Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Podniková bezpečnostná architektúra

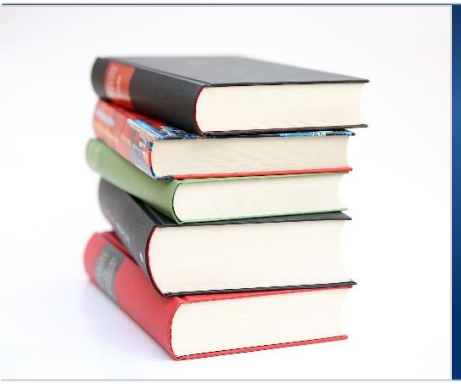
Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

Milan Kubina

KC KYB UNIZA, https://kc.uniza.sk/

milan.kubina@fri.uniza.sk



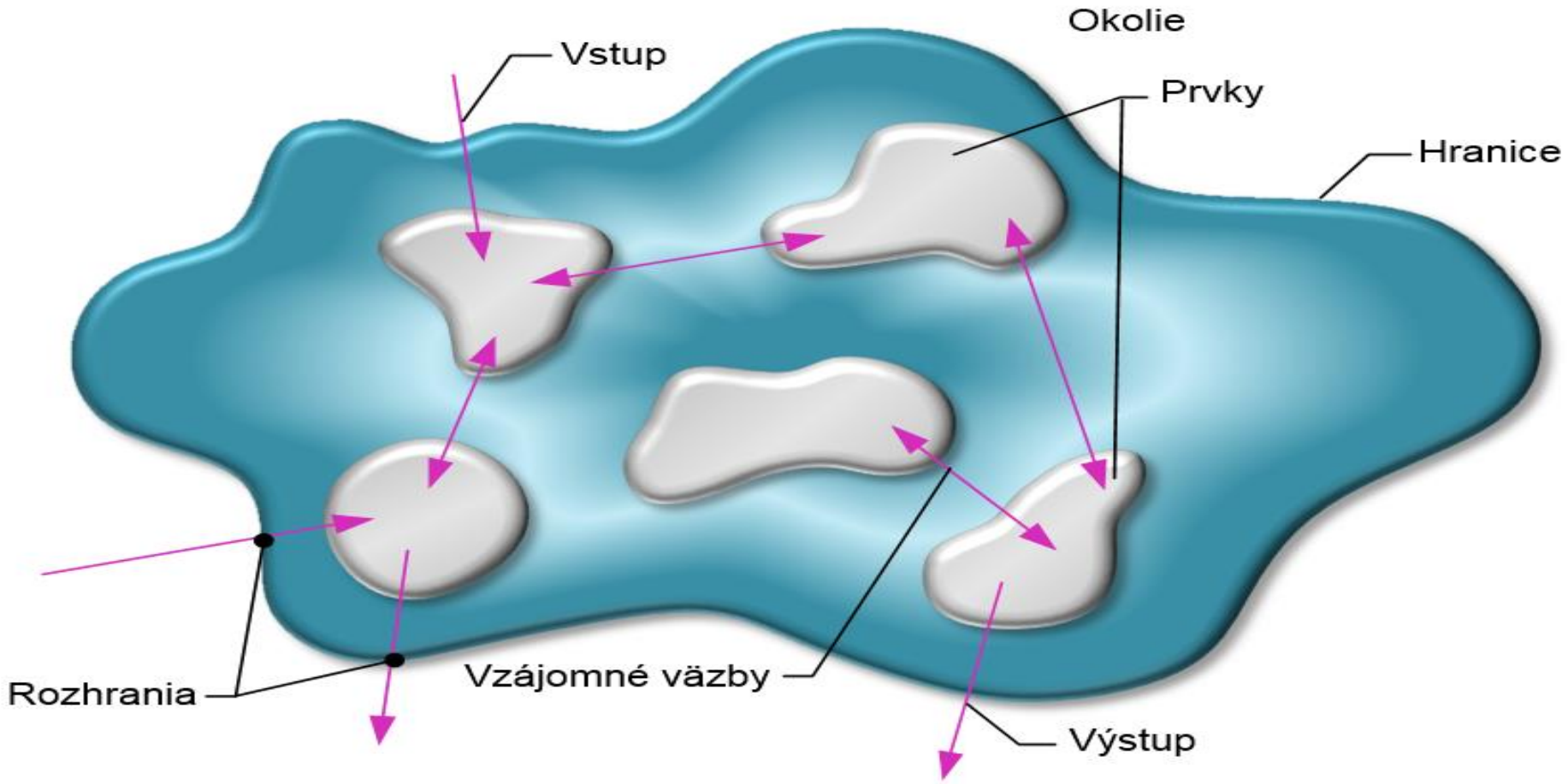
Obsah

1. Princípy podnikovej architektúry
   - Základné pojmy
2. Koncepcia bezpečnostnej architektúry
   - Základné pojmy
3. Referenčné modely podnikovej architektúry
   - Základné pojmy

