SECURITY 4.0

Kaip saugos technologijas keičia 4-oji pramonės revoliucija

Dr. Arūnas Kazlauskas

11-oji Lietuvos asmens ir turto saugos specialistų konferencija

2019.11.21

SECURITY 4.0

Keturios pramonės revoliucijos

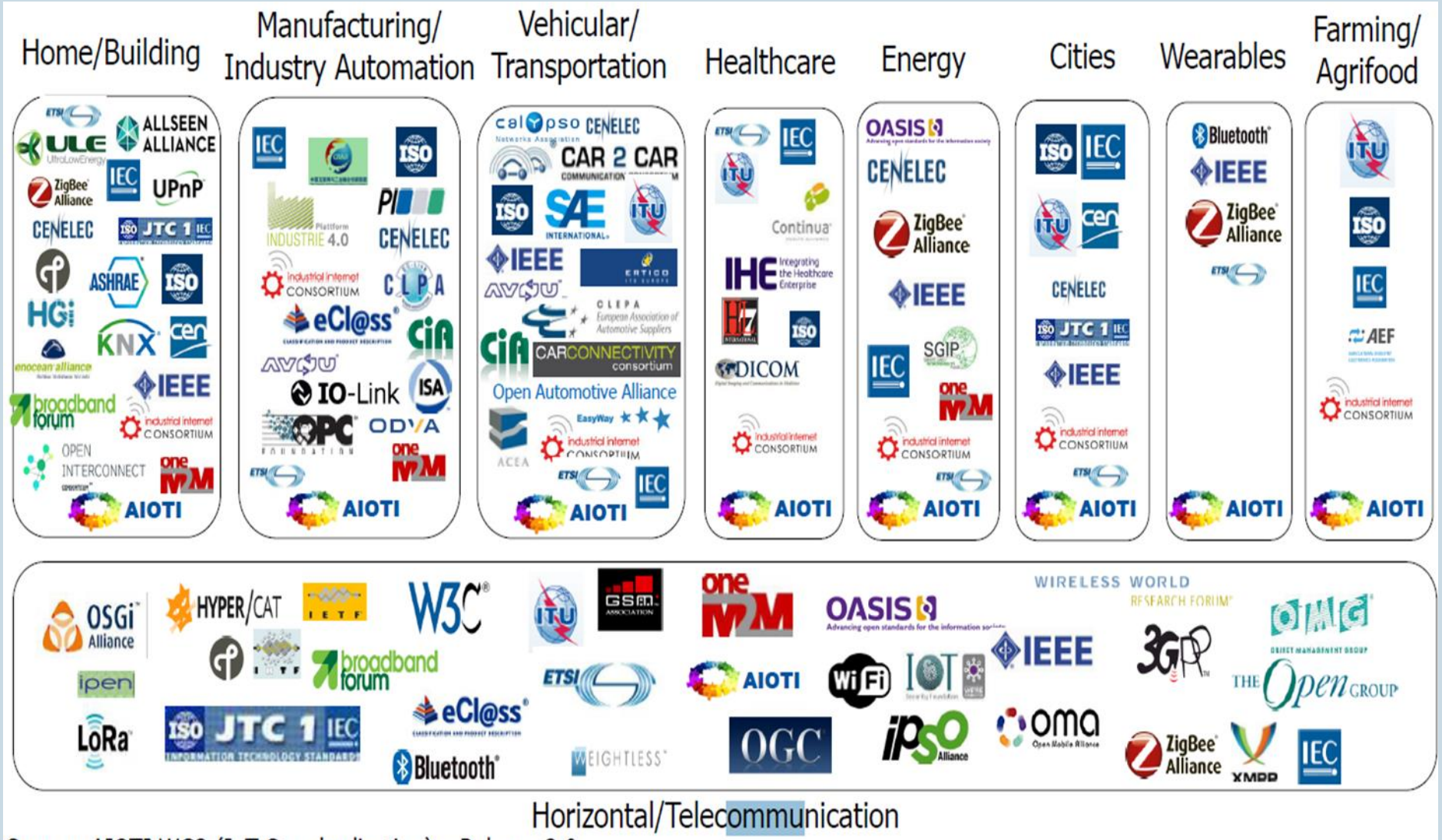
- 1-oji: rankų darbo pakeitimas mechaniniu.
- 2-oji: elektros atradimas ir kiti išradimai, leidę pradėti masinę prekių gamybą.
- 3-oji: kompiuterių atsiradimas ir įsigalėjimas, automatizacijos ir robotizacijos pradžia, interneto įsigalėjimas (e-anything) ir t.t.
- 4-oji: aplinka, kurioje gyvename šiandien.

SECURITY 4.0

Kurios sritys išsivystė 4-osios pramonės revoliucijos dėka:

- Procesų automatizacija.
- Robotizacija.
- Daiktų internetas (IoT).
- Visuotinis mobilumas ir prisijungimas (4G and 5G mobility and connectivity).
- Didžiųjų duomenų ekosistemos (BigData).
- Dirbtinis intelektas (AI).
- Mašininis (ML) ir gilusis mokymasis (DL), dirbtiniai neuroniniai tinklai (ANN).
- Virtualioji ir papildytoji realybė (VR ir AR).
- Debesų kompiuterija.
- Socialiniai tinklai.

