AKARYAKIT İSTASYONLARI OTOMASYON SİSTEMLERİNDE ARANILAN ŞARTLARA İLİŞKİN TEKNİK KILAVUZ

Sürüm 1.0

İÇİNDEKİLER

1 GİRİŞ

Bu Kılavuz, dağıtım şirketleri tarafından akaryakıt istasyonlarında kurdurulma zorunluluğu getirilen otomasyon ve merkez yazılımlarının standardını ve bu yazılımların birbirleri ile olan iletişim kurallarını tanımlamak ve çevre birimleri ve haberleşme kurallarını belirtmek ve istasyon otomasyon sistemlerinde bulunması gereken asgari temel, teknik ve fonksiyonel özellikleri belirlemek amacı ile hazırlanmıştır.

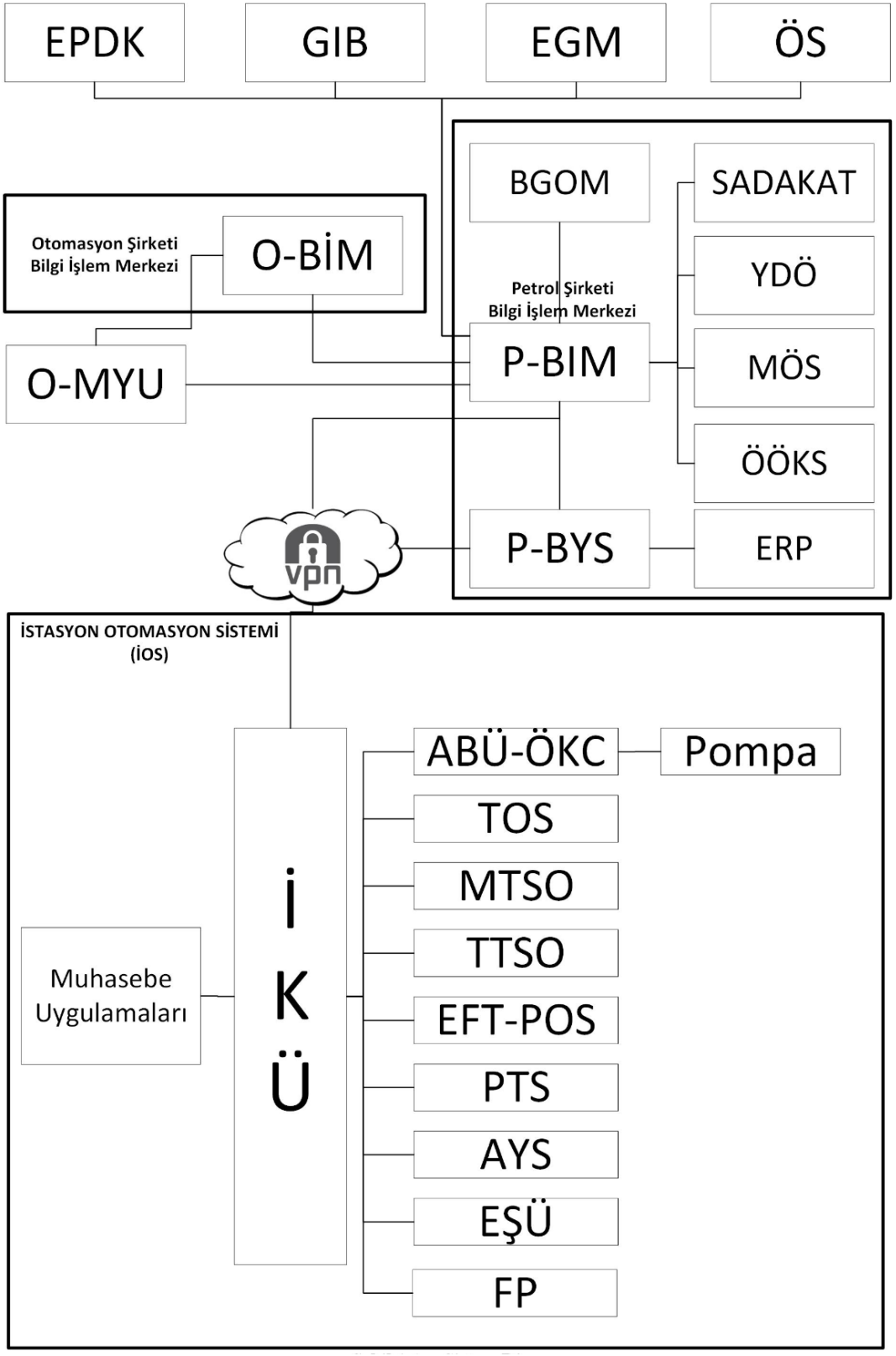
Akaryakıt, LPG, doğalgaz vb. istasyonlarından (bundan sonra istasyon olarak geçecektir) yapılan satışlarda, akaryakıt pompalarına bağlanan ödeme kayıt cihazları tarafından başlatılan işlemlerin istasyon kontrol ünitelerine aktarılması esastır.

2 TANIMLAR ve KISALTMALAR

Bu Teknik Kılavuzda yer verilen kısaltmalar ve anlamları aşağıdaki tabloda belirtilmiştir.

Kısaltma	Açıklama
ABÜ	Ara Birim Ünitesi
AS	Akıllı Switch (Anahtar)
BGOM	Bilgi Güvenliği Operasyon Merkezi
EFT/POS	EMV Uyumlu Kartlı veya Temassız Ödeme Sistemleri Terminali
EGM	Emniyet Genel Müdürlüğü
EPDK	Enerji Piyasası Düzenleme Kurulu
EPDK-DR	EPDK Denetleme Raporu
ERP	Kurumsal Kaynak Planlama
EŞÜ	Elektrik Şarj Ünitesi
FP	Fiyat Panosu
GİB	Gelir İdaresi Başkanlığı
GİB BS	Gelir İdaresi Başkanlığı Bilgi Sistemi
GMP	GİB Mesajlaşma Protokolü
İOS	İstasyon Otomasyon Sistemi
IP	İnternet Protokol
İKÜ	İstasyon Kontrol Ünitesi
LPG	Sıvılaştırılmış Petrol Gazı
MÖS	Mobil Ödeme Sistemi
MTSO	Müşteri Tanıma Sistemi Okuyucusu
O-MYU	Otomasyon Mobil Yönetim Uygulaması
O-BIM	Otomasyon Bilgi İşlem Merkezi. İOS ile Maliye, EPDK, GIB arasındaki iletişimi sağlar.
ÖKC	Akaryakıt Pompalarına Bağlanan Ödeme Kaydedici Cihaz
ÖÖKS	Ön Ödemeli Kart Sistemi
ÖS	Ödeme Sistemleri (Banka & Aracı Kurumlar)
P-BYS	Petrol Şirketi Bilgi Yönetim Sistemi
PTS	Plaka Tanıma Sistemi
ROUTER	Yönlendirici
SAM	Güvenli Erişim Modülü (Secure Access Module)
TKÜ	Taşıt Kimlik Ünitesi
TOS	Tank Otomasyon Sistemi
TTS	Taşıt Tanıma Sistemi
TTSO	Taşıt Tanıma Sistemi Okuyucusu
TYS	Taşıt Yıkama Sistemi
VPN	Sanal Özel Ağ (Virtual Private Network)
WS	Web Servis
YDÖ	Yanlış Dolum Önleme
YOS	Yakıt Otomasyon Sistemi

Şekil 1.A'da IOS genel sistem diyagramı ve sistemlerin birbirleri ile olan bağlantıları çizim halinde sunulmuştur.



3 İstasyon Otomasyon Sistemi (İOS)

İstasyon Otomasyon Sisteminde olması gereken temel teknik özellikler aşağıdaki tabloda gösterilmiştir.

İOS ve İOS'a bağlanacak çevre birimleri temel teknik özellikler tablosu (X=Zorunlu; İ=İhtiyari; 0 =Yok)

Temel Teknik Özellikler İOS

NO	TEMEL TEKNİK ÖZELLİKLER	İOS
1	**İstasyon Otomasyon Sistemi (İOS)**	**X**
1.1	*İstasyon Kontrol Ünitesi (İKÜ)*	X
1.2	*İKÜ Klavye Ünitesi*	X
1.3	*İOS Kabini*	X
1.4	*İOS Kesintisiz Güç Kaynağı (UPS)*	X
1.5	*Kullanıcı ve Müşteri Ekranı*	X
1.6	*İKÜ Yazılımı Genel Özellikleri*	X
1.7	*İKÜ Kullanıcı Yetkilendirmesi*	X
1.8	*Veri tabanı Erişim Güvenliği*	X
1.9	*Çevresel Donanım Erişim Güvenliği*	X
1.10	*Çevre Birim Kontrolü & Alarm*	X
1.11	*Otomatik Güncelleme*	X
2	**Bilgi Güvenliği Operasyon Merkezi (BGOM)**	**X**
2.1	*Veri tabanı*	X
2.2	*Olay Kayıt Özelliği*	X
2.3	*Raporlar*	X
2.4	*Güvenli Veri İletimi*	X
2.5	*Kimlik Doğrulama*	X
2.6	*Yazılım yetkilendirme şifrelemesi*	X
3	**Tank Otomasyon Sistemi (TOS)**	**X**
3.1	*Tank Otomasyon Verilerinin Saklanması*	X
4	**Katma Değerli Hizmetler**	
4.1	*Müşteri Tanıma Sistemi Okuyucusu (MTSO)*	İ
4.2	*Taşıt Tanıma Sistemi Okuyucusu (TTSO)*	İ
4.3	*EFT/POS*	İ
4.4	*Plaka Tanıma Sistemi (PTS)*	İ
4.5	*Taşıt Yıkama Sistemi (TYS)*	İ
4.6	*Mobil Ödeme Sistemi (MÖS)*	İ
4.7	*Ön Ödemeli Kart Sistemi (ÖÖKS)*	İ
4.8	*Grup Kampanya, Kupon, Promosyon vb. Uygulamalar*	İ
4.9	*Fiyat Panosu*	X
4.10	*Otomasyon Mobil Yönetim Uygulaması (O-MYU)*	İ
4.11	*Taşıt Yakıt Tipi Doğrulama Sistemi (YDO)*	İ
5	**Otomasyon Şirketi Bilgi İşlem Merkezi (O-BİM)**	**X**
5.1	*Veri Tabanı*	X
5.2	*Olay Kayıt Özelliği*	X