Princípy podnikovej architektúry

- Systém / Informačný systém
- Architektúra / Architektúra IS
- ISO/IEC/IEEE 42010:2022

Systém


Okolie
Vstup
Prvky
Hranice
Rozhrania
Vzájomné väzby
Výstup

Popis systému

- **Komponenty** *(Components),* ktoré sú buď už ďalej nedeliteľné prvky alebo spojené prvky nazývané subsystémy.
- **Vzájomný vzťah komponentov** *(Interrelationships),* ktorý znamená, že funkcie niektorých komponentov sú viazané na funkcie iných komponentov.
- **Hranice** (*Boundary),* sú ohraničenia vonkajšej a vnútornej časti systému a oddeľujú systém od jeho okolia.
- **Okolie systému** *(Environment),* predstavujúci všetko externé, ktoré je vo vzťahu so systémom.
- **Interfejsy/rozhrania** *(Interfaces),* sú body, kde sa systém stretá s okolím alebo kde sa stretajú dva subsystémy.

Popis systému

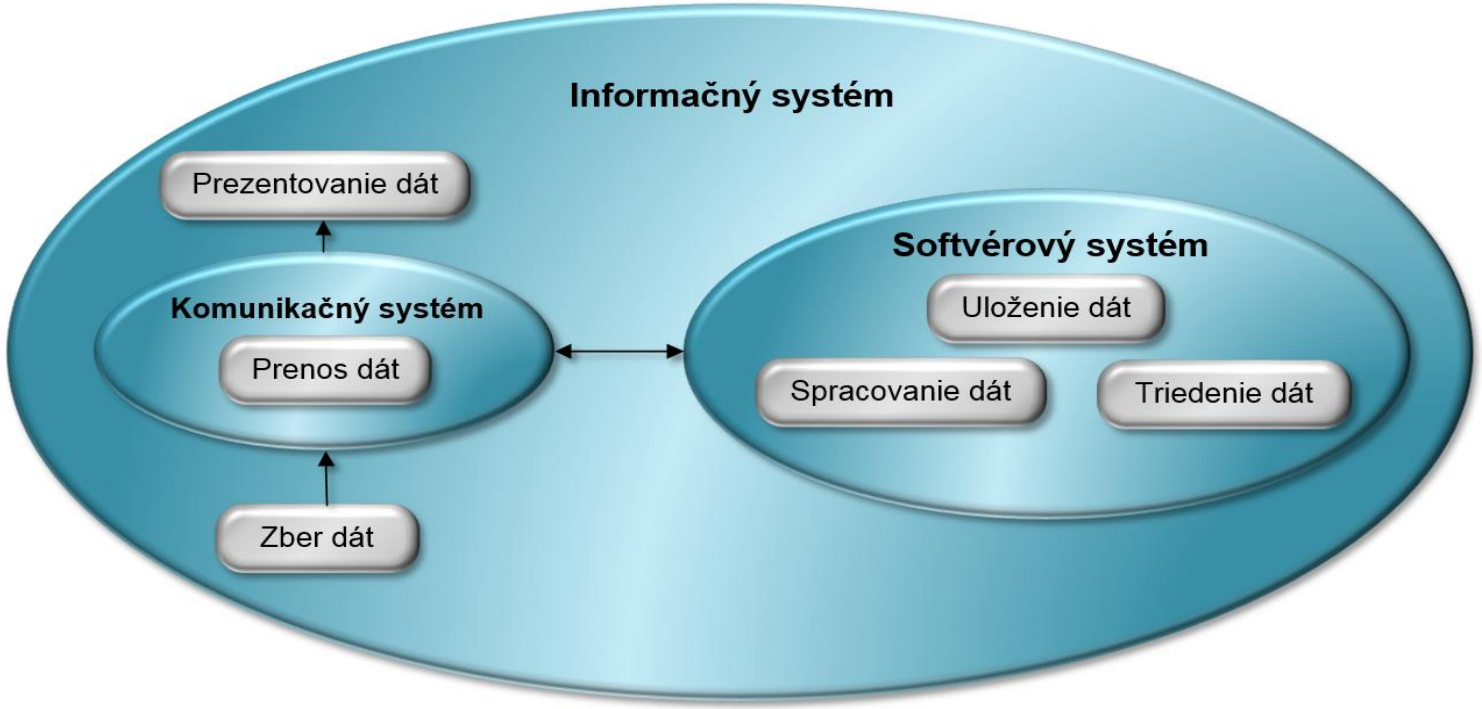
- **Vstup** *(Input),* je „čokoľvek“, čo berie systém z okolia za účelom splnenia jeho požiadavky.
- **Výstup** *(Output),* je „čokoľvek“, čo systém vracia okoliu za účelom splnenia určitej požiadavky.

