üzerinde istenirse yapılan değişiklikler revizyon olarak farklı doyalar halinde tutulabilecektir.

16) Switch konfigürasyon dosyası istenirse şifreli olarak kaydedilebilecektir.

17) Switch Sflow veya muadili bir protokolü desteklemelidir.

18) Switch LLDP ve LLDP-MED protokolü ile kendisine bağlı aynı protokolü destekleyen cihazları tanıyabilecektir.

19) Switch Storm control özelliğini kullanarak broadcast, bilinmeyen unicast ve multicast trafikleri belirli bir eşik değerini aştığında engelleyebilecektir.

20) Switch DHCP snooping özelliğini desteklemelidir.

21) Switch DHCP relay özelliği ile kendisine bağlı cihazların uzak bir sunucudan ip alabilmelerine imkan sağlamalıdır.

22) Switch Mac bazlı vlan özelliğine sahip olmalı. Bir porttaki farklı mac adreslerini farklı vlanlara atayabilecektir.

23) Switch statik yönlendirme yapabilecektir.

24) Switch QinQ protokolü ile vlan stacking desteklemelidir

25) Switch ek lisans alınması durumunda bulut üzerinden yönetilebilecektir.

26) Switch'e bağlanacak yöneticiler cihaz üzerindeki kullanıcı adı ve şifreleri kullanabilecektirler veya Radius, tacacs protokolleri ile harici yetkilendirilmiş olarak giriş yapabilecektirler.

27) Switch MCLAG – Multi Chasis Link Aggregation protokolü ile iki adet aynı model ve işletim sistemine sahip switchin tek bir switch gibi diğer cihazlar ile Link Aggregation kurmasına olanak sağlamalıdır.

10.3.8 Switch -Tip 2

1) Switchin en az 48(kırksekiz) adet 10/100/1000BaseT ethernet portu ve en az 4 adet 10G SFP+ fiber yuvası bulunacaktır.

2) Switch aynı anda 28 adet portu aktif olarak kullanabilecektir.

3) Switch hem web üzerinden hem de SSH protokolleri aracılığı ile komut arayüzü üzerinden yönetilebilecektir.

4) Switchnın anahtarlama kapasitesi en az 128Gbps olmalıdır.

5) Switchnın paket işleme kapasitesi 204Mpps olmalıdır.

6) Switch 16.000 Mac adresi tutma kapasitesine sahip olmalıdır.

7) Switch üzerinde en az 4.000 adet vlan tanımlanabilecektir.

8) Switch 802.1s,802.1d ve 802.1w spanning tree protokollerini desteklemelidir.

9) Switchnın Private VLAN desteği olmalıdır.

10) Switch statik yönlendirme desteklemeli ve üzerinde en az 1000 adet rota bilgisi tutabilecektir.

11) Switch MAC ve Port tabanlı 802.1x erişim yetkilendirme protokolünü desteklemelidir.

12) Switchi yönetecek yöneticiler merkezi Radius sunucusu kullanılarak yetkilendirilebilecektir.

13) Switch http REST API metodu ile yönetilebilmesi ve izlenebilmesi tercih sebebidir.

14) Switch SNMP v1, v2 ve v3 protokolleri ile izlenebilecektir.

15) Switch üzerinde istenirse yapılan değişiklikler revizyon olarak farklı doyalar halinde tutulabilecektir.

16) Switch konfigürasyon dosyası istenirse şifreli olarak kaydedilebilecektir.

17) Switch Sflow veya muadili bir protokolü desteklemelidir.

18) Switch LLDP ve LLDP-MED protokolü ile kendisine bağlı aynı protokolü destekleyen cihazları tanıyabilecektir.

19) Switch Storm control özelliğini kullanarak broadcast, bilinmeyen unicast ve multicast trafikleri belirli bir eşik değerini aştığında engelleyebilecektir.

20) Switch DHCP snooping özelliğini desteklemelidir.

21) Switch DHCP relay özelliği ile kendisine bağlı cihazların uzak bir sunucudan ip alabilmelerine imkan sağlamalıdır.

22) Switch Mac bazlı vlan özelliğine sahip olmalı. Bir porttaki farklı mac adreslerini farklı vlanlara atayabilecektir.

23) Switch statik yönlendirme yapabilecektir.

24) Switch QinQ protokolü ile vlan stacking desteklemelidir

25) Switch ek lisans alınması durumunda bulut üzerinden yönetilebilecektir.

26) Switch'e bağlanacak yöneticiler cihaz üzerindeki kullanıcı adı ve şifreleri kullanabilecektirler veya Radius, tacacs protokolleri ile harici yetkilendirilmiş olarak giriş yapabilecektirler.

27) Switch MCLAG – Multi Chasis Link Aggregation protokolü ile iki adet aynı model ve işletim sistemine sahip switchin tek bir switch gibi diğer cihazlar ile Link Aggregation kurmasına olanak sağlamalıdır.

10.4 Sunucu Altyapı ve Yönetim Sistemleri

10.4.1 Sanallaştırma Sistemi

YÜKLENİCİ, fiziksel makineler üzerinde sanal makineler kurarak önerdikleri SCADA/DMS/OMS Sistemi mimarisini oluşturacaktır. YÜKLENİCİ, aşağıda özellikleri tarif edilen sanallaştırma yazılımını kullanacaktır.

Sanallaştırma sadece sunucu katmanında kullanılacak ve aşağıda belirtilen hususlar göz önünde bulundurulacaktır;

- Hypervisor tabanlı sanallaştırma modeli kullanacaktır,
- Kendisini kanıtlamış, endüstrinin önde gelen sanallaştırma platformlarından biri tercih edilecektir, (VMware, Microsoft Hyper-V, Citrix XenServer vb.) Bu tercih ŞİRKET tarafından belirlenecektir.
- Tüm sanal makinelere ait admin&root şifreleri ile giriş bilgileri ŞİRKET'e teslim edilecektir,
- Sanal makinelerin fiziksel makineler üzerindeki yerleşimi, Sistem yedekliliğini ve performansını en iyi uygun şekilde sağlayacak yapıda olacaktır.

- Sunucuların sanallaştırılması için gerekli olacak tüm yazılım ve lisansların temini ve tesisi YÜKLENİCİ tarafından temin edilecektir.
- Teklif edilen sanallaştırma yazılımı ile her bir sanal makinaya 1TB sanal bellek atanabilecektir.
- Teklif edilen sanallaştırma yazılımı gerektiğinde her bir sanal makine için atanan disk alanın doğrudan disk havuzundan almak yerine, sanal makine diski doldukça büyütebilecektir. (Thin Provisioning)
- Misafir işletim sistemi olarak Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022, Centos, Redhat, Ubuntu, Solaris, MacOSX, FreeBSD desteklemelidir.
- Sanal makinalara verilen disklerin ve sanal makinaların bulunduğu dosya sisteminin sistem çalışırken büyütülmesine izin vermelidir.
- Sanal makinalara 62TB boyutunda sanal diskler atanmasına olanak sağlamalıdır.
- 64TB boyutundaki depolama alanlarını yönetebilecektir
- FC, iSCSI ve NFS gibi veri depolama teknolojilerini ve bu teknolojilerle çalışan veri depolama ünitelerini desteklemelidir.
- Teklif edilen sanallaştırma yazılımı ile sistemde yetkilendirme yapılabilmeli, belirli operasyonel kişilerin tüm sanal sisteme veya sanal sistemin bir kısmına erişmelerine ve yönetim operasyonlarını gerçekleştirebilmelerine imkân tanımalıdır.
- Teklif edilen sanallaştırma yazılımı ile sistem performansı CPU, memory, disk ve network gibi parametreler için anlık veya geçmişe doğru izlenebilmeli, rapor alınabilecektir.
- Teklif edilen sanallaştırma yazılımı tüm sanal sunucuların tek bir merkezden yönetimini sağlayan merkezi yönetim yazılımını içermelidir. (Merkezi yönetim yazılımı lisansları ile teklif edilecektir)
- Teklif edilen sanallaştırma yazılımı ile gelen merkezi yönetim yazılımı web arayüzünden bağlanıp yönetmeye olanak sağlamalıdır.
- Teklif edilen sanallaştırma yazılımı sanal sunuculara VLAN atanmasına izin vermelidir.
- Teklif edilen sanallaştırma yazılımı sanal sunucuların açıkken bir kopyasının çıkarılmasına izin vermelidir.
- Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinaları ihtiyaç duyulduğunda paylaşımlı bir disk alanına ihtiyaç duymaksızın sanallaştırma sistemi içindeki başka bir sunucuya aktarabilmeli, bu işlemi aynı anda birden fazla sanal makina için gerçekleştirebilecektir.
- Tanımlı sunuculardan birisinde kontrol dışı bir durma olduğunda kapanan sanal makinaların sistemdeki diğer sunucular tarafından otomatik olarak çalıştırılması şeklinde kümeleme hizmeti desteği olmalıdır. Bu hizmet için sanal makinalar arasında önceliklendirme yapılabilecektir.
- Teklif edilen sanallaştırma yazılımı içerisinde çalışan Windows ve Linux sanal makinaların yedeklerini disk ortamına alan bir modülü bulunmalıdır. Bu modül yedeklenmiş verileri tekilleştirme yaparak saklayabilecektir.
- Teklif edilen sanallaştırma yazılımı belirlenen sanal makinaların aynı lokasyondaki veya uzak bir lokasyondaki sanallaştırma sunucuları üzerine replikasyon yapmasına olanak tanımalıdır.

- Teklif edilen sanallaştırma yazılımı üçüncü parti antivirus çözümleri ile entegre çalışabilmeli ve ajansız mimari kullanarak sanal makinalar üzerinde virüs taraması yapılmasına olanak sağlamalıdır.
- Teklif edilen sanallaştırma yazılımı kendi üzerinde sanal makine şifrelemesini sağlamalıdır.
- Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinaları diskleri ile birlikte depolama alanları arasında taşıyabilecektir.
- Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinalara CPU, memory, disk ve network kartı eklenmesini desteklemelidir.
- Teklif edilen sanallaştırma yazılımı seçilen sanal makinalar için çalıştığı fiziksel sunucuların plansız bir kesinti yaşaması durumunda, kesintisiz olarak diğer fiziksel sunuculardan çalışmasına devam etmesini sağlayabilecektir.
- Teklif edilen sanallaştırma yazılımı fiziksel sunucular üzerindeki memory koruma yöntemleri ile korunmuş memory alanlarını otomatik olarak algılayıp, kritik sistem bilgilerini bu memory alanlarına yazılmasını sağlayacak bir teknoloji içermelidir.
- Teklif edilen sanallaştırma yazılımı Hadoop kurulumlarını kolaylaştıracak bir modül içermelidir.
- Teklif edilen sanallaştırma yazılımı sanal sunucuların serial port konsoluna network üzerinden bağlanılmasına olanak tanımalıdır.
- Teklif edilen sanallaştırma yazılımı sanal makinaların iş yüklerini sürekli izleyip gerek görmesi durumunda fiziksel makinalar üzerindeki iş yükü dağılımını ayarlamak için sanal makinaları otomatik olarak sisteme dahil fiziksel sunucular arasında taşıyabilecektir. Bu işlemin yapılması istenirse tam otomatik olarak, istenirse de sistem yöneticisine tavsiye şeklinde bilgi vererek gerçekleşebilecektir.
- Teklif edilen sanallaştırma yazılımı fiziksel sunucular üzerinde yük dengelemesi yaparken istenildiğinde yoğun çalışmayan fiziksel makinaların üzerindeki yükü diğerleri üzerine taşıyıp, boşa çıkan fiziksel makinaları elektrik tasarrufu etmek amacıyla kapatılmasına olanak tanımalıdır. Ayrıca ihtiyaç olduğunda kapana fiziksel sunucular tekrar açılabilecektir.
- Teklif edilen sanallaştırma yazılımı depolama ünitesi üzerinde yapılan vm klonlama veya taşıma gibi işlemler sırasında ilgili işlemin iş yükünü depolama ünitesine yükleyerek yapılmasını sağlayabilecektir.
- Teklif edilen sanallaştırma yazılımı üçüncü parti firmaların ürettiği multi-pathing yazılımlarına destek vermelidir.
- Teklif edilen sanallaştırma yazılımı depolama alanlarının doluluk oranlarını ve gecikme(latency) değerlerini izleyip, gerektiğinde sanal makinaları daha müsait depolama alanları üzerine otomatik olarak taşıyabilecektir.
- Teklif edilen sanallaştırma yazılımı disk ve network kullanımını sanal makina bazında önceliklendirebilmeli, seçilen sanal makinaların diğer sanal makinalara göre daha fazla disk ve network I/O kaynağı kullanabilmesini sağlayabilecektir.
- Teklif edilen sanallaştırma yazılımı 10Gbit PCI express kartların mantıksal olarak bölünerek, her bir parçasının sanal makinalara doğrudan kullandırılmasına olanak tanımalıdır.

- Teklif edilen sanallaştırma yazılımı sanal makinalarda çalışan belirli uygulamalar üzerinde meydana gelebilecek servis kesintilerini tespit edip, gerektiğinde ilgili servisi ya da sanal makinayı yeniden başlatarak sorunu düzeltebilecek bir modül içermelidir.
- Teklif edilen sanallaştırma yazılımı PVLAN, LACP, Netflow, ERSPAN, Port Mirroring, ACL, CoS Tagging, DSCP Tagging gibi network servislerine destek verebilen ve tek merkezden yönetilebilen bir network çözümü içermelidir.
- Teklif edilen sanallaştırma yazılımı fiziksel sanallaştırma sunucuları üzerindeki tüm ayarların merkezi bir şablon olarak hazırlanıp yapıdaki tüm sunuculara tek seferde uygulanmasına olanak sağlamalıdır.
- Teklif edilen sanallaştırma yazılımı gerektiğinde fiziksel sunucular üzerine sabit disk takılmasına gerek kalmadan, networkten boot edip çalışabilecektir.
- Teklif edilen sanallaştırma yazılımı fiziksel sunucular üzerindeki SSD diskleri istenilen sanal makinalar için okuma önbelleği (read-cache) olarak kullanabilecektir.
- Teklif edilen çözüme ait lisanslar ile birlikte sözleşme süresi boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilecektir, ayrıca yine sözleşme ve garanti süresi boyunca hafta içi çalışma saatleri içerisinde uzaktan destek hizmeti verilecektir.
- Aynı fiziksel sunucu üzerinde oluşturulacak sanal makinaların mevcut sistem kaynaklarının üzerinde kaynak atanmasına (over-commitment) izin vermelidir.
- SMP (Symetric Multi Processing) desteği olmalıdır. Teklif edilen sistemde her bir sanal makinaya istenildiğinde 64 adet sanal CPU atanabilecektir.

10.4.2 Yedekleme Sistemi

Teklif edilecek yazılım, aşağıda belirtilen gerekli teknik detayları ve özellikleri karşılayabilecek yeterlilikte olacaktır.

Yedekleme Sistemi Yazılımı;

- vSphere (5.5, 6.x, 7.0) ve Hyper-V (2008R2 SP1, 2012, 2012R2, 2016, 2019)'de çalışan sanal makinaların yedeklemesini ve replikasyonunu, ajan kurulumu gerektirmeden, imaj seviyesinde, uygulama tutarlı yapabilmeli, yedekleme ve replikasyon görevlerini tek bir yazılımla tek bir konsoldan yönetebilecektir.
- Yedeklemeleri meta verilerini içerecek şekilde oluşturmalı, herhangi bir kataloğa ve orijinal veri tabanına bağımlılığı olmadan aynı üreticinin farklı bir yedekleme sunucusunda içe aktarılabilecektir.
- Destekleyen Linux işletim sistemleri üzerindeki diskler ile, sabit (immutable) yedekleme havuzu oluşturabilmeli ve hızlı blok klonlama yeteneği bulunmalıdır.
- Herhangi bir ajan kurulumu gerektirmeden özelleştirilebilen ve devre dışı bırakılabilen dâhili sıkıştırma ve tekilleştirme sunmalıdır.
- Tam ve artımlı yedekleri kullanarak yeni tam yedekler oluşturabilecektir.
- Saklanan yedekleri ve ağ trafiğini uçtan uca (kaynakta, aktarırken ve depolarken) AES 256-bit şifreleyebilecektir.
- Görevlerin kullanabileceği network bant genişliğini, eş zamanlı çalışacak görev sayısını, backup diskine aynı anda yazılabilecek kanal sayısı ve veri oranını yöneticinin istediği değerlerde limitleyebilecektir.

- Teklif edilecek yazılım, bir disk alanına alınmış yedeklerin tamamını veya sadece içerisinden seçilen belirli Sanal Makinaların yedeklerini ikincil bir disk alanına; yedeğin kopyalanması veya uzun dönem arşivlenmesi (GFS) amacı ile otomatik olarak kopyalayabilmeli, periyodik doğrulama ve hata giderme yapabilecektir.
- Bir disk alanına alınmış yedekleri ve Windows veya Linux sunucular içerisinden dosyaları teyp ünitelerine, teyp kütüphanelerine ve Sanal Teyp Kütüphanelerine arşivleyebilecektir.
- Teybe yedeklenmiş bir sanal makinanın doğrudan ana sunucu üzerine geri yüklenmesini desteklemelidir.
- Üretici onaylı bulut servis sağlayıcısı tarafından sunulan Bulut ortamını yedek deposu olarak tanımlayabilmeli, yedeklerini veya yedek kopyalarını bu alana gönderebilmeli; replikasyon hedef ana sunucusu olarak tanımlayabilmeli, sanal makina replikasyonu yapabilecektir.
- Üretici onaylı en az üç (3) adet yerel bulut servis sağlayıcısı bulunmalıdır.
- VMware platformunda, HPE 3PAR, Nimle, Primera; NetApp FAS, AFF, Solidfire; DellEMC VNX, VNX2,VNXe, UNITY, SC; Fujitsu Eternus DX/AF; IBM Storwize, SVC; Huawei Oceanstor, Infinidat infinibox; Lenovo V, N; Pure Storage FlashArray; Westerndigital IntelliFlash serileri Veri Depolama ünitelerinin desteklenen bağlantı ve protokolleri üzerinde oluşturduğu veya daha önce oluşturulmuş Donanımsal Snapshot'lar içerisinden komple Sanal Makina, hipervizör tarafından desteklenen tüm işletim sistemlerinden dosya ve uygulama öğesi (Microsoft Exchange, Active Directory, SharePoint, SQL öğeleri) kurtarabilecektir.
- Geçerli bulut hizmetleri abonelik bilgileri sağlandığında, bir sanal makinayı doğrudan Microsoft Azure, Amazon AWS ve Google ortamına geri yükleyebilecektir.
- Sanal makinaya herhangi bir ajan/servis kurulumu gerektirmeden, sunucunun tamamını geri yüklemeye gerek kalmadan istenilen klasör veya dosyaları arama, bulma, dışa aktarma ve geri yükleme yapabilecektir.
- Sunucuya bir ajan/servis kurulumu gerektirmeden, Microsoft Active Directory, Exchange, SQL ve Sharepoint yedekleri içerisinden uygulama öğelerini ve veri tabanlarını yedeklerden ve yedek kopyalarından kurtarabilecektir.
- Bir sanal makinayı doğrudan diskte bulunan tam veya artımlı yedek dosyasından ilave bir kopyalama veya müdahaleye gerek kalmadan çalışır duruma getirebilecektir. Ajanlı ve ajansız alınmış imaj yedeklerini, vSphere, HyperV ortamlarına anında çoklu kurtarma yapabilecektir.
- Sanal makinaları ana sunucu ve disk alanları üzerinde taşıma özelliği sunmalıdır. Bu işlemi VMware vMotion, Storage vMotion veya kendi taşıma teknolojisini kullanarak yapabilecektir.
- Diske alınan yedeği, geri dönüş sağlanırken, komut satırı destekleyen antivirüs yazılımı ile tarama yapılabilmesini destekleyecek ve sonucunda aksiyon alabilecektir.
- Diskte bulunan yedekleri replikasyon kaynağı olarak kullanarak geri dönüş noktalarını yedeklerden oluşturabilecektir.
- Replike edilmiş Sanal Makinayı istenilen geri dönüş noktasından, önceden tanımlanmış Sanal Ağ ayarları ile çalışır duruma getirebilmeli ve Windows sanal makinaları için IP ayarlarını önceden tanımlayabilecektir.
- Veri kaybı olmadan veri merkezi taşımasını organize edecek Planlı Taşıma özelliği sunmalıdır.

- Yedekleri saklamak için CIFS/SMB dosya paylaşımlarını, harici USB disklerini, Windows/Linux işletim sistemlerine doğrudan ve SAN/iSCSI ortamlarından bağlanmış diskleri, üzerinde dâhili tekilleştirme sunan cihazları, S3, Azure Blob ve Google Cloud depolama alanlarını kullanabilecektir.
- Diske alınan sanal makina yedeklerini doğrudan yedek dosyasından izole bir ortamda çalışır hale getirerek, işletim sistemi, hipervizör ve uygulama seviyesinde otomatik test edip, ilgili kullanıcılara raporlayabilecektir.
- VMware platformunda, her bir replikasyon kurtarma noktasını otomatik olarak doğrudan replike edilmiş sanal makinayı izole bir ortamda çalışır hale getirerek, işletim sistemi, hipervizör servisi ve uygulama seviyesinde test ederek bunu rapor olarak ilgili kullanıcılara gönderebilecektir.
- Geri dönüş sırasında sanal makineyi izole bir ortamda açarak içinde gerekli veri temizleme işlemlerini yapabilecek ve KVKK uyumluluk süreçlerine yardımcı olacak teknoloji sunmalıdır.
- Bir veya birden fazla Sanal Makinayı doğrudan yedek dosyasından veya replikasyon noktasından, izole bir ortamda kullanıcının belirleyeceği sıra ve kaynak ile çalışır hale getirerek test, hata tespiti veya eğitim amaçlı kullanılmasını sağlamalıdır.
- Web arayüzü kullanılarak yedekler içerisinden Sanal Makinaların ve Dosyaların geri yüklemesi yapılabilecektir.
- Web arayüzü kullanılarak yedekler içerisinden Exchange 2010, 2013, 2016 posta kutuları ve SQL ve Oracle Veritabanları geri yüklenebilecektir.
- Saklanan yedekleri ve ağ trafiğini uçtan uca AES 256-bit şifreleyebilmeli ve kayıp şifre koruması sunmalıdır.
- Replike edilen sanal makinaları tanımlanan sırayla çalışır hale getirebilecek bir Kurtarma Planı özelliği sunmalıdır
- SQL ve Oracle sanal sunucularında ajan kullanmadan ve yedekleme görevinin zamanlama ayarlarından bağımsız frekanslarda işlem günlüğü yedeği alabilmeli ve veri tabanlarını anında yayınlama ve kurtarma yapabilecektir.
- Tanımlanmış sınırsız sayıda yedekleme deposunu tek bir büyütülebilen yedek deposu olarak kullanarak disk alanı yönetimini basitleştirmeli, tam ve artımlı yedeklerin ayrı depolarda saklanabilmesini, yedeklemelerin arşivlenmesi için Amazon Glacier ve Azure Archieve ortamlarını desteklemelidir.
- Kaynak Sanal Makinaların bulunduğu disk alanlarındaki I/O gecikmelerini izleyebilmeli, eşik değerleri her bir disk alanı (datastore) için farklı olarak ayarlanabilmeli, belirtilen değer aşıldığında o disk alanı üzerinde bir yedekleme veya replikasyon görevi başlatmamalıdır.
- Daha az ağ bant genişliği kullanarak yedekleri ikinci bir disk alanına kopyalamak veya sanal makina replikasyonu yapabilmek için dâhili WAN Hızlandırıcı sunmalıdır. VMware sanal makinaları için sürekli veri koruması sunmalı, saniyeler seviyesinde koruma sağlayabilmeli ve yedekleme, replikasyon ve sürekli veri koruması özellikleri tek bir yazılım ile tek bir konsol üzerinden yönetilmelidir.
- VMware platformunda, HPE 3PAR, Nimle, Primera; NetApp FAS, AFF, Solidfire; DellEMC VNX, VNX2, VNXe, UNITY, SC; Fujitsu Eternus DX/AF; IBM Storwize, SVC; Huawei Oceanstor, Infinidat infinibox; Lenovo V, N; Pure Storage FlashArray; Westerndigital IntelliFlash serileri Veri Depolama ünitelerinin desteklenen bağlantı ve

protokolleri üzerinde oluşturduğu Donanımsal Snapshot'ları kullarak Yedekleme ve Replikasyon kaynağı olarak kullanabilecektir.

- vCloud Director veya vCenter üzerinden kullanıcı yetkilerini çekip ilgili kullanıcıların kendilerine ait makinalar üzerinde yedekleme ve kurtarma işlemlerini web arayüzü üzerinden yapabilmelerine olanak sağlamalıdır.
- Dâhili komut satırı (PowerShell) ve REST API desteği bulunmalıdır.
- Oracle RMAN ve SAP Hana Backint ile bütünleşmiş (entegre) çalışabilen plug-in sunmalıdır.
- Güncel Windows ve Linux işletim sistemi dağıtımlarında, merkezi olarak ajan kurmayı ve yönetmeyi desteklemeli, işletim sistemi ve uygulamalar çalışırken, imaj, disk ve dosya klasör bazında ve uygulama tutarlı yedekleme işlemi yapabilecektir.
- Fidye saldırılarına karşı (ransomware) veriyi istenildiği takdirde mevcut donanımlar kullanılarak güvenli olarak saklayabilecektir. Bu özellik için ilave lisans gerekmesi durumunda teklife dâhil edilmelidir. Bu özelik için ilave saklama ünitesi gerekiyor ise teklife dâhil edilmelidir.
- Yedekleme alan kapasitesi lisansa bağlı olarak teklif edilmesi durumunda en az 1PB için lisans teklife dâhil edilmelidir.
- Yazılım kurulumu, konfigürasyonu yapılmış şekilde teslim edilecektir. Sanal Kurulum için gerekli Windows sanal sunucu kaynağı, proxy sunucu kaynağı ve depolama kaynağı İŞ SAHİBİ tarafından sağlanacaktır.

10.4.3 Ağ Servis ve Kaynaklarını İzleme Sistemi

YÜKLENİCİ çözüm içerisinde kullandığı ürün, servis, ağ cihazı, sunucu gibi ürünlerin erişilirliğini ve kaynaklarını izleyebilmek için detayı aşağıda belirtilen bir yazılım sistemi temin edecektir. Yazılım asgari olarak bu izlemeleri sağlayacak şekilde lisanslanmış olacaktır.

- Yazılım, sanal veya fiziksel sunucuya kurulabilir özellikte olacaktır.
- Yazılım, windows server 2019, windows server 2016, windows server 2012 R2 ve windows 10 işletim sistemleri üzerinde çalışabilir özellikte ve web tabanlı olacaktır.
- Yazılım, tüm izleme faaliyetlerini web ara yüz üzerinden yapacaktır.
- Yazılım, izleme faaliyetleri ile ilgili tüm yapılandırmaları web ara yüz üzerinden yapacaktır. Harici herhangi bir programa ihtiyaç duyulmayacaktır.
- Yazılım, ihtiyaç duyulursa ara yüze bağlanmak için kullanabileceğiniz alternatif bir desktop arabirim yazılımı olmalıdır
- Yazılım, yapılandırıldığı tüm lokasyonlara (merkez ve şubeler) ait bilgileri tek web sayfa üzerinde grafik ara yüzler aracılığıyla görüntüleme yeteneğine sahip olacaktır.
- Yazılım, birden fazla şubelerde bulunan donanım, yazılım ve sanallaştırma ortamlarının izlenmesi yeteneğine sahip olacaktır.
- Yazılım, tüm lokasyonlardan gelen verileri tek bir merkez sunucu üzerinde toplayabilecektir.
- Yazılım, üzerinde anlık grafiksel durum izlenebilmelidir
- Yazılım, cluster yapısını destekleyecektir.
- Yazılım, cluster için ek lisanslama gerektirmeyecektir.
- Yazılım, sensör bazlı lisanslamaya sahip olacaktır.
- Yazılım, lisansı ek modüller, eklentiler ve özellikler için ek lisanslamaya ihtiyaç duymayacaktır.

- Yazılım, eklenmiş olan tüm sensörleri kullanıcının belirleyeceği şekilde gruplandırabilmelidir.
- Yazılım, sınırsız sensör lisansına sahip olacaktır.
- Yazılım, 3 yıllık garantiye sahip olacaktır.
- Yazılım, yıllık bazda lisans yenileme, üretici yenileme gerektirmeksizin kullanılmaya devam edilebilecektir.
- Yazılım, Windows, Linux ve MacOS işletim sistemlerini ajansız olarak izleme yeteneğine sahip olacaktır.
- Yazılım, sanallaştırma platformlarını (en az Ms Hyper-V, Vmware, Esx, Esxi, Vcenter vb.) izleme yeteneğine sahip olacaktır.
- Yazılım, e-posta hizmetlerini (en az Ms Exchange 2016 ve 2019, Linux tabanlı e-posta sunucuları,SMTP, POP3 ve IMAP) izleme yeteneğine sahip olacaktır.
- Yazılım, aktif ağ cihazlarını üretici bağımsız olarak anlık gözleme, hata raporlarını üretme, kayıt altına alma ve detaylı trafik raporlarını oluşturma yeteneklerine sahip olacaktır.
- Yazılım, Snmp, Wmı, Icmp, Http, Mqtt, Soap, Ssh, Ftp, Smtp ve Pop3 yeteneklerine sahip olacaktır.
- Yazılım, NetFlow, sFlow, jFlow yeteneklerine sahip olacaktır.
- Yazılım, otomatik keşif (auto discovery) yeteneğine sahip olacaktır.
- Yazılım, eklenen tüm algılayıcıları (sensörleri) gruplayabilme yeteneğine sahip olacaktır.
- Yazılım, belirli aralıklarla, ağ eklenmiş olan cihazların verilerini yenileyebilme ve kullanıcıdan bağımsız olarak bu işlemi gerçekleştirebilme özelliğine sahip olacaktır.
- Yazılım, tüm cihazlar ve üzerlerinde gerçekleşen olaylara ilişkin kayıtları (log) saklama özelliğine sahip olacaktır.
- Yazılım, en az durum, sistem ve olay bazında olayları kayıt altına alma (log) yeteneğine sahip olacaktır. 29- Yazılım, Olay Kaydı (event log) izleme (monitoring) yeteneğine sahip olacaktır.
- Yazılım, izlediği tüm unsurlar için kullanıcının tanımlayacağı eşik değerlerde alarmlar üretebilmelidir.
- Yazılım, tanımlı eşik değerler ile ilişkili alarm ürettiğinde kullanıcılara e-mail veya sms yolu ile bildirimler gönderebilmelidir.
- Yazılım, üzerindeki standart bildirimlerin kullanıcılar tarafından özelleştirilebilmesine ve kullanıcıların kendilerine özgü bildirimler oluşturmalarına olanak sağlayacaktır.
- Yazılım, verilerin izlenebilmesi amacıyla harici bir veri tabanına ihtiyaç duymayacaktır.
- Yazılım, içerisinde kendisine ait bir veri tabanını barındırmalı, ayrıca bir veri tabanı lisansı gerektirmeyecektir.
- Yazılım, kurulumu esnasında veri tabanını otomatik olarak kurmalı, ayrıca bir veri tabanı kurulumu gerektirmeyecektir.
- Yazılım, kurulum esnasında web sunucuyu otomatik olarak kurmalı, ayrıca bir web sunucusu kurulumu gerektirmemelidir.
- Yazılım, herhangi bir cihazı izlemek için cihaz üzerine yüklenecek bir ajan yazılıma ihtiyaç duymayacaktır.
- Yazılım ile izlenmesi planlanan unsurların disk doluluğunun toplam, fiziki disk bazında ve partition bazında izlenmesi sağlanabilecektir.
- Yazılım ile izlenmesi planlanan unsurların işlemci kullanımının fiziksel işlemci bazında veya çekirdek bazında izlenmesi sağlanacaktır.
- Yazılım ile izlenmesi planlanan unsurların bellek kullanımının izlenmesi sağlanacaktır.

- Yazılım ile izlenmesi planlanan unsurların ağ iletişim miktarının toplam ve interface bazında değerleri izlenmesi sağlanacaktır.
- Yazılım ile Windows servislerinin ve çalışan processlerin izlenmesi sağlanacaktır.
- Yazılım, eklenecek olan tüm cihazların ve cihaz bileşenlerinin, servislerin ve izlenmesi planlanan diğer unsurların kullanıcının belirleyeceği şekilde gruplandırılabilmesini sağlayacaktır.
- Yazılımın yönetimi web üzerinden Http/Https ile yapılabilecektir.
- Yazılım, Icmp, Http, Https, Dns gibi servisler üzerinden izlenilen cihazlardaki servisin durumunu, belirtilen servis sorgularına verdiği yanıtla ve yanıt süresini takip edebilmelidir.
- Yazılım, topladığı verilerin web arayüz üzerinde grafiklerle gösterilebilmesini sağlayacaktır.
- Yazılım ile farklı kullanıcı grupları oluşturularak cihaz izlenilen değer bazlı okuma/yazma gibi yetkilendirme yönetimi yapılabilmelidir.
- Yazılım üzerinde kullanıcılar oluşturulmalı ve bu kullanıcılara izleyici, yönetici gibi haklar verilebilmelidir.
- Yazılım, otomatik tarama yöntemi ile Snmp v2, Snmp v3, Wmı, Icmp protokollerini destekleyen ağdaki cihazları bulma ve izleme işlemini yapabilmelidir.
- Yazılım, ağdaki cihazların manuel yöntemle eklenme ve izleme işlemini yapabilmelidir.
- Yazılım, kurulum ile birlikte üzerinde tanımlı standart raporlar barındırmalıdır.
- Yazılım, istenilen sensörlerden veya sistem durumu ile ilgili olarak oluşturulmuş durumların belirli zamanlarda raporlarını alabilme yeteneğine sahip olacaktır.
- Yazılım, izlediği cihaz, cihaz bileşenleri, servisler ve izlenmesi planlanan unsurların geçmişe dönük izleme verilerini saklayabilmeli.
- Yazılım, geçmişe dönük verilerin raporlarını sağlayabilmeli.
- Yazılım, zamanlanmış raporlama imkanı sağlamalıdır.
- Yazılım, Grafik tabanlı bant genişliği raporları alma ve anlık durum izleme yeteneklerine sahip olacaktır.
- Yazılım Html, Pdf, Csv ve Xml formatlarında raporlama sağlamalıdır.
- Yazılım, Cisco, Hp, Dell, Sonicwall, Juniper, Vmware vs. gibi global ölçekli üreticiler için tanımlanmış hazır izleme yapılarını bulundurmalıdır.
- Yazılım, marka bağımsız olarak tüm ağ cihazlarını izleyebilmelidir.
- Yazılım, izlediği cihazlardan trafik ve cihaz sağlık bilgilerini (Cpu kullanımı, Ram kullanımı, sıcaklık değerleri) alabilmeli ve ara yüzde gösterebilmelidir.
- Yazılım, izlediği cihaz düşme(down) konumuna geçtikten ve ilk alarm üretildikten sonra ayakta (up) konumuna geçene kadar tekrar tekrar düşme (down) bildirimi göndermesini engelleyebilmelidir.

- Yazılım, kullanıcılar tarafından izleme haritaları oluşturulmasını sağlamalıdır

10.4.4 Active Directory/RADIUS

SCADA sunucularının yönetimi için Domain/Active Directory ihtiyaç duyulması halinde kurulumu gerçekleştirilmiştir. Ayrıca buna ek olarak DMZ ortamındaki ürün ve sistemlerin yönetilmesi için de yedekli Active Directory kurulması gerekmektedir. Bu active directory sunucusunun KBS domaini ile bir ilişkisi olmamalıdır.

RADIUS ihtiyaçları için Active Directory ile entegre edilmiş Network Policy Server (NPS) kurulumu yapılacak ve çözümde bulunan ürün ve servisler Active Directory /RADIUS

ortamına entegre edilecektir. Veya YÜKLENİCİ Sisteminin kullanılmasının istenmesi durumunda YÜKLENİCİ Sistemlerinin eklenebilmesi için uç cihazlar üzerinde ayarlandırma desteği verecektir.

10.4.5 Loglama Sistemi

Güvenlik olaylarının tespit edilmesi ve bunlara yanıt verilmesinin desteklenmesi için SCADA/DMS/OMS sistemi ilgili güvenlik olaylarını sürekli günlüğe kaydedecektir.

Ayrıca network cihaz, sunucu, işletim sistemi ve antivirus olayları kaydedilecek ve SIEMe gönderilebilecektir.

Sistemin üretmiş olduğu kayıtların kapsamlı bir şekilde toplanması, birleştirilmesi, saklanması ve doğru analizler gerçekleştirilmesi gibi adımlar sağlanarak saldırının göstergeleri ve delilleri elde edebilir olacaktır.

Sistemin üretmiş olduğu tüm kayıtlar merkezi bir sunucu üzerinde toplanacaktır. Toplanan kayıtların ŞİRKET'in mevcut sistemine gönderimi sağlanacak ve gerekli entegrasyonlar gerçekleştirilecektir.

Kesici ve ayırıcı açma-kapama logları zaman etiketleri ile birlikte SCADA'lı ve SCADA'sız istasyon bilgisi ile birlikte her kesinti özelinde raporlanabilir olacaktır.

Halihazırda şirket tarafından kullanılan sistem YÜKLENİCİ tarafından kullanılamaz ise çözüm için gerekli olan yazılımın kurulması durumunda lisanslı ürün yüklenici tarafından temin edilmelidir.

Çözüm için sunucu yazılım kurulması durumunda lisanslı ürün olmalıdır.

Ürün ve sistemlerden alınan loglar azami olarak aşağıdaki gibi olacaktır;

- SCADA Uygulama ve Sunucu Logları
- Sunucu ILO logları
- Windows Sunucular
    - Security Event Loglar
    - System Event Logları
    - Application Logları
- Network Cihaz Logları
    - Firewall Trafik, IDS, Application Logları
    - Firewall System Events loğları
    - Switch System Events logları
- IIS – Apache Access logları
- Linux Audit logları
- Linux uygulama özelindeki loglar

10.4.5.1 Kullanıcı Kayıtları

SCADA/DMS/OMS sistemi, yerel bir günlükte en az aşağıdakileri içerecek şekilde güvenlik olaylarını kaydedebilecektir;

- Başarılı kimlik doğrulamaları,
- Başarısız kimlik doğrulama girişimleri,
- Sistem saatini değiştirme,
- Anahtarları veya kimlik bilgilerini değiştirme,
- Anahtarları veya kimlik bilgilerini değiştirme girişimi başarısız olması durumları,
- Kullanıcı hesaplarını değiştirme,
- Yetkilerin değiştirilmesi,

Güvenlik olayları için günlük girişleri bir zaman damgası, bir olay açıklaması ve olaya neden olan rolü ve kişiyi içerecektir.

Bir kullanıcıya yönelik tüm konsol etkinliklerini izlemek için ya manuel olarak (Örneğin kontrol odası oturum açma) ya da otomatik olarak (Örneğin uygulamada ve/veya işletim sistemi katmanında oturum açma) bir yöntem belirlenecektir. Neyin günlüğe kaydedildiği, günlüklerin nasıl saklandığı (veya yazdırıldığı), nasıl korunduğu, günlüklere kimin erişimi olduğu ve bunların nasıl/ne zaman gözden geçirildiğine ilişkin politika ve prosedürler oluşturularak ŞİRKET denetimine ve kullanımına sunulacaktır.

10.4.5.2 Sistem Kayıtları

SCADA/DMS/OMS sisteminde bulunan donanım ve yazılımların ürettiği olay kayıtlarının belirlenen kurallar dahilinde kayıt altına alınması sağlanacaktır.

Sistem kayıtları; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulacak ve bütünlüğü zaman damgası ile korunacaktır.

