



سازمان پدافند غیرعامل کشور
سازمانت امور شهری

دوره مجازی کوتاه مدت عمومی پدافند غیرعامل شهری



قرارگاه پدافند سایبری کشور

پدافند سایبری در

هوشمند سازی زیر ساخت ها و اینترنت اشیا

استاد: دکتر محمدرضا فرجی پور

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ
الحمد لله رب العالمين
والصلاة والسلام على
الأنبياء والمرسلين
الكرام



سازمان پدافند غیرعامل کشور
سازمانت امور شهری

لازم است اقدام های
مؤثر در حوزه پدافند
غیر عامل با کار بسیجی
صورت گیرد و از
مصونیت کشور و آمادگی
لازم دفاعی در برابر
دشمن اطمینان حاصل
شود.





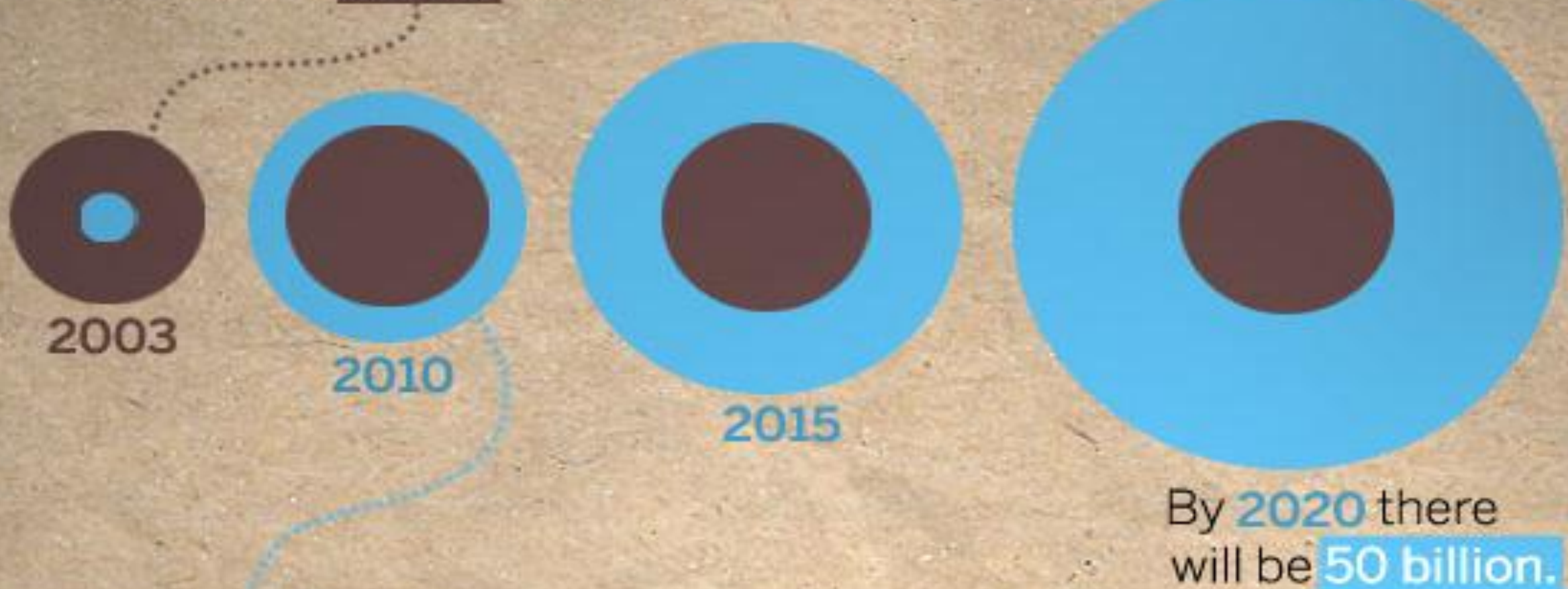
تعریف اینترنت اشیا (IOT)

- مجموعه استانداردها، پروتکلها، دستگاهها و فناوریهای لازم برای **برقراری ارتباط و انتقال اطلاعات بین دستگاههای هوشمند با یکدیگر و با انسان** در سطح جهانی.
- هدف اصلی طراحی این شبکه، **به اشتراک گذاردن اطلاعات موجود** در هر شیء میان سایر اشیاء مرتبط با آن، در هر زمان و در هر مکان مورد نیاز است.
- در واقع اینترنت اشیا، به معنی امکان برقراری ارتباط تمام اشیاء با یکدیگر IOT، و با انسانها IOP، به همراه شناسایی و کشف آنها تحت یک شبکه یکپارچه است (هدف IOE)
- ایده اتصال زنجیره ای دستگاهها و اشیاء در سطح جهانی با ظهور فناوری RFID مطرح شد.
- فناوری IoT از روشهای ارتباطی مختلف مانند، RFID، Zigbee، Wi-Fi، 3G/4G/5G، دستگاههای فشرده و حسگرها را با یکدیگر ترکیب میکند



