

Elektrik Dağıtım Sektörü Siber Güvenlik Yetkinlik Modeli Teknik Kontrol Maddeleri

EPDK, kontrol maddelerinde ekleme, düzenleme ve çıkarma yetkisine sahip tek kurumdur.

Elektrik dağıtım şirketleri için asgari uygulanacak kontroller Seviye 2 olarak belirlenmiştir.

Seviye	Açıklama	Hedeflenen Tamamlama Süresi (Öz Denetim/Fark Analizlerinin Tamamlanmasından Sonra)
Seviye 1	Giriş seviyesi kontroller bu grupta yer almaktadır. İlgili kontrollerin hali hazırda uygulandığı ya da kolayca uygulanabileceği değerlendirilen maddeler bu grupta toplanmıştır. Bu grupta yer alan maddeleri uygulamak zorunludur.	12 Ay
Seviye 2	İkinci aşama kontroller bu grupta yer almaktadır. İlgili kontrollerin uygulanabilmesi için kurum içi değişikliklerin yapılması gerekli kontroller bu grupta toplanmıştır. Bu grupta yer alan maddeleri uygulamak zorunludur.	18 Ay
Seviye 3	Üçüncü seviye kontroller bu grupta yer almaktadır. Bu grupta yer alan kontroller yeni bir projelendirme ya da uzun soluklu değişim gerektirmektedir. Bu grupta yer alan maddeleri uygulamak zorunludur.	24 Ay
Ek Kontroller	Zorluk derecesi yüksek ya da uygulanmasının faydalı olabileceği değerlendirilen kontroller bu grupta toplanmış olup zorunlu değildir.	

Tanım	Açıklama
Tesis	Tek bir lisans sahibi işletmeyi ifadeyi eder.
Otomatik Sayaç Okuma Sistemi (OSOS)	Sayaç verilerinin otomatik olarak uzaktan okunabilmesi, verilerin merkezi bir sisteme aktarılması, doğrulanması, eksik verilerin doldurulması, verilerin saklanması ve ilgili taraflara istenen formatta sunulması amacıyla, TEİAŞ ve dağıtım lisansı sahibi tüzel kişiler tarafından kurulacak olan ve gerekli yazılım, donanım ve iletişim altyapısını kapsayan sistemi ifade eder.
Yerleşke	Yerleşke, kontrol sistemleri ile ilişkili kritik verilerin işlendiği ve saklandığı fiziksel lokasyonları ifade eder.
Uç saha	Endüstriyel kontrol sistemi bileşeni içeren fiziksel lokasyonlar (Örneğin Trafo Merkezi)

TEİAŞ
T.C. Enerji
Bakanlığı

TEİAŞ Genel Müdürlüğü

Yüksek Enerji Kontrol Dairesi Başkanlığı

Yüksek Enerji Kontrol Dairesi Başkanlığı

Yüksek Enerji Kontrol Dairesi Başkanlığı

Yüksek Enerji Kontrol Dairesi Başkanlığı

Yüksek Enerji Kontrol Dairesi Başkanlığı

Yüksek Enerji Kontrol Dairesi Başkanlığı

Yüksek Enerji Kontrol Dairesi Başkanlığı

Endüstriyel Ağ Güvenliği				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-1	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Erişim Kontrolleri	Seviye 1	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) hizmet veren kontrol merkezlerinde yetkisiz kişi ve cihazların endüstriyel ağa girişi (Network Access) kısıtlanmalı (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) veya fiziksel güvenlik önlemleri ile yetkisiz erişimler engellenmelidir. Bu kontroller hem kablolu hem de kablosuz ağlar için uygulanmalıdır.
EAG-2	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Erişim Kontrolleri	Seviye 1	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde hizmet veren acil durum/yedek kontrol merkezlerinde yetkisiz kişi ve cihazların endüstriyel ağa girişi (Network Access) kısıtlanmalı (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) veya fiziksel güvenlik önlemleri ile yetkisiz erişimler engellenmelidir. Bu kontroller hem kablolu hem de kablosuz ağlar için uygulanmalıdır.
EAG-3	Endüstriyel Ağ Güvenliği	Politika, Prosedür, Süreç	Seviye 2	Elektrik dağıtım şebekesi içerisinde mevcut SCADA sistemine bağlı veya ethernet tabanlı ağ yapısı olan tüm trafo merkezleri tüketim yoğunluklarına göre tüketimi çok olandan başlanarak listelenmelidir. (Yükümlü kuruluşlar kendi dağıtım bölgelerinin dinamikleri uyarınca ilave kritiklik belirleme parametreleri de kullanabilir.)
EAG-4	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Erişim Kontrolleri	Seviye 2	Kritiklik seviyesi A sınıfı olan kuruluşlar bir önceki adımda belirlenen trafo merkezi tüketim yoğunluk listesinin ilk %20'sinde bulunan trafo merkezlerinde ağa giriş kontrolleri uygulamalıdır. (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) Kritiklik seviyesi B-C sınıfı olan kuruluşlar bir önceki adımda belirlenen trafo merkezi tüketim yoğunluk listesinin ilk %25'inde bulunan trafo merkezlerinde ağa giriş kontrolleri uygulamalıdır.
EAG-5	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS), kontrol merkezleri ve her türlü uc sahalarla olan haberleşmeler güvenlik duvarı (Referans_Topoloji_Elektrik_Dağıtım: EKS-GD-01) üzerinden sağlanmalıdır. Bu güvenlik duvarı sadece endüstriyel ağların izolasyonu/ayrıştırılması için konumlandırılmalı ve KBS güvenlik duvarından farklı olmalıdır. Kullanılan güvenlik duvarı ilgili kuruluşun endüstriyel protokollerini desteklemelidir. (IEC 104, DNP3 vb.)
EAG-6	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemleri ana kontrol merkezi ve acil durum/yedek kontrol merkezi arasındaki haberleşmeler yukarıda adreslenen endüstriyel ağıın izolasyonu/ayrıştırılması için kullanılan güvenlik duvarı (Referans_Topoloji_Elektrik_Dağıtım: EKS-GD-01) üzerinden ve güvenli bir iletişim kanalı kullanılarak (IPsec vb.) sağlanmalıdır.
EAG-7	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemleri (EKS) kontrol merkezleri arasında Layer2 bağlantı olması durumunda, hem ana kontrol merkezi hem de acil durum/yedek kontrol merkezlerinde aynı ağ güvenlik kontrolleri uygulanıyor olmalıdır.
EAG-8	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar ve harici ağlar arasındaki (güvensiz ağlar) haberleşmeler güvenlik duvarı (Referans_Topoloji_Elektrik_Dağıtım: EKS-GD-01) üzerinden sağlanmalıdır. Bu güvenlik duvarı endüstriyel ağı izole eden güvenlik duvarıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-9	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) farklı kontrol sistemleri ile ICCP üzerinden veri okuma entegrasyonları endüstriyel ağı izole eden güvenlik duvarı (Referans_Topoloji_Elektrik_Dağıtım: EKS-GD-01) üzerinden sağlanmalıdır.
EAG-10	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Ek kontrol	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) farklı kontrol sistemleri ile ICCP üzerinden veri yazma entegrasyonları, ICCP protokolünü tanıyan ve sadece belirli parametrelere izin verebilen bir güvenlik duvarı veya benzeri güvenliği sağlayabilen bir güvenlik bileşeni üzerinden sağlanmalıdır.
EAG-11	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Ek kontrol	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) uç sahalarla olan haberleşmeler için kullanılan endüstriye: protokollerde yetkisiz endüstriyel komutları durdurabilecek güvenlik cihazları (Referans_Topoloji_Elektrik_Dağıtım: EKS-GD-01) konumlandırılmalıdır. (IEC 104, DNP3 protokolleri ile elektrik açma/kesme operasyonları vb.)
EAG-12	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) GES, RES gibi santraller üzerinden elektrik dağıtım şebekesine ait kontrol sistemi bileşenlerine olan bağlantılar güvenlik duvarı (Referans_Topoloji_Elektrik_Dağıtım: EKS-GD-01) üzerinden sağlanmalıdır.
EAG-13	Endüstriyel Ağ Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlara ilişkin mantıksal topolojiler katmanlı güvenlik mimarisiyle tasarlanmalı ve uygun şekilde dokümanite edilmelidir.
EAG-14	Endüstriyel Ağ Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlara ilişkin fiziksel topolojiler dokümanite edilmelidir.
EAG-15	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel bileşenlere güvensiz ağlar ya da yarı güvenli ağlar (DMZ: Demilitarized zone) üzerinden olan erişim trafiği bir saldırı tespit katmanından geçirilmelidir. Bunu sağlamak adına mevcut güvenlik bileşenlerinde IDS imzaları devreye alınabileceği gibi alternatif olarak açık kaynak kodlu teknolojiler de kullanılabilir.
EAG-16	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlarda trafik aynalanması (mirroring) yöntemi ile saldırı tespiti gerçekleştirilebilir. Bu izleme minimum olarak kontrol merkezi ve acil durum kontrol merkezi ağları ile kontrol merkezlerinin uç sahaları WAN haberleşmelerini de kapsamalıdır.
EAG-17	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Ek kontrol	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) trafo merkezleri ağlarında trafik aynalanması (mirroring) yöntemi ile saldırı tespiti gerçekleştirilebilir.
EAG-18	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Kesme	Ek kontrol	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağları izole etmek/ayrıştırmak için konumlandırılan güvenlik duvarı üzerinde (Referans_Topoloji_Elektrik_Dağıtım: EKS-GD-01) endüstriyel protokollere yönelik tehditleri de içeren IPS ve antivirüs vb. güvenlik önlemleri devreye alınmalıdır.
EAG-19	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemleri (EKS) içerisinde bulunan bileşenler görevlerine göre sanal ağlara (VLAN) ayrılmalı ve bu ağlar arasında geçiş kontrolleri uygulanmalıdır. Söz konusu katmanlı yapı; acil durum/yedek kontrol merkezlerinde de gerçekleştirilmelidir. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılara aranacaktır.)

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-20	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) mühendislik iş istasyonları endüstriyel ağlardan izole edilmelidir. Sadece iş ihtiyacı olduğu durumlarda kullanıma tahsis edilmelidir.
EAG-21	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlardan kurumsal ağlara doğru olan haberleşmeler bu haberleşmelere özel oluşturulmuş OT-DMZ ağları ya da izole sanal ağlar (VLAN) üzerinden sağlanmalıdır. Aynı şekilde kurumsal ağlardan endüstriyel ağlara doğru olan haberleşmeler de OT-DMZ ağları ya da izole sanal ağlar (VLAN) üzerinden sağlanmalıdır.
EAG-22	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) sanal ağların (VLAN) devreye alınmasını takiben ağ ve güvenlik cihazlarının yönetim arayüzleri de (management interface) ayrı bir sanal ağ üzerinde konumlandırılmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
EAG-23	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemleri (EKS) altyapısında her bir uç istasyon ağ seviyesinde farklı bir alt ağ olarak oluşturulmalıdır.
EAG-24	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 3	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemleri (EKS) altyapısında her bir uç istasyon için endüstriyel protokol trafiği ve diğer trafikler (kamera, fiziksel güvenlik, sayaç vb.) farklı sanal ağlar (VLAN) olarak yapılandırılmalı ve bu sanal ağlar (VLAN) arası geçiş mevcut ağ/güvenlik cihazları üzerinden kontrollü olarak sağlanmalıdır.
EAG-25	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Ek kontrol	Endüstriyel ağlarla iletişim halinde olan tüm KBS bileşenleri ayrı bir sanal ağ (VLAN) içerisinde konumlandırılmalı ve OT-DMZ ağı üzerinden endüstriyel ağlar ile haberleşmelidir. (CRM, CBS, WorkForce Management, ERP, OMS, Güvenli Uzak Erişim vb.)
EAG-26	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Endüstriyel ağlar ve KBS ağları arasında haberleşmenin yönü endüstriyel ağdan kurumsal ağa olacak şekilde OT-DMZ üzerinden sağlanmalıdır. Kurumsal ağlardan endüstriyel ağlara doğru veri çekme operasyonlarının gerekli olması durumunda bu veri akışı ek kontroller ile gerçekleştirilmelidir.
EAG-27	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 1	Endüstriyel ağlar içerisinde yer alan sunucu ve uygulamalar doğrudan internet üzerinden erişilebilir durumda olmamalıdır.
EAG-28	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 1	Endüstriyel ağlarla iletişimi olan tüm bileşenlerin doğrudan internete olan erişimleri sonlandırılmalıdır.
EAG-29	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Uzak Erişim	Seviye 1	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemi (EKS) bileşenlerine internet üzerinden gerçekleştirilecek tüm uzak erişimler öncelikli olarak KBS/kurumsal ağ üzerinde sonlandırılmalıdır. (VPN vb.) Bu uzak erişim yöntemleri üreticiler, çalışanlar ve alt yükleniciler için farklı yetkilendirme politikalarını destekleyebilmelidir. KBS ağı üzerinden endüstriyel ağlara yönelik uzak erişimler OT-DMZ ağı içerisinde konumlandırılmış güvenli bir atlama noktası/sunucusu/uygulaması üzerinden kontrollü olarak sağlanmalıdır. Uzaktan erişimlere ilişkin tüm süreçler diğer mevcut teknik maddelere uyumlu olarak işletilmelidir. (Olay yönetimi ve süreklilik, kimlik ve erişim yönetimi vb.)
EAG-30	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Uzak Erişim	Ek kontrol	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerine (EKS) yapılacak uzak erişimler için bu işe özelleşmiş teknolojiler kullanılmalıdır. (Oturma kaydetme, oturma yönetimi, çift faktörlü doğrulama, güvenli dosya transferi vb.)

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-31	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 1	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde tüm güvensiz servisler (açık metin protokoller, uzak erişim servisleri, güncelliğini yitirmiş protokoller) periyodik denetim ya da ağ trafiğinin analizi ile tespit edilmelidir.
EAG-32	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Güvenli Konfigürasyon	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde tespit edilen BT tabanlı (TELNET, HTTP, TFTP, vb.) güvensiz servisler devre dışı bırakılmalıdır.
EAG-33	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Güvenli Konfigürasyon	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde tespit edilen gereksiz veya kullanılmayan servisler devre dışı bırakılmalıdır.
EAG-34	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde mevcut varlıkların servisleri sürekli olarak izlenmelidir.
EAG-35	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 1	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) güvenli ve güvensiz ağlar arasında mevcut olan koruma mekanizmalarının bypass edilmesine olanak tanıyabilecek tüm dual-homed arayüzler (interface) devre dışı bırakılmalıdır. İkinci bir arayüz kullanılmasını zorunlu kılan bir durum mevcut ise söz konusu arayüzün bağlantısı güvenlik duvarı (Referans_Topoloji_Elektrik_Dağıtım: EKS-GD-01) üzerinden kontrollü olarak sağlanmalıdır.
EAG-36	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) Seviye-2 ile Seviye-1 (Purdue modeline göre) ağlar arasında mevcut olan koruma mekanizmalarının bypass edilmesine olanak tanıyabilecek tüm dual-homed arayüzler interface'ler devre dışı bırakılmalıdır. İkinci bir arayüz kullanılmasını zorunlu kılan bir durum mevcut ise söz konusu arayüzün bağlantısı güvenlik duvarı üzerinden kontrollü olarak sağlanmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-37	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağ içerisinde bulunan ağ cihazları "Olay Yönetimi ve Süreklilik" başlığının ilgili maddelerini karşılamalıdır.
EAG-38	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Elektrik dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) ana kontrol merkezi ve uç sahalarla olan haberleşmeler şifreli olarak gerçekleştirilmelidir. Şifreli iletilemeyen trafikler izole ağlar üzerinden taşınmalıdır.
EAG-39	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, endüstriyel protokol trafiği bir APN bloğunda izole edilmelidir. Bu izolasyon işlemi aşağıda belirtilen maddeleri de kapsamalıdır; * EKS trafiklerinin taşındığı APN bloku/bloklarında sadece ilgili kuruluşa ait trafiklerin olması * EKS trafiklerinin taşındığı APN bloku/bloklarında sadece EKS trafiklerinin olması (Sayaç, mobil ekip cihazları vb. trafiğinin de bu ağlardan izolasyonu sağlanmalıdır.) * APN bloğundaki EKS trafikleri sadece bir tesise ait olmalıdır.
EAG-40	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, trafo merkezleri arası erişimler uygun bir teknoloji ile kontrol altına alınarak kısıtlanmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-41	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, İnternet Servis Sağlayıcısı (ISP) bünyesinde bulunan APN uç noktaları bir güvenlik duvarı üzerinde sonlandırılmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-42	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, İnternet Servis Sağlayıcısı (ISP) bünyesinde toplanan tüm trafiklerin, ISP güvenlik duvarı üzerinden kuruluşun güvenlik duvarına güvenli teknolojiler (IPsec VPN vb.) kullanılarak iletilmesi sağlanmalıdır.
EAG-43	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, APN ağlarına giriş kısıtlaması uygulanmalıdır. Bunu sağlanması amacıyla kuruluş bünyesinde kimlik doğrulama mekanizmaları kurgulanmalı ve oluşturulacak yapı kuruluş tarafından yönetilmelidir. (Örneğin GSM numaralarının ağa erişimin kısıtlanabilmesi için kullanılabilmesi amacı ile RADIUS sunucular konumlandırılması. Söz konusu RADIUS sunucularının yönetimi kuruluşta olmalı ve kuruluş ağında konumlandırılmalıdır.)
EAG-44	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Ek Kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN), (APN) teknolojisi kullanılması durumunda, APN trafiğinin karıştırıcı (Jammer) sistemleri ile baskılanması sebebiyle servis kesintileri oluşabileceği kuruluş tarafından değerlendirilmeli ve ilgili trafik akışının sürekliliğinin sağlanabilmesi için gerekli tedbirler alınmalıdır.
EAG-45	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda endüstriyel protokol trafiği RF ağında izole edilmelidir. Bu izolasyon işlemi kapsamında haberleşme telsizleri gibi bileşenler endüstriyel trafik ağının dışında tutulmalıdır.
EAG-46	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda trafo merkezleri arası erişimler uygun bir teknoloji ile kontrol altına alınarak kısıtlanmalıdır.
EAG-47	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, RF ağında olan trafo merkezlerine ait endüstriyel trafik kuruluşa ait güvenlik duvarı (Referans_ Topoloji_Elektrik_Dağıtım: EKS-GD-01) üzerinde sonlandırılmalıdır.
EAG-48	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, RF ağında araya girme ve elektromanyetik yayılım (Tempest) saldırılarına karşı önlem alınmalıdır.
EAG-49	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, RF ağından gerçekleştirilecek endüstriyel haberleşme için trafiği şifreli olarak iletebilen teknolojiler kullanılmalıdır.
EAG-50	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, servis kesintisine neden olabilecek saldırılara karşı önlem alınmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-51	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Ek Kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, RF altyapısı olay yönetimi ve süreklilik alanının (domain) ilgili maddelerine uyumlu olacak şekilde tasarlanmalıdır. Mimari tasarımı tekil hata noktası (single point of failure) bulunmamalıdır.
EAG-52	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-SD-WAN	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında, yazılım tanımlı geniş alan ağı (SD-WAN) teknolojilerinin kullanılması durumunda, endüstriyel protokol trafiği için özelleştirilmiş izole bir SD-WAN mimarisi oluşturulmalıdır.
EAG-53	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-SD-WAN	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında, yazılım tanımlı geniş alan ağı (SD-WAN) teknolojilerinin kullanılması durumunda, SD-WAN yapısı içerisinde gerçekleştirilen endüstriyel protokol haberleşmesi için trafiği şifreli olarak iletebilen teknolojiler kullanılmalıdır.
EAG-54	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-SD-WAN	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında, yazılım tanımlı geniş alan ağı (SD-WAN) teknolojilerinin kullanılması durumunda SD-WAN ağında olan trafo merkezlerine ait endüstriyel trafik kuruluşu ait güvenlik duvarı (Referans_Topoloji_Elektrik_Dağıtım: EKS-GD-01) üzerine sonlandırılmalıdır.
EAG-55	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-SD-WAN	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında, yazılım tanımlı geniş alan ağı (SD-WAN) teknolojilerinin kullanılması durumunda trafo merkezleri arası erişimler uygun bir teknoloji ile kontrol altına alınarak kısıtlanmalıdır.
EAG-56	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-MPLS	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) WAN trafiğinde MPLS teknolojilerinin kullanılması durumunda, MPLS omurgasında kuruluşa hizmet eden ağ cihazlarında güncelleme ve yama yönetimi gerçekleştirilmelidir. MPLS sağlayıcısı firma yaması bulunan acil ve kritik seviyeli güvenlik açıklıklarını giderdiğine dair yazılı kanıt sunabilmeli ve kanıtları saklayabilmelidir. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-57	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-MPLS	Seviye 2	Elektrik dağıtım şebekelerinde WAN trafiğinde MPLS teknolojilerinin kullanılması durumunda, MPLS omurgasında kuruluşa hizmet eden ağ cihazlarında güvenli yapılandırma prensipleri uygulanmalıdır. Ağ cihazlarındaki güvenlik yapılandırmaları belirli periyotlarla kuruluş ile paylaşılmalı ya da kuruluşu kalıcı "read-only" bir hesap tanımlanması sağlanmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-58	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-MPLS	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) WAN trafiğinde MPLS teknolojilerinin kullanılması durumunda, MPLS omurgasında kullanılan ağ cihazlarında basit ya da tahmin edilebilir kullanıcı adı ve parola bulundurulmamalıdır. Her bir ağ cihazında özel bir kullanıcı adı ve parola atanmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-59	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-MPLS	Seviye 3	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) WAN trafiğinde MPLS teknolojilerinin kullanılması durumunda, MPLS omurgasında iletilen trafiğin şifreli olarak taşınması sağlanmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
EAG-60	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sisteminde (EKS) endüstriyel ağların izolasyon ve segmentasyonunda yazılım tabanlı teknolojilere ek olarak donanım tabanlı teknolojiler de devreye alınmalıdır.

Endüstriyel İstemci ve Sunucu Güvenliği				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İSG-1	Endüstriyel İstemci ve Sunucu Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucular için endüstriyel üretici tarafından onaylanan ve operasyonel sürekliliği tehlikeye atmayacak uç nokta (endpoint) güvenlik önlemleri (kötü amaçlı yazılım koruma uygulamaları, uç nokta tehdit tespit sistemi, uç nokta güvenlik duvarı vb.) tanımlanmalı ve uygulanmalıdır.
İSG-2	Endüstriyel İstemci ve Sunucu Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren istemciler için endüstriyel üretici tarafından onaylanan ve operasyonel sürekliliği tehlikeye atmayacak uç nokta (endpoint) güvenlik önlemleri (kötü amaçlı yazılım koruma uygulamaları, uç nokta tehdit tespit sistemi, uç nokta güvenlik duvarı vb.) tanımlanmalı ve uygulanmalıdır.
İSG-3	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Medya Güvenliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren istemcilerde harici medya kullanımları devre dışı bırakılmalıdır.
İSG-4	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Medya Güvenliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucularda harici medya kullanımları devre dışı bırakılmış olmalıdır.
İSG-5	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Medya Güvenliği	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde yeni nesil USB tabanlı saldırılara karşı önlem alınmalıdır. (Rubber Ducky vb.)
İSG-6	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Olay Tespiti ve Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde "Olay Yönetimi ve Süreklilik" başlığı altındaki maddelere uygun olarak loglar tutulmalı ve yönetilmelidir.
İSG-7	Endüstriyel İstemci ve Sunucu Güvenliği	Mobil Cihaz Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren taşınabilir mühendislik iş istasyonları (dizüstü vb.) ilgili kuruluş envanterine kayıtlı olmalıdır. Mühendislik operasyonlarında alt yüklenicilere ait güvensiz iş istasyonları endüstriyel ağa dahil edilmemeli ve EKS bileşenlerine bağlanmamalıdır. Kuruluşa ait taşınabilir mühendislik iş istasyonlarının güvenlik seviyesi kuruluş içi ve kuruluş dışında aynı olmalıdır.
İSG-8	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucu Operasyon Güvenliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren mühendislik iş istasyonları günlük operasyonel işlerde kullanılmamalıdır. (E-posta vb.)
İSG-9	Endüstriyel İstemci ve Sunucu Güvenliği	Veri Koruma	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde disk şifreleme yöntemleri uygulanmalıdır.
İSG-10	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde güvenli BIOS yapılandırmaları devreye alınmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İSG-11	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde sadece yetkili kullanıcıların uygulama kurmasına izin verilmelidir.
İSG-12	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde sadece güvenlik onayından geçmiş uygulamaların yüklenmesine ve kullanılmasına izin verilmelidir.
İSG-13	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler için kuruluşa özel güvenli bir kurulum imaj dosyası oluşturulmalı, periyodik olarak kontrol edilmeli ve güncellenmelidir.
İSG-14	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde internet üzerinden güvensiz uzak erişime imkan verecek yazılım ve servisler bulundurulmamalıdır.
İSG-15	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunuculara bulundukları ağ içerisinde uzak erişim (VNC, SSH, RDP vb.) yapılması durumunda ek güvenlik kontrolleri uygulanmalıdır. (sanal ağ ayrıştırma, güvenli atlama noktası, uç nokta güvenlik duvarı ile erişim kısıtlamaları vb.)
İSG-16	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucu Operasyon Güvenliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan tüm uygulamalar lisanslı olmalıdır.
İSG-17	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Olay Tespiti ve Yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler merkezi bir zamanlama sunucusundan senkronize edilmelidir. Bu senkronizasyon işlemi sırasında ağ seviyesinde sadece gerekli servis ve portlara izin verilmelidir.
İSG-18	Endüstriyel İstemci ve Sunucu Güvenliği	GPS Güvenliği	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler için kullanılan merkezi zamanlama sunucusunun GPS tabanlı olması halinde, GPS temelli saldırılara karşı koruma önlemleri alınmalıdır.
İSG-19	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan kötü amaçlı yazılım koruma uygulamaları endüstriyel üreticinin de onayladığı aralıklarla güncellenmelidir. Bu aralıklar 4 aydan daha uzun süreli olarak tanımlanmamalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
İSG-20	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan kötü amaçlı yazılım koruma uygulamaları yüksek yetkili kullanıcılar tarafından da dahil olmak üzere devre dışı bırakılamamalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İSG-21	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güncelleme/Yama Yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerin işletim sistemleri endüstriyel üreticinin de onayladığı tanımlı aralıklarla güncellenmelidir. Bu aralıklar 4 aydan daha uzun süreli olarak tanımlanmamalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
İSG-22	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güncelleme/Yama Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan uygulamalar, üretici güncelleme ve yamalarının yayınlanmış olma ihtimaline karşı belirlenen aralıklarla kontrol edilmelidir. Güvenlik açısından önem arz eden güncellemeler endüstriyel üretici gözetiminde gerçekleştirilmelidir. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
İSG-23	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerin tüm gereksiz kablolu ve kablosuz ağ arayüzleri devre dışı bırakılmalıdır. Ek olarak tüm gereksiz servis ve portlar devre dışı bırakılmalıdır.
İSG-24	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerin ağ servisleri yönetiminde "Endüstriyel Ağ Güvenliği" başlığının ilgili maddelerine uygun hareket edilmelidir.
İSG-25	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde IPv6 ağ arayüzleri devre dışı bırakılmalıdır.
İSG-26	Endüstriyel İstemci ve Sunucu Güvenliği	Veri Koruma	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde imha yönetimi kuruluşun belirlediği politikalar doğrultusunda gerçekleştirilmelidir.
İSG-27	Endüstriyel İstemci ve Sunucu Güvenliği	Beyaz Liste Uygulamaları	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde beyaz liste (Whitelisting) uygulamaları devreye alınmalıdır.
İSG-28	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda endüstriyel etki alanı ile KBS etki alanı birbirinden tamamiyle izole edilmelidir. (Bu amaçla trust, parent-child, farklı OU gibi yöntemler kullanılmamalıdır.)

