Progresivní technologie v informatice II

IoT

inteligentní domácnost, způsoby komunikace, výhody, rizika

Fakulta informačních technologií
České vysoké učení technické v Praze

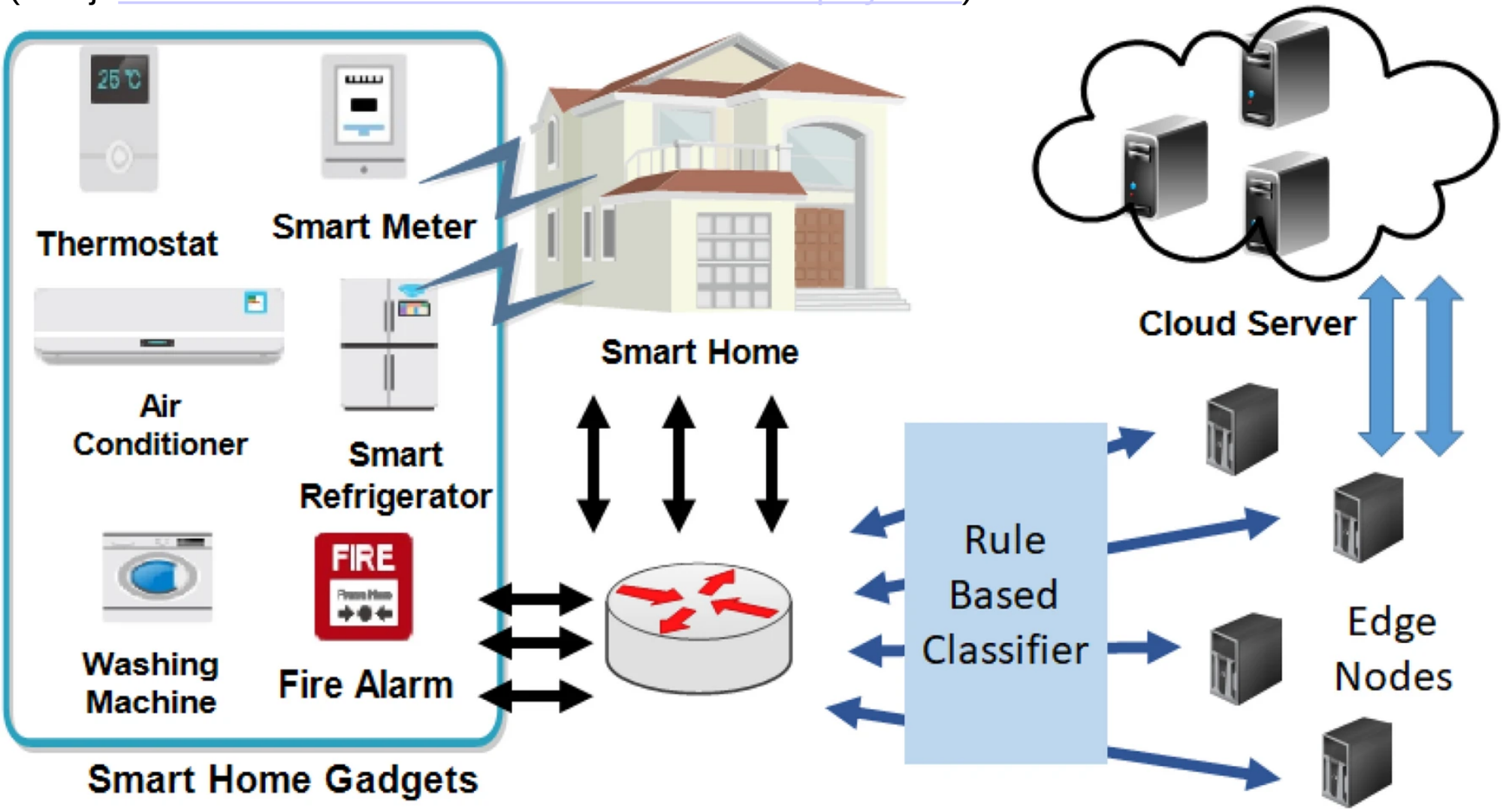
Financováno Evropskou unií
NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

- Úvod
- Technologie, které umožňují rozvoj IoT
- Historie
- Sítě a komunikační protokoly
- Programovací jazyky pro IoT
- Hrozby
- Kryptografické metody
- Příklad IoT
- Budoucnost

- **Internet věcí** – IoT (Internet of things) je systém vzájemně propojených výpočetních zařízení, mechanických a digitálních strojů, předmětů, zvířat nebo osob, které jsou vybaveny jedinečnými identifikátory tzv. UID (unique identifier) a schopností přenášet data po síti, aniž by byla nutná interakce člověka s člověkem nebo člověka s počítačem.
- **Věcí** v IoT může být člověk s implantovaným monitorem srdce, hospodářské zvíře s transpondérem s biočipem, automobil, který má zabudované senzory upozorňující řidiče na nízký tlak v pneumatikách, nebo jakýkoli jiný přírodní či lidmi vytvořený objekt, kterému lze přidělit intenetovou adresu (tzv. IP adresu) a který je schopen přenášet data po síti.
- IoT je senzorová síť miliard zařízení (někdy označovaných jako smart devices), která propojuje lidi, systémy a další aplikace a shromažďuje a sdílí data.