Okrem vyznačených charakteristík systém musí mať špecifikovaný:

- **Dôvod existencie systému** *(Purpose),*ktorý je vyjadrený cieľom/účelom alebo hlavnou funkciou systému.
- **Obmedzenia** (*Constrain*), určujúce limity funkcionalít, ktoré môžu spĺňovať požiadavky okolia.

Informačný systém

- **„Informačný systém** je systém výmeny informácií/správ medzi ľuďmi/strojmi, ktorý využíva technické a technologické prostriedky na zber, prenos, spracovanie, triedenie a uchovanie dát za účelom ich prezentácie ako informácie/správy pre potreby používateľov.“



Architektúra

- **Architektúra (v stavebníctve a umení)**
  - Architektúra je **umenie a veda navrhovania a tvorby budov a iných stavieb**. Zahŕňa estetické, funkčné, technické a environmentálne aspekty výstavby. Architektúra ovplyvňuje spôsob, akým ľudia žijú, pracujú a vnímajú priestor.
- Zložky architektúry:
  - **Estetika** – vzhľad a štýl stavby (napr. gotická, modernistická, minimalistická)
  - **Funkčnosť** – ako dobre stavba slúži svojmu účelu
  - **Konštrukcia** – technické riešenia a materiály
  - **Kultúrny kontext** – odraz doby, spoločnosti a miesta

- **Urbanistická architektúra**
  - Zameriava sa na **plánovanie miest a verejných priestorov**, vrátane dopravy, zelene, infraštruktúry a udržateľnosti.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Architektúra IS

- V informatike architektúra označuje **štruktúru a organizáciu systémov**, napríklad:
  - **Počítačová architektúra** – ako je navrhnutý hardvér počítača (procesor, pamäť, vstupy/výstupy...)
  - **Softvérová architektúra** – ako sú usporiadané komponenty softvéru a ako spolu komunikujú atď.

- **Architektúra informačného systému** je koncepčný rámec, ktorý definuje **štruktúru, komponenty, vzťahy a princípy fungovania informačného systému**.
  - Ide o spôsob, akým sú jednotlivé časti IS navrhnuté, organizované a ako spolu komunikujú, aby efektívne podporovali podnikové procesy a ciele.