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İSG-29	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, endüstriyel etki alanının kapsamı sadece ilgili endüstriyel kontrol sistemini işleten kuruluş ile sınırlı olmalıdır. Üreticinin şablon olarak hazırladığı ya da farklı ortamlarda kullandığı etki alanı yapıları kuruluş endüstriyel kontrol sistemleri içerisinde kullanılmamalıdır.
İSG-30	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, ortak erişime açık klasörler içerisindeki dosyalarda yüksek yetkili kullanıcı bilgileri gömülü olarak saklanmamalıdır.
İSG-31	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisine (domain controller) sadece gerekli protokoller üzerinden erişimi mümkün kılacak kısıtlamalar uygulanmalıdır.
İSG-32	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisi (domain controller) üzerinde gerekli olmayan tüm ağ servisleri devre dışı bırakılmalıdır.
İSG-33	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisi (domain controller) yedekli mimaride tasarlanmalıdır.
İSG-34	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı bileşenlerinde üretici tarafından sıkça kullanılan kullanıcı adı ve parolalar bulundurulmamalıdır.
İSG-35	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisi (domain controller) sunucusunun tekil görev için kullanılması sağlanmalıdır. DHCP, DNS ve dosya paylaşım vb. servisler için farklı sunucular konumlandırılmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
İSG-36	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanına ait tüm bileşenler yama yönetim politikalarına uygun olarak yönetilmelidir.
İSG-37	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan tüm bileşenler "Tehdit ve Zafiyet Yönetim" başlığına uygun olarak güvenlik denetimi ve sızma testlerine tabi tutulmalıdır. (İstemci, sunucu, konfigürasyon, GPO vb.)

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İSG-38	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan sunucular için güvenli konfigürasyon kontrol listesi oluşturmalıdır.
İSG-39	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan sunucular oluşturulan güvenli konfigürasyon kontrol listesine göre periyodik gözden geçirilmelidir. Konfigürasyon değişikliklerini anlık olarak loglayacak yapılandırmalar devreye alınmalıdır.
İSG-40	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan Grup İlkeleri (GPO) güvenli bir şekilde uygulanmalıdır.
İSG-41	Endüstriyel İstemci ve Sunucu Güvenliği	HMI Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS), operatörler günlük operasyonları gerçekleştirdikleri arayüzler (HMI) üzerinde operasyonu gerçekleştirmek için gerekli olan en düşük yetki ile çalışmalıdır. Arayüzler (HMI) yetki aşımına izin vermeyecek şekilde yapılandırılmalıdır.
İSG-42	Endüstriyel İstemci ve Sunucu Güvenliği	HMI Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan arayüzler (HMI) devre dışı bırakma (bypass) ve kaçış saldırılarını engelleyebilecek şekilde yapılandırılmalıdır. Bu yapılandırmalar "Tehdit ve Zafiyet Yönetim" başlığına uygun şekilde periyodik olarak test edilmelidir.

Endüstriyel Tehdit ve Zafiyet Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TZY-1	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi için gerekli bilgi kaynakları belirlenmelidir.
TZY-2	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi amacı ile belirlenen kaynaklardan siber güvenlik tehdit bilgisi toplanmalı ve işlenmelidir.
TZY-3	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinin (EKS) güvenliği ve sürekliliği için risk teşkil edebilecek tehditler belirlenmeli ve bu tehditlerin yönetimi için iyileştirme aksiyonları belirlenmelidir.
TZY-4	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin profilendirilmesi için tehdit hakkında en az aşağıdaki bilgiler edinilmelidir. -Tehdidin hedefi -Kabiliyetleri -Tehdit hedefinin endüstriyel operasyondaki önemi
TZY-5	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi için belirlenen bilgi kaynakları önceliklendirilmeli ve sürekli olarak takip edilmelidir.
TZY-6	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik risk teşkil edebileceği değerlendirilen tehditler analiz edilmeli, sınıflandırılmalı ve önceliklendirilmelidir.
TZY-7	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik zafiyetlerin yönetilebilmesi için gerekli bilgi kaynakları belirlenmelidir.
TZY-8	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi amacı ile belirlenen kaynaklardan siber güvenlik zafiyet bilgisi toplanmalı ve işlenmelidir.
TZY-9	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinin (EKS) güvenliği ve sürekliliği için risk teşkil edebilecek zafiyetler belirlenmeli ve bu zafiyetlerin yönetimi için iyileştirme aksiyonları belirlenmelidir.
TZY-10	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	"Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddeleri doğrultusunda elektrik dağıtım şebekesi endüstriyel kontrol sistemleri (EKS) için güvenlik analizleri ve testleri gerçekleştirilmelidir.
TZY-11	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik risk teşkil edebileceği değerlendirilen zafiyetler analiz edilmeli, sınıflandırılmalı ve önceliklendirilmelidir.
TZY-12	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik risk teşkil edebileceği değerlendirilen zafiyetler önceliklerine göre yönetilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TZY-13	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine ait siber güvenlik yamaları "İstemci ve Sunucu Güvenliği" başlığına uygun olacak şekilde yamaların operasyonlara olan etkisi de gözden geçirilerek uygulanmalıdır.
TZY-14	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit ve zafiyet yönetim yaklaşımı dokümanite edilmiş olmalıdır.
TZY-15	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit ve zafiyet yönetim sürecinde ihtiyaç duyulabilecek tüm üçüncü taraflar belirlenmeli ve bu süreçte dahil edilmelidir.
TZY-16	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit ve zafiyet yönetimi için gerekli standart, kılavuz ve yasal mevzuatlar belirlenmelidir.
TZY-17	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit istihbaratı, bir bütün olarak izlenmelidir.
TZY-18	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Tehdit yönetimi kapsamında arz güvenliğini riske atabilecek, doğal afetler, terör vb. gibi bilgiler de bütüncül bir yaklaşım sergileyecek şekilde değerlendirilmelidir.
TZY-19	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin yerel ve küresel tehdit istihbarat kaynakları bir bütün olarak yönetilmelidir. (Bu kaynaklar üretici sayfaları, küresel bilgilendirme sayfaları gibi kaynaklar olabilir.)
TZY-20	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	KBS ve EKS'e ilişkin tehdit istihbarat kaynakları bir bütün olarak yönetilmelidir.
TZY-21	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit tespiti	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehditler (saldırgan aktiviteleri) gerçek zamanlı olarak izlenebilir. Bu izleme, istemci ve sunucu üzerinden bilgi toplanarak ve ağ trafiği takip edilerek gerçekleştirilebilir.
TZY-22	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit tespiti	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin bir saldırı tespiti yapılması durumunda, söz konusu saldırılar sınıflandırılmalıdır. (operasyonel tehditler, siber güvenlik tehditleri, fiziksel, ağ tehditleri vb.)
TZY-23	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizi "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddelerine göre aktif veya pasif yöntemlerle (manuel ya da otomatize araçlarla) en az yılda bir kez gerçekleştirilebilir durumda olmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TZY-24	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizi "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği"nin ilgili maddelerine uygun yöntemlerle gerçekleştirilmeli ve en az aşağıda belirtilen bileşenleri kapsamalıdır. -EKS sunucu ve istemci işletim sistemleri -Kontrol katmanı bileşenleri (PLC/RTU, Röle, Giriş/Çıkış (I/O) Modülleri vb.) -Sayacılar, ölçüm cihazları -Dönüştürücüler (Protokol ve seri/ethernet) -Ağ cihazları -Endüstriyel uygulama yazılımları -Siber güvenlik teknolojileri
TZY-25	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizleri farklı kaynakları girdi olarak kullanılmalıdır. (Sızma testleri, güvenlik testleri, analizleri, zafiyet taramaları vb.)
TZY-26	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizleri için otomatize bir araç kullanılacaksa seçilen aracın teknolojisi, protokol desteği ilgili altyapıya uygun olmalıdır.
TZY-27	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin siber güvenlik zafiyetleri bir yaşam döngüsü şeklinde yönetilmelidir. (Tespit, iyileştirme, doğrulama, kapatma, kabul vb.)
TZY-28	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tespit edilen her bir siber güvenlik zafiyeti için ilgili birim ve personellere sorumluluk ataması gerçekleştirilmelidir.
TZY-29	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin risk analizi, sızma testi, güvenlik analizi çıktılarının eğilimi sürekli olarak izlenmelidir.
TZY-30	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri ana kontrol ve acil/yedek kontrol merkezleri bileşenlerini içermelidir.
TZY-31	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri uç saha bileşenlerini (ağ, haberleşme, çevirici, protokol vb.) içermelidir.
TZY-32	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri endüstriyel kontrol sistemlerinin bulunduğu tüm fiziksel lokasyonları içermelidir.
TZY-33	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri, EKS varlıklarının sürüm bilgisinden zafiyet tespitine imkan vermemelidir. Bu amaçla manuel veya otomatize yöntemler kullanılabilir.

Endüstriyel Siber Güvenlik Risk Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
ERY-1	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi Stratejisi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemleri (EKS) için dokümente edilmiş bir endüstriyel siber güvenlik risk yönetimi stratejisi olmalıdır. Risk yönetim metodolojisi endüstriyel altyapılar için özelleştirilmiş olmalıdır.
ERY-2	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi Stratejisi	Seviye 1	Endüstriyel siber güvenlik risk yönetim stratejisi, endüstriyel operasyonlara etkinin dikkate alınması da dahil olmak üzere, risk önceliklendirmesi için bir yaklaşıma sahip olmalıdır. Bu strateji endüstriyel operasyonlar dikkate alınarak hazırlanmalıdır.
ERY-3	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Belirlenen riskler, risk azaltma, risk kabulü, riskten kaçınma veya riskin transferi işlemleri çerçevesinde yönetilmelidir. Bu süreçte ilişkin gerekli dokümantasyon oluşturulmalı ve bu dokümanlar üç yıl süreyle saklanmalıdır.
ERY-4	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme dokümanı asgari olarak, "risk numarası, risk kategorisi, riskin oluşması için koşullar, zafiyet, tehdit, risk, riski taşıyan bileşen/bileşen grubu, riskten etkilenen bileşen/bileşen grubu, riskin etki değeri, riskin gerçekleşme olasılığı" başlıklarını içermelidir.
ERY-5	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme dokümanı, endüstriyel operasyonlarda veya bilgi sisteminde (yeni tehdit ve zafiyetler belirlendiği durumlar dahil olmak üzere) önemli değişiklikler olduğunda veya sistemin güvenlik durumunu etkileyebilecek diğer koşullar olduğunda güncellenmelidir.
ERY-6	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Riskin gerçekleşme olasılığı "normal, yüksek ya da çok yüksek" dereceleri kullanılarak değerlendirilmelidir.
ERY-7	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk işleme planları, risklerin azaltılmasına ilişkin uygulanması veya alınması gereken önlem ve kontrolleri içermelidir.
ERY-8	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Tespit edilen riskler analiz edilerek, risk yönetimi stratejisine uygun olarak işleme faaliyetleri önceliklendirilmelidir.
ERY-9	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Tespit edilen riskler, risk yönetimi stratejisine uygun olarak izlenmelidir.
ERY-10	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk analizi sonuçları, ağ (KBS ve/veya EKS) mimarisine ait risk değerlendirme sonuçlarını da içermelidir. Risk analizlerinde mimari hatalar ve zafiyetler de girdi olarak kullanılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
ERY-11	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Endüstriyel siber güvenlik risk yönetimi faaliyetleri için oluşturulan dokümanlar düzenli olarak takip edilmelidir. (Strateji dokümanları, politika ve prosedürler, formlar vb.)
ERY-12	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Risk yönetimi faaliyetleri için paydaşlar belirlenmeli ve risk yönetimi sürecine dahil edilmelidir.
ERY-13	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Risk yönetimi faaliyetlerini desteklemek için yeterli kaynak (insan kaynağı, finansman vb.) sağlanmalıdır.
ERY-14	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Risk yönetimi faaliyetlerinin içeriğinde yer alacak standartlar ve/veya kılavuzlar belirlenmelidir. (NIST 800-53, NIST800-82, ISA 62443, ISO 27019, C2M2 vb.)
ERY-15	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi nitel ve nicel olarak ölçüme olanak tanımalıdır.
ERY-16	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi risk kabul kriterlerini ve risk kabul değerini tanımlamalıdır.
ERY-17	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi risk sahibini tanımlamalıdır. Riskler ilgili risk sahibine atanmalıdır.
ERY-18	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Endüstriyel siber güvenlik risk belirleme sürecinde endüstriyel operasyonlara etkiye göre derecelendirme yapılmalıdır.
ERY-19	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi tekrar edilebilir, karşılaştırılabilir ve tutarlı sonuçlar üretebilir olmalıdır.
ERY-20	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri, ana kontrol/yedek kontrol odalarını ve bileşenlerini içermelidir.
ERY-21	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri, trafo merkezleri ve bileşenlerini içermelidir.
ERY-22	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri, endüstriyel sistemlerin olduğu tüm fiziksel lokasyonlar için fiziksel güvenlik risklerini içermelidir.
ERY-23	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri endüstriyel iletişim protokollerini içermelidir.
ERY-24	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk Yönetim faaliyetleri uç sahalarla haberleşme ve ağ güvenlik risklerini içermelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
ERY-25	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetimi faaliyetlerinde, Enerji Sektöründe EKS Güvenlik Kontrolleri başlıkları en az aşağıdaki bileşenler için uygulanmalıdır. - İş istasyonu riskleri - İnsan Makine arayüzü (HMI) iş istasyonu riskleri - Sunucu tabanlı riskler (SCADA, OPC, Historian vb.) - Endüstriyel yazılım uygulamaları riskleri (SCADA yazılımı) - Siber güvenlik uygulama ve çözümleri - Mühendislik iş istasyonu riskleri - Endüstriyel ağ ve ekipmanları güvenlik riskleri - Endüstriyel altyapı kontrol katmanı ekipmanları güvenlik riskleri (PLC, RTU, Röle) - Sayaçlar - KBS ağları entegrasyon riskleri (CRM, CBS, OMS, ERP, Çağrı Merkezi vb.)
ERY-26	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetimi üçüncü taraf bilgi güvenliği risklerini içermelidir.
ERY-27	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci ISO 27001 BGYS ve CB-DDO formlarına uygun olarak işletilmelidir.
ERY-28	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci kapsamında artık risk yönetim ilkeleri tanımlanmalıdır. Risk işleme sonrası kalan artık riskler; risk sahibi ve üst yönetim tarafından onaylanmalıdır.
ERY-29	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci, operasyonel süreklilik risklerini içermelidir.
ERY-30	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Siber güvenlik riskleri ethernet ve seri iletişim tabanlı saldırı vektörleri dikkate alınarak belirlenmelidir.
ERY-31	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim sürecinde; sızma testleri, güvenlik analizleri, iç denetim çıktıları da girdi olarak kullanılmalıdır.
ERY-32	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme sürecinde her bir endüstriyel siber güvenlik riskinin, çevre etkisi, finansal etkisi ve insana etkisi (abone sayısı) belirlenmelidir.
ERY-33	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme sürecinde her bir endüstriyel siber güvenlik riskinin diğer kritik altyapılara olan etkisi de değerlendirilmelidir. (Su yönetimi, haberleşme, ulaşım, bankacılık vb.)
ERY-34	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci insan temelli riskleri de içermelidir. (Personel, operator, mühendis, KBS çalışanı, siber güvenlik çalışanı, üretici ve alt yüklenici çalışanları)

Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
VKY-1	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları için envanter oluşturulmalıdır. Envanter Yönetimi amaca özel olarak oluşturulmalıdır.
VKY-2	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	Bu envanter, siber saldırı hedefi olabilecek her türlü bileşeni de içermelidir. (Yazıcı, IoT Cihazlar, kartlı geçiş sistemi vb.)
VKY-3	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları envanteri, siber güvenlik süreçlerini destekleyen öznitelikler içermelidir. (Konum, varlık önceliği, işletim sistemi ve donanım yazılımı sürümleri, varlık sahibi, varlık emanetçisi vb.) Envanterdeki KBS ve EKS varlıklarına, bilgi varlıklarının fonksiyon ve görev önemine göre tanımlanmış CB DDO kriterlerini de göz önünde bulundurarak öncelik verilmelidir.
VKY-4	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları için oluşturulan envanter periyodik olarak ve sistem değişikliği durumunda güncellenmelidir.
VKY-5	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 2	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları envanteri, varlık kullanım ömrü (end-of-life) ve üretici desteğinin sonlanması (end-of-support) gibi bilgileri içermelidir.
VKY-6	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	Envanterde kullanım ömrü sonuna gelmiş veya değişimi yapılacak olan KBS ve EKS varlıklarına ait veriler güvenli bir şekilde silinmelidir.
VKY-7	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Bilgi Varlığı Envanteri Yönetimi	Seviye 2	Elektrik dağıtım prosesinin devamlılığı için önemli olan bilgi varlıklarının envanteri oluşturulmalıdır. (Bu bilgi varlıkları, SCADA analog komutlar, özel konfigürasyon parametreleri ve müşteri bilgileri olabilir) Envanter yönetimi endüstriyel prosese özel olmalıdır.
VKY-8	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 1	Temel konfigürasyon mimarisi oluşturulmalıdır. Konfigürasyonlarda siber güvenlik açısından gerekli olan minimum isterler dokümanite edilmelidir. (IP adresleri, parolalar, servis/port, kritik set değerleri vb.)
VKY-9	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 2	Temel konfigürasyon mimarisi, varlıklara konfigürasyon dağıtımı ve geri yükleme süreçlerinde kullanılmalıdır.
VKY-10	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 2	Yeni gerçekleştirilen varlık konfigürasyonlarının, temel konfigürasyon mimarisine göre tutarlılıkları izlenmelidir.
VKY-11	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 1	Temel konfigürasyon mimarisi, periyodik olarak, sistem değişiklikleri ve siber güvenlik mimarisindeki değişikliklere göre gözden geçirilmeli ve güncellenmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
VKY-12	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Değişikliklerinin Yönetimi	Seviye 1	Varlıklarda yapılacak temel mimari konfigürasyon değişiklikleri, uygulanmadan önce, kurum tarafından tanımlanmış ve dokümente edilmiş olan sistem etkisi ve siber güvenlik isterlerine göre değerlendirilmeli, test edilmeli ve onaylanmalıdır. Bu testler siber güvenlik gereksinimlerini karşılamalıdır. Değişikliklere ilişkin kayıtlar tutulmalıdır.
VKY-13	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Değişikliklerinin Yönetimi	Seviye 1	Değişim yönetimi takibi, varlıkların tüm yaşam döngüsünü ele almalıdır. (Satın alma, dağıtım, operasyon, kullanımdan kaldırılması vb.)
VKY-14	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Değişikliklerinin Yönetimi	Seviye 1	Değişiklik kayıtları, varlıkların siber güvenlik gereksinimlerini etkileyen değişikliklerle ilgili bilgileri de içermelidir.
VKY-15	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Varlık yönetim sürecinde dokümente edilmiş prosedürler oluşturulmalıdır. İlgili prosedürler takip edilmeli ve sürdürülmelidir. Varlık yönetim sürecinde gerekli üst yönetim desteği sağlanmalıdır. Süreçten sorumlu personeller atanmalı ve gerekli yetkilendirilmeler yapılmalıdır. Varlık yönetim sürecinin etkinliği değerlendirilmeli ve izlenmelidir.

Endüstriyel Kimlik ve Erişim Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
KEY-1	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan operatör iş istasyonlarında, sunucularda, mühendislik iş istasyonlarında, uygulamalarda ve ağ cihazlarında tahmin edilebilir ya da basit kullanıcı adı/parola kullanılmamalıdır. Sistem tarafından karmaşık parola atamaları zorlanmalıdır.
KEY-2	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan operatör iş istasyonlarında, sunucularda, mühendislik iş istasyonlarında, uygulamalarda ve ağ cihazlarında alt yükleniciler tarafından atanan parolalar değiştirilmelidir. Her bir tesis kendine özel kullanıcı adı ve parolalara sahip olmalıdır.
KEY-3	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan bileşenlerde operatör yetkisi ve mühendislik yetkisi ayrıştırılmalıdır.
KEY-4	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Ek Kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) uygulamalarında (SCADA) operatörlerin yaptıkları işlemlere göre yetki ayrıştırması yapılmalıdır.
KEY-5	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) uygulamalarına (SCADA) ait kullanıcı ve yetkilendirme dosyaları, kullanıcıların erişebildiği alanlarda saklanmamalıdır. Bu tür dosyalara erişimler kısıtlanmalıdır.
KEY-6	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Ek Kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sisteminde (EKS) işletim sistemi kullanıcılarıyla endüstriyel uygulama (SCADA) kullanıcıları birbirinden ayrıştırılmalıdır.
KEY-7	Endüstriyel Kimlik ve Erişim Yönetimi	Hesap Yönetimi	Ek Kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) operatör kullanıcılarına ait hesaplar tekil kullanıcı esasına göre oluşturulmalıdır.
KEY-8	Endüstriyel Kimlik ve Erişim Yönetimi	Hesap Yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine ait kullanıcı adı ve parolalar ilgili sistemden farklı bir dijital ortamda ya da fiziksel olarak saklanmamalıdır. (Dosya sunucusu, excel dosyaları, kağıt ve panolarda saklama vb.)
KEY-9	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sisteminde (EKS) gerçekleştirilecek kontrol işlemleri (yüksek yetkili manevra vb.) için ikinci bir kimlik doğrulama mekanizması kurgulanmalı ya da söz konusu işlemler için "izleme" ve "kontrol" yetkileri ayrıştırılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
KEY-10	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) uygulamalarında (SCADA) mevcut kullanıcıdan farklı bir kullanıcı ya da yetkiye geçiş yapılırken parola doğrulaması yapılmalıdır.
KEY-11	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) uygulamalarına (SCADA) ait parola bilgileri tersine mühendislik ile elde edilemeyecek şekilde oluşturulmalıdır.
KEY-12	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim için kullanılacak kullanıcı adı ve parolalar, endüstriyel bileşenlere ait kullanıcı adı ve parolalardan farklı olmalıdır.
KEY-13	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	KBS altyapılarında kullanılan ve elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine entegrasyonu olan sistem ve uygulamalara ait kullanıcı adı ve parolalar, endüstriyel bileşenler üzerinde tanımlı kullanıcı adı ve parolalardan farklı olmalıdır.
KEY-14	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda iki faktörlü kimlik doğrulama mekanizmaları devreye alınmalıdır.
KEY-15	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda uzak erişim sağlayan her bir kullanıcıya özel kullanıcı adı ve parola bilgisi atanmalıdır.
KEY-16	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim için kullanılacak hesaplar geçici süre ile oluşturulmalıdır.
KEY-17	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda erişime ilişkin tüm kayıtlar saklanmalıdır. (Erişim talebi, erişim onayı, erişim sırasında oluşan sistem kayıtları vb.)
KEY-18	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim için bir atlama noktası (jump box) kullanılıyorsa ilgili bileşen üzerinde bulunan hesapların ele geçirilmesini önlemek amacıyla gerekli sıkılaştırmalar devreye alınmalıdır.
KEY-19	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda, uzak erişimin sadece izin verilen bileşen ve sisteme yapılmasını garanti altına alacak ağ ve sistem tabanlı erişim kısıtlamaları uygulanmalıdır.