- Bezdrátové sítě, bezdrátové senzory
  - 4G/LTE, 5G, Bluetooth, Wi-Fi, atd.
- Cloudové služby
  - Umožňující vysokou škálovatelnost a dostupnost
- Analýza velkých dat (tzv. Big Data)
  - Využívající algoritmy pro zpracování velkoobjemových dat získaných z IoT
- Komunikační protokoly
  - Umožňující zabezpečné, spolehlivé a nízkoenergetické přenášení dat.
- Vestavěné systémy (embedded systems)
  - Umožňují integraci většiny funkcí na jednom čipu a tím rozšiřují možnosti, kde lze IoT použít (díky menším rozměrům a nižší energetické náročnosti).

Architektura inteligentní domácnosti
(zdroj: IoT Data Classifications for Smart Home Deployment)

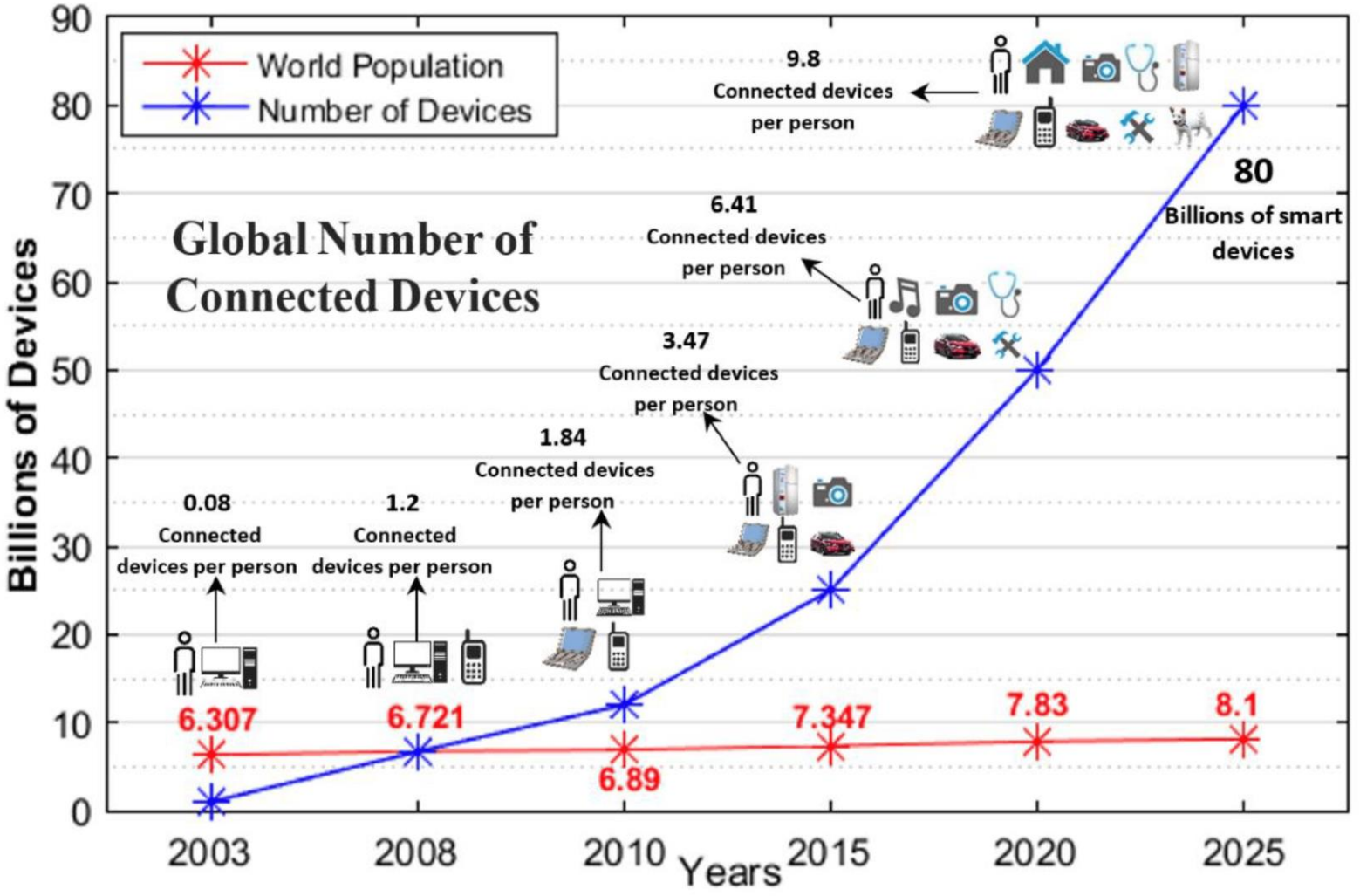


- 1982 - Skupina studentů z Carnegie Melon univerzity vytvořila způsob, jak přimět automat na Coca-Colu v kampusu, aby prostřednictvím sítě informoval o svém obsahu a ušetřil jim tak cestu, pokud by v automatu došla Coca-Cola.