10.5 Siber Güvenlik

SCADA/DMS/OMS'in güvenli olması gerekir. Bu yükümlülüğü yerine getirmek için alınan önlemler, çalışanlar üzerindeki geçmiş kontrollerinden tesislere erişimin kısıtlanması ve dijital olarak kaydedilmesine kadar geniş bir yelpazeyi kapsamaktadır. Çalışan eğitimini, ŞİRKET içi müşteri sistemlerine, belgelere ve verilere erişimi kısıtlamayı, uzaktan erişim yeteneklerini korumayı ve güvenlik açıkları hakkındaki bilgileri korumayı içerir.

6 Haziran 2023 Tarih ve 32213 sayılı Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği ile Enerji Sektörü ŞİRKETlerinin uyması gereken minimum siber güvenlik kontrolleri listelenmiştir. Ayrıca aynı yönetmelik ile Elektrik Dağıtım ŞİRKETlerinin uyması gereken referans topolojinin (EPDK Enerji Sektöründe Siber Güvenlik Olgunluk Modeli Referans Topoloji Elektrik Dağıtım) çerçevesi belirlenmiştir. Proje kapsamında yapılacak işler referans topolojiye göre orta seviye olan Ana Kontrol Merkezi / Yedek Kontrol Merkezi bölgelerindeki şartname ile adreslenmiş iş, ürün ve sistemleri kapsamaktadır. Bu çerçevede Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliğindeki kontroller bu açıdan değerlendirilmiş uyulması gereken Seviye-1, Seviye-2, Seviye-3 kontroller için Şartname kapsamında olan maddeler için sorumluluk YÜKLENİCİ de olacaktır. Sorumluluk ve Faaliyet Alanı, YÜKLENİCİ ile belirtilen kontrollerin YÜKLENİCİ tarafından, ŞİRKET/YÜKLENİCİ ile belirtilen kontrollerin devreye alınması için YÜKLENİCİ ve ŞİRKET iş birliği içerisinde, UYUMLULUK ile belirtilen alanda iş bu sözleşme kapsamında sunulan hizmet, yazılım,

çözüm vb. için uyum zorunluluğu belirtilmiştir. Bu iş birliği bilgi alışverişini, YÜKLENİCİnin kontroller için danışmanlığını ve/veya sistemin kurulumu, işletilmesi süresince ŞİRKET ve YÜKLENİCİ'nin beraber dikkat etmesi gerektiği kontrolleri kapsamaktadır. Bu kontroller için de ŞİRKETin üzerine düşen görevleri yerine getirmesi beklenmektedir. YÜKLENİCİ ekte belirtilen kontrollere uygunluk durumunu, kurulum öncesi dokümanlarında belirtecektir.

Bu isterlere ilişkin testler yapıldığında ve ilgili kapsam ve ekteki kontrol maddeleri ile sorun görülmesi durumunda, YÜKLENİCİ tarafından taahhüt verilecektir ve sistem yapılacak değişikliklere uyumlu olacaktır. Siber tehditlere karşı koruma ve önleme, bilinmeyen tehditlere karşı tespit faaliyetleri yapabilmek için; siber güvenlik ve güvenli sistem yönetimi ile ilgili kanun, yönetmelik ve en iyi pratikler gözetilerek ŞİRKET tarafından uygun görülen yapıda gerekli güvenlik önlemlerinin alınması sağlanacaktır. Eğer 6 Haziran 2023 Tarih ve 32213 sayılı Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği ile Enerji Sektörü ŞİRKETlerinin uyması gereken minimum siber güvenlik kontrolleri üzerinde değişiklik yapılır ve ek donanım veya yazılım gerektirmesi durumunda sorumluluk ŞİRKET'e aittir.

YÜKLENİCİ EK-2.3 Elektrik Dağıtım Sektörü Siber Güvenlik Yetkinlik Modeli Teknik Kontrol Maddeleri'nde belirtilen idari maddeleri iş bu sözleşme ile kabul ettiğini ve uygulamış olduğunu kabul ve beyan etmiş sayılacaktır.

10.5.1 Güvenlik Mimarisi ve Tasarımı

YÜKLENİCİ, SCADA/DMS/OMS için bir sistem planı ve ilgili belgeleri sağlamalıdır. Bu materyal, önerilen bir ağ düzenini gösteren bir diyagram içermelidir. Derinlemesine savunma sağlamak için, sistem bu bölgeler arasında sıkı ve güvenli güvenlik seviyeleri oluşturulmalıdır.

Ana kontrol merkezinde en az 4 güvenlik seviyesi olacak şekilde ana güvenlik seviyeleri olmalıdır. Bu güvenlik seviyeleri fiziksel olarak yedekli çalışan anahtarlama sistemleri(switch) ile oluşturulmalıdır. Anahtarlama sistemine bağlanacak uç noktalar ilgili güvenlik seviyesi switchine bağlanmalıdır. Güvenlik seviyeleri saldırı tespit yetenekleri de olan fiziksel yedekli güvenlik duvarları ile korunmalıdır. Bu güvenlik duvarları detayı şartnamede verilen Tip-1 güvenlik duvarı özelliklerini asgari olarak sağlamalıdır. Ana güvenlik seviyelerine bağlı alt güvenlik seviyeleri olabilir ve bunlar sanal olarak oluşturulabilir. Bu azami güvenlik şartlarını fiziksel, sanal ve mantıksal olarak sağlamak şartıyla daha üst çözümler sunulabilir.

Gebze lokasyonlu kontrol merkezinde en az 1güvenlik seviyesi olacak şekilde ana güvenlik seviyeleri olmalıdır. Bu güvenlik seviyeleri fiziksel olarak yedekli çalışan anahtarlama sistemleri(switch) ile oluşturulmalıdır. Anahtarlama sistemine bağlanacak uç noktalar ilgili güvenlik seviyesi switchine bağlanmalıdır. Güvenlik seviyeleri saldırı tespit yetenekleri de olan fiziksel yedekli güvenlik duvarları ile korunmalıdır. Bu güvenlik duvarları detayı şartnamede verilen Tip-2 güvenlik duvarı özelliklerini asgari olarak sağlamalıdır. Ana güvenlik seviyelerine bağlı alt güvenlik seviyeleri olabilir ve bunlar sanal olarak oluşturulabilir. Bu azami güvenlik şartlarını fiziksel, sanal ve mantıksal olarak sağlamak şartıyla daha üst çözümler sunulabilir.

Acil Durum Kontrol merkezinde en az 4 güvenlik seviyesi olacak şekilde ana güvenlik seviyeleri olmalıdır. Bu güvenlik seviyeleri fiziksel olarak yedekli çalışan anahtarlama sistemleri(switch) ile oluşturulmalıdır.Anahtarlama sistemine bağlanacak uç noktalar ilgili güvenlik seviyesi switchine bağlanmalıdır. Güvenlik seviyeleri saldırı tespit yetenekleri de

olan fiziksel yedekli güvenlik duvarları ile korunmalıdır. Bu güvenlik duvarları detayı şartnamede verilen Tip-1 güvenlik duvarı özelliklerini asgari olarak sağlamalıdır. Ana güvenlik seviyelerine bağlı alt güvenlik seviyeleri olabilir ve bunlar sanal olarak oluşturulabilir. Bu azami güvenlik şartlarını fiziksel, sanal ve mantıksal olarak sağlamak şartıyla daha üst çözümler sunulabilir.

EK-2.4. EPDK Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Referans Topoloji referans olarak düşünülmelidir, YÜKLENİCİnin en az bu çözümleri sunması beklenir. YÜKLENİCİ bu kapsamda belirleyeceği topolojiyi proje canlıya alınmadan önce ŞİRKETe sunacak ve onaylatacaktır.

Sistemin temel bileşenlerini içeren en içteki bölgedeki temel sistem: Gerçek Zamanlı İletişimci (COM) sunucuları, yönetici (ADM) veya HIS sunucuları ve güvenlik araçları. Bu bölge fiziksel olarak yedekli ağ anahtarlama cihazları ile oluşturulmalıdır.

Komşu ve ortak yardımcı programlarla iletişim kurmak için kullanılan ICCP sunucuları başka bir bölgededir. Bu bölge fiziksel olarak yedekli ağ anahtarlama cihazları ile oluşturulmalıdır.

Saha cihazlarıyla iletişim kuran Veri Toplama (Ön Uç) sunucuları üçüncü bir bölgededir. Örneğin, trafo merkezi denetleyicileri, RTU'lar ve saha aygıtları.

Kontrol odası operatörlerine erişim sağlayan UI (Kullanıcı Arabirimi) sunucuları ayrı bir bölgededir. Bu bölge fiziksel olarak yedekli ağ anahtarlama cihazları ile oluşturulmalıdır.

Kontrol merkezinin dışındaki kullanıcı arabirimi konsollarını destekleyen web sunucuları ayrı bir Askerden Arındırılmış Bölge (DMZ) içindedir. Bu bölge bir HIS sunucusu da içerebilir. Bu bölge fiziksel olarak yedekli ağ anahtarlama cihazları ile oluşturulmalıdır.

Kesinti Yönetim Sistemi (OMS) ayrı bir bölgede yapılandırılır.

Dış kullanıcı arabirimi konsolları (salt görüntüleme) ayrı bir bölgededir.

Uygulamalar bölgesi, dahili kullanıcılara erişim sağlayan UI sunucularını ve dahili kullanıcılara (yani kontrol odası operatörleri) erişim sağlayan HIS sunucularını içerir.

Operatör Eğitim Simülatörü ayrı bir bölgede bulunur.

Test Sistemleri ayrı bölgelerde yapılandırılmıştır.

Aşağıda siber güvenlikle ilgili SCADA/DMS/OMS'in gereksinimleri listelenmiştir.

10.5.2 Erişim Kontrolü

Sertifika Yetkilisi ve Dijital Sertifikalar

Dağıtılmış şebeke kontrol sistemi içinde güvenli veri alışverişi için dijital sertifikaları yönetmek üzere bir Sertifika Yetkilisi (CA) varlığı sağlanacaktır. CA'ya yalnızca sistem yöneticileri erişebilir.

Dijital sertifikalar, aşağıdaki hizmetlerin kimlik doğrulaması ve şifrelenmesi için kullanılacaktır:

Sunucular arasında işlemler arası iletişim,

Uzak iş ortağı sistemleri arasında veri alışverişi,

Kullanıcı arabirimi erişimi,

Veri tabanı erişimi,

Kimlik Doğrulama, Yetkilendirme ve Denetim

Sistem, bireysel kullanıcının kimliğini doğrulamak için bir kullanıcı adı ve şifre gerektirecektir. Oturum açma başarılı olursa, çoklu oturum açma sistemi konsola benzersiz (şifrelenmiş) bir belirteç atar. Bu belirteç, oturum sırasında kullanıcının ve konsolun yetkiye sahip olduğu hizmetlere erişmek için kullanılır. Jetonun süresi çıkış sırasında sona erer.

Kurumsal düzeyde çoklu oturum açma özelliğine sahip kullanıcıların, işletim sistemi kimlik doğrulaması oturum açma işlemini tamamladıktan sonra SCADA/DMS/OMS 'e doğrudan erişebilmeleri mümkün olacaktır. Çok faktörlü kimlik doğrulaması, en azından işletim sistemi oturumu için desteklenmelidir.

Sistem işletme ve destek aşamalarında ve ihtiyaç halinde uzaktan erişimlerde ŞİRKET'e ait Privileged Access Maangement (PAM) ürünü kullanılacaktır. Ürünlerin PAM ürünü ile entegrasyonunu ŞİRKET yerine getirecektir. YÜKLENİCİ eklenmesi gereken ürün üzerinde yapılması gereken ayarlamalar için ŞİRKET'e destek olacaktır.

Active Directory (AD) ile tümleştirme, tüm iş istasyonlarında etkileşimli erişim kimlik doğrulaması için isteğe bağlı olarak kullanılabilir.

Yönetici, kullanıcının hangi uygulamalara erişmesine izin verildiğini belirtebilir. SCADA/DMS/OMS, güvenlikle ilgili olayları günlüğe kaydeder.

Kullanıcı SCADA/DMS/OMS'e bağlandıktan sonra, kendi kendini denetleme amacıyla son başarılı oturum açma zamanını veya son başarısız oturum açma zamanını görüntüleyebilecektir.

Fiziksel Erişim Kontrolleri

SCADA/DMS/OMS fiziksel sunucularını korumak için kullanılmayan USB bağlantı noktalarının, CD/DVD'nin ve diğer kaldırma aygıtlarının veya medya aygıtlarının devre dışı bırakılması mümkün olacaktır.

SCADA/DMS/OMS sunucu BIOS'unu (Temel Giriş/Çıkış Sistemi) korumak için önlemler de sağlanacaktır.

SCADA/DMS/OMS Linux Kullanıcı Arabirimi istemci iş istasyonları için, operatörün iş istasyonu ortamını değiştirmesine izin vermemek için kısıtlayıcı bir ortam mevcut olacaktır (kiosk çalışma moduna benzer).

10.5.3 Şifreleme

SCADA/DMS/OMS'de, kimlik bilgileri gibi kullanıcı açısından hassas bilgileri korumak için gizliliğin gerekli olduğu durumlarda şifreleme kullanılacaktır. Ayrıca, kullanıcı arayüz konsolları ile değiş tokuş edilen verilerin gizliliğini sağlamak için de kullanılacaktır. Onlar ve SCADA/DMS/OMS arasındaki iletişim güvensiz ağlardan geçer. Bu nedenle, Kullanıcı Arayüzü HTTPS ve TLS şifreli iletişimi için AES kullanacaktır.

10.5.4 Anti-Virüs Yazılımı

- Teklif edilecek Antivirüs Yazılımını oluşturan tüm bileşenler aynı üreticiye ait tek bir ürün olacaktır. Aynı üreticiye dahi ait olsa farklı ürünlerin bir araya getirilmesinden oluşturulan bir çözüm olmayacaktır.
- Teklif edilecek Antivirüs Yazılımı fiziksel, sanal ve bulut ortamdaki sunucu sistemlerin güvenlik politikalarını tek bir noktadan yönetebilecek özellikte olacaktır.
- Teklif edilecek Antivirüs Yazılımı, Merkezi Yönetim Sistemi ve İşletim sistemi ajan uygulamalarından oluşacaktır.
- Teklif edilecek Antivirüs Yazılımı aşağıdaki işletim sistemi platformlarında çalışabilecektir:
  - Microsoft Windows
  - Red Hat Enterprise Linux
  - Centos
  - Oracle Linux
  - SUSE Linux
  - Ubuntu
  - Debian
  - Cloud Linux
  - Amazon Linux
- Teklif edilecek Antivirüs Yazılımı yüksek erişilebilir mimaride çalışmayı desteklemelidir.
- Teklif edilecek Antivirüs Yazılımı Merkezi Yönetim Sistemi Linux (Red Hat) ve Windows işletim sistemleri üzerinde çalışmayı destekleyecektir.
- Teklif edilecek Antivirüs Yazılımı Merkezi Yönetim Sistemi veri tabanı olarak Oracle, PostgreSQL ve Microsoft SQL Server ile çalışmayı destekleyecektir.
- Teklif edilecek Antivirüs Yazılımı üzerinde saldırı tespit ve önleme, güvenlik duvarı, zararlı yazılım önleme, web sitesi güvenilirliği, bütünlük gözleme, kütük inceleme ve uygulama kontrolü bileşenleri bulunacak, bu işlevlerle ilgili tüm bileşenler teklif edilecektir.
- Teklif edilecek Antivirüs Yazılımı üzerinde bulunacak saldırı tespit ve önleme bileşeni gelen ve giden trafiği tarayabilecek ve derin paket inceleme (DPI) çalışabilecek mimaride olacaktır.
- Teklif edilecek Antivirüs Yazılımı, sanal yama (host based IPS) özelliğini barındıracaktır. Sanal yama özelliği ile sunucular üzerinde bulunan ağ zafiyetleri tespit edilebilecek, isteğe bağlı olarak manuel ve otomatik olarak kapatılabilecektir.
- Teklif edilecek Antivirüs Yazılımı üzerinde bulunacak olan güvenlik duvarı, keşif taramalarını engelleme yeteneğine sahip olmalıdır. Bu güvenlik duvarı ile MAC, IP, Protokol, Port bazlı erişim kuralları uygulanabilecektir.
- Teklif edilecek Antivirüs Yazılımı üzerinde bulunacak bütünlük gözleme bileşeni kritik işletim sistemi dosyaları, dizinleri, kayıt defteri (registry) anahtar ve değerlerindeki değişiklikleri gerçek zamanlı izleyerek rapor edebilecek, alarm üretebilecektir.
- Teklif edilecek Antivirüs Yazılımı üzerinde bulunacak zararlı yazılım önleme bileşeni aynı üreticiye ait davranış tabanlı analiz motorunu kullanacaktır. Üçüncü taraf bir üreticiye ait motor kullanmayacaktır.
- Teklif edilecek Antivirüs Yazılımı üzerinde bulunacak kütük inceleme bileşeni çalıştığı işletim sistemi üzerindeki işletim sistemi ve uygulamalara ait günlük kayıtları ve kütükleri izleyerek şüpheli durumları rapor edebilecek, alarm üretebilecektir.

- Teklif edilecek Antivirüs Yazılımı uygulama kontrolü özelliği ile işletim sistemi üzerinde çalışan uygulamalarda beyaz liste ve kara liste oluşturabilecektir. Bu modül mevcut envanteri çıkarıp ona izin verecek ve sonrasındaki yeni gelen veya değişen uygulamaları bloklayabilecektir.
- Teklif edilecek Antivirüs Yazılımı sanal yama, kütük inceleme ve bütünlük gözleme bileşeni için sunucuda bir keşif taraması yaparak çalışan uygulama ve rollere göre otomatik olarak kurallar önerebilecektir. Böylece her sunucu için o sunucuya özgü bir kural setini otomatik olarak uygulayabilecektir.
- Teklif edilecek Antivirüs Yazılımı sanal yama özelliği ile sistemde bulunan zafiyetlerle ilgili gerekli güvenlik yamaları sisteme uygulanana kadar sistemi gelebilecek ağ seviyesinde saldırılara karşı koruma sağlayabilecektir.
- Teklif edilecek Antivirüs Yazılımı VMware NSX ile entegre çalışabilecektir ve sunucularda ajansız koruma sağlayabilecektir.
- Teklif edilecek Antivirüs Yazılımı üreticinin Global Tehdit İstihbarat hizmetine erişebilecek, bu hizmet sayesinde web sayfaları, elektronik posta kaynakları ve dosyalar için saygınlık sorguları yapabilecektir.
- Teklif edilecek Antivirüs Yazılımı “docker” içeren bir işletim sistemi içinde çalışan konteynerlar için antivirüs, IPS ve firewall korumasını destekleyecektir. Aynı işletim sistemi içindeki iki konteyner arasındaki trafiği inceleyebilecek ve atakları bloklayabilecektir.
- Teklif edilecek ve kurulumda kullanılacak işletim sistemlerinin hepsi bahsi geçen antivirus kurulumu yapılacaktır. Ayrıca ek olarak 8.1 YÜKLENİCİ sorumlulukları maddesinde belirtilen adet için lisanslar temin edilecektir.

10.5.5 Ağ İzleme ve Anomali Tespiti Sistemi

Çözüm Ağ saldırı tespit ve izleme yetenekleri olan ve detayı EPDK Siber Güvenlik Olgunluk Modelinde belirtilen ve aynalama yöntemi ile çalışan bir saldırı tespiti yazılımı ürününü de içermelidir. Bu izleme minimum olarak kontrol merkezi ve acil durum kontrol merkezi ağları ile kontrol merkezlerinin uç sahalarla WAN haberleşmelerini de kapsamalıdır. Çözüm fiziksel donanım veya sanallaştırma desteği olan bir ürün olabileceği gibi her ikisinden oluşan entegre bir gönderici ve analizci fonksiyonlarından oluşan bir çözüm olabilir.

Bu ürün toplamda en az 1000 IP adresi için belirleme ve kontrol edecek şekilde lisanslanmalıdır.

Ürün özellik ve yetenek detayları aşağıda verilmiştir.

- Önerilen çözüm, ICS networkünü öğrenip anlayabilmek için Makine Öğrenimi ve Yapay Zekayı kullanma yeteneği olacak
- Önerilen çözüm, 'gerçek zamanlı' ağ izleme gerçekleştirecek ve oluşan eventleri, alarmları ve bildirimleri gösteriyor olabilecek
- Önerilen Ağ izleme ve anomali tespiti çözümü kimlik doğrulama yenilgisi (authentication defeat (Brute force attack)) ve bilgi hırsızlığı (information theft (Application Scanning)) gibi non-vulnerability tabanlı atakları tespit edebilme yeteneğine sahip olacaktır
- Temel Ağ izleme ve anomali tespiti gereksinimleri şunlardır:

- Anomali tespiti
- Ağ görselleştirme
- Varlık envanter yönetimi
- Zaafiyet değerlendirmesi
- Hibrit ICS tehdit algılama (imza tabanlı + davranış tabanlı anomali tespiti)
- Raporlama

- Önerilen çözüm, sistem yöneticilerine esnek bir dashboard sunacaktır.
- Önerilen çözüm, anormal veya kötü amaçlı bir olay tespit ettiğinde sistem yöneticisine birden fazla formatta uyarı sunacaktır.
- Çözüm, zaman zaman meydana gelen benzer aktiviteleri keşfetmek için "pattern discovery" yeteneği sağlamalıdır. (Örneğin: Slow-and-low Attack)
- Önerilen çözüm güvenlik alertleri/bildirimleri ve event verilerini mail yolu ile ya da syslog gibi external uygulama üzerine gönderebiliyor olmalıdır.
- Önerilen Çözüm, etkin olay işlemeyi sağlamaya yardımcı olmak için ilgili ekibin müdahalesine hızlı bir şekilde öncelik vermesini sağlayan bilgileri içermeli ve ilişkilendirmelidir.
- Önerilen çözüm, müşterinin mevcut ve gelecekteki büyüme gereksinimlerini karşılamak için çok katmanlı desteğe ve esnek bir ölçeklenebilir mimariye sahip olacaktır.
- Önerilen çözüm, insan müdahalesine gerek kalmadan tüm bileşenleri (yeni ürün sürümleri ve içerik güncellemeleri) otomatik olarak güncelleyebilen ölçeklenebilir bir mimariye sahip olacaktır.
- Önerilen çözüm, belirli ağ segmentindeki varlıkların otomatik olarak keşfedilmesini ve sınıflandırılmasını destekleyebilmelidir.
- Önerilen Çözüm, farklı kullanıcı gruplarına özgü farklı raporlara ve kaynaklara erişmesi için güvenli rol tabanlı erişim sağlanabilecektir.
- Önerilen çözüm, esnek raporlama ve dashboard ekranı sunabilmelidir.
- Önerilen çözüm, gerçek zamanlı dashboard ekranından event listesi özelliğine kadar detaylı inceleme olanağı sunmalıdır
- Önerilen çözüm, operatörün veri ve raporları çoklu formatlarda oluşturmasına ve dışa aktarmasına ve bu raporları ve verileri sırasıyla yazdırmasına izin verecektir. Formatlar şunları içerecektir; .CSV .XLS
- Önerilen çözüm, izlenen endüstriyel ağa 'Pasif' bir şekilde bağlanacaktır. Ağ TAP'leri veya endüstriyel ağ anahtarlarındaki Mirror/Span portları aracılığıyla izlenen endüstriyel ağa bağlanabilecektir.
- Önerilen çözüm, Ethernet IP, SNMPv1, SNMPv2, SNMPv3, SSH, WMI, WinRM, CB Defense, Modicon Modbus, SEL, Aruba Clearpass, Cisco ISE, ServiceNow ve DNS Reverse Lookup aracılığıyla varlık bilgilerini elde etmek için aktif bir moda sahip olacaktır.
- Önerilen çözüm, platformun 'desteklenen protokoller' listesinde görünen kullanılan tüm ağ protokollerini otomatik olarak tanımlayacak ve kullanılmayan protokolleri sürekli olarak izleyecektir.
- Dağıtılmış Mimari

  Tüm bileşenler ölçeklenebilir olmalı ve katmanlı bir mimari sağlayarak zaman içinde büyümeye izin vermelidir.

- Ölçeklenebilirlik.
    a. Tüm bileşenler ölçeklenebilir olmalıdır. AĞ IZLEME VE ANOMALI TESPITI ÇÖZÜMÜ sensörü, fiziksel cihazlarda, ortak hipervizör ortamlarındaki Sanal Makinelerde ve bir anahtar Docker/Container mimarisinin bir parçası olarak desteklenecektir."
    b. Merkezi Yönetim Konsolu bileşeni, fiziksel cihazlarda, Sanal Makinelerde ortak hypervisor ortamlarında ve Microsoft Azure ve Amazon AWS örneklerinin bir parçası olarak desteklenecektir
    c. Çözüm, uzak konumlardan veri yakalamak için düşük hesaplamalı fiziksel veya sanal bir cihaza sahip olmalıdır."
- Veri Gizliliği ve Bütünlüğü

  Duran ve hareket halindeki veriler güvenli ve emniyetli bir şekilde işlenecek ve bu nedenle şifreleme kullanılacaktır.

- Platform Esnekliği

  Önerilen çözüm hem fiziksel hem de sanal platform formatlarında sunularak esnek bir çözüm sunacaktır.

- Dinamik Ağ Öğrenimi
    a. Önerilen Endüstriyel AĞ IZLEME VE ANOMALI TESPITI ÇÖZÜMÜ çözümü, öğrenme döngüsünün sonunda manuel müdahale olmaksızın öğrenme modundan koruma moduna dinamik olarak geçebilecektir."
        i. Ayrıca önerilen çözüm, yeni bir öğrenme aşamasına girmeye gerek kalmadan öğrenilen verilerin güncellenebilmesini sağlayacaktır.
        ii. Ayrıca, önerilen çözüm, endüstriyel ağ ortamının farklı alanları aynı anda hem öğrenme hem de koruma aşamasında olacak şekilde, endüstriyel ağ ortamını öğrenmeye 'aşamalı' bir yaklaşıma sahip olma yeteneği sağlayacaktır.
- Anomali tespiti
    a. Önerilen çözüm, 'sıfır gün' saldırılarını tespit etmek için irregularity tabanli algılama sağlayacaktır."
    b. Önerilen çözüm, şüpheli davranışlarla ilgili varlık profili raporlamasına dayalı olarak OT ve IoT varlık davranışlarını tespit etme yeteneği sağlayacaktır."

    c. Önerilen Çözüm, ayrıntılı bir anormallik tabanlı yaklaşım sağlama yeteneği sağlayacaktır, bu nedenle baseline üzerinden sapmalar tespit edilecek ve uyarılacaktır."
- OSI Model Desteği

  Önerilen çözüm, OSI Ağ Oluşturma Modelinin tüm 7 katmanını anlayacak ve OSI katmanlarındaki sorunlar için uyarılar sağlayacaktır.

- Protokol Kapsamı -IEC-60870-5-104, IEC-61850, Modbus, DNP3, Ethernet/IP
- İmza eşleştirme kuralları/tetikleyicileri -Önerilen çözüm, aşağıdakileri kullanma ve/veya birleştirme yeteneğine sahip olacaktır:
    a. Anormal ve kötü niyetli davranışların imzalarını tetiklemek için ağ trafiği/paket eşleştirme kuralları

b. Bilinen kötü amaçlı içeriğin imzalarını tetiklemek için Yük/Veri içerik kalıbı eşleştirme kuralları
c. Belirli kullanım durumları ve senaryolarında tetiklemek için müşteri tarafından tasarlanan özel kurallar

- Riske Dayalı Uyarı- Algılanan uyarılar, tehdit etkisine veya risk derecesine göre kategorilere ayrılmalıdır.
- Saldırı Anatomisi- Uyarı sistemi, ilgili uyarıları tek bir olayda toplama yeteneğine sahip olacaktır. (Attack Flow Aggregation)
- Hibrit ICS Tehdit Tespiti-

  Önerilen çözüm, protokolün kötüye kullanılması, kötü amaçlı yazılım iletişimi, tünel açma girişiminin yanı sıra izinsiz giriş ve bilgisayar korsanlığı girişimleriyle sınırlı olmayan tüm kötü niyetli ve anormal faaliyetleri tespit edecektir.

- Endüstriyel Ağ Bütünlüğü-

  Sistem, yanlış yapılandırmaları belirtmek için alt ağ çakışmalarını tanıyacak ve alt ağları tanımak/düzenlemek için kullanılacaktır.

- Tehdit Avcılığı ve Öğrenme Doğrulaması-

  Sistem, öğrenme aşamasının sonunda makul sorunları / hatalı verileri 'kısa listeye alma' yeteneğine sahip olacaktır

- Sistem Birlikte Çalışabilirliği-

  Sistem, çözümden tüm bilgileri (varlıklar, kayıtlı konuşma, temel vb.) dışarıya çıkarmak için API ve sorgu motoru arasında tek bir sorgu dili sağlayan RESTful OpenAPI'yi içerecektir.

- Kullanım kolaylığı-

  Sistem, Pano, Grafikler, Trendler ile tehditlerin özeti, uyarılar vb. gibi formatlar sunarak tüm tehditleri ve sistem izlemeyi basit ve anlaşılır bir biçimde sunabilmelidir,

- Yetkisiz Erişim-

  Sistem, ICS ağına bağlı bilgisayar/dizüstü bilgisayar/mobil cihaz vb. aracılığıyla herhangi bir yetkisiz giriş veya sızma girişimini tespit edecek ve gösterge panosunda bir uyarı oluşturacaktır.

- Sistem Bütünlüğü-

  Sistem erişimi ve yönetiminin tam denetim izi alınır.

- Varlık Keşfi-

a. Sistem, aşağıdakiler dahil olmak üzere otomatik varlık envanteri keşfini destekleyecektir:
    i. Varlık türü ve rolüyle ilgili ayrıntılar
    ii. Varlığı zone veya protokole göre gruplama yeteneği

- Varlık Değişim Yönetimi-

  Sistem, envanter değişikliklerini tespit edecek ve uyaracaktır.

- Varlık Yönetimi-

  Sistem, yaşam döngüsü boyunca her bir varlık için sınıflandırma bilgilerini depolayabilecek ve sürdürebilecektir.

- Environment Değişikliği Yönetimi-

  Sistem, ağ yapılandırmasındaki değişiklikler ve sapmalar için geçmiş zaman çizelgesinde iki tam sistem anlık görüntüsünü (ağ görselleştirme, varlık envanteri, sistem süreçleri vb.) karşılaştırabilecektir.

- Üçüncü Taraf"" Sistem Entegrasyonu-
    a. Sistem, diğer sistem ve araçlarla entegrasyona izin verebilecektir:
        i. Security Information and Event Monitoring (SIEM) systems and Threat Management Platforms (TMP).
        ii. Industrial Firewalls.
        iii. Automation Applications (Configuration Files.)
        iv. Other 'Third Party' solutions and platforms via an Open API. (Such as Asset Management Database or Incident Ticketing and Mitigation Workflow platform.)
- Pasif Güvenlik Açığı Değerlendirmesi-

  Endüstriyel AĞ IZLEME VE ANOMALI TESPITI ÇÖZÜMÜ çözümü, National Grid'in ICS ağ ortamında bulunan sistemler ve cihazlar hakkında yayınlanmış güvenlik açığı verilerini sunabilecektir, bu bilgiler müdahaleci olmayan bir şekilde ve ağ cihazı taramaları (yani NMAP) gerçekleştirilmeden toplanacaktır.

- Aktif Güvenlik Açığı Değerlendirmesi-

  Endüstriyel AĞ IZLEME VE ANOMALI TESPITI ÇÖZÜMÜ çözümü, pasif yaklaşımla toplanan verileri geliştirmek için National Grid'in ICS ağ ortamında bulunan sistemler ve cihazlar hakkında yayınlanmış güvenlik açığı verilerini sunabilecektir. Veri toplamak ve cihazlarda kesinti ve yavaşlık uygulamayacak

10.5.6 Arayüzler (Harici)

ICCP alt sistemi, uluslararası IEC standartlarına dayanan güçlü kimlik doğrulama ve şifreleme kullanarak güvenli uzak varlıklarla veri alışverişini desteklemelidir.

Güvenli ICCP kimlik doğrulama ve şifrelemesi, dijital sertifikalar ve Transport Layer Security (TLS) protokolü kullanılarak desteklenmelidir.

10.6 SCADA/DMS/OMS Yazılımı

SCADA/DMS/OMS çözümü, dağıtık bilgisayarlarda kurulu modüller arasındaki veri yönetimi, veri değişimi ve iletişimi için kullanılan çeşitli genel hizmetler ve sistemleri içerir.

10.6.1 İşletim sistemi

1) SCADA/DMS/OMS, anahtar POSIX standartlarına uyumlu olan ve bağımsızlığı destekleyen, doğal 64 bit mimariye sahip yaygın bir işletim sistemi temeline dayanmaktadır. Tercih edilen işletim sistemleri Redhat Enterprise Linux (RHEL) ve Windows Server'dir.
2) İş istasyonlarının RHEL veya Microsoft Windows üzerinde çalıştırılabilmesi ve 5 yıl süresince end of life olmayacak ve YÜKLENİCİ tarafından 10 sene destek taahhüttü verilebilecek işletim sistemi kurulmalıdır.

10.6.2 Çoklu Bilgisayar Yönetimi

Dağıtık bilgisayarlar arasındaki iletişimi yönetecek, bir arıza durumunda operasyonu etkilenmemesi için donanım ve yazılım yedekliliği, çoklu bilgisayar koordinasyonu ve sistem durumu izleme gibi çeşitli hizmetler sunacaktır.

1) Genel Bakış

SCADA/DMS/OMS bir Local Area Network (LAN) üzerinde çalışacak sistemi, genel sistem durumunu kontrol edip, yüksek düzeyde denetim ve güvenilirliği desteklemek için, şunları sağlayacaktır:

a) İşletim Sistemi desteği,
b) Sunucu İşletim Modları ve Bilgisayar Durumları,
c) Farklı amaçlar için yedeklilik stratejileri,
d) Veri tabanı Senkronizasyonu ve Yedekleme,
e) Yazılım Sistem İzleme, hata tespiti ve otomatik kurtarma,
f) Tarih ve Saat Güncelleme ve Senkronizasyonu,
g) LAN İzleme,
h) SNMP tabanlı cihaz izleme,

2) Yedeklilik

SCADA/DMS/OMS sistemi, Kontrol Merkezleri Arası yedekliliğin haricinde, kontrol merkezi içerisinde sunucu yedekliliğine sahip olmalıdır. Talep edilen yedeklilik mimarileri:

a) LAN Yedekliliği:

Sistemde kullanılacak donanımlarda, yedekli LAN bağlantıları ile NIC Teaming yapılacaktır. NIC teaming, bir bağlantı hatası olduğunda bunu algılayıp ve otomatik olarak takımı yedek bağlantıya geçiş yapmalıdır. Sistemde bu geçiş sırasında herhangi bir fonksiyon kaybı yaşanmamalıdır.

b) Hot Standby Yedeklilik:

Bu yöntem, tek bir amaç için özel olarak ayrılmış iki sunucu gerektirir:

I. PC durumunda bir aktif sunucu ve bekleme durumundaki (SB) ikinci bir pasif sunucu bulunmalıdır.
II. PC ve SB sunucuları paralel olarak işlem yapmalıdır.
III. SB sunucuları PC ile aynı bilgileri alıp, ancak sadece PC veri ve komutları iletimi yapmamalıdır (her iki sunucu da kullanılan heartbeat veya life-check sinyallerini iletir).
IV. Çalışma durumunda SB sunucusu PC sunucusundan güncellenmelidir.
V. Her iki sunucu da arızaları tespit etmek için kullandığı heartbeat mesajlarını iletmelidir.
VI. SB sunucusu, PC'deki bir arıza tespit ettiğinde online işlem kontrolünü devralmalıdır.
VII. Otomatik bir yedekleme için operatör müdahalesi gerekmemelidir.
VIII. Hot Standby yapısında, SB sunucusu sürekli olarak güncellendiği için, veri kaybı olmadan yedekleme kısa süre içinde gerçekleştirmelidir.

c) Spare Yedeklilik:

Spare yedeklilikte, Hot Standby gibi aktif-aktif çalışma beklenmemektedir. Sunucular birbirinin soğuk yedeği olmalı ve ana sunucu arızalandığında, en fazla 5 dakika içerisinde yedek sunucu bütün fonksiyonel görevi üzerine almalıdır. Bu süreçte gerçek zamanlı SCADA operasyonları etkilenmemelidir.

d) Veri tabanı Yedekliliği:

YÜKLENİCİ yedekli senkron veri tabanı çözümü sağlayacaktır. Veri tabanı sunucularından bir tanesi arızalı duruma geçtiğinde diğer sunucu üzerinden en geç 10 saniye içerisinde tüm SCADA/DMS/OMS fonksiyonları çalışmaya devam edecektir. Sağlanacak veri tabanı çözümü backup/restore uygulamalarıyla uyumlu olacaktır.

3) Veri Tabanı Güvenlik Özellikleri

Aşağıdaki veri tabanı güvenlik özellikleri sağlanacaktır:

a) Güvenlik yamalarının veya büyük yazılım güncellemelerini sistemde minimum kesinti süresiyle yapmalıdır.

b) SCADA/DMS/OMS uygulamaları, veri tabanı şifrelerinin kolay bakımı ve yönetimi için şifrelenmiş bir şifre dosyası kullanarak veri tabanına giriş yapacaktır. Bu işlem, güvenlik için gereken şifre değişikliklerinin kolayca yapılmasını sağlayacaktır.

c) Kullanıcı etkinliğinin denetlenmesi ve değişikliklerinin denetlenmesi, güvenlik yönlerinin izlenmesine ve geçersiz giriş denemelerinin kolayca tespit edilmesine ve herhangi bir kullanıcının yaptığı değişikliklerinin takibine olanak tanıyacaktır. Kullanıcılarının eklenmesi veya kaldırılması, ayrıcalıkları ve rolleri gibi herhangi bir değişikliğin izlenmesi mümkün olacaktır.

d) Kullanıcı parola değişiklikleri için veri tabanı parola karmaşıklık kuralları uygulanmalıdır.

4) Yazılım Sistem İzleme

Sorunsuz sistem işletimi için, sistem ve modülleri sürekli olarak izlenmelidir. Bu izlenme sonuçları çeşitli ekranlar ile kullanıcılar tarafından takip edilebilir olmalıdır.

5) Hata Tespiti ve Otomatik Kurtarma

a) SCADA/DMS/OMS yazılımı, hatalı durumları mümkün olan en erken zamanda tanımalıdır. Tüm fonksiyon (alt program) çağrıları, bir hata bayrağı olarak çağıran programa döndürülecek bir hata kodu ile sonuçlandırılmalıdır. Bir hata değerlendirme alt sistemi, bu hata bayraklarını değerlendirecektir.

b) Hata İzleme

Yazılım izleme sistemi, hata izleme fonksiyonu ile tüm hataları bildirecek ve cevap verecektir. Hata değerlendirme alt sistemi bu hataları değerlendirecektir. Veri ve sistem testi aşamalarında hata sistemi devre dışı bırakılabilir. Hata sistemi devre dışı bırakıldığında hatalar bildirilir ancak herhangi bir yanıt üretmemelidir Üretim işlemi sırasında, sistem belirli hatalara otomatik olarak tepki vermelidir.

c) Hata Sınıflandırması

SCADA/DMS/OMS hata mesajları kaynak ve kritiklik seviyesine (hata sınıfı) göre sınıflandırılacaktır. Her hata seviyesi, atanan bir hata ağırlık faktörüne sahip olacak ve önceden tanımlanmış bir tepkiye neden olacaktır. Hataların belirli sınıflara atanması projeye özel olarak tanımlanabilir.

6) Tarih ve Saat Güncelleme ve Senkronizasyonu

1) SCADA/DMS/OMS, bir saat cihazı içermelidir. Bu cihaz, Ağ Zaman Protokolü (NTP) kullanarak sistemin geri kalanını zamanlayabilmelidir.
2) Sistemdeki her sunucu, periyodik olarak saati almak ve zamanını NTP sunucusundaki zamana senkronize etmek için bir NTP istemcisi çalıştırmalıdır. NTP, bir grup zaman sunucusundan en iyi zamanı belirlemek ve buna göre senkronize olmaya çalışmak için algoritmalar kullanmalıdır. Ayrıca, yerel sunucunun saat kaymasını izleyecektir. Eğer

zaman sunucusu mevcut değilse, bu bilgiyi kullanarak yerel sistem saatinin düzeltilmesi gerekmektedir. Bu, sunucunun bu tür düzeltmeler olmadan çok daha iyi zaman tutabilmesine olanak tanır. NTP, yerel LAN' da birkaç milisaniye senkronizasyon sağlayabilir.