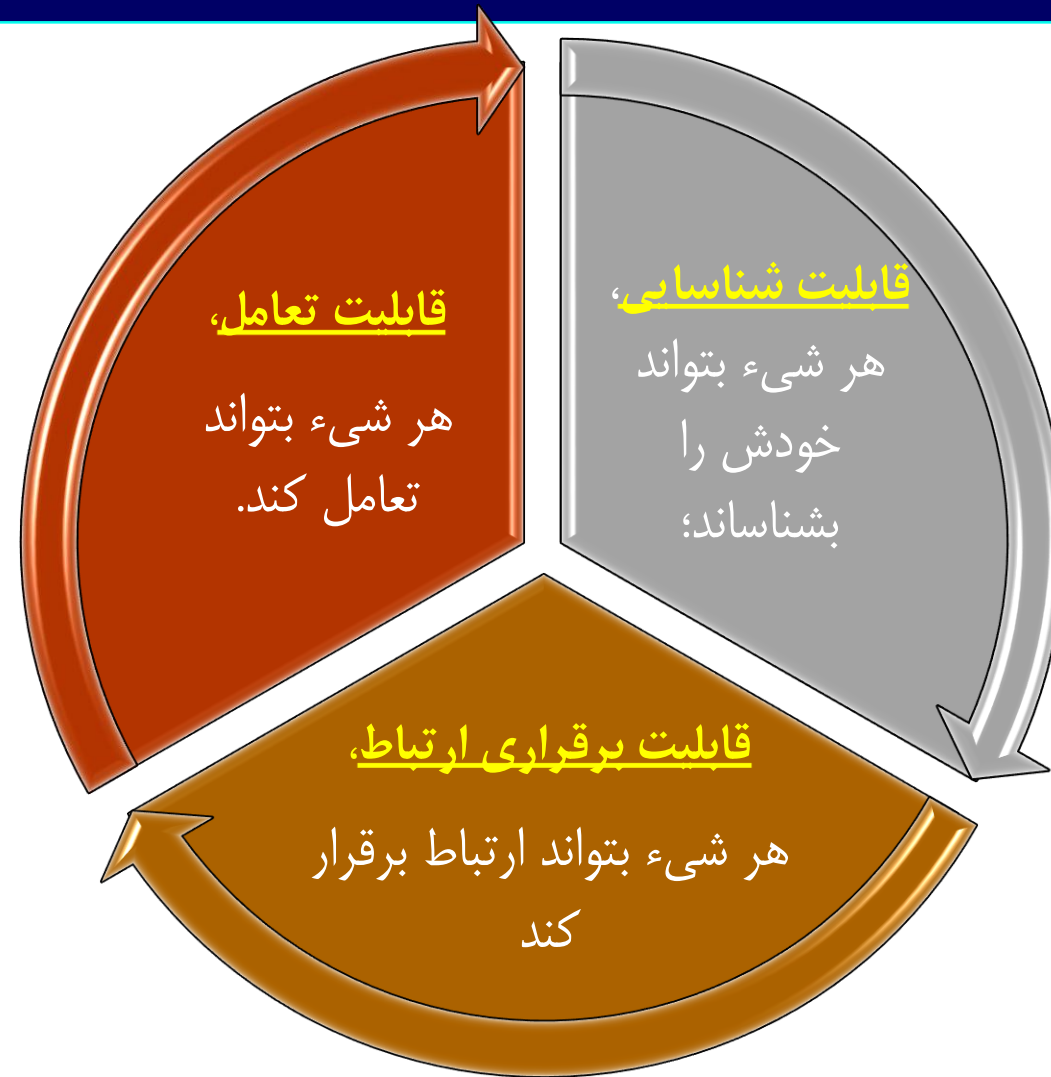
سازمان مدافعان غیرعالم کشور
سازمانت امور شهری

During 2008, the number of **things** connected to the Internet exceeded the number of **people** on earth.





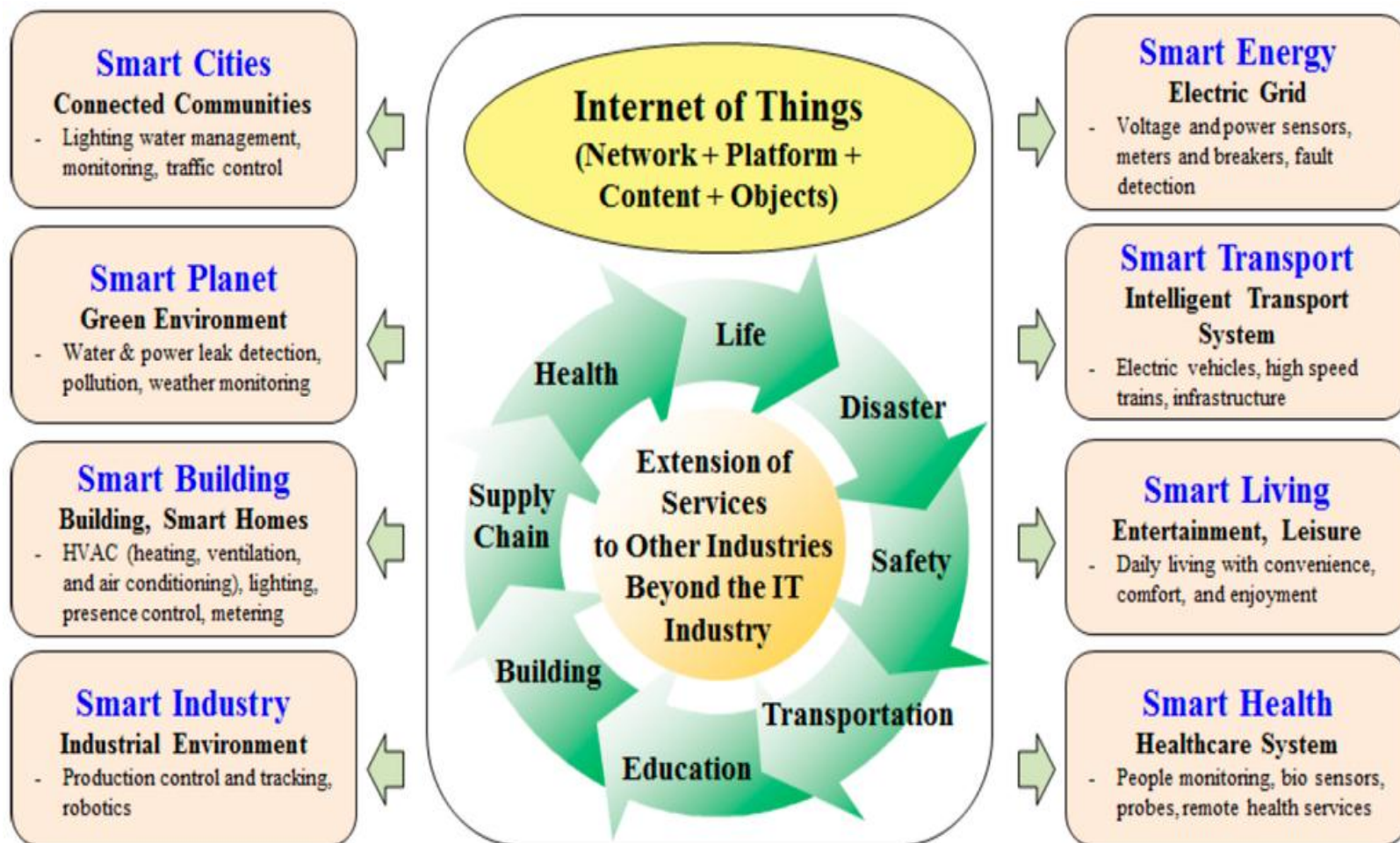
تعریف اینترنت اشیا (IOT)