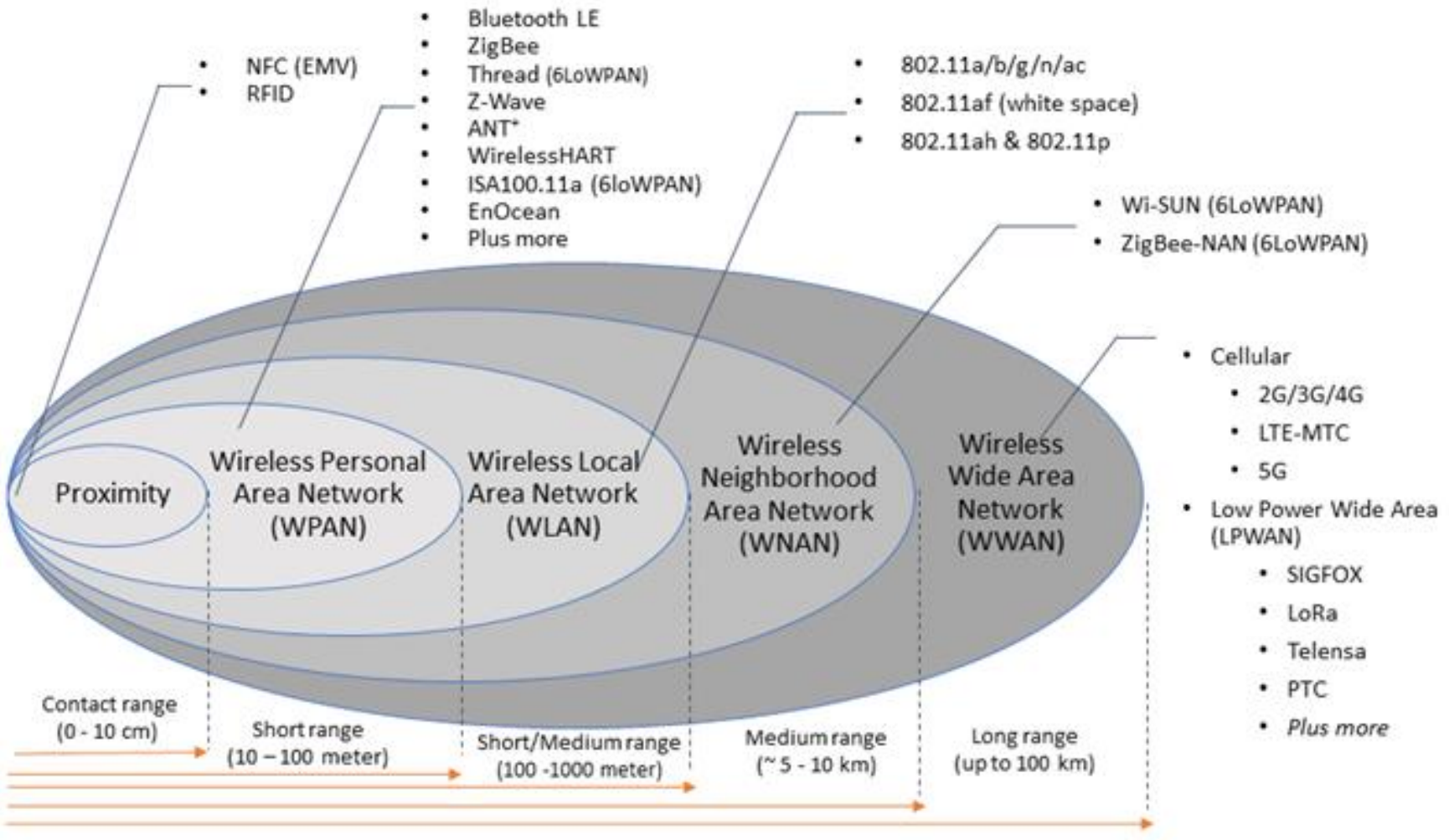
- 1999 - Kevin Ashton poprvé popsal termín "internet věcí". Během svého působení ve společnosti Procter & Gamble navrhl umístit na výrobky čipy pro radiofrekvenční identifikaci (RFID), aby je bylo možné sledovat v dodavatelském řetězci.

- 2000 - LG Internet Digital DIOS (R-S73CT)
byla chladnička s připojením na Internet, která díky dotykové obrazovce umožňovala zobrazovat nejrůznější informace o zařízení a čerstvosti uložených potravin jejichž snadnou evidenci zprostředkovala vestavěná kamera. Chladnička umožňovala i automatické on-line objednávání potravin.

~2008 - Počet zařízení připojených k internetu překročil celosvětovou lidskou populaci (zdroj: článek z časopisu Sensors 2022).