5.3	*Güvenli Veri İletimi*	X
5.4	*Kimlik Doğrulama*	X
5.5	*Yazılım Güvenliği*	X
5.6	*Sunucu*	X
5.7	*Acil Durum*	X
6	**Petrol Şirketi Bilgi Yönetim Sistemi (P-BYS)**	**X**
6.1	*İşletim Sistemi*	X
6.2	*Veri Tabanı*	X
6.3	*Olay Kayıt Özelliği*	X
6.4	*Güvenli Veri İletimi*	X
6.5	*Kimlik Doğrulama*	X
6.6	*Yazılım Güvenliği*	X
6.7	*Sunucu*	X
6.8	*ERP*	X
6.9	*EPDK 1240 Sayılı Kurul Kararı Uygunluğu*	X
6.10	*GİB Bilgi Sistemleri ile Haberleşme*	X
6.11	*Özel Sanal Ağ - Virtual Private Network (VPN)*	X
6.12	*Yönlendici (Router)*	X
6.13	*P-BYS Haberleşmesi*	X
6.14	*Kapalı Bilgisayar Ağı*	X
6.15	*Router*	X
6.16	*Kullanıcı Yetkilendirilmesi*	X
7	**Servis Organizasyonu**	**X**
7.1	*Olağanüstü Durum Merkezi*	X
8	**Mühürleme**	**X**
8.1	*İKÜ Mühürlemesi*	X
8.2	*Tank Kontrol Ünitesi Mühürlemesi*	X
8.3	*Tank Seviye Ölçüm Çubukları Mühürlemesi*	X

3.1 İstasyon Kontrol Ünitesi (İKÜ)

İstasyonlarda konumlandırılan İKÜ ve alt yazılımlarının tamamının üzerinde çalıştığı, fiziksel iletişim ara yüz desteği bulunan bilgisayar tabanlı kontrol ünitesidir. İKÜ, pompa, tank ve diğer birimlere kablolu veya kablosuz olarak bağlanabilir. İOS (İstasyon Otomasyon Sistemi) ve diğer yazılımların ürettiği tüm verileri (satış, dolum, stok, alarm) İKÜ üzerinde toplanır.

3.1.1 İKÜ Donanım Özellikleri

- İKÜ üzerindeki işletim sistemi IPv4 ve IPv6 protokollerini desteklemelidir.
- İşletim sistemi desteği devam eden Windows sürümlerinden biri olmalıdır.
- Minimum Donanım Özellikleri
- İOS (İstasyon Otomasyon Sistemi) ve diğer yazılımların ürettiği tüm verileri (satış, dolum, stok, alarm) İKÜ üzerinde toplanır.
- İKÜ üzerindeki işletim sistemi IPv4 ve IPv6 protokollerini desteklemelidir.
- İşletim sistemi desteği devam eden Windows sürümlerinden biri olmalıdır.
- Minimum Donanım Özellikleri
- 8 GB Bellek
- Çoklu işlemi destekleyen minimum 32 bit işlemci
- Dahili disk 250 GB SSD

- 2 çıkışlı ethernet kartı
- Çevre birimler için I/O (RS232/ RS422/ RS485/ CL/ USB)

3.1.2 İKÜ Klavye Ünitesi

İKÜ kullanım ihtiyaçlarını karşılayacak şekilde "Q" veya "F" klavye dizilimine sahip olan tuş takımı ünitesidir. Alternatif olarak sanal klavye de (dokunmatik ekran) kullanılabilir.

3.1.3 İOS Kabini

İOS donanımlarının, haberleşme kablolarının ve elektrik kablolarının birleştirildiği ünitedir.

3.1.4 İOS Kesintisiz Güç Kaynağı (UPS)

YOS'a bağlı olan ve elektrik enerjisi ile beslenen tüm cihazların hem şebekede meydana gelen veya gelebilecek çöküntüler, yükselmeler, ani değişikler, harmonikler gibi gerilim dalgalanmalarına karşı koruyan hem de enerji kesintisi sırasında enerji üreterek sistemin devamlılığını sağlayan kesintisiz güç kaynakları tarafından beslenmesi gerekmektedir.

Satış anında yaşanabilecek elektriksel dalgalanmalar sonucu veri kaybı yaşanmaması için ABÜ' ye bağlı olan elektronik pompa beyinlerinin de kesintisiz güç kaynağı tarafından beslenmelidir.

Kesintisiz güç kaynağı, İOS'a bağlı tüm bileşenleri minimum 20 dk süresince çalıştırmalıdır.

3.1.5 Kullanıcı ve Müşteri Ekranı

İKÜ aşağıda özellikleri belirtilen 2 adet ekrana görüntü gönderme özelliğine sahip olmalıdır.

- **Kullanıcı Ekranı:** İKÜ üzerinde yapılabilecek tüm işlemlerin gösterilmesi gereken ekrandır. Kullanıcı izinleri doğrultusunda menü görünümü değişken olmalıdır. İKÜ işlevlerinin tamamı bu ekran üzerinden yapılmalıdır.
- **Müşteri Ekranı:** Müşteri ödeme noktasına konumlandırılan ve müşterinin anlık olarak satışları takip edebildiği, içerisinde plaka, miktar ve tutar bilgilerinin bulunduğu ekrandır.

3.1.6 İKÜ Yazılımı Genel Özellikleri

- İKÜ yazılımı, istasyon ağında bulunan tüm ÖKC ve Ara Birim Ünitesi (ABÜ) marka ve modelleri ile iletişim kurabilmesini sağlamalıdır.
- İKÜ yazılımı her satış sonrasında arabirim üzerinden pompa sayaç (totalizatör) bilgisinin başlangıç ve bitiş değerlerini kayıt altına alabiliyor olmalıdır.
- İKÜ yazılımı Özel Entegratörler ile GİB'e her satışı gerçek zamanlı gönderebilmelidir.

  Özel Entegratör'e gönderilecek bilgiler aşağıdaki gibidir;

  - Otomasyon Firması Tanımı
  - Petrol Şirketi Adı
  - İstasyon Adı
  - Mersis Numarası
  - Adresi
  - Pompa No
  - ÖKC Sicil Numarası
  - Tarih, Saat
  - Fiş No
  - Plaka / Satış tipi (Bidon, Transfer vb.)

- Ürün Adı
- Litre
- Birim Fiyat
- Toplam Fiyat
- KDV
- Toplam
- Ödeme Türü

- İKÜ Yazılımı, yerel filo veya özel müşteri tanımları için de elektronik ödeme sistemi (RFID anahtarlık, mifare kart, tag, mobil vs.) uygulama imkânına sahip olabilir, bu tipte müşteriler için gerçekleştirilen tüm işlemlerin ekstrelerini verebilir, düzenleme ile ilgili bilgi ve rapor üretebilir.
- ÖKClardan seçilen ödeme türleri (Nakit, Kredi Kartı vb.) otomasyon tarafından kayıt altına alınabilmeli ve raporlanabilmelidir.
- İKÜ yazılımı, elektronik ödeme sistemlerinden (kredi kartı, müşteri tanıma ve araç tanıma) bağımsız olarak çalışabilmelidir.
- ÖKC bazlı rapor alabilme imkânı bulunmalıdır.
    - Seri numarası (Yeni Nesil ÖKC)
    - ÖKC fiş numarası
    - Mali fişin içerdeği bilgiler
    - Z raporu (Yeni Nesil ÖKC)
    - X raporu (Yeni Nesil ÖKC)
- Gün sonu işlemi ÖKClar üzerinden (“Z” raporu) tek tek yapılabileceği gibi, aynı işlem otomasyon üzerinden gönderilen bir komutla yapılabilmelidir (Yeni nesil ÖKC için geçerlidir). Gün sonu raporu (“Z”), otomasyon sistemi üzerinden görüntülenebilmelidir.
- İstasyonlarda isteğe bağlı alınan vardiya sonu işlemi ÖKC’ler üzerinden (“ZZ” raporu) tek tek yapılabileceği gibi, aynı işlem otomasyon üzerinden gönderilen bir komutla yapılabilmelidir (Yeni nesil ÖKC için geçerlidir). Vardiya sonu raporu (“ZZ”), otomasyon sistemi üzerinden görüntülenebilmelidir.

    - Müşteri/Filo Adı
    - Araç Plaka
    - Dolum Tarihi
    - Dolum Saat
    - Fiş No
    - Pompa No
    - Tabanca No
    - Yakıt Tipi
    - Yakıt Litre
    - Yakıt Fiyatı
    - Tutar
    - Ödeme Tipi
    - Kart No
    - Araç Kilometre
    - Araç Motor Saati
    - ÖKC Seri Numarası

- İKÜ yazılımı, arabirime gönderdiği komutlar vasıtası ile satışı durdurabilmeli, yeniden başlatabilmelidir.
- İKÜ yazılımı, sistem parametre tablosunda bulunan tercihlere göre satış işlemi öncesi otorizasyon yapabilmelidir. (Araç-yakıt tipi doğrulama, kara liste kontrolü vb.)

- Satış öncesi otorizasyonu, akaryakıt satış görevlisi yetki kartı (mifare, RFID kart) ile gerçekleştirilebilmelidir.
- Pompa görevlisinin, tüm pompalar üzerinden satış yapmasına imkân vermelidir.
- İKÜ yazılımı, yakıt için kurulmuş, yeni nesil ÖKC'ye entegre veya market içerisinde bulunan elektronik ödeme sistemlerinin işleyişini destekleyecektir.
- İKÜ yazılımı, ön ödemeli ve/veya limitli otorizasyonu desteklemelidir.
- Müşteri ve taşıt tanıma işlemlerinde kullanılabilecek olan teknolojiler aşağıdaki gibidir;
    - Manyetik kart
    - Sadece okunabilir RFID ve diğer akıllı kartlar
    - Sadece okunabilir RFID taşıt kimlik ünitesi
    - İKÜ, bu sistemlerin okuyucuları ile iletişim kurabilmeli, uygulama ve üniteler İKÜ sisteminde aktif çalışabilir durumda olmalıdır.
- Pompa yakıt birim fiyatları, İKÜ üzerinden yetkili kullanıcılar tarafından değiştirilebilmelidir. Fiyatlar, anlık olarak veya planlanan bir tarih ve saatte geçerli olacak şekilde değiştirilebilmelidir.
- Sistem, yerel filo veya özel müşteri tanımları için de elektronik ödeme sistemi (RF anahtarlık, kart, TKÜ) uygulama imkanına sahip olabilir.
- İKÜ'de tank-pompa-tabanca eşleştirme özelliği olmalıdır. Tank-pompa-tabanca eşleştirme tablosu istasyon yetkilisinin beyanı ile birlikte yetkili servisler tarafından tutanak ile yapılmalıdır. Tank-pompa-tabanca eşleştirme tarihçesi, İKÜ ve P-BYS tarafında, kayıt altına alınmalıdır.
- İKÜ yazılımı kapsamında çalışan uygulamalar aşağıdaki şekilde olmalıdır;
  Windows Servisi: İKÜ'ye bağlı donanımların yöneten yazılımlardır. Bu yazılımlar herhangi bir kullanıcı ara yüzü ile ilişkilendirilmemeli, herhangi bir kullanıcı ara yüzünün kapatılması ile pasif hale getirilememelidir.
  Masaüstü veya İnternet Uygulaması: İKÜ yönetim panelleri ve raporlama araçlarını yöneten yazılımlardır.
- İKÜ, sahada gerçekleşen satış işlemini P-BYS 'ye göndermeden önce doğruluk kontrolü yapmalıdır. ABÜ'nün gönderdiği yakıt birim fiyatı ve hacim (litre) çarpılıp, toplam tutar ile karşılaştırılacaktır. Karşılaştırma sonucunda çıkan fark %5'ten büyük ise alarm üretilecektir. Bu alarm vardiya raporunda uyarı olarak gösterilecektir.
- İKÜ, MÖS, ÖÖKS, TTS, EFT-POS vb. sistemlerle entegre olarak tahsilat gerçekleştirilebilmelidir. İKÜ, ödeme sistemleri merkezleri ile P-BİM üzerinden, istasyon lokalindeki EFT-POS ile TCP/IP protokolü ile haberleşebilmelidir.