Endüstriyel Olay Yönetimi ve Süreklilik				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-1	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale politika ve prosedürleri, elektrik dağıtım şebekesi endüstriyel kontrol sistemlerini (EKS) kapsayacak şekilde hazırlanmalıdır.
OYS-2	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Kurumsal SOME rehberinde adreslendiği şekilde kurum içi rol ve sorumluluklara uygun olarak olay müdahale eğitimleri alınmalıdır.
OYS-3	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale eğitimleri siber güvenlik kaynaklı olarak oluşabilecek kriz yönetimini de içermelidir.
OYS-4	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale eğitimleri elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) siber güvenlik kaynaklı olarak oluşabilecek "görünürlük kaybı" ve "kontrol kaybı" etkilerine sahip senaryoları içermelidir.
OYS-5	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Kuruluş, olay müdahale testleri kapsamında, kendi yetkinliklerini belirli periyotlarla simülasyonlar aracılığı ile test etmelidir.
OYS-6	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale testleri, iş sürekliliği, acil durum yönetimi, kriz yönetimi gibi süreç ve planlarla koordine olarak gerçekleştirilmelidir.
OYS-7	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale testleri kapsamında performans ölçümleri gerçekleştirilmelidir. (Ekip performansı, sistem yeterlilikleri, testlerin uygunluğu, birimler arası koordinasyon yeteneği vb.)
OYS-8	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale için gerekli yöntemler tanımlanmalı ve uygulanmalıdır. (Log toplama, ağ trafiği toplama, adli bilişim verisi toplama vb.)
OYS-9	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Ek kontrol	Olay müdahale kapsamında olaylara otomatik cevap verme süreçleri tanımlanmalıdır. (Route ekleme çıkarma, kural ekleme çıkarma vb.)
OYS-10	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale kapsamında, endüstriyel operasyonların sürekliliğine ilişkin senaryolar tanımlanmalıdır. (Manuel operasyona geçiş, yedek kontrol merkezine geçiş vb.)
OYS-11	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale yaklaşımı iç tehditlerin (çalışanlar, ağa erişim yetkisi olan alt yükleniciler ve üreticiler vb.) tespiti içerecek şekilde tasarlanmalıdır.
OYS-12	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale kapsamında, kurum içi birimlerin koordinasyonu tanımlanmalıdır. (İK, İşletme Birimleri, Hukuk vb.) Her bir olay için bilgi verilen, raporlanan, sorumlu kişi/birim şeklinde sınıflandırmalar yapılmalıdır.
OYS-13	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale ve sonrasında, kurum dışı otoritelerle iletişim ve koordinasyon gereklilikleri tanımlanmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-14	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale ve sonrasında, gerek duyulması halinde kuruluşa hizmet veren alt yüklenici ve üreticilerle gerçekleştirilecek koordinasyon süreci tanımlanmalıdır.
OYS-15	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale ekibi, Kurumsal SOME yönergeleri kapsamında oluşturulmalıdır.
OYS-16	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Tüm olay müdahale süreçleri Kurumsal SOME Rehberine uyumlu olmalıdır.
OYS-17	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale süreçleri, zararlı yazılım analizi ve adli bilişim analizini kapsamalıdır.
OYS-18	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale kapsamında, kurum anormal durum tespit yeteneklerine sahip olmalıdır. Kurumlar bunu sağlamak için istemci/sunucu, uygulama veya ağ tabanlı bir çözüm kullanabilir.
OYS-19	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale süreçleri, medya ve müşteri/abone iletişimlerini içermelidir.
OYS-20	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay yönetimi süreci, elektrik dağıtım operasyonlarına özel endüstriyel proses, varlık ve ekipmanlara uyumlu şekilde tanımlanmalıdır.
OYS-21	Endüstriyel Olay Yönetimi ve Süreklilik	Olay İzleme	Seviye 2	Olay izleme süreçleri endüstriyel kontrol sistemleri (EKS) için de devreye alınmalıdır.
OYS-22	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Raporlama	Seviye 1	Olay raporlama süreçleri Kurumsal SOME rehberine uyumlu olmalıdır.
OYS-23	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Raporlama	Seviye 1	Olay raporlama süreçleri, olayın yaşanmasına neden olan zafiyetlerin bilgisini içermelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-24	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale Planı	Seviye 1	Kurum kendine özgü olay müdahale planlarını geliştirmelidir. Bu planlar en az aşağıdaki başlıkları içermelidir. - Olay müdahale organizasyonu (Roller ve görevler) - Olay tanımı (Olay sınıflandırma) - Raporlama (Olay bildirimi, analizi) - Kaynakların sağlanması - Bilgi paylaşımı (Kurum ve kurum dışı iletişim esasları) - Doküman yönetimi (Doküman güncelleme ve dağıtımı) - Kök neden analizi (Olayların kök neden analiz yöntemi ve raporlaması. Üçüncü taraflarda meydana gelebilecek olayların kök neden analizi hususuna sözleşmelerde yer verilmelidir.) - Olaylardan alınan dersler (lessons learned) ve olayların tekrarlanmasının engellenmesi - <u>Olay müdahale simülasyonu ve başarı performans ölçümü</u>
OYS-25	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Tespit Etme	Seviye 1	Tespit edilen olaylar belirli bir rol ya da kişiye atanmalıdır.
OYS-26	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Tespit Etme	Seviye 1	Olay tespiti için kriterler belirlenmelidir. (Olay tanımı, nereye bakılacağı vb.)
OYS-27	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesindeki kontrol merkezleri ve "Endüstriyel Ağ Güvenliği" başlığında belirlenen kritik trafo merkezlerinde bulunan ağ ve güvenlik cihazları log üretme kapasitesine sahip olmalıdır.
OYS-28	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesindeki kontrol merkezlerinde bulunan ağ ve güvenlik cihazları log yönlendirme kapasitesine sahip olmalıdır.
OYS-29	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesindeki kontrol merkezlerinde bulunan ağ ve güvenlik cihazları log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.
OYS-30	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesindeki kontrol merkezlerinde bulunan ağ ve güvenlik cihazlarına ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-31	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan ve kritik olarak belirlenen trafo merkezlerinde bulunan ağ cihazları log yönlendirme kapasitesine sahip olmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-32	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan ve kritik olarak belirlenen trafo merkezlerinde bulunan ağ cihazları log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.
OYS-33	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan ve kritik olarak belirlenen trafo merkezlerinde bulunan ağ cihazlarına ilişkin log'lar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-34	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan trafo merkezlerindeki endüstriyel cihazlar (RTU, IED, Röle) log tutma kapasitesine sahip olmalıdır.
OYS-35	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan trafo merkezlerindeki endüstriyel cihazlar (RTU, IED, Röle) log yönlendirme kapasitesine sahip olmalıdır.
OYS-36	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan trafo merkezlerindeki endüstriyel cihazlar (RTU, IED, Röle) log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.
OYS-37	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan trafo merkezlerindeki endüstriyel cihazlara (RTU, IED, Röle) ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-38	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan yazılım ve uygulamalar (SCADA yazılımları, veri toplama yazılımları, sayaç yönetim uygulamaları vb.) log üretme kapasitesine sahip olmalıdır.
OYS-39	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan yazılım ve uygulamalar (SCADA yazılımları, veri toplama yazılımları, sayaç yönetim uygulamaları vb.) log yönlendirme kapasitesine sahip olmalıdır.
OYS-40	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan yazılım ve uygulamalar (SCADA yazılımları, veri toplama yazılımları, sayaç yönetim uygulamaları vb.) log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-41	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan yazılım ve uygulamalara (SCADA yazılımları, veri toplama yazılımları, sayaç yönetim uygulamaları vb.) ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anımlandırılmalıdır.
OYS-42	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan akıllı sayaçlar log tutma, yönlendirme, derecelendirme ve sınıflandırma kapasitesine sahip olmalıdır.
OYS-43	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan akıllı sayaçlara ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anımlandırılmalıdır.
OYS-44	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Olay yönetimi gerçekleştirebilmek için kullanılan tüm log kaynakları aynı saat dilimi üzerinden senkronize edilmelidir.
OYS-45	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucularda aşağıdaki tipteki loglar tutulmalıdır. - İşletim sistemi logları - Bileşen üzerindeki güvenlik yazılımları logları (kötü amaçlı yazılım koruma uygulamaları, whitelisting uygulamaları) - Bileşen üzerinde bulunan diğer yazılımlara ilişkin loglar
OYS-46	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucular log yönlendirme kapasitesine sahip olmalıdır.
OYS-47	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucular log derecelendirme ve sınıflandırma kapasitesine sahip olmalıdır.
OYS-48	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucularda kayıt altına alınan loglar merkezi olarak toplanmalı, işlenmeli ve anımlandırılmalıdır.
OYS-49	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Tespit Etme	Seviye 2	Olay tespit yetenekleri, tehdit, zafiyet ve risk yönetim süreçleri ile bütünlük olmalıdır.
OYS-50	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 1	Hangi olayların USOM'a bildirileceğine dair ilişkin kriter tanımlanmalıdır. (operasyonların etkilenmesi, hizmet verememe, endüstriyel operasyonlara etki ve etkilerin dereceleri vb.) Olay bildirim kriteri belirli periyotlarla gözden geçirilmeli ve gerekli durumlarda güncellenmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-51	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) gerçekleşen siber güvenlik bildirimleri sürekli izlenerek ve analiz edilerek bildirim sürecinde girdi olarak kullanılabilir.
OYS-52	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 1	Siber güvenlik bildirimlerinin siber güvenlik olayı olup olmadığına karar vermek için kriterler belirlenmelidir.
OYS-53	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 1	Olayların yaşam döngüsü uçtan uca takip edilmelidir. (Kime atandığı, nasıl çözüldüğü, kimin çözdüğü vb.)
OYS-54	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Yönetiminde İş Sürekliliği	Seviye 1	Belirli olay ve bildirimlerin yaşanması durumunda kullanılacak iş sürekliliği planları geliştirilmelidir. (Hizmet kesintisi, operasyonel arıza vb.)
OYS-55	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan tüm ağ ve güvenlik cihazlarının konfigürasyonları periyodik olarak alınmalı, güvenli şekilde saklanmalı ve periyodik geri dönüş testleri gerçekleştirilmelidir.
OYS-56	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan tüm endüstriyel ekipman, uygulama ve bileşenlerin lojik ve/veya konfigürasyonları periyodik olarak yedeklenmeli , yedekler güvenli şekilde saklanmalı ve periyodik geri dönüş testleri gerçekleştirilmelidir.
OYS-57	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucuların imaj ve veri yedekleri periyodik olarak alınmalı, güvenli şekilde saklanmalı ve periyodik geri dönüş testleri gerçekleştirilmelidir.
OYS-58	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) iş sürekliliği planları hazırlanırken olası olayların etkileri girdi olarak kullanılmalıdır. (Hizmet kesintisi, görüntü kaybı, kontrol kaybı, üretim kaybı vb.)
OYS-59	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) operasyonların devamlılığı için gerekli olan varlık ve süreçler iş sürekliliği planına dahil edilmelidir.
OYS-60	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Hazırlanan süreklilik planları periyodik olarak test edilmeli ve gerekli durumlarda güncellenmelidir.
OYS-61	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Alınan veri, imaj konfigürasyon/lojik yedekleri orijinal veri seviyesinde korunmalıdır.
OYS-62	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Alınan tüm yedekler, mantıksal ve fiziksel olarak orijinal verilerden ayrıştırılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-63	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Operasyon açısından önem arz eden varlıklar için kurtarma süresi hedefleri (RTO) ve kurtarma noktası hedefleri (RPO) süreklilik planlarına dahil edilmelidir.
OYS-64	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Hazırlanan süreklilik planlarının ne zaman devreye alınacağına dair kriter tanımlanmalıdır.
OYS-65	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Hazırlanan süreklilik planı, tehdit, zafiyet ve risk yönetim süreçleri ile bütünleşik olarak işletilmelidir.
OYS-66	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Süreklilik planının testleri ya da icrası sonucu oluşan sonuçlar plan ile karşılaştırmalı gerekli durumlarda güncellenmelidir.
OYS-67	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Ek kontrol	(Ülkemizin yer aldığı coğrafyada yaşanan ve yaşanması olası doğal afetler göz önünde bulundurulduğunda)Kuruluşlar, ISO 22301 standardına sahip olmalıdır.
OYS-68	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden tüm kritik bileşenler yedekli yapıda olmalıdır. (Ağ ve güvenlik cihazları, sunucular, mühendislik iş istasyonları, kritik endüstriyel ekipmanlar vb.)
OYS-69	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 3	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden ağ bileşenleri için en az 1 adet olacak şekilde soğuk yedek (cold backup) tutulmalıdır. (Switch, router vb.)
OYS-70	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden güvenlik bileşenleri için en az bir adet soğuk yedek tutulmalıdır. (Güvenlik duvarı, IPS vb.)
OYS-71	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Ek kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden supervisory katmanda yer alan sunucu/istemci için en az bir adet soğuk yedek tutulmalıdır.
OYS-72	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Kurum, kurumsal misyon, iş süreci veya sistem düzeyinde tanımlanan acil durum planlama politikası; amaç, kapsam, roller, sorumluluklar, yönetim desteği, kurumsal varlıklar arasındaki koordinasyon ve uyumluluğu ele almalıdır . Acil durum planlama politikası; kurumun diğer politika ve prosedürleri ile uyumlu olmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-73	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Mevcut acil durum planı, politika ve prosedürleri Kurum tarafından tanımlanan olay veya zaman periyotlarına göre gözden geçirilmeli ve güncellenmelidir.
OYS-74	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planlarında ilgili kişi ve birimlerin iletişim bilgileri yer almalıdır.
OYS-75	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planları, bir sistem kesintisinde, siber saldırı veya arıza durumlarına rağmen işletmenin misyon ve fonksiyonlarını sürdürmeyi ele almalıdır.
OYS-76	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planı, yetkisiz ifşa ve içeriğinin değiştirilmesine karşı korunmalıdır.
OYS-77	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planı, normal operasyonlara dönüş planlarını içermelidir.
OYS-78	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum gereksinimlerini sağlamak için acil durum planı, harici hizmet sağlayıcıların acil durum planlarıyla koordine edilmelidir.
OYS-79	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Kriz durumlarında personelin etkin müdahalesini kolaylaştırmak için acil durum eğitimleri periyodik olarak düzenlenmelidir.
OYS-80	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planları, simülasyon ortamlarında ya da yedek/acil durum kontrol merkezinde test edilmelidir.
OYS-81	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planları, bölge çapında genel bir hizmet kesintisi veya felaket durumunda planların çalıştırılabilmesi için gerekli önlemleri içermelidir.
OYS-82	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Süreklilik gereksinimlerine uygun olarak kritik hizmet sağlayıcılar yedeklenmelidir. (Telekom hizmetleri vb.)
OYS-83	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Kuruluşlar, hizmet sağlayıcılardan acil durum planlarını oluşturmalarını istemelidir. Hizmet sağlayıcıların acil durum planları periyodik olarak gözden geçirilmelidir.
OYS-84	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Ek kontrol	Acil durum testleri kapsamında tüm yedeklilik senaryoları test edilmelidir.

Akıllı Cihaz Güvenliği				
No	Ana kontrol	Alt Kontrol	Seviye	Kontrol
ACG-1	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında yer alan tüm bileşenlerin ve iletişim cihazlarının bir envanteri oluşturulmalıdır.
ACG-2	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç mimarisinde yer alan tüm bileşenler "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddelerine uygun şekilde periyodik olarak güvenlik testlerine tabi tutulmalıdır.
ACG-3	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında yer alan tüm bileşenler risk yönetim süreci içerisinde değerlendirilmelidir.
ACG-4	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısı içerisinde gömülü yazılıma (firmware) sahip bileşenler için güvenli yapılandırma kontrol listesi hazırlanmalı ve işletme için minimum güvenlik kontrolleri belirlenmelidir. (Örnek referans: https://www.opencompute.org/documents/csis-firmware-security-best-practices-position-paper-version-1-0-pdf)
ACG-5	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısı içerisinde bulunan cihazlar üzerindeki debug arayüzleri (JTAG, SWD) müşteri ortamında devre dışı bırakılmalı veya uygun yetkilendirme yöntemleri ile aktif edilebilmelidir. (JTAG Enabling, SWD authentication vb.)
ACG-6	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısı içerisinde bulunan cihazlarda code integrity/kod bütünlük koruma mekanizmaları sahaya gönderilmeden önce devreye alınmalı ve bu durumun korunması sağlanmalıdır. (Secure boot, boot konfigürasyonlarının devre dışı bırakılması vb.)
ACG-7	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Ek kontrol	Akıllı cihazlar üzerinde kritik parametrelerin saklanması, cihaz kimliğinin değiştirilemez şekilde eşsiz bir anahtar ile ayırt edilebilmesi ve trust anchor (Root of Trust) amacıyla SE (Secure Element), HSM (Hardware Security Module), TPM (Trusted Platform Module), TEE (Trusted Execution Environment - ARM Trustzone) gibi bileşenler akıllı cihaz tarafından kullanılmalıdır.
ACG-8	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Ek kontrol	Elektrik dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerin üzerinde kullanılan üçüncü taraf kodlar statik kod analizi ile gözden geçirilmeli ve herhangi bir arka kapı (backdoor) olmadığı doğrulanmalıdır.
ACG-9	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenler merkezi bir noktadan güvenli bir şekilde güncellenme yeteneğine sahip olmalıdır. [Secure-FOTA (Firmware Over the Air Update) vb.]

No	Ana kontrol	Alt Kontrol	Seviye	Kontrol
ACG-10	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç mimarisinde yer alan sayaçlar log toplama mekanizmalarını desteklemelidir. Başarılı, başarısız kullanıcı giriş denemeleri, debug fonksiyonlarına erişim denemeleri gibi aktiviteler kayıt altına alınmalıdır. Bunlara ek olarak akıllı cihazlar fiziksel saldırılara karşı da log üretebilmelidir.
ACG-11	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerden alınan log kayıtları en az olay tipi, zaman damgası, kaynak, sonuç bilgilerini içermelidir.
ACG-12	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenler güvenilir bir zaman sunucusu üzerinden senkronize edilmelidir.
ACG-13	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerden alınan loglar üzerinde kritik/hassas bilgilerin olmadığı doğrulanmalıdır. (Kullanıcı bilgisi, kriptografik anahtarlar vb.)
ACG-14	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerden alınan loglar, ilgili bileşenler üzerinde ve toplama noktalarında uygun güvenlik kontrolleri ile korunmalıdır. Logların bileşenler üzerinden merkezi noktaya aktarımında güvenli iletişim teknolojileri kullanılmalıdır. (Anlık ya da cihaz üzerinden)
ACG-15	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerden alınan logların saklanmasına ilişkin süreler ilgili yasal düzenlemelere uygun olarak belirlenmelidir.
ACG-16	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Yasal Uyumluluk	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında kullanılan bileşenler üzerinde tutulan, işlenen ve saklanan tüm veriler için ilgili yasal düzenlemelere uygun hareket edilmelidir. (KVKK vb.)
ACG-17	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında kullanılan bileşenler üzerinde çalışan servisler belirlenmeli ve gereksiz olduğu değerlendirilen servisler devre dışı bırakılmalıdır.
ACG-18	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısına ilişkin risk analizi sürecinde tüm mimariye ilişkin saldırı vektörleri belirlenmeli ve uygun tehdit modelleme çalışmaları gerçekleştirilmelidir.
ACG-19	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısında kullanılan tüm iletişim kanalları ve protokoller belirlenmeli ve dokümente edilmelidir. (WAN, HAN vb.)
ACG-20	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Elektrik dağıtım şebekesi akıllı cihaz mimarisi uçtan uca belirlenmeli ve dokümente edilmelidir. Bu dokümantasyon kapsamında tüm bileşenler bir topoloji üzerinden gösterilmelidir.
ACG-21	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısında kullanılan tüm cihazlar belirlenerek, bunların üzerindeki erişim arayüzleri (USB, PS2 vb.) uygun seviyede güvenlik kontrolleri ile korunmalıdır. Kullanılmayan veya gereksiz olduğu değerlendirilen arayüzler devre dışı bırakılmalıdır.

No	Ana kontrol	Alt Kontrol	Seviye	Kontrol
ACG-22	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısında kullanılan cihazlar üzerindeki debug portları ve CLI (Command Line Interface) erişimleri belirlenerek uygun seviyede güvenlik kontrolleri ile korunmalıdır.
ACG-23	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Ek kontrol	Elektrik dağıtım şebekesi akıllı sayaç yapısı kapsamındaki kritik veriler HSM, SE, TPM vb. içerisinde saklanmalıdır.
ACG-24	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Ek kontrol	Gömülü kod (firmware) snarfing'e karşı uygun güvenlik kontrolleri tanımlanmalı ve korunmalıdır. Bunu sağlamak adına FLASH ve EEPROM alanlarında şifreleme teknikleri uygulanmalıdır. Temel prensip olarak durağan veri (data at rest) güvenliğini sağlamak adına dosya sistemi veya depolama alanlarında şifreleme teknikleri uygulanmalıdır.
ACG-25	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısında kullanılan cihazların iletişim protokolleri/arayüzleri güvenli şekilde yapılandırılmalıdır. (UART, I2C, SPI vb.)
ACG-26	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Haberleşme Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısı içerisindeki WAN haberleşmeleri izole veya şifreli kanallardan gerçekleştirilmelidir.
ACG-27	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Haberleşme Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç protokolleri replay saldırılarına karşı dirençli olmalıdır.
ACG-28	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Haberleşme Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç protokolleri araya girme saldırılarına karşı dirençli olmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
ACG-29	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısı içerisinde hizmet eden sunucular izole bir ağ üzerinde konumlanmalıdır.
ACG-30	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısı içerisindeki izole ağlara erişimler kısıtlanmalıdır. (Uzak erişim, üçüncü taraf, son kullanıcılar, diğer sunucular vb.)
ACG-31	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 1	Elektrik dağıtım şebekesi akıllı sayaç yapısı içerisinde hizmet eden sunucular uygun şekilde sıkılaştırılmalıdır. (Veri tabanı, uygulama sunucusu vb.)
ACG-32	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısında bulunan veri toplama (data concentrator) bileşenlerinden uç bileşenlere yönelik erişimler güvenilir kanallardan sağlanmalıdır.
ACG-33	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısında bulunan veri toplama noktaları arasındaki iletişimler kısıtlanmalıdır.
ACG-34	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısında kullanılan tüm bileşenlerde, gömülü ve basit parola kullanımı engellenmelidir.
ACG-35	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç altyapısında ağa giriş (access control) kontrolleri uygulanmalıdır.

No	Ana kontrol	Alt Kontrol	Seviye	Kontrol
ACG-36	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Tehdit ve Zafiyet Yönetimi	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısında kullanılan tüm bileşenlerin "Tehdit ve Zafiyet Yönetimi" başlığının ilgili maddelerine uygunluğu sağlanmalıdır.
ACG-37	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Tehdit ve Zafiyet Yönetimi	Seviye 2	Elektrik dağıtım şebekesi akıllı sayaç yapısında kullanılan tüm bileşenler anlık olarak izlenebilir durumda olmalıdır.

Endüstriyel Operasyon Güvenliği

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EOG-1	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan RTU'lar sadece belirli sunuculardan (Master) komut alacak şekilde yapılandırılmalıdır.
EOG-2	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) lojik işleyen bileşenlere sadece mühendislik iş istasyonunu üzerinden lojik güncellemeyi sağlayacak kontroller devreye alınmalıdır.
EOG-3	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Elektrik dağıtım şebekesinde, Endüstriyel Kontrol Sistemleri mimarisinde kullanılan lojik işleyen bileşenlere lojik güncellemeleri sırasında ek bir parola doğrulaması zorlanmalıdır.
EOG-4	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon değişimleri sadece yetkili iş istasyonları üzerinden sağlanmalıdır.
EOG-5	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Ek Kontrol	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon değişimleri sırasında ek bir parola doğrulaması zorlanmalıdır.
EOG-6	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Veri Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon dosyaları ve lojik dosyaları için bütünlük kontrolleri devreye alınmalıdır.
EOG-7	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyon Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon dosyaları ve lojik dosyaları sürüm numaraları ile takip edilebilmelidir.
EOG-8	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Erişim ve Yetkilendirme	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon dosyaları ve lojik dosyalarının saklandığı alanlara sadece yetkili kişi ve grupların eriştiği garanti altına alınmalıdır.
EOG-9	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Veri Güvenliği	Seviye 2	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon dosyaları ve lojik dosyaları kişisel bulut tabanlı sistemlerde ve dosya paylaşım alanlarında saklanamaz. Bu verilerin kurumsal bulut tabanlı sistemler ve dosya paylaşım alanlarında kullanılmasının zorunlu olduğu durumlarda; T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanarak yayımlanan Bilgi ve İletişim Güvenliği Rehberinde "4.3 Bulut Bilişim Güvenliği" tedbirleri sağlanarak saklanmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EOG-10	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Veri Güvenliği	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan ve üzerinde konfigürasyon veya lojik bilgisi bulunan ekipmanlar kurum dışına çıkarılacaksa (bakım, hibe vb.) söz konusu konfigürasyon ve lojik bilgileri ilgili bileşen üzerinden silinmelidir.