از نقطه نظر مفهومی،
اینترنت اشیا بر اساس
سه رکن اساسی
ساخته می شود که مرتبط
با قابلیت های اشیا
هوشمند است.



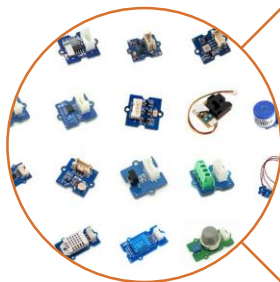
ابعاد مختلف هوشمندی در اینترنت اشياء





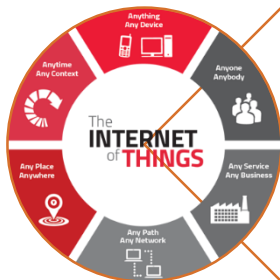
سازمان مراکز غیرعامل کشور
معاونت امور شهری

اکوسیستم اینترنت اشیاء



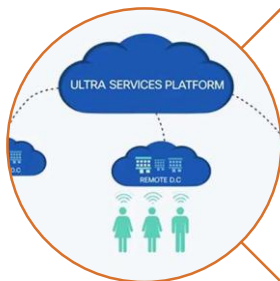
سخت افزار

(شامل سنسورها، عملگرها و دروازه‌های اتصال به شبکه)



شبکه‌های ارتباطی

(شامل شبکه انتقال مبتنی بر IP و شبکه دسترسی)



بستر ابری

(مرکز داده، پلتفرم تحلیل کلان داده و میان افزار ارایه سرویس)

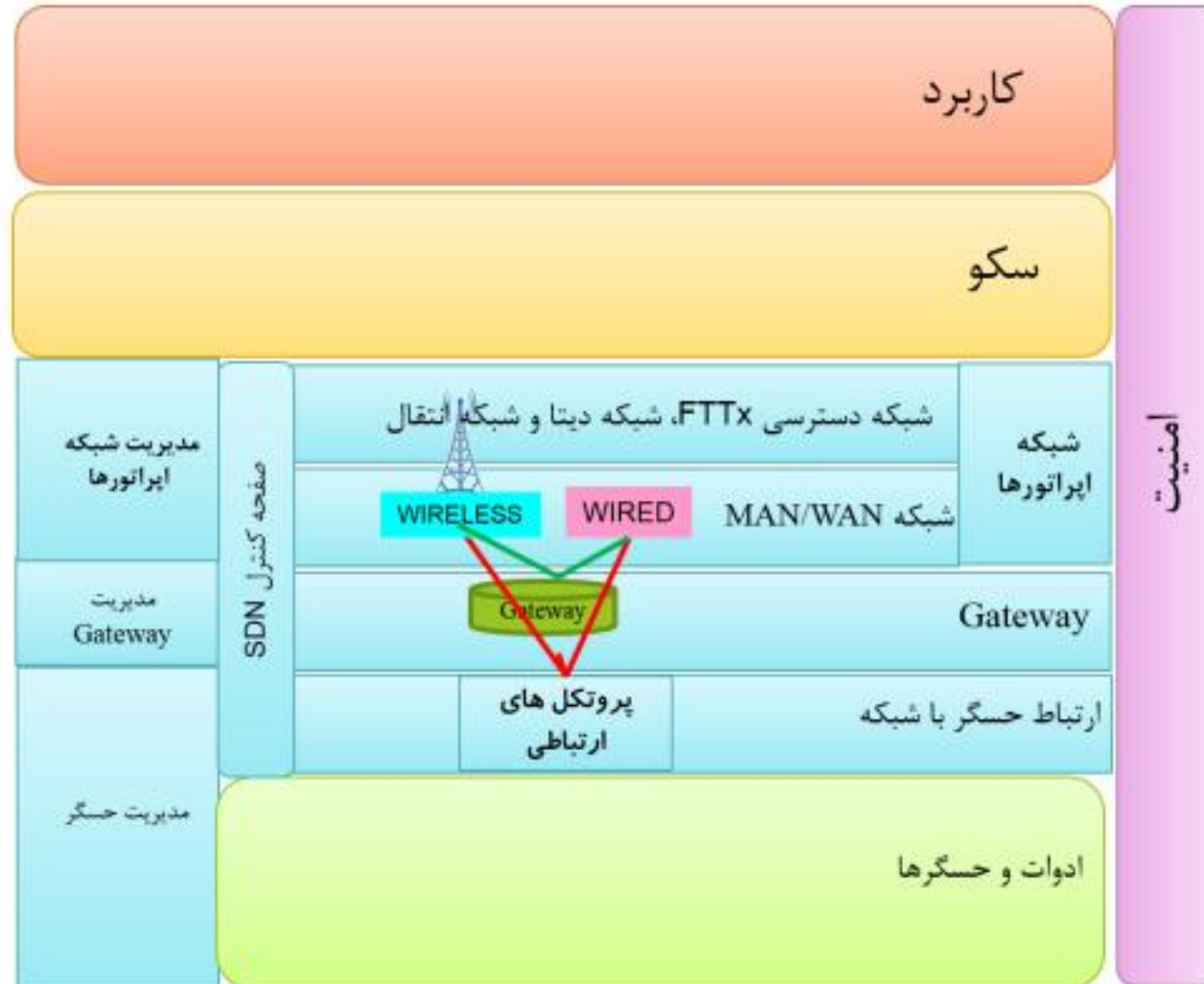


برنامه‌های کاربردی

(شامل توسعه‌دهندگان سرویس و سرویس‌گیرندگان)