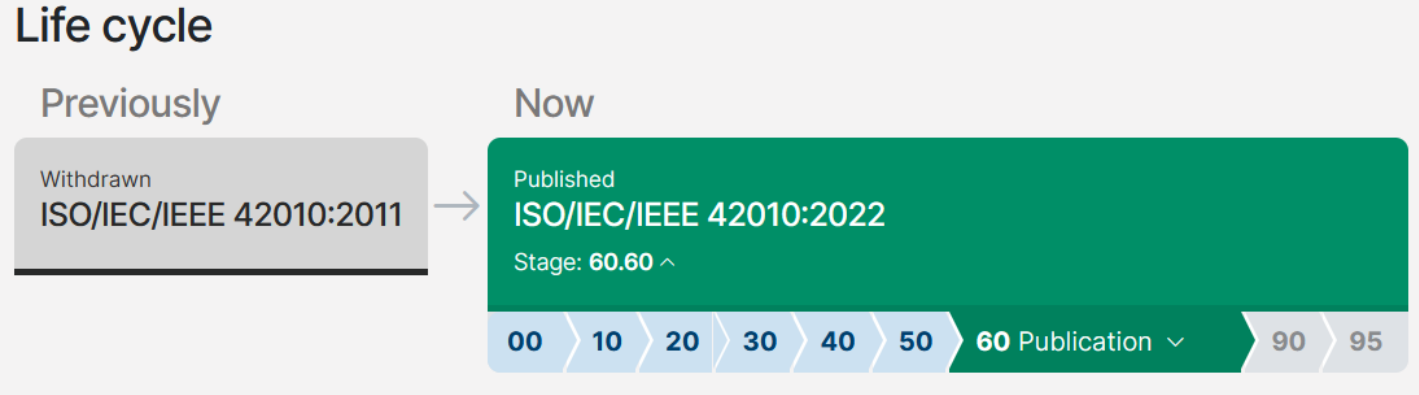
Porovnanie

Komponenty urbanistickej architektúry	Komponenty IT architektúry
Vízia mesta a urbanistický dizajn	IT stratégie a aktivity pre plánovanie
Zónovanie a prideľovanie kódov budovám	IT princípy, štandardy a postupy
Mapy a plány	Architekturálne moduly
Procesy pre zmenu plánov mesta a priestor pre možné výnimky	Procesy pre správu architektúry IS

- Pri stavbe domu sú zainteresovaní: vlastník stavby, architekt, staviteľ, statik...
  - Pri stavbe sa využívajú stavebné plány (rôzne pohľady na budovu, inštalácie...)
- Pri vývoji IS sú to: vlastník spoločnosti, užívateľ, architekt IS, analytik, vývojár...
  - Pri vývoji IS sa používa dokumentácia vývoja (postup a plány, ako realizovať vývoj IS až po jeho nasadenie v konkrétnom prostredí

Norma ISO/IEC/IEEE 42010:2022

- Norma ISO/IEC/IEEE 42010:2022 je medzinárodná norma, ktorá sa zaoberá architektúrou systémov a informačných (softvérových) systémov. Jej oficiálny názov je: "Systems and software engineering — Architecture description„
- **Zmeny oproti verzii z roku 2011**
  - Vylepšené definície a terminológia
  - Lepšia integrácia so systémovým inžinierstvom
  - Dôraz na konzistenciu medzi pohľadmi a modelmi
  - Lepšie nástroje na sledovanie požiadaviek zainteresovaných strán



Hlavné body normy ISO/IEC/IEEE 42010:2022

- Popis architektúry (Architecture Description, AD)
  - Norma definuje spôsob, akým má byť architektúra systému popísaná, aby bola konzistentná, úplná a zrozumiteľná pre všetky zainteresované strany.

- Zainteresované strany a ich záujmy (Stakeholders and Concerns)
  - Identifikuje, že rôzne zainteresované strany (napr. vývojári, zákazníci, prevádzkovatelia) majú rôzne záujmy, ktoré musí AD riešiť.

- Architektonické pohľady (Views) a perspektívy (Viewpoints)
  - Norma zavádza koncept „pohľadov“, ktoré reprezentujú architektúru z rôznych hľadísk podľa potrieb zainteresovaných strán. Každý pohľad je vytvorený podľa „perspektívy“ – definovanej šablóny, ktorá špecifikuje, čo má pohľad obsahovať.

Hlavné body normy ISO/IEC/IEEE 42010:2022

- Modely architektúry (Architectural Models)
  - Podporuje použitie modelov a diagramov na dokumentovanie jednotlivých aspektov architektúry.

- Súvislosti medzi normami
  - ISO/IEC/IEEE 42010:2022 nadväzuje na predchádzajúce vydanie z roku 2011
  - je kompatibilná s inými normami ako napríklad:
    - ISO/IEC/IEEE 15288 (systémový životný cyklus)
    - ISO/IEC/IEEE 12207 (softvérový životný cyklus)

Architektúra podľa normy ISO/IEC/IEEE 42010:2022

- Norma ISO/IEC/IEEE 42010:2022 definuje architektúru nasledovne:

„Architecture is the fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution.“