İnsan Kaynakları Güvenliği				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İKG-1	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	EKS altyapılarında çalışacak tüm personel yasal mevzuata uyumlu şekilde, gerekli güvenlik kontrollerinden geçirilmelidir. (Adli sicil, güvenlik soruşturması, referans ve belge kontrolü vb.)
İKG-2	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	EKS altyapılarında çalışacak personelin, işe uygunluk ve sağlık raporları bulunmalıdır.
İKG-3	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	EKS altyapılarında çalışacak personelle sözleşme imzalanmalıdır. (Bu sözleşmeler gizlilik sözleşmesi şeklinde olabileceği gibi ana sözleşmelerin gizlilik ve siber güvenlik maddelerini içermesi şeklinde de olabilir.)
İKG-4	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	Personelle yapılacak sözleşmelerde siber güvenlik ve gizlilik maddeleri en az aşağıdakileri içermelidir: - Gizli bilginin korunması, - Kurumsal hassas ve kritik bilgilerin korunması, - Kurumun uyguladığı veya uygulayacağı tüm siber güvenlik kontrollerine uyum, - Kuruluşa ait; lojik, konfigürasyon bilgileri, yedek dosyalar ve tasarımların kişisel disk, bilgisayar ya da bulut ortamlarında saklanmayacağına dair beyan, - Yasal, sözleşme kaynaklı veya müşteri gereksinimlerinden doğan siber güvenlik politika, prosedür ve uygulamalarına uyumlu çalışma.
İKG-5	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	İşe alım ilanları, ilgili tesisin siber güvenlik açısından bağlayıcı olan teknolojileri ile ilgili bilgi içermemesini sağlayacak politika, prosedür ve süreçler çerçevesinde tasarlanmalıdır.
İKG-6	İnsan Kaynakları Güvenliği	İstihdam Sırasında	Seviye 1	Personel, çalışma süresince tüm siber güvenlik politika, prosedür ve uygulamalarına uyumlu hareket etmelidir.
İKG-7	İnsan Kaynakları Güvenliği	İstihdam Sırasında	Seviye 1	Tüm EKS personeli periyodik siber güvenlik farkındalık programına dahil edilmelidir.
İKG-8	İnsan Kaynakları Güvenliği	İstihdam Sırasında	Seviye 1	Siber güvenlik operasyonlarını yürütecek personelin EKS bileşenleri ile ilgili eğitim almaları sağlanmalıdır.
İKG-9	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	Tüm EKS personeli için siber güvenlik ihlallerine ilişkin disiplin süreçleri tanımlanmalıdır.
İKG-10	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	Sözleşme ve uygulamalar, istihdam sonrası koşulları içermelidir.
İKG-11	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İstihdamın sonlandırılması ile birlikte tüm EKS varlıklarına olan mantıksal ve fiziksel erişimler sonlandırılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İKG-12	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İstihdam sonlanması ile birlikte tüm gerekli taraflar bilgilendirilmelidir.
İKG-13	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İstihdam sonlanması sürecinde operasyonel süreklilik için önem arz eden tüm varlıklar (proses, lojik vb.) güvenli bir şekilde devredilmelidir.
İKG-14	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İlgili istihdam sonlandırma süreci, olaylı ayrılma durumlarını da içermelidir.
İKG-15	İnsan Kaynakları Güvenliği	Üçüncü Taraf Güvenliği	Seviye 1	EKS altyapılarında üçüncü taraflarca sağlanan taşıeron personellerin hem birinci derece bağlı oldukları hem de hizmet sundukları kuruluşlar için bu başlık altındaki süreçler işletilmelidir. Alt yükleniciler, farklı bir alt yüklenici kullandığında sorumluluk devredemeyeceği gibi bu madde kapsamında doğan yükümlülükleri de yerine getirmelidir.
İKG-16	İnsan Kaynakları Güvenliği	Üçüncü Taraf Güvenliği	Seviye 1	Üçüncü taraflara veya üreticiye bağlı olarak çalışan personel kuruluşun belirlediği gizlilik ve siber güvenlik gereksinimlerinden muaf tutulamaz. Gerekli koşullarda ilgili personelle de ek bir gizlilik sözleşmesi veya siber güvenlik maddelerini içeren sözleşme yapılmalıdır.

Fiziksel Güvenlik				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-1	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke girişinde giriş çıkış kaydı tutulmalıdır.
FZG-2	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke girişinde yetkisiz erişime karşı önlemler alınmalıdır.
FZG-3	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke giriş prosedürleri tanımlanmalıdır. Yerleşke giriş prosedürleri, ziyaretçi, geçici-kalıcı çalışan, acil giriş durumlarını içermelidir.
FZG-4	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke girişlerinde uygun güvenlik ve emniyet eğitimleri verilmelidir.
FZG-5	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke giriş çıkışlarını izleyen elektronik sistemlerde zaman senkronizasyonu sağlanmalıdır.
FZG-6	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke giriş çıkışlarını izleyen elektronik sistemlerde merkezi kayıt yönetim sistemi entegrasyonu sağlanmalıdır.
FZG-7	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke giriş çıkışlarını izleyen elektronik sistemlerde yedekleme politikaları oluşturulmalı, yedekler alınmalı ve yedekler test edilmelidir.
FZG-8	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke çevresini izlemek için kameralar kurulmalıdır. Bu sistemler sürekli olarak izlenmelidir.
FZG-9	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke çevresi kamera kayıtları ilgili yasal süre kadar saklanmalıdır.
FZG-10	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Kamera sistemlerinde zaman senkronizasyonu sağlanmalıdır.
FZG-11	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Çevresel güvenlik bileşenleri izole ağlarda konumlanmalıdır.
FZG-12	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Çevresel güvenlik bileşenlerine erişim kullanıcı adı ve parola ile sağlanmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-13	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Çevresel güvenlik bileşenleri yetkisiz fiziksel erişime karşı korunmalıdır.
FZG-14	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Merkezi kontrol sistemi bileşenlerinin bulunduğu alanlara fiziki erişimin tamamıyla kontrol altına alınabileceği herhangi bir noktada X-RAY cihazı konumlandırılmalıdır.
FZG-15	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Araçlar gerekli kontrollerden geçirilerek yerleşkeye alınmalıdır.
FZG-16	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kayıt tutulmalıdır.
FZG-17	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemlerde zaman senkronizasyonu sağlanmalıdır.
FZG-18	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemler merkezi kayıt yönetim sistemine entegre edilmelidir.
FZG-19	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemlerde yedekleme politikaları oluşturulmalı, yedekler alınmalı ve yedekler test edilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-20	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemler izole ağlarda konumlandırılmalıdır.
FZG-21	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları çevresel güvenlik bileşenlerine erişim kullanıcı adı ve parola ile sağlanmalıdır.
FZG-22	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemlerde güçlü parola kullanılmalıdır.
FZG-23	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında kurum harici çalışanlara kurum personeli eşlik etmelidir.
FZG-24	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarını izlemek için kameralar kurulmalıdır. Bu sistemler sürekli olarak izlenmelidir.
FZG-25	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kamera kayıtları ilgili yasal süre kadar saklanmalıdır.
FZG-26	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kamera sistemlerinde zaman senkronizasyonu sağlanmalıdır.
FZG-27	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kamera sistemleri IP tabanlı ise ayrı izole bir ağ üzerinde konumlandırılmalıdır.
FZG-28	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kamera bileşenleri kullanıcı adı ve parola ile korunmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-29	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları çevresel güvenlik bileşenleri (Kamera, kartlı geçiş, yangın algılama vb.) yetkisiz fiziksel erişime karşı korunmalıdır.
FZG-30	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında bulunan kameralar proseslerin izlendiği HMI'ları görmeyecek şekilde konumlandırılmalıdır.
FZG-31	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kapıları otomatik olarak kapanmalıdır.
FZG-32	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarından acil çıkış mümkün olmalıdır.
FZG-33	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında yer alan çevresel izleme sensörleri yetkisiz fiziksel erişime olanak vermeyecek şekilde konumlandırılmalıdır.
FZG-34	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 2	Kontrol odalarının kapıları açık kaldığında alarm üretmelidir.
FZG-35	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında çevresel izleme sensörleri konumlandırılmalıdır. (Yangın, su, nem, sıcaklık vb.)
FZG-36	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında kullanılan çevresel izleme sistemleri alarm üretebilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-37	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları çevresel izleme sensörleri merkezi olarak izlenmelidir.
FZG-38	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş kontrolleri, enerjisiz kaldığında da aynı güvenlik seviyesini korumalıdır.
FZG-39	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarındaki tüm güvenlik bileşenleri yedek bir enerji ya da kesintisiz bir enerji kaynağı üzerinden beslenmelidir.
FZG-40	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 2	Endüstriyel operasyonlara hizmet eden istemci ve sunuculara fiziksel erişimler kısıtlanmalıdır.
FZG-41	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi hizmetlerinin üçüncü taraflardan temin edilmesi durumunda; alınması gerekli tedbirler sözleşmeler ile hüküm altına alınmalıdır. Paylaşımlı veri merkezlerinde tüm tarafların güvenliği ve gizliliği hizmet sağlayıcı tarafından güvence altına alınmalıdır.
FZG-42	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş-çıkış kayıtları tutulmalıdır.
FZG-43	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi elektronik geçiş kontrol sistemlerinde zaman senkronizasyonu sağlanmalıdır.
FZG-44	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi elektronik geçiş kontrol sistemlerinde merkezi log/kayıt yönetim entegrasyonu sağlanmalıdır.
FZG-45	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi elektronik geçiş kontrol sistemlerinde yedekleme politikaları oluşturulmalı, yedekler alınmalı ve yedekler test edilmelidir.
FZG-46	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi elektronik geçiş kontrol sistemleri kullanıcı adı ve parola ile korunmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-47	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi ziyaretlerinde yetkili personel ziyaretçilere eşlik etmelidir. Ziyaretçi ve refakatçi kayıtları en az bir yıl süre ile saklanmalıdır.
FZG-48	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezlerini izlemek için kamera sistemi kurulmalıdır.
FZG-49	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kameralara ilişkin kayıtlar belirlenen yasal süre kadar saklanmalıdır.
FZG-50	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kameralarda zaman senkronizasyonu sağlanmalıdır.
FZG-51	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kamera bileşenleri mantıksal izole bir ağ üzerinde konumlandırılmalıdır.
FZG-52	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kamera bileşenleri kullanıcı adı ve parola ile korunmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-53	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kameralar fiziksel erişime karşı koruma altına alınmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-54	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kameralar kör nokta olmaksızın konumlandırılmalıdır.
FZG-55	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş çıkış kapıları otomatik olarak kapanmalıdır.
FZG-56	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş çıkış kapıları acil çıkış prosedürlerine uygun olmalıdır.
FZG-57	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş çıkış noktalarında olan sensörler yetkisiz erişime olanak vermeyecek şekilde konumlandırılmalıdır.
FZG-58	Fiziksel Güvenlik	Veri Merkezi	Seviye 2	Veri merkezi kapıları açık kaldığında alarm üretebilmelidir.
FZG-59	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde çevresel izleme sensörleri konumlandırılmalıdır.
FZG-60	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi çevresel izleme sensörleri alarm üretme kabiliyetine sahip olmalıdır.
FZG-61	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi çevresel izleme sensörleri merkezi olarak izlenebilmelidir.
FZG-62	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş çıkış kontrolleri, elektrik kesintilerinde aynı koruma seviyesine sahip olmalıdır.
FZG-63	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi çevresel izleme bileşenleri yedek enerji kaynaklarıyla ya da kesintisiz enerji kaynakları üzerinden beslenmelidir.
FZG-64	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde deprem koruma önlemleri alınmalıdır.
FZG-65	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde su baskını koruma önlemleri alınmalıdır.
FZG-66	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi yangın koruma/söndürme sistemleri bulundurulmalıdır.
FZG-67	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi yangın koruma/söndürme sistemlerinin periyodik bakımları yapılmalıdır.
FZG-68	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi yangın koruma/söndürme sistemleri elektronik ortamlar için uygun olmalıdır.
FZG-69	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi uygun iklimlendirme altyapısına sahip olmalıdır.
FZG-70	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde kablolama güvenliği ilkeleri uygulanmalıdır.
FZG-71	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde kablolar etiketlenmelidir.
FZG-72	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde yedek enerji besleme kaynakları bulundurulmalıdır.
FZG-73	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde enerji besleme bileşenlerinin periyodik bakımları gerçekleştirilmelidir.
FZG-74	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan ve kritik ekipmanların olduğu alanlar için giriş-çıkış kontrolleri uygulanmalıdır. (Bu kontroller kilitli kapı, kilitli kabin vb. uygulamaları da içerir.)
FZG-75	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan ve personel bulunan uç sahalarda giriş-çıkış kayıtları tutulmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-76	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda bulunan kritik ekipmanlar kilitli alanlarda saklanmalıdır.
FZG-77	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda deprem koruma önlemleri kapsamında panolar yere sabitlenmelidir. Panolar içerisindeki ekipmanlar da pano içerisinde sabitlenmelidir.
FZG-78	Fiziksel Güvenlik	Uç Saha	Seviye 1	Su baskını tehdidi olduğu değerlendirilen kontrol sistemi bileşeni olan uç sahalarda su baskını koruma önlemleri alınmalıdır.
FZG-79	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda yangın koruma/söndürme önlemleri alınmalıdır.
FZG-80	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda yangın koruma/söndürme bileşenlerinin periyodik bakımları yapılmalıdır.
FZG-81	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda yangın koruma/söndürme bileşenleri elektronik ortamlar için uygun olmalıdır.
FZG-82	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda kablolama güvenliği ilkeleri uygulanmalıdır.
FZG-83	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda kablolar etiketlenmelidir.
FZG-84	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda yedek enerji beslemeleri kullanılmalıdır.
FZG-85	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda yedek enerji besleme bileşenlerinin periyodik bakımları gerçekleştirilmelidir.
FZG-86	Fiziksel Güvenlik	Uç Saha	Seviye 2	Kontrol sistemi bileşeni olan uç sahalarda acil durum tahliye prosedürleri tanımlanmalı ve uygulanmalıdır. (elektriksel yangın ya da patlama anında ilgili lokasyonunun güvenli şekilde tahliye edilmesi vb.)
FZG-87	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda yer alan çevresel izleme sensörleri yetkisiz erişime olanak vermeyecek şekilde konumlandırılmalıdır.
FZG-88	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda kapılar açık kaldığında alarm üretilmelidir.
FZG-89	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda çevresel izleme sensörleri konumlandırılmalıdır.
FZG-90	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda çevresel izleme sensörleri alarm üretebilmelidir.
FZG-91	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda çevresel izleme sensörleri merkezi olarak izlenebilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-92	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda giriş çıkış kontrolleri enerji olmadığında mevcut güvenlik seviyesini sürdürebilmelidir.
FZG-93	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda çevresel izleme bileşenleri yedek enerji beslemelerinden veya kesintisiz güç kaynağından beslenebilmelidir.
FZG-94	Fiziksel Güvenlik	Uç Saha	Seviye 3	Kontrol sistemi bileşeni olan uç sahalarda kullanılan fiziksel anahtarların yönetimi için tekil anahtar kullanılması durumunda kullanılacak anahtarın kopyalanmama özelliği olmalıdır. Anahtar dağıtımlarına ilişkin kayıtlar tutulmalı ve üç yıl süreyle saklanmalıdır. Personelin işten ayrılması durumunda bu anahtarlar teslim alınmalıdır.
FZG-95	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda kullanılan tüm fiziksel anahtarlar kopyalamaya karşı korunmalıdır.
FZG-96	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda ziyaretlere (trafo istasyonu vb.) ilişkin kayıtlar tutulmalı ve bir yıl süreyle saklanmalıdır.

Tedarikçi Yönetimi

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TDY-1	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluşun tedarikçiye olan bağımlılıklarını belirlemek için bağımlılık kriterleri tanımlanmalıdır.
TDY-2	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinin (EKS) devamlılığının sağlanması için önem arz eden tüm EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) tedarikçileri ve bu tedarikçilerin bağımlılıkları belirlenmelidir.
TDY-3	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluş, tüm kritik veya tekil kaynak bağımlılıklarını tanımlamalıdır.
TDY-4	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluş, tedarikçileri bağımlılıklarına göre önceliklendirmelidir.
TDY-5	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçiler ve diğer bağımlılıklardan kaynaklanan önemli siber güvenlik riskleri tanımlanmalı ve adreslenmelidir.
TDY-6	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Kuruluş, tedarikçi bağımlılıklarından kaynaklanan risk yönetimi aktivitelerini, mevcut risk yönetim süreçlerine dahil etmelidir.
TDY-7	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçiler ve diğer üçüncü taraflar ile yapılan sözleşmelerde siber güvenlik gereksinimleri dikkate alınmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır)</i>
TDY-8	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü taraflarla (üretici, mühendislik firmaları, altyükleniciler) yapılan sözleşmeler ve anlaşmalar aşağıdakileri içermelidir: - Üçüncü tarafların sunduğu ürün ve hizmetlerde ortaya çıkan zafiyetler, - Üçüncü tarafların kendisine ya da sunduğu ürünlere yönelik saldırı/tehdit bilgileri. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-9	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçiler kuruluşlara sunduğu ürün ve hizmetler için güvenli yazılım geliştirme süreçleri de dahil olacak şekilde siber güvenlik kontrollerine sahip olmalıdır. Sunulan ürün ve hizmetler bu kontrollere uygun olarak yürütülmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TDY-10	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Tedarikçiler ile yapılan sözleşmeler, tedarikçinin sağladığı hizmetlerin sahip olduğu veya gelecekte oluşabilecek güvenlik açıklarını bildirme sürecini içermelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-11	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçi tarafından sağlanan tüm yazılım ve yamaların bütünlüğü ve orijinallliği kontrol edilerek bu yazılım ve yamaların değiştirilmediği garanti altına alınmalıdır.
TDY-12	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçilerin sisteme uzaktan erişim için talepleri kapsamında dokümanite edilmiş uzak erişim bağlantı süreçleri ve kontrol yöntemleri tanımlanmalıdır. Tedarikçi erişimleri "Kimlik ve Erişim Yönetimi" başlığına uygun olarak yürütülmelidir.
TDY-13	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçi ile yapılan sözleşmelerde, elektrik dağıtım şebekesi endüstriyel kontrol sistemlerinin (EKS) sürekliliğini tehdit eden arıza ve problemlere müdahale süreçleri belirlenmeli ve oluşabilecek riskler, risk yönetim sürecine dahil edilmelidir.
TDY-14	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçilerin ve diğer harici kuruluşların değerlendirilmesi ve seçimi süreçlerinde, tedarikçilerin siber güvenlik gereksinimlerini karşılama yetenekleri değerlendirilmelidir.
TDY-15	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Tedarikçilerle yapılan sözleşmeler ya da yapılacak işi tanımlayan teknik şartnameler, bir siber güvenlik olayı veya ihlaline ilişkin bildirimleri de içermelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-16	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Kuruluşun bilgi varlıklarına geçici ya da kalıcı olarak erişebilen (uzak erişimler de dahil olmak üzere), bunu işletebilen, depolayabilen, iletebilen veya kuruluşun bilgi varlıkları için KBS altyapı bileşenlerini temin eden tedarikçilerin her biri ile sözleşme yapılmalı ve sözleşmeler bilgi güvenliği gereksinimlerini içermelidir.
TDY-17	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Üçüncü taraflardan doğan risklere ilişkin azaltıcı/yok edici kontroller uygulanmalıdır.
TDY-18	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Kuruluş tarafından üçüncü taraflara yönelik uygulanacak siber güvenlik kontrolleri, üçüncü tarafın kritikliğine ve risk seviyesine uyarlanabilir olmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TDY-19	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü taraf siber güvenlik süreç yönetiminde ve seçiminde destek sonu (end of support) ömür sonu (end of life) durumları göz önünde bulundurulmalı, sözleşmelere dahil edilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-20	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü tarafların lisanslı olmayan ürün sağlamasının önüne geçilmelidir. Bu konuyla ilgili oluşabilecek güvenlik ihlalleri sözleşme ya da teknik şartnamelerde ele alınmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır)</i>
TDY-21	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Siber güvenlik gereksinimlerinin karşılanmasına ilişkin kabul testleri (SAT ve FAT) tanımlanmalı ve gerçekleştirilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır)</i>
TDY-22	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü tarafların siber güvenlik kapasite yeterliliği periyodik olarak gözden geçirilmeli, tanımlı metriklerle ölçülmelidir. İşletmeler, belirli puanın altında kalan tedarikçilerle olan çalışmalarını gözden geçirmelidir.
TDY-23	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluş, tedarikçilerden doğan değişiklikleri yönetmelidir. Bu değişikliklerin siber güvenlik risk durumuna olan etkileri risk yönetim süreci kapsamında ele alınmalıdır.
TDY-24	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflara yönelik uygulanacak politika ve prosedürler periyodik olarak veya ihtiyaçlara uygun şekilde güncellenmelidir.
TDY-25	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflarla olan ilişkileri yöneten ve hizmetleri sağlayan personelde gerekli siber güvenlik yetkinlikleri aranmalıdır. Yetkinliklere ilişkin şartlar sözleşmelerle ya da teknik şartnamelerle garanti altına alınmalıdır.
TDY-26	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflarla olan ilişkileri yöneten personele ilişkin sorumluluklar, yetki ve hesap verilebilirlik durumu dokümanite edilmiş olmalıdır.
TDY-27	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflara ilişkin aktiviteler (itibar durumları, veri sızıntısı, hedefli saldırı, zararlı yazılım, fidye vb. saldırılara karşı durumları vb.) sürekli olarak izlenmeli ve değerlendirilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TDY-28	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü tarafların hizmet sunduğu kuruluşa ait bilgileri halka açık ağlarda izinsiz yayınlamayacağı ve referans gösteremeyeceği hususu şartnameler ya da sözleşmelerle garanti altına alınmalıdır.

Doğal Gaz Dağıtım Sektörü Siber Güvenlik Yetkinlik Modeli Teknik Kontrol Maddeleri

EPDK, kontrol maddelerinde ekleme, düzenleme ve çıkarma yetkisine sahip tek kurumdur.

Doğal gaz dağıtım şirketleri için asgari uygulanacak kontroller Seviye 1 olarak belirlenmiştir.

Seviye	Açıklama	Hedeflenen Tamamlama Süresi (Öz Denetim/Fark Analizlerinin Tamamlanmasından Sonra)
Seviye 1	Giriş seviyesi kontroller bu grupta yer almaktadır. İlgili kontrollerin hali hazırda uygulandığı ya da kolayca uygulanabileceği değerlendirilen maddeler bu grupta toplanmıştır. Bu grupta yer alan maddeleri uygulamak zorunludur.	18 Ay
Seviye 2	İkinci aşama kontroller bu grupta yer almaktadır. İlgili kontrollerin uygulanabilmesi için kurum içi değişikliklerin yapılması gerekli kontroller bu grupta toplanmıştır. Bu grupta yer alan maddeleri uygulamak zorunludur.	24 Ay
Seviye 3	Üçüncü seviye kontroller bu grupta yer almaktadır. Bu grupta yer alan kontroller yeni bir projelendirme ya da uzun soluklu değişim gerektirmektedir. Bu grupta yer alan maddeleri uygulamak zorunludur.	30 Ay
Ek Kontroller	Zorluk derecesi yüksek ya da uygulanmasının faydalı olabileceği değerlendirilen kontroller bu grupta toplanmış olup zorunlu değildir.	

Tanım	Açıklama
Tesis	Tek bir lisans sahibi işletmeyi ifadeyi eder.
Yerleşke	Yerleşke, kontrol sistemleri ile ilişkili kritik verilerin işlendiği ve saklandığı fiziksel lokasyonları ifade eder.
Lokal kontrol sistemi (Local SCADA)	Doğal gaz dağıtım şebekesinde RMS-A istasyonlarda, ana kontrol sistemi(SCADA) sistemine ek olarak ilgili istasyon için yönetim ve izleme kabiliyeti sunan sistemler bütünüdür.
Acil Durum Planı	İşyerlerinde meydana gelebilecek acil durumlarda yapılacak iş ve işlemler dâhil bilgilerin ve uygulamaya yönelik eylemlerin yer aldığı plan.
Kontrol Merkezi	Merkezi kontrol sistemlerinin olduğu fiziksel alanlar/odalar ve lokal kontrol sistemlerinin olduğu uç istasyonlar (RMS-A vb.)

