

Nesnelerin İnterneti Güvenlik ve Güç Tüketimi

Özen Özkaya

24 MAYIS 2017

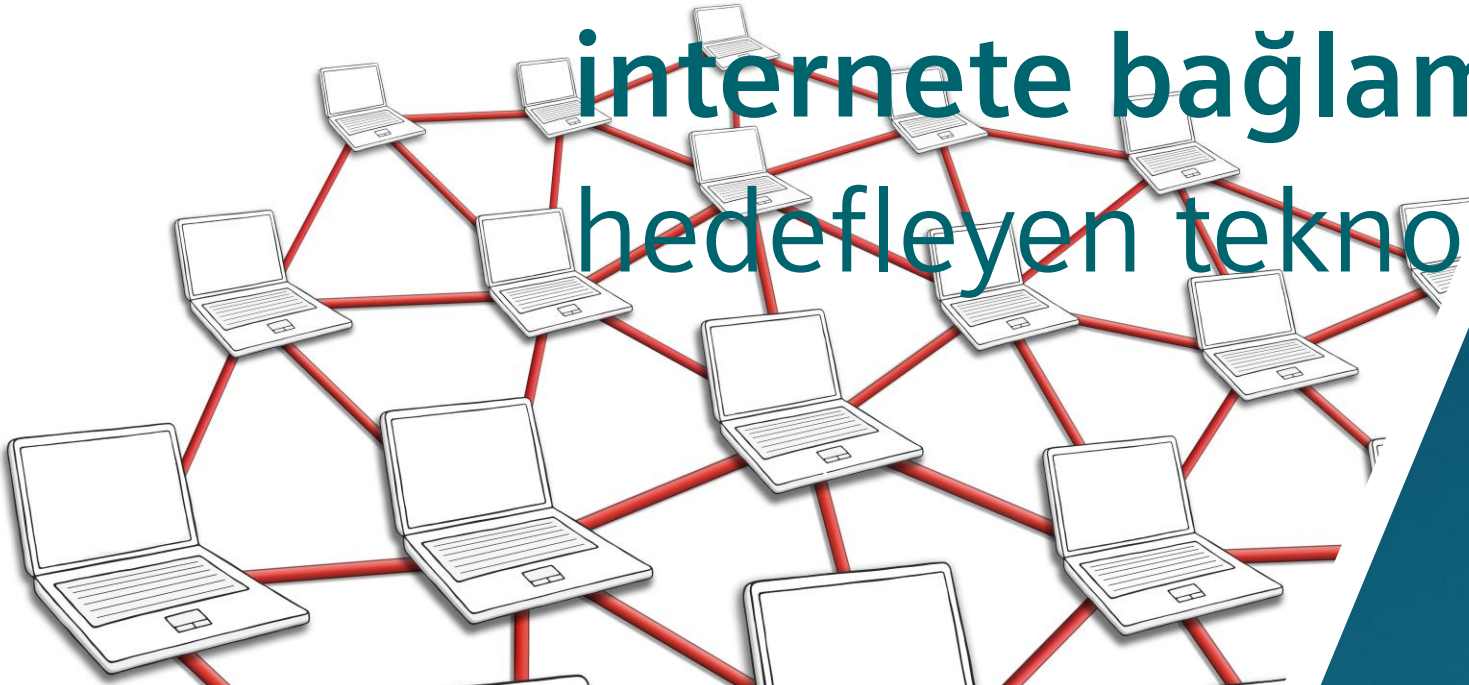
EMO SEMİNER DİZİSİ - 2



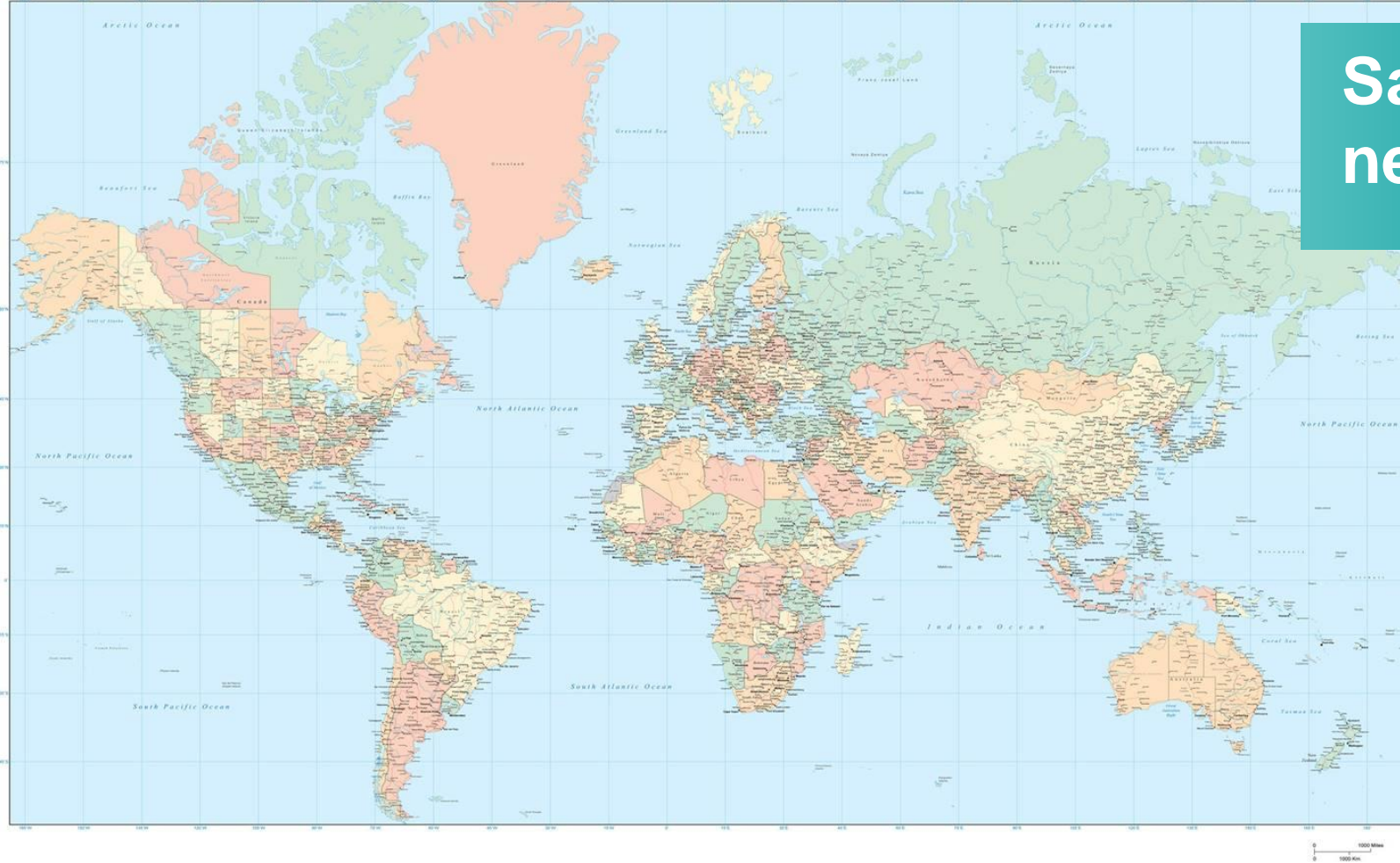
bilgisayarların
interneti...

**Nesnelerin interneti, 4.
sanayi devrimi ile ortaya
çıkan, tüm nesneleri**

**internete bağlamayı
hedefleyen teknolojidir.**



Keşfedilmemiş bir dünya: tam bağlı nesnelere!