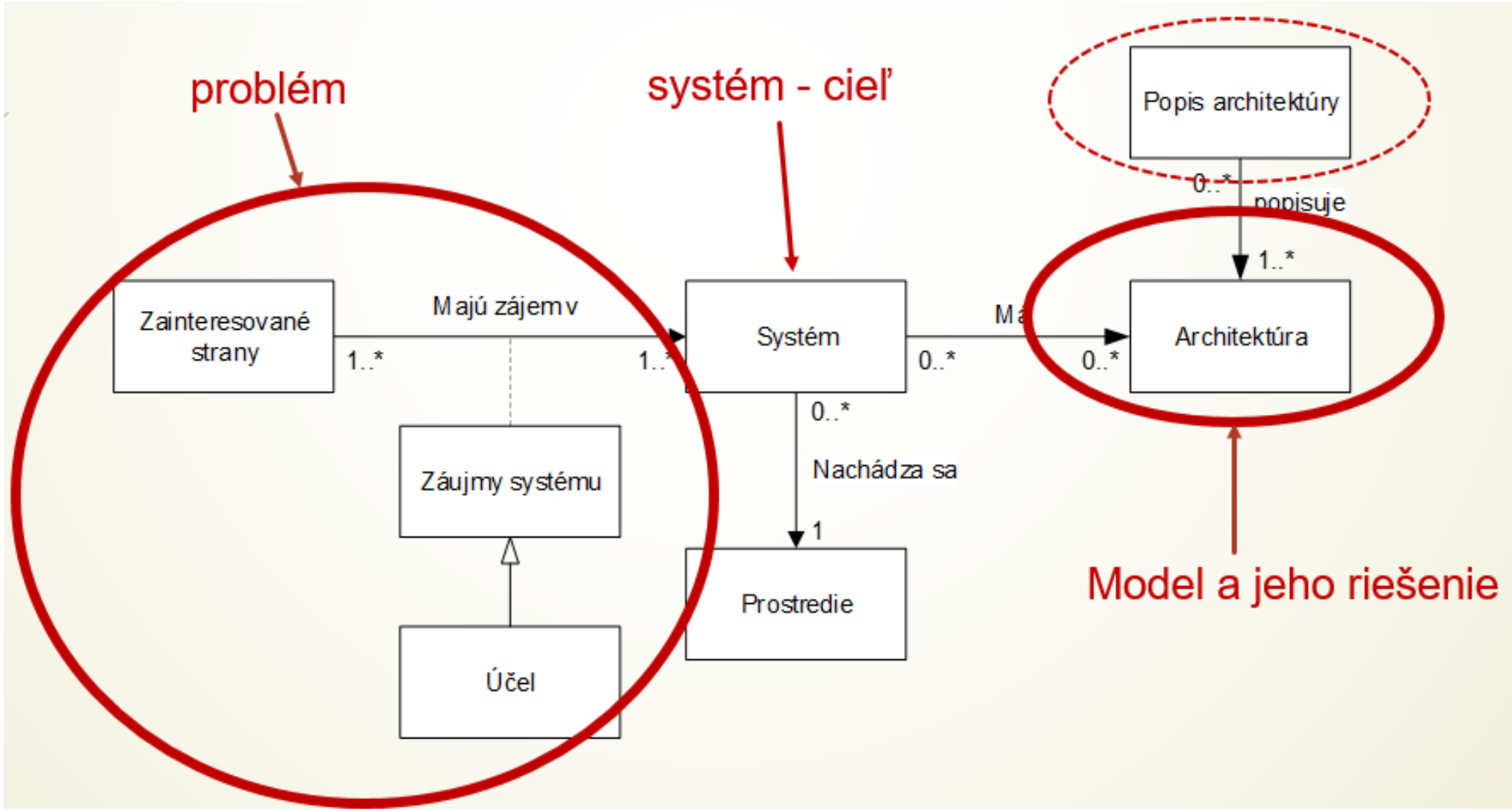
„Architektúra je súbor základných koncepcií alebo vlastností systému v jeho prostredí, ktoré sú vyjadrené prostredníctvom jeho prvkov, ich vzťahov a zásad jeho návrhu a vývoja.“

- Definícia zdôrazňuje, že architektúra **nie je len technický výkres**, ale zahŕňa aj **dôvody, kontext a princípy**, na základe ktorých bola vytvorená. To umožňuje lepšie porozumenie, komunikáciu a údržbu systémov počas celého ich životného cyklu.