Endüstriyel Ağ Güvenliği				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-1	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Erişim Kontrolleri	Seviye 1	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) hizmet veren kontrol merkezlerinde yetkisiz kişi ve cihazların endüstriyel ağa girişi (Network Access) kısıtlanmalıdır. (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) Bu kontroller hem kablolu hem de kablosuz ağlar için uygulanmalıdır.
EAG-2	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Erişim Kontrolleri	Seviye 1	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde hizmet veren acil durum/yedek kontrol merkezinde yetkisiz kişi ve cihazların endüstriyel ağa girişi (Network Access) kısıtlanmalıdır. (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) Bu kontroller hem kablolu hem de kablosuz ağlar için uygulanmalıdır.
EAG-3	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Erişim Kontrolleri	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) hizmet veren RMS-A tipi uç istasyonlarda yetkisiz kişi ve cihazların endüstriyel ağa girişi (Network Access) kısıtlanmalı veya fiziksel güvenlik önlemleri ile yetkisiz erişimler engellenmelidir. (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) Bu kontroller hem kablolu hem de kablosuz ağlar için uygulanmalıdır.
EAG-4	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS), kontrol merkezleri ve her türlü uç sahaları olan haberleşmeler güvenlik duvarı (Referans_Topoloji_Doğal_Gaz_Dağıtım: EKS-GD-01) üzerinden sağlanmalıdır. Bu güvenlik duvarı sadece endüstriyel ağların izolasyonu/ayırıştırılması için konumlandırılmalı ve KBS güvenlik duvarından farklı olmalıdır. Kullanılan güvenlik duvarı ilgili kuruluşun endüstriyel protokollerini desteklemelidir. (IEC 104, DNP3, MODBUSTCP vb.)
EAG-5	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemleri ana kontrol merkezi ve acil durum/yedek kontrol merkezi arasındaki haberleşmeler yukarıda adreslenen endüstriyel ağın izolasyonu/ayırıştırılması için kullanılan güvenlik duvarı (Referans_Topoloji_Doğal_Gaz_Dağıtım: EKS-GD-01) üzerinden ve güvenli bir iletişim kanalı kullanılarak (IPsec vb.) sağlanmalıdır.
EAG-6	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemleri (EKS) kontrol merkezleri arasında Layer2 bağlantı olması durumunda, hem ana kontrol merkezi hem de acil durum/yedek kontrol merkezlerinde aynı ağ güvenlik kontrolleri uygulanıyor olmalıdır.
EAG-7	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar ve harici ağlar arasındaki (güvensiz ağlar) haberleşmeler güvenlik duvarı (Referans_Topoloji_Doğal_Gaz_Dağıtım: EKS-GD-01) üzerinden sağlanmalıdır. Bu güvenlik duvarı endüstriyel ağı izole eden güvenlik duvarıdır.
EAG-8	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) farklı kontrol sistemleri ile Doğal gaz iletim altyapısı ile gerçekleştirilecek veri akışları hardwired kanallar üzerinden sağlamalıdır. (Referans_Topoloji_Doğal_Gaz_Dağıtım: EKS-GD-01) (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-9	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Ek kontrol	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) uç sahaları olan haberleşmeler için kullanılan endüstriyel protokollerde yetkisiz endüstriyel komutları durdurabilecek güvenlik cihazları (Referans_Topoloji_Doğal_Gaz_Dağıtım: EKS-GD-01) konumlandırılmalıdır. (IEC 104, DNP3, MODBUSTCP protokolleri ile doğal gaz vana açma/kapama operasyonları vb.)
EAG-10	Endüstriyel Ağ Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlara ilişkin mantıksal topolojiler katmanlı güvenlik mimarisiyle tasarlanmalı ve uygun şekilde dokümanite edilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-11	Endüstriyel Ağ Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlara ilişkin fiziksel topolojiler dokümanite edilmelidir.
EAG-12	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel bileşenlere güvensiz ağlar ya da yarı güvenli ağlar (DMZ: Demilitarized zone) üzerinden olan erişim trafiği bir saldırı tespit katmanından geçirilmelidir. Bunu sağlamak adına mevcut güvenlik bileşenlerinde IDS imzaları devreye alınabileceği gibi alternatif olarak açık kaynak kodlu teknolojiler de kullanılabilir.
EAG-13	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlarda trafik aynalanması (mirroring) yöntemi ile saldırı tespiti gerçekleştirilebilir. Bu izleme minimum olarak kontrol merkezi ve acil durum kontrol merkezi ağları ile kontrol merkezlerinin uç sahalarla WAN haberleşmelerini de kapsamalıdır.
EAG-14	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Ek kontrol	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) RMS-A istasyonlarında trafik aynalanması (mirroring) yöntemi ile saldırı tespiti gerçekleştirilebilir.
EAG-15	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Kesme	Ek kontrol	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağları izole etmek/ayırıştırmak için konumlandırılan güvenlik duvarı üzerinde (Referans_Topoloji_Doğal_Gaz_Dağıtım: EKS-GD-01) endüstriyel protokollere yönelik tehditleri de içeren IPS ve antivirüs vb. güvenlik önlemleri devreye alınmalıdır.
EAG-16	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemleri (EKS) içerisinde bulunan bileşenler görevlerine göre sanal ağlara (VLAN) ayrılmalı ve bu ağlar arasında geçiş kontrolleri uygulanmalıdır. Söz konusu katmanlı yapı acil durum/yedek kontrol merkezlerinde de gerçekleştirilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
EAG-17	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) mühendislik iş istasyonları endüstriyel ağlardan izole edilmelidir. Sadece iş ihtiyacı olduğu durumlarda kullanıma tahsis edilmelidir.
EAG-18	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlardan kurumsal ağlara doğru olan haberleşmeler bu haberleşmelere özel oluşturulmuş OT-DMZ ağları ya da izole sanal ağlar (VLAN) üzerinden sağlanmalıdır. Aynı şekilde kurumsal ağlardan endüstriyel ağlara doğru olan haberleşmeler de OT-DMZ ağları ya da izole sanal ağlar (VLAN) üzerinden sağlanmalıdır.
EAG-19	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) sanal ağların (VLAN) devreye alınmasını takiben ağ ve güvenlik cihazlarının yönetim arayüzleri de (management interface) ayrı bir sanal ağ üzerinde konumlandırılmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
EAG-20	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemleri (EKS) altyapısında her bir uç istasyon ağ seviyesinde farklı bir alt ağ olarak oluşturulmalıdır.
EAG-21	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 3	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemleri (EKS) altyapısında her bir uç istasyon için endüstriyel protokol trafiği ve diğer trafikler (kamera, fiziksel güvenlik, sayaç vb.) farklı sanal ağlar (VLAN) olarak yapılandırılmalı ve bu sanal ağlar (VLAN) arası geçiş mevcut ağ/güvenlik cihazları üzerinden kontrollü olarak sağlanmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-22	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Ek kontrol	Endüstriyel ağlarla iletişim halinde olan tüm KBS bileşenleri ayrı bir sanal ağ (VLAN) içerisinde konumlandırılmalı ve OT-DMZ ağı üzerinden endüstriyel ağlar ile haberleşmelidir. (CRM, CBS, WorkForce Management, ERP, Güvenli Uzak Erişim vb.)
EAG-23	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Endüstriyel ağlar ve KBS ağları arasında haberleşmenin yönü endüstriyel ağdan kurumsal ağa olacak şekilde OT-DMZ üzerinden sağlanmalıdır. Kurumsal ağlardan endüstriyel ağlara doğru veri çekme operasyonlarının gerekli olması durumunda bu veri akışı ek kontroller ile gerçekleştirilmelidir.
EAG-24	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 1	Endüstriyel ağlar içerisinde yer alan sunucu ve uygulamalar doğrudan internet üzerinden erişilebilir durumda olmamalıdır.
EAG-25	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 1	Endüstriyel ağlarla iletişimi olan bileşenlerin doğrudan internete olan erişimleri kontrollü olarak sağlanmalıdır.
EAG-26	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Uzak Erişim	Seviye 1	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemi (EKS) bileşenlerine internet üzerinden gerçekleştirilecek tüm uzak erişimler öncelikli olarak KBS/kurumsal ağ üzerinde sonlandırılmalıdır. (VPN vb.) Bu uzak erişim yöntemleri üreticiler, çalışanlar ve alt yükleniciler için farklı yetkilendirme politikalarını destekleyebilmelidir. KBS ağı üzerinden endüstriyel ağlara yönelik uzak erişimler OT-DMZ ağı içerisinde konumlandırılmış güvenli bir atlama noktası/sunucusu/uygulaması üzerinden kontrollü olarak sağlanmalıdır. Uzakten erişimlere ilişkin tüm süreçler diğer mevcut teknik maddelere uyumlu olarak işletilmelidir. (Olay yönetimi ve süreklilik, kimlik ve erişim yönetimi vb.)
EAG-27	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Uzak Erişim	Ek kontrol	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerine (EKS) yapılacak uzak erişimler için bu işe özelleşmiş teknolojiler kullanılmalıdır. Bu teknolojilerde oturum kaydetme, oturum yönetimi, çift faktörlü doğrulama, güvenli dosya transferi gibi yeterlilikler aranmalıdır.
EAG-28	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 1	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde tüm güvensiz servisler (açık metin protokoller, uzak erişim servisleri, güncelliğini yitirmiş protokoller) periyodik denetim ya da ağ trafiğinin analizi ile tespit edilmelidir.
EAG-29	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Güvenli Konfigürasyon	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde tespit edilen KBS tabanlı (TELNET, HTTP, TFTP, vb.) güvensiz servisler devre dışı bırakılmalıdır.
EAG-30	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Güvenli Konfigürasyon	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde tespit edilen gereksiz veya kullanılmayan servisler devre dışı bırakılmalıdır.
EAG-31	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde mevcut varlıkların servisleri sürekli olarak izlenmelidir.
EAG-32	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 1	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) güvenli ve güvensiz ağlar arasında mevcut olan koruma mekanizmalarının bypass edilmesine olanak tanıyabilecek tüm dual-homed arayüzler (interface) devre dışı bırakılmalıdır. İkinci bir arayüz kullanılması zorunlu kılan bir durum mevcut ise söz konusu arayüzün bağlantısı güvenlik duvarı (Referans_Topoloji_Doğal_Gaz_Dağıtım: EKS-GD-01) üzerinden kontrollü olarak sağlanmalıdır.
EAG-33	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) Seviye-2 ile Seviye-1 (Purdue modeline göre) ağlar arasında mevcut olan koruma mekanizmalarının bypass edilmesine olanak tanıyabilecek tüm dual-homed arayüzler interface'ler devre dışı bırakılmalıdır. İkinci bir arayüz kullanılması zorunlu kılan bir durum mevcut ise söz konusu arayüzün bağlantısı güvenlik duvarı üzerinden kontrollü olarak sağlanmalıdır. (Bu kontrol, altıyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan alt yapılarla aranacaktır.)

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-34	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağ içerisinde bulunan ağ cihazları "Olay Yönetimi ve Süreklilik" başlığının ilgili maddelerini karşılamalıdır.
EAG-35	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmantasyonu	Seviye 2	Doğal gaz dağıtım şebekeleri endüstriyel kontrol sistemlerinde (EKS) ana kontrol merkezi ve uç sahalarla olan haberleşmeler şifreli olarak gerçekleştirilmelidir. Şifreli iletilmeyen trafikler izole ağlar üzerinden taşınmalıdır.
EAG-36	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, endüstriyel protokol trafiği bir APN bloğunda izole edilmelidir. Bu izolasyon işlemi aşağıda belirtilen maddeleri de kapsamalıdır; * EKS trafiklerinin taşındığı APN bloku/bloklarında sadece ilgili tesise ait trafiklerin olması * EKS trafiklerinin taşındığı APN bloku/bloklarında sadece EKS trafiklerinin olması (Sayaç, mobil ekip cihazları vb. trafiğinin de bu ağlardan izolasyonu sağlanmalıdır.) * APN bloğundaki EKS trafikleri sadece bir tesise ait olmalıdır.
EAG-37	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, RMS istasyonları arası erişimler uygun bir teknoloji ile kontrol altına alınarak kısıtlanmalıdır.
EAG-38	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, Internet Servis Sağlayıcısı (ISP) bünyesinde bulunan APN uç noktaları bir güvenlik duvarı üzerinde sonlandırılmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-39	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, Internet Servis Sağlayıcısı (ISP) bünyesinde toplanan tüm trafiklerin, ISP güvenlik duvarı üzerinden kuruluşun güvenlik duvarına güvenli teknolojiler (IPsec VPN vb.) kullanılarak iletilmesi sağlanmalıdır.
EAG-40	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) erişim noktası adı (APN) teknolojisi kullanılması durumunda, APN ağlarına giriş kısıtlaması uygulanmalıdır. Bunu sağlamanın amacıyla kuruluş bünyesinde kimlik doğrulama mekanizmaları kurgulanmalı ve oluşturulacak yapı kuruluş tarafından yönetilmelidir. (Örneğin GSM numaralarının ağa erişimin kısıtlanabilmesi için kullanılabilmesi amacı ile RADIUS sunucular konumlandırılması. Söz konusu RADIUS sunucularının yönetimi kuruluştaki olmalı ve kuruluş ağında konumlandırılmalıdır.)
EAG-41	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-APN	Ek Kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN), (APN) teknolojisi kullanılması durumunda, APN trafiğinin karıştırıcı (Jammer) sistemleri ile baskılanması sebebiyle servis kesintileri oluşabileceği kuruluş tarafından değerlendirilmeli ve ilgili trafik akışının sürekliliğinin sağlanabilmesi için gerekli tedbirler alınmalıdır.
EAG-42	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda endüstriyel protokol trafiği RF ağında izole edilmelidir. Bu izolasyon işlemi kapsamında haberleşme telsizleri gibi bileşenler endüstriyel trafik dışında tutulmalıdır.
EAG-43	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda RMS istasyonları arası erişimler uygun bir teknoloji ile kontrol altına alınarak kısıtlanmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-44	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, RF ağında olan RMS istasyonlarına ait endüstriyel trafik kuruluşa ait güvenlik duvarı (Referans_Topoloji_Doğal_Gaz_Dağıtım: EKS-GD-01) üzerinde sonlandırılmaktadır.
EAG-45	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, RF ağında araya girme ve elektromanyetik yayılım (Tempest) saldırılarına karşı önlem alınmalıdır.
EAG-46	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, RF ağından gerçekleştirilecek endüstriyel haberleşme için trafiği şifreli olarak iletebilen teknolojiler kullanılmalıdır.
EAG-47	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, servis kesintisine neden olabilecek saldırılara karşı önlem alınmalıdır.
EAG-48	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-RF	Ek Kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında (WAN) Radyo Frekans (RF) teknolojilerinin kullanılması durumunda, RF altyapısı olay yönetimi ve süreklilik alanının (domain) ilgili maddelerine uyumlu olacak şekilde tasarlanmalıdır. Mimari tasarımda tekil hata noktası (single point of failure) bulunmamalıdır.
EAG-49	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-SD-WAN	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında, yazılım tanımlı geniş alan ağı (SD-WAN) teknolojilerinin kullanılması durumunda, endüstriyel protokol trafiği için özelleştirilmiş izole bir SD-WAN mimarisi oluşturulmalıdır.
EAG-50	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-SD-WAN	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında, yazılım tanımlı geniş alan ağı (SD-WAN) teknolojilerinin kullanılması durumunda, SD-WAN yapısı içerisinde gerçekleştirilen endüstriyel protokol haberleşmesi için trafiği şifreli olarak iletebilen teknolojiler kullanılmalıdır.
EAG-51	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-SD-WAN	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında, yazılım tanımlı geniş alan ağı (SD-WAN) teknolojilerinin kullanılması durumunda SD-WAN ağında olan RMS istasyonlarına ait endüstriyel trafik kuruluşa ait güvenlik duvarı (Referans_Topoloji_Doğal_Gaz_Dağıtım: EKS-GD-01) üzerinde sonlandırılmaktadır.
EAG-52	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-SD-WAN	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) geniş alan ağında, yazılım tanımlı geniş alan ağı (SD-WAN) teknolojilerinin kullanılması durumunda RMS istasyonları arası erişimler uygun bir teknoloji ile kontrol altına alınarak kısıtlanmalıdır.
EAG-53	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-MPLS	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) WAN trafiğinde MPLS teknolojilerinin kullanılması durumunda, MPLS omurgasında kuruluşa hizmet eden ağ cihazlarında güncelleme ve yama yönetimi gerçekleştirilmelidir. MPLS sağlayıcısı firma yaması bulunan acil ve kritik seviyeli güvenlik açıklıklarını giderdiğine dair yazılı kanıt sunabilmeli ve kanıtları saklayabilmelidir. [Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.]

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-54	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-MPLS	Seviye 2	Doğal gaz dağıtım şebekelerinde WAN trafiğinde MPLS teknolojilerinin kullanılması durumunda, MPLS omurgasında kuruluşa hizmet eden ağ cihazlarında güvenli yapılandırma prensipleri uygulanmalıdır. Ağ cihazlarındaki güvenlik yapılandırmaları belirli periyotlarla kuruluş ile paylaşılmalı ya da kuruluşa kalıcı "read-only" bir hesap tanımlanması sağlanmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
EAG-55	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-MPLS	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) WAN trafiğinde MPLS teknolojilerinin kullanılması durumunda, MPLS omurgasında kullanılan ağ cihazlarında basit ya da tahmin edilebilir kullanıcı adı ve parola bulundurulmamalıdır. Her bir ağ cihazında özel bir kullanıcı adı ve parola atanmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
EAG-56	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda WAN Güvenliği-MPLS	Seviye 3	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) WAN trafiğinde MPLS teknolojilerinin kullanılması durumunda, MPLS omurgasında iletilen trafiğin şifreli olarak taşınması sağlanmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
EAG-57	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sisteminde (EKS) endüstriyel ağların izolasyon ve segmentasyonunda yazılım tabanlı teknolojilere ek olarak donanım tabanlı teknolojiler de devreye alınmalıdır.

Endüstriyel İstemci ve Sunucu Güvenliği

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İSG-1	Endüstriyel İstemci ve Sunucu Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucular için endüstriyel üretici tarafından onaylanan ve operasyonel sürekliliği tehlikeye atmayacak uç nokta (endpoint) güvenlik önlemleri (kötü amaçlı yazılım koruma uygulamaları, uç nokta tehdit tespit sistemi, uç nokta güvenlik duvarı vb.) tanımlanmalı ve uygulanmalıdır.
İSG-2	Endüstriyel İstemci ve Sunucu Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren istemciler için endüstriyel üretici tarafından onaylanan ve operasyonel sürekliliği tehlikeye atmayacak uç nokta (endpoint) güvenlik önlemleri (kötü amaçlı yazılım koruma uygulamaları, uç nokta tehdit tespit sistemi, uç nokta güvenlik duvarı vb.) tanımlanmalı ve uygulanmalıdır.
İSG-3	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Medya Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren istemcilerde harici medya kullanımları devre dışı bırakılmalıdır.
İSG-4	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Medya Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucularda harici medya kullanımları devre dışı bırakılmış olmalıdır.
İSG-5	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Medya Güvenliği	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde yeni nesil USB tabanlı saldırılara karşı önlem alınmalıdır. (Rubber Ducky vb.)
İSG-6	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Olay Tespiti ve Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde "Olay Yönetimi ve Süreklilik" başlığı altındaki maddelere uygun olarak loglar tutulmalı ve yönetilmelidir.
İSG-7	Endüstriyel İstemci ve Sunucu Güvenliği	Mobil Cihaz Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren taşınabilir mühendislik iş istasyonları (dizüstü vb.) ilgili kuruluş envanterine kayıtlı olmalıdır. Mühendislik operasyonlarında alt yüklenicilere ait güvensiz iş istasyonları endüstriyel ağa dahil edilmemeli ve EKS bileşenlerine bağlanmamalıdır. Kuruluşa ait taşınabilir mühendislik iş istasyonlarının güvenlik seviyesi kuruluş içi ve kuruluş dışında aynı olmalıdır.
İSG-8	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucu Operasyon Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren mühendislik iş istasyonları günlük operasyonel işlerde kullanılmamalıdır. (E-posta vb.)
İSG-9	Endüstriyel İstemci ve Sunucu Güvenliği	Veri Koruma	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde disk şifreleme yöntemleri uygulanmalıdır.
İSG-10	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde güvenli BIOS yapılandırılmaları devreye alınmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İSG-11	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde sadece yetkili kullanıcıların uygulama kurmasına izin verilmelidir.
İSG-12	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde sadece güvenlik onayından geçmiş uygulamaların yüklenmesine ve kullanılmasına izin verilmelidir.
İSG-13	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler için kuruluşa özel güvenli bir kurulum imaj dosyası oluşturulmalı, periyodik olarak kontrol edilmeli ve güncellenmelidir.
İSG-14	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde internet üzerinden güvensiz uzak erişime imkan verecek yazılım ve servisler bulundurulmamalıdır.
İSG-15	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunuculara bulundukları ağ içerisinden uzak erişim (VNC, SSH, RDP vb.) yapılması durumunda ek güvenlik kontrolleri uygulanmalıdır. (sanal ağ ayırıştırma, güvenli atlama noktası, uç nokta güvenlik duvarı ile erişim kısıtlamaları vb.)
İSG-16	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucu Operasyon Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan tüm uygulamalar lisanslı olmalıdır.
İSG-17	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Olay Tespiti ve Yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler merkezi bir zamanlama sunucusundan senkronize edilmelidir. Bu senkronizasyon işlemi ağ seviyesinde güvenlik kontrolleri (port bazlı erişim kısıtlamaları vb.) ile sağlanmalıdır.
İSG-18	Endüstriyel İstemci ve Sunucu Güvenliği	GPS Güvenliği	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler için kullanılan merkezi zamanlama sunucusunun GPS tabanlı olması halinde, GPS temelli saldırılara karşı koruma önlemleri alınmalıdır.
İSG-19	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan kötü amaçlı yazılım koruma uygulamaları endüstriyel üreticinin de onayladığı aralıklarla güncellenmelidir. Bu aralıklar 4 aydan daha uzun süreli olarak tanımlanmamalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
İSG-20	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan kötü amaçlı yazılım koruma uygulamaları yüksek yetkili kullanıcılar tarafından da dahil olmak üzere devre dışı bırakılamamalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
ISG-21	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güncelleme/Yama Yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerin işletim sistemleri endüstriyel üreticinin de onayladığı tanımlı aralıklarla güncellenmelidir. Bu aralıklar 4 aydan daha uzun süreli olarak tanımlanmamalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
İSG-22	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güncelleme/Yama Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan uygulamalar, üretici güncelleme ve yamalarının yayınlanmış olma ihtimaline karşı belirlenen aralıklarla kontrol edilmelidir. Güvenlik açısından önem arz eden güncellemeler endüstriyel üretici gözetiminde gerçekleştirilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
ISG-23	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerin tüm gereksiz kablolu ve kablosuz ağ arayüzleri devre dışı bırakılmalıdır. Ek olarak gereksiz servis ve portlar devre dışı bırakılmalıdır.
İSG-24	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerin ağ servisleri yönetiminde "Endüstriyel Ağ Güvenliği" başlığının ilgili maddelerine uygun hareket edilmelidir.
İSG-25	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde IPv6 ağ arayüzleri devre dışı bırakılmalıdır.
İSG-26	Endüstriyel İstemci ve Sunucu Güvenliği	Veri Koruma	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde imha yönetimi kuruluşun belirlediği politikalar doğrultusunda gerçekleştirilmelidir.
İSG-27	Endüstriyel İstemci ve Sunucu Güvenliği	Beyaz Liste Uygulamaları	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) içerisinde hizmet veren sunucu ve istemcilerde beyaz liste (Whitelisting) uygulamaları devreye alınmalıdır.
İSG-28	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda endüstriyel etki alanı ile KBS etki alanı birbirinden tamamiyle izole edilmelidir. (Bu amaçla trust, parent-child, farklı OU gibi yöntemler kullanılmamalıdır.)

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
ISG-29	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, endüstriyel etki alanının kapsamı sadece ilgili endüstriyel kontrol sistemini işleten kuruluş ile sınırlı olmalıdır. Üreticinin şablon olarak hazırladığı ya da farklı ortamlarda kullandığı etki alanı yapıları kuruluş endüstriyel kontrol sistemleri içerisinde kullanılmamalıdır.
ISG-30	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, ortak erişime açık klasörler içerisindeki dosyalarda yüksek yetkili kullanıcı bilgileri gömülü olarak saklanmamalıdır.
ISG-31	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisine (domain controller) sadece gerekli protokoller üzerinden erişimi mümkün kılacak kısıtlamalar uygulanmalıdır.
ISG-32	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisi (domain controller) üzerinde gerekli olmayan tüm ağ servisleri devre dışı bırakılmalıdır.
ISG-33	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisi (domain controller) yedekli mimaride tasarlanmalıdır.
ISG-34	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı bileşenlerinde üretici tarafından sıkça kullanılan kullanıcı adı ve parolalar bulundurulmamalıdır.
ISG-35	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisi (domain controller) sunucusunun tekil görev için kullanılması sağlanmalıdır. DHCP, DNS ve dosya paylaşım vb. servisler için farklı sunucular konumlandırılmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
ISG-36	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanına ait tüm bileşenler yama yönetim politikalarına uygun olarak yönetilmelidir.
ISG-37	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan tüm bileşenler "Tehdit ve Zafiyet Yönetim" başlığına uygun olarak güvenlik denetimi ve sızma testlerine tabi tutulmalıdır. (İstemci, sunucu, konfigürasyon, GPO vb.)