3.1.7 İKÜ Kullanıcı Yetkilendirmesi

- İstasyon Müdürü: İstasyon yetkilisi/sahibine verilmesi gereken ve aşağıdaki ekranlara erişim izni olan kullanıcıdır.
    - Vardiya İşlemleri
    - Pompa Otomasyon Sistemi Raporları
    - Tank Otomasyon Sistemi Raporları
    - Pompa Görevlisi Tanımlama İşlemleri
    - İndirim Tanımlama İşlemleri
    - Anlık İstasyon İzleme Ekranları
    - Cihaz Haberleşme Durum Ekranı
    - İstasyon Alarm Ekranı

- İstasyon Çalışanı: Kullanıcı tanımı istasyon müdürü tarafından yapılan ve aşağıdaki ekranlara erişim izni olan kullanıcı tipidir.
    - Anlık İstasyon İzleme Ekranları
    - Vardiya İşlemleri

- İstasyon Alarm Ekranı

- Teknik Servis: İKÜ 'ye yetkisiz erişimlerin ve müdahalelerin engellenmesi için olması gereken bir güvenlik katmanıdır. Bu kapsamda İKÜ içerisinde yer alan ve sadece yönetici yetkisindeki teknik servis personellerinin erişmesine izin verilen modüller bulunabilir.
- İKÜ yönetim paneli, İKÜ istasyon kurulum ayarları vs. bu modüllere erişimin parola ile korunması gereklidir.
- İKÜ uygulamasına admin/teknik servis haklarıyla erişim için sistem aşağıdaki maddeleri karşılamalıdır;
    - Parola dinamik olmalı, üretilen şifre tekrar üretilmemeli ve otomasyon firmasına ait bir güvenlik algoritması ile üretilmelidir.
    - Parola merkezi yönetim sisteminde üretilmeli ve kullanıcı girişi yapıldığında verilmelidir.
    - Kullanıcılara verilen parolaların tarihçesi O-BİM sisteminde kayıt altına alınmalıdır.
    - Parola alabilecek kullanıcılar O-BİM üzerinden aktif/pasif edilebilmelidir.

Yukarıdaki maddeler sayesinde, sabit bir parola kullanılma ve bu parolanın da yanlış ellere geçmesi riskinin önüne geçilmektedir.

- İKÜ yönetim paneli üzerinde yapılan tüm kullanıcı hareketleri kayıt altına alınması ve merkezi izleme sistemine doğrudan gönderilmelidir.

3.1.8 Veri tabanı Erişim Güvenliği

İKÜ bünyesinde kullanılan ve elde edilen bütün veriler veri tabanı içerisinde güvenli ve silinemeyecek şekilde ve saklanmalıdır. Veri tabanlarına erişimin güvenli bir parola ile korunması gereklidir. İKÜ ve alt modülleri dışında hiçbir yazılımın, veri tabanı erişimine izin verilmemesi önem arz etmektedir. Veri tabanına erişmesi gereken uygulamalar için gerekli yetkilere sahip kullanıcı tanımları ve yetkilendirmeleri yapılmalıdır. Bu yetkiler; sadece okuma, yedek alma, okuma-yazma şeklinde olabilir, hiçbir düzeydeki yetkilinin söz konusu verileri silme kabiliyeti olmamalıdır.

Veri tabanına IKÜ bünyesinde veya dışarıdan yapılan her işlem kayıt altına alınmalı ve P-BYS ' e doğrudan gönderilmelidir.

3.1.9 Çevresel Donanım Erişim Güvenliği

İKÜ'nün çalıştığı bilgisayar sistemlerinde USB, CD, DVD vb. harici donanımlara erişim kısıtlaması İKÜ tarafından yapılmalıdır. Yetkisiz kullanıcıların ilgili bilgisayara erişimi engellenerek verilerin güvenliği sağlanmalıdır.

3.1.10 Çevre Birim Kontrolü & Alarm

İKÜ, iletişimde olduğu ve destekleyen çevre birimlerinin (ABÜ, MTSO, TTSO vb.) seri numarası veya MAC adreslerini takip edebilmeli, onaysız değişen çevre birimlerin çalışmasına engel olabilmeli ve alarm üretebilmelidir. Bu alarmları anlık olarak P-BYS ve O-BİM'e iletmelidir.

3.1.11 Otomatik Güncelleme

İKÜ, sürüm değişikliklerini P-BYS üzerinden periyodik olarak kontrol edebilmeli ve güncel bir sürüm var ise tanımlanan zamana göre güncellemeyi alarak yeni sürüme otomatik olarak geçebilmelidir.

Hata durumunda bir önceki sürüme dönüş;

İstasyon otomasyon uygulaması, uzaktan güncelleme yapmadan önce, güncelleme sırasında karşılaşılabilecek olası problemleri göz önünde bulundurarak eski uygulamanın ve veri tabanının bir yedeğini almalı, ardından güncelleme işlemi başlatmalıdır. Güncelleme işleminin başarısız olması durumunda hem uygulama hem de veri tabanı geri dönülebilir olmalıdır. İKÜ üzerinde geriye dönük olarak uygulamanın iki eski sürümleri saklanmalıdır.

Sürüm güncelleme ve güncelleme tarihçesi raporlaması;

Sürüm güncelleme işlemi ardından İKÜ yazılımı, güncelleme işlem sonucunu P-BYS bildirmelidir. Bu bildirim içinde istasyon koduyla birlikte yapılan güncelleme işlemine ait detaylar ve güncelleme sonucu bulunmalıdır.

3.1.12 Bilgi Güvenliği Operasyon Merkezi (BGOM)

- BGOM (Bilgi Güvenliği Operasyon Merkezi) sistemi, İOS'ta oluşan olay günlüklerini toplayabilmelidir.
- Veri tabanına yapılan erişimler BGOM'da toplanmalıdır. Yetkisiz kullanıcı erişimleri BGOM sistemi ile engellenebilmelidir.
- Veri tabanında yapılan her türlü işlem (okuma-yazma–güncelleme-silme), BGOM sisteminde saklanmalıdır.
- Veri tabanında yapılan sorgular detaylı olarak denetim günlüğünde saklanmalıdır.

Denetim Günlüğünde aşağıdaki bilgiler olmalıdır;

  - Kullanıcı
  - Bağlantı Kuran Adres (IP)
  - Veri tabanı
  - Tablo
  - Sütun ID
  - İşlem (Okuma-Yazma-Güncelleme-Silme)

- İstasyon otomasyonu sisteminde oluşan alarmlar, BGOM sisteminde korelasyonlara dahil edilmeli ve gerekli durumlarda alarmı tetikleyen etkenler için aksiyon alınmalıdır.
- İstasyon otomasyonu çevre birimlerinde bulunan uygulamaların SHA-256 Hash değerleri çıkartılmalı ve BGOM sisteminden otomatik olarak SHA-256 Hash sorgusu 3. Parti uygulamalara yapılabilmelidir.
- İstasyon otomasyonu çevre birimleri üzerindeki uygulama işlemleri gerçekleştirirken bir bozulmaya uğraması durumunda Hash değeri değişeceği için dosyanın bozulmaya uğradığını tespit edip dosyanın BGOM sistemi ile silinebilmesi sağlanmalıdır.
- İstasyon otomasyonu çevre birimlerinde solucan, truva atı, casus yazılım, reklam yazılımı, fidye yazılımı, illegal botlar, parazit kripto madenciliği yazılımı veya dolandırıcı yazılımı görülmesi halinde BGOM sistemi ile zararlı yazılım barındıran sistemin ağdan izole edilmesi sağlanmalıdır. Sistemde zararlı yazılım temizlendikten sonra sistemi ağa tekrar dahil edilebilmelidir.
- İstasyon otomasyonu çevre birimlerinde dosya bütünlüğü kontrolü yapılabilmelidir. Dosya bütünlüğü ile ilgili tüm veriler BGOM sistemi üzerinde toplanmalıdır.
- BGOM sistemi, istasyon otomasyonu çevre birimleri üzerinde aktif olarak çalışan güvenlik duvarında yapılacak kural değişikliklerini takip edebilmeli ve gerekli durumlarda kuralları güncelleyebilmelidir.
- BGOM sistemi istasyon otomasyonu çevre birimlerinde aktif olarak çalışmayan haberleşme portlarını izlemeli ve 1 ay süre sonunda hiç kullanılmayan portları firewall üzerinde otomatik kapatmalıdır.

3.1.13 Veri tabanı

Veri tabanı, üretilen bilgilerin saklandığı, erişim imkânı olan, yönetilebilen, güncellenebilen ve başka bir noktaya taşıma imkânı olan dosyalardır.

