İSTANBUL
SU VE KANALİZASYON
İDARESİ
İSKİ

SCADA SİSTEMLERİ
NETWORK VE BİLGİ GÜVENLİĞİ

İsmail İNAN
Mühendis

BİLGİ İŞLEM DAİRE BAŞKANLIĞI
Donanım Şube Müdürlüğü

İSTANBUL
SU VE KANALİZASYON
İDARESİ
İSKİ

Sunum İçeriği

- SCADA Sistemleri Güvenliği
- SCADA Sistemlerinde Güvenliği Sağlanması Gereken Kritik Bileşenler
- SCADA Sistemlerine Uygulanabilecek Güvenlik Çözümleri
- SCADA Sistemleri Network Yapılandırması
- SCADA Networklerinde Karşılaşılan Zorluklar
- SCADA'da Uygulanabilecek Network Çözümleri
- Örnek SCADA Sistemi

İSTANBUL
SU VE KANALİZASYON
İDARESİ
İSKİ

SCADA Sistemleri Güvenliği

SCADA sistemleri; yerel veya uzak endüstriyel proseslerin kontrolü, gerçek zamanlı verileri izlemek toplamak ve işlemek, sensör gibi cihazlarla doğrudan etkileşim ve olay kayıtlarını tutmak gibi servisleri sunan yazılım ve donanım tabanlı endüstriyel denetim sistemleridir.

SCADA sistemleri kritik altyapıları denetleme işlemini gerçekleştirdikleri için siber saldırılardan korunmaları büyük önem taşımaktadır.