Sahiden, tam bağlı nesnelere nedir?

Nesnelerin interneti (IoT) ile hedeflenen, tüm elektronik sistemlerin birbirine bağlanması ve bu elektronik sistemlerin arka planda birbirleriyle haberleşerek hayatı kolaylaştırmasıdır.

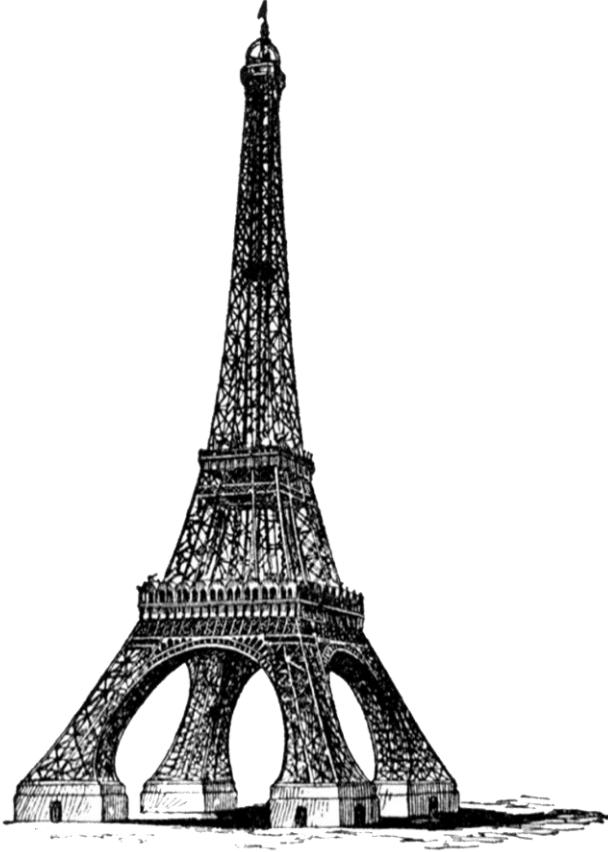
Başlamadan önce...
temelleri sağlamlaştırmak



İOT SİSTEMLERİ GÜVENİLİR VE GÜVENLİ Mİ?