3) Senkronizasyon işlemi, evrensel koordineli zaman (UTC) uygulayarak, zaman kaymalarından (örneğin, yaz saati uygulamalarından) etkilenmeyecektir. Tarih veya saat yalnızca gösterildiğinde yerelleştirilecektir.
4) SCADA/DMS/OMS, NTP zaman senkronizasyonunun durumunu izleyecek ve NTP sunucusu devre dışı kalırsa veya istemci herhangi bir nedenle zamanını senkronize edemezse hataları raporlayacaktır.

7) LAN İzleme

LAN izlemesi, SCADA/DMS/OMS'nin life-check ve hata teşhisi için gereklidir. Heartbeat mesajları, LAN durumlarını izlemek için kullanılacaktır. İzleme süresi dolmadan heartbeat alınamazsa bağlantı kapatılacaktır.

7) SNMP Tabanlı Cihaz İzleme

1) Basit Ağ Yönetim Protokolü (SNMP), ağdaki cihazlarla etkileşim ve izleme için kullanılacaktır. Sistem, SNMP kullanarak ağdaki bilgileri görüntüleyecek ve raporlayacaktır. SNMP, cihazlardan (örneğin, sunucular, anahtarlar ve yazıcılar) bilgi toplayacak ve verileri SCADA alt sistemi içine gönderecektir. Cihazlar, IP adresi veya ağ cihazının adı ve bir Nesne Tanımlayıcısı (OID) değerleriyle tanımlanır. SNMP arayüzü, değerleri ilgili SCADA işleme birimlerine iletecektir. SCADA sistemi mesajları ve değerleri işleyecek ve verileri kullanıcı arayüzüne gönderecektir.
2) SNMP arabirimi aşağıdakileri sağlamalıdır:

a) Çalıştırma sonrası tüm cihazlardan genel sorgu.
b) Cihaza özgü OID sorgu döngüsüne göre periyodik raporlama.
c) Denetlenen cihazlardaki ajan örnekleri tarafından gönderilen sonucu işleme.

10.6.3 Veri Tabanı sistemi

1) SCADA/DMS/OMS, aşağıdaki gibi çeşitli veri tabanı sistemlerini kullanır;

a) Gerçek zamanlı işlemler için ilişkisel bir Gerçek Zamanlı Veri tabanı (RTDB).
b) Veri Mühendisliği Uygulaması tarafından yönetilen model tanımları ve mühendislik verileri için veri tabanı sistemi,
c) Ağ Uygulamaları ve Tarihsel Bilgi Sistemleri (HIS) gibi belirli uygulamalar için bir dizi veri tabanı.

2) SCADA/DMS/OMS veri tabanı sisteminin başlıca özellikleri şunlar olmalıdır:

a) Standart İlişkisel Veri tabanı Yönetim Sistemi (RDBMS) kullanılarak, fiziksel veri depolama, gerçekleştirilecektir. Ortak Bilgi Modeli (CIM) formatında import/export edilebilen bir mühendislik veri tabanı ileriki süreçte uyum sağlayabilmelidir.

b) İşlem verileri ve uygulama verileri içeren Gerçek Zamanlı Veri tabanı (RTDB) aşağıdaki özelliklere sahip olacaktır:

c) Yayılmış sistemde veri tutarlılığının sağlanması,

d) Saniyeler içinde (aktif bekleme) veri tabanlarının yedeklenmesi,

e) Tüm paylaşılan yönetim sistem verileri için ortak veri modeli,

3) Gerçek Zamanlı Veri tabanı (RTDB)

a) Sistem, ölçülmüş veri, hesaplanmış veri, durum verisi, ağ konfigürasyonu gibi gerçek zamanlı veriyi depolamak için yüksek performanslı gerçek zaman veri tabanına sahip olacaktır.
b) Gerçek zamanlı veri tabanı, veri tabanı düzenleme, değiştirme, bakımı ve konfigürasyonu için araçlara ve kullanıcı kılavuzuna sahip olacaktır.
c) Sistem, gerçek zamanlı veriyi farklı dosya formatları halinde harici sistemlere aktarabilecektir.
d) Veri tabanının tüm kullanıcı adı ve şifreleri ile ilgili tablo ve kolon yapılarının detayları ŞİRKET ile paylaşılacaktır.

10.6.4 Simülasyon Özelliği

SCADA/DMS sistemi şebeke modeli üzerinden DMS fonksiyonlarını test etme, canlı sistemi etkilemeden şebeke modeli üzerinde değişiklikler yaparak çalışmalar yapmasına imkan sağlamak için simülasyon özelliği sunacaktır.

10.7 Veri Yönetimi

10.7.1 Canlı İstasyon Veri Mühendisliği Uygulaması

6) Canlı İstasyon Veri Mühendisliği Uygulaması, Kullanıcının merkezi bir veri tabanında dağıtım şebekesine ilişkin tüm mühendislik verilerini verimli bir şekilde girmesine ve bakımını yapmasına olanak tanımalıdır. Güç sistemi kaynaklarını, ilişkileriyle birlikte nesne sınıfları ve nitelikleri olarak temsil etmenin standart bir yolunu sağlamalıdır. Şebeke yönetiminde kullanılan mühendislik verileri aşağıdaki veri türlerinden oluşmalıdır:

a) Şebeke Veriler

b) Ekipman, ölçümler, topoloji ve istasyon tek hat ekranları dahil.

c) Konfigürasyon Verileri

d) Donanım ve yazılım uygulama yapılandırması.
e) Bu şebeke veri modelini yönetirken, bu işe uygun olarak geliştirilmiş editörlerin sistemde bulunması ve kullanılması mümkün olmalıdır.

7) Canlı İstasyon Veri Mühendisliği Uygulaması aşağıdaki temel özelliklere sahip olmalıdır:

a) CIM Modeli kullanılması durumunda import/export desteği sağlamalıdır.

b) Kullanıcı, hangi veri değişikliklerin yapıldığını kontrol altında tutabilecektir. Birden fazla işin oluşturulabilmesi ve aynı anda var olabilmesi mümkün olmalıdır.

c) Veri Mühendisliği Uygulaması operasyonel veri tabanını etkilemeden, güvenli bir ortamda aynı anda birden fazla kullanıcının veriyi değiştirmesine izin verecektir.

d) İş Kilidi, birden fazla kullanıcının aynı veri parçasını değiştirmesini ve böylece birbirlerinin üzerine yazmasını önlemelidir. İş Kilidi, çalışılan alanda mümkün olan en küçük şebeke unsuruna ait kilitlemeyi gerçekleştirmelidir.

e) Veri Mühendisliği Uygulaması veri değişiklikleri için yaşam döngüsü yönetimi sağlamalıdır.

f) Veri Mühendisliği Uygulaması kullanıcıların herhangi bir zamanda yaptıkları tüm değişikliklerin denetimini yapılmasına olanak sağlayacak şekilde denetim sağlamalıdır.

g) Veri Mühendisliği Uygulaması işlem kontrolünü kesintiye uğratmadan işletme sistemi üzerindeki artımlı veri değişikliklerinin çevrimiçi olarak aktarılmasını sağlamalıdır ve değişikliklerin geri alınmasına da benzer şekilde olanak sağlamalıdır.

h) Kullanıcı yetkilendirmesi, kullanıcı ve Veri Mühendisliği Uygulaması konsolu erişim hakları ve seviyeleri gibi çok düzeyli güvenlik hizmeti sağlanmalıdır.

i) Sistemdeki verilerde yapılan her değişikliğin denetim kayıtları tutulmalıdır. Kullanıcı-job-log kaydı eşleşmesine uygun yapıda olmalıdır.

j) Modelin bütünlüğünü sağlamak için doğrulama metotları kullanılmalıdır.

k) Tüm veri mühendisliği alanlarını kapsayan veri girişleri için bir kullanıcı arayüzü sunmalıdır.

l) Veri Mühendisliği Uygulaması çoklu ekran ve çoklu pencere veri girişi oturumları sağlamalıdır.

m) Çevrimiçi yardım sunmalıdır.

10.7.2 CBS'den Gelen Veriler için Veri Mühendisliği Uygulaması

1) Sistem CBS' den gelen verilerin için düzenlenmesi, yeni veri eklenmesi ya da silinmesi için veri mühendisliği uygulaması sağlayacaktır.
2) Bir nesne için veri girişi, birden fazla kullanıcının belirli bir değer üzerinde birbiriyle çakışan eylemlere neden olmamalarını sağlayacak şekilde sınırlandırılacaktır. Bir nesnenin bir kullanıcının kontrolü altında olması durumunda, başka bir kullanıcı tarafından bu nesne için veri girişi fonksiyonunu başlatma girişimi, ikinci veri girişi moduna girme teşebbüsünün reddedilmesine neden olacak ve çakışma, diğer kullanıcıya bildirilecektir.
3) Düzenleyiciler her katmanda aynı zamanda en az üç operatörün şebekenin farklı bölümlerinde veri girişi yapmasına izin verecektir.

10.8 Uç Nokta Haberleşme Arayüzü

10.8.1 Özellik

Uç nokta haberleşme arayüzü farklı üreticilere ait Uzak Terminal Birimlerinin (RTU'lar) SCADA/DMS/OMS'e bağlamak için kullanılacak sunucu tabanlı bir arayüzüdür.

1) SCADA/DMS/OMS'e sisteminin bütünleşik parçası olmalıdır.
2) Haberleşme sisteminin veri modellemesi Veri Mühendisliği Uygulaması üzerinden yapılacaktır.
3) Yüksek esnekliğe sahip olacaktır. Genişletilebilir olacaktır. Genişleme için ek lisans bedeli talep edilmemelidir.
4) Yük paylaşımı ile yedekli çalışan sunucu çiftleri olacaktır.

10.8.2 İletişim Protokolleri

1) Aşağıdaki iletişim protokolleriyle uyumlu RTU tipleri için birlikte çalışabilirlik sağlanmalıdır:

   a) IEC 60870-5-104 (Client Server functionality) Secured

2) Tüm iletişim protokolü modülleri sahada kanıtlanmış olmalı ve birçok kurulumda başarıyla çalışmalıdır. İzleme ve dinleme modları (protokole özgü) dahil olmak üzere kapsamlı iletişim tanılama yeteneği mevcut olmalıdır.

10.8.3 İletişim Hizmetleri

Yazılım paketi protokollere özgü tüm iletişim prosedürlerini yerine getirecektir. Ayrıca, her protokol için iletişim prosedürü için tüm özel işlevleri yerine getirecektir.

10.8.4 Eksiksizlik ve Güncelleme Kontrolü

1) Verileri tutarlı ve güncel tutmak için, uzaktan iletilen bilgilere bir eksiksizlik kontrolü uygulanmalıdır.
2) Eksiksizlik kontrolü, Genel Sorgulama (GI) komutunu takip edecektir. Bu komutu RTU'lara gönderecektir.
3) Bu komutun, bir sistem bileşeninin çalıştırılmasından sonra, zamanlayıcı kontrollü veya operatör müdahalesiyle manuel olarak verilmesi mümkün olacaktır.
4) GI sonlandırıldıktan veya GI zamanlayıcısının süresi dolduktan sonra, verilerin eksiksizliğini kontrol edecektir. GI tam değilse, tekrarlanmalıdır (yapılandırılabilir).
5) Tekrarlanan denemelerden sonra GI eksik kalırsa, bir alarm mesajı oluşturulmalı ve operatöre bildirilecektir.
6) Kullanıcı, kullanıcı arayüzünden tüm RTU'lar için bir GI verebilir olacaktır.

10.8.5 Veri Ön İşleme

Sahadan SCADA sunucularına gereksiz veri akışını önlemek ve bunları rutin işlemeden kurtarmak için, aşağıdaki ön işleme işlevleri bulunmalıdır:

1) Kendiliğinden iletilen durumlar ve ölçümler için eski-yeni karşılaştırma yapılmalı,
2) Çift kutuplu bilgi için ara durum bastırma yapılabilecek; her veri noktası için ayrı ayrı yapılandırılabilecektir. Ayrıca, hata durumuyla (11) kullanım için de yapılandırılabilir olmalıdır.
3) Analog değerlerin eşik kontrolü (entegrasyon yöntemi),
4) Analog değerlerin sıfır noktası bastırılması (ihmal edilebilir değerler sıfıra zorlanır),
5) RTU'lardan alınan sayaç okumaları (veya IEC terminolojisinde Entegre Toplamlar), protokole özgü formattan SCADA/DMS/OMS dahili işleme ve sunumuna dönüştürülmelidir.
6) Olayların sırası (SOE) nesne başına ayrı ayrı işlenmelidir.
7) Sinyal durumunun tersine çevrildiği dijital değerlerin tersine çevrilmesi. Çift kutuplu bir nesne 00 ve 11'i tersine çevirmemelidir. Kullanıcı, bir nesne için hem monitör hem de komut yönünde bireysel olarak ayarlayabilecektir.
8) IEC104 protokolü için: Tüm türler için kötü kalite bastırma özelliği bulunmalıdır. Bu özellik, her RTU için veya her veri noktası için ayrı ayrı yapılandırılabilir olmalıdır.
9) Zaman bilgisinin değer ile iletilmemesi durumunda Zaman Damgası özelliği kullanılabilir olmalıdır. Bu özelliğin çözünürlüğü 10 milisaniye olmalıdır.
10) Telemetri ile iletilen zaman damgasının çözünürlüğü 1 milisaniye aralığında olmalıdır. (Bu özellik RTU ve protokol türüne bağlıdır).
11) IEC için iletişim istatistikleri bulunmalıdır.

10.8.6 Yüksek Kullanılabilirlik

1) İlgili bileşen son derece kritik bir sistem bileşenidir ve bu nedenle en yüksek kullanılabilirliğe sahip olacak şekilde tasarlanmalıdır.
2) Yüksek kullanılabilirliği şu şekilde sağlanacaktır:

   a) Etkin sunucu hatası durumunda yedek sunucu yük devretme,

   b) Uç nokta haberleşme sunucusu çifti yedekliliği

3) Her bir sunucu çifti (yedekli sunucular) için, her iki sunucu da etkin durumda olacaktır. Yedek iletişim hatları bulunması durumunda sunucular arasında veya aynı sunucudaki hatlar arasında kanal seviyesinde geçiş yapılabilecektir.
4) İstenilen RTU grupları için haberleşme durdurulabilir ve başlatılabilir olacaktır.
5) Hat seviyesinde veya sunucular arasında geçiş, aşağıdaki gibi tetiklenebilecektir:

   a) Elle

   b) Etkin bir arabirimi engelleyen bir hattın değiştirilmesi (devre dışı bırakılması),

c) Hat yedekliliği durumunda etkin bir bağlantıyı engelleyerek bir RTU'nun değiştirilmesi (protokole özgü),

d) Otomatik olarak

e) Bir bağlantı arızası algılandıktan sonra tek bir RTU'nun değiştirilmesi,

f) Bir arayüz arızasının algılanmasından sonra tüm hattın değiştirilmesi,

g) Bir sunucu hatası üzerine geçiş,

6) Yalnızca etkilenen RTU bağlantıları, mühendislik verileri kanal veya RTU düzeyinde değiştirildiğinde ve etkinleştirildiğinde (minimum) kesintiye uğrayacaktır.
7) Tek bir haberleşme noktasında yapılan veri mühendisliğinde, etkinleştirme kesintiye neden olmayacaktır.

10.8.7 Test ve Teşhis Özellikleri

Aşağıdaki test ve teşhis özellikleri Haberleşme Sunucusu sistemine entegre edilmelidir:

1) Sunucu ve RTU arasındaki telegramların izi takip edilebilir olmalıdır. Telegramlar protokole özgü bilgilere kodlanacaktır.
2) Sunucu ve RTU arasındaki telegram dahili protokol izlemesi yapılmalıdır. Kodlama mümkün değilse, gelen tüm veriler HEX formatında yazdırılacaktır.
3) Her iletişim bağlantısı için, RTU'dan cevap gelmediğinde gönderilen mesajları, alınan mesajları, mesaj hatalarını ve zaman aşımlarını saymak için ölçümler yapılacaktır.Örneğin iletişim hatasının istatistiki bir veri olarak tutulan ekrana(pivot vb) sahip olması.
4) İletişim Durumu Ekranı, RTU'ları ve kanal durumlarını görüntülemek için dinamik bir durum ve kontrol ekranı sağlayacaktır.
5) Tek bir RTU'ya veya çoklu bırakma modunda tüm bir kanala iletişimi etkinleştirme veya devre dışı bırakma yeteneğinin yanı sıra GI'yi etkinleştirme ve RTU'ya sıfırlama komutu (protokole özgü) yeteneği sağlayacaktır.

10.8.8 İzleme Kullanıcı Arabirimi

IEC-104 protokolleri için, protokol telegramını izlemek ve operatör için bir Kullanıcı Arayüzünde (yorumlanmış görünüm ve HEX görünümü) görüntülemek mümkün olacaktır.

10.9 ICCP Veri Bağlantısı

ICCP, kontrol merkezleri arasında gerçek zamanlı veri alışverişi için kullanılan SCADA iletişim alanının bir parçası olacaktır. SCADA ICCP uygulaması, farklı kontrol merkezleri ile iletişim kurabilecektir.

10.9.1 Yapılandırma Özellikleri

1) Kontrol Merkezleri Arası İletişim Protokolü (ICCP), IEC 60870-6 TASE.2 standardına göre uygulanacaktır.

2) Değiştirilen veriler, döngüsel verileri, gerçek zamanlı verileri (ölçülen değerler gibi) ve ölçülen değerler ve operatör mesajları gibi denetleyici kontrol komutlarını içermelidir.
3) ICCP sunucusu, bir istemci veri istediğinde erişim kontrolünden sorumlu olacaktır. Bir ICCP sunucusu birkaç istemciyle etkileşime girebilecektir.
4) Yönlendiriciler, *"Mesh router network", "X.25"* veya *"Frame Relay"* gibi farklı WAN türlerine erişim sağlayacaktır.
5) YÜKLENİCİ Istasyon/cihaz kimliğini destekleyen IEC 60870-6 TASE 2-ICCP protokolüne, iki-durum kontrol ve gösterge, tarih ve saat senkronizasyonu verisi, dosya aktarımı, e-postaya dayalı olarak gelecek hizmetler arası iletişimler için tüm gerekli tedarikleri sağlayacaktır. Proje kapsamında, ICCP tam işlevsel olarak test edilecektir.
6) Eş zamanlı olarak birden fazla partner ile ICCP haberleşme kurulabilecektir. Mevcutta bir (1) partner ile ICCP haberleşme kurulacak olup ileri dönük partner sayısı artırılabilecektir. En az 300 ICCP noktasıyla sorunsuz haberleşme kurulabilecek olup ileri dönük artırılabilecektir.

10.9.2 Yedeklilik

1) ICCP veri bağlantısı, etkin ve bekleme modunda çift iletişim sunucularını kullanan sıcak yedekli bir yapılandırmayı desteklemelidir. Aktif sunucu, yapılandırılmış farklı yolları kullanarak uzak sistemle iletişim kurmaya çalışacaktır. Aktif sunucu arızalanırsa, bekleme sunucusu devralıp ve uzak sistemle iletişim kurmaya çalışacaktır.
2) Sunucuların Etkin/Bekleme durumu, SCADA/DMS/OMS sistemi tarafından, birincil ve bekleme arasında kesintisiz yük devretme kullanılarak kontrol edilecektir.
3) Tüm iletişim yolları periyodik olarak test edilmeli ve durum bir İletişim Durumu Ekranında gösterilecektir.

10.9.3 Güvenlik İşlevleri

1) ICCP protokolü ICCP Secured olacaktır.
2) TCP/IP bağlantısı üzerinden TLS protokolünü kullanarak güvenli(secured) modda çalışabilecektir. ICCP uygulaması, yerel ve uzak bağlantının güvenliğini sağlamak ve doğrulamak için Uygulama Kimlik Doğrulaması' nı kullanacak şekilde de yapılandırılabilecektir.
3) ICCP PKI güvenlik standardını (SSL Protokolü) kullanarak güvenli iletişim sağlamalıdır.
4) Dijital sertifikalar, kimlik doğrulama ve veri şifreleme seçimi için kullanılacaktır.
5) Dış Sertifika Yetkilisi ile veya Yetkilisi olmadan çalışma.
6) X.509 standardını kullanmalıdır.
7) Güvenli ve güvenli olmayan bağlantıları aynı anda desteklemelidir.
8) Durum ekranında gösterilen güvenlik durumu belirtilebilecektir.
9) Güvenli mod, bağlantı bazında bir bağlantı üzerinde yapılandırılabilir. SSL teknolojisini kullanarak her bağlantının güvenliğini sağlamak için bir PKI yaklaşımı olacaktır.
10) Sistemde kullanılan tüm SCADA protokolleri (IEC 60870-5 serisi, IEC 60870-6 serisi, IEC 61970 serisi ve IEC 61968 serisi dahil) IEC 62531 Veri ve İletişim Güvenliğine uygun olacaktır.

10.9.4 Operasyonel Özellikler

1) ICCP uygulaması, veri bütünlüğünü ve bakım kolaylığını sağlamak için aşağıdakiler gibi ek özelliklere sahip olmalıdır:

a) Veri noktalarının bağlantıyı kesmeden eklenebileceği veya kaldırılabileceği çevrimiçi veri tabanı aktivasyonu

b) Eğim ve ofset kullanarak analog dönüştürme

2) İstatistikler oluşturulacak ve bir İletişim Durumu Ekranında gösterilecektir. İzlenen istatistikler aşağıdakileri içerecek, ancak bunlarla sınırlı olmayacaktır:

a) Bağlantının kaç kez kurulduğu ve koptuğu bilgisi

b) Gönderilen veya alınan verilerin sayısı

c) Gelen veri noktaları için iyi kalite oranı (İyi Oran = İyi kaliteye sahip veri noktası sayısı/Toplam veri noktası sayısı)

3) Modbus TCP/IP, ICCP, IEC 61850'nin en son sürümlerini ve diğer ilgili protokolleri ve standartları destekleyecektir. YÜKLENİCİ yukarıda belirtilmiş olan tüm protokoller ve standartların Garanti Süresi sonuna kadarki muhtemel versiyonları için lisanslarını ihale bedeli içerisinde tüm sistem bileşenleri için sağlayacaktır.

10.9.5 ICCP Telegram İzleme Ekranı

ICCP izleme ekran ile kullanıcı, OKUMA, YAZMA ve BİLGİLENDİRME mesajlarını görüntüleyebilecektir.

10.10 SCADA/DMS Uygulamaları

10.10.1 Genel

Denetleyici Kontrol ve Veri Toplama (SCADA), aşağıdakiler gibi temel yetenekleri sağlamak için gruplandırılabilecek çeşitli işlevler sağlayacaktır:

1) Telemetri
2) İzleme ve Alarm Verme
3) Kontrol

10.10.2 Fonksiyonellik

1) Veri İşleme

Veri işlemesi, işlenmiş verileri sisteminden alarak daha fazla işlem için kullanacaktır. Değer değişiklikleri izlenecek ve veriler diğer sistemlere dağıtılacak ve log kayıtlarına yazılacaktır. Hesaplamalar, mantıksal işlemler ve özel veri türleri için özel işleme işlevleri yapılacaktır.
Veri işlemenin alt işlevleri şunlar olacaktır:

a) Önceden işlenmiş süreç verilerinin elde edilmesi. Örneğin, dijital değerler, ölçülen değerler ve ölçülmüş değerler.

b) Dijital değerlerin işlenmesi.

Alarmlar ve anahtarlama durumları işlenecek ve gerekli onaylar izlenecektir. Proses verisi değişikliklerinde, topoloji yeniden hesaplanacaktır.

c) Ölçülen değerlerin işlenmesi.

Ölçülen değer hesaplaması, ikame değerler, limit kontrolü, ortalama, maksimum ve minimum değerlerin hesaplanması ve gradyan hesaplamaları gibi çeşitli işleme fonksiyonları sağlayacaktır.

d) Ölçülmüş değerlerin işlenmesi.

İşleme fonksiyonları, ölçülen değer hesaplamasını, eksiksizlik kontrolünü, toplamların hesaplanmasını, maksimum ve minimum değerleri, çalışma saatlerini ve anahtarlama döngüsü sayımını, tarife süresi işlemeyi vb. içerecektir.

e) Mantık işlemleri.

Genel bir hesaplama fonksiyonu, hesaplama kuralları kullanılarak operasyonel veri tabanında saklanan çeşitli veri türlerinin birleştirilmesine ve hesaplanmasına izin verecektir. Kendi kodlamalarını oluşturmaya fırsat tanıyabilecektir. Bunlar Mühendislik Veri Uygulaması kullanılarak tanımlanmalı ve atanmalıdır.

f) İşlenen verilerin operasyonel veri tabanında depolanması (sapmalar ve hatalar hakkındaki verilerin otomatik olarak güncellenmesi).

g) İşlenen verilerin diğer alt sistemlere dağıtılması.

2) Denetleyici Kontrol

a) SCADA/DMS, yürütme süresini azaltan ve operasyonel güvenilirliği artıran yerleşik bir şebeke kontrol konseptine sahip olmalıdır. Enerji şebekesinin kontrol edilebilir elemanları için şebeke kontrolünün izin verilen operatör konsollarından gerçekleştirilmesi mümkün olacaktır.

b) Bireysel anahtarlama işlemleri ve anahtarlama sıraları uygulanacaktır.

c) Genel kilitleme koşulları ve güvenlik özellikleri, çalışma modunda ön test gibi verimli ve güvenli kontrol eylemleri sağlamalı ve işlemlerinin hızlı bir şekilde yürütülmesine olanak tanımalıdır.

d) Operasyonel güvenilirliği sağlamak için, SCADA/DMS/OMS'in şebeke kontrol konsepti çeşitli ek güvenlik özellikleri içermelidir:

I. Çeşitli kilitleme koşullarını kontrol edilebilmesi,

II. Planlı anahtarlama işlemlerinin şebeke güvenilirliği izlenebilmesi,

III. Anahtarlama işlemi sırasında şebeke değişikliklerinin izlenebilmesi,

3) Geçici Şebeke Ekipmanları

a) SCADA/DMS/OMS, jumper, hat bölümlendirme, topraklama ve jeneratörler bağlantısı gibi geçici şebeke elemanlarının çevrimiçi olarak konumlandırılmasına ve veri

mühendisliği sistemine veri girmek zorunda kalmadan bunları ekleme/silme yeteneğine izin verecektir.

b) Şebeke elemanları konumlandırılırken yorum yazma zorunlu olacaktır ve kullanıcı adı otomatik eklenir durumda olmalıdır. İstenildiğinde raporlanabilir ve takip edilebilir durumda olması sağlanacaktır.

c) Geçici şebeke elemanları topolojide aktif hale gelecek ve ayrıca kilitleme veya izleme fonksiyonları tarafından yeni bir şebeke elemanıymış gibi şebekeye işlemin hemen etki etmesi gerekmektedir.

d) Geçici şebeke elemanları kaldırılıncaya kadar topolojide aktif kalacaklardır.

e) Her bir şebeke elemanından en az 50hat bölücü, 50 jumper,50 jeneratör ve 50 topraklama bağlantısı koyulabilecektir.

f) Geçici bir şebeke öğesinin, bağlam menüsü kullanılarak hızlı bir şekilde eklenmesi de mümkün olacaktır.Geçici şebeke elemanı, örneğin izleme için topolojik olarak derhal etkili hale gelecektir.
g) Geçici şebeke elemanları otomatik olarak bir isimle donatılacak ve bir özet halinde rapor edilecektir.
h) Geçici şebeke elemanlarının miktarı yapılandırılabilir olmalıdır.
i) Geçici jumper, cut ve mobil jeneratörler için sembollerin serbestçe tanımlanabilmesi mümkün olacaktır. Sistem parametrelendirmesi sırasında, bu semboller normal ekipmandan açıkça ayırt edilebilir hale getirecek şekilde tasarlanmalıdır.

4) Seçim Yönetimi

Ekrandaki sesli alarmlar ve yanıp sönen gösterge elemanları, alarmlar ve enerji besleme şebekesinin normal durumundan sapmalar hakkında bilgi sağlamalıdır.

5) Genel Özet

a) Genel Özet, herhangi bir eylemi bildirmek veya bir ekranın genel bilgilerini kaydetmek için sağlanacaktır, örneğin veri kaynaklarındaki değişiklikler, ikame eylemi, denetleyici kontrol eylemleri, etiket işlemleri vb.
b) Genel Özet, denetleyici kontrol eylemleri, manuel güncelleme eylemleri ve etiket işlemleri gibi sistemde gerçekleştirilen herhangi bir eylemi raporlamak için kullanılabilecektir.

6) Operasyon Günlüğü

a) Operasyon Günlüğü, önemli değişiklikleri ve operatörün girdiği önemli bilgileri toplayacaktır. İşlem kayıt düzenlenebilir olacaktır.
b) Bazı alarm mesajlarının operasyon kayıt defterine otomatik olarak eklenecek şekilde parametrelendirilmesi mümkün olacaktır.
c) Alternatif olarak, operatör alarm mesajlarını genel özetten operasyon kayıt defterine de kopyalayabilecektir.
d) Bir operatörün geçerli kayıt defterine farklı türlerde mesajlar ekleyebilmesi mümkün olacaktır.

7) Açık uçlu hatları görüntüleme

Her iki tarafa da bağlı olmayan hatlar görsel olarak ayrı bir renkle sunulacaktır veya raporlanabilecektir

8) Yedekli Veri Kaynakları

a) Yedekli Veri Kaynakları özelliği hem dijitalleri hem de analogları desteklemelidir.

b) Analogların en az dört (4) yedekli veri kaynağına sahip olmasına izin verilecektir.

c) Ortaya çıkan teknolojik adres, trafo merkezi tek hatlarına bağlanacaktır. Kaynak teknolojik adres, RTU verilerini veya ICCP verilerini tanımlamak için kullanılacaktır.

d) Operatör şunları yapabilecektir:

I. Bir kaynağın otomatik seçimini geçersiz kılınabilmesi,

II. Kaynakların önceliğinin değiştirilebilmesi,

III. Bir kaynağı engelleme veya yeniden etkinleştirebilme,

9) Topoloji Analizi ve Şebeke Renklendirme

a) İnteraktif topolojik yol izleme, operatörün dağıtım şebekesindeki elektrikle bağlı ekipmanlar arasındaki yolları belirlemesine izin verecektir. Genişletilmiş izleme işlevleri, yükler, müşteriler, sorun çağrıları, kesintiler vb. gibi ek bilgileri içerecektir.

b) İzleme sonucu, açık olan tüm coğrafi veya şematik ekranlarda (farklı bir renkle) vurgulanmalıdır. Kullanıcı ikinci bir izleme başlatırsa, sonuç, ilk izlemenin sonucuna ek olarak, ancak kullanıcının sonuçları karşılaştırmasına izin vermek için farklı bir renkle görüntülenecektir.

c) Şebeke renklendirme fonksiyonu, bireysel ekipman öğelerinin çeşitli özelliklerine bağlı olarak ekipmanın renkli gösterimini kontrol etmelidir. Kısmi şebekeler, şebeke grupları (örneğin, gerilim seviyeleri) veya ekipmanın çalışma durumları (örneğin topraklanmış ve tanımlanmamış) farklı renklerde vurgulanmalıdır.

10) Kontrol Alanı (AOC)

a) Bir AOC, çeşitli Sorumluluk Alanlarının (AOR'ler) bir gruplandırması olacaktır.

b) AOR'ler ve AOC'ler sistemde (ŞYA'da) yapılandırılabilir olmalıdır. Örneğin, bir AOC'nin bir kullanıcının sorumlu olabileceği coğrafi bir bölge olması mümkün olacaktır.

c) Bir kullanıcının bir veya daha fazla AOC'ye atanması mümkün olacaktır. Bir AOC'ye yalnızca bir kullanıcıya izin verilip verilmediği veya bir AOC'ye birden fazla kullanıcıya izin verilip verilmeyeceği bir sistem yapılandırması olacaktır.

d) Kullanıcıların ve AOC'lerin atanmasının çalışma zamanında yapılabilmesi mümkün olacaktır. Bir kullanıcı oturumu kapatmaya çalıştığında, sistem tüm aktif kullanıcıları izlemelidir.

10.10.3 Veri İşleme

a) Genel

I. Veri işleme, süreç arayüzü veya diğer sistemler (örneğin, SCADA IM/DM ekranları ve topoloji çözümleri) tarafından sağlanan verileri işleyecek, değişiklikleri izleyecektir.

II. Veri hesaplamaları, veri kombinasyonları ve benzersiz veri türleri için özel işlemler gerçekleştirilecektir.

III. Veri işleme sisteminin temel özellikleri şunlar olacaktır:

- Verilerin tekil ve toplu olarak giriş yapılabilmesi,
- İşlenen verilerin loglanarak depolanabilmesi ve ulaşılabilir olması,

b) Veri Toplama

I. Veri işleme, proses arayüzünden (örneğin RTUveya ICCP) güç sistemi verilerini alacaktır.

II. Durum değişikliği üzerine iletilen durum göstergeleri, güç sistemi alarmları ve dahili olarak oluşturulan sinyaller arayüzden alınabilmelidir.

III. İşlenen Verilerin Saklanması

a) Veri işleme, veri tabanı için herhangi bir zamanda veri bütünlüğünü sağlayacaktır.

b) Analog veri girişleri-değer kalitesi bayrakları ve zaman damgası ile saklanacaktır.

c) Verilerin İşlenmesi Süreci

I. Bazı verilerin dağıtılması engellenirse (Alarm Engelleme), engellenen mesaj normal şekilde işlenmelidir.

II. Veri işleme sistemi, durum değişikliği üzerine iletilecek olan süreç arayüzünden veri alacaktır.

III. Mesajlar aşağıdaki veri formatında alınmalıdır:

- Zaman damgası

Normal mesajlar için, zaman damgası haberleşme sunucusundaki kabul saatini içermelidir. SOE mesajları için, zaman damgası RTU zaman damgasını (msec) içermelidir.

- Tekil ID,
- Durum,
- Kalite bayrakları,

Mesaj işleme aşağıdaki işlevleri sağlamalıdır:

I. Temel alarm ve durum işleme,

II. İşletimsel veri tabanında depolama,

III. İletilerin diğer fonksiyonlar tarafından kullanılabilmesi,

İşlem arabiriminden veya başka bir fonksiyondan durum veri işlemeye gönderilen iletiler aşağıdaki adımdan geçecektir:

I. Onay için izleme, Durum değişikliğinin bir operatör eyleminin sonucu olup olmadığını belirleme,

II. Topoloji yeniden hesaplama,

Analog Veri İşleme

a) Güç sisteminden gelen analog değerler belirli bir eşikten daha fazla değiştiği her seferinde bir veri iletimi gerçekleştirilecektir.

b) Her değer aşağıdaki veri biçimine sahip olmalıdır:

I. Öncelikle RTU zaman damgası olmadığı durumda SCADA Zaman damgası,

II. Tekil ID,

III. Değer,

IV. Kalite bayrakları,

c) Analog veri işleme aşağıdaki işlevleri içermelidir:

I. El ile değiştirilen değerlerin değiştirme değerleri olarak kullanılması,

II. Mevsimsel limit kontrolü,

III. Entegre ve ortalama değerlerin hesaplanması,

IV. Maksimum ve minimum değerlerin hesaplanması,

V. Formül kullanarak hesaplama,

VI. Değişim hızı limit kontrolü,

VII. İşletimsel veri tabanına depolama

d) Limit Türleri ve Öncelikleri

I. Manuel sınırlar (en yüksek öncelikli) Dijital ve analog sinyallerde belirli sayı üzerine çıkılması veya belirli sınırın altına inmesi durumunda limit alarm üretebilecektir. Manuel olarak değiştirilen tüm sınırların bir özet halinde görüntülenmesi mümkün olacaktır.

II. Sınır kümeleri (varsayılan) En az dört (4) mevsimsel limit seti ve dört (4) ek limit seti mevcut olacaktır. Belirlenen her sınır en az beş (5) alt ve beş (5) üst sınır sağlayacaktır. Kullanıcı, Sınırlar Ekranında hangi sınırın kullanılacağını seçebilecektir. Belirlenen varsayılan limit (gerçek sezon) seçilirse, mevsimsel sınırlar tanımlanan zamanda mevsim değişikliği üzerine otomatik olarak değiştirilecektir.

III. İki tür limit kümesi olacaktır:

ŞYA aracı kullanılarak girilen statik sınırlar,

SCADA/DMS/OMS sisteminde hesaplanabilen veya harici bir sistemden alınan dinamik sınırlar (örneğin sıcaklığa bağlı olarak)

e) Deadband

I. Her değeri bir dizi üst ve alt sınıra karşı kontrol etmek mümkün olacaktır.

II. Limitler, her bir değer için ayrı ayrı nominal değer veya yüzdesi olarak tanımlanabilecektir. Sınırın etrafında salınan değerler ve gereksiz sınır ihlallerini önlemek için, değer ve sınırın karşılaştırılmasında önceden tanımlanmış bir Deadband eşiği kullanılmalıdır.

III. SCADA/DMS/OMS, operatörün üst ve alt limitleri tanımlayabileceği bir uygulama sağlayacaktır.

f) Entegre Değerlerin ve Ortalama Değerlerin Hesaplanması

I. Entegre değer (integral), geçen süre ile birleştirilen alınan değerlerin toplamı olacaktır.
II. Ortalama değer, entegre değerden türetilecek ve tanımlanmış bir zaman aralığına bölünecektir.
III. Entegre değerin hesaplanması, dönemin geçerli değerlerinin sayısını dikkate alacaktır. Geçerli değerlerin sayısı tanımlanmış bir minimum değerin altındaysa, entegre değere hesaplamanın başarısız olduğunu belirten bir kalite kodu atanır.
IV. İntegral (baz integralin hesaplanması) acil bir prosedür olsa da ortalama değerler ve takip integralleri periyodik olarak hesaplanmalıdır. Örneğin, bu özellik, aktif güç değerlerine dayalı enerjinin hesaplanmasına izin verecektir.

g) Maksimum ve Minimum Değerlerin Hesaplanması

Tanımlanmış bir zaman dilimi içinde, bir kaynak için en yüksek ve en düşük değer seçilmeli ve meydana geldiği tarih ve saatle birlikte veri tabanında saklanmalıdır.

h) Formül Kullanarak Hesaplama

I. Genel bir hesaplama formülü tanımlanabilir olmalıdır, örneğin sqrt (a*a+b*b).
II. Formül bir model olarak hizmet edecek ve belirtilen nesnelere uygulanacaktır.
III. Hesaplama sonuçları veri tabanında saklanacaktır. Bu sonuçlar diğer hesaplamalar için kaynak olacaktır. Tipik bir uygulama, ölçülen gerçek güce ve reaktif güce dayanarak görünür gücün hesaplanmasıdır.

I) Değişim Oranı Limit Kontrolü

I. Değişim oranı limit kontrolü yapılacak ve limit ihlalleri için alarmlar verilecektir. Değişim oranı, bir değerin büyüklüğünün ne kadar hızlı değiştiğini gösterir ve hız, bir değişim hızı sınırına göre kontrol edilir.
II. Artan veya azalan değişiklikler için kontroller yapılacaktır. Kontrollerin son değer karşılaştırılarak yapılabilmesi mümkün olacaktır.
III. Operatör, değişim limiti kontrollerinin hızını açıp kapatabilmeli ve önceden tanımlanmış değişim oranı sınır değerlerini değiştirebilecektir.