İSTANBUL SU VE KANALİZASYON İDARESİ
İSKİ

2013

İran, New York Barajı C&C sistemine sızdı

2014

Havex

Avrupa EKS sistem üretici ve organizasyonları hedeflendi

2015

Black Energy

Ukrayna enerji şirketleri hedeflendi

2016

Undisclosed malware

İngiltere enerji ve Telekom sektörü hedeflendi

2016

Industroyer / Crashoverride

Kiev enerji kesintisi

2017

Triton/Trisis

Suudi petrokimya emergency shutdown sistemi hedeflendi

2017

NotPetya Ransomware

Ukrayna, Amerika ve Avrupa enerji sektörü, bankalar ve hükümet hedeflendi

2018

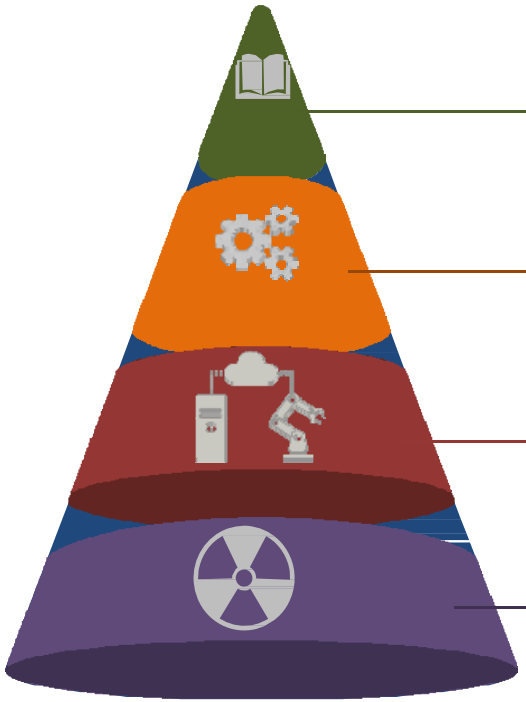
Grizzly Steppe

Amerika enerji sektörü APT saldırısı

İSTANBUL SU VE KANALİZASYON İDARESİ
İSKİ

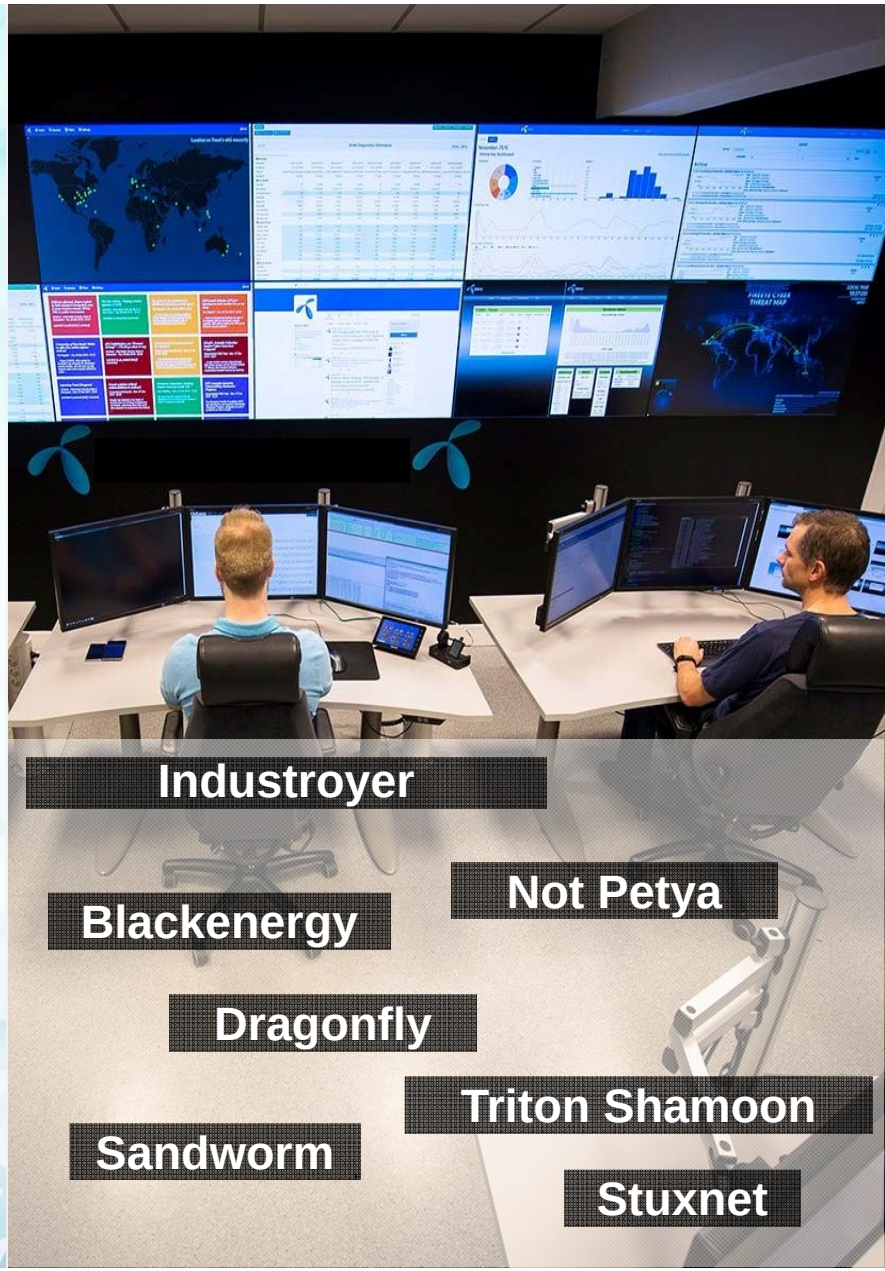
IT / OT Siber Güvenlik İhtiyacı

Hedef Odaklı Saldırılar → Siber Savaş → Suç Örgütleri Terörizm → Artan Siber Tehditler



- UYUM
- SÜREÇ İHTİYAÇLARI
- TEKNOLOJİK GELİŞMELER

SİBER GÜVENLİK RİSKLERİ



İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

SCADA Sistemlerinde Güvenliği Sağlanması Gereken Kritik Bileşenler

- Süreçleri izleme ve kontrol etmeye yardımcı olan insan-makine ara yüzünden oluşan kontrol paneli
- Sensörler ile SCADA sistemi arasındaki iletişimi sağlayan Uzak Uç Birimi
- Programlanabilir Mantıksal Denetleyici(PLC) ve RTU
- Denetim sistemini sahadaki cihazlara ve uzak uç birimlere bağlayan haberleşme altyapısı
- İnternet, kurum ağı ve çevrel bileşenler
- Ağ mimarisi(güvenlik duvarı, yönlendirici(router), anahtarlama cihazları(switch), VPN'ler)
- Bilgisayar güvenliği(sunucu ve iş istasyonu güvenliği)

İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

SCADA Sistemlerine Uygulanabilecek Güvenlik Çözümleri

- SCADA sistemine özel güvenlik politikaları oluşturmak ve uygulamak
- Kritik iletişimin en güvenli katmanda gerçekleşmesini sağlayacak şekilde katmanlı bir ağ topolojisi uygulamak
- Kurum ve SCADA ağları arasında mantıksal bir bölümleme uygulamak
- Kurum ve SCADA ağları arasında doğrudan trafiği önlemek için DMZ ağ mimarisini uygulamak
- Kritik bileşenlerin yedekli(redundant) olduğunu ve yedekli ağ içerisinde olduğunu denetlemek
- SCADA'nın çalışma sistemini bozmayacak şekilde kullanılmayan port ve servislerin engellenmesi
- SCADA ağ ve cihazlarına fiziksel erişimi kısıtlama

İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

SCADA Sistemlerine Uygulanabilecek Güvenlik Çözümleri

- SCADA kullanıcı haklarını rol tabanlı erişim kontrolü sistemine göre belirlemek
- SCADA kullanıcıları ve kurum ağı kullanıcıları için ayrı kimlik doğrulama sistemi uygulamak
- Zararlı yazılımın yayılmasını tespit etmek, önlemek ve zararlarını azaltmak gibi güvenlik süreçlerini uygulamak için saldırı tespit, anti-virüs ve dosya bütünlüğü kontrolü yazılımları ile güvenlik kontrollerini sağlamak
- Güvenli ağ protokollerini ve servislerini kullanmak. (https, snmpv3, sftp)
- SCADA trafiğini izleyerek anomalileri tespit etmek ve önlem almak.
- NAC çözümleri uygulamak, fiziksel port güvenliğini sağlamak.

İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

SCADA Sistemleri Network Yapılandırması

- SCADA sistemlerinde fiber optik, GSM, kiralık karasal hatlar, radyolink, radyofrekans veya uydu haberleşmeleri tercih edilebilir.
- Scada networkü oluşturulurken ilgili lokasyondaki data altyapısına göre en ideal network çözümüne karar vermek gerekmektedir.
- Scada sistemlerinin kritiklik durumuna göre network yedekliliği önem arz etmektedir.
- Güvenli haberleşme protokollerini destekleyen router ve yönetilebilir switchler ile haberleşme sağlanmalıdır.
- Cihaz konfigürasyonları eksiksiz yapılmalı default ayarlarla hiçbir cihaz sahada konumlandırılmamalıdır.

İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

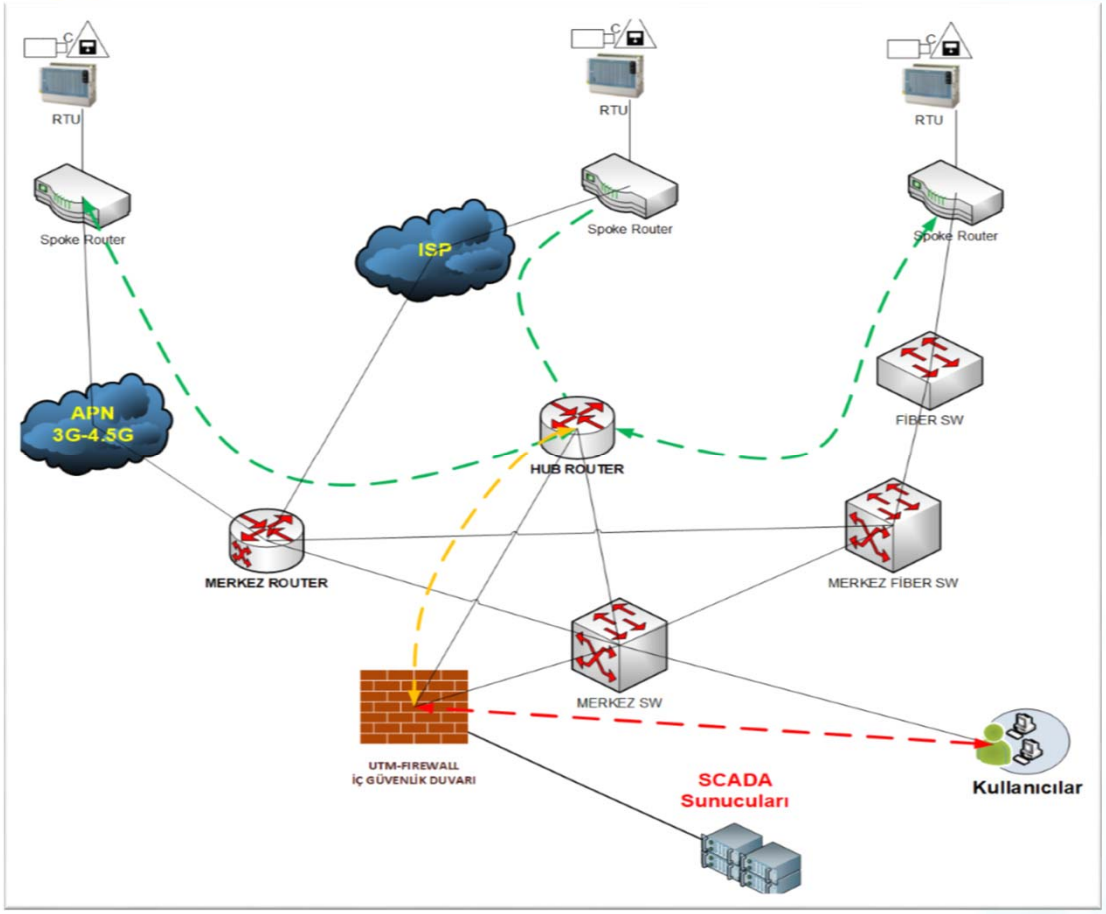
SCADA Networklerinde Karşılaşılan Zorluklar