Bir çok bakımdan; DEĞİL

Başlamadan önce...
temelleri sağlamlaştırmak



**IoT SİSTEMLERİ GÜVENİLİR VE GÜVENLİ
OLABILIR MI?**

Olmak ZORUNDA

Başlamadan önce...

istek listesi nedir

Tam bağlı	Kolay entegre olan
Ucuz	Güvenli
Düşük güç tüketimi	Güvenilir
Küçük	Stabil



The IoT is big news because it ups the ante: 'Reach out and touch somebody' is becoming 'reach out and touch everything'.

-
«Parker Trewin»

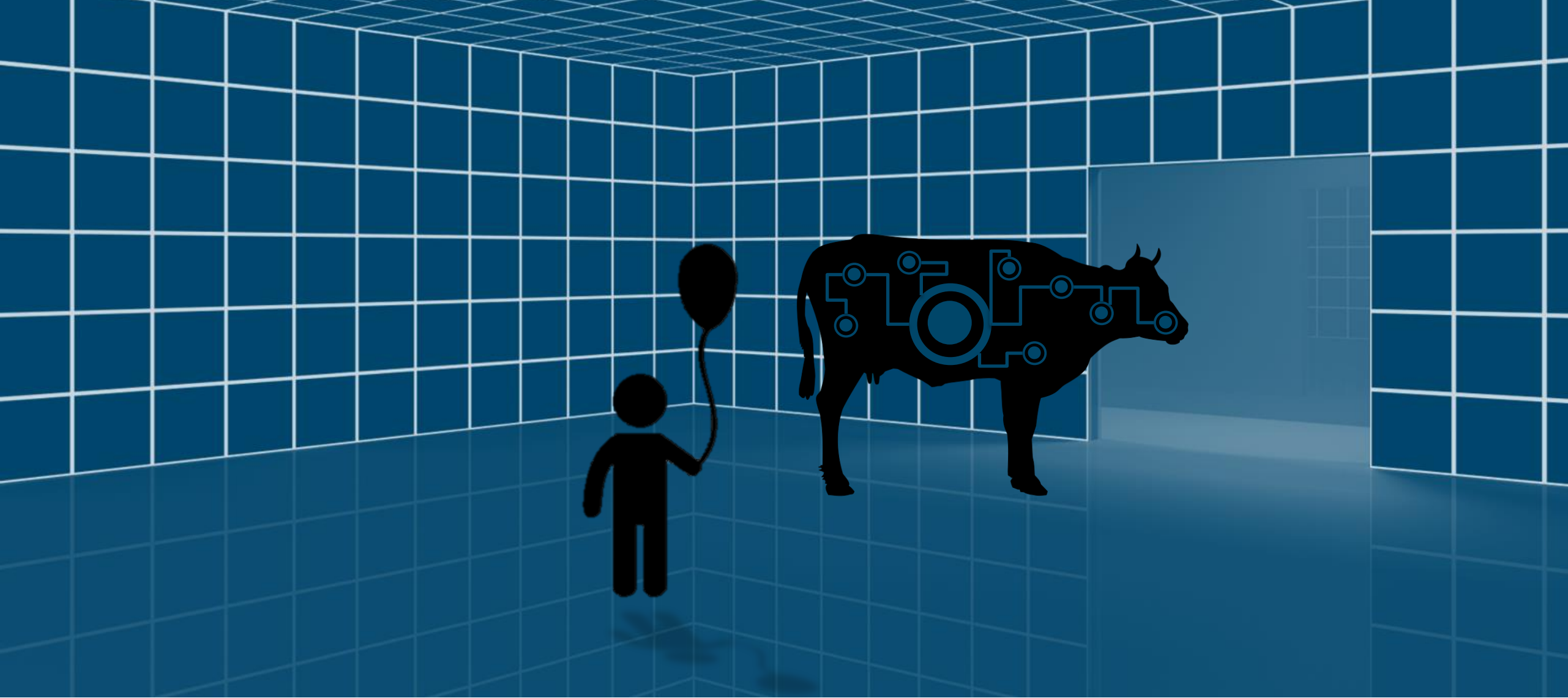
En büyük deęişim: İnsan 4.0!



İnsan 4.0 nedir?