I. Veri Hesaplamaları

a) Ortak veri hesaplamaları için, SCADA/DMS/OMS genel bir hesaplama ve kombinasyon fonksiyonu sağlamalıdır. Bu işlev, hesaplama kuralları kullanılarak operasyonel veri tabanında depolanan farklı veri türlerinin birleştirilmesine ve hesaplanmasına izin verecektir. Hesaplama kuralları Veri Mühendisliği Uygulamasında tanımlanmalı ve atanmalıdır.

b) Formülleri Kullanarak Veri Hesaplama

Aşağıdaki veri türleri, hesaplamalar veya kombinasyonlar için girdi olarak kullanılacaktır:

I. İkili veri,
II. Değer,
III. Örnek Formüller, Aritmetik ve Mantık İşlevleri

Aritmetik işleçler	+ - * / div modu

Karşılaştırma işleçleri	= < > <= >= <>
Mantık işleçleri	AND OR NOT EQ EXOR IF THEN ELSE
İşlevsel operatörler	SQR SQRT EXP SIN COS TAN ARCTAN MAX MIN ABS SIGN LN INT FRAC

Tablo-1: Örnek Formüller, Aritmetik ve Mantık İşlevleri

IV. Tekil ID, operasyonel veri tabanındaki veri noktaları için bir tanımlayıcı görevi görecektir. Seçilen Tekil ID'ya uygulanan formül, formülün işaretleri, Tekil ID adı, Tekil ID metni, değeri, kalitesi ve kaynak Tekil ID'ların birimi gibi hesaplanan veri noktaları hakkında bilgi belirlemek mümkün olacaktır.

V. Hesaplama ifadelerinde farklı veri türlerinin kullanılması mümkün olacaktır. Hesaplamalarda kullanılan bir ifadenin değerlendirilmesi için öncelik, parantezler de dahil olmak üzere standart cebirsel öncelik kurallarına uymalıdır.

VI. İşaretlere bağlı olan hesaplamanın sonucunun, ikili veri veya operasyonel veri tabanına geri depolanacak bir değer olması mümkün olacaktır. Hesaplanmış veriler, ayrı bir teknolojik adres ile saklanacaktır; daha sonraki hesaplamalar için girdi olarak kullanılması mümkün olacaktır. Bu amaçla, yürütme sırası belirlenir ve her hesaplamaya bir yürütme önceliği atanır.

VII. Aşağıdaki işleme hesaplamaları mevcut olacaktır:

1:1 işleme,

Formül yalnızca belirtilen veri noktaları için geçerli olacaktır.

Anlık işleme,

Kaynak değerin değiştirilmesinden sonra, tüm bağımlı birleşik değerler otomatik olarak yeniden hesaplanır.

Gecikmeli işleme,

Kaynak değerin değiştirilmesinden sonra, tüm bağımlı birleşik değerlerin hesaplanması geciktirilecektir. Operatör gecikme süresini yapılandırabilecektir.

Periyodik,

Hesaplama periyodik olarak yapılacaktır.

10.10.4 Topolojik Şebeke Renklendirme

1) Topoloji Analizi

Topoloji analizi aşağıdaki görevleri içermelidir:

a) Şebeke renklendirme, kendiliğinden olaylardan sonra (arıza trip vb.) veya alternatif olarak, anahtarlama durumlarındaki değişiklikler şebeke topolojisinde bir değişikliğe neden olduktan sonra otomatik olarak etkinleştirilecektir.

b) İnteraktif Topolojik İzleme fonksiyonu için topoloji analizi,

c) Kesinti Yönetimi uygulamaları için şebeke elemanlarının analizi,

2) Şebeke Boyama

a) Şebeke Boyama fonksiyonu, şebeke diyagramlarındaki operasyonel ekipmanın renk gösterimini kontrol edecektir.
b) Renklendirme seçeneği değiştirilebilir olmalıdır.
c) Aynı anda İki farklı şebeke renklendirilip, ortak kesişen şebeke unsurları gösterilecektir.
d) Aşağıdaki kısıtlamalar ekipmanın renk gösterimini etkileyecektir:

I. Bir elektrik alt şebekesi, farklı enjeksiyon noktalarından başlayarak altındaki hatları, kabloları, baraları ve diğer operasyonel ekipmanlardan oluşacaktır. Farklı alt şebekeler farklı renklenmelidir.
II. Alt şebeke sınırları parametrelendirilebilir olmalıdır.
III. Şebeke grupları,
IV. Gerilim seviyesine göre farklı renklendirme yapılabilir olmalıdır. Elektriksel çalışma durumu,
V. Enerjisi kesilmiş,
VI. Topraklı,
VII. Enerjili,
VIII. Anormal pozisyon,
IX. Döngü,
X. Paralel

3) İnteraktif Topolojik İzleme

a) İnteraktif Topolojik İzleme**,** operatörün bir dağıtım şebekesi içindeki elektrikle bağlı ekipman arasındaki yolları izleyerek bir bağlantı analizi yapmasını sağlayacaktır.
b) Operatör bir ekranda (şematik veya coğrafi) şebeke ekipmanı seçebilmeli ve bağlam menüsünden bir izleme türü seçebilecektir. Birkaç izleme türü, operatörün seçebileceği iki veya daha fazla şebeke ekipmanı türünün seçilmesini gerektirir.
c) İzlemenin sonuçları ekranda farklı bir renk kullanılarak gösterilecektir. Operatör, elektrik bağlantısının önceden tanımlanmış normal anahtarlama durumuna mı yoksa gerçek anahtarlama durumuna mı bağlı olduğunu seçebilecektir.
d) Aşağıdaki eser türleri mevcut olacaktır:

İzleme Türü	**Tarif**
Yukarı yönde izleme	Belirli bir şebeke elemanından başlayarak, yukarı akım yönünde elektrikle bağlı tüm şebeke elemanları için izlenebilmesi,
Üst Ekipmana Doğru İzleme	Belirli bir şebeke elemanından başlayarak tüm şebeke unsurları ile birlikte ilk oluşumu için yukarı akışı izlenebilmesi,
Aşağı Doğru İzleme	Belirli bir şebeke elemanından başlayarak elektrikle bağlı tüm şebeke elemanları için aşağı yönde izlenebilmesi,
Ekipmanlar Arası	Seçilen iki eleman arasındaki elektriksel bağlantı için iz.

İzleme Türü	Tarif
Hepsi	Seçilen şebeke öğesine bağlı tüm şebeke öğeleri için izlenebilmesi,
Ortak Nokta	İki veya daha fazla seçili şebeke öğesinin yukarı akış yönündeki ortak yolu izlenebilmesi,
Fider	Radyal yukarı akış yolu ve aşağı akış şebeke kısmının birleşimi olan seçili ağ öğesinin tüm besleyici uzantısı için izlenebilmesi,

Tablo-2: İzleme Türleri

e) Paralel ve Döngü tespiti mümkün olacaktır.
f) TRACE sonuçları tüm ekipmanlar (trafo, hat, kesici vb.) tipinde ve bağlı müşteriler bazında tablolar üzerinde gösterilebilir olacaktır.

10.10.5 Denetleyici Kontrol

1) Genel bakış

Yetkili operatörler herhangi bir güç sistemi cihazını kontrol edebilecektir. Denetleyici kontrol eylemleri, işletme güvenliğini sağlamak için her zaman iki aşamalı operasyonlar olacaktır.

2) Kullanılabilir İşlevler

Aşağıdaki standart kontrol fonksiyonlarının, önceden tanımlanmış noktalar için kontrol işlemleri kullanılarak etkinleştirilmesi mümkün olacaktır:

Anlık Anahtarlama

I. Anahtar,
II. Ayar noktası,

3) Güvenlik Özellikleri

SCADA/DMS, denetleyici kontrol için çok sayıda güvenlik özelliği sunacaktır.

a) Ek özellikler şunları içerecektir:

I. İlgili her bir operasyon adımı için operatör yetki/sorumluluk kontrolü yapılabilmesi,
II. Gereksiz kontrol işlemlerini önlemek için çeşitli kilitleme koşullarının kontrol edilebilmesi,
III. Planlı kontrol operasyonları için şebeke güvenliğinin izlenebilmesi,
IV. Eşzamanlı kontrol işlemlerinin birbirine karışmasının önlenebilmesi,
V. Bir kontrol işlemi gerçekleştirilirken şebeke değişikliklerinin izlenebilmesi,
VI. Denetim kontrol eylemlerinin Genel Özet'te günlüğe kaydedilmesi. Her denetleyici kontrol girişi, tarihini, saatini ve kullanıcı kimliğini içermelidir.

b) Kilitleme Koşulları

Personel yaralanmasını veya maddi hasarı önlemek için, çeşitli kilitleme koşullarına karşı kontrol edilmeden hiçbir kontrol emri gerçekleştirilmeyecektir.

c) Topolojik Kilitleme Koşulları

I. SCADA/DMS güç sisteminin genel topoloji tanımına dayanarak kilitleme koşulları sağlayacaktır. Genel topoloji açıklaması, veri tabanının bir parçası olacaktır.

II. Topolojik kilitleme koşullarının değerlendirilmesinde karar tabloları yerine temel topolojik algoritmalar kullanılmalıdır.

III. Aşağıdaki topolojik kilitleme koşulları mevcut olacaktır:

- Topraklanıp topraklanmadığını kontrol edilmesi,
- Operasyonel ekipmanın topraklanmadan önce izole edilip edilmediğini kontrol edilmesi,
- Operasyonel ekipman etiketini kontrol edilmesi,

IV. Genel şebeke topolojisi diğer SCADA/DMS/OMS işlevleri için zaten kullanıldığından, bu işlevsellik için ek veri girişi ve veri testi gerekmemelidir.

d) Genel Kilitleme Koşulları

SCADA/DMS/OMS, aşağıdaki güvenlik kontrollerini manuel ya da otomatik olarak yapabilmelidir.

I. Çeşitli denetleyici kontrol operasyonları için genel kilitleme koşullarını içermelidir.

II. SCADA/DMS/OMS' te eklemiş olacağımız bir kuralın bağlı bulunduğu tüm alanda geçerli olması sağlanacaktır. (örnek: SCADA kabin için bu kural uygun olurken devreye aldığımız üretici SCADA sı için de bu kural geçerli olacaktır.)

III. Aşağıdaki belirtilen aksiyonlar için engelleme yapmak mümkün olacaktır.

- Açma komutu
- Kapama komutu
- Pozisyon değiştirme
- Enerjilendirme
- Enerjisiz bırakma
- Topraklama
- Çalışma İzni
- Ayırıcıların yük altında açılması

IV. Hücre veya RTU lokal durumdayken uzaktan sadece onay verilerek açma yapılabilmesi mümkün olacaktır.

V. SCADA'lı ekipmanların belirli koşullarda oluşan pozisyon değişiklikleri ile alarm üretilebilecek bir kural ŞİRKET tarafından oluşturulabilecektir.

VI. Operatör tarafından konulan çalışma var uyarısı ile etiket koyulmuş bir hücreye müdahale edilememesi sağlanacaktır. Etiketin yetkili tarafından kaldırılması sonrası aktive olabilmesi sağlanacaktır.

e) Etkileşimlerin Takibi

I. SCADA/DMS/OMS denetleyici kontrolü, kontrol işlemlerinin eş zamanlı olarak yapılmasını sağlayacaktır. Bu tür kontrol operasyonları arasındaki olası bir etkileşim, tüm kontrol işlemlerinin izlenmesiyle kilitlenecektir. Bu izleme herhangi bir operatör eylemi gerektirmeyen bir arka plan özelliği olacaktır. Şebeke değişikliklerinin izlenmesine benzer şekilde, eylem alanı olarak adlandırılan bir izleme aralığının tanımlanabilmesi mümkün olacaktır.

II. Eylem alanı aşağıdakiler için yapılandırılabilir olmalıdır:

Bir eylem alanı için aynı anda bir (1) kontrol operasyonunun gerçekleştirilebilmesi mümkün olacaktır. Eylem alanında bir kontrol operasyonu aktifse, kullanılan iş istasyonundan bağımsız olarak diğer herhangi bir kontrol işlemi reddedilecektir.

f) Check-Back Sinyal İzleme

Komut iletiminden sonra, ilgili geri dönüş sinyalinin alınması, serbestçe parametrelendirilebilecek bir zaman aralığı boyunca izlenmelidir.

4) Anlık Kontrol

I. SCADA/DMS/OMS ile gerçekleştirilen kesiciler, bara ayırıcıları, trafo kademe değiştiriciler, ayar noktası komutları ve diğer uzaktan kumandalı şebeke elemanları ile tek kontrol işlemlerinin bağlam menüleri üzerinden basit ve konforlu bir şekilde yapılabilmesi mümkün olacaktır. Örneğin; SCADA ekranından istasyonların açılmasını sağlayan özelleştirilmiş butonlar yardımı ile kontrol edilmesi planlanan telemetrili kabinleri, trafo merkezleri ya da bölgeye ait şebeke haritası ekranda yeni bir pencerede açılmalıdır.

II. Kontrol edilebilir şebeke elemanına sağ tıklandığında ilişkili bağlam menüsü açılması ve içerik olarak, söz konusu şebeke elemanına ilişkin tüm işlemleri gösterecektir.

III. Tüm eylemler birbirine kenetlenme koşullarına karşı kontrol edilecektir. Kilitleme koşulları ihlal edilirse, uygun teşhis mesajları görüntülenecektir. Herhangi bir ihlal tespit edilmezse, operatör gerekli anahtarlama işlemini onaylamalı ve kontrol komutu trafo merkezine gönderilecektir.

5) Ayar Noktası (Setpoint) ve Pals Komutu

I. SCADA/DMS/OMS, setpoint komutu verme işlevselliğini sağlayacaktır. Setpoint komutları, analog ayar noktalarını RTU'ları kullanarak yerel denetleyicilere iletmek için kullanılır. Bir setpoint değeri girerken (TI50), sistem değerin izin verilen aralıkta olup olmadığını kontrol etmelidir. Aksi takdirde, operatöre bildirilecektir. SCADA/DMS/OMS, yerel kontrollerin gerçek değerlerini analog değerler olarak işleyecektir.

II. Manuel olarak girilen setpoint komutları otomatik olarak iletilmeli ve iletişim hataları denetleyici kontrol ekranında raporlanmalıdır. Her ayar noktası komut çıktısından sonra, değerin başarılı bir aralıkta kalmasını sağlamak için değer parametreli bir süre boyunca izlenmelidir. Aksi takdirde, operatör denetleyici kontrol ekranında

bilgilendirilecektir. Seçilen bir elemanın gerçek değerini, başka bir eleman için ayar noktası değeri olarak kullanmak mümkün olacaktır.

III. Başvurulan bir elemanın gerçek değerini bir ayar noktası komutu olarak almak mümkün olacaktır.

6) Etiketleme ve manuel güncelleme

a) Genel bakış

Hem etiketleme hem de manuel güncelleme, tek kontrol ve önceden tanımlanmış kontrol dizileri gibi diğer denetleyici kontrol işlemlerine benzer olmalıdır. Bu işlemler etkinleştirilmeli ve başlatıldıktan hemen sonra kilitleme koşulları açısından kontrol edilmelidir. Bunlar yalnızca işlem veri tabanındaki şebeke öğesi durumlarını etkileyecektir. Trafo merkezine hiçbir kontrol komutu gönderilmeyecektir.

b) Etiketleme

I. Operatör, uzaktan kumanda veya uzaktan kumandalı anahtar durumlarının Operasyonel Veri Tabanına girilmesi için önemli olan özelliklere işaret etmek üzere anahtarları, operasyonel ekipmanı ve anahtar bölmelerini etiketleyebilecektir.

II. Her ayar veya silme, Genel Özet'e ve ilgili etiketleme özetine girilmesine neden olmalıdır.

III. Etiketler ayrıca kilitleme kontrolleri için de kullanılacaktır. Örneğin, tipik bir uygulama, mevcut değil olarak etiketlenmiş operasyonel ekipman üzerindeki anahtarlama işlemlerinin birbirine kenetlenmesidir.

IV. Etiketlerin, anahtar bölmeleri, trafo merkezi içindeki gerilim seviyeleri veya komple trafo merkezleri gibi münferit şebeke elemanlarına veya komple teknolojik alanlara uygulanabilmesi mümkün olacaktır. Etiketler, SCADA Tek Hat haritasında, seçilen elemanın veya teknolojik alanın yakınında karşılık gelen bir simge aracılığıyla gösterilecektir.

V. Etiket ayarlama, düzenleme ve temizleme

Etiketlerin, şebeke elemanlarının bağlam menüsü veya şebeke diyagramındaki teknolojik alanlar kullanılarak ayarlanabilmesi ve temizlenmesi mümkün olacaktır.

Bir eleman veya teknolojik alan üzerinde, Çalışma İzni etiketi hariç, her türden yalnızca bir etiket yerleştirilecektir. En az 6 adet Çalışma İzni etiketi sağlanacaktır.

VI. Kontrol Engelleme

Bu etiket, etiketlenmiş şebeke elemanı veya etiketli alan (trafo merkezi, gerilim seviyesi veya besleyici) için uzaktan kumanda komutlarının çıkışını kilitlemek ve engellemek için kullanılacaktır.

Etiket, ayar noktası olan bir analog değer için kullanılmalıdır.

VII. Operasyondan Kaldırıldı

Telemetrili istasyonlarda Operasyondan Kaldırıldı etiketi konulduğunda hangi elemente konulduysa dijital/analog manuel değişiklikleri yapmasına olanak sağlayacaktır.

VIII. Testteki Nesne

Bu etiketi kullanarak, operatör ilişkili elemanlar için başka bir mesaj dağılımı yapılandırması tanımlayabilecektir, örneğin sesli alarm yok, alarm özetlerinde görüntülenmiyor, ancak Test Edilen Nesne Olayları Özetinde görüntüleniyor.

Alarm alanında etiket ayarlanmadan önce alarmlar zaten etkin olduğunda, etiket ayarlandığında alarmlar otomatik olarak onaylanmalıdır.

Bu etiketin analog değerler ve birikmiş değerler için de kullanılması mümkün olacaktır.

IX. Dikkat

Bir cihazda bir 'Dikkat' etiketi ayarlandığında ve operatör bu cihazı kontrol etmeye çalıştığında, operatörü bir uyarı etiketinin ayarlandığı konusunda uyaran bir mesaj görüntülenir. Operatör bu etiketi geçersiz kılabilecektir.

X. Bilgi

Bu etiketin denetleyici kontrol üzerinde hiçbir etkisi olmayacaktır. Şebeke diyagramındaki bir elemanın yanındaki ilgili simge, eleman için mevcut bilgilerin olduğunu gösterecektir. Operatör, bilgileri okumak için kullanıcı arayüzü ekranının 'Etiketler' sekmesini açabilecektir.

XI. Çalışma İzni

Çalışma İzni etiketi, bakım çalışmalarının yapıldığı ağ alanları için kullanılacaktır. Etiketli şebeke öğesi veya etiketli alan için herhangi bir uzaktan kumanda komutunu engelleyecektir.
Birden fazla Çalışma İzni etiketi teknolojik bir unsura ayarlanırsa, çalışma izni alan her kişi ve amaçlanan her çalışma ayrı ayrı görüntülenir.

XII. Alarm Engelleme

Bu etiketin analog veya dijital bir değere ayarlanması alarm verilmesini önleyecektir. Diğer tüm işlemler gerçekleştirilecektir. Alarm olayıyla ilgili mesajlar Genel Özette gösterilecek, ancak alarm özetlerinde görüntülenmeyecektir.

7) Manuel Güncelleme

I. Çevrimiçi operasyonlar için güncel ve tutarlı bir gerçek zamanlı veri tabanı (RTDB) sağlamak amacıyla, SCADA/DMS/OMS, RTDB manuel güncellemesi için ek özellikler sağlayacaktır.Bu özellik, operatörün şebeke elemanı durumunu manuel olarak geçersiz kılmasını sağlayacaktır. Bir telemetri hatasındaki (RTU arızası) işletimsel veri tabanını güncelleştirmek için, var olan bir veri tabanı işlem etiketinden taşınabilecektir.

II. Güncelleme amaçları için (örneğin, dağıtım şebekelerindeki anahtarlama işlemlerinin manuel olarak güncellenmesi), SCADA/DMS/OMS, operatörün manuel güncelleme işleminin otomatik olarak oluşturulan zaman damgasını kullanmak yerine, ilgili anahtarlama işleminin gerçek tarihini ve saatini sahaya manuel olarak girmesine izin verecektir. Ek olarak, operatör sahada anahtarı çalıştıran ekip üyesinin adını girebilecektir.

8) Bilgi Notu Ekleme

Operatör, trafo merkezinde bir şebeke elemanı seçerek trafo merkezi için bilgi notu yükleyebilir veya bir trafo merkezi için yüklenmiş olan bilgi notunu açabilir ve o anda yüklenen tüm bilgilerin olduğu ilgili ekranı açabilir. Her bilgi bir bağlantı olarak gösterilecektir; bağlantıya tıklandığında ilgili bilgi açılır. Bu ekrandaki özel düğmeleri kullanarak, operatör bir bilgi yükleyebilir veya listeden bir bilgi bağlantısını silebilir.

9) Şebeke Öğesi Bilgilerini Görüntüleme

Operatörün, şebeke elemanı için statik ve dinamik bilgileri görüntülemek üzere bir şebeke elemanı seçebilmesi mümkün olacaktır. Dinamik değerler sürekli güncellenecektir.

10) Yorumlar ve Notlar

I. SCADA/DMS/OMS, operatörün aşağıdakileri girmesini sağlayacaktır:

- Etiketler için yorumlar,
- SCADA GIS haritası için notlar,

II. Girilen notların, RealTime sunucu resetlenmesi esnasında ister dışı olarak toplu silinmesi ya da GIS importu esnasında karışması gibi durumlar önlenecektir.

III. Etiket ayarladıktan sonra yorum girme

Operatör söz konusu şebeke öğesiyle ilgili bir ekran açarak, istenen etiketi seçerek etiket için yorum girebilecektir.
Operatör, etiketli şebeke öğesinin bağlam menüsünü kullanarak etiketi kaldırabilecektir. Etiket için girilen yorum da otomatik olarak silinecektir.

IV. SCADA GIS Haritası için Not Girme

notlar, bir şebeke diyagramına eklenebilecek metinler ve ekler olacaktır. Bu amaçla, bir SCADA GIS haritasının bağlam menüsü, notların oluşturulması, düzenlenmesi ve silinmesi için girişler sağlayacaktır.
Operatör SCADA GIS haritasının bağlam menüsünde ilgili öğeyi seçtikten sonra, not metnini girmek için bir ekran açılacaktır.
bir notun girilmesi veya silinmesi Genel Özet'e kaydedilecektir.

V. Not Alma

Tüm free notların bir listesini sağlanacaktır. Özel bir düğme seçerek, operatör free notu içeren ilgili SCADA GIS haritasını çağırabilecektir. SCADA GIS haritasındaki notun bağlam menüsü, not metnini okumak için bir ekran açmak ve notu silmek için girişler sağlayacaktır.

VI. Anımsatıcı Tanımlama

Etiketler ve izinler için olduğu gibi, free bir not için de bir hatırlatmanın tanımlanması mümkün olacaktır.

11) Anahtarlama Dizileri

I. Operatör tarafından tanımlanabilecek iki (2) tip anahtarlama sırası olmalıdır:

- Şebeke kontrol komutları,
- Süreç kontrollü işler,

II. Şebeke kontrol komutları

Şebekenin özel alanları için, operatör tarafından seçilen bir komutun otomatik olarak bölgeye özgü komutlarla değiştirileceğini yapılandırmak mümkün olacaktır. Bu amaçla, operatör anahtarlama adımlarının sırasını içeren bir şebeke kontrol emri tanımlayabilecektir.

III. **Süreç kontrollü işler**
Süreç kontrollü bir iş, belirli bir durum değişikliği meydana geldiğinde, bir zaman çizelgesine göre veya manuel olarak yürütülen bir dizi anahtarlama adımı olacaktır.

10.11 DMS Fonksiyonları

10.11.1 Genel

a) SCADA/DMS/OMS 'in Dağıtım Şebekesi Uygulamaları, Dağıtım şebekesinin gözlemlenebilirliğini arttıracak ve kullanıcıya mevcut şebeke durumunun kapsamlı bir gerçek zamanlı görünümünü sağlayacaktır.

b) Elemanlar veya bölgeler için arıza koşullarını otomatik olarak tespit eder ve etkilenen alanların optimal restorasyonunu hakkında öneriler verir ve kullanıcı kontrolünde hızlı uygulama imkânı sağlar.

c) DMS Modüllerinin kendilerinden beklendiği şekilde çalışabilmesi için, şebeke elemanları için gerekli veriler ve öz nitelik verileri GIS ve SAP entegrasyonu ile sağlanacaktır. Bununla birlikte GIS ve SAP entegrasyonu dışında gerekli bilgilerin entegre edilebilmesi ve manuel de girişi mümkün olacaktır. DMS modüllerinin etkin çalışabilmesi için gerekli şebeke verilerinin SCADA/DMS/OMS Sistemine aktarılması YÜKLENİCİ kapsamında olacaktır.

d) Dağıtım şebekesinin mevcut durumunun yük akışının tam ve tutarlı bir şekilde hesaplanmasını sağlayacaktır.

e) Burada ilgili analizler çalıştırıldığında hatanın neden kaynaklı olduğunun raporlanabilir olmalıdır.

f) Sözleşme gücü, aylık ve yıllık tüketim, yük profili gibi veriler GIS ve SAP entegrasyonları ile alınacaktır.

g) Çalışma modunda operasyonel planlama yapabilmeyi destekleyecektir. DMS, artan dağıtım şebekesi güvenilirliğini ve verimliliğini desteklemek için kapsamlı bir uygulama paketi sağlayacaktır:

I. Arıza Bulucu (FLO),

II. İzolasyon ve Restorasyon (I&R),

III. Dağıtım Sistemi Güç Akışı

10.11.2 Arıza Yönetimi

Arıza Tespit Yönetimi, sistem olaylarını tespit etmek ve dağıtım şebekelerinde arıza (veya planlı kesinti) izolasyonu ve restorasyonu sağlamak için kullanılacaktır.

Arıza Tespit Yönetimi işlevselliği şunlardan oluşacaktır:

a) Arıza Bulucu (FLO)

Arıza Bulucu, Arıza Yönetimi uygulamasının bir parçası olarak, kalıcı arızaların bulunmasına yardımcı olacaktır ve arızalar dikkate alınacaktır. Arıza tespiti, örneğin koruma cihazlarından ve arıza göstergelerinden uzaktan kontrol edilen ve manuel olarak güncellenen bilgiler kullanılarak gerçekleştirilecektir. Arıza bulucu, SCADA ve/veya saha ekipmanlarından gelen mevcut gerçek zamanlı verilere dayanarak arızalı bölümü mümkün olduğunca yakın bir şekilde belirleyecektir.

b) İzolasyon ve Restorasyon (I&R)

İzolasyon fonksiyonu, şebekenin bir alanını izole etmek için bir dizi anahtarlama işlemini belirlemek için gerçekleştirilecektir. Arızalı ekipmanın veya alanın konumlandırılmasıyla veya doğrudan kullanıcı arayüzünde bölümler seçilerek fonksiyon başlatılacaktır. Arıza izolasyonu sırasında, araç, şebekenin & hattın enerjisi kesilmiş arızalı olmayan alanlarına enerji hizmetini geri beslemek için bir dizi anahtarlama işlemi tanımlamak adına kullanılmalıdır. Amaç, şebeke üzerindeki kesinti etkisini en aza indirmek için izole isteği ile belirtilen şebekenin ya da fiderin bölümlerini veya alanlarını izole etmektir. I&R'nin bakım çalışmaları nedeniyle ekipmanların ya da alanın izolasyonu için de kullanılması mümkün olacaktır.

10.11.3 Dağıtım Sistemi Güç Akışı

a) Dağıtım Sistemi Güç Akışı (DSPF) fonksiyonu, sahadan gelen ölçümleri, kullanıcı tarafından belirlenmiş ve atanmış yük tiplerini ve anlık topoloji verilerini kullanarak sistemin her noktasındaki akım, voltaj, aktif/reaktif güç ve diğer güç verilerini hesaplamalıdır.

b) DSPF fonksiyonu aşağıdaki işlevleri yerine getirebilir olmalıdır.

I. Gerçek zamanlı mod, o andaki ölçümler ve anahtar durumları için çalışacaktır.

II. Gerçek zamanlı modda simüle edilmiş (O andaki geçerli anahtar durumlarını ve kullanıcı tarafından değiştirilen saha ölçüm değerleri için çalışacaktır.)

III. Eğitim modu (Bu modda tamamen kullanıcının belirlediği koşullarda çalışacaktır. Belli bir anda gerçek sistem veri tabanına kopyalanacak, kullanıcı bu kopya üzerinde istediği gibi oynayıp ilerde gerçekleşmesi muhtemel bazı senaryoları simüle edebilecektir.)

c) Ana Güç Akışı Aşağıdaki Özellikleri sunacaktır.

I. Radyal, döngülü ve ring topolojide simetrik dengeli güç akışı,

II. Dengeli uyumlu yükler ve yük-gerilim bağımlılığı,

III. Kademe değiştiricilerin ve şöntlerin (kapasitör ve reaktörlerin) çok fazlı yerel kontrolünün yapılması,

IV. Kontrollü PQ ve PV jeneratörlerini desteklemeli,

V. İsteğe bağlı olarak eklenen jumper ile şebekeyi hesaplamalı,

d) Güç akışı, anahtarlama işlemini gerçekleştirmeden önce, anahtarlama işleminin dağıtım şebekesi üzerindeki etkisi hakkında bir ön izleme sağlayacaktır.

10.12 Kesinti Yönetimi Sistemi

10.12.1 Genel

1) Kesinti Yönetimi Sistemi EK-2.5.Tedarik Sürekliliği Kayıt Sistemi Kuruluna ve Entegrasyonuna İlişkin Yükümlülükler EK-1 e tam uyumlu olacaktır.
2) Sistem tüm regülatif değişimleri sağlayabilecek standartta tasarlanacaktır.
3) Kesinti Yönetimi (OMS), bir operatörün veya kullanıcının, elektrik şebekesinde meydana gelen kesintilerin tespitini, konumunu, izolasyonunu, düzeltilmesini ve restorasyonunu yönetmek için kullandığı fonksiyon, araçlar ve prosedürlerden oluşan bir sistemdir.
4) OMS ayrıca, şebeke için planlanan kesintilerin hazırlanmasını, anahtarlama prosedürün işletilmesi ve sürecin yönetilmesini sağlayacaktır.
5) OMS süreçleri, şebekeyi etkileyen kesintilerin ele alınmasıyla ilgili görevlerin yerine getirilmesini hızlandırmak ve bir çağrı kaydı alınması veya bir kesintinin SCADA göstergesi gibi olaylardan başlayarak, tüm müşterilere güç sağlanana kadar kesinti yaşam döngüsünün tüm aşamalarında operatörlere destek sağlamak için kullanılacaktır.
6) Kesinti bazında, kesinti noktasından o an beslendiği kaynağa kadar izlenen şebeke modeli raporlanabilir olmalıdır.
7) OMS süreçleri ayrıca, kesintinin müşteriye güç sağlayan tek bir şebeke bağlantı noktası düzeyinde mi yoksa birçok enerji tüketicisine enerji sağlayan şebeke kaynağı noktaları (BİNA, SDK KOLU, SDK, AG KOL, TRAFO, HAT BÖLÜCÜLER, DM, IM) düzeyinde mi olduğunu çözmek için kullanılacaktır.
8) Bu süreçlerde meydana gelen tüm işlemler, yetkilendirmeler ve yorumlar belgelenecek ve kesinti kayıtlarında toplanacaktır. Bu bilgilerin, daha ileri istatistiksel analiz ve işleme için harici sistem ya da entegrasyonlara sunulması mümkün olacaktır.
9) OMS, şebekedeki değişiklikleri izlemek için kullanılan bir kesinti kaydının otomatik olarak işlenmesini sağlayacaktır. Dış uygulamalarla veri iletişimi, çerçevesinde web hizmeti bağdaştırıcıları aracılığıyla etkinleştirilecektir. Harici sistemlerle veri alışverişi, OMS çözümünün önemli bir parçası olacaktır. Bunun için web arayüzleri, Müşteri İlişkileri Yönetimi, İş Gücü Yönetimi ve OSOS gibi dış sistemlere önemli OMS verilerini alacak veya sağlayacaktır.
10) Eşik süre sayı bilgisi, planlı kesinti eşik bilgisi gibi cezai koşullar konusunda uyarabilecek sistem eklenecektir.
11) Kesintiler kademeli şekilde saha ekibinden gelen bilgiye göre kapatılabilecek, kademe kesintilerin şebeke unsurları, etkilenen trafo bölgesi ve abone sayıları her bir kademe için ayrı ayrı raporlanabilecek ve sistem üzerinde arşivlenebilecektir.
12) Planlanmamış kesintiler için OMS, bir şebekedeki fazdan faza veya fazdan toprağa kesintiler ve OMS tarafından iletilen ve toplanan verileri ile ele alacaktır:

I. Müşterilerden gelen çağrı kayıtları,
II. Akıllı sayaçlardan enerji var/yok sinyalleri,
III. Anahtarlardan telemetreli durum değişikliği göstergeleri,
IV. Manuel anahtar işlemleriyle güncellemeler

13) Planlı kesintiler için OMS , toplanan veriler ile birlikte ele alınacaktır:

I. Müşterilerden gelen çağrı kayıtları,
II. Akıllı sayaçlardan enerji var/yok sinyalleri,

III. Anahtarlardan telemetreli durum değişikliği göstergeleri,

IV. Manuel anahtar işlemleriyle güncellemeler

14) OMS tarafından desteklenen süreç aşağıdaki adımları içermelidir:

I. Kesinti tespiti ve/veya kesinti kaydı oluşturma,

II. Enerjilendirme,

III. Kesinti kaydı arşivleme,

15) OMS, müşteri çağrıları, OSOS verisi, şebeke arızalarına ait sinyal/durum/verilere dayanan her kesintiyi tahmin etmek ve oluşturmak için gerçek zamanlı OG ve AG topoloji modelini kullanacaktır. Kesinti tahmini kaynağa kadar gidebilmeli ayrıca kesinti noktası ekip tabletleri tarafından aşağı ve yukarı yönlü taşınabilmelidir.

16) OMS; ilgili algoritmaları çalıştırılarak kesinti çağrılarını şebeke unsurlarındaki kesintilerin tahmin edilmesi için gruplayacaktır. Çağrı gruplaması ve de tahmin algoritması çıktısı olarak otomatik olay oluşturulması yeteneği en az şu çözünürlük ve detayları içerecektir: TEİAŞ Merkezleri, TM Fideri, DM/İM/KÖK istasyonları, OG Fideri, Dağıtım Transformatörü, AG Fideri, Saha Dağıtım Kutusu (SDK), SDK Çıkışı, AG Direği, Abone Tesisi, Bina, Tek Müşteri. Teklif Sahipleri, OMS uygulamasının arıza yeri tespit algoritması ve otomatik olay yaratılması ile ilgili olarak tanımlanan gereksinimleri nasıl karşılayacağı ile ilgili detaylı açıklamalar sunacaktır.

17) Kesinti Yönetiminde kesinti içerisinde yapılan her türlü işlem kaydı(ŞİRKET tarafından belirlenecektir) kullanıcı bilgileriyle birlikte zaman bazlı loglanacaktır,

18) Tahmini Enerjilendirme Süresi (ETR)

a) Sistem, bir kesinti için Tahmini Enerjilendirme Süresini hesaplayacak ve görüntüleyecektir. Her kesinti için ETR değeri, kesinti önceliği, ekip tarafından kullanılabilirliği ve iş yükü gibi girdilere veya etkilenen bölgedeki aktif bir fırtına gibi diğer etkileyici faktörlere dayanarak dinamik olarak oluşturulacaktır. OMS operatörü, ETR değerini görüntüleyebilmeli ve inceleyebilmelidir. Operatör otomatik ETR hesaplamalarını açıp kapatabilecektir. Otomatik ETR hesaplaması devre dışı bırakıldığında, operatör manuel ETR değerlerini girmeye devam edebilecektir. WFM Entegrasyonu ile Saha ekiplerinin veri girişi ile tahmini enerjilendirme süresi değiştirilebilecektir.

b) OMS ile ilgili olaylar, örneğin yeni gelen kesintiler, kesinti önceliğindeki değişiklikler, öngörülen kesinti konumundaki değişiklikler veya ETR sona ermesi, uyarılar, alarmlar veya bildirimlerle operatör tarafından takip edilebilir olacaktır.

c) Planlı ve Plansız kesintilerde ETR ve ilgili kesintiye ait etkilenen abone listesi CRM tarafına anlık veri gönderebilecek şekilde olacaktır.

d) Kesinti olan noktada, bölgeyi enerjilendirmek için gereken anahtarlama adımları, gerekli şebeke güvenliğini göz önünde bulundurarak (topraklı ya da enerjili hattı besleme vb. durumuna yönelik uyarı oluşturma) anahtarlama prosedürü kullanılmalıdır. Anahtarlama prosedürünün sonuçları ve gerekli operatör yorumları kesinti kaydının bir parçası haline gelecektir. Etiket yapısı olmalıdır. Bu etiketler uyarı ve iş güvenliği için

kullanılabilir olmalıdır. Örneğin toprak ayırıcısı kapatıldığında SCADA'da toprak ayırıcısı kapalı ikonu harita üzerinde gösterilmelidir.

e) Bir kesinti enerjilendirildikten sonra (restore edildikten ve iş tamamlandıktan sonra), karantina durumunda kabul edilecektir.
f) Karantina süresi sona erdikten sonra, kesintiler otomatik olarak kapatılacak ve bunlarla ilişkili herhangi bir anahtarlama prosedürü de dahil olmak üzere tüm destekleyici verilerle birlikte arşivlenecektir. Karantina süresi ŞİRKETİN belirleyeceği zaman dilimini kapsayacaktır.

g) ŞİRKET, arşivlenmiş kesinti kayıtlarını görüntüleyebilecek ve değişiklik yapabilecektir.

h) Arşivlenen verilerin arşivden çıkartılıp düzenleme / değişikliğe izin vermemesi durumunda ise ŞİRKETİN belirleyeceği zaman dilimine kadar kesinti kayıtları karantina süresi aşamasında saklanabilecektir.

i) Şebeke topolojisinde bir anahtarın durumu değiştiğinde analiz yürütülür. Durum değişikliğinin manuel bir değişiklik mi yoksa telemetreli bir değişiklik mi olduğu bu durum söz konusu olacaktır. Topoloji analizi, şebeke bağlantı noktasının mevcut enerjilendirme durumunu önceki durumlarıyla karşılaştırmalıdır.
j) Bir şebeke bağlantı noktası enerjilendirilmiş bir durumdan enerjisiz bir duruma değiştiyse, bir kesinti meydana gelmiştir. Topoloji analizi, değişiklikleri değerlendirmeli ve etkilenen yük unsurları ve anahtarları tanımlamalıdır. Topoloji analizinden alınan verilere dayanarak, OMS ya yeni bir kesinti kaydı oluşturacak ya da verileri mevcut bir kesinti kaydına ekleyecektir.

10.12.2 Kesinti Yönetimi

1) Bağlantı Noktası Bilinmeyen Çağrılar

OMS içinde, şebeke ile ilişkilendirilemeyen, ancak bir tür sorun özelliği olan her türlü çağrıların operatörün takdirine ve şikâyete bağlı olarak diğer olaylara veya servis noktalarına veya şebeke bağlantı noktalarına göre gruplandırılması mümkün olacaktır. Herhangi bir iş emri/kesinti ile eşleştirilemeyen bu ihbarları operatör kesinti kaydına dönüştürebilir olacaktır. Bunun için şebekede anahtar, kesik atma gibi bir işlemle kesinti oluşturularak kesinti içine dahil edilmelidir. Oluşturulan tüm kesintiler şebeke ile bir objeyle ilişkilendirilmelidir. Ayrıca kavramsal tasarım dokümanı hazırlama sürecinde belirlenecek metodoloji ile bu çağrıların kesinti kayıtlarına otomatik atanması sağlanacaktır.