- Güvenli bir network oluşturmak için gerekli olan network cihazlarının pahalı olması.
- Farklı Müdürlüklerin yaptığı ihalelerde aynı işi yapabilen çeşitli network ürünleri tarif etmeleri sonucunda farklı marka cihazların uyum sorunu.
- Kurulacak SCADA sistemlerine göre network tipi ve network cihaz çeşitliliğinin artması.
- SCADA Network trafiğinin izlenmesi ve anomalilerin tespitinde sıkı bir çalışma gerektirmesi.
- Teknik destek alınan firmalar ile Network ve Siber Güvenlik ekibinin yetkinliğinin istenilen düzeyde olmaması.

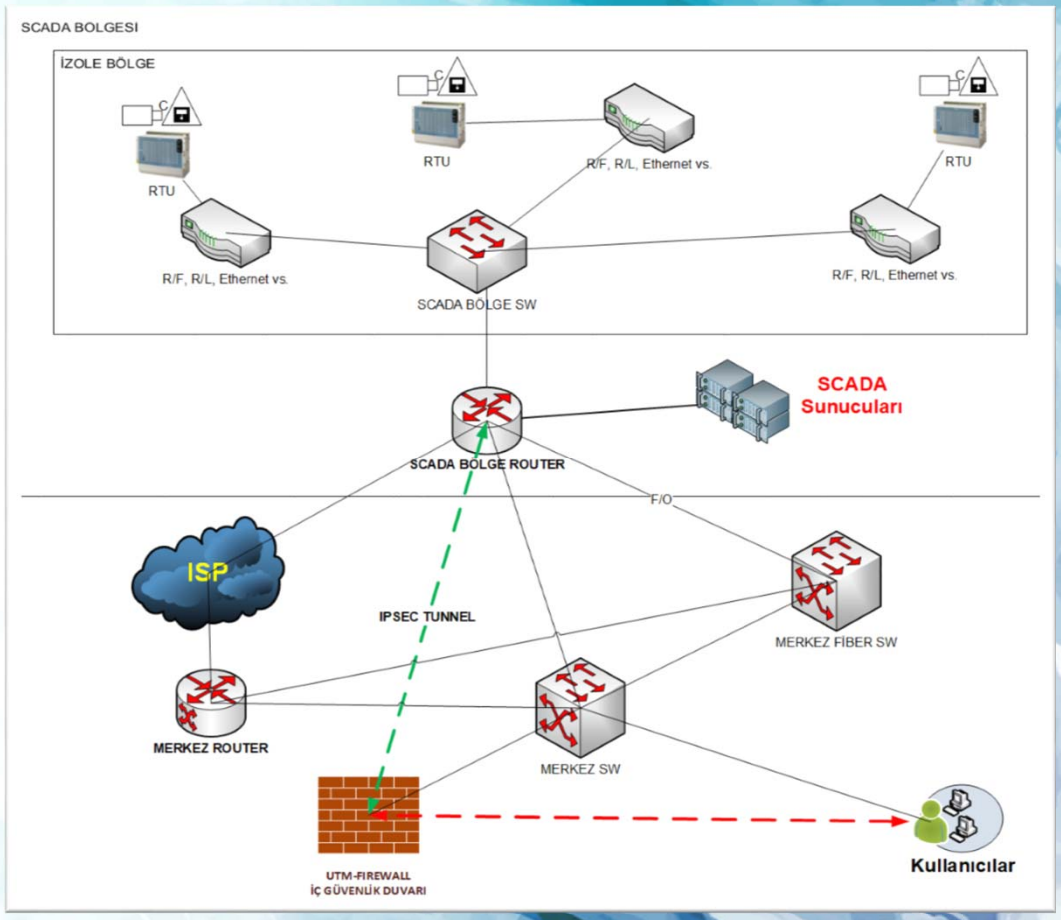
İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