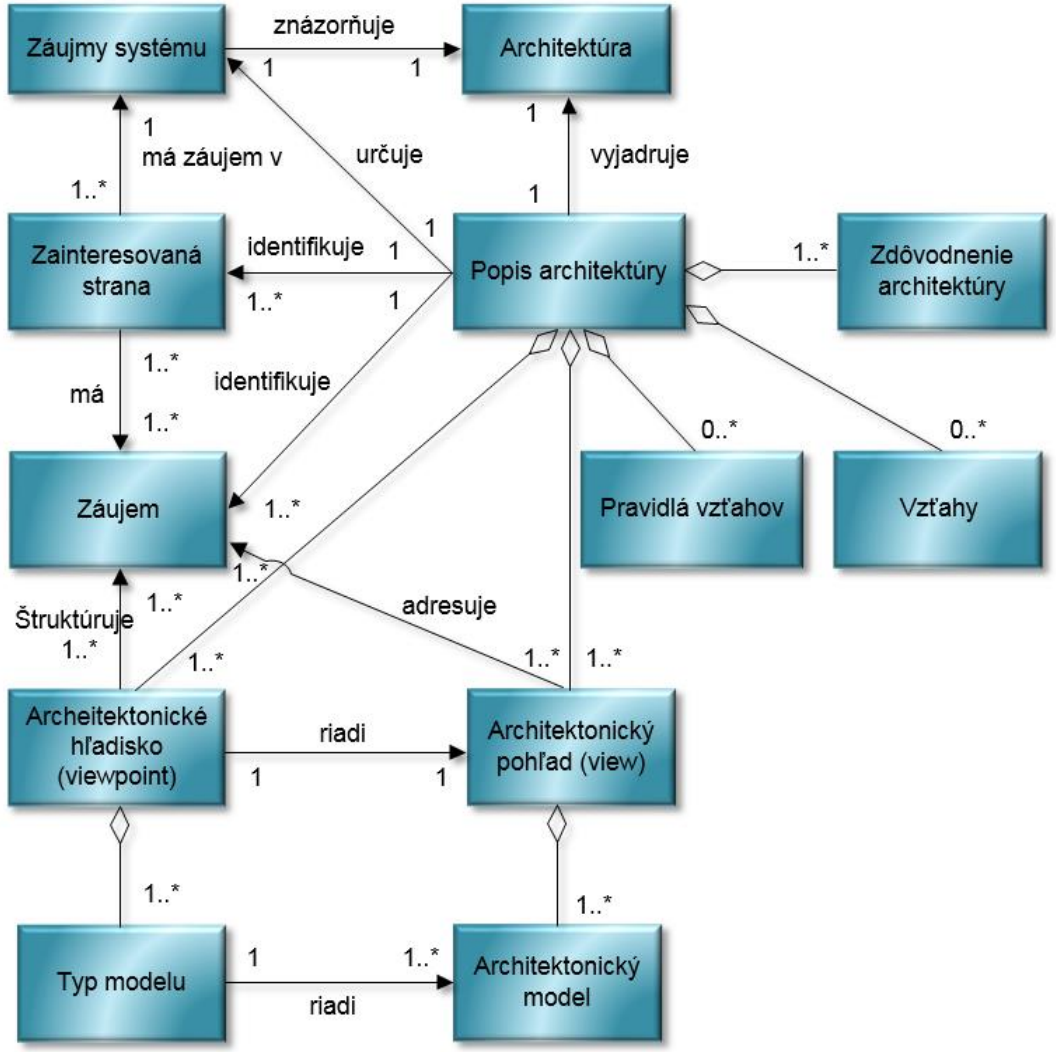
Architektúra podľa normy ISO/IEC/IEEE 42010:2022

- Základné koncepcie alebo vlastnosti
  - Architektúra neznamená len „diagramy“, ale aj koncepty ako modularita, bezpečnosť, výkonnosť, rozšíriteľnosť.
- Systém v prostredí
  - Architektúra sa nevzťahuje len na samotný systém, ale aj na jeho interakciu s vonkajším prostredím – inými systémami, užívateľmi, technológiami, atď.
- Prvky systému
  - Konkrétne komponenty, moduly, subsystémy – teda „z čoho je systém zložený“.
- Vzťahy medzi prvkami
  - Ako spolu tieto prvky komunikujú, aké majú závislosti, aké sú dátové a riadiace toky.
- Zásady návrhu a vývoja
  - Pravidlá a rozhodnutia, ktoré viedli k navrhnutiu architektúry – napríklad architektonické štýly, vzory (patterns), rozhodnutia o technológiách, atď.