- Veri tabanı sistemi küme altyapısına sahip olmalıdır.
- Veri tabanı gerektiğinde İKÜ sisteminden ayrı bir alanda konumlandırılabilir olmalıdır.
- Veri tabanı sisteminde kullanıcı yönetimi yapılabiliyor olmalıdır.
- Bu veri tabanı içerisinde saklanacak olan bilgiler ayrı ama birbirleri ile ilişkili bilgi kümeleri halinde saklanmaktadır. Veri tabanı aşağıdaki özelliklere sahip olmalıdır:
    - Veri tabanına erişim, bir parola ile korunabilmelidir.
    - Veri kaydetme, düzenleme, sorgulama özelliğine sahip olmalıdır.
    - Saklanan verilere hızlı erişim için gerekli özelliklere (Indeks) sahip olmalıdır.
    - Veri tabanında kayıtlı bulunan bilgiler, silinmeye karşı koruyabilecek kullanıcı yetkilendirme mekanizması olmalıdır.
    - Veri tabanındaki veri bütünlüğünün otomasyon şirketinin sorumluluğunda olması nedeniyle veri tabanına olan erişimler otomasyon firmasının kontrolünde olmalıdır.

3.1.14 Olay Kayıt Özelliği

Otomasyon yazılımı içerisinde yapılan her türlü işlem (çevresel birimlerin haberleşme durumları, uygulama içerisinde gerçekleştirilen işlem ve fonksiyon detayları ve sonuçları, karşılaşılan sorunların ve hataların detayları vs.) esnasındaki olaylar ayrı ayrı ve detaylı bir şekilde ve son 90 günü kapsayacak şekilde saklanmalıdır. İhtiyaç duyulması halinde bu olay kayıtları yetkili servisleri tarafından incelenebilmeli ve otomasyon sistemi içerisindeki akışlar takip edilebilmelidir.

İKÜ önemli olay kayıtları aşağıdaki güvenlik özelliklerine sahip olmalıdır:

- Olay kayıtları kritiklik seviyesine (1 acil, 2 yüksek, 3 uyarı, 4 bilgi) göre sınıflandırılabilmelidir.
- Olay kayıtları doğru zaman bilgisi ile alınmalı ve bütünlüğü korunmalıdır. Zaman bilgisi P-BYS ile senkronize olacaktır.
- Kaydedilen olay bilgileri İKÜ'de saklanacaktır.
- İKÜ'de son 90 günü kapsayacak olay kaydı geriye dönük olarak ayrı bir veri tabanı içerisinde tutulacaktır.
- Acil kritiklik seviyesine sahip olay kayıtları saatlik olarak GİB'e O-BİM üzerinden iletilebilmelidir.
- Olay kaydı içerisinde İKÜ tekil olarak tanımlayacak bilgi de gönderilmelidir.
- Olay kayıtlarında IOS ID, olay kritiklik seviyesi, zaman bilgisi ve açıklama alanları bulunmalıdır.
    - Pompa Haberleşme kesintisi
    - ÖKC haberleşme kesintisi
    - Tank otomasyon haberleşme kesintisi
    - Prob haberleşme kesintisi
    - Veri tabanına İKÜ dışında yapılan tüm erişimler

3.1.15 Raporlar

İstasyonda gerçekleşen satış, dolum, tank stok vb. tüm süreçlerin raporlarının oluşturulduğu bölümdür. Asgari aşağıdaki raporlar içermelidir;

3.1.15.1 EPDK ve GİB Denetleme Raporu

- İstasyon Kimlik Bilgileri (Şirket/EPDK Lisans Numarası/Adres/İletişim)
- İOS Tedarikçi Bİlgileri (Şirket/Adres/İletişim)
- Pompa Marka/Model/Adet
- ÖKC Marka/Adet
- Tank Kontrol Ünitesi Marka
- Tank Seviye Ölçüm Çubuğu Adet
- Tank-Pompa-Tabanca Eşleştirmeleri
- Anlık Tank Envarter Raporu
- Alarm Raporları (Son 1 ay)

3.1.15.2 Satış Raporları

3.1.15.3 Vardiya Raporları

3.1.15.4 Tank Raporları

3.1.15.5 Totalizör Raporu

3.1.15.6 ÖKC Z Raporu (Yeni Nesil ÖKC için geçerlidir.)

3.1.15.7 ÖKC X Raporu (Yeni Nesil ÖKC için geçerlidir.)

3.1.15.8 ÖKC ZZ Raporu (Yeni Nesil ÖKC için geçerlidir.)

3.1.16 Güvenli Veri İletimi

İOS sisteminin her türlü veri iletimi güvenli bir yapı üzerinde olmalıdır. Başlıca veri akışları aşağıdaki gibi olmaktadır:

- Çevre birimler ile İKÜ arasındaki veri iletimi: İstasyon bünyesinde çalışan ve İKÜ için veri kaynağı niteliğinde olan bütün çevre birimler ile olan iletişimi kapsamaktadır.
- İOS sisteminin merkez ile olan veri iletişimi: İOS sistemi tarafından üretilen verilerin petrol şirketi merkezine iletilmesi ve petrol şirketindeki birtakım verilerin de İOS sistemine transfer edilmesi gerekebilir. Veriler istasyon ile merkez arasında SSL sertifikasıyla veya TLS v1.2 protokolü ile şifrelenerek gönderilmelidir. Merkez ile istasyon arasındaki ağ dışarıdan erişime kapalı olmalıdır.
- Dışa bilgi aktarımı: İOS sistemi tarafından üretilen bazı bilgilerin harici uygulamalar (puan yönetimi, muhasebe vs.) tarafından kullanımına imkân verebilmek için üretilen verilerin belirlenen bir desen ve kurallar ile dışarı aktarılabilme imkânı olmalıdır. Bu aktarım anlık veya belirli aralıklarla olabilir. Bu aktarım işlemi; özel tasarlanmış dosyalar veya XML formatına sahip dosyalar ile yapılabilmektedir.

3.1.17 Kimlik Doğrulama

İOS sistemi içerisindeki her bir otomasyon bileşeninin veya servisinin (bilgisayar, veri tabanı, windows servis vs.) kullanımının kimlik doğrulama yöntemi ile güvenlik altına alınması gerekmektedir.

Otomasyon şirketi çalışanlarının, Petrol Şirketi Merkez sunucularına erişmeden önce elektronik onay sürecinden geçmesi zorunludur. VPN üzerinden giriş yapılmak(login) istendiğinde;

- Petrol şirketi yetkilisi onay verdikten sonra bağlantı sağlanacaktır.

- Kullanıcıya özel tek seferlik şifre SMS olarak gönderilir, kullanıcı kendisine gönderilen şifreyi petrol şirketinin sistemine girerek ağ bağlantısı sağlanacaktır. Aynı şekilde Otomasyon şirketi çalışanları IOS'a erişirken O-MYU veya IOS üzerinden onay almalıdır.

3.1.18 Yazılım yetkilendirme şifrelemesi

İKÜ üzerinde çalışan yazılımlara yetkisiz erişimin engellenmesi zorunludur. İKÜ yazılımları içerisindeki modüllere erişim sağlanabilmesi için parola koruması olmalıdır. Özellikle istasyonun çalışmasını doğrudan ilgilendiren yönetim, kurulum ve ayarlar modüllerine giriş için parola korumasının olmalıdır.

Bilgisayar güvenliğini sağlamak amacıyla uzaktan yönetilebilir; konsol erişimleri denetlenebilir, kullanıcı ve uygulama kısıtlaması yapılabilir olmalıdır.

Antivirüs yazılımı yüklenebilir ve güncellemeler uzaktan yapılabilir olmalıdır. Gerektiğinde etki alanına üye yapılarak yerel ve grup politikalar uygulanabilmelidir.

Otomasyon şirketi, ISO 27001:2013 Bilgi Güvenliği Sistemi belgesine sahip olmalıdır.

3.2 Tank Otomasyon Sistemi (TOS)

Akaryakıt ve LPG istasyonlarında, satışı yapılan her ürün için bir veya birden fazla akaryakıt ve LPG tankı bulunmaktadır. Bu tanklardaki her türlü hareketin (dolum, seviye ölçümü, azalma, alarm vs.) kayıt altına alınması ve gerek duyulması halinde istenildiği zaman raporlanabilmesi gerekmektedir. Özellikle; 1240 sayılı EPDK Kurul Kararı kapsamında istasyondaki her türlü tank hareketinin merkezi olarak kayıt altına alınması ve izlenmesi kanuni bir zorunluluktur.

TOS, bütün tank hareketlerini izleyerek kayıt altına almakta ve elde edilen verileri belirlenen zaman aralıklarında P-BYS 'ye iletmelidir.

TOS donanımları, İKÜ'ye RS232, RS485, TCP/IP veya kablosuz haberleşme protokolleri ile bağlanabilir.

Tank seviye ölçüm çubuğu ;

- TOS seviye ölçüm çubukları, istasyonlarda yer alan tank seviyelerinin çaplarına bağlı olarak %100'nü ölçebilecek şekilde olmalıdır.
- TOS seviye ölçüm çubukları ile sıcaklık, su ve akaryakıt ürün seviyelerini maksimum ± 0,5 mm hassasiyetle ayrı ayrı ölçebilmelidir.
- TOS seviye ölçüm çubukları, yer altı tankları için uygun ölçülerdeki manşonlara monte edilebilmelidir.
- Yer altı tankları için ölçüm ve tekrarlanabilirlik hassasiyeti minimum %0,1 olmalıdır.
- Tanklardaki yakıt sıcaklığı çok noktalı ölçülebilmeli (minimum 2 adet sensör ile) ve sistem tanklardaki yakıtın cinsine göre sıcaklık düzeltmesi yapabilmelidir.
- TOS seviye ölçüm çubuklarının çalışma aralığı -20 °C ile +50 °C arasında olmalıdır.
- TOS'inde kullanılan seviye ölçüm çubukları, ilgili tüm kalite ve gerekli güvenlik belgelerine sahip olmalıdır. (ATEX Bölge 0)
- Tank seviye ölçüm çubuklarına giden gerilim Zener diyotlar barındıran bariyer üzerinden geçmelidir.
- Ürün Değişimlerinde farklı şamandıra kullanılmamalıdır. Aynı şamandıralar farklı ürünlerde parametrik olarak değiştirilebilen Off-set ayarı ile kullanılabilir olmalıdır.
- Sıcaklık hassasiyeti ± 0,3 °C olmalıdır.
- Tank Seviye Ölçüm Çubuğu uzunluğu 1.000-3.500 mm aralığında olabilmelidir.

3.2.1 Tank Otomasyon Verilerinin Saklanması ve Kalibrasyon Tablosu

Tank otomasyon uygulaması, akaryakıt tanklarına ait dolum, durum, kayıp/kazanç vb. bilgi kalemlerini dağıtım şirketlerinin belirlediği merkez sunuculardaki uygulamaya göndermelidir. Veri gönderimleri, anlık olarak yapılacaktır. Tank kalibrasyon tablolarının her değişiminden sonra 24 saat içerisinde, otomatik/dinamik kalibrasyon tablolarının ise her değişiminde İKÜ üzerinde bir kopya ve belirlenen merkezi sistem üzerinde bir başka kopya olacak şekilde yedeklenecektir. İstasyon otomasyon uygulamasında tank kalibrasyon verilerine ilişkin bir problemle karşılaşıldığında, ilgili tanka ait kalibrasyon cetveli, alınmış olan en son yedekten dönülecektir.