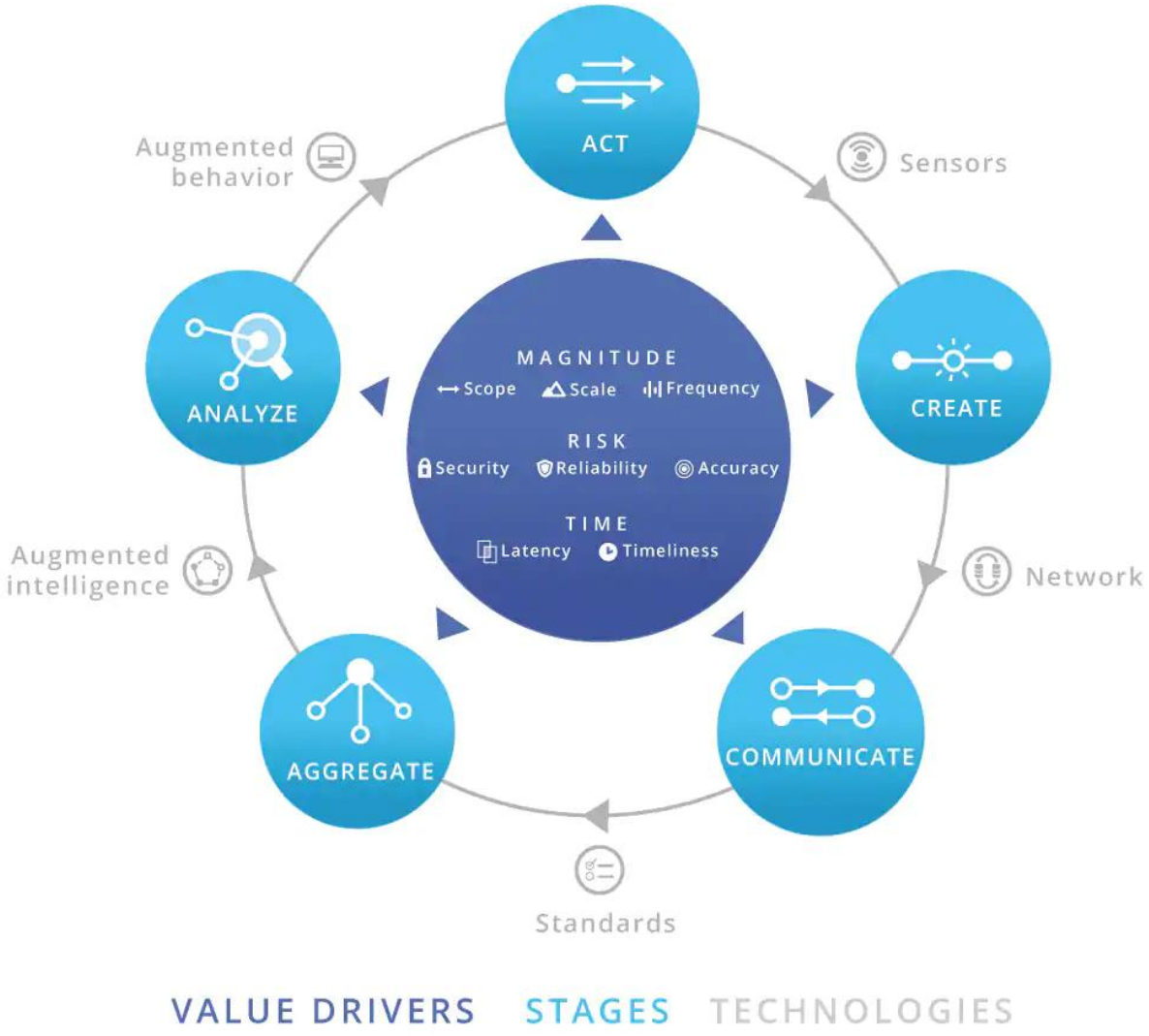
SECURITY 4.0



Source: AIOTI WG3 (IoT Standardisation) – Release 2.0

SECURITY 4.0

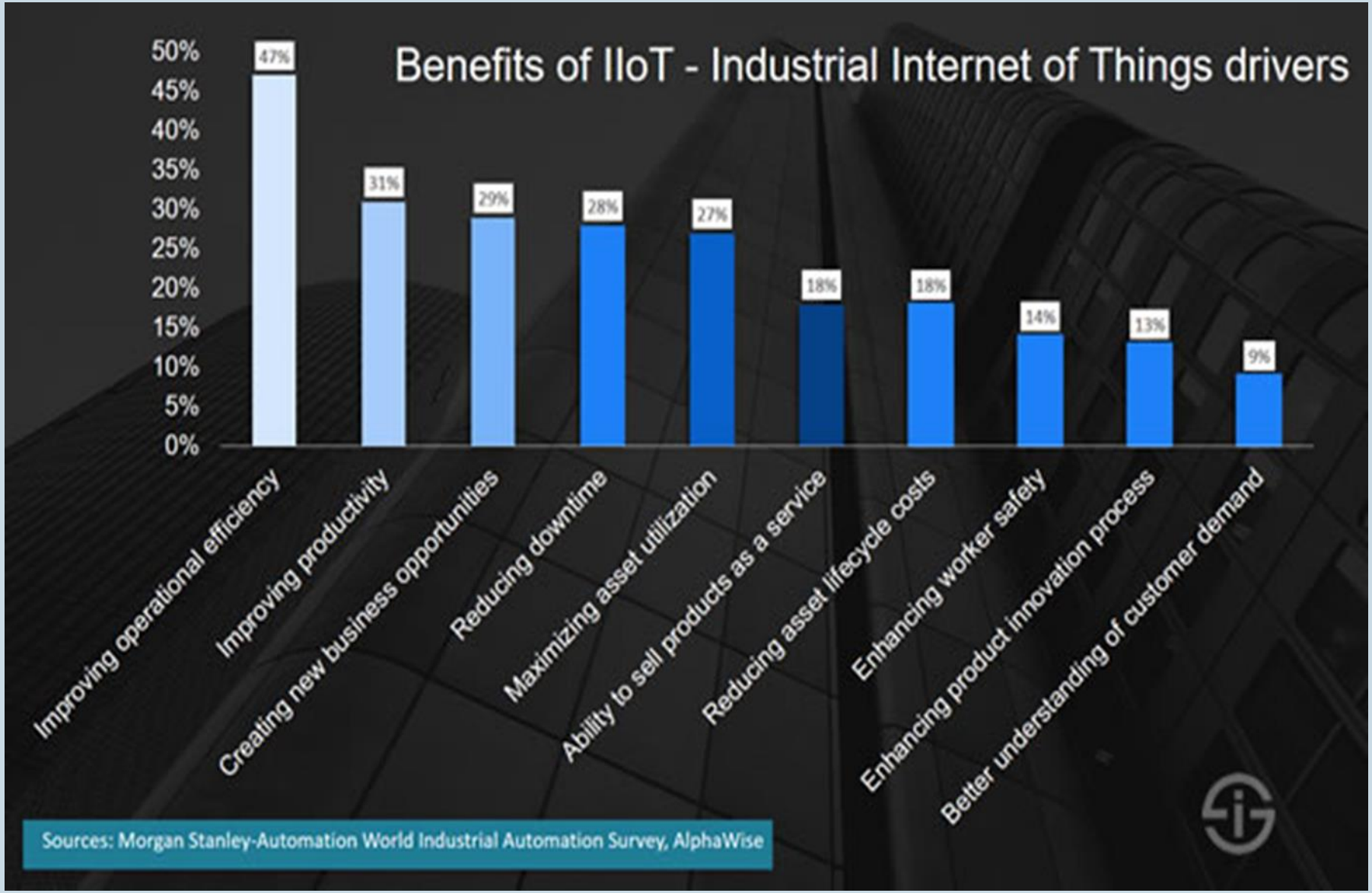