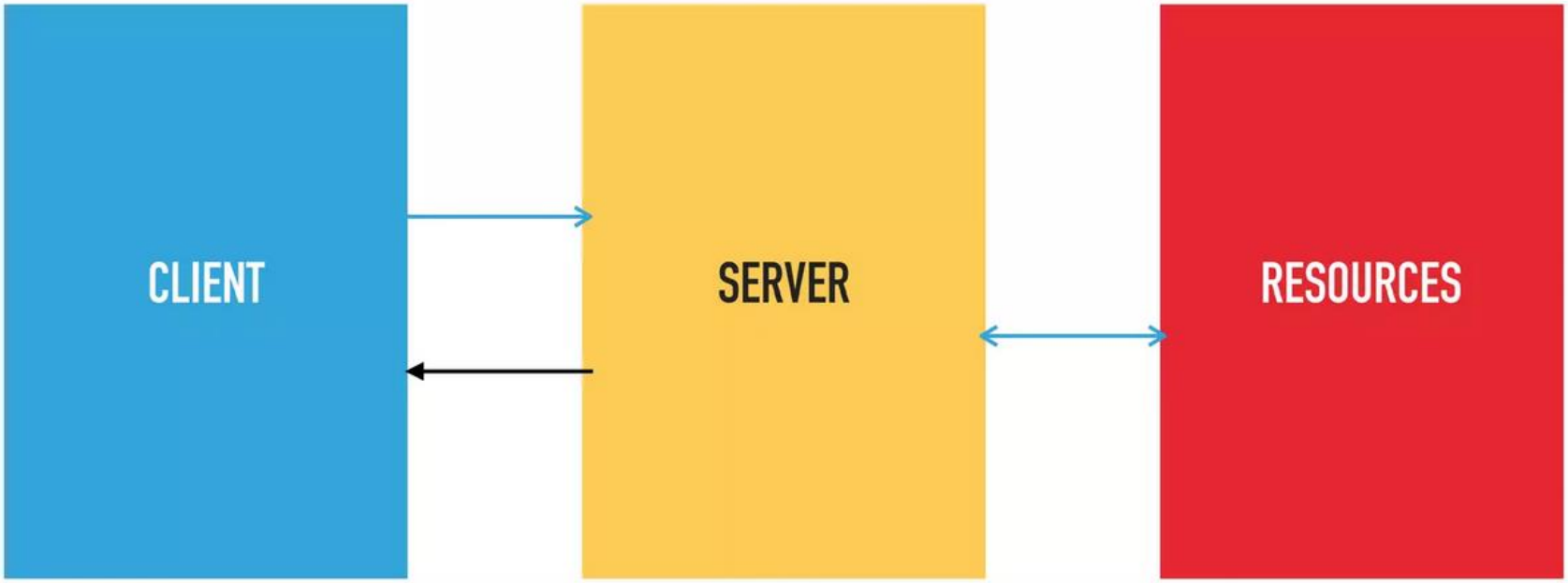


IPv4	IPv6
První nasazení 1981	První nasazení 1998
32-bit IP address	128-bit IP address
4.3 miliard adres Stejné adresy je nutné použít vícekrát a maskovat	**3.4×10^{38} adres** Každé zařízení mé jedinečnou adresu
192.168.5.18	**Alphanumeric hexadecimal notation** **50b2:6400:0000:0000:6c3a:b17d:0000:10a9** **(Simplified - 50b2:6400::6c3a:b17d:0:10a9)**
DHCP nebo manuální konfigurace	Podporuje autokonfiguraci