معماری چند لایه اینترنت اشیاء





پلتفرم های IOT و IIOT

عامل مدیریت
مرکزی

با قابلیت‌های مختلف از
تحلیل و نمایش داده گرفته،
تا پردازش پیشرفته داده،
امنیت، مصورسازی،
حسابرسی و ...

PaaS با
قابلیت
توسعه برنامه
کاربردی

GW
موجود در
محیط

سیستم
عامل موجود
در محیط



پلتفرم های IOT و IIOT

پلتفرم های تجاری

Cisco ,IBM ,Microsoft ,Intel,
Bosch ,Google ,ARM ,GE ,
AT&T ,Oracle ,HP ,Amazon ,
Samsung , ...

پلتفرم های متن باز

Hub-of-All-Things یا HAT ،
LinkSmart ,OpenIoT ،
OpenRemote ,TerraSwarm ،
Ericsson IoT-Framework ،
ThingSpeak ,AirVantage,
Exosite ,NinjaBlock ,Device
Hub ,Mango ,Nimbits ،
SiteWhere , ...

سیستم عاملهای اینترنت اشياء

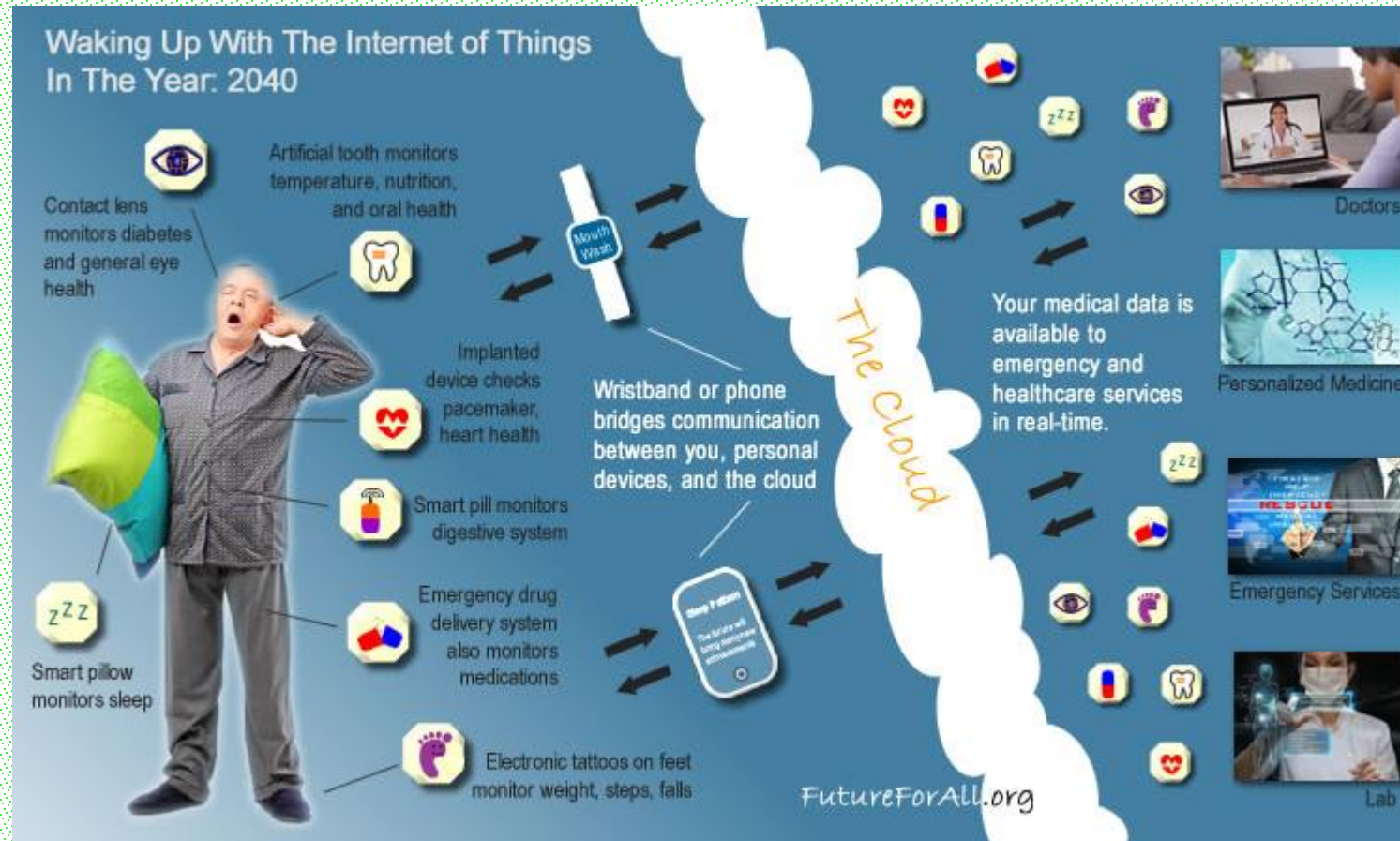
Contiki ,AllJoyn ، RIOT
Spark ,Raspbian, ...