Figure 3. The Information Value Loop



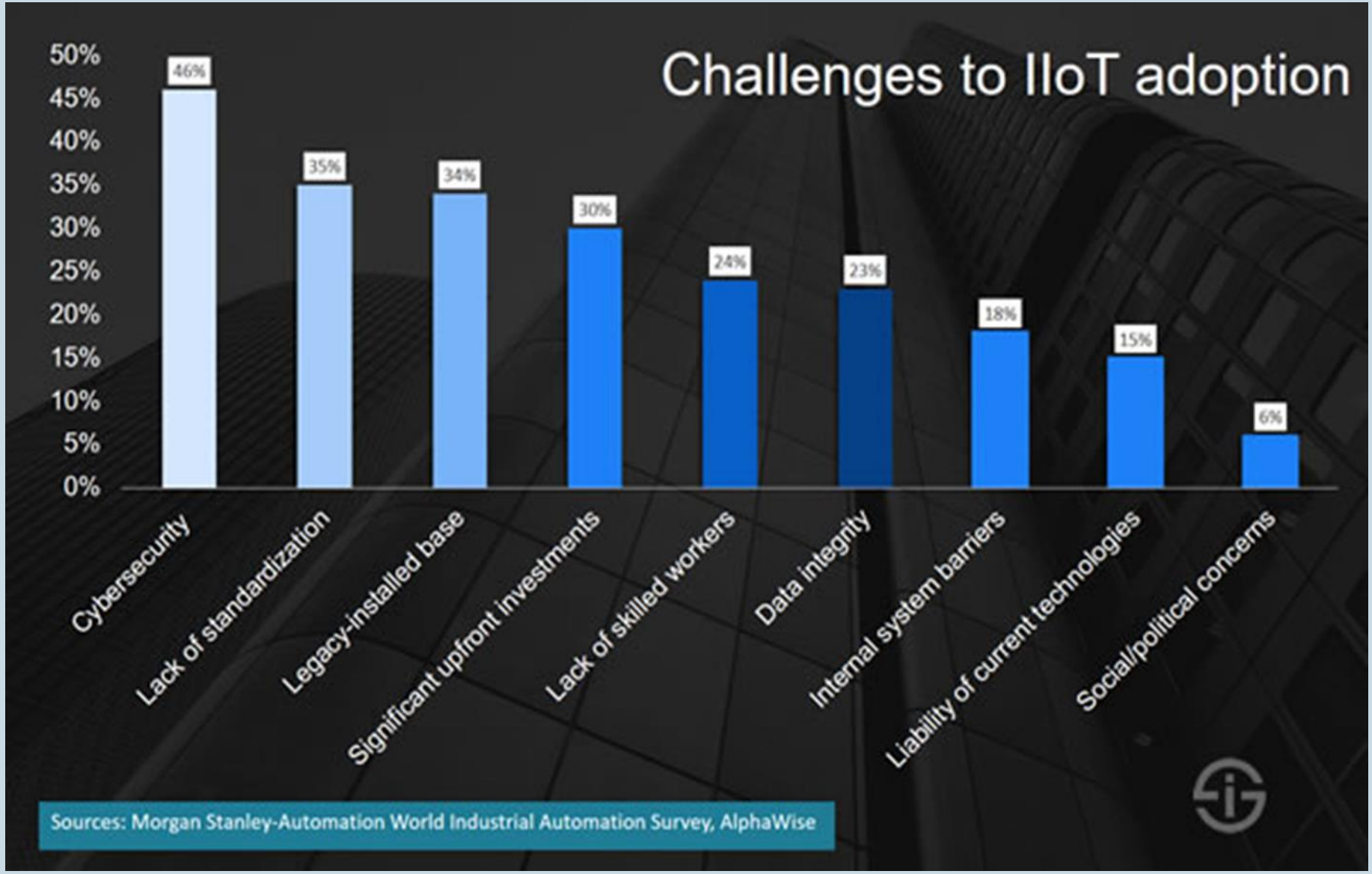
Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