Otomasyon firması kalibrasyon tipi ayrımı olmaksızın tüm tankların güncel kalibrasyon tablolarını zaman damgası ile damgalayarak P-BYS'nde saklanmalıdır.

3.2.2 TOS Yazılımı Genel Özellikleri

- Kullanılan seviye ölçüm çubukları aracılığı ile istasyonda bulunan akaryakıt tanklarının su ve yakıt seviyelerini mm ve litre cinsinden anlık miktarını ve ◦C cinsinden sıcaklığını verecektir. Bu veriler belirlenen periyodlar ile kayıt altına alınmalı ve P-BYS 'e gönderebilmelidir.
- Tank yüksekliğine göre belirlenen kritik seviye aşıldığında taşma alarmı oluşturabilmelidir..
- Tüm tanklar için dolum esnasında yaşanabilecek yüksek dolum ve taşma miktarları yüzde (%) cinsinden parametrik olarak girebilmelidir..
- Tüm tanklar için anlık ölçülen sıcaklık değeri ◦C cinsinden belirlenen sıcaklık değerini aştığı zaman yüksek sıcaklık alarmı oluşturabilmelidir.
- Tanklardaki yakıt miktarı dağıtım firmasının belirleyeceği seviyeye geldiğinde, düşük ürün alarmı oluşturabilmelidir.
- Tanklardaki çekmez seviyesi 150 mm altında olmayacaktır. TOS yazılımı, tanktaki yakıt seviyesi 150 mm altına indiğinde otomatik olarak İKÜ ile entegre olup ilgili tanktan satış yapılmasını engelleyebilmelidir. Tanktaki yakıt seviyesinin 150 mm'nin altına inme durumu anlık P-BYS 'ye gönderilebilmelidir.
- Tanka bağlı akaryakıt pompası üzerinden satış yapılmadığı zaman aralığında, tanktan minimum 0,382 lt/sa yakıt eksilmesidurumunda otomatik alarm oluşturulacaktır. Bu alarm anlık P-BYS 'ye gönderebilmelidir.
- Tank otomasyon sistemlerinin ürettiği alarmların hata oranı %1'den büyük olmamalıdır.
- TOS tarafından verilen her uyarı günlük olay kayıt tablosuna işlenmelidir. Uygun rapor formatında tüm ikaz ve uyarılar belirlenecek sınıflandırmalar ile geriye dönük olarak 1 (bir) yıl raporlanabilir durumda olmalıdır.
- Tank kontrol ünitesi otomatik dolum algılayabilmelidir. Dolum bilgileri otomatik olarak TOS yazılımının dolum kayıtlarına ve olay kayıt tablosuna işlenmelidir. Otomatik dolum esnasında pompalardan yapılan satış miktarı, TOS yazılımı tarafından hesaplanarak TOS dolum verisine eklenmelidir.
- Manuel veya otomatik dolumların tamamının dâhil edileceği tank dolum raporu olmalıdır. İlgili rapor dolum başlangıç ve bitiş tarih ve zamanını, dolumun başladığı ve tamamlandığı andaki ürün miktarlarını ve sıcaklık değerleri ile dolum yapılan miktarı belirtmelidir. Ayrıca söz konusu raporda net ve brüt dolum miktarı ve kesafet miktarı gibi değerlere ulaşılabilmelidir.
- Üretilen tüm alarmlar kayıt ve takip altına alınacaktır. Sistem, tüm alarmların ışıklı veya sesli ikaz yöntemlerini kullanarak görsel/işitsel olarak duyurulması için gerekli altyapıya sahip olacaktır. Opsiyonel olacak bu ekipmanlar talep edilmesi durumunda sistem üzerinde bir revizyona gerek kalmadan montaj ve devreye alma işlemleri yapılabilir olmalıdır.

- Otomatik kalibrasyon yapabilmelidir. Tüm kalibrasyon bilgileri sistemde kayıtlı olarak yedeklenebilmeli ve gerektiği durumda kalibrasyon tipi ve tablonun yüklenme tarihi bilgilerini içerecek şekilde raporlaması yapılabilmelidir. İlgili raporun çıktısı alınabilmelidir.
- Sistem istasyonlarda bulunan her tanka ait LT/mm kalibrasyon tablosunu içinde barındıracak, gerekmesi halinde kalibrasyon tabloları ayrı ayrı yazıcı çıktısı vererek manuel olarak tanklardaki seviyelerin ölçümüne olanak tanıyacaktır.
- TOS, lazer ya da benzeri bir teknoloji ile yapılmış kalibrasyon tablolarını kullanabilir özellikte olmalıdır.
- İstasyondaki sistem içinde toplanan her türlü kayıda ilişkin rapor çıktısı alınabilecektir.
- İstasyon akaryakıt depolama tanklarında yapılan dolumları otomatik dolum algılayabilmeli ve dolum bilgileri otomatik olarak dolum kayıtlarına ve olay kayıt dosyasına işlenebilmelidir.
- Anlık ve tarih / saatler arasında tank bazlı envanter ve dolum raporları alınabilmelidir.
- Tank otomasyon sistemi her vardiya sonrasında, günlük veya belirlenecek ilave bir zaman periyodunda periyodik veya manuel olarak çalıştırılabilecek mutabakat raporu olmalıdır. Söz konusu raporda tanktan eksilen ile pompadan çıkan karşılaştırılmalıdır.
- Sistem her ürün için ortalama günlük satış miktarını takip edebilmeli ve haftanın her günü için satış miktarını hesaplayabilmeli ve ilgili raporu üretebilmelidir. Ayrıca istasyondaki her ürün için hesapladığı günlük ortalama satış miktarı üzerinden istasyonun tankında kaç günlük yakıt kaldığına dair tahmini hesaplamayı yapabilmeli ve ilgili raporu üretebilmelidir.
- TOS yazılımı kullanıcılara yetki seviyesine göre erişim yetkisi sağlayacak bir altyapıya sahip olmalıdır. Sistem parametrelerine yetkisiz kullanıcıların erişimi ve değişiklik yapması engellenmelidir.
- TOS belirlenen periyotlarda tank verilerini İKÜ'ne göndermelidir.

4 KATMA DEĞERLİ HİZMETLER

4.1 Müşteri Tanıma Sistemi Okuyucusu (MTSO)

İstasyonundan hizmet alacak olan müşterilerin ödeme ve sadakat uygulamaları için tanınması ve pompacıların vardiya işlemleri için tanınmasını sağlayan ve bir RFID kartın okutulması ile çalışan bir cihazdır. Müşteri ve Pompacı tanıma cihazları, yaygın olarak pompa üzerine monte edilen bir kart okuyucu ile sağlanmaktadır. MTSO'lar İKÜ tarafından yönetilmektedir. Cihazlar IKÜ'ye TCP/IP, Kablosuz veya RS485 ile bağlanabilir.

4.2 Taşıt Tanıma Sistemi Okuyucusu (TTSO)

TTS, istasyonlardan hizmet alacak olan şirket veya bireylere ait araçlarının otomatik olarak tanınması sağlayan bir sistemdir.

Bu sistem 3 bileşenden oluşmaktadır.

Taşıt Tanıma Sistem Okuyucu (TTSO): İKÜ'ye TCP/IP veya RS485 ile bağlanabilir. TTSO kablosuz ise dışarıdan dinlemeye açık olacağı için haberleşme verilerinin şifrelenmiş olması gerekmektedir. TTSO kablosuz ise dinleme ve tekrarlama yöntemiyle RFID kimliği okunmuş gibi sisteme gönderilebilir. Bu yüzden haberleşme paketi içerisindeki veriler el sıkışma yöntemi ile doğrulanmalıdır.

Taşıt Kimlik Ünitesi (TKÜ): Taşıtın deposuna takılmış ve içinde taşıt kimlik bilgilerini şifreli olarak barındıran ünitedir. Söküldüğünde pasif duruma geçmelidir.

RFID Tabanca Okuyucusu: Pompa tabancasına takılmış, ATEX Bölge 0 onaylı, bilgileri güvenli bir şekilde TKÜ'den okuyup TTSO'ya ileten ünitedir. RFID Tabanca Okuyucusu kablosuz olup, söküldüğünde pasif duruma geçmelidir.

4.3 EFT/POS

İstasyonlardan hizmet veya ürün alan müşterilerden ödeme alınmasını, sadakat kart müşterilerin tanınmasını, ön ödemeli kartlar ile ödeme yapılmasını sağlayan ödeme cihazlarıdır. Cihazlar İKÜ'ye TCP/IP veya RS485 protokolü üzerinden bağlanacaktır.

4.4 Plaka Tanıma Sistemi (PTS)

İstasyona giriş / çıkış yapan taşıt plakalarının tespit edilmesini sağlayan otomatik tanıma sistemidir. ÖKC üzerinden giriş yapılan plaka ile PTS üzerinden otomatik olarak algılanan plaka bilgisi doğrulanır. Doğrulanmaması durumunda istasyon pompa satış görevlisine MTSO ekranı aracılığı görsel ve işitsel uyarı verilir.

4.5 Taşıt Yıkama Sistemi (TYS)

İKÜ, istasyonlardaki otomatik araç yıkama sistemleri ile entegre olabilir. Cihazlar İKÜ'ye TCP/IP, kablosuz veya RS485 ile bağlanabilir.

4.6 Mobil Ödeme Sistemi (MÖS)

Müşterilerin istasyondan aldıkları yakıtın karşılığını mobil uygulamaya ve plaka ile ilişkilendirilmiş kredi kartı ile ödeyebildikleri sistemdir. Yakıt alımı öncesinde veya sonrasında sanal pos ile kredi kartından ön ödeme alınması suretiyle süreç yakıt satış gerçekleştirilebilmelidir. Süreç ÖKC'den plaka girilerek veya mobil uygulama üzerinden istasyonun ilgili pompasına P-BİM üzerinden istek gönderilerek başlatılabilmelidir.

4.7 Ön Ödemeli Kart Sistemi (ÖÖKS)

İçine yakıt alabilecek bakiye yüklenen kartların istasyonlardan yakıt almasını sağlayan sistemdir. Kart, MTSO veya EFT POS ile okunur, alınacak tutar girilir, P-BİM aracılığı ile ÖÖKS den alınan onaya istinaden yakıt verilmelidir. İkmal tamamlandıktan sonra kartın tipine göre TTS veya mali değeri olan ÖKC fişi basılır. Gerçekleşen ikmale ait tutar, kart numarası, litre, birim fiyat ÖÖKS ye P-BİM üzerinden iletilir. Karta tanımlanan taşıt plakası ile ÖKC de girilen taşıt plakası eşleşmelidir.