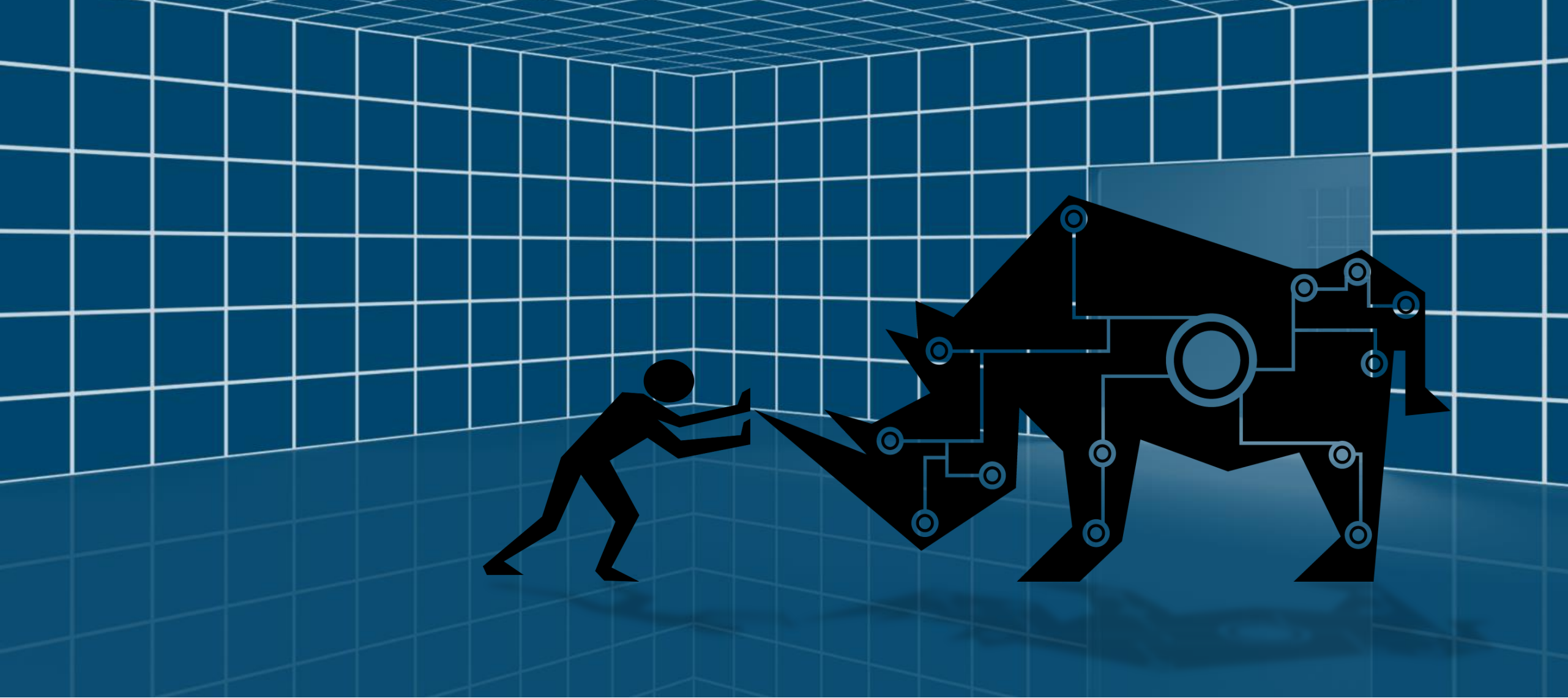
Endüstri 4.0 ve IoT ile gerçekleşen teknolojik devrimin, bu teknolojiyle yaşayacak insanları da deęiştireceęi açıktır.

Teknolojide tek bir sabit vardır:
DEĞİŞİM nedir?