Základný konceptuálny model architektúry



Popis architektúry



Koncepcia bezpečnostnej architektúry

- Zero-trust architektúra (ZTA)

Zero-trust architektúra (ZTA)

- Zero Trust architektúra (ZTA) je **bezpečnostný prístup**, ktorý vychádza z princípu:

„Nikomu never, vždy overuj.“

- **Tradičný model:** Akonáhle máš kľúč od budovy (VPN prístup), môžeš chodiť všade.
- **Zero Trust:** Pri každom dverách musíš znova preukázať identitu a oprávnenie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Základné princípy ZTA

Zero Trust Architektúra (ZTA) má svoje princípy definované v štandarde **NIST SP 800-207**

1) **Žiadna implicitná dôvera** – každý prístup (používateľ, zariadenie, aplikácia) sa overuje bez ohľadu na to, či prichádza zvnútra alebo zvonku organizácie.
2) **Overovanie identity a kontextu** – používa sa viacfaktorová autentifikácia, správa identít, kontrola polohy, zariadenia, stavu systému.
3) **Najmenšie privilégium (Least Privilege)** – používatelia a aplikácie majú len také oprávnenia, aké nevyhnutne potrebujú.
4) **Segmentácia siete a mikroslužieb** – minimalizuje sa možnosť laterálneho pohybu útočníkov.
5) **Kontinuálne monitorovanie a logovanie** – každý prístup a aktivita sa sledujú v reálnom čase.
6) **Dátová a aplikačná bezpečnosť** – ochrana citlivých dát je priamo súčasťou architektúry.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Komponenty ZTA

1. Policy Engine (PE) – rozhodovač

- Hlavný mozog Zero Trust.
- Vyhodnocuje, či má používateľ/zariadenie získať prístup k zdroju.
- Používa vstupy ako:
  - identita (ID, MFA, certifikáty),
  - stav zariadenia (patching, antivirus, MDM compliance),
  - kontext (lokácia, čas, správanie),
  - rizikové signály (SIEM, UEBA, SOAR, threat intelligence).
- Na základe toho vydá **povolenie** alebo **zákaz**.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Komponenty ZTA

2. Policy Administrator (PA) – vykonávateľ

- Preloží rozhodnutie Policy Engine do konkrétnej akcie:
  - nastavenie firewall pravidiel,
  - proxy politiky,
  - SSO tokeny,
  - API gateways.
- Typicky sú to IAM systémy, SDP controllery alebo cloudové bezpečnostné služby.

Komponenty ZTA

3. Policy Enforcement Point (PEP) – kontrolór

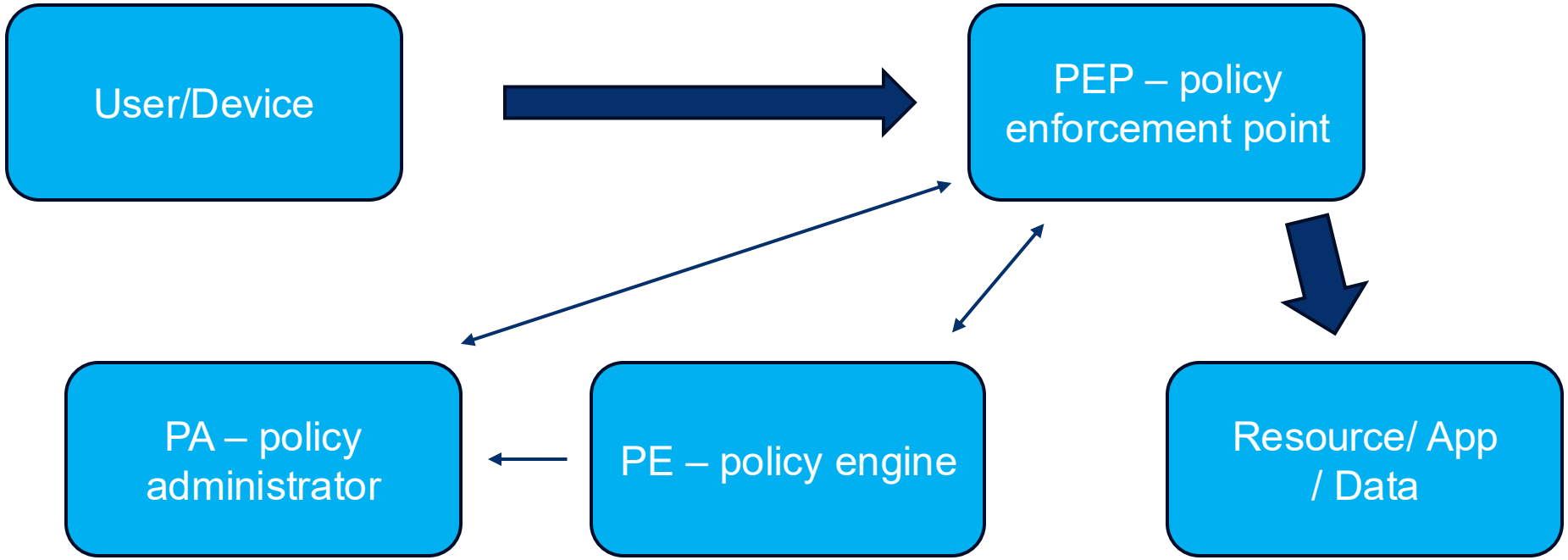
- Bod, kde sa skutočne **blokuje alebo povoľuje prístup**.
- Môže to byť:
  - aplikačný proxy,
  - API gateway,
  - mikrosegmentačný agent (napr. v endpointe),
  - cloudový access broker.