کاربردهای اینترنت اشیا

- جمع آوری داده‌های مرتبط با علائم حیاتی بیمار از طریق شبکه سنسورهای متصل به تجهیزات پزشکی و بدن بیمار
- ارسال داده‌های جمع‌آوری شده به بستر ابری مرکز پزشکی مربوطه (برای مثال، یک بیمارستان) برای ذخیره‌سازی و پردازش آنها
- تحلیل و مدیریت اطلاعات فراهم‌شده از طریق سنسورها
- تضمین دسترسی فراگیر (از هر جا و در هر زمان) و به اشتراک‌گذاری داده‌های پزشکی
- ارسال محتوای هوشمند به کاربر
- جمع‌آوری پارامترهای خاص مرتبط با بیماری‌های مزمن و شایع به صورت دوره‌ای
- هزینه‌های درمانی به طور قابل ملاحظه‌ای کاهش یافته و نتایج درمان بهبود می‌یابد
- کاشت تراشه‌های ارتباطی





کاربردهای اینترنت اشیا

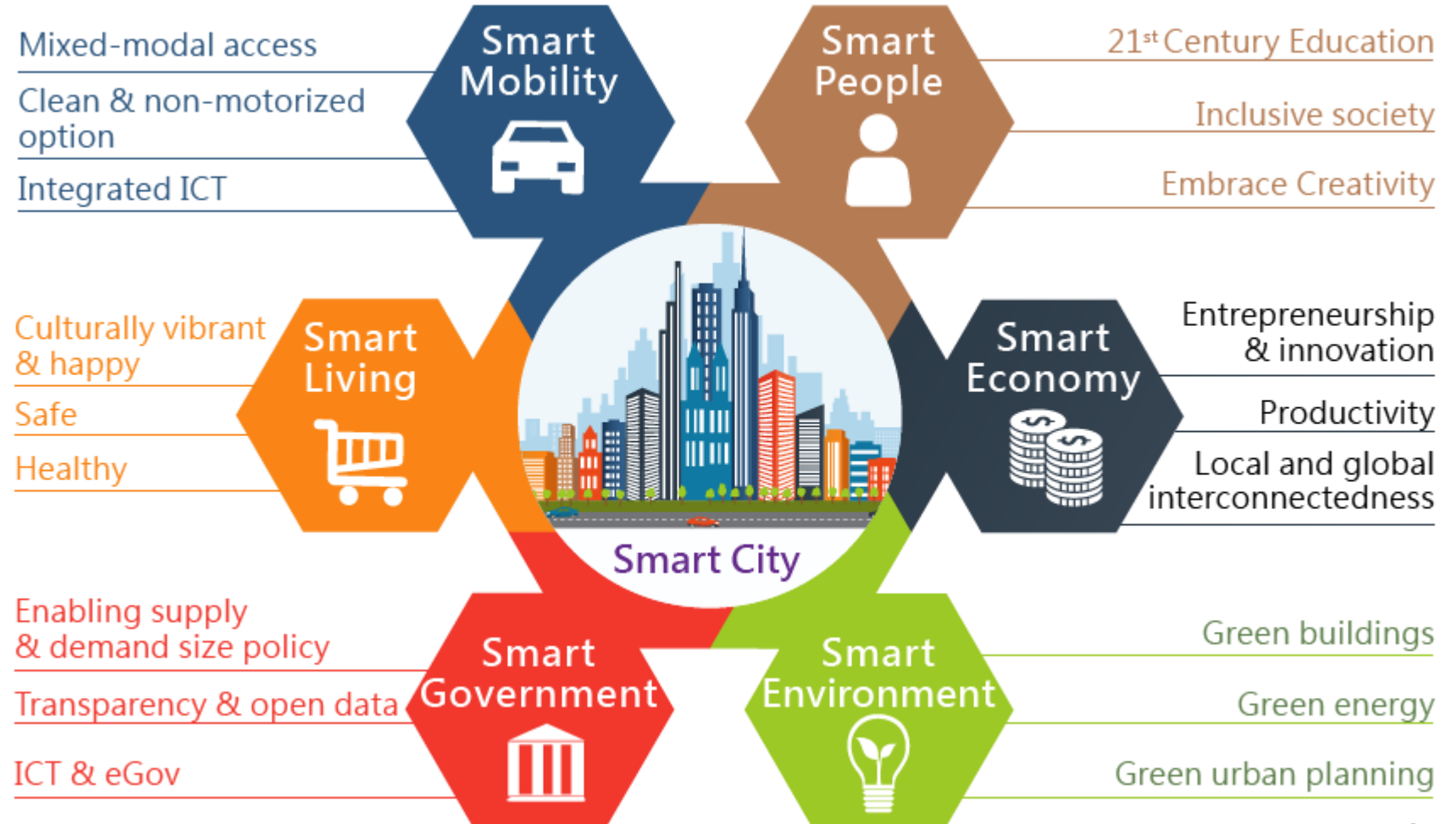
• شهر هوشمند، شهری نوآور است که از فناوری اطلاعات و ارتباطات (ICT) و وسایل دیگر استفاده بهینه می کند تا کیفیت زندگی، کارایی عملیات شهری و خدمات، به علاوه رقابت پذیری را ارتقا دهد درحالی که سازگاری و مطابقت با نیازهای نسل های کنونی و آتی را با توجه به جنبه های اقتصادی، اجتماعی و زیست محیطی تضمین می کند. (UNECE and ITU, October 2015)

• شهر هوشمند نتیجه هوشمند سازی شهر با استفاده از فناوریهای رایانش هوشمند برای افزایش هوشمندی، یکپارچگی و کارایی اجزای تشکیل دهنده زیرساختها و خدمات اساسی مورد نیاز یک شهر است که شامل اداره شهر، آموزش، خدمات درمانی، امنیت عمومی، ترابری، انرژی و آب است. (Doug Washburn and Usman Sindhu-2010)