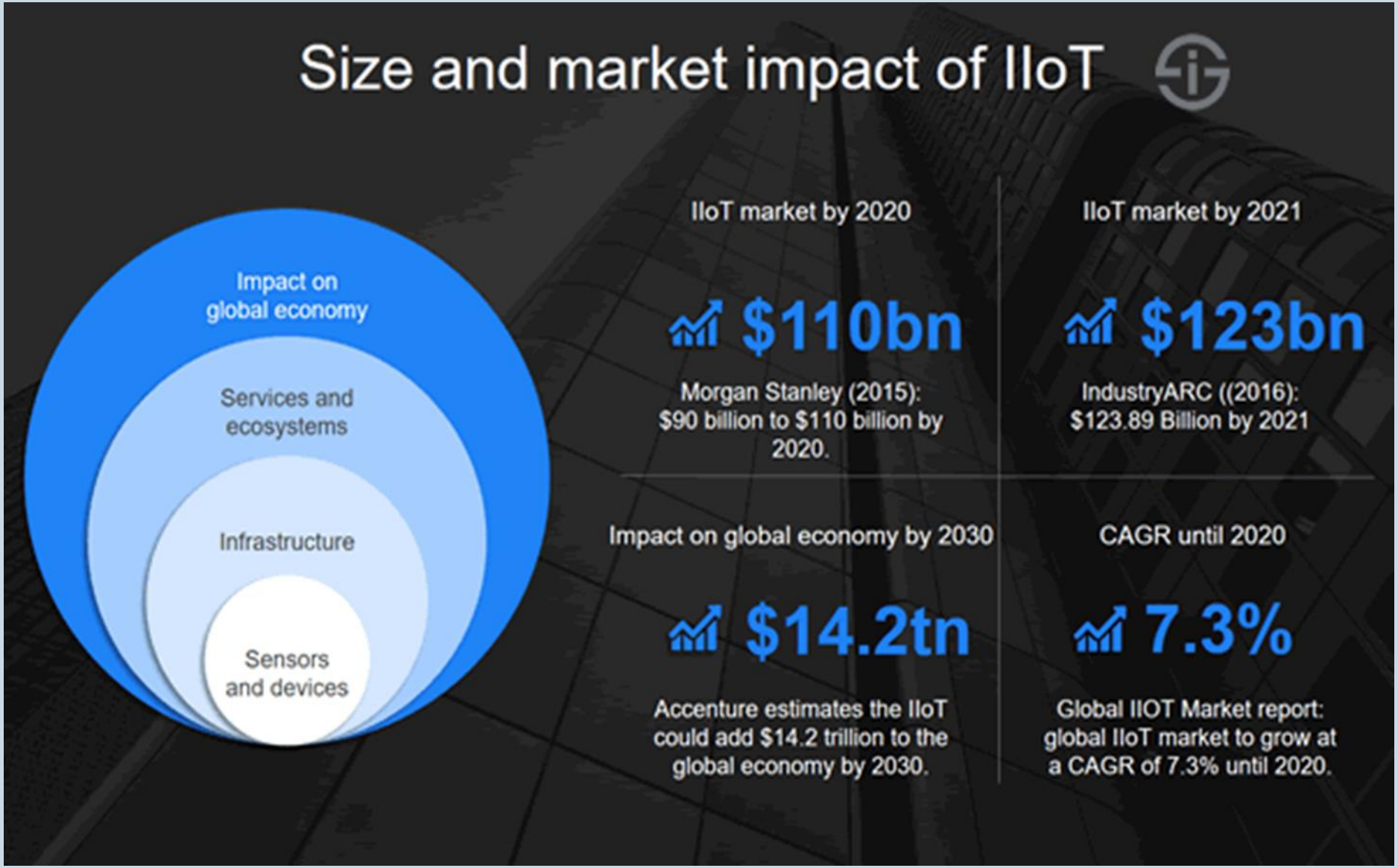
SECURITY 4.0


Benefits of IIoT - Industrial Internet of Things drivers
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
47%
31%
29%
28%
27%
18%
18%
14%
13%
9%
Improving operational efficiency
Improving productivity
Creating new business opportunities
Reducing downtime
Maximizing asset utilization
Ability to sell products as a service
Reducing asset lifecycle costs
Enhancing worker safety
Enhancing product innovation process
Better understanding of customer demand