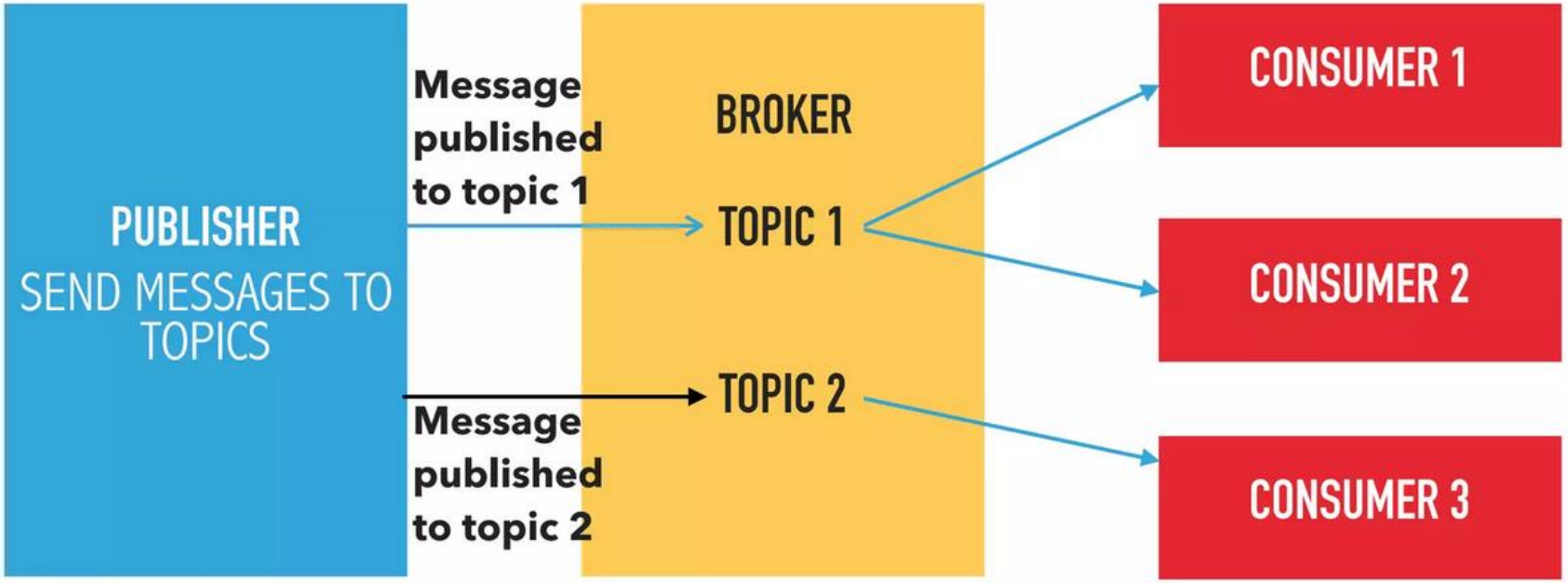

NFC (EMV)
RFID
Bluetooth LE
ZigBee
Thread (6LoWPAN)
Z-Wave
ANT*
WirelessHART
ISA100.11a (6loWPAN)
EnOcean
Plus more
802.11a/b/g/n/ac
802.11af (white space)
802.11ah & 802.11p
Wi-SUN (6LoWPAN)
ZigBee-NAN (6LoWPAN)
Cellular
2G/3G/4G
LTE-MTC
5G
Low Power Wide Area (LPWAN)
SIGFOX
LoRa
Telensa
PTC
Plus more
Proximity
Wireless Personal Area Network (WPAN)
Wireless Local Area Network (WLAN)
Wireless Neighborhood Area Network (WNAN)
Wireless Wide Area Network (WWAN)
Contact range (0 - 10 cm)
Short range (10 – 100 meter)
Short/Medium range (100 -1000 meter)
Medium range (~ 5 - 10 km)
Long range (up to 100 km)

OSI model	TCP/IP model	IoT protocols
7 Application	Application	HTTPS, XMPP, CoAP, MQTT, AMQP
6 Presentation		
5 Session		
4 Transport	Transport	UDP, TCP
3 Network	Internet	IPv6, 6LoWPAN, RPL
2 Data link	Network access & physical	IEEE 802.15.4 Wifi (802.11 a/b/g/n) Ethernet (802.3) GSM, CDMA, LTE
1 Physical		

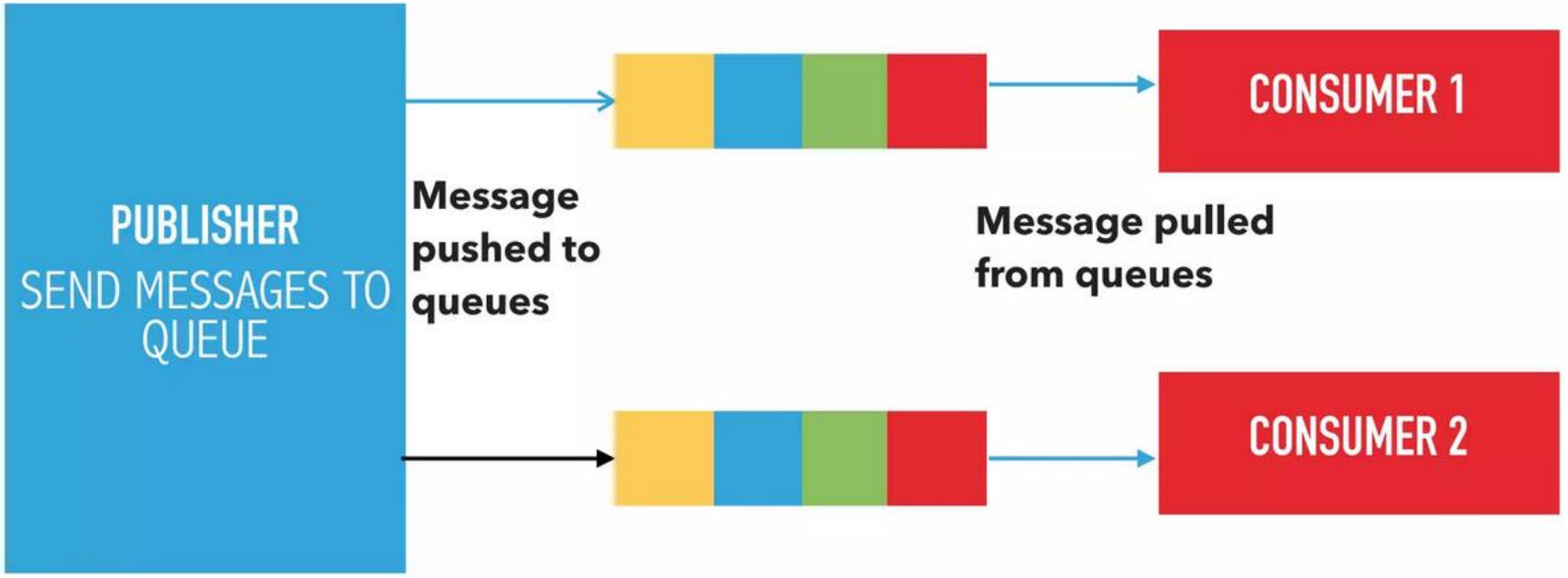
- Client-server model komunikace
  - HTTP (Hypertext Transfer Protocol)