2) Planlı/Plansız İş Kayıtları

Bir kesinti kaydı en az aşağıdaki bilgileri içermelidir:

a) Kesintiyi tanımlayan üstbilgi,

b) Kesinti durumu ve kesinti yeri, etkilenen müşteri sayısı, etkilenen dağıtım trafoları, etkilenen mahalle bilgisi, dağıtılamayan enerji veya beklenen restorasyon süresi, anlık etkilenen müşteri sayısı gibi temel karakteristik değerler hakkında temel bir genel bakış sağlayacaktır.

c) Kesintinin SAIDI SAIFI etkisi

d) SMS ve Mail prosedürleri belirlenerek talebe göre değiştirilebilir farklı algoritmalar çerçevesinde kesinti bilgisi, etkilenen abone bilgisi, VIP abone bilgisi gönderilecektir. Şirket tarafından belirlenecek prosedürlere göre kesinti bilgisi SMS ve mail yoluyla bilgilendirilebilir olmalıdır.

3) Şebeke Etkisi

OMS, her anahtar durumu değişikliğinin, etkilenen yük objelerinin ve etkilenen dağıtım trafoları zaman damgasını otomatik olarak saklayacaktır. Enerjilendirmeden sonra, etkilenen her yük objesi ve dağıtım trafosu için enerjilendirme süresi de otomatik olarak saklanmalıdır. OMS sistemi web tabanlı izlenebilir ve planlı kesintiler bu sistem üzerinden tetiklenebilir olmasına imkan sağlayan arayüz olmalıdır. Kesinti bazlı kesinti noktasından o an beslendiği kaynağa kadar izlenen şebeke modeli raporlanabilir olmalıdır.

4) Kesinti Çağrıları

Kesinti kaydına atanan kesinti çağrıları listelenir olacaktır.

5) Görevler ve Ekip

İş emrine atanan saha ekibi ve araç bilgisi görüntülenebilecektir.

6) Anahtar İşlemleri

a) Ekipmanın enerjisinin kesilmesine veya yeniden enerjilendirilmesine neden olan Şebeke modeli anahtarlama eylemleri sağlanacaktır. Manuel güncelleme için, enerjilendirme süresinin gerçek anahtarlama süresini karşılayacak şekilde düzeltilebilmesi mümkün olacaktır. Anahtar işlemleri ile kesinti kaydını eşleştirmek mümkün olacaktır.

b) Anahtarlama işlemleri ayrıca WFM sistemi üzerinden de gelmektedir. Bu tip hatalı anahtarlamaların düzeltilebilmesi için ŞİRKET ile YÜKLENİCİ kavramsal tasarım sürecinde bir yöntem belirleyip uygulayacaktır. (Örneğin Saha ekipleri kesintili iş emirleri için tabletlerine gönderilen kesinti ekipmanını onaylayabilecek ya da yeni kesinti ekipmanına ait anahtarlama yapabilecektir. Bu anahtarlama sadece aynı topolojiye sahip hat için geçerli olacaktır.)

7) Anahtarlama Prosedürleri

a) Güvenlik Kontrollü Anahtarlama/ Anahtarlama Doğrulama uygulaması, anahtarlama eylemleri gerçekleştirilmeden önce sonuçlarının gözlemlenmesine izin verecektir ve anahtarlama eylemleri limit ihlallerine yol açacaksa alarm veya uyarı oluşturacaktır.

b) Bu uygulama anahtarlama eylemlerini operasyonel gereksinimlere ve güvenli anahtarlama prosedürlerine göre kontrol edecektir ve anahtarlama eylemlerini onaylayacaktır.

c) Anahtarlama sırası gerçek zaman ya da çalışma modunda koşturulabilecektir. Çalışma modu; anahtarlama işlemlerinin dağıtım şebekesi üzerindeki potansiyel etkilerini, uygulanmadan önce operatörler tarafından belirlenmesini sağlayacaktır.

d) SCADA/DMS/OMS, anahtarlama prosedürünün herhangi bir adımında DPF'in çalışma modunda koşarak sistemdeki olası etkilerin belirlenmesini sağlayacaktır.

e) Uygulama; anahtarlama işlemleri için ilgili kuralların oluşturulmasına olanak tanıyacaktır. Uygulanacak bu kurallar güvenlik kitlemeleriyle birlikte diğer genel operasyonel ilkeleri içerecektir.

f) Güvenlik Kontrollü Anahtarlama/ Anahtarlama Doğrulama uygulaması, anahtarlama emri oluşturulma sürecini kolaylaştırmak için normal işletme prosedürlerini içerecektir (örneğin topraklama ile ilgili kurallar).

g) Uygulama her anahtarlama eyleminin sonuçlarını bir anahtarlama sırası içinde hesaplayacaktır ve sonuçları şebeke diyagramları üzerinde sunacaktır. Şebeke diyagramları üzerindeki limit ihlalleri için uygun alarmlar veya uyarılar oluşturulacaktır.

h) Bu uygulamanın gerçekleştirilmesi gerçek zamanlı operasyonları etkilemeyecektir.

i) Kesinti kaydı ile ilgili anahtarlama prosedürleri ve kuralları YÜKLENİCİ ile kavramsalda detaylandırılacaktır.

8) Müşteri Bağlantı Noktası

a) Etkilenen tüm Müşteri bağlantı noktalarının listesi arayüzden görüntülenebilir olacaktır. Şebekenin bir kısmı kısmen enerjilendiğinde, Müşterilerin enerjilendirme durumu buna göre güncellenecek ve buna göre şebeke topolojisi renklendirilecektir.
b) Her müşteri için ilgili -varsa- akıllı sayacın enerji durumu gösterilecek ve müşteri tarafında enerji var/yok bilgisini OSOS' dan anlık sorgulama işlevini sağlayacaktır. OSOS sisteminden alınan enerji var yok bilgisinin tarih ve saati çağrı kaydının içine getirilecektir.
c) Planlı İşin yürütülmesinden etkilenecek Planlı İş için müşteri listesini oluşturmak mümkün olacaktır. Planlı kesintilerde anahtarlama prosedürü oluşturulabilecek, müşterinin etkilendiği toplam kesinti miktari ve tazminat bedeli görülebilir olacaktır.

9) Arıza Noktası Kayıtları

Kesintiye neden olan ekipman kesinti bilgi ekranında gösterilecektir. Sorunun nedeni ile ilgili bu bilgiler, otomatik olarak entegrasyon ve raporlamalara iletilebilecektir. Saha ekibi veri girişiyle entegre olarak revize edilebilir olacaktır.

10) Kesinti Kaydı Ekleri

Kesintinin içine gerekli veriyi iliştirebilmek için mevzuat kapsamında istenen tüm dokümanlar eklenebilecektir.

11) Sinyaller

Akıllı sayaçlardan türetilen sinyaller, örneğin enerji var/yok olayları, burada listelenebilecektir.

12) Değişiklik geçmişi

Kesinti Kaydı değişiklik geçmişi olmalıdır. Detayları kavramsalda belirlenecektir.

13) Kesinti Tahmini

a) OMS tahmin işlemesi, farklı kaynaklardan gelen çağrılarının değerlendirilmesini sağlayacak ve şebeke teknolojik adresiyle ilişki kurabilecektir.
b) OMS'nin önemli bir bileşeni olacak ve gelen çağrı kayıtlarını işlemek ve kesinti kayıtlarını oluşturmak için farklı modüllerden oluşacaktır. Diğer bir deyişle, çağrılar

gruplandırılmalı ve yapılandırılabilir kurallara dayalı olarak tahmin edilen bir kesinti olayıyla ilişkilendirilecektir. Çağrı kayıtları manuel olarak veya Müşteri Bilgi Sistemi (CRM), İnteraktif Sesli Yanıt (IVR), OSOS gibi harici uygulamalar veya kurumsal web siteleri tarafından oluşturulacaktır. Tahmin kuralları yapılandırılabilir olmalıdır (kuralların eklenmesi, değiştirilmesi ve silinmesi). Kuralların Kontrol Alanı ve olay moduna (normal mod ve kriz modu) göre gruplandırılması mümkün olmalıdır.

c) Kesinti Tahmini, Alçak Gerilim Şebekesi için de çalışmalıdır. Kesinti tahminin kaynağa kadar gidebilmesi, bunun yanında kesinti noktası ekip ve/veya oporatör tarafından aşağı veya yukarıya taşınabilir nitelikte olmalıdır.
d) Çağrı kaydının bir parçası olarak gönderilen bilgilere ve veri tabanında önceden var olan müşteri ve ekipman verilerine dayanarak, OMS tahmin işlemi farklı kaynaklardan gelen çağrıları değerlendirecek ve bu çağrıları bir servis noktası ve ilgili üst nokta şebeke modeli ilişkilendirecektir.
e) Kesinti tahmin kurallarının ve parametrelerinin OMS' deki belirli bir Tahmin Kuralları mühendisliği kullanıcı arayüzünde kolayca yapılandırılması ve uyarlanması mümkün olmalıdır.
f) Tahmini sıfırlamak ve seçilen bir besleyicinin veya tüm şebekenin yeniden tahmin edilmesini tetiklemek mümkün olacaktır.
g) Kesinti tahminleme mantığını YÜKLENİCİ teklif dokümanında sunmalıdır.

14) Kriz Modu

a) Birçok kesintinin mümkün olduğu veya halihazırda devam etmekte olduğu belirli yoğun koşullar (örneğin, aşırı hava koşulları) sırasında, operatörün rehberliğe ve en önemli olaylara odaklanmasına ihtiyacı vardır. OMS hem müşterilerden hem de akıllı sayaçlardan gelen çok sayıda kaydı işleme olanağı sağlayacaktır.
b) Özel bir Kriz Modu kullanıcı arayüzü ile operatörler, sisteme giren yüksek konsantrasyonda çağrıların beklentisine veya mevcut senaryosuna dayanarak, sistemin çeşitli kriz modu olaylarını ve türlerini listelemesini kullanarak dağıtılmış kriz alanlarını kolayca önceden tanımlayabilecektir. Kriz Modu, kriz derecesine bağlı olarak dağıtım şebekesinin bazı kısımları veya tüm sistem için yapılandırılabilir.
c) Kriz Modunun etkinleştirilmesi, OMS tahmin işlemine kriz durumlarında kullanılan bir dizi kural parametresine geçme isteğiyle sonuçlanır. Bu parametreler kullanıcı tarafından (Admin) kontrol edilebilir olacaktır.
d) Sistem, saha ekibinin uygunluğu ve vardiya planları, arıza değerlendirme bilgileri ve kesinti öncelikleri gibi etkileyen faktörleri dinamik olarak göz önünde bulundurarak, krizle ilgili tüm kesintilerin ne zaman geri yüklendiğini operatöre göstermek için krize özgü bir ETR hesaplayacak ve görüntüleyecektir.
e) Bir kriz sırasında meydana gelen tüm çağrıların, kesintilerin ve etkinliklerin kriz modu özet ekranında kolayca gözden geçirilmesi mümkün olacaktır.

15) İç İçe Kesintileri Algılama

Bir kesinti tamamlandıktan ve müşterilere enerji verildikten sonra, iç içe kesintilerde aynı müşterinin 2 kesintinin parçası olarak 2 kez kesinti raporlarında bulunmaması sağlanacaktır.

16) Enerji Var/Yok Sorgulama

a) Müşterilerin enerjilendi durumunu belirlemek için başka bir seçenek, İnteraktif Sesli Yanıt (IVR) sistemi veya Müşteri Bilgi Sistemi ile entegrasyonudur. Bir sayacın enerjilenme doğrulaması Kesinti Yönetimi bir IVR / Müşteri Bilgi Sistemi kullanarak bir geri arama isteği göndermeyi destekleyecektir. Kesinti Yönetimi operatörü, Kesinti Kaydı ekranından gelen talebi tetikleyebilecektir. Kesinti Yönetimi, entegrasyon servisi üzerinden IVR/CRM sistemlerine mesaj gönderecektir. Gelen sonuca istinaden gerekli aksiyonu alabilir olacaktır. Detaylar Kavramsalda belirlenecektir.

b) OSOS ile, enerji var yok durumunu doğrulamak için müşterilerin modemlerine ping atma isteği gönderilebilir olacaktır. Belirlenen süre içerisinde osos sinyali tek müşteriden gelmişse öncelikle otomatik ping isteği atılacak ve otomatik IVR / CIS sistemi kullanarak bir geri arama isteği göndermeyi destekleyecektir.

10.12.3 Kesinti Analitik Ekranlar

1) Genel

a) OMS, ŞİRKET' in işletme veya yönetici personelini destekleyen çeşitli grafik veya tablolar bulunduran bir arayüze sahip olacaktır.

b) Örneğin, aşağıdaki bilgiler bu ekranlarda sunulmalıdır:

I. Özet bilgiler, kesintiler, saha ekipleri, Çağrı kaydı veya performans göstergeleri ile ilgili gerçek zamanlı veriler ile Kesinti Yönetimine Genel Bakış görselleştirilebilecektir.

II. Anlık enerjisi kesilmiş tüm dağıtım trafolarını (kurum-özel) listeleyen tablosal ekranlar.

III. Anlık enerjisi kesilmiş mahalle/köy/ilçe bilgilerini listeleyen tablolu ekranlar

IV. Anlık enerjisi kesilmiş tüm müşteri listeleyen tablolu ekranlar.

V. Her müşteri için kesinti ve sorun çağrısı geçmişini gösteren müşteri odaklı ekranlar.

VI. Besleme noktalarının geçmiş kesintilerini gösteren tablolar (besleyici, trafo merkezi, transformatör vb. başına)

c) Kullanıcıya özel ekranları tanımlamak ve kaydetmek mümkün olacaktır. OMS operatörünün ekranları tercihlerine göre kolayca önceden tanımlayabilmesi, sütunları ayarlayabilmesi, çoklu seçim yapabilmesi, filtreleme ve sıralama kriterleri uygulayabilmesi ve ekranları bir sonraki girişte ayarların geri yüklenmesi için kaydedebilmesi mümkün olacaktır.

2) Rapor

OMS' te oluşan veriler, sistemde mevcut olan PRISM, PowerBI uygulamaları ile rapor oluşturabilir olmalıdır.

3) Çoklu Bölge Ataması

Veriler anlık oturum açmış olan operatöre yetki durumuna göre ve kullanılan konsola atanan bölgeler için görünür olacaktır.

10.12.4 Kullanıcı Arayüzü

1) OMS Kullanıcı Arayüzü

OMS, dağıtıcının veya operatörün farklı pencerelerde aynı anda çeşitli bilgi türlerini görüntülemesini sağlayan pencere arayüzleri kullanacaktır. OMS kullanıcı arayüzü açılır menülerle kullanılabilir olmalıdır.
OMS kullanıcı arayüzü en az aşağıdakileri içerecektir.

a) OMS Genel Bakış Ekranı

OMS Genel Bakış Ekranı, tüm OMS kayıtlarının başlıklarını gösterecek (çıktı filtreleme mümkün olacaktır) ve kullanıcının birçok kesinti kaydını hızlı bir şekilde gözden geçirmesine olanak tanıyan özet bilgiler sağlayacaktır. Ekran, OMS kayıtlarını yönetmek için kullanılacaktır.
Bu ekranlarda bulunacak alanlar kavramsal tasarım dokümanında ŞİRKET'in onayı alınarak oluşturulacaktır.

b) Kesinti Ekranı

Kesinti Ekranı, kullanıcının söz konusu kesinti ile ilgili ayrıntılı bilgileri görüntülemesine ve düzenlemesine olanak tanıyan bir arayüz sağlayacaktır. Bu ekranlarda bulunacak alanlar kavramsal tasarım dokümanında ŞİRKET'in onayı alınarak oluşturulacaktır.

c) Planlı İş Ekranı

Planlı İş Ekranı, kullanıcının belirli bir planlı kesinti ile ilgili ayrıntılı bilgileri görüntülemesine ve düzenlemesine izin verecektir. Bu ekranlarda bulunacak alanlar kavramsal tasarım dokümanında ŞİRKET'in onayı alınarak oluşturulacaktır.

d) Kriz Yönetimi Ekranı

Kriz Yönetimi Ekranı, belirli bir kriz durumunun, kriz alanının, küresel krize özgü ETR'nin ve restorasyon durumunun verilerini gösterecektir.
Kesintiler, çağrı kayıtları ve sayaç olayları (örneğin, akıllı sayaçların son canlı sinyali) otomatik olarak ilgili kriz ile ilişkilendirilecek ve kullanıcı arayüzünde görüntülenecektir.

e) OMS Arşivi

OMS Arşivi, kayıtları arşiv veri tabanında raporlayabilir/listeleyebilir olacaktır. Bu kayıtların düzenlenmesi yetki verilmiş kullanıcıların haricinde yasaklanmalıdır.

f) SCADA GIS Haritasındaki Kesinti Bilgileri

Coğrafi veya şematik haritalarında, saha ekibi konumu, kesintiler, müşteri çağrıları, hasar kayıtları ve acil durum müşterileri gibi bilgileri görüntülemek için kesinti yönetimi ile ilgili katmanların açılabilmesi mümkün olacaktır.
Simgeler coğrafi konumu gösterecektir. Simgeye tıklandığında, özet bilgileri görüntüleyebilecektir.

10.12.5 Entegrasyon Arayüzleri

1) Genel

a. SCADA/DMS/OMS' in entegrasyonları web servise dayanarak operasyonel verimliliği ve güvenilirliği artıran kesinti yönetimi ile ilgili verilerin değişimi için Müşteri Bilgi

Sistemi (CRM) / İnteraktif Sesli Yanıt (IVR), Otomatik Araç/Tablet Konumu ve Sayaç Veri Yönetimi (OSOS), İş gücü Yönetimi WFM (Sentinel), TEDAŞ Talep Takip, EDVARS gibi harici sistemlerle çeşitli entegrasyonlar sağlayacaktır.

b. OMS, aşağıdaki harici uygulamalarla veri alışverişi için aşağıdaki Arayüzleri sağlayacaktır:

I. Sayaç durumunu kontrol etme,
II. Sayaç olayları hakkında bilgi gönderme,
III. OMS'den OSOS'ye kesinti bilgileri gönderme (kesinti durumu, ETR),
IV. Saha ekibi ve kişi verileri,
V. Kesinti ve görev bilgileri,
VI. Anahtarlama prosedürleri ve anahtarlama talimatları,
VII. Müşteri Bilgi Sistemi,
VIII. Çağrı Kayıtları,
IX. Kesinti bildirimleri,
X. Otomatik Araç/Tablet Konumlandırma Sistemi,
XI. Ekip durumları,
XII. Saha ekibi veya araç verileri,
XIII. Varlık Yönetim Sistemi,
XIV. İş talepleri,

10.12.6 OMS Çağrı Kaydı Yönetimi

1) Genel

a) Çağrı Kaydı Yönetimi sahadaki sorunları bildiren müşteri telefon çağrı bilgilerini ve Sayaç Veri Yönetimi (OSOS) ve SCADA sisteminden gelen çağrı kayıtlarını kaydetmesi için bir arayüz sağlayacaktır. Kesinti tanımlama, izleme ve çözüm için OMS Kesinti Yönetiminin Tahmin İşleme gibi diğer araçlarla entegre çalışacaktır.
b) İnteraktif Sesli Yanıt (IVR), Müşteri Bilgi Sistemi , Sayaç Veri Yönetimi (OSOS) veya Kurumsal Web Siteleri gibi sorun çağrıları üreten harici sistemleri bağlamak için arayüz olanakları bulunacaktır. ŞİRKET tarafından harici sistemlere ait bilgiler kavramsalda belirtilecektir.

2) Çağrı Kaydı Oluşturma

a) Çağrı kayıtlarının entegrasyon ile otomatik olarak SCADA ya aktarılamadığı durumlarda Çağrı kaydı operatörü, bu ekrandan gelen çağrı için bir çağrı kaydı oluşturur.

b) Çağrı kaydı operatörünün, müşteri veri tabanındaki müşteri bilgilerini kolayca aramak ve bu bilgileri çağrı kaydına kopyalamak için bir arama işlevi kullanabilmesi mümkün olacaktır, örneğin:

I. Müşteri adresi,
II. Müşteri Adı-Soyadı
III. TC ve Vergi Numarası
IV. Müşteri iletişim bilgileri,
V. Hesap numarası (Tüketim Numarası, Muhatap Numarası vb.)
VI. Cihaz adı ve alanı,

c) Sayaç Veri Yönetimi arayüzü ile, operatörün doğrudan çağrı kaydından bir güç durumu doğrulama talebi başlatması mümkün olacaktır.
d) Operatör çağrı kaydını kaydettiğinde, çağrı kaydı bilgilerini OMS Tahmin İşleme' ye iletecektir. OMS tahmin işlemi, kesinti türünü ve önceliğini tahmin etmeli ve yeni bir kesinti kaydı oluşturmalıdır. Otomatik birleştirilemeyen / kesinti oluşturmayan çağrı kayıtlarını manuel olarak kesinti kaydına birleştirecek çözüm sunulacaktır.

e) Çağrı kaydı ekranında aşağıdaki bilgilerin gözden geçirilmesi mümkün olacaktır:

I. Kesinti kayıt numarası,
II. Kesinti durumu, (Saha ekibinin aksiyon durumu)
III. Kesinti oluşma türü (osos,tcall,scada,oms, crm),
IV. İhbar geliş Kanalı (ÇM, MHM, WEB, Mobil, TEDAŞ Mobil)
V. Kesinti türü (Planlı/Plansız)
VI. Kesinti nedeni
VII. Kesinti başlangıç saati ve süresi, (gün, ay, yıl, saat, dakika, saniye)
VIII. Tahmini Enerjilendirme Süresi (ETR),
IX. Çağrı kaydı ayrıntıları, (Açıklama, Yorumlar alanı, CRM ID)
X. Çağrı kaydı zamanı (gün, ay, yıl, saat, dakika, saniye)
XI. Çağrı kaydı durumu,
XII. Çağrı kaydı türü veya şikâyet türüyle ilgili ayrıntılar,
XIII. Çağrı kaydı önceliği,
XIV. Arayanın adı ve iletişim bilgileri,
XV. Ek arayan yorumları,
XVI. Bildirim isteği,

f) Çağrı kaydı operatörü, müşteri tarafından talep edildiği gibi veya operatörün takdirine bağlı olarak belirli bir olay durumunda bildirim çağrılarını işaretleyebilecektir. Bir çağrı kaydı bildirim için işaretlenirse, olay gerçekleştiğinde müşteriye otomatik bilgilendirme araması yapılabilmesi için gerekli entegrasyon bulunacaktır.

g) Kesintili olmayan ihbarlar için örneğin gerilim düşüklüğü ihbarı vb. bildirmesi durumunda, sistem bu bilgileri çağrı olarak saklama olanağı sağlayacaktır. Sistem operatörü bir çağrı kaydı oluşturabilecektir. Bu çağrı kayıtları için de operatör kesinti kaydı oluşturabilecektir. Detayları kavramsalda ŞİRKET ile değerlendirilecektir.

3) Kesinti Analizini Tetikleme

a) Bilgileri yeni oluşturulan bir çağrı kaydı girildikten veya harici bir sistemden servis ile çağrı kaydı bilgileri alındıktan sonra, kavramsalda belirlenecek kriterlere uygun olan çağrı kayıtları otomatik kesinti kaydı oluşturabilecektir. Kesintisiz olarak değerlendirilen ihbarlardan oluşan iş emirleri, operatör tarafından kesintili iş emrine dönüştürülebilecektir

b) Sayaç durumu bilgisi alınırsa (OSOS) bu bilgiler kesinti yönetimi tahmin işlemeye iletilecektir. Bu sinyaller kesinti oluşturabilecektir.

c) Kesintili olmayan ihbarlara Tahmin İşleme'yi tetiklemeyecekler, ancak operatör tarafından manuel olarak gruplandırılabilmeleri ve bir kesinti veya planlı bir işe atanabilmeleri mümkün olacaktır. Kesintiye atanmayan çağrılar bir kesintiye ihtiyaç duymadan saha ekiplerine iş emri olarak iletilebilmelidir.
d) Çağrı kaydı Yönetimi, Müşteri Bilgi Sistemi (CRM) veya İnteraktif Sesli Yanıt (IVR) gibi harici sistemlerle entegrasyon sağlayacaktır. Detaylar kavramsalda ŞİRKET ile belirlenecektir.

4) Çağrı Kaydı Yönetimi Kullanıcı Arayüzü

a) Genel

I. Mevcut tüm çağrı kaydının başlıkları bir tabloda gösterilecektir.
II. Bu ekran, sorumlu çağrı operatörünün aşağıdaki işlemleri gerçekleştirmesini sağlayacaktır:

- Bir çağrı kaydı oluşturulabilmesi, görüntüleyebilmesi ve değiştirebilmesi,
- Çağrı kaydıyla ilişkili kesinti için bir Kesinti Ayrıntıları Ekranı açılması.
- Çağrı kaydını filtreleme,
- Çağrı kayıtlarında çoklu seçim yapabilme veya birleşmeyen hatalı birleşen çağrı kayıtlarına manuel müdahale edebilecek çözüm sunmak.
- Çağrı kaydı listesini dışa aktarma ve yazdırma,

III. Çağrı kaydı ekranından, seçilen müşteri için Çağrı kaydı geçmişini, Kesinti geçmişini ve yorumlarını gösteren geçmiş ekranlara gitmek mümkün olmalıdır.

b) Sinyal Ekranı

I. Sayaç Veri Yönetimi (OSOS) sisteminden türetilen sayaç sinyalleri gösterilebilecektir. Sayaç sinyalleri, sorun çağrısı bilgileriyle aynı şekilde görüntülenecek ve işlenecektir.

II. Yetkili Operatör için, kesinti tahmin motoru tarafından kullanılan OSOS sayaç sinyallerini/tesisatını görüntülemek, filtrelemek, durumu değiştirmek veya engellemek, engelini kaldırmak mümkün olmalıdır.

c) Coğrafi Ekranlarda Çağrı kaydı Bilgileri

I. Çağrı kayıtlarının (kesintili, kesintisiz ve bağlantı noktası belli olmayan) yeri ile ilgili bilgiler coğrafi ekranlarda da gösterilecektir. Simgeler, bireysel çağrı kayıtlarını gösterecektir. Ekranın yakınlaştırma faktörüne bağlı olarak, daha iyi görünürlük için birkaç çağrı kaydı simgesi, çağrı kayıtlarının sayısını gösteren bir sayı ile tek bir simgeye gruplandırılmalıdır.

II. Çağrı kayıtları hakkında ayrıntılı bilgi içeren çağrı kayıtları ekranının, ilgili çağrı kaydı simgesinin bağlam menüsü kullanılarak doğrudan coğrafi ekrandan açılabilmesi mümkün olmalıdır. Bunun tersi de mümkün olmalıdır.

10.13 Entegrasyonlar

10.13.1 CBS Verileri (Şebeke ve Üretici Verileri) Entegrasyonu

1) Genel

a) CBS entegrasyonu, ADMS' in dağıtım şebekesi için kaynak yöneticisi olmalıdır.

b) CBS ortamında oluşturulan OG ve müşteri bağlantı noktasına kadar AG şebeke katmanlarına ait envanter ile elektriksel bağlantı verilerini ve İl, ilçe, işletme sınır haritalarını, kofre bilgilerini içererek SCADA/DMS/OMS sistemine içe aktaracaktır. Bu aktarım sırasında operasyonel faaliyetler durdurulmayacak ve veri kaybı yaşanılmayacaktır. Hatların parça parça alınması yerine hiç saplama veya hat yoksa ilgili şebeke tek node (düğüm) olarak sisteme alınmalıdır. DMS fonksiyonlarının hızlı çalışmasını sağlamalıdır.

c) SCADA/DMS/OMS'e aktarılan veri, CBS'deki OG ve müşteri bağlantı noktasına kadar AG dağıtım şebekesinin enerjilendirilme durumunun görselleştirilebilmesine olanak sağlayacaktır. SCADA/DMS/OMS'de oluşan anahtar pozisyonları sağlanacak entegrasyon ile CBS'ye aktarılabilmesine imkan sağlayacaktır. Aktarım periyodu ŞİRKET tarafından belirlenecektir.

d) CBS ortamında bulunmayan verilerin Veri Mühendisliği Uygulaması kullanılarak manuel girilebilmesi mümkün olacaktır.

e) CBS ortamında bulunan üretici ve yenilenebilir enerji noktaları ile şarj istasyonları katmanı verileri içe aktarılabilir olacaktır.

f) CBS'deki öznitelik verileri ADMS'e yüklenecek ve veriler/metinler ADMS Şebeke modeli üzerinde gösterilebilecektir. CBS harita altlığını (örneğin; Google maps, OpenStreetView) kullanabilecek ve ADMS Sistem görüntüleri ile senkronize edilmiş yakınlaştırma, kaydırma, ölçeklendirme tekniklerine sahip olabilecektir.

~~g)~~ CBS Şebeke Modeli BT ve ADMS sistem fonksiyonlarına entegre olacaktır. YÜKLENİCİ tarafından dxf,csv formantında import/export desteği sağlanmalıdır.

h) CBS'den aktarılan verilerin işlendiği ADMS şebeke haritası her zoom seviyesinde farklı şebeke unsurları, İl, İlçe ve işletme sınırları gösterebilir nitelikte olacaktır. Zoom

seviyelerine ait gösterilen veriler kullanıcı tarafından güncellenebilir olacaktır. Sistem açılırken işletme sınırları veya il bazlı seçim yapılarak yetkilendirme yapılabilmelidir.

i) Her zoom seviyesinde CBS'de mevcut olan coğrafi altlık (Google maps ,OpenStreetView) arka planının içeriye aktarmak için haritaların kullanılması ve sistemde performans kaybı yaşanmaması sağlanacaktır.

j) CBS veri içe aktarma aracı, mevcut kullanılan Popular Visualization CRS ölçüm tabanlı koordinat sistemi kullanarak ekipmanların coğrafi koordinatlarını işleyebilecektir. Koordinat gösterimi için dosya formatında tanımlı x,y ve hat benzeri yapılar için koordinat dizisi içermektedir.

k) CBS veri importunda, hat, bara, telemetrili ve diğer kabinlere ait şebeke verilerinin (Hat uzunluğu, gerilimi, tipi ve kesiti vb.) DMS modüllerinin çalışması için gerekli alanları/tabloları manuel veri girişine gerek olmadan otomatik olarak doldurulması sağlanacaktır. Manuel girişi de destekleyebilir olacaktır. ADMS fonksiyonlarında kullanılacak şebeke elemanlarına ait öz nitelik verileri CBS entegrasyonu ile otomatik olarak alındığı kontrol edilecektir.

l) Telemetrili kabinlere ait ekipmanların tip, elektriksel şebeke bağlantı ve öznitelik verilerinin CBS importu ile güncellenmesi sağlanacaktır.

m) CBS içe aktarma işleminden sonra jumper, hat ayırıcıları, topraklama ekipmanları ve mobil jeneratörler vb. gibi operasyonel değişiklikleri içeren (Geçici Şebeke Elemanları) destekleyecektir.

n) ADMS Şebeke haritasında Afad il Md., Polis Merkezleri, Hastaneler, Okullar ve OSOS vb. önemli lokasyonlar ayrı ikonlar ile gösterilecektir. Etiketleme yapılabilir olacaktır.

o) CIM verilerine dönüşüm ve entegrasyon da sağlanabilecektir. CIM ile entegrasyon olması durumunda ŞİRKET, YÜKLENİCİ ve CBS çözüm ortağı birlikte hareket ederek entegrasyon çözümü sunacaktır. Mevcutta kullanılan CBS tarafından paylaşılan SCADA/DMS/OMS data formatının XML/XDF verilerine dönüşüm sağlanacaktır. CBS verilerinin CIM olarak dönüşümü ŞİRKET tarafından sağlanacaktır.

2) Değişiklik Yönetimi

a) Değişim Yönetimi için aşağıdaki tüm kriterlerde çözüm sunulmalıdır.

b) Toplu İçe Aktarma: Başlangıç(ilk) yükleme için tam dönüşüm. Önceki tüm mevcut verilerin üzerine yazılır.

c) Artımlı İçe Aktarma: CBS Veri kümelerinin iki sürümü arasında bağlantı, öznitelik ve grafikle ilgili değişiklikleri içeren değişikliklerin algılanmasını ve günlük olarak içe aktarılmasını sağlamalıdır.

d) Delta İçe Aktarma: Artışları (delta) CBS verilerini almalı ve herhangi bir değişiklik algılaması yapmamalıdır. Günlük olarak içe aktarılmasını sağlamalıdır.

e) Fark dataları için ADMS ve CBS arasındaki farklar ekipman bazlı sayı olarak sunulabilmelidir.

3) Veri Doğrulama

a) İçe aktarılan verilerin doğruluğunu kontrol etmek için dönüştürme modülü tarafından doğrulama kuralları yürütülmelidir. Kullanıcı arayüzünde, operatör veri doğrulamayı etkinleştirebilir veya devre dışı bırakabilir ve doğrulama kurallarından hangisinin uygulanacağını seçebilir. En az aşağıdaki kriterleri sağlayabilmelidir.

I. Özellik kontrolleri (ayırıcı tipi, hattın havai/yeraltı olması vb.),
II. Boş veri kontrolü,
III. Standart karakter sayısı kontrolü,
IV. Numaralandırma kontrolü,
V. Tutarlılık denetimleri,
VI. Faz ve gerilim kontrolü,

b) Veri importu yapılacak datanın içeriğini gözlemlemek ve dönüştürülecek birden fazla datanın son durumunu göstermek mümkün olacaktır.
c) Veri importu esnasında kontrol adımlarında ilerlemeyi engelleyen herhangi bir hata alınırsa import işlemi durdurulabilecektir.
d) Veri doğrulama aracında şebeke modeli katman kontrolü bulunmalıdır.
e) Import edilen Şebeke modeli verilerinde bulunan ancak ADMS sisteminde bağlantısallığı yapılamamış şebeke verileri için uyarı desteği sunulmalıdır.
f) Mevcut veri ile import edilen veri karşılaştırıldığında OG ve müşteri bağlantı noktasına kadar AG şebeke verilerinde bulunamayan silinmiş şebeke verilerinde uyarı desteği sağlanmalıdır.
g) ADMS uygulamalarında kullanılacak şebeke elemanlarına ait öz nitelik verileri CBS entegrasyonu ile otomatik olarak alındığı kontrol edilecektir ve eksik veri uyarı desteği sunulacaktır.
h) Import ve veri doğrulama süreci sonucunda belirlenen kişilere entegrasyondaki durum ve sonucu hakkında mail atılabilecektir. ŞİRKET ihtiyaç duyulan mail sunucusunu sağlayacaktır.
i) Geçmiş ve yeni CBS importu datalarının grafiksel olarak tarihsel karşılaştırmalı analizi yapılabilecektir.

4) Model Dönüşümü

a) SCADA/DMS/OMS Sistemi ile GIS entegrasyonunu çift yönlü olacak şekilde gerçekleştirilebilecek şekilde ve dinamik yapıda güncel verilerin paylaşılmasını sağlayacaktır. CBS Entegrasyonu üzerinden; dağıtım sistemi, besleme topolojisi ve dağıtım sistemine bağlı cihazlar ile bu cihazlara ait özellik, öznitelik ve bağlantısallık da dahil tanımlayıcı bilgiler alınacaktır.
b) CBS'den alınacak veriler ADMS sistemine dahil edilmeden önce 'Otomatik' ve 'Manuel' olmak üzere iki aşamalı onaylama işlemine tabi olacaktır.

c) SCADA/DMS/OMS Sistemi, verileri CBS'den ilk alındığı anda otomatik denetim ve onaylama işlemlerini uygulayacaktır. Otomatik onaylama işlemi sırasında aşağıdaki denetimler gerçekleştirilecektir:

I. Aktarılan ekipmanlar içerisinde bağlantısallık problemi olan kayıtlar vurgulanmalı ve sorgulanabilir olmalıdır.
II. Bağlantısı olmayan tüm cihazlar ve hat segmanları tanımlanmalı ve vurgulanmalıdır.
III. Alınan veriler, bir tabloda listelenmiş ve ekran üzerinde işaretli olacak şekilde gösterilen tüm hatalar ile birlikte geçici bir katmana yerleştirilebilmelidir. Kullanıcı için hataları işaretleme ve eksik veriyi belirtme özelliği bulunacaktır. Bu bilgiler CBS'de gerekli düzeltmelerin yapılması için kullanılabilecektir. Bu sayede, uygun olarak yetkilendirilen bir kullanıcı, farklı bir adımda da geçici katmandaki veriyi inceleyebilecek ve kabul etmeyi seçebilecektir.

d) Sadece onay denetimi adımlarından bütünüyle geçtikten ve yetkili bir kullanıcı tarafından onay verildikten sonra ADMS veriyi sisteme dahil edecektir.
e) YÜKLENİCİ, sistemler arası veri transferinin gerçekleşmesini sağlayacak veri modeli uyumluluğunu ve/veya uyumluluğu sağlayacak araçların sağlanmasını garanti edecektir.
f) ADMS Şebeke modeli yapılandırması için ara yüz performansı (Değişen object/connection başına süre kavramsalda belirlenecektir), ŞİRKET tarafından analiz edilecek ve gerekli görülmesi durumunda ŞİRKET tarafından iyileştirme talep edilebilecektir.
g) Veri güncelleme sürecinden ADMS ve fonksiyonları ile operasyonel faaliyetlerde herhangi bir performans kaybı ve duraksama meydana gelmemelidir.
h) CBS Import için ara yüz performansı ŞİRKET tarafından analiz edilecek ve gerekli görülmesi durumunda ŞİRKET iyileştirmeyi talep edebilecektir.

5) Kullanıcı Arayüzü ve İş Akışı

a) Kullanıcı arayüzü, tüm sürecin görselleştirilmesi de dahil olmak üzere tüm CBS verisi içe aktarma iş akışının kontrolünü destekleyecektir.
b) Kullanıcı, sürekli yürütmeyi veya manuel adım adım yürütmeyi seçebilecektir.
c) Kullanıcı arayüzü aşağıdaki özellikleri sağlamalıdır;

I. Çalışma modunun seçimi: Toplu veya artımlı içe aktarma veya delta içe aktarma,
II. Sürekli yürütme veya kademeli yürütme seçimi,
III. İçe aktarma işleminin durumunun görselleştirilmesi,
IV. Doğrulama kontrollerinin seçimi,
V. Değişiklik Yönetimi ve Dönüşüm dahil olmak üzere iş akışını kontrol etme,
VI. Veri tabanını hazırlamayı, aktarmayı ve etkinleştirmeyi kontrol etme,
VII. Import veri setinin gerektiğinde geri alınması ve yinelenmesi, veri sorunları bulunursa import veri setinin atılması/geçersiz kılınması,

10.13.2 Müşteri Bilgileri Entegrasyonu

a) Müşteri bilgileri SAP'den SCADA/DMS/OMS'e günlük aktarılacaktır. Detaylar kavramsalda ŞİRKET ile değerlendirilecektir.
b) Mevcutta bulunan veri en az aşağıdaki başlıkları içerir şekilde olup bilgi amaçlıdır.

I. Müşteri kimliği,
II. Müşteri Adı/Soyadı,
III. Müşterinin Adresi,
IV. Ev Telefonu Numarası,
V. Cep Telefonu Numarası
VI. Müşteri Tipi(AG-OG),
VII. Müşteri Önceliği (Önemli Müşteriler),
VIII. Şebeke Bağlantı Noktası
IX. Bina Numarası
X. Faal Bilgisi
XI. Kent içi-Kent altı-Kırsal
XII. Tarife Tipi ve Sınıfı

c) SCADA/DMS/OMS tüm müşterilerin (en az 2 milyon ve üstü müşteri) bilgilerini içeriye aktarabilecektir.
d) OSOS, AFAD, Hastane, Polis Merkezi vb. önemli lokasyonların bilgilerinin aktarılması ile GIS haritada ayrı bir ikon ile belirlenebilecektir.
e) Sisteme gelen trafo sayaçları gibi sanal tesisatlar etkilenen abone listesinde raporlanmamalıdır.