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İSG-38	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan sunucular için güvenli konfigürasyon kontrol listesi oluşturmalıdır.
İSG-39	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan sunucular oluşturulan güvenli konfigürasyon kontrol listesine göre periyodik gözden geçirilmelidir. Konfigürasyon değişikliklerini anlık olarak loglayacak yapılandırmalar devreye alınmalıdır.
İSG-40	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan Grup İlkeleri (GPO) güvenli bir şekilde uygulanmalıdır.
İSG-41	Endüstriyel İstemci ve Sunucu Güvenliği	HMI Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS), operatörler günlük operasyonları gerçekleştirdikleri arayüzler (HMI) üzerinde operasyonu gerçekleştirmek için gerekli olan en düşük yetki ile çalışmalıdır. Arayüzler (HMI) yetki aşımına izin vermeyecek şekilde yapılandırılmalıdır.
İSG-42	Endüstriyel İstemci ve Sunucu Güvenliği	HMI Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan arayüzler (HMI) devre dışı bırakma (bypass) ve kaçış saldırılarını engelleyebilecek şekilde yapılandırılmalıdır. Bu yapılandırmalar "Tehdit ve Zafiyet Yönetim" başlığına uygun şekilde periyodik olarak test edilmelidir.



Yatay ve Dikey Okuma ve Yazma Becerileri

Endüstriyel Tehdit ve Zafiyet Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TZY-1	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi için gerekli bilgi kaynakları belirlenmelidir.
TZY-2	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi amacı ile belirlenen kaynaklardan siber güvenlik tehdit bilgisi toplanmalı ve işlenmelidir.
TZY-3	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinin (EKS) güvenliği ve sürekliliği için risk teşkil edebilecek tehditler belirlenmeli ve bu tehditlerin yönetimi için iyileştirme aksiyonları belirtilmelidir.
TZY-4	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin profilendirilmesi için tehdit hakkında en az aşağıdaki bilgiler edinilmelidir. -Tehdidin hedefi -Kabiliyetleri -Tehdit hedefinin endüstriyel operasyondaki önemi
TZY-5	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi için belirlenen bilgi kaynakları önceliklendirilmeli ve sürekli olarak takip edilmelidir.
TZY-6	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik risk teşkil edebileceği değerlendirilen tehditler analiz edilmeli, sınıflandırılmalı ve önceliklendirilmelidir.
TZY-7	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik zafiyetlerin yönetilebilmesi için gerekli bilgi kaynakları belirlenmelidir.
TZY-8	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi amacı ile belirlenen kaynaklardan siber güvenlik zafiyet bilgisi toplanmalı ve işlenmelidir.
TZY-9	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinin (EKS) güvenliği ve sürekliliği için risk teşkil edebilecek zafiyetler belirlenmeli ve bu zafiyetlerin yönetimi için iyileştirme aksiyonları belirtilmelidir.
TZY-10	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	"Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddeleri doğrultusunda doğal gaz dağıtım şebekesi endüstriyel kontrol sistemleri (EKS) için güvenlik analizleri ve testleri gerçekleştirilmelidir.
TZY-11	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik risk teşkil edebileceği değerlendirilen zafiyetler analiz edilmeli, sınıflandırılmalı ve önceliklendirilmelidir.
TZY-12	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) yönelik risk teşkil edebileceği değerlendirilen zafiyetler önceliklerine göre yönetilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TZY-13	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine ait siber güvenlik yamaları "İstemci ve Sunucu Güvenliği" başlığına uygun olacak şekilde yamaların operasyonlara olan etkisi de gözden geçirilerek uygulanmalıdır.
TZY-14	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit ve zafiyet yönetim yaklaşımı dokümanite edilmiş olmalıdır.
TZY-15	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit ve zafiyet yönetim sürecinde ihtiyaç duyulabilecek tüm üçüncü taraflar belirlenmeli ve bu süreç dahil edilmelidir.
TZY-16	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit ve zafiyet yönetimi için gerekli standart, kılavuz ve yasal mevzuatlar belirlenmelidir.
TZY-17	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit istihbaratı, bir bütün olarak izlenmelidir.
TZY-18	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Tehdit yönetimi kapsamında arz güvenliğini riske atabilecek, doğal afetler, terör vb. gibi bilgiler de bütüncül bir yaklaşım sergileyecek şekilde değerlendirilmelidir.
TZY-19	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin yerel ve küresel tehdit istihbarat kaynakları bir bütün olarak yönetilmelidir. (Bu kaynaklar üretici sayfaları, küresel bilgilendirme sayfaları gibi kaynaklar olabilir.)
TZY-20	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	KBS ve EKS'ye ilişkin tehdit istihbarat kaynakları bir bütün olarak yönetilmelidir.
TZY-21	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit tespiti	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tehditler (saldırgan aktiviteleri) gerçek zamanlı olarak izlenebilmelidir. Bu izleme, istemci ve sunucu üzerinden bilgi toplanarak ve ağ trafiği takip edilerek gerçekleştirilebilir.
TZY-22	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit tespiti	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin bir saldırı tespiti yapılması durumunda, söz konusu saldırılar sınıflandırılmalıdır. (operasyonel tehditler, siber güvenlik tehditleri, fiziksel, ağ tehditleri vb.)
TZY-23	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizi "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddelerine göre aktif veya pasif yöntemlerle (manuel ya da otomatize araçlarla) en az yılda bir kez gerçekleştirilebilir durumda olmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TZY-24	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizi "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddelerine uygun yöntemlerle gerçekleştirilmeli ve en az aşağıda belirtilen bileşenleri kapsamalıdır. -EKS sunucu ve istemci işletim sistemleri -Kontrol katmanı bileşenleri (PLC/RTU, Giriş/Çıkış (I/O) Modülleri vb.) -Sayaçlar, ölçüm cihazları (Akış bilgisayarı (Flow computer), gaz kromatograf vb.) -Dönüştürücüler (Protokol ve seri/ethernet) -Ağ cihazları -Endüstriyel uygulama yazılımları -Siber güvenlik teknolojileri
TZY-25	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizleri farklı kaynakları girdi olarak kullanılmalıdır. (Sızma testleri, güvenlik testleri, analizleri, zafiyet taramaları vb.)
TZY-26	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizleri için otomatize bir araç kullanılacaksa seçilen aracın teknolojisi, protokol desteği ilgili altyapıya uygun olmalıdır.
TZY-27	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin siber güvenlik zafiyetleri bir yaşam döngüsü şeklinde yönetilmelidir. (Tespit, iyileştirme, doğrulama, kapatma, kabul vb.)
TZY-28	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin tespit edilen her bir siber güvenlik zafiyeti için ilgili birim ve personellere sorumluluk ataması gerçekleştirilmelidir.
TZY-29	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin risk analizi, sızma testi, güvenlik analizi çıktılarının eğilimi sürekli olarak izlenmelidir.
TZY-30	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri ana kontrol ve acil/yedek kontrol merkezleri bileşenlerini içermelidir.
TZY-31	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri uç saha bileşenlerini (ağ, haberleşme, çevirici, protokol vb.) içermelidir.
TZY-32	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri endüstriyel kontrol sistemlerinin bulunduğu tüm fiziksel lokasyonları içermelidir.
TZY-33	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri, EKS varlıklarının sürüm bilgisinden zafiyet tespitine imkan vermemelidir. Bu amaçla manuel veya otomatize araçlar kullanılabilir.

Endüstriyel Siber Güvenlik Risk Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
ERY-1	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi Stratejisi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemleri (EKS) için dokümanite edilmiş bir endüstriyel siber güvenlik risk yönetimi stratejisi olmalıdır. Risk yönetim metodolojisi endüstriyel altyapılar için özelleştirilmiş olmalıdır.
ERY-2	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi Stratejisi	Seviye 1	Endüstriyel siber güvenlik risk yönetim stratejisi, endüstriyel operasyonlara etkinin dikkate alınması da dahil olmak üzere, risk önceliklendirmesi için bir yaklaşıma sahip olmalıdır. Bu strateji endüstriyel operasyonlar dikkate alınarak hazırlanmalıdır.
ERY-3	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Belirlenen riskler, risk azaltma, risk kabulü, riskten kaçınma veya riskin transferi işlemleri çerçevesinde yönetilmelidir. Bu süreçle ilişkin gerekli dokümantasyon oluşturulmalı ve bu dokümanlar saklanmalıdır.
ERY-4	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme dokümanı asgari olarak, "risk numarası, risk kategorisi, riskin oluşması için koşullar, zafiyet, tehdit, risk, riski taşıyan bileşen/bileşen grubu, riskten etkilenen bileşen/bileşen grubu, riskin etki değeri, riskin gerçekleşme olasılığı" başlıklarını içermelidir.
ERY-5	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme dokümanı, endüstriyel operasyonlarda veya bilgi teknolojileri sistemlerinde (yeni tehdit ve zafiyetler belirlendiği durumlar dahil olmak üzere) önemli değişiklikler olduğunda veya sistemin güvenlik durumunu etkileyebilecek diğer koşullar oluştuğunda güncellenmelidir.
ERY-6	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Riskin gerçekleşme olasılığı "normal, yüksek ya da çok yüksek" dereceleri kullanılarak değerlendirilmelidir.
ERY-7	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk işleme planları, risklerin azaltılmasına ilişkin uygulanması veya alınması gereken önlem ve kontrolleri içermelidir.
ERY-8	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Tespit edilen riskler analiz edilerek, risk yönetimi stratejisine uygun olarak işleme faaliyetleri önceliklendirilmelidir.
ERY-9	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Tespit edilen riskler, risk yönetimi stratejisine uygun olarak izlenmelidir.
ERY-10	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk analizi sonuçları, ağ (KBS ve/veya EKS) mimarisine ait risk değerlendirme sonuçlarını da içermelidir. Risk analizlerinde mimari hatalar ve zafiyetler de girdi olarak kullanılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
ERY-11	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Endüstriyel siber güvenlik risk yönetimi faaliyetleri için oluşturulan dokümanlar düzenli olarak takip edilmelidir. (Strateji dokümanları, politika ve prosedürler, formlar vb.)
ERY-12	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Risk yönetimi faaliyetleri için paydaşlar belirlenmeli ve risk yönetimi sürecine dahil edilmelidir.
ERY-13	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Risk yönetimi faaliyetlerini desteklemek için yeterli kaynak (insan kaynağı, finansman vb.) sağlanmalıdır.
ERY-14	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Risk yönetimi faaliyetlerinin içeriğinde yer alacak standartlar ve/veya kılavuzlar belirlenmelidir. (NIST 800-53, NIST800-82, ISA 62443, ISO 27019, C2M2 vb.)
ERY-15	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi nitel ve nicel olarak ölçüme olanak tanımalıdır.
ERY-16	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi risk kabul kriterlerini ve risk kabul değerini tanımlamalıdır.
ERY-17	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi risk sahibini tanımlamalıdır. Riskler ilgili risk sahibine atanmalıdır.
ERY-18	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Endüstriyel siber güvenlik risk belirleme sürecinde endüstriyel operasyonlara etkiye göre derecelendirme yapılmalıdır.
ERY-19	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi tekrar edilebilir, karşılaştırılabilir ve tutarlı sonuçlar üretebilir olmalıdır.
ERY-20	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri, ana kontrol/yedek kontrol odalarını ve bileşenlerini içermelidir.
ERY-21	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri, RMS istasyonlarını ve bileşenlerini içermelidir.
ERY-22	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri, endüstriyel sistemlerin olduğu tüm fiziksel lokasyonlar için fiziksel güvenlik risklerini içermelidir.
ERY-23	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri endüstriyel iletişim protokollerini içermelidir.
ERY-24	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk Yönetim faaliyetleri uç sahalarla haberleşme ve ağ güvenlik risklerini içermelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
ERY-25	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetimi faaliyetlerinde, "Enerji Sektöründe EKS Güvenlik Kontrolleri" başlıkları en az aşağıdaki bileşenler için uygulanmalıdır. - İş istasyonu riskleri - İnsan Makine arayüzü (HMI) iş istasyonu riskleri - Sunucu tabanlı riskler (SCADA, OPC, Historian vb.) - Endüstriyel yazılım uygulamaları riskleri (SCADA yazılımı) - Siber güvenlik uygulama ve çözümleri - Mühendislik iş istasyonu riskleri - Endüstriyel ağ ve ekipmanları güvenlik riskleri - Endüstriyel altyapı kontrol katmanı ekipmanları güvenlik riskleri (PLC, RTU, Flow Computer, Gaz Kromotograf) - Sayaçlar - KBS ağları entegrasyon riskleri (CRM, CBS, ERP, Çağrı Merkezi vb.)
ERY-26	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetimi üçüncü taraf bilgi güvenliği risklerini içermelidir.
ERY-27	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci ISO 27001 BGYS ve CB-DDO formlarına uygun olarak işletilmelidir.
ERY-28	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci kapsamında artık risk yönetim ilkeleri tanımlanmalıdır. Risk işleme sonrası kalan artık riskler; risk sahibi ve üst yönetim tarafından onaylanmalıdır.
ERY-29	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci, operasyonel süreklilik risklerini içermelidir.
ERY-30	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Siber güvenlik riskleri ethernet ve seri iletişim tabanlı saldırı vektörleri dikkate alınarak belirlenmelidir.
ERY-31	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim sürecinde; sızma testleri, güvenlik analizleri, iç denetim çıktıları da girdi olarak kullanılmalıdır.
ERY-32	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme sürecinde her bir endüstriyel siber güvenlik riskinin, çevre etkisi, finansal etkisi ve insana etkisi (abone sayısı) belirlenmelidir.
ERY-33	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme sürecinde her bir endüstriyel siber güvenlik riskinin diğer kritik altyapılara olan etkisi de değerlendirilmelidir. (enerji üretimi, sanayi üretimi, vb.)
ERY-34	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci insan temelli riskleri de içermelidir. (Personel, operatör, mühendis, KBS çalışanı, siber güvenlik çalışanı, üretici ve alt yüklenici çalışanları)

Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
VKY-1	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları için envanter oluşturulmalıdır. Envanter Yönetimi amaca özel olarak oluşturulmalıdır.
VKY-2	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	Bu envanter, siber saldırı hedefi olabilecek her türlü bileşeni de içermelidir. (Yazıcı, IoT Cihazlar, kartlı geçiş sistemi vb.)
VKY-3	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları envanteri, siber güvenlik süreçlerini destekleyen öznitelikler içermelidir. (Konum, varlık önceliği, işletim sistemi ve donanım yazılımı sürümleri, varlık sahibi, varlık emanetçisi vb.) Envanterdeki KBS ve EKS varlıklarına, bilgi varlıklarının fonksiyon ve görev önemine göre tanımlanmış CB DDO kriterlerini de göz önünde bulundurarak öncelik verilmelidir.
VKY-4	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları için oluşturulan envanter periyodik olarak ve sistem değişikliği durumunda güncellenmelidir.
VKY-5	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 2	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları envanteri, varlık kullanım ömrü (end-of-life) ve üretici desteğinin sonlanması (end-of-support) gibi bilgileri içermelidir.
VKY-6	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	Envanterde kullanım ömrü sonuna gelmiş veya değişimi yapılacak olan KBS ve EKS varlıklarına ait veriler güvenli bir şekilde silinmelidir.
VKY-7	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Bilgi Varlığı Envanteri Yönetimi	Seviye 2	Doğal gaz dağıtım prosesinin devamlılığı için önemli olan bilgi varlıklarının envanteri oluşturulmalıdır. (Bu bilgi varlıkları, SCADA analog komutlar, özel konfigürasyon parametreleri ve müşteri bilgileri olabilir) Envanter yönetimi endüstriyel prosese özel olmalıdır.
VKY-8	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 1	Temel konfigürasyon mimarisi oluşturulmalıdır. Konfigürasyonlarda siber güvenlik açısından gerekli olan minimum isterler dokümanite edilmelidir. (IP adresleri, parolalar, servis/port, kritik set değerleri vb.)
VKY-9	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 2	Temel konfigürasyon mimarisi, varlıklara konfigürasyon dağıtımı ve geri yükleme süreçlerinde kullanılmalıdır.
VKY-10	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 2	Yeni gerçekleştirilen varlık konfigürasyonlarının, temel konfigürasyon mimarisine göre tutarlılıkları izlenmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
VKY-11	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 1	Temel konfigürasyon mimarisi, periyodik olarak, sistem değişiklikleri ve siber güvenlik mimarisindeki değişikliklere göre gözden geçirilmeli ve güncellenmelidir.
VKY-12	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Değişikliklerinin Yönetimi	Seviye 1	Varlıklarda yapılacak değişiklikler, uygulanmadan önce, kurum tarafından tanımlanmış ve dokümente edilmiş olan sistem etkisi ve siber güvenlik isterlerine göre değerlendirilmeli, test edilmeli ve onaylanmalıdır. Bu testler siber güvenlik gereksinimlerini karşılamalıdır. Değişikliklere ilişkin kayıtlar tutulmalıdır.
VKY-13	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Değişikliklerinin Yönetimi	Seviye 1	Değişim yönetimi takibi, varlıkların tüm yaşam döngüsünü ele almalıdır. (Satın alma, dağıtım, operasyon, kullanımdan kaldırılması vb.)
VKY-14	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Değişikliklerinin Yönetimi	Seviye 1	Değişiklik kayıtları, varlıkların siber güvenlik gereksinimlerini etkileyen değişikliklerle ilgili bilgileri de içermelidir.
VKY-15	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Varlık yönetim sürecinde dokümente edilmiş prosedürler oluşturulmalıdır. İlgili prosedürler takip edilmeli ve sürdürülmelidir. Varlık yönetim sürecinde gerekli üst yönetim desteği sağlanmalıdır. Süreçten sorumlu personeller atanmalı ve gerekli yetkilendirilmeler yapılmalıdır. Varlık yönetim sürecinin etkinliği değerlendirilmeli ve izlenmelidir.

Endüstriyel Kimlik ve Erişim Yönetimi

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
KEY-1	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan operatör iş istasyonlarında, sunucularda, mühendislik iş istasyonlarında, uygulamalarda ve ağ cihazlarında tahmin edilebilir ya da basit kullanıcı adı/parola kullanılmamalıdır. Sistem tarafından karmaşık parola atamaları zorlanmalıdır.
KEY-2	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan operatör iş istasyonlarında, sunucularda, mühendislik iş istasyonlarında, uygulamalarda ve ağ cihazlarında alt yükleniciler tarafından farklı tesislerde aynı kullanıcı ve parola kullanılmamalıdır.
KEY-3	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan bileşenlerde operatör yetkisi ve mühendislik yetkisi ayrıştırılmalıdır.
KEY-4	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Ek Kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) uygulamalarında (SCADA) operatörlerin yaptıkları işlemlere göre yetki ayrıştırması yapılmalıdır.
KEY-5	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) uygulamalarına (SCADA) ait kullanıcı ve yetkilendirme dosyaları, kullanıcıların erişebildiği alanlarda saklanmamalıdır. Bu tür dosyalara erişimler kısıtlanmalıdır.
KEY-6	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Ek Kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sisteminde (EKS) işletim sistemi kullanıcılarıyla endüstriyel uygulama (SCADA) kullanıcıları birbirinden ayrıştırılmalıdır.
KEY-7	Endüstriyel Kimlik ve Erişim Yönetimi	Hesap Yönetimi	Ek Kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) operatör kullanıcılarına ait hesaplar tekil kullanıcı esasına göre oluşturulmalıdır.
KEY-8	Endüstriyel Kimlik ve Erişim Yönetimi	Hesap Yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine ait kullanıcı adı ve parolalar ilgili sistemden farklı bir dijital ortamda ya da fiziksel olarak saklanmamalıdır. (Dosya sunucusu, excel dosyaları, kağıt ve panolarda saklama vb.)
KEY-9	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sisteminde (EKS) gerçekleştirilecek kontrol işlemleri (yüksek yetkili manevra vb.) için ikinci bir kimlik doğrulama mekanizması kurgulanmalı ya da söz konusu işlemler için "izleme" ve "kontrol" yetkileri ayrıştırılmalıdır.
KEY-10	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) uygulamalarında (SCADA) mevcut kullanıcıdan farklı bir kullanıcı ya da yetkiye geçiş yapılırken parola doğrulaması yapılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
KEY-11	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) uygulamalarına (SCADA) ait parola bilgileri tersine mühendislik ile elde edilemeyecek şekilde oluşturulmalıdır.
KEY-12	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim için kullanılacak kullanıcı adı ve parolalar, endüstriyel bileşenlere ait kullanıcı adı ve parolalardan farklı olmalıdır.
KEY-13	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	KBS altyapılarında kullanılan ve doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine entegrasyonu olan sistem ve uygulamalara ait kullanıcı adı ve parolalar, endüstriyel bileşenler üzerinde tanımlı kullanıcı adı ve parolalardan farklı olmalıdır.
KEY-14	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda iki faktörlü kimlik doğrulama mekanizmaları devreye alınmalıdır.
KEY-15	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda uzak erişim sağlayan her bir kullanıcıya özel kullanıcı adı ve parola bilgisi atanmalıdır.
KEY-16	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim için kullanılacak hesaplar geçici süre ile oluşturulmalıdır.
KEY-17	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda erişime ilişkin tüm kayıtlar saklanmalıdır. (Erişim talebi, erişim onayı, erişim sırasında oluşan sistem kayıtları vb.)
KEY-18	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim için bir atlama noktası (jump box) kullanılıyorsa ilgili bileşen üzerinde bulunan hesapların ele geçirilmesini önlemek amacıyla gerekli sıkılaştırmalar devreye alınmalıdır.
KEY-19	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda, uzak erişimin sadece izin verilen bileşen ve sisteme yapılmasını garanti altına alacak ağ ve sistem tabanlı erişim kısıtlamaları uygulanmalıdır.

Endüstriyel Olay Yönetimi ve Süreklilik				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-1	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale politika ve prosedürleri, doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerini (EKS) kapsayacak şekilde hazırlanmalıdır.
OYS-2	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Kurumsal SOME rehberinde adreslendiği şekilde kurum içi rol ve sorumluluklara uygun olarak olay müdahale eğitimleri alınmalıdır.
OYS-3	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale eğitimleri siber güvenlik kaynaklı olarak oluşabilecek kriz yönetimini de içermelidir.
OYS-4	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale eğitimleri doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) siber güvenlik kaynaklı olarak oluşabilecek "görünürlük kaybı" ve "kontrol kaybı" etkilerine sahip senaryoları içermelidir.
OYS-5	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Kuruluş, olay müdahale testleri kapsamında, kendi yetkinliklerini belirli periyotlarla simülasyonlar aracılığı ile test etmelidir.
OYS-6	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale testleri, iş sürekliliği, acil durum yönetimi gibi süreç ve planlarla koordine olarak gerçekleştirilmelidir.
OYS-7	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale testleri kapsamında performans ölçümleri gerçekleştirilmelidir. (Ekip performansı, sistem yeterlilikleri, testlerin uygunluğu, birimler arası koordinasyon yeteneği vb.)
OYS-8	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale için gerekli yöntemler tanımlanmalı ve uygulanmalıdır. (Log toplama, ağ trafiği toplama, adli bilişim verisi toplama vb.)
OYS-9	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Ek kontrol	Olay müdahale kapsamında olaylara otomatik cevap verme süreçleri tanımlanmalıdır. (Route ekleme çıkarma, kural ekleme çıkarma vb.)
OYS-10	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale kapsamında, endüstriyel operasyonların sürekliliğine ilişkin senaryolar tanımlanmalıdır. (Manuel operasyona geçiş, yedek kontrol merkezine geçiş vb.)
OYS-11	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale yaklaşımı iç tehditlerin (çalışanlar, ağa erişim yetkisi olan alt yükleniciler ve üreticiler vb.) tespiti içerecek şekilde tasarlanmalıdır.
OYS-12	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale kapsamında, kurum içi birimlerin koordinasyonu tanımlanmalıdır. (İK, İşletme Birimleri, Hukuk vb.) Her bir olay için bilgi verilen, raporlanan, sorumlu kişi/birim şeklinde sınıflandırmalar yapılmalıdır.
OYS-13	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale ve sonrasında, kurum dışı otoritelerle iletişim ve koordinasyon gereklilikleri tanımlanmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-14	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale ve sonrasında, gerek duyulması halinde kuruluşa hizmet veren alt yüklenici ve üreticilerle gerçekleştirilecek koordinasyon süreci tanımlanmalıdır.
OYS-15	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale ekibi, Kurumsal SOME yönergeleri kapsamında oluşturulmalıdır.
OYS-16	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Tüm olay müdahale süreçleri Kurumsal SOME Rehberine uyumlu olmalıdır.
OYS-17	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale süreçleri, zararlı yazılım analizi ve adli bilişim analizini kapsamalıdır.
OYS-18	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale kapsamında, kurum anormal durum tespit yeteneklerine sahip olmalıdır. Kurumlar bunu sağlamak için istemci/sunucu, uygulama veya ağ tabanlı bir çözüm kullanabilir.
OYS-19	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale süreçleri, medya ve müşteri/abone iletişimlerini içermelidir.
OYS-20	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay yönetimi süreci, doğal gaz dağıtım operasyonlarına özel endüstriyel proses, varlık ve ekipmanlara uyumlu şekilde tanımlanmalıdır.
OYS-21	Endüstriyel Olay Yönetimi ve Süreklilik	Olay İzleme	Seviye 2	Olay izleme süreçleri endüstriyel kontrol sistemleri (EKS) için de devreye alınmalıdır.
OYS-22	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Raporlama	Seviye 1	Olay raporlama süreçleri Kurumsal SOME rehberine uyumlu olmalıdır.
OYS-23	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Raporlama	Seviye 1	Olay raporlama süreçleri, olayın yaşanmasına neden olan zafiyetlerin bilgisini içermelidir.