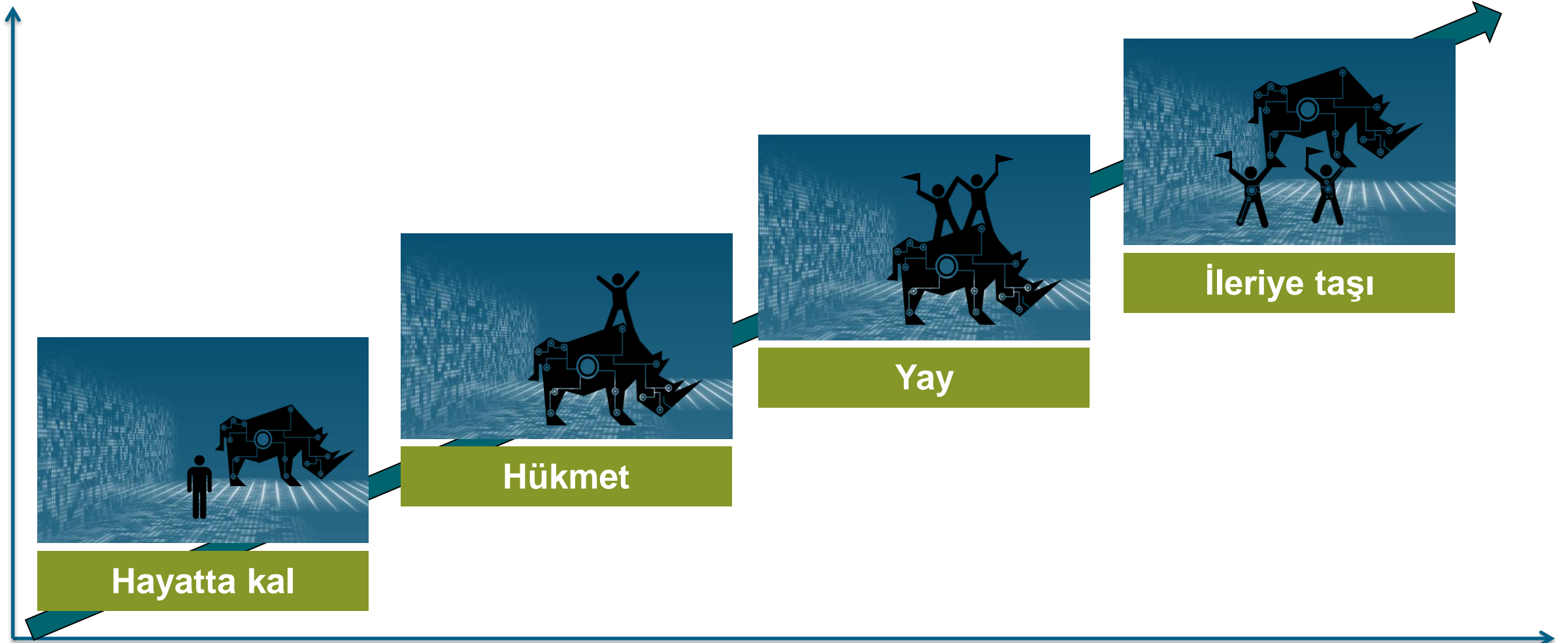


Değişimle savaşarak bir yere varamayız...

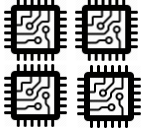
Onu **YÖNETMELİYİZ.**



Nesnelerin internetine giden yolda...



IoT, klasik internetin tüm özelliklerini miras alır. Ancak bazı farklarla...



Cihaz, hem de çok sayıda



Uzun pil ömrü veya çalışma süresi



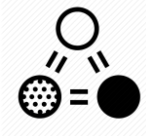
Nadir güncelleme sıklığı



Küçük cihazlar



Kişisel veriler, hiç olmadığı kadar çok



Cihaz çeşitliliği çok fazla

IoT sistemlerinde mimari hedefler

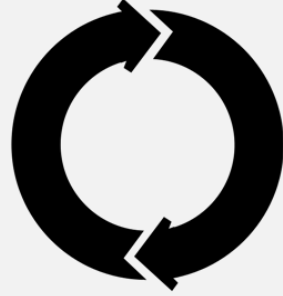
Nesnelerin İnterneti	Düşük maliyetli	Az yer kaplayan	Az güç harcayan	Birlikte işlerliği olan
Güvenlik ve mahremiyet	Bellek efektif	Modüler	Genişletilebilir	Performanslı
Endüstri 4.0	Fonksiyonel	Güvenli	Ölçülebilir	Taşınabilir
Gömülü Sistemler	Yeniden Yapılandırılabilir	Hata toleranslı	Sınanabilir	Ölçeklenebilir

Güvenilir ve güvenli olmayan bir sistem kullanılabilir değildir.