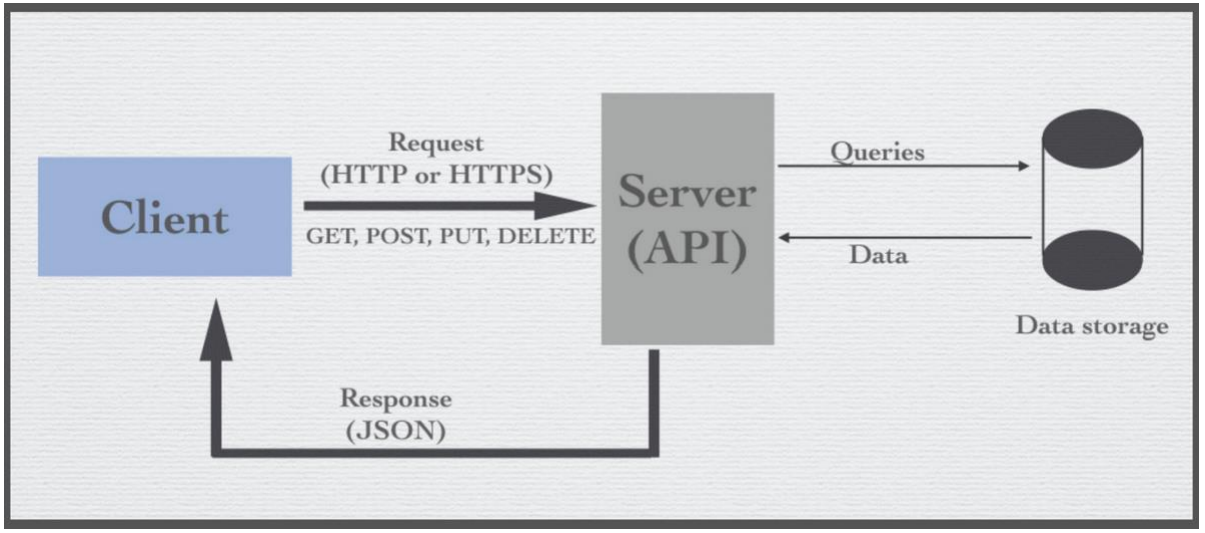
- # Publish-subscribe model komunikace
  - MQTT (MQ Telemetry Transport)
  - AMQP (Advanced Message Queuing Protocol)
  - OPC UA (OPC Unified Architecture)



- Push-pull model komunikace
  - AMQP (Advanced Message Queuing Protocol)
  - Apache Kafka



- REST (**Re**presentational **S**tate **T**ransfer) API je softwarová architektura pro *distribuované hypermediální systémy*, kterou popsal Roy Thomas Fielding ve své disertační práci z roku 2000.
- Vlastnosti:
  1. Client - Server
  2. bezstavový (stateless)
  3. umožňuje cachování
  4. jednotný interface
  5. vrstevnatost (různé části můžou běžet na různých serverech)
  6. umožňuje zaslání kódu ze serveru na vyžádání (Code-On-Demand)



- **C**
  - Efektivní využití systémových prostředků
  - Výkon / rychlost
- **C++**
  - Podpora objektově orientovaného programování
- **Java**
  - Nezávislost na platformě: Kód lze spustit na jakémkoli zařízení s nainstalovaným virtuálním strojem Java (JVM)
  - Bezpečnost běhu: automatická správa paměti a kontrola typů, které pomáhají předcházet běžným bezpečnostním zranitelnostem známým z C/C++
- **Python**
  - Snadné používání
  - Rozsáhlé knihovny s efektivními implementacemi např. pro zpracování obrazu, strojového učení, atd.
  - V současnosti jeden z nejpopulárnějších programovacích jazyků vůbec ➔ velká komunita a podpora řešení na nejrůznějších internetových fórech

Typický postup:

- Přístup do vybraného podsystému
- Hledání zranitelných míst
- Proniknutí a řízení podsystému

- Pasivní (jen sbírání tajných informací)
- Aktivní (modifikace chování napadeného systému)

Obrana: detekce útoků (detekce anomálií), firewally, zmírnění následků útoku

Bezpečnostní politika na všech úrovních včetně organizačních pravidel (Je známo, že mnoho bezpečnostních incidentů je způsobováno lidmi a ne technickými chybami v návrhu systému).

- Zákeřný útok na kód

  virus, červ, Trojský kůň (statický i dynamický)

- Spoofing

  útočník se maskuje jako legitimní uživatel (např. phishing)

- Nalezení hesla

  slovníkové metody (obvykle používaná hesla) x hrubá síla

- Útok na šifrovaný text

  Při znalosti šifrované zprávy se zkouší odvodit původní zpráva a šifrovací klíč. (obrana AES - Advanced Encryption Standard)

- Odmítnutí služby (denial of service)

  např. umělé zahlcení sítě

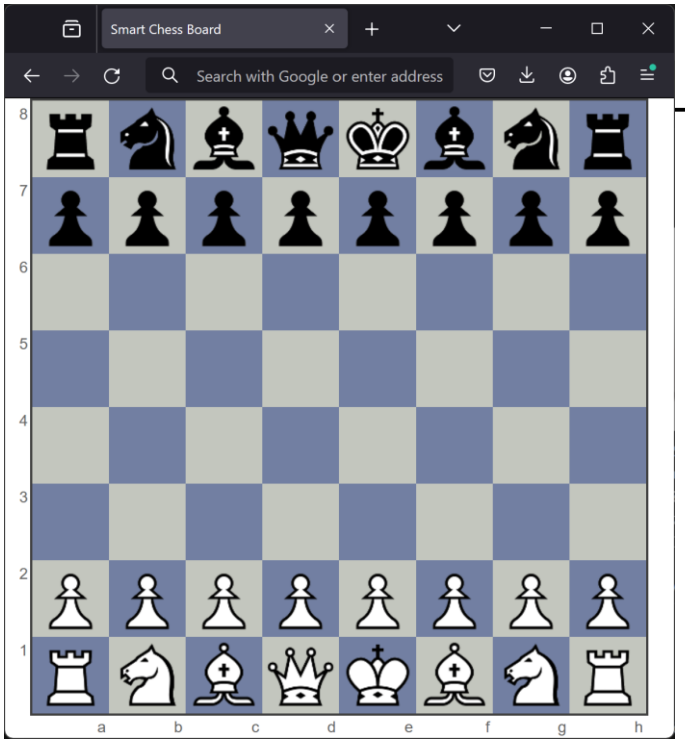
- „Botnet“ útok

  napadení sítě uzlů a znemožnění práce uživatelům („bot“ je zkratka robota)