10.13.3 OSOS Entegrasyonu

a) OSOS ve OMS sistemleri arasındaki entegrasyon tüm ilgili paydaşlarıyla çalışılarak sağlanacaktır. Entegrasyon akışları ve tipleri karşılıklı çalıştaylarla netleştikten sonra, entegrasyonların ADMS tarafı YÜKLENİCİ, diğer birimlerin entegrasyon uçları sorumlulukları ŞİRKETE ait olacaktır.
b) Çift taraflı entegrasyon gerçekleştirilecek olup, anlık olarak OMS sisteminden belirlenen bir OSOS sayacının enerji var yok sinyali Otomatik Sayaç Okuma Sistemine webservis ile sorgulayabilecektir. Ayrıca sayacın enerjisinin gittiği ve geldiği anda OSOS üzerinden OMS sistemine ihbar olarak değerlendirilmek için ve OSOS kesinti başlangıç-bitiş zamanları gönderilecektir. Kesinti kaydının OSOS zaman etiketi ile oluşması sağlanmalıdır. Topolojiye göre adresleme gerçekleştirmelidir. OMS sistemi üzerinden etkilenen kullanıcı sayısı ve güç değerleri hesaplanmalıdır. Kesinti durumunda SCADA GIS haritasında şebekenin topolojik olarak renklendirmesini sağlamalıdır. Kesintiden etkilenen OSOS'ların enerjisi gelmesi durumunda kesinti içerisinde farklı renkle gösterilecektir. OMS tarafında ilgili OSOS'un eşleştiği kesinti bilgisi OSOS sistemine de gönderilebilecektir.
c) Kesinti kapatılırken etkilenen ososlara ping atılıp enerjinin var/yok bilgisi sorgulanabilir olacaktır. Eğer enerji var sinyali gelmemişse yeni osos kesinti çağrısı oluşturabilecektir.

d) Çift taraflı entegrasyonla kesintiyle ilişkilenen OSOS çağrılarının kesinti numarası Otomatik Sayaç Okuma Sistemine aktarılacaktır.
e) Kesinti ile ilişkilendirilemeyen OSOS çağrılarının hata nedenleri raporlanacaktır.
f) Mevcutta bulunan mesaj içerikleri en az aşağıdaki başlıkları içerir şekilde olup bilgi amaçlıdır.

I. Ekipman numarası
II. Sinyal Tipi
III. Sinyal Oluşma zamanı
IV. Sonuç Kodu
V. Osos sinyal numarası
VI. OSOS Kesinti Başlangıç-Bitiş Zamanı

Detaylar kavramsalda ŞİRKET ile değerlendirilecektir.

10.13.4 WFM Entegrasyonu

a) Kesinti yönetimine ait iş emirleri WFM sistemine iletilerek bir iş emri oluşturması için ilgili entegrasyonu kullanılacaktır.
b) Kesinti Yönetimine ait iş emri tipleri aşağıda belirtildiği şekildedir:

I. Kesintisiz iş emirleri
II. Kesintili İş Emirleri
III. Planlı(Anahtarlama) İş Emirleri
IV. Kesintiye ait çağrılar (öncelik ve tehlike etiketi olanlar)

c) Entegrasyon iki sistemdeki değişiklikleri de birbirine aktararak iş emirlerine ait belirlenen verilerin eşlenmesini sağlayacaktır.

d) Bir kesintiye ait birden fazla iş emri oluşturulabilecektir. Aynı kesintiye ait farklı iş emirleri birden fazla ekip tabletine gönderilebilmesi sağlanacaktır. İş emri ile ilgili ekip tabletlerinden yapılacak güncelleme kuralları ve detayları ŞİRKET ile birlikte kavramsalda değerlendirilecektir.

e) Kesinti Yönetimi Sistem'inden WFM'e gönderilen iş emirleri iş havuzuna düşecektir. Operasyon saha ekip tabletine seçilen sipariş gönderilecektir. Ekip tabletinde iş süreci durumu aşamaları, kesintiye ait yapılan anahtarlamalar ve açıklama bilgileri girilmesi ile eş zamanlı olarak bu bilgiler kesinti yönetimi sistemine aktarılacaktır.

f) Saha ekipleri kesintili iş emirleri için tabletlerine gönderilen kesinti ekipmanını onaylayabilecek ya da yeni kesinti ekipmanına ait anahtarlama yapabilecektir.

g) SCADA GIS haritasında saha ekip tabletlerinin anlık konumları gösterilecektir. Bu sebeple WFM entegrasyonu ile tablet konum bilgileri alınarak coğrafi şebeke modeline işlenmelidir.

Detaylar kavramsalda ŞİRKET ile değerlendirilecektir.

10.13.5 CRM Müşteri Yönetimi Entegrasyonu

a) ŞİRKET'in Elektrik Dağıtım Hizmetinden Sorumlu olduğu bölge içerisinde oluşan ihbarlar Çağrı Merkezi aracılıyla anlık olarak sisteme kaydedilmektedir. Alınan ilgili ihbarlar CRM entegrasyonu ile Kesinti Yönetimi Sistemi'ne aktarılacaktır. Alınan ihbarlar arıza kategorisi, müşteri bilgisi, adres ve şebeke bağlantı noktası gibi veriler ile iletilecektir.

b) Mevcutta bulunan mesaj içerikleri en az aşağıdaki başlıkları içerir şekilde olup bilgi amaçlıdır.

I. Çağrı Kaydı Numarası
II. Çağrı Kategorisi (Tel Kopuğu, Yangın, Voltaj Düşüklüğü, Direk Yıkılması vb.)
III. Tarih Saat
IV. Lokasyon (İl/İlçe/Mah.)
V. Öncelik Seviyesi
VI. İhbar Açıklaması
VII. Referans Adres
VIII. Müşteri Ad/Soyadı/Telefon Bilgileri
IX. Şebeke Bilgisi
X. Bina Numarası
XI. Tesisat Numarası

c) Kesinti Yönetimi Sistemi'nde oluşan ihbarlar ve ihbarlara ait kesintilere yönelik güncel veriler CRM'e gönderilecektir. Kesinti kayıtları için de kesinti bilgisi ve bu kesintiden etkilenen müşteri şebeke bağlantı bilgileri iletilir.

d) Mevcutta bulunan mesaj içerikleri en az aşağıdaki başlıkları içerir şekilde olup bilgi amaçlıdır. Mevcut mesaj içerikleri kontrol edilerek kavramsalda ayrıca detaylandırılıacaktır.

I. Kesinti Numarası
II. Kesinti Durumu
III. Kesinti Açıklaması
IV. Kesinti Oluşma Tarih Saat
V. Öncelik Seviyesi
VI. Kesintiden Etkilenen Ekipman Listesi

e) SCADA/DMS/OMS günlük olarak en az 7.000 çağrı kaydı alacak ve işleyecektir. SCADA/DMS/OMS kesinti kayıtları oluşturmak ve mevcut kesinti kayıtlarını otomatik olarak güncellemek için çağrı kayıtlarını kullanacak bir hizmet sağlayacaktır.

Detaylar kavramsalda ŞİRKET ile değerlendirilecektir

10.13.6 Üreticilerin Sisteme Entegrasyonu

a) Üretim Santralleri İzleme Modülü, bahse konu dağıtık üretim santrallerinin EK-2.1'de tanımlı örnek sinyal listesi uyarınca izleme, kontrol ve raporlamalarının yapılacağı ve aynı zamanda e-şarj, enerji depolama tesisleri ve çatı Ges uygulamaları gibi gelecekte AG dağıtım şebekesinin önemli bir parçası olması muhtemel alternatif üretim/tüketim noktalarının izlenip yönetilebileceği SCADA/DMS/OMS yazılımının bir parçası olacaktır.

b) ŞİRKET dağıtım şebekesinde bulunan dağıtık üretim santrallerine ait yaklaşık 800 RTU noktası halihazırda farklı bir APN'e tanımlıdır. Bu nedenle YÜKLENİCİ, tekliflerinde Üretim Santralleri İzleme Modülü için öngördükleri mimariyi ayrıca belirteceklerdir. Dağıtık Üretim Santrallerine ait RTU noktaları için kullanılacak olan haberleşme sunucuları diğer kapsam merkezlerinden ayrı olacaktır. Mimari tasarım noktasında, YÜKLENİCİ gerekli donanımları Şartnamenin diğer hükümlerini göz önünde bulundurarak fiziki veya sanal olarak seçip ayrıntılı olarak açıklayacaklardır.

c) ŞİRKET mevcut izleme ve kontrol sistemine tanımlı dağıtık üretim santrallerinin örnek sinyal listesi Şartname eki EK-2.1'de detaylı olarak belirtilmiştir. Teklif edilecek ürün, IEC104 protokolü ile dahil edilecek üretim santrallerinin izleme, kontrol ve raporlamalarını yapacak aynı zamanda ICCP protokolü ile TEİAŞ Sistemine veri iletiminde bulunabilecek yeterlilikte olacaktır. Bunlara ek olarak, modül en az 2000 Dağıtık Üretim Santralinin ve gelecekte dağıtım şebekesine dahil olacak; şarj istasyonları, çatı Ges ler ve enerji depolama tesisleri gibi alternatif tüketim ve üretim noktalarının analiz, izleme ve kontrolünü herhangi bir performans kaybı olmaksızın yönetebilir olacaktır.

d) Üretim Santralleri İzleme Modülüne eklenecek istasyonların ekran çizimleri, veri girişleri vb. süreçleri tümüyle ilgili modül içerisinde, diğer istasyonlardan ayrı olacaktır. Üretim Santralleri İzleme Modülüne eklenecek dağıtık üretim santralleri yazılım ara yüzünde, bağlı bulundukları TEİAŞ TM'sinin altında gruplandırılacak, gösterilecek ve ara yüz ile ekran detayları proje içerisinde ŞİRKET talepleri doğrultusunda hazırlanacaktır.

e) Üretim Santralleri İzleme Modülü ile;

I. Tanımlı istasyonlara ait üretim/tüketim verilerinin gerçekleşen değeri ile beklenen değeri arasındaki fark, gerçekleşme yüzdesi,
II. Güç aşımı,
III. Şebeke gerilimine etkisi,
IV. Üretim/tüketim durumu,
V. Reaktif enerji oranları,
VI. Aktif/Pasif istasyonların özeti,
VII. Genel ya da özel amaçla tanımlanmış alarm durumları, vb. süreçler operasyonel ihtiyaçlar dahilinde izlenebilir ve raporlanabilir olacaktır.

f) Ayrıca modül içerisinde doğrudan sahadan gelen veriler ya da bir koşula bağlanmış verilerin alarm olarak gösterilmesi mümkün olacaktır. Modül içerisinde, geçmiş ve canlı dataların grafiksel olarak analiz edilebileceği kullanıcı izleme sayfaları ve sayfalar üzerinde canlı kadran, seviye, trend vb. canlı görseller yerleştirilebilir olmalıdır.

Üreticilerin, Sistem mimarisinde bağlı olduğu haberleşme sunucuları, diğer haberleşme sunucularından ayrı tasarlanmalıdır.

10.13.7 PRISM Entegrasyonu

Yeni SCADA/DMS/OMS den, Raporlama Sistemine entegrasyon ile anlık veri akışı sağlanması beklenmektedir.
Detaylar kavramsalda ŞİRKET ile değerlendirilecektir.

10.13.8 EDVARS Entegrasyonu

Elektrik Dağıtım ŞİRKETlerine ait kesinti kaydı verilerinin toplandığı yerdir. İlgili entegrasyon sistemi ile günlük olarak ŞİRKET'e ait kesinti yönetimi sistemi verilerinin aktarılması sağlanır.

10.13.9 TEDAŞ TALEP TAKİP Entegrasyonu

Elektrik Dağıtım ŞİRKETlerine ait kesinti kaydı verilerinin toplandığı yerdir. İlgili entegrasyon sistemi ile anlık olarak ŞİRKET'e ait kesinti yönetimi sistemi verilerinin aktarılması sağlanır. Edvars tarafından değiştirilen veriler OMS tarafında da otomatik bir şekilde değiştirilecektir. Değiştirilen verilere ilişkin bilgiler OMS tarafında kayıt edilir ve istenildiği taktirde geri alınarak Edvars tarafı tetiklenir. Tüm neden sonuç kesinti süresi çağrı ekleme çıkarma işlemleri Edvars tarafından da mevzuat gereği yapılabilecektir. OMS tüm değişiklikleri kendine kayıt edecek ve ay sonu Edvars ile farkını raporlayabilir olacaktır.

10.13.10 Planlı Bakım Entegrasyonu

Planlı kesinti girişleri SPM den manevralar girilerek ya da dış sistemden (SAP/CBS) entegrasyon ile oluşturulacak ve bu manevralar sonucunda etkilenen trafo ve müşteri bilgilerine istinaden, etkilenen kullanıcılara otomatik SMS atılacaktır ve ŞİRKET web sitesinde ilana çıkılacaktır.

Planlı Kesinti başvuru süreci çözüm ortaklarıyla birlikte hareket edilerek dijitalleştirilecek ve yukarıda belirtilen süreç ile ilişkilendirilecektir.

Detaylar kavramsalda ŞİRKET ile değerlendirilecektir.

10.13.11 SCADA Alarm Yönetimi

Gelecekte, SCADA saha alarmlarının iş emri olarak Sentinel sistemine iletilebileceği bir yapının kurulabilmesi için imkan sağlanacaktır.

10.14 Anahtarlama Prosedürü (SPM)

10.14.1 Genel

a) Şebeke Kontrol Merkezi Sistemine ait Anahtarlama Prosedürü Yönetimi operatörün anahtarlama prosedürleri, anahtarlama dizileri ve şebeke kontrol emirleri oluşturmasına,

değiştirmesine ve yürütmesine bununla birlikte tüm bu koşulların farklı anahtarlama prosedürü tiplerinde kaydedilmesine izin vermelidir. Kullanıcı bu tiplerin detaylarını belirleyebilmeli ve yeni tipler oluşturabilmelidir.

b) Bir anahtarlama prosedürü, anahtarlama işlemlerinin belirli bir sırasını içermelidir. Operatör, şebekede çalışma talebine yanıt olarak bir anahtarlama prosedürü oluşturur. Alternatif olarak, bir sistem uygulaması, sağlanan bir arayüz aracılığıyla örneğin izolasyon ve restorasyon prosedürleri gibi bir anahtarlama prosedürü üretebilecektir.
c) SPM yetenekleri, şebeke operasyonlarının hazırlanmasını, incelenmesini ve yürütülmesini sağlayacaktır. SPM ayrıca, arıza koşullarını hafifletmek veya bir arızadan sonra gücü geri yüklemek için anahtarlama işlemlerini yürütmek ve ayrıca şebeke çalışmasının optimizasyonu için de kullanılabilecektir.
d) Operatörün eylemlerini kaydederek ve sonra mevcut bir prosedürü değiştirmek, operatörün eylemlerini gerçek zamanlı modda kaydederek veya Dağıtım Şebekesi Uygulamaları gibi uygulamalar tarafından otomatik olarak bir anahtarlama prosedüründe girişler oluşturmak mümkün olmalıdır.
e) Anahtarlama dizileri, belirli bir şebeke elemanı üzerinde tanımlanmış bir anahtar eylemi gerçekleştirildiğinde yürütülen bir dizi anahtarlama adımı içermelidir.
f) Operatör anahtarlama adımlarının sırasını içeren bir şebeke kontrol emri tanımlayabilecektir.
g) Planlı kesintiler için uygun manevra, Dağıtım merkezinde fider değişimi, Trafo merkezinin devre dışı kalması durumunda, Yük limit eşiği geçtiğinde, manevra durumunda, Yük Akışı gibi DMS fonksiyonlarının anahtarlama durumlarını belirlemek için anahtarlama adımları planlanabilecektir.

10.14.2 SPM İşlemleri

a) Anahtarlama Prosedürü Oluşturma

I. Operatör bir anahtarlama prosedürü oluşturduğunda, otomatik olarak bir iş numarası ve oluşturma zamanı oluşturulacaktır. Operatör anahtarlama prosedürü ile ilgili yorumlar ekleyebilecek ve başlangıç ve bitiş zamanlarını tanımlayabilecektir.
II. Bir anahtarlama prosedürünün başlık bilgileri en azından aşağıdakileri içermelidir:

- Başlık,
- Prosedürü oluşturan kullanıcı,
- Oluşturma tarihi,
- Son değişikliğin tarihi ve saati,
- Zamanlanmış ve fiili başlangıç ve bitiş tarihleri,
- Durum,
- Tür,
- Kesinti kaydı,
- Anahtarlama prosedürünün atandığı kullanıcı,
- Alan,
- Açıklama,

- Prosedürün onaylanıp onaylanmadığı hakkında bilgi,
- Otomatik yürütülecek belirlenmiş anahtarlama adımları
- Zaman çizelgesi,
- Anahtarlama yürütülmesini tetikleyen işlem olayı,

b) Anahtarlama Prosedürünü Düzenleme

Yetkili operatör, oluşturulan bir anahtarlama prosedürüne adımlar ekleyebilecektir.

c) Adım Türleri

Aşağıdaki adımlar mümkün olacaktır:

I. Kontrol Eylemleri

Bir anahtarlama prosedürünün aşağıdakileri içermesi mümkün olmalıdır:

- Denetleyici kontrol eylemleri,
- Geçici Şebeke Öğeleri,
- Değişiklikleri kontrol edebilme,
- Etiketlerin ayarlanması veya temizlenmesi,
- Durum,

Uygun kontrol emirleri için, operatörün, adımı gerçekleştirmeden önce şebeke elemanının zaten hedef konumda olup olmadığının kontrol edilip edilmeyeceğini seçmesi mümkün olmalıdır.

II. Organizasyon Adımları

Bir anahtarlama prosedürünün aşağıdakileri içermesi mümkün olmalıdır:

- Bekleme adımı

Anahtarlama işleminin yürütülmesi herhangi bir süre için duraklattırabilir (saniye cinsinden). Bekleme süresi girildiğinde boşta kalma süresi yapılandırılmalıdır. Boşta kalma süresi dolduktan sonra, anahtarlama prosedürünün yürütülmesine otomatik olarak devam edilmelidir.

- Duraklama adımı

Anahtarlama prosedürünün yürütülmesini duraklatır. Operatör, uygun bir düğmeye tıklayarak anahtarlama prosedürünün yürütülmesine manuel olarak devam edebilmelidir.

- Yorum adımı

Anahtarlama prosedürü adımları arasında yorum eklenmesine izin vermelidir.

d) Düzenleme

Bir anahtarlama prosedürünü aşağıdakileri kullanarak düzenlemek mümkün olmalıdır:

I. Operatör, eylemlerini bir şebeke modeli üzerinde kaydedebilecektir. Ayrıca, operatör eylemlerini süreç modunda kaydederek yeni anahtarlama adımları oluşturabilecektir.

II. Operatör, gerçek bir anahtarlama işlemi olmadan yeni anahtarlama adımları oluşturabilecektir.

III. Operatör, mevcut işlerin bölümlerini (bir veya daha fazla anahtarlama adımı) kopyalayabilecek ve girişleri başka bir anahtarlama prosedürüne yapıştırabilecektir. Bir anahtarlama prosedürüne girilen adımların silinebilmesi de mümkün olmalıdır.

IV. SPM ters çevirme özelliği, operatörün işlemleri bir prosedürde kopyalamasına ve bunları ters sırada ve ters çevrilmiş kontrollerle (orijinal kontrollere karşı) yapıştırmasına izin vermelidir.

e) Anahtarlama Prosedürünü Seçme, Sıralama ve Filtreleme

I. Operatör, *SPM özet ekranını* kullanarak bir anahtarlama prosedürü seçebilecektir. Bu özet, doğru anahtarlama prosedürü seçimini sağlamak için her anahtarlama prosedürü için bir başlık satırı ve ekran seçim düğmesi seçilerek yapılmalıdır.

II. Operatör ayrıca, gerekli anahtarlama prosedürünü mümkün olan en kısa sürede bulmak için özet ekranını önceden tanımlanmış sıralama ve filtreleme kriterlerine göre sıralayabilecektir.

f) Bir Anahtarlama Prosedürünün Yürütülmesi

I. Tek Adımlı Yürütme

Tek adımlı yürütme, anahtarlama prosedüründeki sıralarını göz ardı eden bir veya daha fazla bireysel eylemin doğrudan yürütülmesini sağlayacaktır. Operatör, bireysel eylemlerden geçerek anahtarlama prosedürü eylemlerini yürütebilecektir.

II. Sıralı Yürütme

Sıralı yürütmede, anahtarlama prosedüründe yer alan tüm işlemler, hazırlandıkları kesin sırada yürütülecektir. Bir duraklama adımı varsa, yürütmenin durması ve devam ettirilmesi mümkün olmalıdır.

g) Anahtarlama Prosedürlerinin Arşivlenmesi ve Yeniden Kullanılması

Anahtarlama prosedürleri, ilişkili kesinti yönetimi kayıtlarıyla birlikte arşivlenecektir. Arşivlendikten sonra, bir anahtarlama prosedürünün değiştirilmesi artık mümkün olmayacaktır. Ancak arşivlenmiş bir anahtarlama prosedürü, yeni bir anahtarlama prosedürü için bir model olarak görüntülenebilir ve yeniden kullanılabilir olmalıdır.

h) Bir Anahtarlama Prosedürünün Ön Test ve Kontrolü

İşi gerçek zamanlı olarak yürütmeden önce bir anahtarlama prosedürünün etkisinin kontrol edilebilmesi mümkün olmalıdır. Bir ön anahtarlama prosedürü kontrolü, çalışma modunda bir anahtarlama prosedürü yürütecek ve sonuçlar çalışma modunda tek hat içinde görülecektir.

10.14.3 SPM Kullanıcı Arayüzü

a) SPM, operatörün anahtarlama prosedürlerinin yönetimine devam edebileceği ve bunları izleyebileceği ekranlar sağlanmalıdır.

Aşağıdaki ekranlar en azından mevcut olacaktır:

I. Anahtarlama prosedürlerinin özet görünümü,
II. Görüntüleme, düzenleme ve yürütme için ayrı bir anahtarlama prosedürü için görüntüleme,
III. Arşivlenmiş anahtarlama prosedürlerinin özet görünümü,
IV. Oluşturulan anahtarlama prosedürlerinin bölgesel bazda filtrelenmesi,
V. Anahtarlama prosedürü adımlarına göre etkilenen müşteri ve *etkilenen trafo listesi görüntülenebilir ve dışarı aktarılabilir olacaktır.

10.14.4 Şematik ve Coğrafi Şebeke Ekranları

Herhangi bir anahtarlama prosedüründe yer alan anahtarlama eylemlerinin tek hat diyagramda görüntülenmesi mümkün olmalıdır.

10.15 SCADA /DMS / OMS Test Sistemi

10.15.1 Genel

a) SCADA /DMS / OMS Test sistemi, sistem üzerindeki mevcut entegrasyonlar, değişiklikler vb. işlemlerin canlı sistemi etkilemeden uygulanması ve doğrulanması için kullanılacaktır.

b) CBS entegrasyonuyla aktarılan şebeke modeli öncelikle test sistemine aktarılacak , gerekli kontrollerden geçmesi akabinde canlı sisteme aktarılabilecektir.
c) Sisteme dahil edilecek tüm merkezler, öncesinde üzerinde çizimleri ve bağlantılarıyla test edilecektir. Veri girişleri ve gerekli tanımlamalar yapılarak istenilen testler gerçekleştirildikten sonra ŞİRKETİN onayı doğrultusunda merkezin gerçek sistem üzerine aktarımı sağlanacaktır. Merkeze ait tüm tanımlamaların (veri girişleri, ekran çizimleri vb.) aktarımı otomatik olarak gerçekleştirilecektir.

d) Test Sistemi, Canlı sisteme herhangi bir müdahalede bulunmadan veri değişikliklerinin test edilmesine izin vermelidir. Canlı sistem ve Test Sistemi birbirinden bağımsız olacaktır. Test sistemi, veri modeli yöneticisi rolünü üstlenecektir. Değiştirilen ve başarıyla test edilen veri tabanı işleri, test sistemi aracılığı ile canlı sisteme aktarılabilecektir.

e) Test sistemi çalıştığı ve canlı sistem tarafından erişilebilir olduğu sürece, canlı sistemdeki veri tabanı yönetim aracında etki ettiği şebeke unsuru verilerinin değiştirilmesine izin verilmeyecektir.

f) Test sistemi canlı sistemde mevcut olan tüm entegrasyonlara sahip olacaktır. Ve ŞİRKETİN ilgili test sistemleriyle entegre olacaktır. Bu kurulacak sistemin gerekli mimari siber güvenlik koşulları göz önünde bulundurularak YÜKLENİCİ tarafından tasarlanacaktır.

g) Operatör OMS eğitimleri bu test sistemi üzerinden verilebilecektir. Burada oluşturulan herhangi bir kesinti kaydı canlı sistemi etkilemeyecektir. Ayrıca entegrasyon simülasyonları yapılabilecektir.

10.16 Tarihsel Arşiv Sistemi

10.16.1 Genel

a) Tarihsel Arşiv Sistemi SCADA/DMS/OMS SCADA, İletim Yönetimi ve Dağıtım Yönetimi gibi kaynaklardan güç sistemi geçmiş verilerini depolamak için sağlam ve güvenilir bir arşiv sağlanmalıdır.

b) HIS'in temel özellikleri şunlardır:

I. Spontane veri toplama ve gerçek zamanlı değerlerin depolanması,

II. Büyük (Terabayt) hacimli verileri işlemek için ölçeklendirilebilir olmalıdır. Herhangi bir kod değişikliği yapmadan yapılandırma parametrelerini değiştirerek çeşitli boyutlardaki gereksinimler için Tarihsel Arşiv Sistemini yapılandırmak mümkün olacaktır.

III. Entegre veri azaltma ve sıkıştırma özellikleri,

IV. Tarihsel Arşiv Sistemi analog verileri, ölçüm ve hesaplanan şebeke verilerini, durum verilerini, operatör tarafından girilmiş verileri ve diğer ilgili şebeke verilerini saklayabilecek ve verilere erişebilecek ve yeniden yapılandırabilecektir. YÜKLENİCİ, ŞİRKET'in proje yürütümü esnasında talep edebileceği tüm veri unsurların arşivleme sistemine dahil etmekten sorumlu olacaktır.Hesaplama fonksiyonları bulunmalı, hesaplamalar anlık ve kalıcı yapılabilir olmalıdır.(Cebirsel İşlemler-Karşılaştırma fonksiyonları-Koşullu fonksiyonlar-Güç/Enerji işlemleri, Min/Max/Avg vb) DMS uygulamaları içerisinde belirtilen fonksiyonlar için oluşturulan sonuçlar kaydedilebilir olmalıdır.

V. Değişikliklerin günlüğe kaydedilmesi için denetim izi de dahil olmak üzere çevrimiçi arşivdeki değerlerin güncellenmesi,

VI. Kısa, orta ve uzun vadeli arşiv,

VII. Kolay post-mortem analiz için Tarihsel Arşiv Verisi Replay,

VIII. Arşiv sisteminin sistem durumu ve kaynak izlemesi,

c) AKM ve ADKM için; YÜKLENİCİ'nin sağlayacağı bir veritabanı sunucusuna belirtildiği gibi yedekleme işlemi gerçekleştirmek için otomatik bir yedekleme ve arşivleme kurulacaktır.Arşivlenen bilgileri müşteri tarafından seçilebilen bir süre boyunca (örneğin 1 yıl) tüm yetkili kullanıcılara çevrimiçi olarak sağlayacaktır. Uzun

süreli arşivleme için (örneğin 15 yıl) verilerin çevrimdışı dosyalara taşınması mümkün olmalıdır. ŞİRKET tarafından bu süreler kavramsalda belirlenecektir.

d) HIS, Arşivlenecek SCADA veri noktalarının seçiminin Veri Mühendisliği Uygulaması ile tanımlanması mümkün olmalıdır.
e) Tekrar oynatmayı desteklemek için, topoloji bilgileri Tarihsel Arşiv Verisinde saklanmalıdır.
f) Uzun vadeli arşive taşınmış olan veriler hakkındaki bilgiler, gelecekte alınmak üzere veri tabanında saklanmalıdır.
g) Tarihsel Arşiv veri tabanı yedekli olmalıdır.

10.16.2 Kullanıcı Arayüzü

Kullanıcı ara yüzü, yetkili kullanıcılara aşağıdaki özellikleri sağlamalıdır:

- Arşiv verilerinin tablosal ekranları ve grafikleri,
- İlgilenilen veri noktasına hızlı bir şekilde odaklanmak için güçlü filtreler ve sıralama mekanizması,
- Özel veya genel olarak düzenlenmiş kullanıcı görüntüleri,
- Veri noktasına özgü parametreler de dahil olmak üzere arşivleme için yapılandırılan veri noktalarının listesi,
- Seçilen arşiv verilerinin yazdırılması,
- MS Excel ve CSV dosyalarına aktarılması.

10.16.3 Tarihsel Arşiv Verisi Yeniden Oynatma Fonksiyonu

a) Yeniden Oynatma Fonksiyonu, kullanıcının belirlenen süre içerisinde anahtarlama eylemlerini görüntülemesine izin vermelidir.
b) Uygulama anahtarlama sırası ve ilgili olayları tarihsel verileri kullanarak simüle edebilecektir.
c) Uygulamanın sonuçları şebeke diyagramlarında gösterilecektir. Simülasyon anında canlı sisteme etki etmeyecektir.

10.16.4 Arabirim

a) Ağ Kontrol Merkezi Sistem arşivi, işletme genelinde farklı özel raporlar için ham veri sağlayıcısı olacaktır. Arşiv, harici bir raporlama aracı için veri kaynağı olarak hizmet edecektir.
b) Kullanıcı, ofis ortamında karmaşık veri analizi raporları ve çizelgeleri oluşturabilir ve sürdürebilir olmalıdır. Ofis yazılımından arşive olan bağlantıyı yenileyerek ham verilerin periyodik olarak güncellenmesi mümkün olmalıdır.

c) Aşağıdaki arayüzler sağlanmalıdır:

I. *.csv biçimli bir dosyaya dayalı arayüzü içe ve dışa aktarılması,
II. Excel gibi MS-Office araçlarıyla ve diğer dış uygulamalarla sağlanmalıdır.

10.17 Kullanıcı Arayüzü

10.17.1 Genel

a) SCADA/DMS/OMS'de gerçekleştirilecek tüm işlevler için kullanıcıya ortak bir görünüm sunan, tek bir Kullanıcı Arayüzüne sahip olmalıdır.

b) Kullanıcı Arayüzü Türkçe klavye girdisi için Türkçe içeren diyalogları destekleme özelliği gibi Grafik Kullanıcı Arabirimi (GUI) için kabul gören uluslararası ve endüstriyel standartları sağlayacaktır. İngilizce tabanlı olan Kullanıcı Arayüzü fonksiyonları operatör ekranları için uygun Türkçe karşılıklarına tercüme edilmelidir.

c) Durum/Alarm verileri ve RTU'lar tarafından edinilen analog değerler, hesaplanan/manüel olarak güncellenen veri ve grafik şematik diyagramlar dahil olmak üzere, tablo ve şema halinde olan veri sunumlarını monitörler üzerinde görüntülemek için Windows yeteneği sağlamalıdır.

d) SCADA/DMS/OMS ile ilgili diğer fonksiyonların gerçekleştirilmesi için bir temel sağlamalıdır, buna grafik görüntüsü ve rapor düzenleyiciler dahildir.

e) Kabul ve onay (Accept and Acknowledge) işlemleri fare hareketleri ("sürükle-bırak", "işaretle ve tıkla") ve klavye girişi ile yapılabilecektir.

f) RTU'lar tarafından gönderilen alarm ve olay verileri ile analog değişkenler, tablo şeklinde ekranlar üzerinde sunulabilecektir.

g) Alarm ve olay verilerine ait değişimleri görsel ve/veya sesli olarak bildirmelidir.

h) Rapor yazılımları gibi diğer SCADA/DMS/OMS uygulamalarının yürütülmesini de sağlanmalıdır.

i) Şebeke coğrafik haritasında, entegrasyonla alınan saha ekip konum bilgilerine istinaden özelleştirilerek oluşturulmuş ikonun anlık değişimi ile görüntü vermesi sağlanacaktır. Entegrasyonla alınan verilere istinaden ikonla ilgili renk vb. değişim imkanı sağlanacaktır. Örneğin çalışıyor durumda olan araç ikonunun kırmızı renge dönmesi, üzerinde iş olmayan ekibin yeşil renk ile gösterilmesi vb.

j) Kontrol merkezi, ofis ve uzak iş yerleri için ortak bir görünüm sunmalıdır.

k) Karanlık ve aydınlık ortamlar için optimize edilmiş renk temaları; Kullanıcı oturum açtıktan sonra renk temasını seçebilecektir.

l) İçeriğe duyarlı menüler, sürükle ve bırak, araç ipuçları ve yüksek çözünürlüklü monitörler için destek gibi standart teknikler sunmalıdır.

m) İçeriğe duyarlı çevrimiçi yardım sistemi sunmalıdır.

n) Gerçek zamanlı ortamın çalışma modundan net bir şekilde ayırt edilmesi sağlanmalıdır.

o) Belirli müşteri gereksinimlerine uyarlanabilir kullanıcı arayüzü sağlanmalıdır.

p) Aynı görüntüleyicide coğrafi ve şematik ekranlar için destek sağlanmalıdır. Gerekli bilgilere hızlı erişim ve SCADA/DMS/OMS uygulamalarının sorunsuz etkileşimi sağlanmalıdır. (Örneğin şebeke diyagramları ve kesinti bilgileri arasında).

q) Ekranlar arasında sürükleyip bırakma geçişi sağlanmalıdır.

r) Konturlama gibi gelişmiş görselleştirme dahil olmak üzere görev odaklı görünümler sunmalıdır.

s) Katmanları ve yakınlaştırma düzeylerini kullanarak mevcut gereksinimlere göre bilgilerin dağınıklığını giderme sağlanmalıdır.

t) Duruma göre dinamik renklendirme ile denetleyici kontrol için güvenlik kurallarının ve kilitlerin hızlı ve güvenli bir şekilde ele alınması sağlanmalıdır.

u) Operatörler ve operatör konsolları için erişim hakları ve kontrol alanları sağlanmalıdır.

v) Gerçek zamanlı operasyonel pencereler sağlanmalıdır.

w) Ekranlar kullanıcı bazında özelleştirilebilir olmalıdır.

x) ADMS Şebeke modeli gerilim seviyesi, şebeke katmanı bazında filtrelenebilir olmalıdır.

y) ADMS Şebeke Modeli her zoom seviyesinde farklı şebeke unsurları, İl, İlçe ve işletme sınırları gösterebilir nitelikte olacaktır. Zoom seviyelerine ait gösterilen veriler kullanıcı tarafından güncellenebilir olacaktır.

10.17.2 Operatör Konsolu

a) Operatör konsolu birden fazla monitör, büyük ekran projektör, TV, yazıcı ve ses çıkışından oluşacaktır. Oturum sırasında, bir konsol iş istasyonuna bağlanır. Birden fazla operatör konsolunun LAN ile iş istasyonuna uzaktan bağlanabilmesi mümkün olmalıdır.

b) Büyük Ekran Projeksiyonu

SCADA/DMS/OMS, büyük ekran projeksiyonu kullanma yeteneği sağlayacaktır. Büyük ekran projeksiyonunun ölçeklenebilir temsil tekniği (bir araya getirilmiş veya istiflenmiş neredeyse sınırsız sayıda projeksiyon modülü), dinamik bilgilerin (örneğin, bir trafo merkezinden canlı bilgiler veya bir ADMS Şebeke modeli haritası) büyük ekran gösterimine izin verecektir. Yazılım tarafından Büyük Ekran Projeksiyon Ekranına operatör konsolu atanabilir olmalıdır.

c) Ses Çıkışı

Sesli sinyaller, operatör konsolundaki güç sisteminden gelen alarmları duyuracaktır. Operatör onayı sesli alarmı susturacaktır. Sesli alarmın çalması tek bir yetki alanı atanması ile değil, çoklu yetki alanları sağlanarak da gerçekleştirilebilmesi sağlanmalıdır ve tüm iş istasyonlarında geçerli olmalıdır.

10.17.3 Kullanıcı Arayüzü Mimarisi

a) Kullanıcı Arayüzü, MS Windows veya Linux işletim sistemini çalıştıran X86 PC'lerde 7 / 24 saat çalışacak şekilde barındırmalıdır.
b) Her operatör konsolu en az 4 ekrana hizmet verebilecektir. Ekran içeriğini ayrı monitörler arasında taşımak mümkün olacaktır. Öte yandan, 4 ekranı tek bir sanal ekran olarak kullanmak ve bir pencere çerçevesini tüm ekran alanına (4 ekrandan) yaymak da mümkün olmalıdır.
c) Operatör konsolları ve kullanıcıları, SCADA/DMS/OMS'te tam olarak yönetilebilecektir.
d) Zengin istemci grafik uygulamasının sunucu istemcisi iletişimi için de uygun güvenlik araçları gereklidir.
e) Ofis ortamındaki bilgisayarların Kontrol Merkezi verilerine erişebilmesi öngörülmelidir.

10.17.4 Yetki ve Kullanıcı Yönetimi

a) SCADA/DMS/OMS, yetkisiz kullanıma karşı korumalara sahip olmalıdır. Bu amaçla, her operatörün üzerinde çalıştıkları Şebeke Kontrol Merkezi Sistemi üzerinde bir kullanıcı profili bulunmalıdır. Ayrıca, SCADA/DMS/OMS, farklı erişim hakları türlerini tanımlama olanağı sağlayacaktır. Hem konsollar (konsol otoritesi) hem de operatör (kullanıcı otoritesi) için bu yetkiler olacaktır.
b) Yetkiler, konsollar ve kullanıcılar için işlevlerin, bölgelerin yapılandırılabilir atama setleriyle kontrol edebilecektir:
   I. İşlevlerin bir konsola/kullanıcıya atanması,
   II. Bölgelerin konsola/kullanıcıya atanması,
c) Yetkili kullanıcılar, bireysel kullanıcıların yetkilerini düzenleyebilecektir. Kullanıcı arayüzü, alanların seçimini desteklemek için çok hiyerarşili bir ağaç sağlamalıdır.
d) Operatörün konsol üzerindeki etkin yetkisi, kullanıcı yetkisi ve konsol yetkisinin mantıksal ve kombinasyonu olmalıdır.

e) Kullanıcı Yönetimi

Kullanıcılar sisteme ancak geçerli bir kullanıcı profiline ve geçerli bir şifreye sahip olduklarında erişebilecektir. SCADA/DMS/OMS, sistem yöneticisinin kullanıcı profillerini ve yetki yapılandırmalarını tanımlamasına ve yönetmesine ve bir operatörün SCADA/DMS/OMS işlevlerine yetkililer atayarak veya kaldırarak erişme yeteneğini kontrol etmesine olanak tanıyan bir Konsol ve Kullanıcı Yönetim Aracı sağlamalıdır.

f) Oturum Açma ve Oturumu Kapatma

SCADA/DMS/OMS, çoklu oturum açmayı destekleyecektir; İlk girişten sonra operatör tüm yetkili ekranlara ve fonksiyonlara erişebilecektir. SCADA/DMS/OMS kullanıcı kimlik doğrulama yöntemleri şöyle olmalıdır:

g) Uygulama Düzeyi Kimlik Doğrulaması:

Operatör, iş istasyonu işletim sisteminde (OS) tek faktörlü işletim sistemi kullanıcı kimliği ve parolası veya çok faktörlü kimlik doğrulaması (kullanıcı kimliği ve RSA SecurID belirteci) ile oturum açmalıdır. İşletim sistemine giriş yaptıktan sonra SCADA/DMS/OMS, operatörün kimlik doğrulama için SCADA/DMS/OMS kullanıcı kimliğini ve şifresini girmesini gerektiren ek bir güvenlik katmanını destekleyecektir.

h) Kurumsal Düzeyde Kimlik Doğrulama:

Operatör, iş istasyonu işletim sisteminde tek faktörlü işletim sistemi kullanıcı kimliği ve parolası veya çok faktörlü kimlik doğrulaması (kullanıcı kimliği ve RSA SecurID belirteci) ile oturum açmalıdır. Bireysel kullanıcı için dağıtılan SCADA/DMS/OMS dijital sertifikasıyla, yetkili kullanıcılara ek kimlik bilgileri girmelerine gerek kalmadan SCADA/DMS/OMS 'e erişim izni verilir. Sertifika tabanlı kimlik doğrulama, yalnızca yetkili kullanıcıların SCADA/DMS/OMS'e erişmesine izin verilmesini sağlar.

i) Bir kullanıcı şifresi, siber güvenlik gereksinimlerine dayalı şifre kurallarını yerine getirmelidir.
j) Uygulama ve Kurumsal Düzeyde erişim için, ŞİRKET güvenlik ilkesine uyumu desteklemek üzere parola karmaşıklık kuralları uygulanacaktır. Şifreler şifreli bir biçimde saklanacaktır. Kullanıcı adı, sisteme erişen kişiyi tanımlamalıdır.
k) Operatör eylemlerinin sonucu olan tüm olaylar (manuel güncelleme, etiketleme vb.) bireysel kullanıcı kimliği ile günlüğe kaydedilmelidir.
l) Operatör vardiyayı tamamladığında, operatör konsoldaki oturumu kapatmalıdır. Denetim nedenleriyle, tüm başarılı ve başarısız oturum açma ve kapatma olayları özetlere girilecektir.
m) Vardiya değişimi sırasında kullanıcıların değiştirilmesini desteklemek için, sistem kullanıcıları değiştirmek için hızlı bir seçenek sunmalıdır. Şu anda oturum açmış olan kullanıcının ekranları, kullanıcıya özgü erişim hakları göz önünde bulundurularak, kullanıcılar arasında sorunsuz bir geçiş sağlamak için açık tutulmalıdır. Tüm kontrol alanları sürekli olarak denetlenecektir. Kullanıcı Değiştir özelliği, Uygulama Düzeyi Kimlik Doğrulama yapılandırmaları için geçerli olmalıdır.