No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-24	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale Planı	Seviye 1	Kurum kendine özgü olay müdahale planlarını geliştirmelidir. Bu planlar en az aşağıdaki başlıkları içermelidir. - Olay müdahale organizasyonu (Roller ve görevler) - Olay tanımı (Olay sınıflandırma) - Raporlama (Olay bildirimi, analizi) - Kaynakların sağlanması - Bilgi paylaşımı (Kurum ve kurum dışı iletişim esasları) - Doküman yönetimi (Doküman güncelleme ve dağıtımı) - Kök neden analizi (Olayların kök neden analiz yöntemi ve raporlaması. Üçüncü taraflarda meydana gelebilecek olayların kök neden analizi hususuna sözleşmelerde yer verilmelidir.) - Olaylardan alınan dersler (lessons learned) ve olayların tekrarlanmasının engellenmesi - Olay müdahale simülasyonu ve başarı performans ölçümü
OYS-25	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Tespit Etme	Seviye 1	Tespit edilen olaylar belirli bir rol ya da kişiye atanmalıdır.
OYS-26	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Tespit Etme	Seviye 1	Olay tespiti için kriterler belirlenmelidir. (Olay tanımı, nereye bakılacağı vb.)
OYS-27	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesindeki kontrol merkezleri ve RMS-A istasyonlarındaki ağ ve güvenlik cihazları log üretme kapasitesine sahip olmalıdır.
OYS-28	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesindeki kontrol merkezlerinde bulunan ağ ve güvenlik cihazları log yönlendirme kapasitesine sahip olmalıdır.
OYS-29	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesindeki kontrol merkezlerinde bulunan ağ ve güvenlik cihazları log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.
OYS-30	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesindeki kontrol merkezlerinde bulunan ağ ve güvenlik cihazlarına ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-31	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan RMS-A istasyonları veya yerel kontrol sistemi (local SCADA) bulunan istasyonlarındaki ağ cihazları log yönlendirme kapasitesine sahip olmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
OYS-32	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan RMS-A istasyonları veya yerel kontrol sistemi (local SCADA) bulunan istasyonlarındaki ağ cihazları log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
OYS-33	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan RMS-A istasyonları veya yerel kontrol sistemi (local SCADA) bulunan istasyonlarındaki ağ cihazlarına ilişkin log'lar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
OYS-34	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan RMS istasyonlarındaki endüstriyel cihazlar (RTU, PLC, Flow Computer, Gaz Kromatograf) log tutma kapasitesine sahip olmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
OYS-35	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan RMS istasyonlarındaki endüstriyel cihazlar (RTU, PLC, Flow Computer, Gaz Kromatograf) log yönlendirme kapasitesine sahip olmalıdır.
OYS-36	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan RMS istasyonlarındaki endüstriyel cihazlar (RTU, PLC, Flow Computer, Gaz Kromatograf) log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-37	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan RMS istasyonlarındaki endüstriyel cihazlar (RTU, PLC, Flow Computer, Gaz Kromatograf) ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-38	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan yazılım ve uygulamalar (SCADA yazılımları, veri toplama yazılımları, sayaç yönetim uygulamaları vb.) log üretme kapasitesine sahip olmalıdır.
OYS-39	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan yazılım ve uygulamalar (SCADA yazılımları, veri toplama yazılımları, sayaç yönetim uygulamaları vb.) log yönlendirme kapasitesine sahip olmalıdır.
OYS-40	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan yazılım ve uygulamalar (SCADA yazılımları, veri toplama yazılımları, sayaç yönetim uygulamaları vb.) log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.
OYS-41	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemi (EKS) bünyesinde bulunan yazılım ve uygulamalar (SCADA yazılımları, veri toplama yazılımları, sayaç yönetim uygulamaları vb.) ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-42	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan akıllı sayaçlar log tutma, yönlendirme, derecelendirme ve sınıflandırma kapasitesine sahip olmalıdır.
OYS-43	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan akıllı sayaçlara ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-44	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Olay yönetimi gerçekleştirebilmek için kullanılan tüm log kaynakları aynı saat dilimi üzerinden senkronize edilmelidir.
OYS-45	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucularda aşağıdaki tipteki loglar tutulmalıdır. - İşletim sistemi logları - Bileşen üzerindeki güvenlik yazılımları logları (kötü amaçlı yazılım koruma uygulamaları, whitelisting uygulamaları) - Bileşen üzerinde bulunan diğer yazılımlara ilişkin loglar

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-46	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucular log yönlendirme kapasitesine sahip olmalıdır.
OYS-47	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucular log derecelendirme ve sınıflandırma kapasitesine sahip olmalıdır.
OYS-48	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucularda kayıt altına alınan loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-49	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Tespit Etme	Seviye 2	Olay tespit yetenekleri, tehdit, zafiyet ve risk yönetim süreçleri ile bütünsel olmalıdır.
OYS-50	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 1	Hangi olayların USOM'a bildirileceğine dair ilişkin kriter tanımlanmalıdır. (operasyonların etkilenmesi, hizmet verememe, endüstriyel operasyonlara etki ve etkilerin dereceleri vb.) Olay bildirim kriteri belirli periyotlarla gözden geçirilmeli ve gerekli durumlarda güncellenmelidir.
OYS-51	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) gerçekleşen siber güvenlik olay bildirimleri sürekli izlenerek ve analiz edilerek olay bildirim süreçlerinin iyileştirilebilmesi için girdi olarak kullanılmalıdır.
OYS-52	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 1	Siber güvenlik bildirimlerinin siber güvenlik olayı olup olmadığına karar vermek için kriterler belirlenmelidir.
OYS-53	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 1	Olayların yaşam döngüsü uçtan uca takip edilmelidir. (Kime atandığı, nasıl çözüldüğü, kimin çözdüğü vb.)
OYS-54	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Yönetiminde İş Sürekliliği	Seviye 1	Belirli olay ve bildirimlerin yaşanması durumunda kullanılacak iş sürekliliği planları geliştirilmelidir. (Hizmet kesintisi, operasyonel arıza vb.)
OYS-55	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan tüm ağ ve güvenlik cihazlarının konfigürasyonları periyodik olarak alınmalı, güvenli şekilde saklanmalı ve periyodik geri dönüş testleri gerçekleştirilmelidir.
OYS-56	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan tüm endüstriyel ekipman, uygulama ve bileşenlerin lojik ve/veya konfigürasyonları periyodik olarak yedeklenmeli , yedekler güvenli şekilde saklanmalı ve periyodik geri dönüş testleri gerçekleştirilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-57	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucuların imaj ve veri yedekleri periyodik olarak alınmalı, güvenli şekilde saklanmalı ve periyodik geri dönüş testleri gerçekleştirilmelidir.
OYS-58	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) iş sürekliliği planları hazırlanırken olası olayların etkileri girdi olarak kullanılmalıdır. (Hizmet kesintisi, görüntü kaybı, kontrol kaybı, üretim kaybı vb.)
OYS-59	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) operasyonların devamlılığı için gerekli olan varlık ve süreçler iş sürekliliği planına dahil edilmelidir.
OYS-60	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Hazırlanan süreklilik planları periyodik olarak test edilmeli ve gerekli durumlarda güncellenmelidir.
OYS-61	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Alınan veri, imaj konfigürasyon/lojik yedekleri orijinal veri seviyesinde korunmalıdır.
OYS-62	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Alınan tüm yedekler, mantıksal ve fiziksel olarak orijinal verilerden ayrıştırılmalıdır.
OYS-63	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Operasyon açısından önem arz eden varlıklar için kurtarma süresi hedefleri (RTO) ve kurtarma noktası hedefleri (RPO) süreklilik planlarına dahil edilmelidir.
OYS-64	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Hazırlanan süreklilik planlarının ne zaman devreye alınacağına dair kriter tanımlanmalıdır.
OYS-65	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Hazırlanan süreklilik planı, tehdit, zafiyet ve risk yönetim süreçleri ile bütünlük olarak işletilmelidir.
OYS-66	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Süreklilik planının testleri ya da icrası sonucu oluşan sonuçlar plan ile karşılaştırmalı gerekli durumlarda güncellenmelidir.
OYS-67	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Ek kontrol	(Ülkemizin yer aldığı coğrafyada yaşanan ve yaşanması olası doğal afetler göz önünde bulundurulduğunda)Kuruluşlar, ISO 22301 standardına sahip olmalıdır.
OYS-68	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden tüm kritik bileşenler yedekli yapıda olmalıdır. (Ağ ve güvenlik cihazları, sunucular, mühendislik iş istasyonları, kritik endüstriyel ekipmanlar vb.)

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-69	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 3	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden ağ bileşenleri için en az 1 adet olacak şekilde soğuk yedek (cold backup) tutulmalıdır. (Switch, router vb.)
OYS-70	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden güvenlik bileşenleri için en az bir adet soğuk yedek tutulmalıdır. (Güvenlik duvarı, IPS vb.)
OYS-71	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Ek kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden supervisory katmanda yer alan sunucu/istemci için en az bir adet soğuk yedek tutulmalıdır.
OYS-72	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Kurum, kurumsal misyon, iş süreci veya sistem düzeyinde tanımlanan acil durum planlama politikası; amaç, kapsam, roller, sorumluluklar, yönetim desteği, kurumsal varlıklar arasındaki koordinasyon ve uyumluluğu ele almalıdır. Acil durum planlama politikası; kurumun diğer politika ve prosedürleri ile uyumlu olmalıdır.
OYS-73	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Mevcut acil durum planı, politika ve prosedürleri Kurum tarafından tanımlanan olay veya zaman periyotlarına göre gözden geçirilmeli ve güncellenmelidir.
OYS-74	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planlarında ilgili kişi ve birimlerin iletişim bilgileri yer almalıdır.
OYS-75	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planları, bir sistem kesintisinde, siber saldırı veya arıza durumlarına rağmen işletmenin misyon ve fonksiyonlarını sürdürmeyi ele almalıdır.
OYS-76	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planı, yetkisiz ifşa ve içeriğinin değiştirilmesine karşı korunmalıdır.
OYS-77	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planı, normal operasyonlara dönüş planlarını içermelidir.
OYS-78	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum gereksinimlerini sağlamak için acil durum planı, harici hizmet sağlayıcıların acil durum planlarıyla koordine edilmelidir.
OYS-79	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Kriz durumlarında personelin etkin müdahalesini kolaylaştırmak için acil durum eğitimleri periyodik olarak düzenlenmelidir.
OYS-80	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planları, simülasyon ortamlarında ya da yedek/acil durum kontrol merkezinde test edilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-81	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planları, bölge çapında genel bir hizmet kesintisi veya felaket durumunda planların çalıştırılabilmesi için gerekli önlemleri içermelidir.
OYS-82	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Süreklilik gereksinimlerine uygun olarak kritik hizmet sağlayıcılar yedeklenmelidir. (Telekom hizmetleri vb.)
OYS-83	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Kuruluşlar, hizmet sağlayıcılardan acil durum planlarını oluşturmalarını istemelidir. Hizmet sağlayıcıların acil durum planları periyodik olarak gözden geçirilmelidir.
OYS-84	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Ek kontrol	Acil durum testleri kapsamında tüm yedeklilik senaryoları test edilmelidir.

Akıllı Cihaz Güvenliği				
No	Ana kontrol	Alt Kontrol	Seviye	Kontrol
ACG-1	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında yer alan tüm bileşenlerin ve iletişim cihazlarının bir envanteri oluşturulmalıdır.
ACG-2	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç mimarisinde yer alan tüm bileşenler "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddelerine uygun şekilde periyodik olarak güvenlik testlerine tabi tutulmalıdır.
ACG-3	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında yer alan tüm bileşenler risk yönetim süreci içerisinde değerlendirilmelidir.
ACG-4	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısı içerisinde gömülü yazılıma (firmware) sahip bileşenler için güvenli yapılandırma kontrol listesi hazırlanmalı ve işletme için minimum güvenlik kontrolleri belirlenmelidir. (Örnek referans: https://www.opencompute.org/documents/csis-firmware-security-best-practices-position-paper-version-1-0-pdf)
ACG-5	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısı içerisinde bulunan cihazlar üzerindeki debug arayüzleri (JTAG, SWD) müşteri ortamında devre dışı bırakılmalı veya uygun yetkilendirme yöntemleri ile aktif edilebilmelidir. (JTAG Enabling, SWD authentication vb.)
ACG-6	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısı içerisinde bulunan cihazlarda code Integrity/kod bütünlük koruma mekanizmaları sahaya gönderilmeden önce devreye alınmalı ve bu durumun korunması sağlanmalıdır. (Secure boot, boot konfigürasyonlarının devre dışı bırakılması vb.)
ACG-7	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Ek kontrol	Akıllı cihazlar üzerinde kritik parametrelerin saklanması, cihaz kimliğinin değiştirilemez şekilde eşsiz bir anahtar ile ayırt edilebilmesi ve trust anchor (Root of Trust) amacıyla SE (Secure Element), HSM (Hardware Security Module), TPM (Trusted Platform Module), TEE (Trusted Execution Environment - ARM Trustzone) gibi bileşenler akıllı cihaz tarafından kullanılmalıdır.
ACG-8	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Ek kontrol	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerin üzerinde kullanılan üçüncü taraf kodlar statik kod analizi ile gözden geçirilmeli ve herhangi bir arka kapı (backdoor) olmadığı doğrulanmalıdır.
ACG-9	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenler merkezi bir noktadan güvenli bir şekilde güncellenme yeteneğine sahip olmalıdır. [Secure-FOTA (Firmware Over the Air Update) vb.]

No	Ana kontrol	Alt Kontrol	Seviye	Kontrol
ACG-10	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç mimarisinde yer alan tüm bileşenler log toplama mekanizmalarını desteklemelidir. Başarılı, başarısız kullanıcı giriş denemeleri, debug fonksiyonlarına erişim denemeleri gibi aktiviteler kayıt altına alınmalıdır. Bunlara ek olarak akıllı cihazlar fiziksel saldırılara karşı da log üretebilmelidir.
ACG-11	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerden alınan log kayıtları en az olay tipi, zaman damgası, kaynak, sonuç bilgilerini içermelidir.
ACG-12	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenler güvenilir bir zaman sunucusu üzerinden senkronize edilmelidir.
ACG-13	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerden alınan loglar üzerinde kritik/hassas bilgilerin olmadığı doğrulanmalıdır. (Kullanıcı bilgisi, kriptografik anahtarlar vb.)
ACG-14	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerden alınan loglar, ilgili bileşenler üzerinde ve toplama noktalarında uygun güvenlik kontrolleri ile korunmalıdır. Logların bileşenler üzerinden merkezi noktaya aktarımında güvenli iletişim teknolojileri kullanılmalıdır. (Anlık ya da cihaz üzerinden)
ACG-15	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında yer alan bileşenlerden alınan logların saklanmasına ilişkin süreler ilgili yasal düzenlemelere uygun olarak belirlenmelidir.
ACG-16	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Yasal Uyumluluk	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında kullanılan bileşenler üzerinde tutulan, işlenen ve saklanan tüm veriler için ilgili yasal düzenlemelere uygun hareket edilmelidir. (KVKK vb.)
ACG-17	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında kullanılan bileşenler üzerinde çalışan servisler belirlenmeli ve gereksiz olduğu değerlendirilen servisler devre dışı bırakılmalıdır.
ACG-18	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısına ilişkin risk analizi sürecinde tüm mimariye ilişkin saldırı vektörleri belirlenmeli ve uygun tehdit modelleme çalışmaları gerçekleştirilmelidir.
ACG-19	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında kullanılan tüm iletişim kanalları ve protokoller belirlenmeli ve dokümanite edilmelidir. (WAN, HAN vb.)
ACG-20	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Doğal gaz dağıtım şebekesi akıllı cihaz mimarisi uçtan uca belirlenmeli ve dokümanite edilmelidir. Bu dokümantasyon kapsamında tüm bileşenler bir topoloji üzerinden gösterilmelidir.

No	Ana kontrol	Alt Kontrol	Seviye	Kontrol
ACG-21	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında kullanılan tüm cihazlar belirlenerek, bunların üzerindeki erişim arayüzleri (USB, PS2 vb.) uygun seviyede güvenlik kontrolleri ile korunmalıdır. Kullanılmayan veya gereksiz olduğu değerlendirilen arayüzler devre dışı bırakılmalıdır.
ACG-22	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında kullanılan cihazlar üzerindeki debug portları ve CLI (Command Line Interface) erişimleri belirlenerek uygun seviyede güvenlik kontrolleri ile korunmalıdır.
ACG-23	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Ek kontrol	Doğal gaz dağıtım şebekesi akıllı sayaç yapısı kapsamındaki kritik veriler HSM, SE, TPM içerisinde saklanmalıdır.
ACG-24	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Ek kontrol	Gömülü kod (firmware) snarfing'e karşı uygun güvenlik kontrolleri tanımlanmalı ve korunmalıdır. Bunu sağlamak adına FLASH ve EEPROM alanlarında şifreleme teknikleri uygulanmalıdır. Temel prensip olarak durağan veri (data at rest) güvenliğini sağlamak adına dosya sistemi veya depolama alanlarında şifreleme teknikleri uygulanmalıdır.
ACG-25	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında kullanılan cihazların iletişim protokolleri/arayüzleri güvenli şekilde yapılandırılmalıdır. (UART, I2C, SPI vb.)
ACG-26	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Haberleşme Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısı içerisindeki WAN haberleşmeleri izole veya şifreli kanallar üzerinden gerçekleştirilmelidir.
ACG-27	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Haberleşme Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç protokolleri replay saldırılarına karşı dirençli olmalıdır.
ACG-28	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Haberleşme Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç protokolleri araya girme saldırılarına karşı dirençli olmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
ACG-29	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısı içerisinde hizmet eden sunucular izole bir ağ üzerinde konumlanmalıdır.
ACG-30	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısı içerisindeki izole ağlara erişimler kısıtlanmalıdır. (Uzak erişim, üçüncü taraf, son kullanıcılar, diğer sunucular vb.)
ACG-31	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi akıllı sayaç yapısı içerisinde hizmet eden sunucular uygun şekilde sıkılaştırılmalıdır. (Veri tabanı, uygulama sunucusu vb.)
ACG-32	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında bulunan veri toplama (data concentrator) bileşenlerinden uç bileşenlere yönelik erişimler güvenilir kanallar üzerinden sağlanmalıdır.
ACG-33	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında bulunan veri toplama noktaları arasındaki iletişimler kısıtlanmalıdır.

No	Ana kontrol	Alt Kontrol	Seviye	Kontrol
ACG-34	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında kullanılan tüm bileşenlerde, gömülü ve basit parola kullanımı engellenmelidir.
ACG-35	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç altyapısında ağa giriş (access control) kontrolleri uygulanmalıdır.
ACG-36	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Tehdit ve Zafiyet Yönetimi	Seviye 2	Doğal gaz şebekesi akıllı sayaç yapısında kullanılan tüm bileşenlerin "Tehdit ve Zafiyet Yönetimi" başlığının ilgili maddelerine uygunluğu sağlanmalıdır.
ACG-37	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Tehdit ve Zafiyet Yönetimi	Seviye 2	Doğal gaz dağıtım şebekesi akıllı sayaç yapısında kullanılan tüm bileşenler anlık olarak izlenebilir durumda olmalıdır.

Endüstriyel Operasyon Güvenliği				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EOG-1	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan RTU'lar sadece belirli sunuculardan (Master) komut alacak şekilde yapılandırılmalıdır.
EOG-2	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) lojik işleyen bileşenlere sadece mühendislik iş istasyonu üzerinden lojik güncellemeyi sağlayacak kontroller devreye alınmalıdır.
EOG-3	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Doğal gaz dağıtım şebekesinde, Endüstriyel Kontrol Sistemleri mimarisinde kullanılan lojik işleyen bileşenlere lojik güncellemeleri sırasında ek bir kimlik doğrulama mekanizması devreye alınmalıdır.
EOG-4	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon değişimleri sadece yetkili iş istasyonları üzerinden sağlanmalıdır.
EOG-5	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Ek Kontrol	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon değişimleri sırasında ikinci bir kimlik doğrulama mekanizması uygulanmalıdır.
EOG-6	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Veri Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon dosyaları ve lojik dosyaları için bütünlük kontrolleri devreye alınmalıdır.
EOG-7	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyon Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon dosyaları ve lojik dosyaları sürüm numaraları ile takip edilebilmelidir.
EOG-8	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Erişim ve Yetkilendirme	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon dosyaları ve lojik dosyalarının saklandığı alanlara sadece yetkili kişi ve grupların eriştiği garanti altına alınmalıdır.
EOG-9	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Veri Güvenliği	Seviye 2	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan SCADA konfigürasyon dosyaları ve lojik dosyaları kişisel bulut tabanlı sistemlerde ve dosya paylaşım alanlarında saklanamaz. Bu verilerin kurumsal bulut tabanlı sistemler ve dosya paylaşım alanlarında kullanılmasının zorunlu olduğu durumlarda; T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanarak yayımlanan Bilgi ve İletişim Güvenliği Rehberinde "4.3 Bulut Bilişim Güvenliği" tedbirleri sağlanarak saklanmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EOG-10	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Veri Güvenliği	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinde (EKS) kullanılan ve üzerinde konfigürasyon veya lojik bilgisi bulunan ekipmanlar kurum dışına çıkarılacaksa (bakım, hibe vb.) söz konusu konfigürasyon ve lojik bilgileri ilgili bileşen üzerinden silinmelidir.

İnsan Kaynakları Güvenliği				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İKG-1	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	EKS altyapılarında çalışacak tüm personel yasal mevzuata uyumlu şekilde, gerekli güvenlik kontrollerinden geçirilmelidir. (Adli sicil, güvenlik soruşturması, referans ve belge kontrolü vb.)
İKG-2	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	EKS altyapılarında çalışacak personelin, işe uygunluk ve sağlık raporları bulunmalıdır.
İKG-3	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	EKS altyapılarında çalışacak personelle sözleşme imzalanmalıdır. (Bu sözleşmeler gizlilik sözleşmesi şeklinde olabileceği gibi ana sözleşmelerin gizlilik ve siber güvenlik maddelerini içermesi şeklinde de olabilir.)
İKG-4	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	Personelle yapılacak sözleşmelerde siber güvenlik ve gizlilik maddeleri en az aşağıdakileri içermelidir: - Gizli bilginin korunması, - Kurumsal hassas ve kritik bilgilerin korunması, - Kurumun uyguladığı veya uygulayacağı tüm siber güvenlik kontrollerine uyum, - Kuruluşa ait; lojik, konfigürasyon bilgileri, yedek dosyalar ve tasarımların kişisel disk, bilgisayar ya da bulut ortamlarında saklanmayacağına dair beyan, - Yasal, sözleşme kaynaklı veya müşteri gereksinimlerinden doğan siber güvenlik politika, prosedür ve uygulamalarına uyumlu çalışma.
İKG-5	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	İşe alım ilanları, ilgili tesisin siber güvenlik açısından bağlayıcı olan teknolojileri ile ilgili bilgi içermemesini sağlayacak politika, prosedür ve süreçler çerçevesinde tasarlanmalıdır.
İKG-6	İnsan Kaynakları Güvenliği	İstihdam Sırasında	Seviye 1	Personel, çalışma süresince tüm siber güvenlik politika, prosedür ve uygulamalarına uyumlu hareket etmelidir.
İKG-7	İnsan Kaynakları Güvenliği	İstihdam Sırasında	Seviye 1	Tüm EKS personeli periyodik siber güvenlik farkındalık programına dahil edilmelidir.
İKG-8	İnsan Kaynakları Güvenliği	İstihdam Sırasında	Seviye 1	Siber güvenlik operasyonlarını yürütecek personelin EKS bileşenleri ile ilgili eğitim almaları sağlanmalıdır.
İKG-9	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	Tüm EKS personeli için siber güvenlik ihlallerine ilişkin disiplin süreçleri tanımlanmalıdır.
İKG-10	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	Sözleşme ve uygulamalar, istihdam sonrası koşulları içermelidir.
İKG-11	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İstihdamın sonlandırılması ile birlikte tüm EKS varlıklarına olan mantıksal ve fiziksel erişimler sonlandırılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İKG-12	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İstihdam sonlanması ile birlikte tüm gerekli taraflar bilgilendirilmelidir.
İKG-13	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İstihdam sonlanması sürecinde operasyonel süreklilik için önem arz eden tüm varlıklar (proses, lojik vb.) güvenli bir şekilde devredilmelidir.
İKG-14	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İlgili istihdam sonlandırma süreci, olaylı ayrılma durumlarını da içermelidir.
İKG-15	İnsan Kaynakları Güvenliği	Üçüncü Taraf Güvenliği	Seviye 1	EKS altyapılarında üçüncü taraflarca sağlanan taşıeron personellerin hem birinci derece bağlı oldukları hem de hizmet sundukları kuruluşlar için bu başlık altındaki süreçler işletilmelidir. Alt yükleniciler, farklı bir alt yüklenici kullandığında sorumluluk devredemeyeceği gibi bu madde kapsamında doğan yükümlülükleri de yerine getirmelidir.
İKG-16	İnsan Kaynakları Güvenliği	Üçüncü Taraf Güvenliği	Seviye 1	Üçüncü taraflara veya üreticiye bağlı olarak çalışan personel kuruluşun belirlediği gizlilik ve siber güvenlik gereksinimlerinden muaf tutulamaz. Gerekli koşullarda ilgili personelle de ek bir gizlilik sözleşmesi veya siber güvenlik maddelerini içeren sözleşme yapılmalıdır.