Sources: Morgan Stanley-Automation World Industrial Automation Survey, AlphaWise

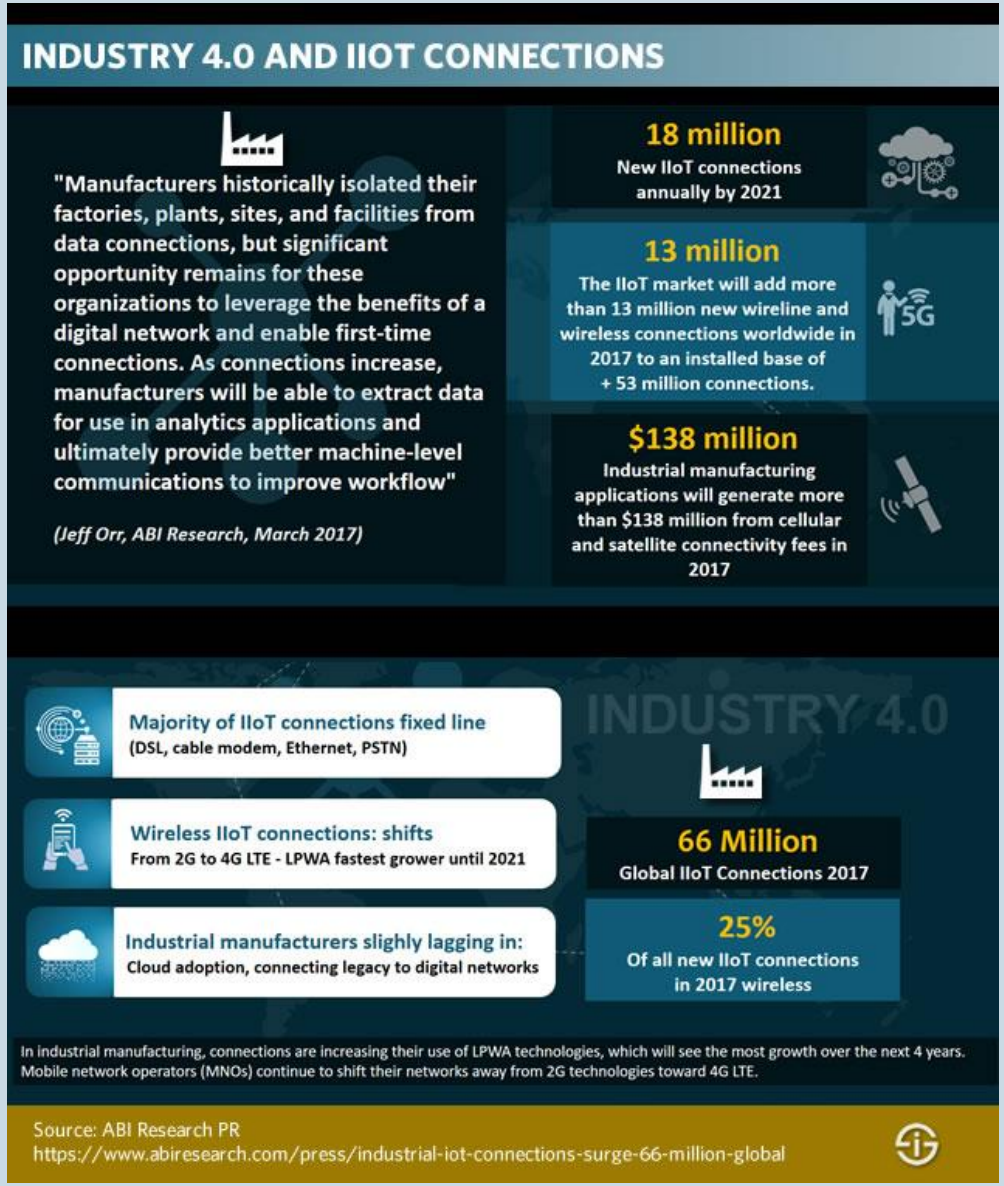
SECURITY 4.0


Challenges to IIoT adoption
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
46%
35%
34%
30%
24%
23%
18%
15%
6%
Cybersecurity
Lack of standardization
Legacy-installed base
Significant upfront investments
Lack of skilled workers
Data integrity
Internal system barriers
Liability of current technologies
Social/political concerns
Sources: Morgan Stanley-Automation World Industrial Automation Survey, AlphaWise