4.8 Grup Kampanya, Kupon, Promosyon vb. Uygulamalar

İKÜ, Müşteri sadakatini arttırma amacı ile müşteriye verilen kart ile veya plaka numarası üzerinden sadakat sistemi entegrasyonlu yakıt ikmali gerçekleştirebilir. Bu ikmal gerçekleştirilirken müşteriye indirim, puan kazandırılabilmeli ve puan harcatabilmelidir.

Kart, müşteri, plaka, ürün ve istasyon bazında kampanyalar sadakat sisteminde tanımlanabilir ve bu tanımlara göre de istasyonlarda sadakat sistemi entegrasyonlu yakıt ikmali İKÜ tarafından gerçekleştirilebilir.

4.9 Fiyat Panosu

İKÜ, dijital fiyat panosu ile entegre olabilmeli ve fiyat güncellemesi İKÜ üzerinden yapılabilmelidir. Dağıtım şirketinin yayınladığı ilçe bazlı akaryakıt birim fiyatları ile İKÜ entegre çalışabilmelidir.

4.10 Otomasyon Mobil Yönetim Uygulaması (O-MYU)

İOS'un uzaktan yönetimini sağlayan mobil uygulamadır. İOS uygulaması verileri P-BİM'e göndermelidir. IOS & Android olmak üzere iki farklı platformda çalışabilmelidir.

4.11 Taşıt Yakıt Tipi Doğrulama Sistemi (YDO)

Petrol şirketi bazında istasyonlarda araçların plaka bazında yakıt alımlarına veya müşterinin beyanına göre belirlenen ürün grubu dışında ürün almalarını engelleyen sistemdir. YDO merkez sunucuları ile İOS arasındaki iletişim P-BİM üzerinden sağlanmalıdır.

4.12 İOS Haberleşme Protokolleri

İKÜ'ye bağlı pompa üzerindeki MTSO ve TOS kontrol cihazının İKÜ ile haberleşmesini sağlayan haberleşme protokolleri herkese açık şekilde olmalıdır.

5. MERKEZ YÖNETİM YAZILIMLARI

5.1 Otomasyon Şirketi Bilgi İşlem Merkezi (O-BİM)

O-BİM, Otomasyon şirketinin sunucu parkında konumlandırılır.

O-BİM'in temel görevleri aşağıda sıralanmıştır;

- İKÜ yazılımı sürüm kontrolleri,
- İKÜ yazılımı kurulum ayarları,
- İOS alarmlarının yönetilmesi,
- Tank kalibrasyon işlemlerinin yönetilebilmesi,
- İOS donanım seri numara takibi,
- O-MYU kullanıcı tanımlama ve yetkilendirme

Otomasyon şirketi çalışanlarının O-BİM'e erişmeden önce elektronik onay sürecinden geçmesi zorunludur.

VPN üzerinden giriş yapılmak istendiğinde;

- Otomasyon şirketi yetkilisi onay verdikten sonra bağlantı sağlanacaktır.
- Kullanıcıya özel tek seferlik şifre SMS olarak gönderilir, kullanıcı kendisine gönderilen şifreyi petrol şirketinin sistemine girerek ağ bağlantısı sağlanacaktır.

Ayrıca O-BİM'in olası mücbir sebeplerden etkilenmemesi için Felaket Kurtarma Çözümü oluşturulması gereklidir.

5.2 Petrol Şirketi Bilgi İşleme Merkezi (P-BİM)

P-BİM, İOS ile merkezdeki sunucular arasındaki iletişimi yönetir ve Petrol Şirketinin güvenli sunucu parkında konumlandırılır. Sadakat, mobil ödeme, taşıt-yakıt tipi doğrulama, ön ödemeli kart sistemi gibi tüm süreçler bu birim üzerinden ilerlemelidir.

P-BİM ve O-BİM'ye bağlanacak çevre birimleri temel teknik özellikler tablosu (X=Zorunlu; İ=İhtiyari; 0 =Yok)

Temel Teknik Özellikler	OMS
1. Veri tabanı	İ
2. Olay Kayıt Özelliği	X
3. Güvenli Veri İletimi	X
4. Kimlik Doğrulama	X
5. Yazılım Güvenliği	X
6. Sunucu	X
7. GİB BS ile Haberleşme	X
8. Acil Durum	X

P-BİM üzerinde oluşan güvenlik olayları ajanlı ya da ajansız olarak toplanabilmeli ve Bilgi Güvenliği Operasyon Merkezine (BGOM) göndermelidir.

5.2.1 Veri Tabanı

P-BİM üzerinde herhangi bir veri işleme ve saklama işlemi yapılmayacağı için veri tabanı barındırılması veya erişimi zorunlu değildir.

5.2.2 Olay Kayıt Özelliği

P-BİM üzerinde yapılan her türlü işlem (dışarıdan gelen istekler ve bunlara verilen cevaplar, uygulama içerisinde gerçekleştirilen işlem ve fonksiyon detayları ve sonuçları, karşılaşılan sorunların ve hataların detayları vs.) esnasındaki olaylar ayrı ayrı ve detaylı ve en az 5 yıl süreyle silinemeyecek bir şekilde saklanmalıdır. İhtiyaç duyulması halinde bu olay kayıtları incelenebilmeli ve otomasyon sistemi içerisindeki akışlar takip edilebilmelidir.

5.2.3 Güvenli Veri İletimi

P-BİM'ne birçok noktadan erişim sağlanabileceği için veri transferinin üst seviyede güvenli olması gerekmektedir. Bu veriler SSL (Secure Sockets Layer, Güvenli Giriş Katmanı) sertifikası ile şifrelenerek güvenlik altına alınmalıdır.

5.2.4 Kimlik Doğrulama

P-BİM ve O-BİM sistemine birçok farklı noktadan erişim sağlanabileceği için burada çalışan uygulama veya servislerin kullanımının kimlik doğrulama yöntemi ile güvenlik altına alınması gerekmektedir. Bu kapsamda; ilgili sisteme ve çalıştığı sunucuya erişim sağlayacak her uygulama için güvenlik politikalarının tanımlanması ve uygulanması gereklidir. Her erişimde kimlik doğrulaması yapılmalı. Belirlenen süreler içerisinde hiçbir işlem yapmamış olan kullanıcıların bağlantıları sonlandırılarak tekrar doğrulama yapmaları istenilmelidir.

5.2.5 Yazılım Güvenliği

P-BİM içerisinde çalışacak yazılımlar, kullanım amacına ve alanına göre tasarlanmalıdır. İşletim sistemi düzeyindeki dizin ve dosya yetkilendirmelerinin, veri tabanı kullanıcı tanımlamaları ve yetkilendirmelerinin, uygulamayı kullanırken kimlik denetiminin doğru yapılması, işletim sistemi komut sızıntılarına, veri tabanı sızıntılarına ve hizmet dışı bırakma saldırılarına karşı önlemler içermelidir. Uygulamalar en üst yetkili veri tabanı kullanıcısı ile çalıştırılmamalıdır.

5.2.6 Sunucu

P-BİM bünyesinde hizmet veren ve otomasyon ile ilgili bütün merkezi uygulama veya servislerin koştuğu ana bilgisayarlardır. Bu sunucular, üst seviye güvenlik katmanına sahip olmalıdır. Ayrıca, P-BİM sunucusu ek güvenlik cihazları ve yazılımları ile de korunmalıdır. Sunucular için aşağıdaki koruma sistemleri kullanılabilir:

- Güvenlik duvarı
- Anti virüs yazılımları
- İzleme ve uyarı sistemleri
- P-BİM Sunucusu üzerindeki tüm olay günlükleri ajanlı ya da ajansız olarak BGOM sisteminde toplanmalıdır.
- P-BIM Sunucusunda kayıt defteri hareketleri anlık olarak BGOM sistemine aktarılmalıdır.
- P-BIM Sunucusunda yetkisiz erişim kontrolleri BGOM üzerinde oluşturulan korelasyonlar ile desteklenmeli ve gerekli durumlarda erişimlerin engellenmesi sağlanmalıdır.
- P-BIM Sunucusu üzerindeki uygulamaların SHA-256 Hash değerleri çıkartılmalı ve BGOM sisteminden otomatik olarak SHA-256 Hash sorgusu 3. Parti uygulamalara yapılabilmelidir.
- P-BIM Sunucusu üzerindeki uygulama işlemleri gerçekleştirirken bir bozulmaya uğraması durumunda Hash değeri değişeceği için dosyanın bozulmaya uğradığını tespit edip dosyanın BGOM sistemi ile silinebilmesi sağlanmalıdır.
- P-BIM Sunucusunda solucan, Truva atı, casus yazılım, reklam yazılımı, fidye yazılımı, illegal botlar, parazit kripto madenciliği yazılımı veya dolandırıcı yazılımı görülmesi halinde BGOM sistemi ile zararlı yazılım barındıran sistemin ağdan izole edilmesi sağlanmalıdır. Sistemde zararlı yazılım temizlendikten sonra sistemi ağa tekrar dahil edilebilmelidir.
- P-BIM sunucusunda dosya bütünlüğü kontrolü yapılabilmelidir. Dosya bütünlüğü ile ilgili tüm veriler BGOM sistemi üzerinde toplanmalıdır.
- BGOM sistemi P-BIM sunucusu üzerinde aktif olarak çalışan güvenlik duvarında kural değişikliklerini takip edebilmeli ve gerekli durumlarda kuralları güncelleyebilmelidir.

5.2.7 GİB Bilgi Sistemleri ile Haberleşme

Akaryakıt istasyonlarından yapılan satış bilgileri, P-BYS ’ne anlık olarak iletilmelidir.

Bu bilgiler, GİB tarafından belirlenen format ve içeriğe uygun olarak GİB tarafından belirlenen zaman periyodları da dikkate alınarak GİB sunucularına elektronik ortamda iletilebilmelidir.