Ölçeklenebilir



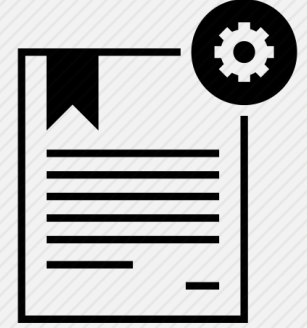
Uçtan uca



Sistem seviyesinde



Standart



Ataklara dayanıklı



Adaptif



Düşük güçlü



Uyumlu

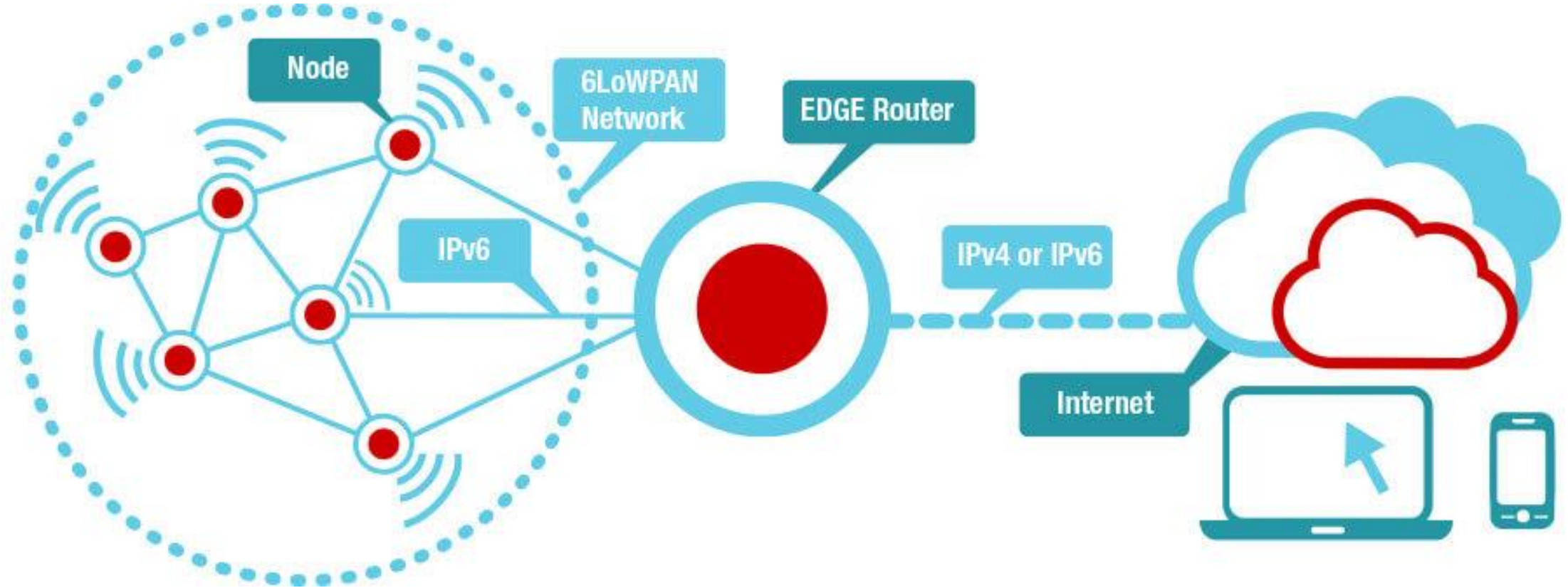


Akademi ne diyor...

- IoT'de karşımıza çıkan, benzeri görülmemiş bağlantı çeşitliliği ve sayısı neticesinde ortaya çıkan güvenlik zafiyetleri de benzersizdir. (Folk vd., 2015)
- Hewlett Packard tarafından 2014 yılında yürütülen çalışmaya göre mevcut zamanda var olan IoT cihazlarının 70%'i ciddi güvenlik zafiyetleri barındırmaktadır. (Lee & Lee, 2015)
- IoT doğası gereği heterojen ve çok katmanlı bir ağ yapısına sahiptir. Her bir katman için çok sayıda güvenlik kriteri ve çözümü olmakla birlikte, katmanlar arasındaki etkileşimlerde, ve heterojen ağların etkileşimlerinde çok sayıda yeni güvenlik açıkları ortaya çıkmıştır. (Jing vd., 2014).