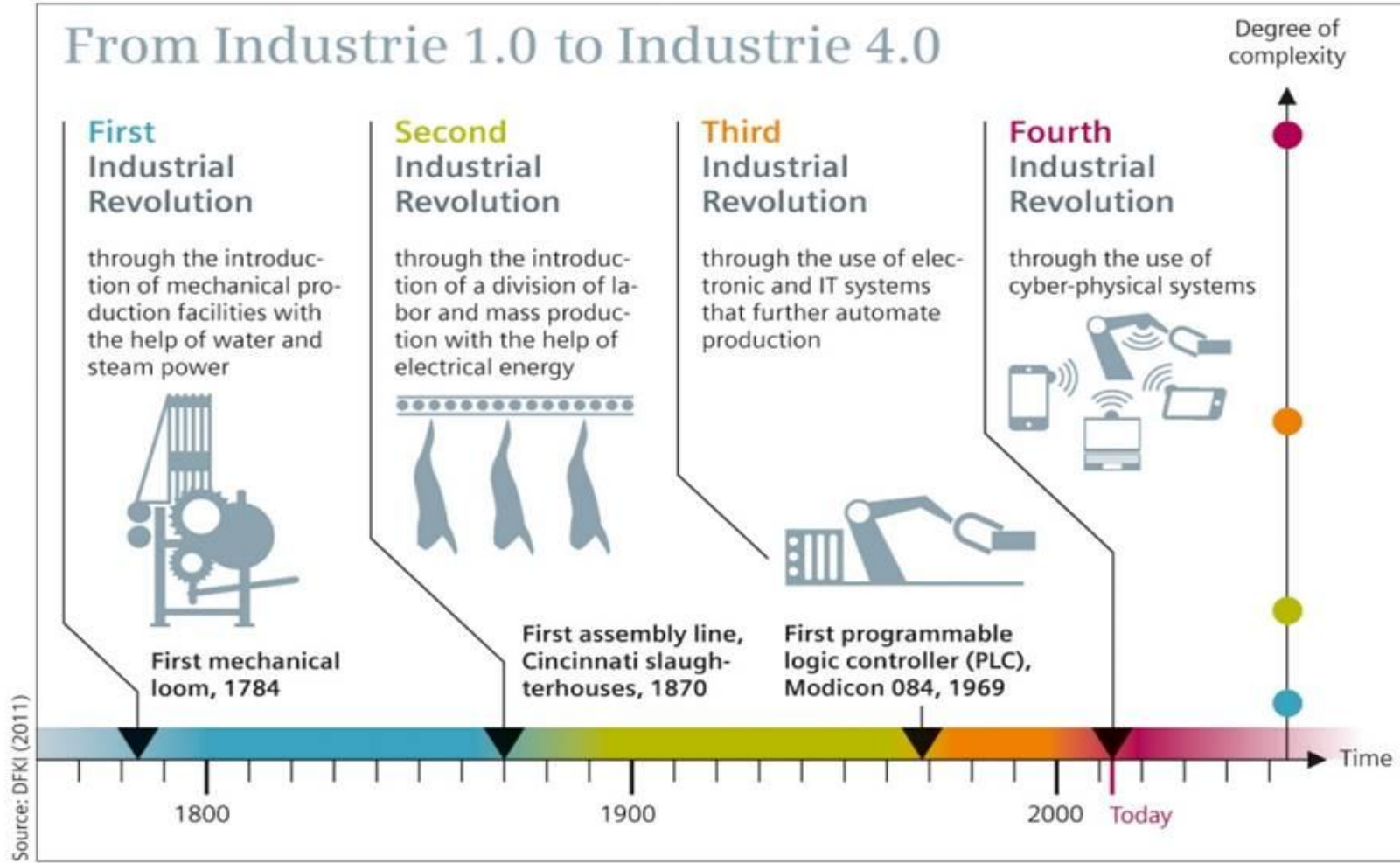
کاربردهای اینترنت اشیا

شهر هوشمند





زیرساخت های صنعتی (IIOT)