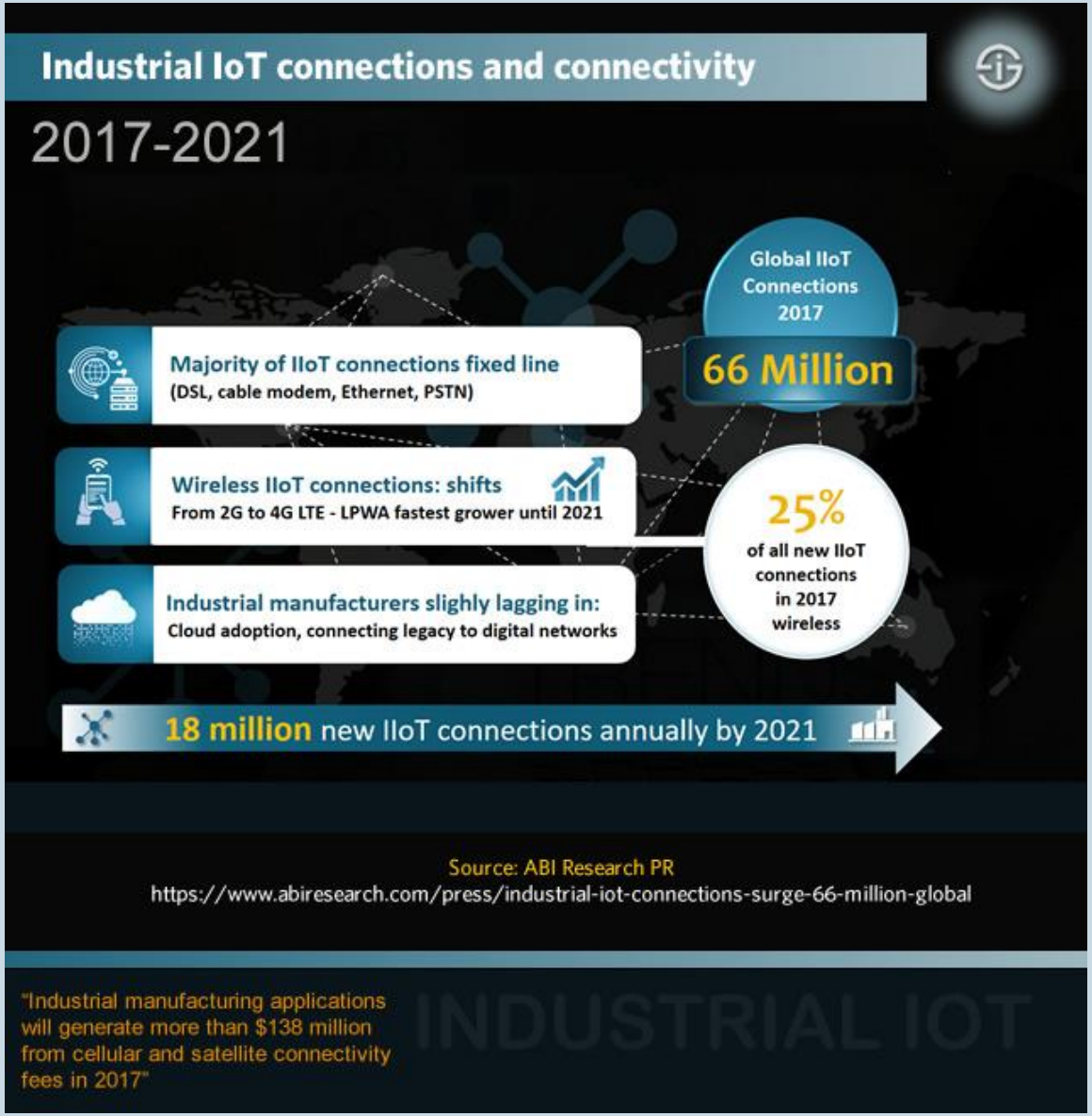
SECURITY 4.0


Size and market impact of IIoT
Impact on global economy
Services and ecosystems
Infrastructure
Sensors and devices
IIoT market by 2020
$110bn
Morgan Stanley (2015): $90 billion to $110 billion by 2020.
IIoT market by 2021
$123bn
IndustryARC ((2016): $123.89 Billion by 2021
Impact on global economy by 2030
$14.2tn
Accenture estimates the IIoT could add $14.2 trillion to the global economy by 2030.
CAGR until 2020
7.3%
Global IIOT Market report: global IIoT market to grow at a CAGR of 7.3% until 2020.