Mali ÖKC fişi üzerinde olan bilgiler;

- İstasyon Ünvanı
- Tarih-Saat
- Fiş No
- Plaka
- Birim Fiyat
- Litre
- Tutar
- Ürün Adı
- KDV

- Toplam Tutar
- Ödeme Tipi
- Pompa No

5.2.8 Acil Durum

Sunucularda oluşabilecek her türlü felaket senaryosuna karşın acil durum eylem planlarının hazır olması gerekmektedir. Bu kapsamda aşağıdaki özelliklerin barındırılması gerekmektedir:

- Yedek sunucunun hazır bulundurulması
- Sunucuların önünde Load Balancer (Yük Dengeleyici) sisteminin hazırlanması
- İzleme ve uyarı sistemleri

5.3 Petrol Şirketi Bilgi Yönetim Sistemi (P-BYS)

P-BYS ile çalışacak sistemlerin temel teknik özellikler tablosu (X=Zorunlu; İ=İhtiyari; 0 =Yok)

Temel Teknik Özellikler	**P-BYS**
1. İşletim Sistemi	X
2. Veri tabanı	X
3. Olay Kayıt Özelliği	X
4. Güvenli Veri İletimi	X
5. Kimlik Doğrulama	X
6. Yazılım Güvenliği	X
7. Sunucu	X
8. Merkezi Kaynak Planlama Uygulamaları (ERP)	İ
9. EPDK 1240 Sayılı Kurul Kararı Uygunluğu	X
10. Özel Sanal Ağ (VPN)	X
11. Yönelndirici (Router)	X
12. Taşıt Yakıt Tipi Doğrulama Sistemi (YDO)	İ
13. Mobil Ödeme Sistemi (MÖS)	İ
14. Ön Ödemeli Kart Sistemi (ÖÖKS)	İ

5.3.1 İşletim Sistemi

Petrol şirketi merkezinde hizmet verecek olan sunucular üzerinde çalışacak işletim sistemi aşağıdaki özelliklere sahip olmalıdır:

- En az 32 bit veya daha yüksek veri işleme kapasitesine sahip işlemci üzerinde çalışabilmelidir.
- IPv4 ve IPv6 protokollerini desteklemelidir.
- Aynı anda çoklu işlem özelliğine sahip olmalıdır.
- Ayrı kullanıcı grupları için ayrı yetkiler tanımlanabilmesi özelliğine sahip olmalıdır.
- Sistem üzerinde üreyen güvenlik olayları ajanlı ya da ajansız olarak toplanabilmeli ve Bilgi Güvenliği Operasyon Merkezine (BGOM) gönderilmelidir.

5.3.2 Veri Tabanı

Petrol şirketi merkez sunucularında barındırılacak Veri tabanı, akaryakıt istasyonlarından, merkez uygulamalardan veya petrol şirketinin diğer otomasyon sistemlerinden gelen verilerin saklandığı ve

işlendiği, erişim imkânı olan, yönetilebilen, güncellenebilen ve başka bir noktaya taşıma imkânı olan güvenli veri depolama dosyalarıdır. Bu dosyalar içerisinde saklanacak olan bilgiler ayrı ama birbirleri ile ilişkili bilgi kümeleri halinde saklanmaktadır. Veri tabanı aşağıdaki özelliklere sahip olmalıdır :

- Veri tabanına erişim parola ile korunabilmelidir.
- Çoklu işlemlere aynı anda cevap verebilmeli ve işlem yapabilmelidir.
- Veri kaydetme, düzenleme, sorgulama ve raporlama özelliğine sahip olmalıdır.
- Veri tabanına sadece yetkili uygulamalar üzerinden erişilmelidir.
- Saklanan verilere hızlı erişim için gerekli indeks tanımlarına sahip olmalıdır.
- Veri kaybını önlemek için; veri tabanı yedekleme sistemine ve acil durum kurtarma senaryoları ve altyapısına sahip olmalıdır.
- Veri tabanında kayıtlı bulunan bilgiler silinmeye karşı korumalı olmalıdır.
- Veri tabanına yapılan erişimler BGOM sisteminde toplanmalıdır.
- Veri tabanında yapılan Listeleme, Güncelleme, Silme, Ekleme vb. işlemlerin tamamı BGOM sistemine bildirilmelidir.
- Veri tabanında yapılan sorgular detaylı olarak veritabanı denetim günlüğünde saklanmalıdır.

Veritabanı denetim günlüğünde aşağıdaki bilgiler olmalıdır;

  - Kullanıcı
  - Bağlantı Kuran Adres (IP)
  - Veri tabanı adı
  - Tablo adı
  - Kayıt ID
  - İşlem (Listeleme, Güncelleme, Silme, Ekleme)

Veri tabanı sistemindeki güvenlik olay günlükleri BGOM Sisteminde kayıt altına alınmalı ve saklanmalıdır.

5.3.3 Olay Kayıt Özelliği

P-BYS , petrol şirketi bünyesindeki bütün İOS' lerinden gelen verilerin saklanacağı ve yönetileceği ana sunucu olduğu için burada çalışacak bütün merkezi uygulamaların olay kayıtlarının anlık ve detaylı olarak silinemeyecek şekilde saklanması zorunludur. Karşılaşılan sorunların ve hataların detayları bu modül ile kayıt altına alınarak izlenebilmelidir.

5.3.4 Güvenli Veri İletimi

Petrol şirketi merkezi sisteminde farklı veri iletim yöntemleri kullanılabilir. Başlıca veri iletim yöntemleri aşağıdaki gibi olmaktadır.

- İOS ve P-BYS arasındaki veri iletimi: İOS'lerinde üretilen verilerin merkez sistemine aktarılmasıdır. Veri aktarımında kullanılan paketler şifrelenerek transfer edilmelidir.
- P-BYS içerisindeki alt modüller ve uygulamalar arasındaki veri iletimi: P-BYS birden fazla alt modül, uygulama veya servisten oluşabilir. Bütün bu alt bileşenler arasındaki veri iletimi belirlenen protokoller çerçevesinde yapılmalı ve protokole uygun olmayan veri paketleri dikkate alınmamalıdır.
- P-BYS ile olan diğer sistemler arasındaki veri iletişimi: P-BYS ile petrol şirketi merkezindeki diğer otomasyon sistemleri (muhasebe, müşteri yönetim sistemi vs.) arasında veri transferi yapılabilir. Bu durumda kullanılacak olan veri iletim paketlerinin gizlenmesi ve yetkisiz dış erişimlere kapalı olması gereklidir.

5.3.5 Kimlik Doğrulama

P-BYS sistemi içerisindeki dış dünyaya açık olan her bir sistem, uygulama veya servis (bilgisayar, veri tabanı vs.) kullanımının kimlik doğrulama yöntemi ile güvenlik altına alınması gerekmektedir.

Bu kapsamda; ilgili sisteme ve çalıştığı sunucuya erişim sağlayacak her kullanıcı ve uygulama için güvenlik politikalarının tanımlanması ve uygulanması gereklidir.

Her erişimde kimlik doğrulaması yapılmalıdır.

Belirlenen süreler içerisinde hiçbir işlem yapmamış olan kullanıcıların bağlantıları sonlandırılarak tekrar doğrulama yapmaları istenmelidir.

5.3.6 Yazılım Güvenliği

P-BYS, işletim sistemi düzeyindeki dizin ve dosya yetkilendirmelerinin, veri tabanı kullanıcı tanımlamaları ve yetkilendirmelerinin, uygulamayı kullanırken kimlik denetiminin doğru yapılması, işletim sistemi komut sızıntılarına, veri tabanı sızıntılarına ve hizmet dışı bırakma saldırılarına karşı önlemler içermelidir. Uygulamalar en üst yetkili veri tabanı kullanıcısı ile çalıştırılmamalıdır.

5.3.7 Sunucu

P-BYS bünyesinde hizmet veren ve otomasyon ile ilgili bütün merkezi uygulama veya servislerin koştuğu ana bilgisayarlardır. Bu ana sunucular, kullanım alanına ve tercihe göre farklı özelliklere ve güvenlik katmanlarına sahip olabilirler. Başlıca kullanılan sunucu katmanları:

- **Uygulama Sunucusu:** P-BYS bünyesinde çalışan İOS'a bağlı uygulama ve servislerin koşturulduğu ana sunucudur. İOS, petrol şirketi bünyesindeki diğer alt otomasyon yazılımları (muhasebe, müşteri yönetim sistemi vs.) sadece bu sunucuya ve burada çalışan ilgili servislere erişebilir.
- **Veri Tabanı Sunucusu:** P-BYS bünyesindeki bütün veri tabanı sistemlerinin çalıştığı ve veri tabanı dosyalarının saklandığı sunucudur. Uygulama Sunucusu maddesinde bahsi geçen hiçbir kullanıcı, servis veya uygulama direkt olarak veri tabanı sunucusuna bağlanamaz. Sadece, uygulama sunucusunda çalışan uygulamalar belirlenmiş bağlantı tanımları ve yetkiler ile veri tabanı sunucuna erişebilir ve işlem yapabilirler.
- **İnternet Uygulama Sunucusu:** P-BYS bünyesinde hizmet veren internet uygulamalarının (web uygulaması) ve web servislerinin çalıştığı sunucudur. Bu sunucu dış dünya açık olduğu için güvenlik seviyesinin en üst düzeyde olması gereklidir.

Her sunucu bulunduğu katmana göre aşağıdaki güvenlik cihazları ve yazılımları ile korunmalıdır.

    - Güvenlik duvarı
    - Anti virüs yazılımları
    - İzleme ve uyarı sistemleri
- Internet Uygulama sunucusu üzerindeki tüm aktivitelerin olay günlükleri BGOM Sisteminde kayıt altına alınmalı ve saklanmalıdır.
- Internet Uygulama Sunucusunda kayıt defteri hareketleri anlık olarak BGOM sistemine aktarılmalıdır.
- Internet Uygulama Sunucusunda yetkisiz erişim kontrolleri BGOM üzerinde oluşturulan korelasyonlar ile desteklenmeli ve gerekli durumlarda erişimlerin engellenmesi sağlanmalıdır.
- Internet Uygulama Sunucusu üzerindeki uygulamaların SHA-256 Hash değerleri çıkartılmalı ve BGOM sisteminden otomatik olarak SHA-256 Hash sorgusu 3. Parti uygulamalara yapılabilmelidir.
- Internet Uygulama Sunucusu üzerindeki uygulama işlemleri gerçekleştirirken bir bozulmaya uğraması durumunda Hash değeri değişeceği için dosyanın bozulmaya uğradığını tespit edip dosyanın BGOM sistemi ile silinebilmesi sağlanmalıdır.