انقلاب چهارم صنعتی مبتنی بر فضای سایبری

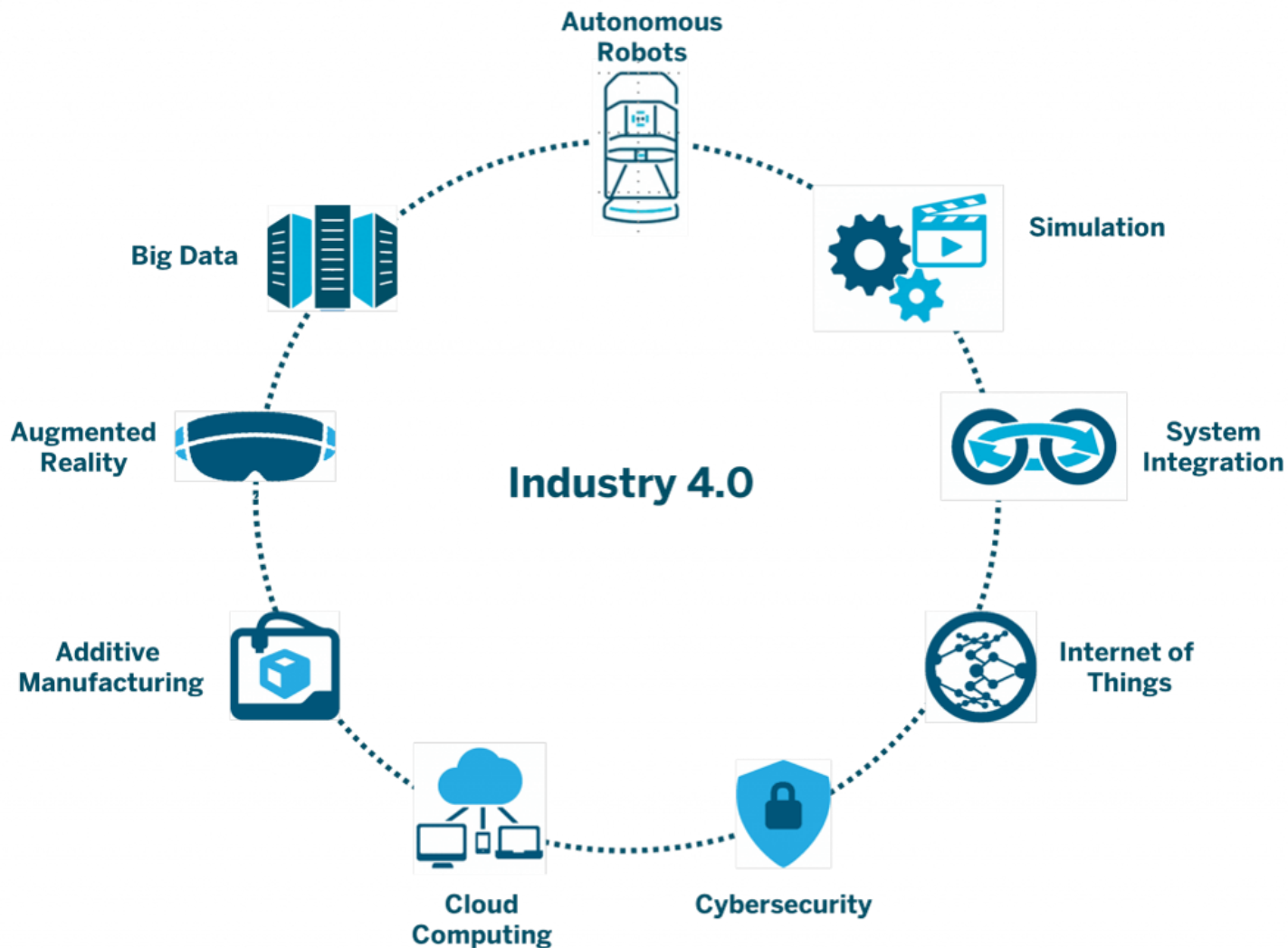


کاربردهای اینترنت اشیا

- در نسل جدید صنعت، راهکار اینترنت اشیا در محیط های صنعتی (IIoT) منجر به توسعه سیستم های نوآورانه و کارآمد با هدف افزایش بهره وری عملیاتی و کاهش چشمگیر هزینه های تولید شده است.
- در نتیجه این فناوری، طیف گسترده ای از برنامه های کاربردی اینترنت اشیا، تحت چارچوب های متفاوتی به وجود آمده است.



زیرساخت های صنعتی (IIOT)





چالشهای IOT و IIOT





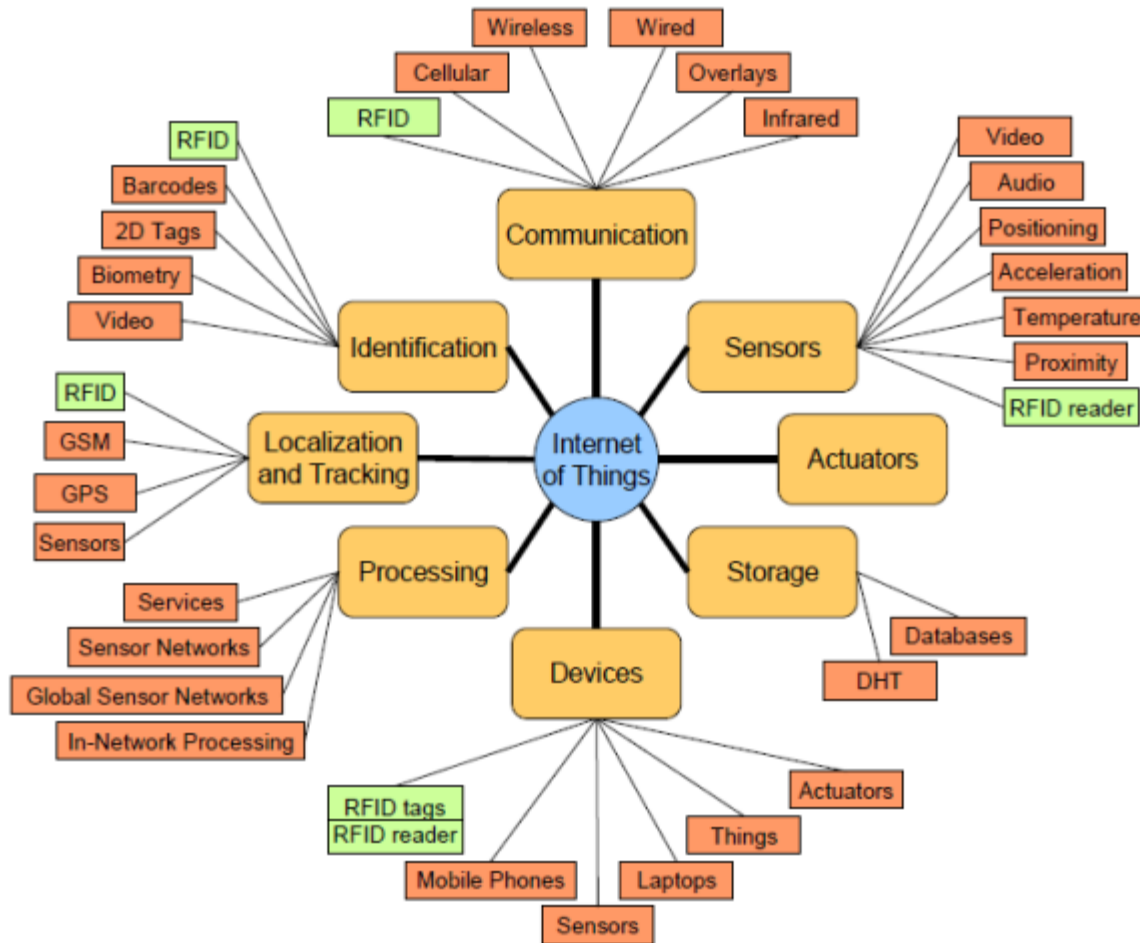
تهدیدات، آسیب پذیریها و مخاطرات IOT و IIOT