SECURITY 4.0


INDUSTRY 4.0 AND IIOT CONNECTIONS
"Manufacturers historically isolated their factories, plants, sites, and facilities from data connections, but significant opportunity remains for these organizations to leverage the benefits of a digital network and enable first-time connections. As connections increase, manufacturers will be able to extract data for use in analytics applications and ultimately provide better machine-level communications to improve workflow"
(Jeff Orr, ABI Research, March 2017)
18 million
New IIoT connections annually by 2021
13 million
The IIoT market will add more than 13 million new wireline and wireless connections worldwide in 2017 to an installed base of + 53 million connections.
5G
$138 million
Industrial manufacturing applications will generate more than $138 million from cellular and satellite connectivity fees in 2017
Majority of IIoT connections fixed line
(DSL, cable modem, Ethernet, PSTN)
Wireless IIoT connections: shifts
From 2G to 4G LTE - LPWA fastest grower until 2021
Industrial manufacturers slighly lagging in:
Cloud adoption, connecting legacy to digital networks
INDUSTRY 4.0
66 Million
Global IIoT Connections 2017
25%
Of all new IIoT connections in 2017 wireless
In industrial manufacturing, connections are increasing their use of LPWA technologies, which will see the most growth over the next 4 years. Mobile network operators (MNOs) continue to shift their networks away from 2G technologies toward 4G LTE.
Source: ABI Research PR
https://www.abiresearch.com/press/industrial-iot-connections-surge-66-million-global

SECURITY 4.0


Industrial IoT connections and connectivity
2017-2021
Global IIoT Connections 2017
66 Million
Majority of IIoT connections fixed line
(DSL, cable modem, Ethernet, PSTN)
Wireless IIoT connections: shifts
From 2G to 4G LTE - LPWA fastest grower until 2021
25%
of all new IIoT connections in 2017 wireless
Industrial manufacturers slighly lagging in:
Cloud adoption, connecting legacy to digital networks
18 million new IIoT connections annually by 2021
Source: ABI Research PR
https://www.abiresearch.com/press/industrial-iot-connections-surge-66-million-global
"Industrial manufacturing applications will generate more than $138 million from cellular and satellite connectivity fees in 2017"
INDUSTRIAL IOT

SECURITY 4.0

SECURITY 4.0

Dirbtinis intelektas saugos technologijose turi daug potencialo sustiprinti daugelį saugos sistemų komponentų:

- Vaizdo stebėjimo sistemos – įvairi vaizdo duomenų analitika ir veiksmų algoritmai.
- Patekimo kontrolės sistemos – vidinių rizikų valdymas ir prognozavimas.
- Įėjimo taškų kontrolė – lankytojų srautų valdymas.
- Perimetro apsauga – nutolusių vietų stebėjimas ir saugojimas.
- Savavaldės transporto priemonės ir dronai – pavojingų vietų stebėjimas ir pasiekiamumas.
- Specializuoti robotai – veiksmai žmogui nepasiekiamose ir pavojingose vietose ir situacijose.
- Ryšių tinklai – visų integruotų saugos sistemų pagrindas.
- Programinė įranga – visų saugos ir pastatų gyvybės palaikymo sistemų sujungimo platforma.

SECURITY 4.0

SECURITY 4.0

Dirbtinio intelekto naudojimo saugos technologijose iššūkiai ir pasekmės:

- Robotai keičia žmones.
- Realizuojami specialaus, bet ne bendrojo, dirbtinio intelekto sprendiniai:
  - *Vaizdo signalų analitika.*
  - *Biometrinių duomenų naudojimas.*
  - *Socialinio elgesio analitika.*
- Savavaldžių transporto priemonių (antžeminių, povandeninių ir orinių) įgalinimas.
- Asmens duomenų problematika, naudojant vaizdo stebėjimo ar biometrines sistemas.
- Skaitmeninio saugumo problematika (*cybersecurity*).