- Internet Uygulama Sunucusunda solucan, Truva atı, casus yazılım, reklam yazılımı, fidye yazılımı, illegal botlar, parazit kripto madenciliği yazılımı veya dolandırıcı yazılımı görülmesi halinde BGOM sistemi ile zararlı yazılım barındıran sistemin ağdan izole edilmesi sağlanmalıdır. Sistemde zararlı yazılım temizlendikten sonra sistemi ağa tekrar dahil edilebilmelidir.
- Internet Uygulama sunucusunda dosya bütünlüğü kontrolü yapılabilmelidir. Dosya bütünlüğü ile ilgili tüm veriler BGOM sistemi üzerinde toplanmalıdır.
- BGOM sistemi Internet Uygulama sunucusu üzerinde aktif olarak çalışan güvenlik duvarında kural değişikliklerini takip edebilmeli ve gerekli durumlarda kuralları güncelleyebilmelidir.
- Internet Uygulama sunucusuna yapılan istekler BGOM sisteminde kayıt altına alınabilmelidir.
- Internet Uygulama sunucusuna yapılan isteklerde SQL Injection, XSS , CSRF vb. duruma rastlanması durumunda istek yapan Host ya da IP adresi Firewall üzerinden engellenebilmelidir.

5.3.8 ERP

P-BYS, farklı Merkezi Kaynak Planlama Uygulamaları sistemlerine (muhasebe, müşteri yönetim sistemi vs.) sahip olabilmektedir. Bunların bütününe genel anlamda ERP sistemi denilmektedir.

Petrol şirketleri kendi iç süreçlerini bu ERP sistemleri üzerinden yönetmektedir.

ERP ile P-BYS arasında bir entegrasyon kurulması gerektiği durumlarda; P-BYS, aşağıdaki yöntemlerden birini kullanmaldır :

- Web Servis
- Paylaşımlı Veri tabanı

5.3.9 EPDK 1240 Sayılı Kurul Kararı Uygunluğu

EPDK 1240 Sayılı Kurul Kararı gereği; her dağıtım şirketi kendi bünyesindeki her türlü akaryakıt satış, dolum, istasyon akaryakıt envanteri, istasyon durumları gibi akaryakıt hareketlerini belirlenen süreler içerisinde EPDK sistemine iletmekle mükelleftir.

P-BYS içerisinde yer alan EPDK modülü, EPDK'nın belirlediği kurallar çerçevesinde belirlenen verileri oluşturarak otomatik olarak EPDK' ya iletmelidir.

Hazırlanan ve iletilen verilerin durumu ve geçmişi anlık olarak izlenebilmeli ve gerekli durumlarda gerekli birimlere alarm göndererek bilgilendirme yapabilmelidir.

5.3.10 Özel Sanal Ağ - Virtual Private Network (VPN)

P-BYS , dış dünyaya kapalı ve güvenli bir ağ içerisinde çalışmalıdır.

Petrol şirketi ağı dışındaki hiçbir ortamdan bu sisteme direkt erişim sağlanamaması gerekmektedir. Ancak, gerekli durumlarda P-BYS 'ne dış ortamdan erişim sağlanması ihtiyacı olduğunda petrol şirketinin tanımlamış olduğu VPN sistemleri kullanılarak petrol şirketi kapalı ağ ortamına dahil olunabilir.

Belirlenen kurallar ve yetkiler çerçevesinde P-BYS 'ne dahil olunarak çalışma yapılabilir ve hizmet verilebilir. VPN bağlantı özelliği genel olarak; petrol şirketi personelinin veya otomasyon hizmeti veren firmanın dışarıdan erişim sağlaması için kullanılmaktadır.

- P-BYS sistemindeki tüm VPN hareketlerin logları BGOM sisteminde tutulmalıdır.
- VPN yapan kullanıcı ve IP bilgisi eşleştirilmeli ve eşleşme dışında bir erişim isteği söz konusu olursa BGOM sistemi VPN kullanıcısının hesabını pasif edebilmelidir.

- VPN yapan kullanıcı ve IP bilgisi eşleştirilmeli ve eşleşme dışında bir erişim isteği söz konusu olursa BGOM sistemi VPN kullanıcısının şifresini resetleyebilmeli ve oturumu sonlandırabilme özelliği olmalıdır.
- Farklı bir IP'den VPN erişimi söz konusu olursa ilgili IP P-BYS de bulunan Güvenlik Duvarı üzerinden engellenebilmelidir.
- Güvenlik Duvarı üzerinden engelleme senaryosu görsel editörler ile bir iş akışına bağlanabilmeli ve otomasyon sayesinde engelleme yapılabilmelidir.
- VPN yapan kullanıcısı erişim yetkisi olmayan bir sisteme bağlantı isteği yapması durumunda BGOM sistemi otomatik olarak kullanıcının oturumunu sonlandırabilmelidir.
- VPN kullanıcısı IOS çevre birimlerinden herhangi birinde uygulama kurması durumunda BGOM sistemi uygulamayı tespit edebilecek ve silebilecektir.
- VPN kullanıcısı IOS çevre birimlerinden herhangi birine uygulama kopyalaması durumunda BGOM sistemi kopyalanan uygulamayı tespit edebilecek ve silebilecektir.

5.3.11 Yönlendici (Router)

Temel anlamda router; iki farklı ağ üzerinde çalışmakta olan bilgisayarların birbirlerine güvenli bir şekilde erişebilmelerini sağlayan bir yönlendiricidir. P-BYS dışındaki bir ağın P-BYS 'ne dahil olması gibi bir gereklilik halinde kullanılabilmektedir. Bu sayede sadece tanımlanan bilgisayarlar router'a bağlanabilir ve petrol şirketi ağına erişebilir.

- Router cihazında trafik bilgisinin izlenmesi için Flow (NetFlow, sFlow, jFlow) desteği olmalıdır.
- Trafik bilgisi BGOM sistemine kayıt edilmeli ve anlık olarak izlenmelidir.
- BGOM sistemi P-BYS de bulunan Router'a API veya SSH ile erişim sağlayabilmelidir.
- BGOM sistemi P-BIM yönüne doğru oluşan trafikte normalin dışında (anomali) bir durum tespit ederse kaynaktan gelen trafiği engelleme yeteneğine sahip olmalıdır.
- BGOM sistemi P-BIM tarafından oluşan trafikte normalin dışında (anomali) bir durum tespit ederse kaynağa giden trafiği engelleme yeteneğine sahip olmalıdır.
- BGOM sistemi Router üzerinde kullanılmayan portları tespit edebilmeli ve Administrative Down edebilmelidir.
- BGOM sistemi Router a bağlı cihazlara ilişkin MAC tablosunu kontrol edebilmeli ve Host-MAC eşleşmesi olmayan durumlar için portu pasif (disable) edebilme yeteneğine sahip olmalıdır.

5.4 P-BYS Haberleşmesi

İstasyonlarda çalışan İKÜ'nün bünyesinde bulunduğu ana petrol şirketinin merkez sistemine güvenli çevrimiçi bağlı olması gerekmektedir.

Bu bağlantı ile karşılıklı olarak ve çevrimiçi veri transferi yapılmaktadır.

5.4.1 Kapalı Bilgisayar Ağı

İnternete bağlı olan petrol şirketi merkez ağı ile istasyon ağının güvenli bir tünel(VPN) ile birbirine bağlanmalı ve istasyon ağından internete direkt çıkış engellenmelidir.

İstasyon ağına sadece İKÜ'ye entegre olan bileşenler dâhil edilmelidir.

5.4.2 Router

İstasyon güvenli ağını yöneten cihazdır.

Router istasyon güvenli ağını petrol şirketi merkezine VPN tüneli ile bağlayabilmeli, istasyondaki cihazların erişimlerini IP, PORT ve MAC adresleri ile filtreleyebilmeli ve yönetebilmelidir.

- Router cihazında trafik bilgisinin izlenmesi için Flow (NetFlow, sFlow, jFlow) desteği olmalıdır.
- Trafik bilgisi BGOM sistemine kayıt edilmeli ve anlık olarak izlenmelidir.

- BGOM sistemi O-BİM'de bulunan Router'a API veya SSH ile erişim sağlayabilmelidir.
- BGOM sistemi O-BİM yönüne doğru oluşan trafikte normalin dışında (anomali) bir durum tespit ederse kaynaktan gelen trafiği engelleme yeteneğine sahip olmalıdır.
- BGOM sistemi Router üzerinde kullanılmayan portları 1 ay süre içerisinde tespit edebilmeli ve Administrative Down edebilmelidir.
- BGOM sistemi Router'a bağlı cihazlara ilişkin MAC tablosunu kontrol edip, Host - MAC eşleşmesi olmayan durumlar için cihaz trafiğini engelleme özelliğine sahip olmalıdır.

5.4.3 Kullanıcı Yetkilendirilmesi

Kullanıcı, rol ve modül bazında yetkilendirme yapılabilmelidir.

6. SERVİS ORGANİZASYONU

Otomasyon Şirketi, 7/24 hizmet verebilen çağrı merkezine sahip olmalıdır.

Otomasyon şirketi, 81 ilde yerinde servis verebilecek şekilde en az 30 noktada yetkili servis ağına sahip olmalıdır.

Otomasyon şirketi tarafından yetkili servislere verilen yetki belgesi azami 2 yıl süreli ve GİB tarafından onaylı olmalıdır.

6.1 Olağanüstü Durum Merkezi

Otomasyon şirketi deprem, yangın, terör, afet, sel gibi acil durumlarda çağrı merkezi hizmetini devam ettirebilmek amacıyla Olağanüstü Durum Merkezine (ODM) sahip olmalıdır. Otomasyon şirketi, 22301:2012 iş sürekliliği standardı kapsamında müşterilerine bu hizmeti verebilecek durumda olmalıdır.

7. MÜHÜRLEME

İOS sisteminde kritik verilerin oluşmasında ve saklanmasında kullanılan donanımlar, otomasyon şirketi tarafından mühür altına alınmalıdır.

7.1 İKÜ Mühürlemesi

İOS'ta bulunan tüm verilerin saklandığı İKÜ, kablo bağlantılarına ve elektronik kart kısımlarına erişimin engelleneceği şekilde mühürlenmelidir.

7.2 Tank Kontrol Ünitesi Mühürlemesi

Tank kontrol üniteleri cihazların kart kısmına erişilemeyecek şekilde mühürlenmelidir. Bu mühür kırılmadan tank kontrol ünitesi kablo bağlantılarına müdahale sağlanamamalıdır.

7.3 Tank Seviye Ölçüm Çubukları Mühürlemesi

Tank seviye ölçüm çubuklarının üzerine koruma amaçlı takılan metal kılıfa ait kapaklar, açılması durumunda kırılacak şekilde mühürlenmelidir. Bu mühür kırılmadan seviye ölçüm çubuklarının kablo bağlantılarına erişim sağlanamamalıdır.

EK: İstasyon Otomasyon Sistemi Kontrol Listesi