Fiziksel Güvenlik				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-1	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke girişinde giriş çıkış kaydı tutulmalıdır.
FZG-2	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke girişinde yetkisiz erişime karşı önlemler alınmalıdır.
FZG-3	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke giriş prosedürleri tanımlanmalıdır. Yerleşke giriş prosedürleri, ziyaretçi, geçici-kalıcı çalışan, acil giriş durumlarını içermelidir.
FZG-4	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke girişlerinde uygun güvenlik ve emniyet eğitimleri verilmelidir.
FZG-5	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke giriş çıkışlarını izleyen elektronik sistemlerde zaman senkronizasyonu sağlanmalıdır.
FZG-6	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke giriş çıkışlarını izleyen elektronik sistemlerde merkezi kayıt yönetim sistemi entegrasyonu sağlanmalıdır.
FZG-7	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke giriş çıkışlarını izleyen elektronik sistemlerde yedekleme politikaları oluşturulmalı, yedekler alınmalı ve yedekler test edilmelidir.
FZG-8	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke çevresini izlemek için kameralar kurulmalıdır. Bu sistemler sürekli olarak izlenmelidir.
FZG-9	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Yerleşke çevresi kamera kayıtları en az üç ay süre ile saklanmalıdır.
FZG-10	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Kamera sistemlerinde zaman senkronizasyonu sağlanmalıdır.
FZG-11	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Çevresel güvenlik bileşenleri izole ağlarda konumlanmalıdır.
FZG-12	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Çevresel güvenlik bileşenlerine erişim kullanıcı adı ve parola ile sağlanmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-13	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Çevresel güvenlik bileşenleri yetkisiz fiziksel erişime karşı korunmalıdır.
FZG-14	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Merkezi kontrol sistemi bileşenlerinin bulunduğu alanlara fiziki erişimin tamamıyla kontrol altına alınabileceği herhangi bir noktada X-RAY cihazı konumlandırılmalıdır.
FZG-15	Fiziksel Güvenlik	Yerleşke Güvenliği	Seviye 1	Araçlar gerekli kontrollerden geçirilerek yerleşkeye alınmalıdır.
FZG-16	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kayıt tutulmalıdır.
FZG-17	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemlerde zaman senkronizasyonu sağlanmalıdır.
FZG-18	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemler merkezi kayıt yönetim sistemine entegre edilmelidir.
FZG-19	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemlerde yedekleme politikaları oluşturulmalı, yedekler alınmalı ve yedekler test edilmelidir.
FZG-20	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemler izole ağlarda konumlandırılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-21	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları çevresel güvenlik bileşenlerine erişim kullanıcı adı ve parola ile sağlanmalıdır.
FZG-22	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş ve çıkışlarında kullanılan elektronik sistemlerde güçlü parola kullanılmalıdır.
FZG-23	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında kurum harici çalışanlara kurum personeli eşlik etmelidir.
FZG-24	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarını izlemek için kameralar kurulmalıdır. Bu sistemler sürekli olarak izlenmelidir.
FZG-25	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kamera kayıtları en az üç ay süre ile saklanmalıdır.
FZG-26	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kamera sistemlerinde zaman senkronizasyonu sağlanmalıdır.
FZG-27	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kamera sistemleri IP tabanlı ise ayrı izole bir ağ üzerinde konumlandırılmalıdır.
FZG-28	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kamera bileşenleri kullanıcı adı ve parola ile korunmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-29	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları çevresel güvenlik bileşenleri (Kamera, kartlı geçiş, yangın algılama vb.) yetkisiz fiziksel erişime karşı korunmalıdır.
FZG-30	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında bulunan kameralar proseslerin izlendiği HMI'ları görmeyecek şekilde konumlandırılmalıdır.
FZG-31	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları kapıları otomatik olarak kapanmalıdır.
FZG-32	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarından acil çıkış mümkün olmalıdır.
FZG-33	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında yer alan çevresel izleme sensörleri yetkisiz fiziksel erişime olanak vermeyecek şekilde konumlandırılmalıdır.
FZG-34	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 2	Kontrol odalarının kapıları açık kaldığında alarm üretmelidir.
FZG-35	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında çevresel izleme sensörleri konumlandırılmalıdır. (Yangın, su, nem, sıcaklık vb.)
FZG-36	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarında kullanılan çevresel izleme sistemleri alarm üretebilmelidir.
FZG-37	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları çevresel izleme sensörleri merkezi olarak izlenmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-38	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odaları giriş kontrolleri, enerjisiz kaldığında da aynı güvenlik seviyesini korumalıdır.
FZG-39	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 1	Kontrol odalarındaki tüm güvenlik bileşenleri yedek bir enerji ya da kesintisiz bir enerji kaynağı üzerinden beslenmelidir.
FZG-40	Fiziksel Güvenlik	Kontrol Merkezi ve Acil Durum Kontrol Merkezi	Seviye 2	Endüstriyel operasyonlara hizmet eden istemci ve sunuculara fiziksel erişimler kısıtlanmalıdır.
FZG-41	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi hizmetlerinin üçüncü taraflardan temin edilmesi durumunda; alınması gerekli tedbirler sözleşmeler ile hüküm altına alınmalıdır. Paylaşımlı veri merkezlerinde tüm tarafların güvenliği ve gizliliği hizmet sağlayıcı tarafından güvence altına alınmalıdır.
FZG-42	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş-çıkış kayıtları tutulmalıdır.
FZG-43	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi elektronik geçiş kontrol sistemlerinde zaman senkronizasyonu sağlanmalıdır.
FZG-44	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi elektronik geçiş kontrol sistemlerinde merkezi log/kayıt yönetim entegrasyonu sağlanmalıdır.
FZG-45	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi elektronik geçiş kontrol sistemlerinde yedekleme politikaları oluşturulmalı, yedekler alınmalı ve yedekler test edilmelidir.
FZG-46	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi elektronik geçiş kontrol sistemleri kullanıcı adı ve parola ile korunmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-47	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi ziyaretlerinde yetkili personel ziyaretçilere eşlik etmelidir. Ziyaretçi ve refakatçi kayıtları en az bir yıl süre ile saklanmalıdır.
FZG-48	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezlerini izlemek için kamera sistemi kurulmalıdır.
FZG-49	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kameralara ilişkin kayıtlar belirlenen en az üç ay süre ile saklanmalıdır.
FZG-50	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kameralarda zaman senkronizasyonu sağlanmalıdır.
FZG-51	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kamera bileşenleri mantıksal izole bir ağ üzerinde konumlandırılmalıdır.
FZG-52	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kamera bileşenleri kullanıcı adı ve parola ile korunmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-53	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kameralar fiziksel erişime karşı koruma altına alınmalıdır.
FZG-54	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesindeki kameralar kör nokta olmaksızın konumlandırılmalıdır.
FZG-55	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş çıkış kapıları otomatik olarak kapanmalıdır.
FZG-56	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş çıkış kapıları acil çıkış prosedürlerine uygun olmalıdır.
FZG-57	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş çıkış noktalarında olan sensörler yetkisiz erişime olanak vermeyecek şekilde konumlandırılmalıdır.
FZG-58	Fiziksel Güvenlik	Veri Merkezi	Seviye 2	Veri merkezi kapıları açık kaldığında alarm üretebilmelidir.
FZG-59	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde çevresel izleme sensörleri konumlandırılmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-60	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi çevresel izleme sensörleri alarm üretme kabiliyetine sahip olmalıdır.
FZG-61	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi çevresel izleme sensörleri merkezi olarak izlenebilmelidir.
FZG-62	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi giriş çıkış kontrolleri, elektrik kesintilerinde aynı koruma seviyesine sahip olmalıdır.
FZG-63	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi çevresel izleme bileşenleri yedek enerji kaynaklarıyla ya da kesintisiz enerji kaynakları üzerinden beslenmelidir.
FZG-64	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde deprem koruma önlemleri alınmalıdır.
FZG-65	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde su baskını koruma önlemleri alınmalıdır.
FZG-66	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi yangın koruma/söndürme sistemleri bulundurulmalıdır.
FZG-67	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi yangın koruma/söndürme sistemlerinin periyodik bakımları yapılmalıdır.
FZG-68	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi yangın koruma/söndürme sistemleri elektronik ortamlar için uygun olmalıdır.
FZG-69	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi uygun iklimlendirme altyapısına sahip olmalıdır.
FZG-70	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde kablolama güvenliği ilkeleri uygulanmalıdır.
FZG-71	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde kablolar etiketlenmelidir.
FZG-72	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde yedek enerji besleme kaynakları bulundurulmalıdır.
FZG-73	Fiziksel Güvenlik	Veri Merkezi	Seviye 1	Veri merkezi bünyesinde enerji besleme bileşenlerinin periyodik bakımları gerçekleştirilmelidir.
FZG-74	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan ve kritik ekipmanların olduğu alanlar için giriş-çıkış kontrolleri uygulanmalıdır. (Bu kontroller kilitli kapı, kilitli kabin vb. uygulamaları da içerir.)
FZG-75	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan ve personel bulunan uç sahalarda giriş-çıkış kayıtları tutulmalıdır.
FZG-76	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan ve personel bulunmayan uç sahalara pano açıldı/kapandı kayıtları merkezi olarak izlenmelidir.
FZG-77	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda bulunan kritik ekipmanlar kilitli alanlarda saklanmalıdır.
FZG-78	Fiziksel Güvenlik	Uç Saha	Seviye 1	RMS-A istasyonlarda depreme karşı sabitleme önlemleri alınmalıdır.
FZG-79	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda su baskını koruma önlemleri alınmalıdır.
FZG-80	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda yangın tespit sistemleri konumlandırılmalıdır. (Oda veya kabin içi duman veya sıcaklık algılama sistemleridir.)
FZG-81	Fiziksel Güvenlik	Uç Saha	Seviye 1	RMS-A istasyonlarda yangın koruma/söndürme bileşenleri konumlandırılmalıdır.
FZG-82	Fiziksel Güvenlik	Uç Saha	Seviye 1	RMS-A istasyonlarda yangın koruma/söndürme bileşenlerinin periyodik bakımları yapılmalıdır.
FZG-83	Fiziksel Güvenlik	Uç Saha	Seviye 1	RMS-A istasyonlarda yangın koruma/söndürme bileşenleri elektronik ortamlar için uygun olmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-84	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda kablolama güvenliği ilkeleri uygulanmalıdır.
FZG-85	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda kablolar etiketlenmelidir.
FZG-86	Fiziksel Güvenlik	Uç Saha	Seviye 1	RMS-A istasyonlarda yedek enerji beslemeleri kullanılmalıdır.
FZG-87	Fiziksel Güvenlik	Uç Saha	Seviye 1	RMS-A istasyonlarda yedek enerji besleme bileşenlerinin periyodik bakımları gerçekleştirilmelidir.
FZG-88	Fiziksel Güvenlik	Uç Saha	Seviye 2	RMS-A istasyonlarda acil durum tahliye prosedürleri tanımlanmalı ve uygulanmalıdır. (doğal gaz yangını ya da patlama anında ilgili lokasyonunun güvenli şekilde tahliye edilmesi vb.)
FZG-89	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda yer alan çevresel izleme sensörleri yetkisiz erişime olanak vermeyecek şekilde konumlandırılmalıdır.
FZG-90	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda kapı ya da panolar açık kaldığında alarm üretilebilmelidir.
FZG-91	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda çevresel izleme sensörleri konumlandırılmalıdır.
FZG-92	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda çevresel izleme sensörleri alarm üretebilmelidir.
FZG-93	Fiziksel Güvenlik	Uç Saha	Seviye 1	Uç sahalarda çevresel izleme sensörleri merkezi olarak izlenebilmelidir.
FZG-94	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda elektronik giriş çıkış kontrolleri varsa bu bileşenler enerji olmadığında mevcut güvenlik seviyesini sürdürebilmelidir.
FZG-95	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç saha çevresel izleme bileşenleri yedek enerji beslemelerinden veya kesintisiz güç kaynağından beslenebilmelidir.
FZG-96	Fiziksel Güvenlik	Uç Saha	Seviye 3	Kontrol sistemi bileşeni olan uç sahalarda kullanılan fiziksel anahtarların yönetimi için tekil anahtar kullanılması durumunda fiziksel kopyalamaya karşı korumalı olmalıdır. Anahtar dağıtımlarına ilişkin kayıtlar tutulmalı ve saklanmalıdır. Personelin işten ayrılması durumunda bu anahtarlar teslim alınmalıdır.
FZG-97	Fiziksel Güvenlik	Uç Saha	Seviye 1	Kontrol sistemi bileşeni olan uç sahalarda kullanılan tüm fiziksel anahtarlar kopyalamaya karşı korunmalıdır.

Tedarikçi Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TDY-1	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluşun tedarikçiye olan bağımlılıklarını belirlemek için bağımlılık kriterleri tanımlanmalıdır.
TDY-2	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinin (EKS) devamlılığının sağlanması için önem arz eden tüm EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) tedarikçileri ve bu tedarikçilerin bağımlılıkları belirlenmelidir.
TDY-3	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluş, tüm kritik veya tekil kaynak bağımlılıklarını tanımlamalıdır.
TDY-4	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluş, tedarikçileri bağımlılıklarına göre önceliklendirmelidir.
TDY-5	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçiler ve diğer bağımlılıklardan kaynaklanan önemli siber güvenlik riskleri tanımlanmalı ve adreslenmelidir.
TDY-6	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Kuruluş, tedarikçi bağımlılıklarından kaynaklanan risk yönetimi aktivitelerini, mevcut risk yönetim süreçlerine dahil etmelidir.
TDY-7	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçiler ve diğer üçüncü taraflar ile yapılan sözleşmelerde siber güvenlik gereksinimleri dikkate alınmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-8	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü taraflarla (üretici, mühendislik firmaları, altyükleniciler) yapılan sözleşmeler ve anlaşmalar aşağıdakileri içermelidir: - Üçüncü tarafların sunduğu ürün ve hizmetlerde ortaya çıkan zafiyetler, - Üçüncü tarafların kendisine ya da sunduğu ürünlere yönelik saldırı/tehdit bilgileri. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-9	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçiler kuruluşlara sunduğu ürün ve hizmetler için güvenli yazılım geliştirme süreçleri de dahil olacak şekilde siber güvenlik kontrollerine sahip olmalıdır. Sunulan ürün ve hizmetler bu kontrollere uygun olarak yürütülmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TDY-10	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Tedarikçiler ile yapılan sözleşmeler, tedarikçinin sağladığı hizmetlerin sahip olduğu veya gelecekte oluşabilecek güvenlik açıklarını bildirme sürecini içermelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-11	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçi tarafından sağlanan tüm yazılım ve yamaların bütünlüğü ve orijinallliği kontrol edilerek bu yazılım ve yamaların değiştirilmediği garanti altına alınmalıdır.
TDY-12	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçilerin sisteme uzaktan erişim için talepleri kapsamında dokümanite edilmiş uzak erişim bağlantı süreçleri ve kontrol yöntemleri tanımlanmalıdır. Tedarikçi erişimleri "Kimlik ve Erişim Yönetimi" başlığına uygun olarak yürütülmelidir.
TDY-13	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçi ile yapılan sözleşmelerde, doğal gaz dağıtım şebekesi endüstriyel kontrol sistemlerinin (EKS) sürekliliğini tehdit eden arıza ve problemlere müdahale süreçleri belirlenmeli ve oluşabilecek riskler, risk yönetim sürecine dahil edilmelidir.
TDY-14	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçilerin ve diğer harici kuruluşların değerlendirilmesi ve seçimi süreçlerinde, tedarikçilerin siber güvenlik gereksinimlerini karşılama yetenekleri değerlendirilmelidir.
TDY-15	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Tedarikçilerle yapılan sözleşmeler ya da yapılacak işi tanımlayan teknik şartnameler, bir siber güvenlik olayı veya ihlaline ilişkin bildirimleri de içermelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-16	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Kuruluşun bilgi varlıklarına geçici ya da kalıcı olarak erişebilen (uzak erişimler de dahil olmak üzere), bunu işletebilen, depolayabilen, iletebilen veya kuruluşun bilgi varlıkları için KBS altyapı bileşenlerini temin eden tedarikçilerin her biri ile sözleşme yapılmalı ve sözleşmeler bilgi güvenliği gereksinimlerini içermelidir.
TDY-17	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Üçüncü taraflardan doğan risklere ilişkin azaltıcı/yok edici kontroller uygulanmalıdır.
TDY-18	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Kuruluş tarafından üçüncü taraflara yönelik uygulanacak siber güvenlik kontrolleri, üçüncü tarafın kritikliğine ve risk seviyesine uyarlanabilir olmalıdır.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TDY-19	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü taraf siber güvenlik süreç yönetiminde ve seçiminde destek sonu (end of support) ömür sonu (end of life) durumları göz önünde bulundurulmalı, sözleşmelere dahil edilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-20	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü tarafların lisanslı olmayan ürün sağlamanın önüne geçilmelidir. Bu konuyla ilgili oluşabilecek güvenlik ihlalleri sözleşme ya da teknik şartnamelerde ele alınmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır)</i>
TDY-21	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Siber güvenlik gereksinimlerinin karşılanmasına ilişkin kabul testleri (SAT ve FAT) tanımlanmalı ve gerçekleştirilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-22	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü tarafların siber güvenlik kapasite yeterliliği periyodik olarak gözden geçirilmeli, tanımlı metriklerle ölçülmelidir. İşletmeler, belirli puanın altında kalan tedarikçilerle olan çalışmalarını gözden geçirmelidir.
TDY-23	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluş, tedarikçilerden doğan değişiklikleri yönetmelidir. Bu değişikliklerin siber güvenlik risk durumuna olan etkileri risk yönetim süreci kapsamında ele alınmalıdır.
TDY-24	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflara yönelik uygulanacak politika ve prosedürler periyodik olarak veya ihtiyaçlara uygun şekilde güncellenmelidir.
TDY-25	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflarla olan ilişkileri yöneten ve hizmetleri sağlayan personelde gerekli siber güvenlik yetkinlikleri aranmalıdır. Yetkinliklere ilişkin şartlar sözleşmelerle ya da teknik şartnamelerle garanti altına alınmalıdır.
TDY-26	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflarla olan ilişkileri yöneten personele ilişkin sorumluluklar, yetki ve hesap verilebilirlik durumu dokümanite edilmiş olmalıdır.
TDY-27	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflara ilişkin aktiviteler (itibar durumları, veri sızıntısı, hedefli saldırı, zararlı yazılım, fidye vb. saldırılara karşı durumları vb.) sürekli olarak izlenmeli ve değerlendirilmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TDY-28	Tedarik Zinciri ve Dış Bağılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü tarafların hizmet sunduğu kuruluşa ait bilgileri halka açık ağlarda izinsiz yayınlamayacağı ve referans gösteremeyeceği hususu şartnameler ya da sözleşmelerle garanti altına alınmalıdır.

PLC Güvenliđi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
PLC-1	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	Oluřturulacak PLC yazılımında kodlar modülerize edilerek farklı fonksiyon blokları kullanılmalı ve oluřturulan modüller ve bu fonksiyon blokları bağımsız test edilebilmelidir.
PLC-2	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	PLC çalışma modları takip edilmeli ve RUN modunda deđilse alarm üretilmelidir.
PLC-3	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	Lojik işlemleri mümkün ise PLC üzerinde yapılmalıdır. HMI üzerinde operasyonel lojik yazmaktan kaçınılmalıdır.
PLC-4	PLC Güvenliđi	PLC Güvenliđi	Ek kontrol	Oluřturulan yazılımda bütünlük kontrolünü sağlamak için PLC flagleri kullanılmalı, matematiksel hatalarda, sayaç (counter) taşmasında, negatif sayaçlarda hata flagleri üretilmelidir.
PLC-5	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	PLC kod bütünlüğünü korumak ve yazılım deđiřtiđinde alarm üretmek için PLC checksumları kullanılmalıdır.
PLC-6	PLC Güvenliđi	PLC Güvenliđi	Ek kontrol	Zamanlayıcı (timer) ve sayaç (counter) deđerleri PLC programına yazıldıđında ikincil bir kontrol olarak bu deđerlerin geçerlilik kontrolü yapılmalıdır.
PLC-7	PLC Güvenliđi	PLC Güvenliđi	Ek kontrol	Her iki sinyallin aynı anda gelemeyeceđi durumlar için sinyaller eşleřtirilmeli ve ikisinin aynı anda verilmediđinden emin olunmalı ayrıca fiziksel olarak mümkün olmayan giriř çıkıř durumları oluřtuđuunda alarm üretilmelidir.
PLC-8	PLC Güvenliđi	PLC Güvenliđi	Ek kontrol	PLC deđerkenlerine HMI eriřimi HMI'da belirlenen operasyonel deđer aralıđı ile sınırlandırılmalı ayrıca deđer aralıđı dıřındaki deđerler için de PLC'de çapraz sorgulamalar yapılmalıdır.
PLC-9	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	PLC yazılımında bir register deđerinin bařka bir registerda kullanılmadıđından emin olunmalı ve bunun için önlemler alınmalıdır.
PLC-10	PLC Güvenliđi	PLC Güvenliđi	Ek kontrol	PLC yazılımında tanımlanmıř sinyallere harici yazmaları engellemek, verileri dođrulamak ve korumak, arabellek tařmalarını engellemek için daha önceden belirlenmiř kayıt blokları atanmalıdır.
PLC-11	PLC Güvenliđi	PLC Güvenliđi	Ek kontrol	PLC yazılımında tanımlanmıř farklı proses ekipmanlarının ölçüm deđerlerinin dođruluk kontrolü için çapraz kontroller yapılmalıdır.
PLC-12	PLC Güvenliđi	PLC Güvenliđi	Ek kontrol	PLC yazılımına pratikte fiziksel olarak mümkün deđerlerin girildiđinden emin olunmalı ve bunun yanın sıra fiziksel olarak olması gereken süreler dıřında bir gecikme veya sapmada alarm üretilmelidir.
PLC-13	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	PLC'lerde ön tanımlı (default) olarak aktif gelen ve kullanılmayan haberleřme protokolleri, servisler ve portlar devre dıřı bırakılmalıdır.
PLC-14	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	PLC ile haberleřecek 3. parti arayüzler veya uygulamalar için bađlantı türleri ve paylařılan veriler kısıtlanmalı yalnızca gerekli veriler üzerinden okuma yazma yetkilerine izin verecek řekilde konfigürasyon yapılmalıdır.
PLC-15	PLC Güvenliđi	PLC Güvenliđi	Ek kontrol	PLC nin tekrar bařlaması durumunda proses için güvenli bir durum tanımlanmalıdır.
PLC-16	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	PLC çevrim (cycle) zamanı her iki veya üç saniyede bir özetlenerek HMI'da trend olarak gösterilmelidir.
PLC-17	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	PLC çalışma süresi kayıt altına alınarak HMI tarafında izlenmelidir.
PLC-18	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	Arıza ve kapanmalardan kaynaklanan PLC duruřları kayıt altına alınmalı ve HMI tarafında izlenmelidir.

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
PLC-19	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	PLC yazılımının hafıza kullanımı ölçülmeli ve PLC tarafında izlenmelidir.
PLC-20	PLC Güvenliđi	PLC Güvenliđi	Ek kontrol	PLC yazılımında proses için kritik alarm ve uyarılar belirlenmeli ve bu uyarılar için tuzaklar hazırlanmalıdır.