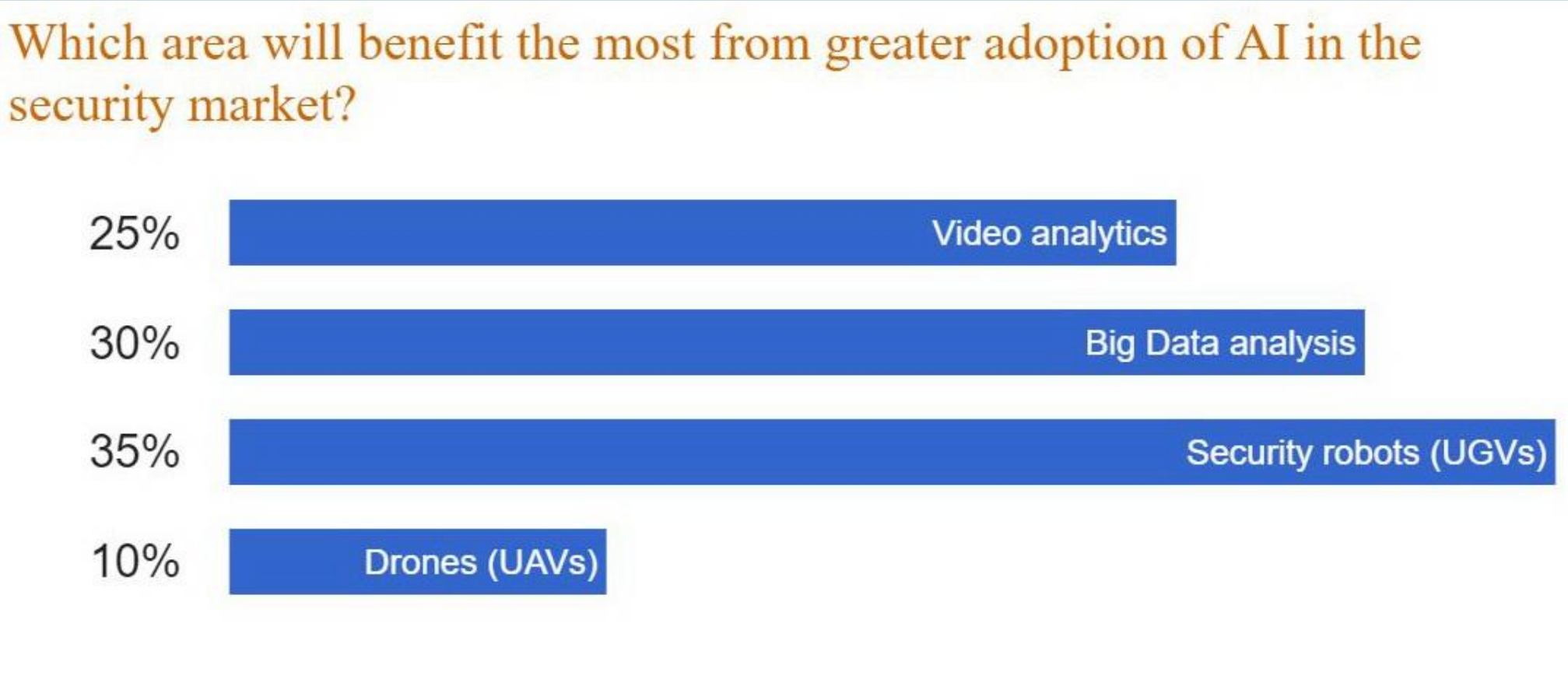
SECURITY 4.0

Dirbtinio intelekto naudojimo saugos technologijose grėsmės:

- <u>Vaizdo kameros nėra gerai apsaugotos</u>
- Žiniasklaidos pranešimų apie saugos sistemų skaitmeninį pažeidžiamumą pavyzdžiai:

- 4/14: Hackers turn security camera DVRs into Bitcoin makers https://goo.gl/yrvstv & **Hikvision** devices open to hackers https://goo.gl/PtHq7r
- 2/16: Cameras reported to “phone home to China” with your video https://goo.gl/MWJ35T
- 9/16: DDoS on *KrebsOnSecurity.com* & OHV DNS service uses 140,000+ network cameras & DVRs https://goo.gl/Df4Mkr
- 10/16: DDoS on 85 web services including Amazon, Financial Times, Netflix, PayPal, Spotify, & Twitter suspected to have included many IoT (Internet of Things) devices from cameras to appliances for loss of $100M https://goo.gl/P7nW46
- 11/16: **Hikvision** cameras reported to send their data to China after being plugged in, Chinese government can access installed cameras when they want https://goo.gl/QAzl04
- 11/16: Security camera infected by malware 98 seconds after plugged in https://goo.gl/QAzl04
- 1/17: 70% of Washington, DC police video cameras & 123 of 187 NVRs hijacked by ransomware attack, days before Trump Presidential Inauguration https://goo.gl/NkuKGW; DC and South Dallas cyberattacks https://goo.gl/Xmhlhr
- 3/17: Why **Genetec** sees **Hikvision** products as security risks http://tinyurl.com/ls44ygl
- 3/17: **Dahua**, **Hikvision** IoT Devices Under Siege https://goo.gl/sO9snH
- 4/17: **Dahua** Devices Dangerously Exposed to Cybersecurity Hack http://tinyurl.com/jxjlc8w

SECURITY 4.0


Which area will benefit the most from greater adoption of AI in the security market?
25%
Video analytics
30%
Big Data analysis
35%
Security robots (UGVs)
10%
Drones (UAVs)

SECURITY 4.0

Dirbtinio intelekto naudojimo saugos technologijose galimi taikymai:

- Gyvenamųjų namų ir jų gyventojų sauga.
- Didelių žmonių srautų viešose vietose ir renginiuose valdymas.
- Didelių ir nutolusių teritorijų stebėjimas.
- Išmaniojo miesto sprendiniai (situacijų valdymo centrai).
- Krašto gynybos (pasienis, strateginiai objektai) sprendiniai.

SECURITY 4.0