IoT bileşenleri



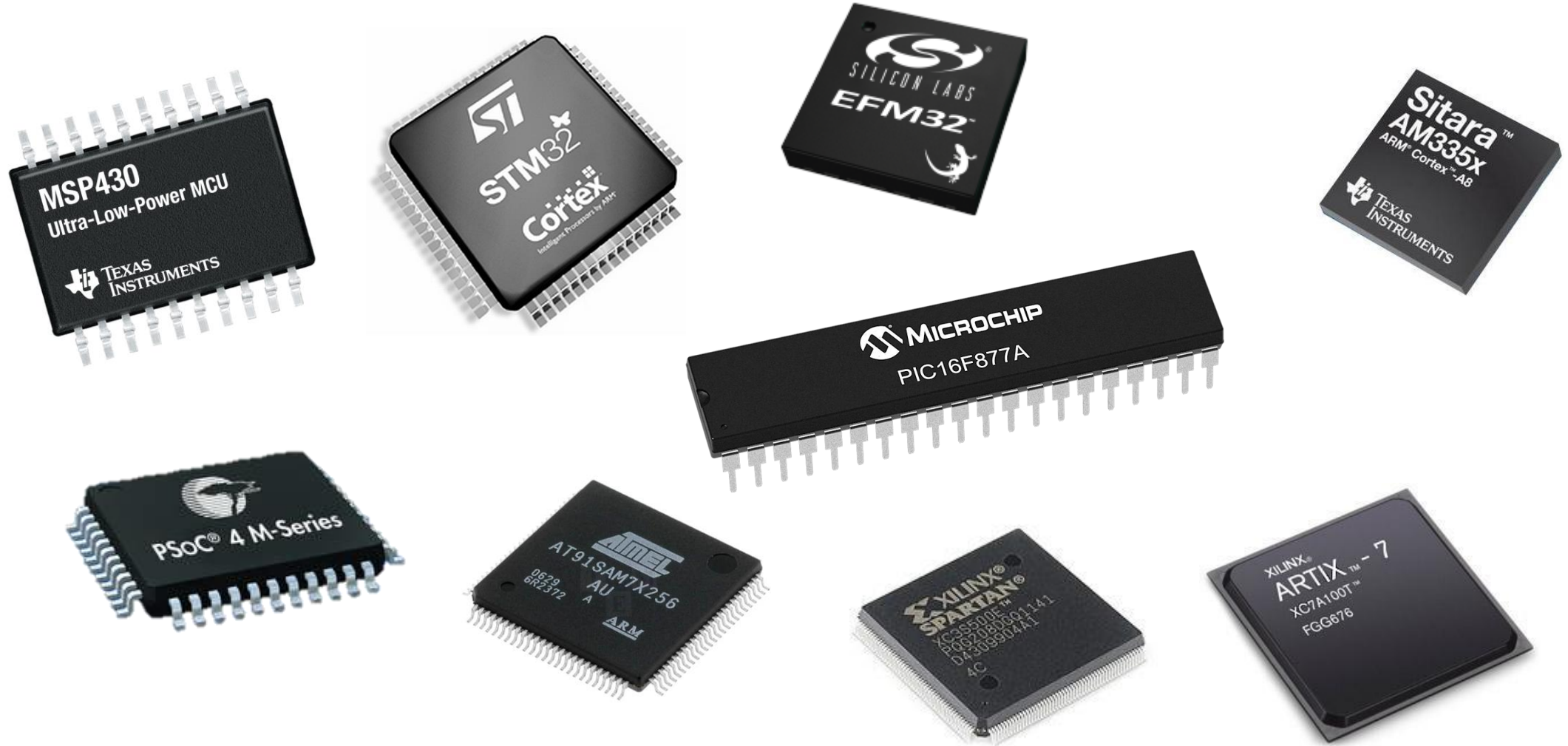
IoT'nin beyni: BULUT



Bulut güvenliđi

Nesnelerin interneti (IoT) düđümlerinden gelecek veriler çođunlukla bulut ortamlarında işlenip bilgiye dönüştürülür. Bilgi güvenliđi için bulut ortamı muhakkak güvenli olmalıdır.