= snížení pravděpodobnosti útoku na minimum

- Časová omezení (určení max. doby (de)kódování)
- Omezení zdrojů
- Bezpečná architektura by měla obsahovat:
  - Kódování symetrickým klíčem
    - Je výpočetně nenáročné a používá se na zpracování většiny dat
  - Kódování asymetrickým (veřejným/privátním) klíčem
    - Je výpočetně náročné a používá se typicky k zabezpečenému získání symetrického klíče pro další komunikaci
  - Hash funkce
    - pro bezpečné ukládání hesel v zařízení
    - pro zabezpečení datové integrity
    - Umožnit bezpečné ověřování (authentication)
  - Generátor náhodných čísel
    - pro generování klíčů

IoT smart šachovnice



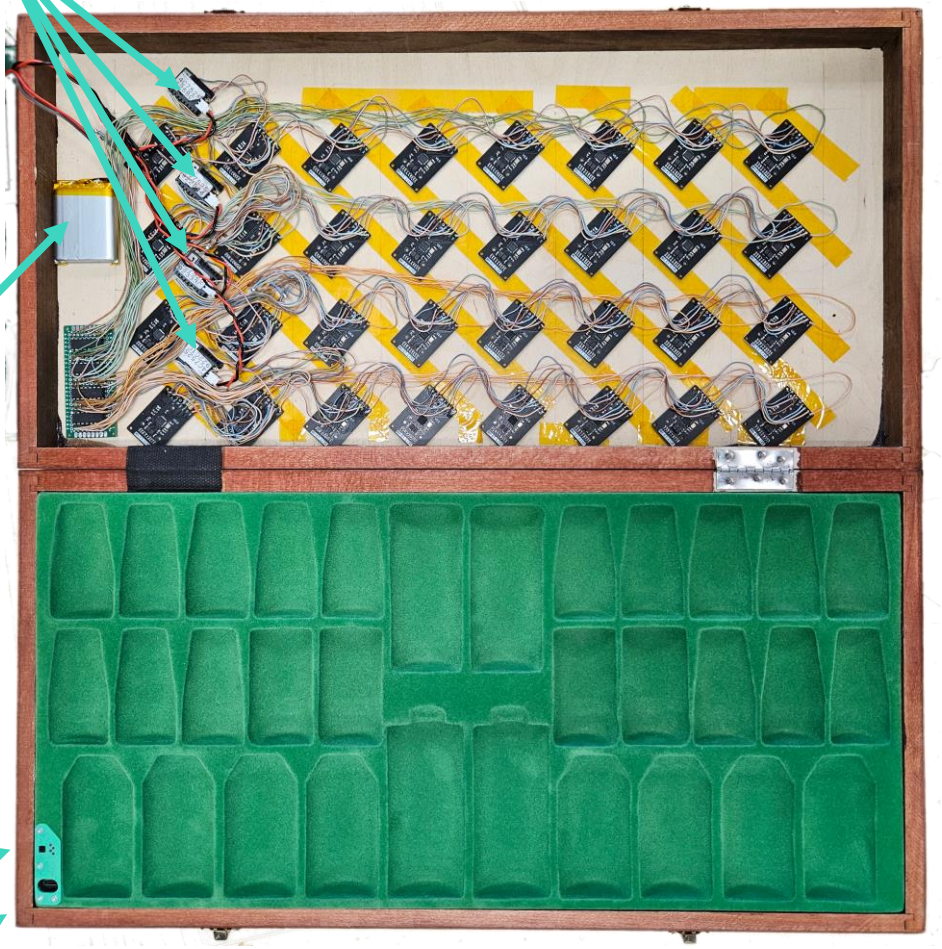