10.17.5 Kullanıcı Arayüzü Ekranları

a) Genel

I. Tüm SCADA/DMS/OMS ekranları, tutarlı bir kullanıcı deneyimi için renkler, düzenler, düğmeler gibi öğeleri belirten bir stil kılavuzuna göre oluşturulacaktır. Tüm ekranlar şunları destekleyecektir:

- Kopyalama ve yapıştırma, kaydırma, bağlam menüleri, araç ipuçları, simgeler ve takvim widget'ı kullanarak tarih ve saat girişi gibi standart işlevler,
- Simgelerin tutarlı kullanımı,
- Ekranlar arasında sürükleyip bırakma özelliğini desteklemelidir.

II. SCADA/DMS/OMS en azından aşağıdaki ekranları içermelidir:

- Yönlendirme (Menü)Gerçek Zamanlı Operasyonel Kontrol Penceresi,

- Grafik Aracı,
- Konsol ve Kullanıcı Yönetimi,
- Olay ve Alarm Özetleri,
- Ekranların Tam Listesi,
- İstasyon Listesi,
- Yönlendirme (Menü)Kullanıcı iş akışlarını ve sistem uygulamalarını başlatmak için merkezi bir sisteme genel bakış ve ortak erişim noktası sağlamalıdır.

b) Şebeke Diyagramları

I. ADMS Şebeke model haritası, şematik ve coğrafi şebeke diyagramlarının görüntülenmesini sağlayacaktır.

II. Şebeke yapısının ve durumunun net bir şekilde görüntülenmesi için statik (çizgiler, daireler, metinler vb.) ve dinamik görüntüleme öğeleri (durum, eğilim, değerler vb.) kullanılacaktır.

III. Sahadan gerçek zamanlı olarak gelen pozisyon değişimleri ADMS şebeke model haritası üzerinde otomatik olarak gösterilecektir. SCADA Sistemine dahil olmayan statik merkezlerdeki anahtarlama elemanlarının pozisyon değişimleri manuel olarak operatör tarafından değiştirilebilecektir. Bu sayede SCADA/DMS/OMS Sistemindeki dağıtım şebeke modelinin anlık olarak güncel kalması ve renk değişiminin buna uyarlanması sağlanacaktır.

IV. SCADA/DMS/OMS Sistemi harita altlığı üzerinde bulunan aktif telemetrili (SCADA olan) ya da statik telemetrisiz (SCADA olmayan) OG ve müşteri bağlantı noktasına kadar AG şebeke seviyesindeki merkezlerde oluşan açma, kapama, manevra vb. rejim değişikliklerinin OG ve müşteri bağlantı noktasına kadar AG şebeke seviyesine etkilerini seçilebilir envanterler bazında gösterebilir ve listelenebilir olacaktır.

V. ADMS şebeke model haritası üzerinde şebeke unsurlarına ait verilerin (hattın kesiti, trafo gücü vb) okunması kullanıcı dostu ve kolay erişilebilir şekilde tasarlanacaktır.

VI. Sokak adları, bölge verileri ve arazi kullanımı ve uydu görüntüleri gibi raster/dxfverileri gibi vektör verileri için destek dahil olmak üzere şematik ve coğrafi şebeke diyagramlarını kullanılabilir olmalıdır.

VII. Raster/dxf grafikleri şebeke diyagramlarına dahil etme özelliği bulunmalıdır.

VIII. Şebeke ve şebekenin farklı bölümlerinin farklı ayrıntı dereceleriyle net bir şekilde görüntülenmesi için şebeke diyagramı konsepti desteği sağlamalıdır.

IX. Şebeke diyagramının her düzlemi, belirli bir ayrıntı düzeyi için tüm şebeke bilgilerini içermelidir. Bu, her düzleme görünür bir büyütme aralığı atanarak kontrol edilecektir. Yakınlaştırma sırasında, bir düzlem yalnızca mevcut büyütme aralığı içinde olduğunda görülebilir olmalıdır.

X. Kaydırma: Şebeke diyagramında görüntülenen alanı kaydırma özelliği bulunmalıdır.

XI. Yakınlaştırma: ekran bölümlerini büyütme veya küçültme bulunmalıdır (Şebeke diyagramının çeşitli düzeylerinin görüntülenmesi ve dolayısıyla seçilen yakınlaştırma faktörüne bağlı olarak farklı ayrıntı dereceleri).

XII. Dağınıklığı giderme(decluttering): Verileri kapama ve ayrıntılı bilgileri görüntüleme

mümkün olmalıdır.

XIII. Şebekenin belirli bölümlerinin özelliklerine bağlı olarak dinamik renklendirilmesi. (Kaynak Trafo bilgisine göre enerjili ya da enerjisiz vb.) Operatörün ilgili araçlara hızlı erişimini sağlamak için özelleştirilebilir ve bağlama duyarlı menüler ve araç çubukları bulunmalıdır.

XIV. Şebeke diyagramının bir parçası olarak arşiv değeri tablolarını görüntüleme özelliği bulunmalıdır.

XV. Daha kolay kullanıcı yönlendirmesi için şebeke diyagramının simge durumuna küçültülmüş bir sürümünü sağlayan gezgin penceresi bulunmalıdır.

XVI. Oturum açmış olan kullanıcının denetimi altında olmayan alanları gösterme işlevi bulunmalıdır.

XVII. Akış yönünün şebeke diyagramlarında nasıl temsil edileceğini belirtme özelliği bulunmalıdır. (Oklar,- veya + işaretleri veya yapılandırılabilir renkler bulunması)

XVIII. Obje ID lerin şebeke diyagramlarında ve grafik kümelerinde nasıl temsil edileceğini seçme özelliği bulunmalıdır. (Adlar (kısa), metin (uzun ad) veya kimlik (sayısal değer))

XIX. Operatör başka bir ekrana geçtiyse, geçerli ekrandan seçilen ekran geri çağrılabilir olmalıdır.

XX. Şebeke diyagramı, aynı alanda bir dizi farklı veri toplamalıdır. Farklı veri kümeleri katmanlar halinde düzenlenecektir. Her katman özel bir bilgi türünü temsil edecektir.

c) Gelişmiş Görselleştirme

I. SCADA/DMS, durumsal farkındalığı desteklemek için güç akışı okları, göstergeler, simgeler ve bilgi kutuları gibi çeşitli mekanizmalar sağlayacaktır. Bir ekran profili seçerek (örneğin, şebeke analizi, voltaj ihlalleri, kesinti bilgileri vb.), Kullanıcı gelişmiş araçlarla görselleştirilecek bilgi türünü seçebilecektir. Ekran profillerinin, Kesinti Yönetimi veya Şebekesi Analizi gibi SCADA/DMS/OMS uygulamalarından gelen bilgileri temsil edecek şekilde yapılandırılabilmesi mümkün olmalıdır.

II. Göstergeler Akış okları, aktif veya reaktif güç akışının yönünü gösterecektir. Akış oku boyutunun ve renginin dinamik olarak değişmesi mümkün olacaktır. Oklar, ciddi bir ihlal olduğunda yanıp sönebilecektir.

III. SCADA/DMS, dinamik bilgileri temsil etmek için ek görselleştirme araçlarını desteklenmelidir

IV. Bir sınır ihlal edilirse, yani bir değer tanımlanan eşikten daha yüksek veya daha düşükse, operatör tarafından talep edilirse, bu ihlaller şebeke diyagramında olarak gösterilebilecektir.

V. Operatörün durumsal farkındalığı geliştirmek için sürekli değerleri görselleştirmesini sağlanacaktır, Bu, operatörün şebekedeki durumu analiz etmesine yardımcı olmalıdır.

d) Hat Yükleme (SCADA)

Hat yüklemesinin şebeke modeli üzerinde gösterilmesi mümkün olacaktır. İsteğe bağlı olarak, kullanıcının dikkatini en ciddi ihlale çekmek için hat yanıp sönebilir yapılabilecektir.

e) Hatlar için Enerjilendirme Durumu

Sistem, farklı hat renkleri kullanarak bir hata enerji verilip verilmediğini, bir tarafın açık veya enerjisinin kesilip kesilmediğini görselleştirmelidir.

f) Şematik ve Coğrafi Şebeke Diyagramları

I. İki tür şebeke diyagramı olacaktır. Kullanıcı, coğrafi ve şematik şebeke diyagramları arasında geçiş yapabilir ve aynı ekipmanı her ikisinde de görüntüleyebilir olacaktır.

II. Şematik şebeke diyagramı (tek hat diyagram)

Elektrik güç sistemini görselleştirmek için basitleştirilmiş bir gösterim olacaktır. Diyagramdaki elemanlar, elektrikli ekipmanın fiziksel boyutunu veya yerini temsil etmek zorunda değildir. Ekran, kullanıcıya şebeke topolojisine iyi bir genel bakış sağlamak için optimize edilmelidir.

III. Coğrafi şebeke diyagramı

Grafik unsurların koordinatlarının gerçek dünyayla bir ilişkisi olacaktır. Kullanıcı, ekipmanın coğrafi konumunu, kesintileri vb. görebilecek. Ayrıca, kullanıcı sokakları, müşterileri, arazi kullanımını veya uydu görüntülerini görüntüleyebilecektir.

IV. Her iki şebeke diyagramı türü de Tutarlı görselleştirme ve etkileşim yetenekleri, örneğin alarmlar, kesinti alanları, yakınlaştırma, kaydırma, değiştirme, not ekleme vb. sağlayacaktır.

V. Her iki şebeke diyagramı türü de Şematik ve coğrafi görünümler arasında geçiş yapmak için bir geçiş sağlayacaktır

VI. Her iki şebeke diyagramı türü de Mevcut şebeke diyagramından yeni bir şebeke diyagramı açma yeteneği (örneğin, coğrafi görünümden şematik görünümü açma veya tam tersi) sağlayacaktır

VII. Kullanıcı, ilgilendiği bilgilere odaklanmak için arka plan renginin parlaklığını veya koyuluğunu dinamik olarak ayarlayabilecektir.

g) Grafik ekranlar

Grafik gösterimi ve grafik yönetimi için, SCADA/DMS/OMS çözüm sunmalıdır.

Veri Mühendisliği Uygulaması ile tercih edilen herhangi bir görüntüleme konumunda grafiklerin (grafik değişkenleri) oluşturulabilmesi mümkün olacaktır. Bir grafik değişkeninin zaman içinde bir sinyal değerini çeşitli tiplerde (çizgi,şubuk,pasta,histogram vb.)grafik olarak düzenleyebilecektir

h) Olay ve Alarm Özetleri

I. Mevcut olayların ve normal şebeke durumundan sapmaların bir görünümü sağlanacaktır. Operatörün yakın geçmişi, örneğin alarm özetlerini ve etiket özetlerini gözden geçirmesine izin vermelidir.

II. Özetin yapılandırmasına bağlı olarak, özetin satırlarına yorum eklenmesi mümkün olacaktır. Özetlerin saat ve tarihe göre, alfabetik ve kronolojik olarak tercihe göre sıralanması mümkün olmalıdır.

III. Özetler, kaydırma, sayfalama ve bağlam menüleri (örneğin, bir alarmı onaylamak için) gibi standart etkileşim ilkelerini desteklemelidir.

IV. Özetler, sütunlar içinde sıralama, sütun genişliğini değiştirme, filtreleme, seçilen duruma göre renklendirme sağlayabilmelidir.

V. Word, Excel gibi diğer programlara kopyalayıp yapıştırılabilme (toplam veya kısmi) sağlayabilmelidir.

VI. Arama özetinin filtre ayarlarıyla doğrudan erişimi sağlayabilmelidir.

VII. Alarmların engellenmesi (sinyal ya da ilgili istasyon bazlı) sağlayabilmelidir.

VIII. Analog – dijital verinin geçmiş verisinin görselleştirilmesi sağlayabilmelidir.

IX. Bağlantı kullanarak ilişkili bir kesinti kaydına erişim sağlayabilmelidir.

X. Alarm konumunu görüntülemek için şebeke diyagramı çağırma sağlayabilmelidir.

i) Operasyon Günlüğü

Operasyon Günlüğü, Operatörlerin sisteme giriş çıkışları ve sistem içerisinde aldıkları aksiyonların zaman bazlı tutulmasını sağlayacaktır.

j) Masaüstü Düzeni Yönetimi

I. Masaüstü Düzeni Yönetimi, kullanıcının işyeri için tercih edilen ekran düzenlemesini kullanıcıya belirtmesine ve çağırmasına izin vermelidir. Bu düzenlemeyi her konsol türüne ve her kullanıcı için kaydetmek ve hatırlamak mümkün olmalıdır. Filtreler ve sıralama düzenleri gibi kullanıcı tarafından seçilebilir özellikler de masaüstü düzeninin bir parçası olarak kaydedilmelidir.

II. Kullanıcı denetleyici, kontrol ve veri girişi için özel düzenler oluşturabilecektir. Kullanıcı, tanımlanan düzenlerden birini tercih edilen varsayılan düzen olarak bildirebilir. Varsayılan düzen, kullanıcı oturum açtığında otomatik olarak yüklenir. Masaüstü düzeni belirli bir kullanıcı konsoluyla ilişkilendirilemez olmalıdır. Diğer bir deyişle, kullanıcı belirli bir konsolda bir düzen sakladığında, bu düzen de görünür olacak ve diğer konsollardan kullanılabilecektir.

III. Sistem yöneticisi varsayılan düzeni tanımlayabilecektir. Sistem varsayılan düzeni, kullanıcı henüz kişisel bir varsayılan düzen tanımlamadığında oturum açıldığında gösterilecektir. Kullanıcının masaüstü düzenlerini diğer kullanıcılarla paylaşması mümkün olmalıdır.

k) Şebeke Modeli Veri Arama

Genel arama ve kategorik arama mümkün olacaktır. Arama, sıralama ve filtreleme mekanizmaları sağlayacak ve ekranların çağrılmasına izin vermelidir. Arama ve sıralamaların görünen ad, ekipman adı,müşteri bilgisiile yapılabilmesi mümkün olmalıdır. Bulunan ekipmanın şebeke modeli üzerindeki yerine gitmek mümkün olacaktır.

l) Raporlama

I. SCADA/DMS, Java Veri tabanı Bağlantısı (JDBC) ve Açık Veri tabanı Bağlantısı (ODBC) sağlayarak Crystal Reports ve Jasper Reports gibi herhangi bir raporlama aracının entegrasyonunu desteklemelidir.

II. SCADA/DMS, geçici ve tekrarlanan raporlar oluşturmak için çözüm sağlamalıdır.

m) İM/DM Gezgini (Geçerli Veriler için Tablolu Ekranlar)

I. İM/DM Gezgini, operatöre mevcut verilere (analog ve dijital) hızlı bir erişim ve ayrıca olası eylemlere de (örneğin, denetleyici kontrol, manuel güncellemeler ve etiketleme) erişim sağlayacaktır. Tercih edilen alanı aramaya izin veren tüm teknolojik adresleri içermelidir. Gezgin, bu işlemleri manuel müdahale olmadan kendi kendine üretmelidir.

II. İM/DM Gezgini aşağıdakilere ilişkin tablo şeklinde bir genel bakış sunmalıdır:

- Mesajlar (dijitalleri),
- Analog değerler,
- Sayaç (Görselleştirilmiş yük durum bilgisi)

III. İM/DM Gezgini aşağıdakileri sağlayacaktır:

- Kaydırma,
- Seçili sütunlarda arama işlevi,
- Seçilen sütuna göre sıralama,
- Biçimlendirilmiş çıktılar (renklendirme dahil),
- İlgili tek hat diyagramın doğrudan çağrılması,
- Renkleri kullanarak bir anahtarlama cihazının durumunu görüntüleme (Örneğin yeşil = açık ve kırmızı = kapalı),

IV. Analoglar ve sayaç için aşağıdakiler sağlanmalıdır:

- Seçilen değerleri kilitleme veya kilidini açma,
- Değer ikamesi

10.17.6 Diğer

a) Kılavuzlu Operatör Alarmı

I. Sesli alarmlar ve monitördeki yanıp sönen göstergeler (şebeke şeması ve alarm özeti), operatörü alarmlar veya güç sistemindeki normal koşullardan sapmalar hakkında bilgilendirmelidir.

II. Butonlara tıklanarak kullanıcı, detaylı bilgi içeren ekranlara yönlendirilecektir. Alarmların alarm özetlerinde veya şebeke diyagramlarında onaylanması mümkün olacaktır.

III. Aşağıdaki olanaklar sağlanacaktır:

IV. Onaylanacak alarmlar, özette veya şebeke diyagramlarının bağlam menüsü kullanılarak tek tek seçilecektir.

V. Sayfada veya şebeke diyagramında şu anda görünür olan tüm alarmların aynı anda onaylanması mümkün olmalıdır. Onaylanan alarm mesajlarının seçilen sayfadan kaldırılması mümkün olmalıdır.

b) Sesli Alarmlar

I. SCADA/DMS/OMS, her kategori için belirli bir öncelik ve ses ile farklı kategorilerde sesli alarmlar sağlamalıdır. Sesli alarmların özel bir ses cihazı (Örneğin, hoparlör) aracılığıyla harici olarak veya iş istasyonu istemcisinin ses cihazı aracılığıyla yerel olarak duyurulabilmesi mümkün olmalıdır. Sesli alarm, operatör onayı ile susturulacaktır. Farklı alarm kategorileri için ses örnekleri yapılandırılabilir olmalıdır.

II. Alarmın yönetimi için konsolların sesli alarm gruplarında bir araya getirilmesi mümkün olmalıdır. Sesli alarm grupları birlikte etkinleştirilmeli ve onaylanmalıdır. Her alarm grubu için operatör, sesli bir alarmın bir grubun tüm konsollarından mı yoksa sadece bir konsoldan mı duyurulacağını yapılandırabilecektir.

III. Bir sesli alarm, bir özet veya şebeke diyagramında ilişkili alarmın onaylanmasıyla susturulmalıdır. Ek olarak, sesli alarmın kapatılabilmesi mümkün olmalıdır.

c) Veri Modları

I. SCADA/DMS/OMS, farklı veri kaynaklarını desteklemek için veri modlarını destekleyecektir. Geçerli veri modu, şebeke diyagramında ve uygulama görüntülerinde, durum çubuğundaki bir simge ve kısa metinle ve başlık çubuğundaki bir metinle belirtilmelidir.

II. Veri modlarına ek olarak, sistem ayrıca gerçek zamanlı, eğitim yedekleme ve test sunucu çalışma modları yukarıda belirtilen veri modlarıyla birleştirilebildiğinden, sunucu çalışma modu durum çubuğundaki bir simge ve kısa bir metinle belirtilmelidir.

III. Gerçek Zamanlı Mod, Çalışma Modu ve Tekrar veri modları desteklenmelidir

IV. Gerçek zamanlı mod, operasyonel veri tabanındaki veya uygulama veri tabanındaki işlem bilgilerini kullanmalıdır. Operatörün, konsolun etkin erişim haklarına dayanarak güç sistemini izlemesine izin vermelidir.

V. Çalışma modunda, operatör gerçek zamanlı operasyonel veri tabanının kopyalarını (anlık görüntülerini) kullanmalıdır. Birden fazla operatör aynı anda birden fazla kopya ile çalışabilecektir. Manuel giriş imkanları gerçek zamanlı moddakiyle aynı olmalıdır. Bu çalışma modu, güncel ve geçmiş verileri kullanan çalışmalar için kullanılmalıdır.

VI. Tekrar modunda, operatörün sürekli veri kaydından bir başlangıç ve bitiş tarihi seçerek geçmiş şebeke durumlarını görüntüleyebilmesi mümkün olacaktır.

d) Notlar

I. SCADA/DMS/OMS, operatöre aşağıdakileri girme olanağı sağlamalıdır:

II. Etiketler için ya da bir şebeke diyagramı hakkında notlar girilebilir ve listelenebilir olmalıdır. Girilen notların kullanıcı bilgisi ve tarihi görülebilir olmalıdır.

III. Operatör bir cihazda bir etiket ayarlarken, bir yorumun girilmesi mümkün olacaktır. Operatör, belirlenmiş bir ekranı kullanarak bir etiket için bir yorum girebilir, değiştirebilir ve silebilir olmalıdır.

IV. Bir şebeke diyagramına eklenebilecek metin olmalıdır. Operatör bir metin girebilecek ve notun yazı tipi rengini serbestçe seçebilecektir.

V. Sistemde saklanmakta olan tüm notlar belirlenmiş bir ekranda listelenmelidir. Bu ekrandan, operatörün notu içeren şebeke şemasını çağırması mümkün olmalıdır.

e) Veri aktarımı

MS Word, MS Excel gibi uygulamalara kopyalayıp yapıştırarak basit veri aktarımı mümkün olmalıdır.

f) Online Çevrimiçi Yardım

Ürün, operatörlere çevrim içi yardım hizmeti sunacaktır.

g) Stil Rehberi

I. SCADA/DMS/OMS kullanıcı arayüzü, tüm uygulamalar ve paylaşılan bileşenler için ortak bir görünüm–ve tutarlı bir kullanıcı deneyimi sağlamalıdır. Tüm kullanıcı arayüzleri, renkleri, düzeni ve etkileşim desenlerini açıklayan ortak bir stil kılavuzunu izlemelidir.

II. Büyük monitör boyutlarını ve kişisel tercihleri kapsayacak esneklik sağlamak için konsol başına yazı tiplerinin ve simgelerin boyutunu artırmak veya azaltmak mümkün olmalıdır.

. **h) Renk Temaları**

Operatör, oturum açtıktan sonra tercih edilen renk temasını seçebilecektir.

10.18 Otomatik Tek hat Oluşturucu

Otomatik tek hat oluşturucu, coğrafik şebeke modelini otomatik olarak şematik tek hat görünümüne dönüştürecektir.
Detaylar Kavramsalda ŞİRKET ile belirlenecektir.

10.19 Yama Yönetimi

10.19.1 Genel

a) Mevcut ticari kullanıma hazır işletim sistemleri ve yazılımları, sürekli bir sistem yamaları akışı sağlar. Aynı zamanda, kontrol merkezleri, güvenlik yaması sıklığından bağımsız olarak son derece kararlı ve güvenilir bir sistem gerektirir. Bu zorluğun üstesinden gelmeye yönelik en iyi uygulamalar, her güvenlik düzeltme eki sürümünün çalışan eksiksiz bir yazılım ve yapılandırma kümesi tanımladığından emin olmak için Standart Çalışma Ortamı yaklaşımından yararlanmalıdır.

b) Güvenlik düzeltme eki uygulama zorluklarını ele almak için, Red Hat Enterprise Linux (RHEL) veya Windows bilgisayarlarından oluşan dağıtılmış bir ağa Standart Çalışma Ortamı dağıtmak mümkün olmalıdır.

c) Şartname kapsamında verilen tüm yazılım ve donanımlar için Zafiyet takipleri YÜKLENİCİ tarafından yapılacaktır. YÜKLENİCİ veya ŞİRKET bildirimi ile CVSS kody 9,10 olan Kritik seviyeli zafiyetler için gerekli yamalar, üretici sitelerinde ve sektörde stabil durumda olduğuna karşılıklı karar verildikten ve riskleri tartışıldıktan sonra çözüme uygulanacaktır. YÜKLENİCİ veya ŞİRKET bildirimi ile CVSS kodu 7,8 olan Yüksek seviyeli zafiyetler için gerekli yamalar, üretici sitelerinde ve sektörde stabil durumda olduğuna karşılıklı karar verildikten ve riskleri tartışıldıktan sonra çözüme uygulanacaktır. Zafiyet kontrol ve yama ihtiyaç belirlemeleri 4 ayı geçmeyecek şekilde periyodik olarak karşılıklı iş birliği içerisinde yürütülecektir.

d) Yazılım güncelleme otomasyon araçları, tek bir bilgisayarın merkezi Yama Yönetimi Desteği (PMS) sunucusu olarak yapılandırılmasına izin verecektir. Yönetici bu bilgisayardan, el ile veya otomatik olarak güncellenecek bir dizi istemci bilgisayar tanımlamalıdır.

e) Önemli APM başarıları şunlar olacaktır:

f) Çok sayıda bilgisayarı aynı anda yamalama maliyetini önemli ölçüde azaltarak, hepsini Standart Çalışma Ortamına sıkı sıkıya uyumlu hale getirir. İstemci bilgisayarlar, her bilgisayara fiziksel olarak erişme ihtiyacını ortadan kaldırarak uzaktan güncellemelidir.

g) Basit ve ekonomik- Red Hat Satellite lisansı gerekli olmamalıdır.

h) PMS, çekirdek Red Hat Linux veya Windows İşletim Sistemini kurmak ve periyodik Red Hat Linux güncellemelerini yüklemek için tekrarlanabilir bir işlem sağlamalıdır.

i) Güvenli kurulum – Yalnızca minimum Red Hat Linux RPM seti veya Windows kurulmalıdır; Red Hat Linux veya Windows İşletim Sistemi sağlamlaştırması kurulum sırasında gerçekleştirmelidir.

10.19.2 Temel Özellikler

a) Merkezi PMS sunucusu, kullanıcının uyumluluk ve güvenlik gereksinimlerini karşılayacak bir yapılandırma dağıtımı seçmesine izin verecek esneklik sağlayacaktır. Tüm SCADA/DMS/OMS sistemlerini yamalamak için tek bir merkezi APM makinesinin kullanılması mümkün olacaktır. Alternatif olarak, bir APM makinesi kritik olmayan siber varlıklara (örneğin Geliştirme ortamı) tahsis edilebilirken, ikinci bir APM makinesi Üretim Sistemine tahsis edilebilir olmalıdır.

b) Mevcut SCADA/DMS/OMS Sistemi çalışırken, Red Hat Linux bilgisayarlarda sürüm yükseltme yapabilecektir.

c) Hangi Linux istemcilerinin dağıtık sistemde kayıtlı olduğunu ve yüklü olan Linux sürümünü görüntüleyen bir PMS Web sayfasını desteklenmelidir.

d) PMS Web sayfasını kullanarak, yöneticiler Red Hat Linux istemcilerini gruplar halinde düzenleyebilecek ve grupları belirli yazılım sürümlerine güncelleyebilecektir.

e) SCADA/DMS/OMS İnternet bağlantısı gerektirmeden Red Hat Linux İşletim Sistemi yükseltmeyi desteklenmelidir.

f) Tek tek Red Hat Linux bilgisayarlar için yama yükleme geçmişini görüntüleme olanağı sağlanmalıdır.

g) Tek tek Red Hat Linux bilgisayarlarda yüklü RPM paketlerinin tam listesini görüntüleme olanağı sağlanmalıdır.

h) PXE önyüklemesini desteklenmelidir.

i) Bir PMS istemcisi normalde PMS sunucusunu yoklar ve bir yama kullanılabilir olur olmaz istemci iş istasyonunu otomatik olarak günceller. İsteğe bağlı olarak, yöneticinin düzeltme eki güncellemesini manuel olarak gerçekleştirmesi mümkün olmalıdır.

10.20 Dağıtım – Operatör Eğitim Simülatörü

10.20.1 Genel

a) Eğitim Simülatörü; ekranları, sayfa formatları ve tüm fonksiyonları ile SCADA/DMS/OMS sisteminin ayrılmaz bir parçası olacaktır. Operatörlerin SCADA

ve DMS/OMS fonksiyonlarını kullanması ve dağıtım şebekesini işletmesi için gerekli eğitim ve test ortamını sağlayacaktır.

b) YÜKLENİCİ, gerçek şebeke modelini temel alarak eğitim simülatörü için çeşitli eğitim senaryoları hazırlayacaktır.

c) Eğitim simülatörünün tepki süreleri ve işleyişi gerçek sistem ile aynı olacaktır. Ayrıca eğitim simülatörü, gerçek zamanlı SCADA/DMS/OMS Sisteminin çalışmasına müdahale etmeyecektir.

d) Eğitmen sistem üzerinde dilediği senaryoyu oluşturabilecek ve eğitilen kişinin tepkilerini değerlendirmek adına sistemde hatalar oluşturabilecektir.

e) Eğitim Simülatörü, operatörlerin simüle edilmiş koşullar altında aşağıdakileri uygulamalarını sağlayacaktır;

I. Sistem çalışması ve restorasyonu,
II. Simüle edilmiş güç sistemi acil durumlarına yanıt,
III. Kesinti Yönetimi,
IV. Anahtarlama işlemleri,
V. Simüle edilmiş coğrafik şebeke haritası topolojisi üzerinde anahtar işlemleri,
VI. Simülatör kontrolü,

f) Eğitim simülatörü, SCADA/DMS/OMS' in benzer bir kullanıcı arayüzüne ve uygulama işlevlerine sahip olacaktır.

g) Eğitim simülatörünün çalışması her zaman kontrol merkezinin çalışmasından bağımsız olacaktır, veri tabanlarının ve uygulamaların kendi kopyaları üzerinde çalışacaktır.

h) Eğitim simülatörü aşağıdakileri destekleyecektir;

I. Eğitmenin eğitim senaryoları ve eğitim oturumları oluşturmasını ve kontrol etmesini sağlayan bir kullanıcı arayüzü sağlayacaktır. Operatörlerin izlenmesine ve onlarla etkileşime girmesine yardımcı olmalıdır.
II. Eğitim senaryosu oluşturmak için, eğitmen temel şebeke koşullarını tanımlayabilmeli ve olay grupları veya sistem hataları yaratabilecektir. Eğitmenin gerçek zamanlı anlık görüntüden veya simülasyon oturumu sırasında etkileşimli olarak temel olay oluşturması sağlanacaktır. Eğitmen temel olayları kaydedebilir ve düzenleyebilir olmalıdır.
III. Eğitmenin eğitim senaryosu oturumu sırasında katılmasını sağlayacaktır. Eğitmenin anahtarlama işlemlerini kontrol etmesi ve gerçekleştirmesi için SCADA tek hat diyagramları gibi özellikler sağlamalıdır.
IV. Güç sistemindeki değişiklikleri kaldırabilmesi mümkün olmalıdır.

V. Veri tabanı sürümündeki değişiklikleri işlemesi mümkün olacaktır. Örneğin eski bir veri tabanı sürümünde oluşturulan bir temel servis talebi, doldurulan geçerli veri tabanı sürümünde tutulabilir olmalıdır.

VI. Gerekirse, eğitim için kullanılan iş istasyonunun, proses sistemine bağlı normal operatör iş istasyonu olarak kullanılmak üzere yeniden yapılandırılabilmesi mümkün olmalıdır.

10.21 Çoklu Kontrol Merkezleri

10.21.1 Genel

a) SCADA/DMS/OMS sisteminin bütün fonksiyonları, Ana Kontrol Merkezi ve Acil durum Kontrol Merkezi olarak iki kontrol merkezi yapısında tam senkron bir şekilde çalıştırabilecektir.

b) Her Kontrol Merkezi, ayrı ayrı planlanmış donanım altyapısına sahip ayrı bir SCADA/DMS/OMS sistemine sahip olmalıdır.

c) Kontrol Merkezleri arası iletişimi ve operasyonları tam senkron bir şekilde çalışmalıdır.

d) Tüm Kontrol Merkezlerinin bütün veri tabanlarının tam senkron olması gerekmektedir.

e) SCADA operasyon komutları, manuel güncellemeleri, etiketlemeleri ve alarm onaylarını anlık senkron etmelidir.

f) Ana Kontrol Merkezinde devam eden operasyonel görevlerin geçici ya da kalıcı olarak Acil Durum Kontrol Merkezine kaydırılmasını desteklemelidir.

g) Tüm Kontrol Merkezleri için tek tip veri modeli olmalıdır.

h) Veri değişiklikleri tüm Kontrol Merkezlerine dağıtmalıdır.

i) Kontrol merkezleri arası iletişim kesilmesi ardından bağlantı tekrar kurulduğunda, eksik verilerin hepsi otomatik ve anlık senkron edilmelidir.

j) Her Kontrol Merkezi'nin bir adı olacaktır. Kontrol Merkezleri, Kontrol Merkezleri arasındaki iletişim ve proses veri senkronizasyonu için dahili olarak yönetilecek ve kullanıcı arayüzünde kullanıcıya adlarıyla tanımlanacaktır.

k) Herhangi bir Kontrol Merkezindeki operatörler, tüm güç sisteminin proses verilerini görüntüleyebilecek ve kontrol edebilecektir. Kontrol Merkezi'nin erişim hakları ve veri sorumlulukları, hangi noktaların alarma geçirildiğini veya kontrol edilebilir olduğunu belirlemelidir.

l) SCADA/DMS/OMS, kullanıcılara ve iş istasyonlarına atanan teknolojik sorumluluk alanları kavramını kullanacaktır kontrol merkezlerine sorumluluk alanları atayarak bu kavram genişletilecektir.

m) Değişiklikleri kontrol merkezi ağı genelinde dağıtmaktan master yapılmış bir kontrol merkezi sorumlu olacaktır. RTU'nun bağlı olduğu kontrol merkezi verilerden sorumlu olacaktır.

n) Bir RTU'nun birden fazla kontrol merkezine bağlı olması durumunda, yalnızca veri sorumlusu olan kontrol merkezine bilgileri işleyecek ve daha sonra verileri, Bilgi Alanları içinde veri noktalarına sahip diğer tüm kontrol merkezlerine iletecektir.

o) Ana Kontrol Merkezi'nde kontrol merkezini operasyon dışı bırakan acil bir durumunun meydana gelmesi halinde SCADA/DMS/ OMS Sistemi fonksiyonlarının tamamı eksiksiz olarak Acil Durum Kontrol Merkezi tarafından gerçekleştirilecektir. ADKM'nin etkinleştirilmesi operatör ekranında, ADKM'ye geçişin nedenini de içeren bir alarmla belirtilecektir.

p) Tüm iş istasyonları ve RTU'lar Ana Kontrol Merkezi ve Acil Durum Kontrol Merkezi ile iletişim kurma yeteneğine sahip olacaktır. ADKM otomatik olarak devreye geçtiğinde ve iş istasyonları ADKM sunucularıyla otomatik olarak iletişim kuracaktır.

q) Saha ekipmanları ve Ana Kontrol Merkezi arasındaki haberleşme, Acil Durum Kontrol Merkezi tarafından AKM'nin sorumlulukları üstlenildiğinde otomatik olarak ADKM'ye yönlendirilecektir. ADKM, tüm saha iletişim cihazlarını iletişimi tekrar yönlendirmesi üzerine tetikleyecektir. RTU ve diğer saha cihazları arasındaki veri trafiği ADKM SCADA sunucularına otomatik olarak yönelecektir. Haberleşme yollarının dinamik olarak geçiş yapması, herhangi bir haberleşme ve veri kaybına yol açmayacaktır. Teklif Sahibi, acil durum şartlarında AKM ve ADKM arasındaki kontrol geçişlerini ve saha ekipmanları ile olan haberleşmenin Acil Durum Kontrol Merkezi'ne nasıl yönlendirileceği ile ilgili detaylı açıklamalar sunacaktır. Beyan edilen çalışma yöntemi en az; herhangi bir kontrol merkezinin devredışı kalması durumunda önerilen kontrolü üzerine alma metodolojisini ve iki kontrol merkezi arasındaki haberleşme hattının servis dışı olması durumunda kontrol merkezleri arasında kontrol devrini belirleyen temel kural ve şartlara açık ve detaylı bir şekilde yer verecektir

11. Testler ve Kabuller

11.1 Genel

11.1.1 Gereklilikler

a) SCADA/DMS/OMS Sistemi (tüm yazılım bileşenleri), Kontrol Merkezi Haberleşme Ağı ve BT Entegrasyonu için testlerin, sistem ve ekipman fonksiyonelliklerinin tam olarak denendiği, bütün yönleriyle kullanıldığını, teslimat öncesinde YÜKLENİCİnin tesislerinde doğrulandığını gösterecektir.

b) Proje süreç aşamaları ŞİRKET in onayı ile belirlenecektir.SCADA/DMS/OMS Sisteminin (10.13 Maddesinde belirtilen entegrasyonlar hariç) 18 ay içerisinde çalışabilir ve kullanıma hazır şekilde teslimi yapılacaktır.

c) Testler, ŞİRKETin personeliyle ve ŞİRKET tarafından yetkilendirilen kişiler birlikte uygulanacaktır. Testler, ŞİRKETin personeliyle ve ŞİRKET tarafından yetkilendirilen kişiler birlikte uygulanacaktır.

d) SCADA/DMS/OMS, Kontrol Merkezi Haberleşme Ağı (tüm ekipman ve sistemleri içerecek şekilde) ve entegrasyonlar için testler her test kitabı için %70 başarı(Bu oran sağlanmış olsa dahi, canlıya alınması ve sürecin yürütülmesine engel teşkil etmesi durumunda birincil testler tekrarlanır) oranı ile tamamlanana kadar tekrarlanacaktır.

Kalan açık maddeler, başarılı tamamlanan testleri kapsamayacak ikincil testlerde tamamlanacaktır.

e) YÜKLENİCİ, ŞİRKET'in birincil testine katılmış olup olmasına bakmaksızın şartnamede belirtilen süre dahilinde sistemlerin teslimatından önce birincil teste hazır olduğu hususunda ŞİRKETi bilgilendirecektir.

f) Test prensibi olarak, YÜKLENİCİ ve ŞİRKET açısından güvenin oluşturulabilmesi için yazılı test, şartnameye uygun olarak resmi testler gerçekleştirilecek ve kayıt altına alınacaktır. Detaylı test kitapçıkları ve test prosedürleri, YÜKLENİCİ tarafından proje esnasında hazırlanarak ŞİRKET onayına sunulacaktır.

g) YÜKLENİCİnin sorumlulukları, aşağıda belirtilen gereklilikleri içermektedir;

I. Tüm testler için Test Planlarının, Çizelgelerin, yöntem beyanlarının, test kaydı belgelerinin ve hata raporlaması için prosedürlerin oluşturulması

II. Testlerle ilgili olan tüm test dokümantasyonu onay amaçlı sunulacaktır

III. Testlerin gerçekleştirilmesi için ekipmanın, test ekipmanının, test yazılımının, personel ve tesislerin temini

IV. Onaylanmış test prosedürlerine göre tüm testlerin başarılı bir şekilde gerçekleştirilmesi ve şahitli kabul testleri öncesinde hataların giderilmesi

V. Tüm test ilerleyişi ve sonuçları hakkında kalıcı kayıtların resmi ve sistematik bir şekilde tutulması

VI. Testlerin başarılı sonuçlanması için gerekli olan tüm iyileştirici işlemlerin gerçekleştirilmesi ve gerekliyse, testlerin yeniden yapılması

VII. Yukarıda belirtilen sorumlulukların her biri ŞİRKET'in onayına tabi olacaktır.

VIII. Birincil testlerin yapılacağı alan ŞİRKET ve YÜKLENİCİ arasında anlaşılarak belirlenecektir.

g) YÜKLENİCİ, aşağıdakileri içerecek, ancak ihtiyaç duyması durumunda test için gerekli olan diğer ekipman ve hizmetleri temin edecektir:

I. Test araçları ve simülasyon ortamı

II. Sistem fonksiyonlarının ve performansın tam olarak test edilebilmesi için özel test ekipmanı, simülatörler ve test yazılımı

III. Test edilen alt-sistemin bir parçası olmasa da YÜKLENİCİnin tedariki olarak belirtilen diğer sistem kalemleri

11.1.2 Testlerin Bildirimi

YÜKLENİCİ, Proje Zaman Çizelgesi dokümanının bir parçası olacak şekilde planlanan test tarihlerini gösteren ana plan temin edecektir ve herhangi bir değişikliğin olması halinde testlerden en az 14 (on dört) gün önce bu planı güncelleyecektir. YÜKLENİCİ, şartnamede belirtilen testlerden önce kendi ön testlerini yaptıktan sonra birincil ve ikincil testlere uygun olduğunu 14 gün önceden yazılı olarak ŞİRKET'e bildirecektir.