SCADA'da Uygulanabilecek Network Çözümleri



HUB-Spoke Mimarisi



IPSEC Mimarisi

İSTANBUL SU VE KANALİZASYON İDARESİ
İSKİ

Örnek SCADA Sistemi

Sürekli Arıtılmış Su İzleme Sistemi (SASİS) Kabini

Şebekeye verilen suyun kalitesi online olarak izlenmektedir. İzlenen değerler;

- Klor
- Renk
- Bulanıklık
- Aleminyum
- Toplam Organik Karbon
- PH
- İletkenlik
- Çözünmüş Oksijen
- THM Kanserojen Madde

İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

Örnek SCADA Sistemi

THM Kanserojen Madde Kontrolü, Aleminyum

İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

Örnek SCADA Sistemi

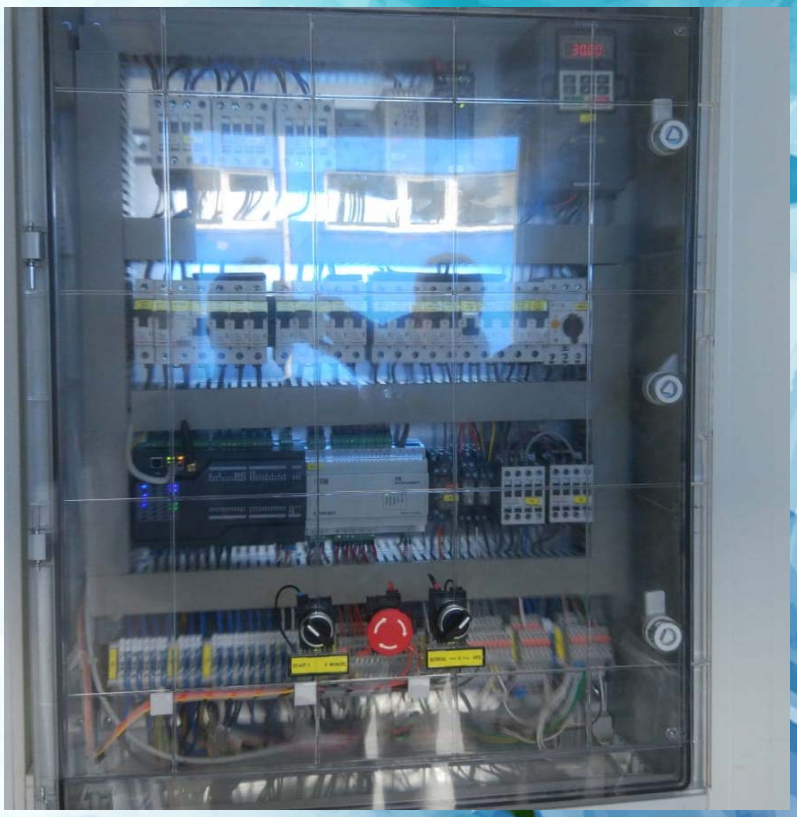
Şeffaf Numune Hattı, Ph, çözünmüş oksijen, iletkenlik ölçümleri

İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

Örnek SCADA Sistemi

Bulanıklık, Toplam Organik Carbon (TOC), renk

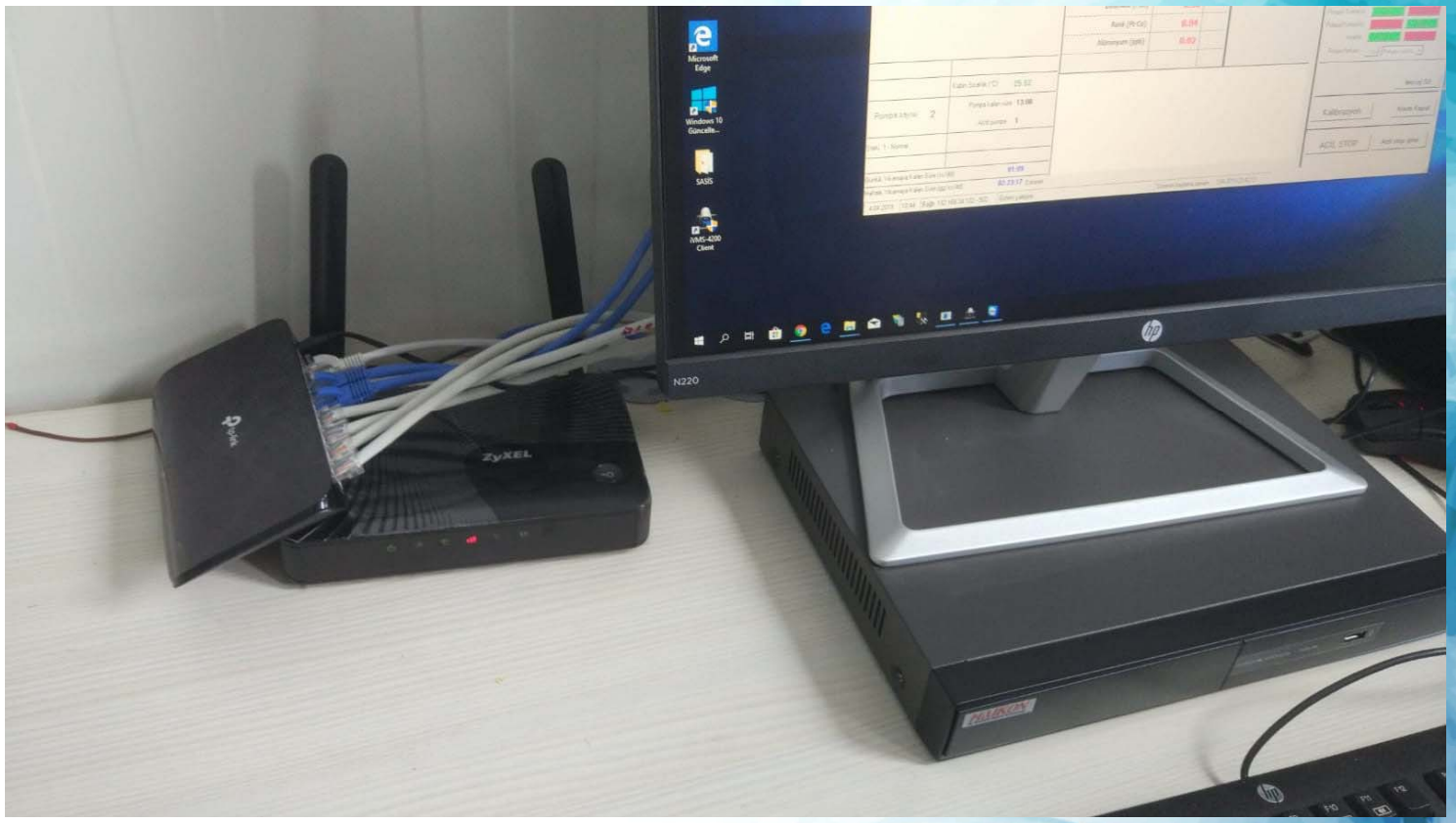


Otomasyon Panosu (Remote Terminal Unit)

İSTANBUL SU VE KANALİZASYON İDARESİ

İSKİ

Örnek SCADA Sistemi



PC, kamera ve network bağlantılarının bulunduğu kısım

İSTANBUL
SU VE KANALİZASYON
İDARESİ
İSKİ

TEŞEKKÜRLER...