Čtečky RFID

Mikrokontroléry

LiPol baterie

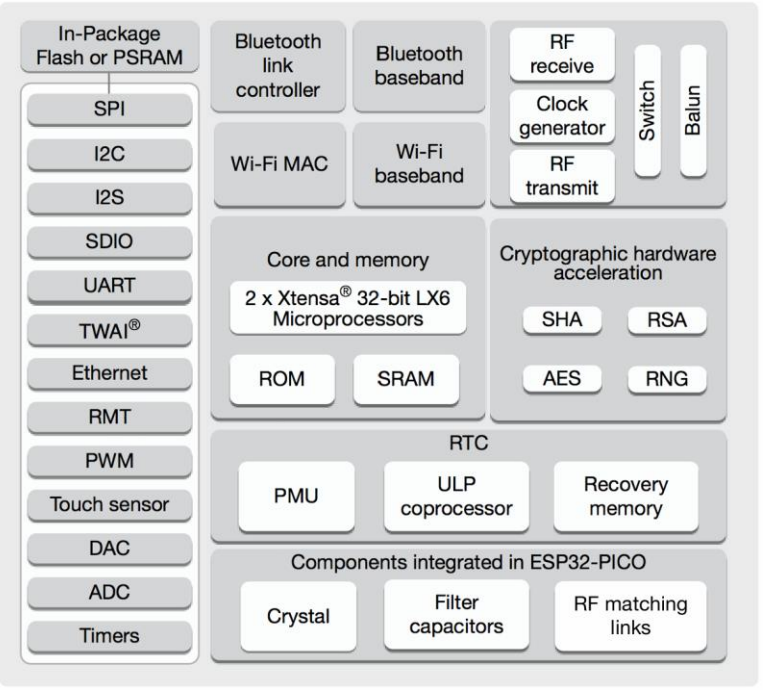
Tlačítko ON/OFF

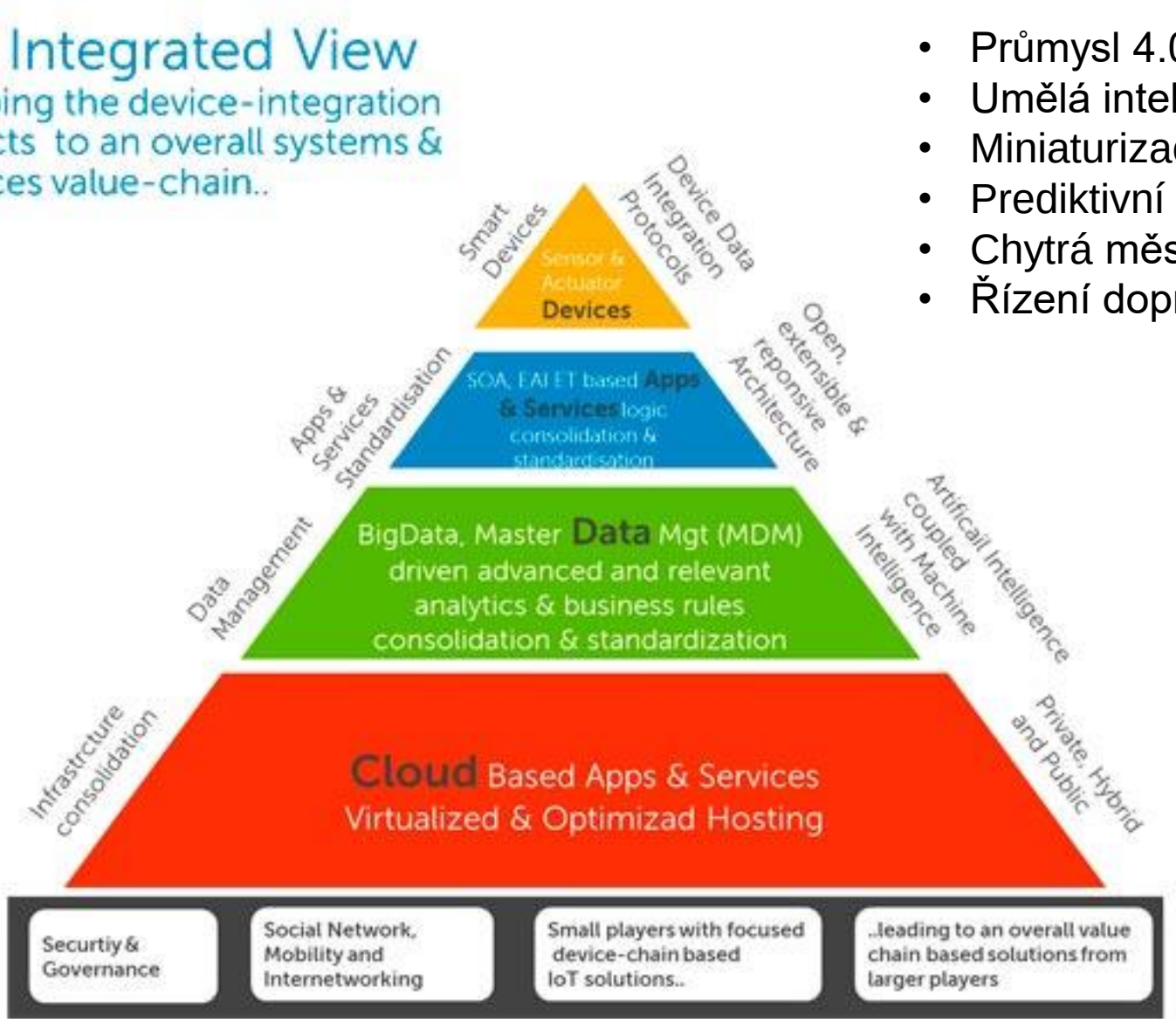
Nabíjecí USB-C



IoT smart šachovnice

- Připojení na Internet pomocí Wi-Fi
  - Aktuální pozice se odesílá pomocí protokolu HTTP/GET na server s REST API.
- Jednotlivé figurky obsahují 13,56 MHz RFID tag (chip s anténou)
- Každý řádek (8 polí) je vyčítán jedním mikrokontrolérem
  - Espresiff ESP32-PICO-D4
    - 2x 32-bit jádra 240MHz
    - 520 kB SRAM
    - 4 MB Flash





- Průmysl 4.0
- Umělá inteligence a strojové učení
- Miniaturizace
- Prediktivní údržba
- Chytrá města (Smart Cities)
- Řízení dopravy