- واسط گرافیکی ناامن
- احراز اصالت و مجوز دهی ناکافی
- سرویس شبکه ناامن
- عدم وجود رمزنگاری در نقل و انتقال
- رابط ابر ناامن
- رابط موبایل ناامن
- تنظیمات امنیتی ناکافی
- سخت افزار / نرم افزار ناامن
- امنیت فیزیکی ضعیف
- نگرانی های حریم خصوصی



الزامات و ملاحظات کلان پدافند سایبری در IOT و IIOT

- طبقه بندی موضوعات و فناوری های اینترنت اشياء و تلاش جهت امن سازی و بومی سازی فناوری ها و تجهیزات حیاتی





الزامات و ملاحظات کلان پدافند سایبری در IOT و IIOT

- ایجاد مشارکت و هماهنگی بین نهادهای مختلف برای بالا بردن سطح امنیت اینترنت اشیا بالاخص برای استفاده در زیرساخت ها
- لزوم راه اندازی مرکزی برای جمع آوری، پردازش و مدیریت اطلاعات مربوط به تهدیدات و آسیب پذیری ها و ارائه هشدارهای امنیتی اینترنت اشیا
- لزوم تدوین استانداردهای امنیتی اینترنت اشیا برای استفاده از این فناوری در سطوح مختلف
- آموزش، فرهنگ سازی و آگاهی بخشی بهترین روش ها و دستورالعمل های امنیتی
- صدور گواهینامه امنیتی برای محصولات حوزه عمومی و گواهینامه پدافند غیرعامل برای حوزه های زیرساختی (برچسب امنیتی برای تجهیزات اینترنت اشیا)



الزامات و ملاحظات کلان پدافند سایبری در IOT و IIOT

- لزوم تعریف دقیق مرز بین حریم خصوصی و امنیت ملی
- لزوم لحاظ نمودن موضوع امنیت سایبری در مرحله طراحی، تولید، استقرار، پیاده سازی و ...
- الزام در نظر گرفتن اصول حریم خصوصی در مرحله طراحی، تولید، استقرار، پیاده سازی و ...
- لزوم ارزیابی تجهیزات، شبکه، ارتباطات و پروتکل های فناوری اینترنت اشیا بر حسب استفاده در زیرساخت های متفاوت بنا بر الزامات و ملاحظات سازمان پدافند غیرعامل کشور
- الزام ایجاد و توسعهی بخش های مختلف اکوسیستم اینترنت اشیا بر مبنای شیوه ها و راه حل های امنیتی رایج مورد تایید



الزامات و ملاحظات کلان پدافند سایبری در IOT و IIOT

- اولویت‌بندی اقدامات امنیتی – پدافندی با توجه به تاثیر بالقوه آن‌ها و تمرکز بر مدیریت و پیامد مخاطره مخاطره
- تدوین و ابلاغ دستورالعمل‌های فنی، امنیتی و پدافندی و خط‌مشی‌های مربوط به حفظ و ارتقای پایداری سیستم
- ایجاد مراکزی جهت جمع‌آوری، اشتراک و تحلیل داده‌ها برای کاربردهای مختلف
- اصلاح و بروزرسانی قوانین داخلی موجود و پرداختن به خلأهای قانونی
- ارزیابی امنیتی – پدافندی جهت بررسی استحکام، اصالت و یکپارچگی ساختار سیستم عامل، پایگاه داده، پروتکل و ... مورد استفاده در هر لایه در آزمایشگاه‌های مورد تأیید سازمان پدافند غیرعامل
- لزوم لحاظ نمودن موضوعات حقوقی مربوط به طیف فرکانسی، نامبرینگ، سویچینگ، آدرس دهی و رومینگ



الزامات و ملاحظات کلان پدافند سایبری در IOT و IIOT

- لزوم ایجاد معماری امنیتی و پدافندی در تمام سطوح اعم از سطوح کاربری، سطوح هسته شبکه، سطوح محتوا و ... بر اساس معماری امن و لایه به لایه مطابق با سیاست ها و ابلاغیات سازمان پدافند غیرعامل و مبتنی بر متدولوژی دفاع در

عمق

- لزوم ایجاد مکانیزم های امنیتی و پدافندی مناسب برای مدیریت و حفاظت از پروفایل کاربران در مقابل مکانیزم های

داده کاوی و حفظ حریم خصوصی

- لزوم بکارگیری وجوه مختلف حفظ محرمانگی مانند محرمانگی اطلاعات، محرمانگی کاربران، محرمانگی پروفایلینگ و ...

را مطابق با سیاست ها و ملاحظات ابلاغی



الزامات و ملاحظات کلان پدافند سایبری در IOT و IIOT

- لزوم تعریف چارچوب تنظیم مقررات برای اینترنت اشیا (فردی، سازمانی، اجتماعی و ملی)

- لزوم استفاده از نرم افزارها، توانمندی ها و فناوری های بومی و امن داخلی در تمام سطوح طراحی، نصب و پیاده سازی، راه اندازی، توسعه، ارائه خدمات و ...

- لزوم ایجاد مکانیزمی برای نگهداری تمامی لاگ ها، رخدادها، هشدارها و ... در سطوح مختلف اعم از کاربری، هسته، محتوا و ... با رعایت اصول پدافندی مانند **Indexing**، **Time Stamp**، **Signing**

- لزوم تعریف پلتفرم استاندارد برای استفاده

- الزامات امنیتی حوزه اینترنت اشیا، در سه بخش تجهیزات / سنسورها؛ انتقال / شبکه و در انتها کاربرد / سرویس تقسیم بندی شود و برای هر قسمت راهکاری مناسب اندیشیده شود

صَلِّ وَسَلِّمْ
عَلَى مُحَمَّدٍ
وَعَلَى آلِهِ
وَجِبْرِيلٍ وَرَحْمَتِهِ

سنة 1430