IoT düğümlerinin hayat bulduğu beden; gömülü sistemler



Güvenli IoT düğümleri için işletim sistemleri



NodeMCU



ANDROID

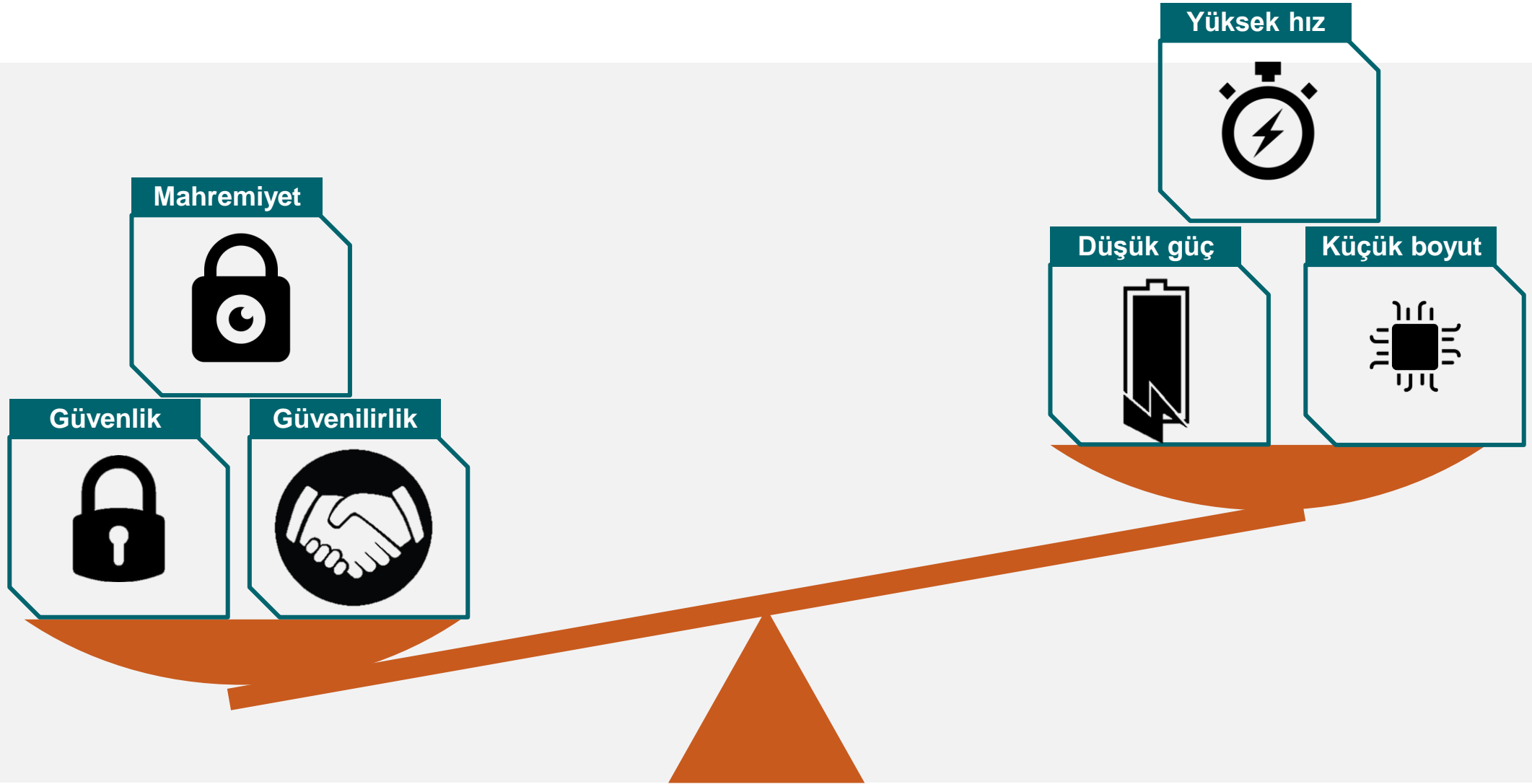


ARM[®]mbed[™]



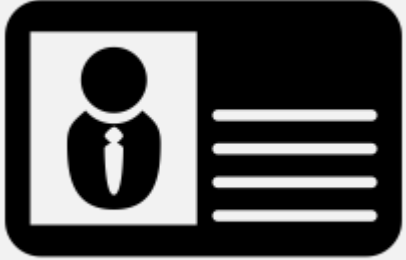
Contiki

IoT güvenlik dengesi



Güvenlik ve mahremiyet eksenleri

Kimliklendirme



Kimlik doğrulama



Yetkilendirme



Gizlilik



Ataklara dayanıklı



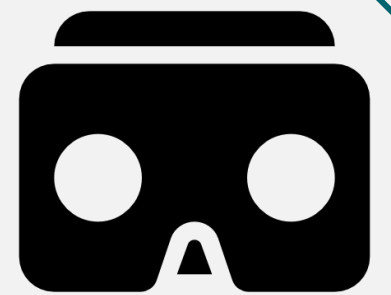
Şifreleme



Tamlık



Gerçeklik



Güvenli IoT düğümleri için yol haritası

İP No	İş Paketi Hedefi	Başarı Ölçütü (%, sayı, ifade, vb.)
1	Literatür analizi	IoT sistemlerinde güvenlik ihtiyaçlarının güncel durumunun belirlenmesi.
2	Güvenli donanım platformunun araştırılması ve bulunması.	Donanım bileşenlerinin güvenli olması.
3	Donanım platformunun güvenliğinin sınanması ve sistem seviyesinde modellenmesi.	Çalışan devrenin ortaya çıkması. (Kontrol, algılama ve haberleşme üniteleri dahil).
4	Sistemsel ve mimari gereksinimlerinin belirlenmesi	Enterprise architect de gereksinim tablolarının oluşturulması
5	Sistemin Enterprise Architect'de UML modeli.	Durum akış, sıralama, senaryo diyagramlarının, fonksiyonel ve mimari modellerin elde edilmesi
6	Kriptografi algoritmalarının çeşitli implementasyonları	Simetrik, asimetrik ve özet fonksiyonu kriptografik algoritmaların yan kanal analizlerine karşı güvenli yazılmış donanım veya yazılım kodları
7	Contiki işletim sisteminin güvenli donanım platformuna port edilmesi	İşletim sisteminin ve sürücülerin çalışır hale getirilmesi
8	IoT düğümü üzerine kurulacak ağlar için gerekli yazılım paketi, sürücü ve standart ağ protokollerinin, IoT düğümüne aktarılması.	Güvenli IoT sisteminin, ağ kurulumlarına hazır hale gelmesi.
9	Tasarım blokları kullanılarak, güvenli nesnelerin interneti ağının tasarımı ve gerçekleştirilmesi	Güvenli IoT sisteminin tasarımı ve gerçekleştirilmesi
10	Sistem modelinin fonksiyonel, performans analizleri	Enterprise architect ve Cooja ortamında de yapılacak analizler
11	Nesnelerin interneti ağının güvenlik test sonuçları	Gerçeklenen düğümün IoT ölçüm ve test düzeneğinde kullanılması ve testlerin gerçekleştirilmesi

**DİNLEDİĞİNİZ İÇİN
TEŞEKKÜRLER!**



Özen Özkaya

--

Proje Yöneticisi

Siemens San. ve Tic. A.S.
CT DD DS EU TR CP CD 2
Yakacik Caddesi No 111
34870 Istanbul, Türkiye
Mobil: +90 530 0476515
ozen.ozkaya@siemens.com