11.1.3 Test Prosedürleri ve Sonuç Belgesi

YÜKLENİCİ, tüm testler için test prosedürleri ve sonuç belgeleri hazırlayacaktır. Ayrıca, Teknik Şartname uyumluluk maddeleri tüm gereksinimlerin testlere dahil edildiğini göstermek amacıyla detaylı bir çapraz referans listesi de hazırlanacaktır. Tüm testler ile geçici kabul testleri için ayrı test prosedürleri ve sonuç belgeleri hazırlanacaktır. Tüm test prosedürleri ve sonuç belgeleri, ŞİRKET'in gözden geçirmesine ve onayına tabidir. Test sonuçları belgesi,

tedarik edilen ekipman, yazılım ve hizmet için kalıcı kalite güvence kaydının bir parçası olarak saklanacaktır.

11.1.4 Testlerin Gerçekleştirilmesi

a) YÜKLENİCİ, testleri onaylanmış prosedüre göre gerçekleştirecektir ve sonuçları sonuçlar belgesinde belirtecektir.
b) Her bir fonksiyon testi maddelerinin %70'in altında başarılı olması, fonksiyon testinin başarısız olarak değerlendirileceği anlamına gelecektir.
c) Test maddeleri, aşağıdaki durumlar halinde başarısız olarak kabul edilecektir:
   I. Test sonucunun test prosedüründe belirtilen beklenen sonuca uygun olmaması,
   II. Test sonucunun test prosedüründe belirtilen beklenen sonuca uygun olması, ancak ŞİRKET tarafından hata olarak görülen, beklenmeyen veya açıklanamayan olayların meydana gelmesi.
d) Testlerin doğruluğunu sağlayabilmek amacıyla YÜKLENİCİ tarafından sağlanan çalışma elkitapları ve diğer dokümanlar, testler esnasında eksiksiz kullanılacaktır. YÜKLENİCİ, ŞİRKET ile iş birliğinin tüm proje boyunca sürdürülmesi ve ortak çalışma ve testlerin gerek proje takvimi gerek ise teknik gereksinimler açısından düzgün ve eksiksiz bir şekilde gerçekleştirilmesinden sorumlu olacaktır.

11.1.5 Arızalar

a) YÜKLENİCİ, test esnasında tespit edilen tüm hataları giderecektir ve eğer test başlığında başarılı olduğuysa testlerin ikincil testlerde değilse birincil testlerde tekrar edilmesini sağlayacaktır.
b) ŞİRKET, sonuçlara göre ekipmanın önemli ölçüde Sözleşme gerekliliklerıyle uyumlu olmadığını göstermesi halinde herhangi bir testin tekrarlanmasını veya bırakılmasını isteme hakkına sahiptir.
c) ŞİRKET, YÜKLENİCİ tarafından tespit edilen, ancak testleri yürütümü esnasında veya en geç 24 saat içinde ŞİRKETe raporlanmayan herhangi bir hatanın ortaya çıkması halinde herhangi bir testi askıya alma hakkına sahiptir. Bu durumda ŞİRKETe raporlama yapılan tarihe kadar ilgili test gerçekleştirilmeyecektir.

11.1.6 Tekrar Testleri

a) YÜKLENİCİ, testler esnasında tespit edilen her hatayı düzeltecek ve ilgili testi yeniden uygulayacaktır.
b) 2. tekrar testinde testlere şahitlik yapan, YÜKLENİCİnin tesislerinde veya test sahasında bekleyen ŞİRKET ve temsilcileri tarafından harcanan süre, ilgili personeller için, personel başına proje sözleşme bedelinin %0.02 i olarak YÜKLENİCİye ceza yazılabilecektir.
c) Testlerin tekrar etmesi durumunda, ŞİRKET danışmanının testlere katılımı süresince oluşacak masraflar (Ulaşım, konaklama, öğün yemekleri) YÜKLENİCİ tarafından karşılanacaktır.

11.2 Birincil Testler- Pilot Saha Kabul Testi

a) PSAT ile amaçlanan, tüm sistem kurulumları gerçekleşmeden önce ŞİRKET mevcut izleme sistemleri içerisinden seçilen RTU noktalarının, Şartnamede belirtildiği şekilde SCADA yazılımı üzerine aktarılması ve bu aktarımın doğru şekilde ve yeterlilikte yapıldığının ŞİRKET tarafından kontrol edilmesidir.

b) PSAT ayrıca veri aktarımı yapmayacak YÜKLENİCİler için merkezlere ait çizilen ekran görünümleri ve veri girişlerine ilişkin ‘’Design Freeze(DF) niteliğinde olacaktır.

c) Söz konusu RTU noktaları, Mevcut Sistem ve Entegrasyonların Dahili bölümünde detayları verilen ve SCADA/DMS/OMS Sistemine aktarılması istenen noktalar içerisinden ŞİRKET tarafından belirlenecektir.

d) Mevcut sistemler içerisinden öz nitelik verileri el ile manuel girilecek ve EK-2.1 verilen tipikleri ŞİRKETİN belirlediği kapsamda SCADA yazılımına aktarılması YÜKLENİCİDEN istenecektir.

e) Hedeflenen yeterliliğin kontrolü için YÜKLENİCİ, gerekli olan en temel donanım/yazılım kurulumlarını gerçekleştirecek, ilgili merkezlerin teklif edilen SCADA yazılımı üzerinde gösterilmesini sağlayacaktır.

f) YÜKLENİCİ ayrıca, ilgili merkezlerin gösterilmesi ve mevcut sistemlerden aktarılan merkezlerin takibinin devam edebilmesi amacıyla ŞİRKET tarafından belirtilen bir noktaya iki (2) adet iş istasyonunu tüm gerekli yazılım/lisans ve ekran gereksinimleri birlikte kuracaktır. Bu iş istasyonları için gerekecek altyapı ŞİRKET’in sorumluluğundadır.

g) YÜKLENİCİNİN Proje çalışmalarına devam edebilmesi için, yukarıda bahsedilen testleri başarıyla tamamlaması ve ŞİRKET onayını alması gerekecektir. ŞİRKET onayı alınmadan Şartnamede belirtilen donanımların/yazılımların kurulmasına ve Proje çalışmalarını durdurma hakkını ŞİRKET saklı tutar.

11.3 İkincil Testler- Saha Kabul Testi

a) SCADA/DMS/OMS Sisteminin montajı ve konfigürasyonu sonrasında YÜKLENİCİ tarafından gerçekleştirilecektir. Saha kabul testi, kontrol merkezinde kurulumları gerçekleştirilen tüm ekipman ve sistemlerle birlikte birincil testlerin tekrarı niteliğinde olacaktır. Kontrol Merkezi için sağlanan tüm ekipman, sistem ve hizmetler test edilecektir.

b) Saha kabul testi, sahalardan toplanan gerçek zamanlı ve sistem veri girişlerinin tamamlanmasıyla gerçekleştirilecek ve saha kabul testinde simülasyon verilerinin kullanımına izin verilmesi ŞİRKET’in insiyatifindedir.

c) YÜKLENİCİ, ŞİRKET’e tespit edilen sonuçlardaki farklılıkları değerlendirmede destek olacaktır ve SCADA/DMS/OMS sistem işlevsellikleri ile ilgili tanımlanan problemleri çözecektir.

11.4 Noktadan Noktaya Testler

a) Noktadan Noktaya Testleri, YÜKLENİCİ ve ŞİRKET ortaklaşa yürütecektir.

b) SCADA kabinlerinin yeniden çizilmesi,sinyallerin eklenmesi ve haberleşme linklemesi yapılması ŞİRKET sorumluluğunda olup , çalışma sürecinde alınan hataların gün içerisinde müdahelesi YÜKLENİCİ sorumluluğunda olacaktır.

c) SCADA kabinlerinin çizilmesi sonrasında tüm SCADA Kabinlerinde PTP ŞİRKET tarafından yapılacaktır. Testler esnasında sorun oluşması durumunda hataların gün

içerisinde müdahelesi YÜKLENİCİ sorumluluğunda olacaktır. Belirlenecek 5 istasyon için PTP sürecinde uzaktan anlık destek YÜKLENİCİ tarafından sağlanacaktır.

11.5 SCADA/DMS/OMS Sistemi Testleri

a) Kontrol Merkezi Haberleşme Network' ünün saha lokasyonları ile kontrol merkezleri (AKM ve ADKM) arasında başarılı bir veri haberleşmesine olanak tanıması gerekliliği ŞİRKET'in sorumluluğundadır.
EK-2.1 de belirtilen mevcut RTU ve EKK sinyallerinin SCADA/DMS/OMS sistemi içerisinde tanımlanması ŞİRKET sorumluluğundadır.

b) EK-2.2 kapsamındaki tüm SCADA işlevselliklerinin gerçekleştirilmesi için gerekli, IP konfigürasyonu, Sinyal işleme ve sahada devreye alınması işlerinin dışında kalan tüm işler YÜKLENİCİ sorumluluğundadır.

c) ŞİRKET ile yapılacak ortak çalışmada Kontrol Merkezi- RTU arasında tesis edilen haberleşmede IEC 104 protokolünün çalışabilirliği sağlanacaktır.

d) ŞİRKET ile yapılacak ortak çalışmada Kontrol Merkezi- Enerji Kalite Kaydedici (EKK) arasında tesis edilen haberleşmede Modbus TCP/IP protokolünün çalışabilirliği sağlanacaktır

e) YÜKLENİCİ, ŞİRKET'in belirlediği saha lokasyonlarını içerecek şekilde test prosedürlerini ve tüm gerekli dokümanları temin edecektir. YÜKLENİCİ, test prosedürleri ve dokümanları ŞİRKET'ın onayına sunacaktır.

f) Noktadan noktaya testler esnasında minör ya da major sorunların ortaya çıkması durumunda; YÜKLENİCİ kontrol merkezi sistemlerinin düzgün olarak çalıştığını ŞİRKET'e ispatlamakla ve tüm sorunların ortadan kaldırılması için ŞİRKET ile bir arada çalışmaktan sorumlu olacaktır. YÜKLENİCİ, noktadan noktaya testlerin gerçekleştirilmesi esnasında SCADA/DMS/OMS ve diğer tüm kontrol merkezi sistem ve ekipmanlarında meydana gelen tüm problemlerin tespit edilmesi ve giderilmesinden sorumludur.

g) Öte yandan; ŞİRKET; SCADA/DMS/OMS ve tüm kontrol merkezi sistemlerinin farklı saha cihazlarıyla birlikte çalışabilirliğini gözlemlemek için; saha kabul testlerinin tamamlanmasından önce; SEDAŞ Şebekesinde kullanılan tüm saha ekipmanlarıyla haberleşebilir olacaktır.

h) Fonksiyon testleri çalışması esnasında minör ya da major sorunların ortaya çıkması durumunda; YÜKLENİCİ kontrol merkezi sistemlerinin düzgün olarak çalıştığını ŞİRKET'e ispatlamakla ve tüm sorunların ortadan kaldırılması için ŞİRKET ve ŞİRKET için çalışan diğer firmalar ile bir arada çalışmaktan sorumlu olacaktır. Bu kapsamda kullanılacak farklı marka ve modeldeki cihazların teminini ŞİRKET sağlayacaktır.

11.6 Entegrasyon Testleri

a) BT Entegrasyonları başlığı altında bulunan GIS, OSOS, WFM, CRM, PRISM, EDVARS, TEDAŞ TALEP TAKİP ile ilgili entegrasyonlara yönelik testler gerçekleştirilecektir.

b) Bu entegrasyonlarla ilgili Stres testleri ayrıca değerlendirilecek olup aynı anda hat açmalarına yönelik yüklenmeler esnasında sistemin performansı değerlendirilecektir. Stres testlerinde uygulanan örnek senaryolara göre Sistem performansının operasyonel

faaliyetleri aksatmaması, yavaşlatmaması ve donmaların yaşanmaması gerekliliği istenecektir.

c) Stres testlerine ait örnek senaryoların kapsamı ŞİRKET ile kavramsalda değerlendirilecektir.

d) YÜKLENİCİnin GIS gerçek verilerini kullanarak SCADA Şebeke İşletim Modelini oluşturmak, gerçek ŞİRKET BT sistemleri verilerini kullanarak her bir ilgili SCADA/DMS/OMS fonksiyonunu başarılı bir şekilde çalıştırmak amacıyla GIS arayüzü için tüm fonksiyonel gereklilikleri yerine getirmek üzere bireysel test uygulaması beklenmektedir.

e) Saha kabul testinde simülasyona izin verilmeyecektir.

f) Saha Kabul test planı, YÜKLENİCİ tarafından hazırlanacak ve ŞİRKET proje ekibi tarafından onaylanacaktır.

g) Gerçek veriler, ŞİRKET'ın belirli bir bölgesi için veya testin gerçekleştirilebilmesi amacıyla temin edilecektir. Söz konusu pilot sahada GIS ile SCADA/DMS/OMS Sistemi arasındaki veri alış-verişinin sağlıklı bir şekilde yapılabildiği kontrol edilecektir.

h) Model, TEİAŞ TM noktasından başlayarak son uç noktaya kadar TM'den enerji alan tüm noktaları gösterecek ve tüm güç akışını şebeke modeli üzerinde gösterecek şekilde eksiksiz olarak SCADA/DMS/OMS ara yüz ekranlarına aktarılacaktır.

i) Yük akışını gösterir uygun renklendirmeler yapılacaktır.

j) Aktarılan model üzerindeki canlı uç noktalara ait I/O tagları vb. dinamik değişkenlerin SCADA ekranlarında gösterilmesinin kontrolü yapılacaktır.

k) Aktarılan model içerisindeki tüm devre elemanları (hat, bara, trafo, jeneratör, kesici, ayırıcı, yük vb.), kaynaktan-uç noktaya kadar birbirleri ile topolojik bağlantısallığı kurulacak şekilde otomatik olarak yapıldığı gösterilecektir.

l) DMS ve SCADA uygulamalarında kullanılacak şebeke elemanlarına ait öz nitelik verileri GIS entegrasyonu ile otomatik olarak alındığı kontrol edilecektir.

m) Trafo kodlarının GIS'ten alınanlar ile aynı tutulduğu kontrol edilecektir.

n) GIS Şebeke modeli üzerindeki güncellemelerin aktarılması periyodu ŞİRKET tarafından belirlenecektir. Güncelleştirmeler için sadece model üzerindeki değişen kısımlar alındığı, modelin bütünüyle yeniden aktarılması ihtiyacı olmayacağı, istenildiği takdirde toplu veri aktarımının da mümkün olabileceği kontrol edilecektir.

o) Sistemin üçüncü parti yazılımlar ile veri alış-verişi testleri gerçekleştirilecektir. Test planı YÜKLENİCİ tarafından hazırlanacak ve ŞİRKET proje ekibi tarafından onaylanacaktır. Testlerde tüm fonksiyonel tasarım şartlarının yerine getirildiğini gösteren bir çapraz referans tablosu da hazırlanacaktır.

p) Veri aktarımı ile ilgili SCADA/DMS/OMS Sistemi uygulamalarının testleri yapılacaktır. Kavramsalda belirlenecek olan arayüz ve entegrasyonlara ait performans ve stres testleri gerçekleştirilecektir.

q) BT entegrasyonu için, Şartnamede belirtilen tüm şartların yerine getirildiğini ve YÜKLENİCİ tarafından belirtilen performans ve işlevsel taleplerin karşıladığını gösterecektir.

r) Test sonuçlarına dayalı olarak ŞİRKET proje ekibinin kabulü alındıktan sonra SCADA'ya ilişkin olarak belirli modüller için harici sistem arayüzüne nihai kabul notu verilecektir.

11.7 Emre-amade Testleri

a) SCADA ve DMS/OMS sistemlerinin geçici kabul testi, saha kabul testlerinin tamamlanmasının ardından uygulanacaktır.

b) Geçici kabul testi, sistemin SKT'den sonra yapılan 720 saat emre amade testleri ile sistemin bütünüyle kullanımını sağlayacaktır.

c) Sistemin kullanılabilirliği, SCADA/DMS/OMS Sisteminin teknik şartnamede belirtilen gereklilikleri karşılayacak veya bunları aşacak şekilde işleyiş göstermesini ifade etmektedir. ŞİRKET, Dağıtım Şebekesini kontrol etmek ve izlemek amacıyla SCADA/DMS/OMS Sistemini kullanacaktır.

d) Geçici kabul testi, aşağıda belirtilenlerin yerine getirilmesi halinde test süresinin bitiminde tamamlanmış olacaktır:

I. Tüm SCADA/DMS/OMS uygulamalarının çapraz referans tablosunda iki tarafında mevcut olması.
II. Diğer sistemlerle entegrasyona ait sistemlerin çalışabilir olması
III. Geçici kabul testinin başarısız olması halinde geçici kabul testi gerekliliklerini karşılayabilmek amacıyla tekrarlanacaktır.
IV. YÜKLENİCİ tarafından belirtilen tüm veri değişim işlemlerinin kullanılabilir olması
V. Aktarılan tüm verilerin bütünlük ve doğruluk açısından doğrulanması
VI. Aktarılan verilere ilişkin tüm SCADA/DMS/OMS uygulamalarının mevcut olması
VII. Şartnamede belirtilen tüm arayüz gerekliliklerinin mevcut olması
VIII. Şartname içerisinde tarif edilen tüm entegrasyonların bilfiil gerçekleştirilmesi ve farklı senaryoların ele alınması.
IX. Geçici kabul testinin başarısız olması halinde geçici kabul testi gerekliliklerinin karşılanması için tekrar edilecektir.

11.8 Geçici Kabul

a) Geçici Kabul aşağıdaki koşulların yerine getirilmesinin ve YÜKLENİCİ tarafından Geçici Kabule hazır olduğu bildirilen sistemin en az 1 ay aktif ve sorunsuz çalışması ardından tamamlanmış sayılacaktır.

b) 1 aylık sürede herhangi bir sorunla karşılaşılması durumunda sorunun giderilmesinden sonra ŞİRKET 1 aylık süreci baştan başlatma hakkına sahiptir.

c) YÜKLENİCİ aşağıda belirtilen tüm hususları tamamladıktan sonra, Geçici kabule hazır olduklarını yazılı olarak ŞİRKET'e bildirecektir:

I. Tüm sunucu/iş istasyonu, yerel ağ vb. yedekli tariflenen donanımlar ile AKM ve ADKM arasındaki yedekliliğin Şartnamede belirtilen tüm gereksinimleri karşılayacak şekilde sağlanması,
II. SCADA/DMS/OMS uygulamalarının ve fonksiyonlarının kullanılabilir hale gelmesi,

III. ŞİRKETE ait mevcut izleme ve kontrol sistemlerinin tümünün SCADA/DMS/OMS Sistemine aktarılması,
IV. GIS ve OMS ile tüm veri aktarımı ile entegrasyon çalışmalarının tamamlanması,
V. GIS Elektrik Şebeke Modelinin tamamının öz nitelik verileri SCADA ekranları üzerine aktarımının gerçekleştirilmesi,
VI. Aktarımı yapılan tüm verilerin bütünlük ve tekillik açısından doğrulanması,
VII. Şartnamede belirtilen tüm arayüz gereksinimlerinin karşılanması,
VIII. SCADA/DMS/OMS Sistemi performans testlerinin istenilen düzeyde başarılı olması,
IX. Proje iş-bitim (as-built) dokümanlarının tamamının teslim edilmesi.

d) ŞİRKET, Geçici Kabullere ait yukarıda belirtilen koşulların en az birinin tamamlanmadığını veya donanım ve SCADA/DMS/OMS yazılımların şartname isterlerinin karşılamadığını ya da kusurlu olduğunu tespit ederse, Geçici Kabul çalışmaları durdurma veya kayıt altına alınan bir eksik listesi ile Geçici Kabul yapma hakkına sahiptir.
e) İlgili Geçici Kabul eksikliklerinin Kesin Kabule kadar tamamlanması YÜKLENİCİNİN sorumluluğundadır.
f) YÜKLENİCİ bütün giderleri kendisine ait olmak üzere tamamlanmamış ya da kusurlu/eksik görülen kısımların sorunlarını giderecektir.
g) Geçici kabul çalışmalarına yeniden başlanabilmesi için YÜKLENİCİ yeniden müracaat edecektir. YÜKLENİCİ bu yükümlülüğünü yerine getirmezse, giderleri YÜKLENİCİ ye ait olmak üzere ŞİRKET bu çalışmaları yapabilecek ve varsa kusurları giderebilecektir.

12. Eğitim

12.1 Genel

a) YÜKLENİCİ, Şartname kapsamında gerçekleştirilen tüm işleri, ilgili personeli kapsayacak şekilde ve zamanlarda projenin uygulanma aşamalarını uygun eğitimlerle bila bedel yürütecektir.
b) Eğitim programı, ŞİRKET personelinin operasyonel, sistem mühendisliği konularında tam bir eğitimden geçmesini sağlayacaktır.
c) Eğitimler çoklu oturum şeklinde yönetilecektir. Eğitim planı ve içeriği sistem mühendisleri ve işletme operatörler için ayrı olacak şekilde tasarlanacaktır.
d) YÜKLENİCİ, eğitimin başlangıcından en az (bir) 1 ay önce eğitim plan ve dokümanlarını onay için ŞİRKET'e teslim edecektir. Eğitimler esnasında tüm katılımcılara birer nüsha ilgili eğitime ait matbu doküman temin edilecektir.
e) Her bir eğitimin içeriği aşağıdaki bilgileri içerecektir;
I. Eğitimin adı,
II. Eğitimin süresi,
III. Eğitim verilecek yer,
IV. Eğitimden yararlanacak personel türü,
V. Eğitime katılacakların vasıflarıyla ilgili ön koşullar,

VI. Hedefler, örneğin eğitimin geliştirmek istediği vasıflar,
VII. Amaçlar, örneğin geliştirilen vasıfların nasıl kullanılacağı,
VIII. Eğitim aktivitelerinin tanımı,
IX. Eğitim dokümantasyonun tanımı.

f) Eğitim sonunda; ŞİRKET çalışanları, sistemi kontrol edebilecek, işletebilecek, izleyebilecek, denetleyebilecek, sistemdeki donanımlara ait arızaları tespit edebilecek ve bakımını yapabilecek seviyeye geleceklerdir. Bu eğitimler sonucunda; ŞİRKET çalışanları, arızanın niteliğine göre, YÜKLENİCİ'nin yapabileceği durumlardaki arızalara da müdahale edip ekipmanın onarım ya da bakımını yapabilecek duruma geleceklerdir.
g) ŞİRKET'in istemesi halinde YÜKLENİCİ mevcut programa ilave eğitim verecektir.
h) YÜKLENİCİ eğitimin tamamlanmasının ardından katılanların seviyesini belirlemek amacıyla bir sınav düzenleyecek ve başarılı olanlara eğitim sertifikası verecektir. Başarısızlık oranının % 50 ve yukarısında olması durumunda, eğitim tekrarlanacaktır. ŞİRKET yetkililerinin eğitimi yetersiz görmesi halinde YÜKLENİCİ'ye istediği eğitimleri tekrar ettirme hakkı olacaktır.
i) Şartnamede belirtilen süre ve kapsam haricinde Garanti süresince yılda 1 kez 2 gün genel bilgilendirme eğitimi verilecektir.
j) Şartname dahilinde belirtilen detaylı tasarımlara bağlı olarak, eğitimler en az aşağıdaki bentlerde belirtilenleri kapsayacak ancak YÜKLENİCİ'nin kapsamı arttırabilmesi mümkün olacaktır.
k) Eğitimler kendi alanlarında uzman eğitmenler tarafından verilecektir. YÜKLENİCİ her bir eğitmenin özgeçmişini ve çalışma sahasını ŞİRKET'in onayına sunacaktır. ŞİRKET'in eğitmenin değiştirilmesini isteme hakkı vardır.
l) Tüm eğitimler, eğitim notları ve dokümantasyon'Türkçe ve İngilizce' olarak hazırlanacaktır. Eğitimlerde gerekli tüm eğitim materyalleri YÜKLENİCİ tarafından sağlanacaktır. Eğitime katılan herkese teknik manüellerin kopyaları ve diğer tüm dokümanların basılı hali ve elektronik sürümleri verilecektir.
m) Yurtdışında SCADA/DMS/OMS sistemini kullanan referans bir firmada, Şirketin 5 personeline 5 gün süreli sistemin işlevselliğini gösterir yerinde eğitim düzenlenecektir. Eğitimde yer alacak 5 şirket personeli için gerekli tüm ulaşım, seyahat, tam konaklama masrafları yüklenici tarafından karşılanacaktır. Türkiye içi ulaşım giderleri de dahil olmak üzere, pasaport, vize, yurtdışı çıkış harcı ŞİRKET sorumluluğunda olacaktır.

12.2 SCADA/DMS/OMS Sistemi Eğitimleri

12.2.1 Genel

SCADA/DMS/OMS Sistemi eğitimleri, sistem mühendisleri ve işletme operatörleri için ayrı olmak üzere iki farklı kapsamda gerçekleştirilecektir. Eğitim planı, teklif ile sunulacaktır. Eğitim zaman planı sözleşme imzalanmasından sonra 60 gün içerisinde ŞİRKET'in onayına sunulacaktır.

12.2.2 Sistem Mühendisleri Eğitimi

a) Sistem mühendisleri için yapılacak eğitimler her kapsam için tek oturumda gerçekleştirilecektir.

b) SCADA Yazılımı ve DMS Uygulamaları Eğitimi önerilen SCADA yazılımının ve DMS uygulamaların üretildiği ve geliştirildiği lokasyondaki eğitim merkezinde ve bu yazılımların/uygulamaların üretici firmanın uzman mühendisleri ve proje süresi içerisinde geliştirilmesi için çalışan proje ekibinde görev almış uzman mühendislerce verilecektir.

c) Bu eğitimler asgari olarak aşağıdaki konuları içerecek fakat bunlarla sınırlı kalmayacaktır;

I. Sistem tasarımı ve detaylı açıklaması,

II. Yazılımların/uygulamaların sistem üzerine kurulumu, parametreleme, devreye alma vb.

III. SCADA Uygulamaları,

IV. DMS Uygulamaları,

V. Ekran oluşturma ve düzenleme,

VI. Veri tabanı kaydı ve düzenleme,

VII. Haberleşme protokolleri ve parametrelenmesi,

VIII. Raporlama, arşivleme, trend vb.

IX. Sistem yedeklemesi,

X. Tanılama prosedürlerinin yürütülmesi ve çıktıların yorumlanması,

XI. Yeni yazılımların/uygulamaların/modüllerin eklenmesi işlemleri vb.

XII. Üçüncü parti yazılımlar ile entegrasyon.

d) Bu eğitimlerin çeşitleri ve süreleri minimum aşağıdaki gibi planlanacaktır.

- GENEL BİLGİLENDİRME bir (1) gün
- SCADA-beş (5) gün
- DMS-iki (2) gün
- OMS-dört (4) gün
- CBS VE DİĞER ENTEGRASYONLAR-üç (3) gün
- VERİ GİRİŞİ-yedi (7) gün
- Admin-beş (5) gün

e) Bu eğitimlere ŞİRKET personelinden altı (10) kişi katılacak olup katılımcılara ait tüm ulaşım, seyahat ve tam konaklama masrafları YÜKLENİCİ tarafından karşılanacaktır. Eğitimler sonrasında katılımcılara ait üretici onaylı eğitim sertifikaları teslim edilecektir.

f) SCADA ve DMS mühendislik eğitimleri, YÜKLENİCİnin merkez ofisinde verilecek olup. Diğer eğitimler ŞİRKET lokasyonunda verilecektir.

g) Eğitim içerikleri, eğitim planları birlikte teklif esnasında sunulacak ve ŞİRKET'in taleplerine göre değiştirilebilecektir.

h) Sistem eğitimleri YÜKLENİCİNİN deneyimli personelleri tarafından verilebilecektir.

12.2.3 Operatör Eğitimi

a) İşletme operatörleri için gerçekleştirilecek eğitimler ŞİRKET vardiya düzenlemeleri sebebiyle birbirleri ile aynı içerikte olan üç (3) farklı oturumda gerçekleştirilecektir. Her bir oturum en az on (10) iş günü olarak planlanacak ve her bir oturuma en az beş (5) ŞİRKET personeli katılacaktır. Söz konusu eğitimler ŞİRKET'in göstereceği lokasyonda yapılacaktır.

b) Bu eğitimler asgari olarak aşağıdaki konuları içerecek fakat bunlarla sınırlı kalmayacaktır;

I. Sistem tasarımı ve detaylı açıklaması,
II. SCADA Uygulamaları ve kullanımları,
III. DMS Uygulamaları ve kullanımları,
IV. OMS Uygulamaları ve kullanımları,
V. Raporlamalar,
VI. Donanımlara yönelik bakım ve arıza giderme.
VII. Tüm ekipmanların koruyucu ve düzeltici bakımlarının pratik olarak eğitimi.

13. Lisanslar

YÜKLENİCİ Sunulacak altyapı için gerekli veri tabanı (ADKM dahil) lisanslarını fiyata dahil etmelidir. İlgili lisanslar sistem ile uyumlu, mümkün olan en güncel sürüm ile teslim edilecek olup donanım kurulumu sonrası güncelleme hakkı en az 3 yıl geçerli olmalıdır. Lisanslar sınırsız süreli ve embedded (gömülü) olacaktır.

14. Raporlama

a) YÜKLENİCİ, sürekli olarak proje zaman planının takipçisi olacak ve haftalık ilerleme raporları düzenleyecektir. Haftalık İlerleme raporu, Sözleşmenin imzalanmasını takip eden ilk ayın sonundan itibaren her haftanın son çalışma günü içerisinde ŞİRKET'e teslim edilecektir. Bu raporlar her bir geçen hafta yapılan ilerlemeleri ve programlanan bitişe göre kümülatif ilerlemeyi yüzde olarak ifade edecek, proje zaman planında belirtilen maddeler doğrultusunda gösterecek ve böylece ŞİRKET ilerlemenin en son durumundan haberdar edilecektir.

b) Haftalık İlerleme Raporlarında ayrıca aşağıdaki başlıklar bulunacaktır:

I. Kapsam,

II. Haftaya ait faaliyetleri ve ilerleme bilgileri,

III. Malzeme temin durumu,

IV. Çalışan ekip durumu,

V. Sorunlar/Çözüm bekleyen işler,

VI. Gelecek haftanın temel faaliyetleri,

VII. İş programına göre ilerleme durumu,

VIII. Kapsam değişiklikleri,

c) Aylık veya ihtiyaç halinde uygulanabilecek yama/versiyon raporu YÜKLENİCİ tarafından paylaşılacaktır.

d) ŞİRKET ve YÜKLENİCİNİN katılımıyla ŞİRKET'in belirleyeceği lokasyonda iki (2) haftada bir proje değerlendirme toplantısı yapılacaktır. Toplantılarda YÜKLENİCİNİN Proje Yöneticisi hazır bulunacaktır. ŞİRKET gerekli gördüğü takdirde toplantı zamanını ve sıklığını değiştirebilecektir.

15. Garanti ve Kabul

15.1 Garanti Şartları ve Süresi

15.1.1 Genel

a) Garanti süresi sözleşme süresi işin tamamlanması sonrası 24 aydır.
b) YÜKLENİCİ, ŞİRKET hizmet alanında bulunan; dağıtım merkezlerinin uzaktan izlenmesi ve kumandasını sağlayan SCADA/DMS/OMS sisteminin, kontrol, destek ve arıza giderme hizmetlerinin yapılması, garanti süresince arızalı donanımlara ait parça değişimi, yenilenmesi işlerini Sözleşme konusu iş kapsamında ve ayrıca bir bedel talep etmeksizin sözleşme süresi boyunca gerçekleştirecektir.
c) Destek ve arıza giderme hizmetleri, mevcut sistemdeki hiçbir ürünün garanti kapsam ve süresini genişletmemekte olup sadece bu şartnamede tanımlanan hizmetleri kapsamaktadır.

15.1.2 Arıza Müdahale Süreçleri

a) YÜKLENİCİ, Proje Sözleşmesi ve Garanti süresi içinde yaptığı ya da yapmayı ihmal ettiği herhangi bir çalışma nedeniyle veya kurulumu yapılan sistemlerden kaynaklı ortaya çıkacak kusur ya da hasarın meydana gelmesi durumunda aşağıda belirtilen süreler içerisinde sorunu gidermekle sorumlu olacaktır.
b) Malzeme değişimi gerektiren arızalarda; YÜKLENİCİ tarafından stokta malzeme tutulmamasından veya YÜKLENİCİ tarafından siparişi verilen malzemenin tedarik süresinin uzamasından kaynaklı gecikmeler, aşağıda belirtilen müdahale sürelerinin uzamasına sebep teşkil edemez.

c) ŞİRKET arıza bildirimini yapacağı yöntemi (yazılı,mail vb) seçme hakkında sahiptir. Tüm süreçler yüklenici tarafından kurulan sistemden ilerletilecektir. Olası geliştirmeler için onay mekanizması da Şirkete tanımlanacaktır.

d) Yüklenici arıza bildirimini sistem üzerinden tarih saat bilgilerini içerecek ve hata nedenlerinin detayını Şirkete açıklayıcı şekilde bildirecektir. Şirket hata nedenlerini açıklanmaması halinde Yükleniciye sözleşmenin binde biri oranında ceza uygulanacaktır.
e) YÜKLENİCİ, Sözleşme kapsamında SCADA/DMS/OMS Sistemi üzerinden izlenmesi ve kontrolü sağlanan tüm merkezler ile alakalı yazılımsal problemlere (haberleşme arızaları vb.) aşağıdaki tablolarda belirtilen Hizmet Düzeyi Kriteri süreleri içerinde müdahale edecektir. Ayrıca entegrasyonlardan kaynaklı problemlere çözüm ortakları ile birlikte aşağıdaki tablolarda belirtilen Hizmet Düzeyi Kriteri süreleri içerinde

müdahale edecektir. SCADA Sunucuları ile saha arasındaki veri yolu trafiğinin kontrolü ve meydana gelecek sorunların düzeltilmesi YÜKLENİCİ sorumluluğunda olacaktır.

Problem Seviyesi	**Tanım**	**Müdahale Süresi**	**Müdahale Süresinin Aşılması Halinde Uygulanacak Cezai Şartlar**
Çok Yüksek	❖ Sistemin tamamen işlemez duruma gelmesi ya da çalışmaması, ❖ Sistemin önemli fonksiyonlarından birinin çalışmaması, ❖ Veri kayıplarının yaşanması. ❖ Sistemin içeriklerinin hiç görüntülenememesi, ❖ Afet, Kriz ve acil durum anında performansa yönelik operasyonel faaliyetlerin aksaması	1 Saat	Aşılan her bir saat için 500€
Yüksek	❖ Kullanıcıların %5 ya da daha fazlasının kullanımını engelleyen bir sorun çıkması, ❖ Sistemin bazı fonksiyonlarının doğru çalışmaması ya da kullanılamayacak kadar yavaş çalışması, ❖ Sistem içeriklerinin doğru görüntülenememesi.	4 Saat	Aşılan her bir saat için 400€
Orta	❖ Kullanıcıların %5 ya da daha azının kullanımını engelleyen bir sorun çıkması, ❖ Sistem içeriklerinin doğru görüntülenememesi.	8 Saat	Aşılan her bir saat için 300€
Düşük	❖ Tekrarlanmayan hataların bulunması, ❖ Sistemin daha iyi çalışması için gerekli düzeltmelerin yapılması.	1 Gün	Aşılan her bir gün için 200€

Tablo-3: Problem Kriterlerine Göre Müdahale Süresi ve Cezai Koşullar Tablosu

f) Bildirilen arızalar, geliştirmeler için YÜKLENİCİ firma ile SLA raporunu içerecek şekilde Ticket sistemi geliştirilecektir. Sistemin geliştirilmesi, lisansı ve her türlü giderleri YÜKLENİCİ'ye aittir.

15.2 Kesin Kabul

a) Geçici kabul tutanağının ŞİRKET tarafından onaylanmasından itibaren işleyecek 24 (yirmi dört) aylık garanti süresinin bitiminden sonra Kesin Kabul yapılacaktır.

b) Kesin Kabul işlemleri için YÜKLENİCİ, ŞİRKET'ine yazılı bildirimde bulunmalıdır. YÜKLENİCİ tarafından yapılacak yazılı bildirimin ŞİRKET'ine ulaşmasından itibaren 30 (otuz) gün içerisinde kabul işlemleri tamamlanacaktır.

c) Eğer Geçici Kabul bir eksik listesi ile yapıldıysa söz konusu eksikliklerin kesin kabule kadar tamamlanması YÜKLENİCİ sorumluluğundadır. Geçici Kabul eksik listesinin tamamlanması Kesin Kabul için bir ön şarttır.

d) YÜKLENİCİ, söz konusu kabule katılmakla yükümlü olacaktır. Kesin Kabul tutanağının YÜKLENİCİ tarafından imzalanmaması halinde, ŞİRKET tarafından tutulacak Kesin Kabul kayıtları YÜKLENİCİ tarafından kabul edilmiş sayılır.

16. İşin Yürütülmesi için Gerekli Personel ve Araç, Gereç ve Malzemeler

Sözleşmeye konu olan işe ilişkin gerekli makine, ekipman, işyerleri, malzemeler ve çalışanların teminini sağlamakla YÜKLENİCİ sorumludur.

17. Diğer

17.1 Proje Zaman Planı

YÜKLENİCİ, taslak proje zaman planını paylaşacaktır. Proje zaman planında, bu şartnamede belirtilen iş kalemlerini gerçekleştirmek için planlanan tarihleri sunacaktır.

17.2 Sapmalar

a) YÜKLENİCİ, bu şartnameden var ise sapmalarını liste halinde paylaşacaktır. Verilen sapma listesi iş bu şartnamenin ana ve alt başlıklarında/ maddelerinde belirtilen fonksiyon özelliklerinin tamamı için olmaz.

b) Ayrıca sapma listesi toplamda en fazla 10 (on) özellik için verilebilir. ŞİRKET bu sapma listesini, mevcut işletme koşullarına ve bağlı olduğu yönetmeliklere uygunluğuna göre kabul etmeme hakkını saklı tutar.

c) Bu listede açıkça belirtilmeyen şartname maddeleri kabul edilmiş sayılacaktır.

18. Ekler

EK-2.1. SCADA ve Üretim Tesisleri Tepiklerine Ait Sinyaller

EK-2.2. SCADA Kapsamındaki Mevcut Kabinler

EK-2.3. Elektrik Dağıtım Sektörü Siber Güvenlik Yetkinlik Modeli Teknik Kontrol Maddeleri

EK-2.4. EPDK Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Referans Topoloji

EK-2.5.Tedarik Sürekliliği Kayıt Sistemi Kuruluna ve Entegrasyonuna İlişkin Yükümlülükler