Komponenty ZTA

Doplnkové prvky architektúry:

- **Identity Provider (IdP)** – SSO, MFA, správa identít (Azure AD, Okta, Keycloak).
- **Device Management** – MDM/UEM systémy, ktoré overujú stav zariadenia.
- **Security Analytics** – SIEM, SOAR, UEBA, ktoré dodávajú signály o hrozbách.
- **Data Security** – DLP, šifrovanie, klasifikácia dát.
- **Network segmentation** – mikrosegmentácia, softvérové definované perimeter (SDP).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



každá žiadosť o prístup sa overuje v reálnom čase a nikdy sa nepovažuje za automaticky dôveryhodnú.

Tok prístupu ZTA

1) Používateľ alebo zariadenie požiada o prístup k zdroju.
2) PEP zachytí žiadosť a odošle ju PE.
3) PE vyhodnotí podmienky (identity, device health, risk scoring).
4) PA aplikuje rozhodnutie (vydá token, nastaví pravidlo).
5) PEP buď pustí, alebo odmietne spojenie.
6) Neustále monitorovanie – ak sa stav zmení (napr. zariadenie sa stane kompromitovaným), prístup sa okamžite zruší.

Príklad

1. Používateľ/Zariadenie → PEP
•Žiadosť o prístup k aplikácii alebo dátam prechádza cez **Policy Enforcement Point**.
2. PEP → PE/PA
•PEP odosiela požiadavku na **Policy Engine** a **Policy Administrator**, aby overili identitu, stav zariadenia a kontext.
3. Policy Engine (PE)
•Vyhodnotí politiku prístupu (identity, rizikové signály, stav zariadenia, lokalita, čas).
•Rozhodne **grant / deny / conditional access**.
4. Policy Administrator (PA)
•Preloží rozhodnutie PE do konkrétnych pravidiel – vydanie tokenu, nastavenie firewallu, proxy politiky a pod.
5. PEP → Resource
•PEP pustí alebo zablokuje prístup k aplikácii / dátam podľa rozhodnutia PE/PA.
6.Kontinuálne monitorovanie
•Aj po udelení prístupu sa všetko monitoruje.
•Ak sa stav zmení (napr. zariadenie stratí compliance, detekuje sa hrozba), prístup sa okamžite odoberie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Prečo používať ZTA

- Kybernetické útoky sú čoraz sofistikovanejšie.
- Rastúci počet vzdialených používateľov (home office).
- Cloudové služby a hybridné IT prostredia rušia jasný perimeter siete.
- Organizácie potrebujú **odolnejší a flexibilnejší bezpečnostný model**.

👉 ZTA je **ekosystém**, kde sa nepredpokladá žiadna dôvera a každý request je validovaný cez **PE → PA → PEP**, pričom všetko je pod dohľadom monitoringu a adaptívnej politiky.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Referenčné modely podnikovej architektúry

- TOGAF
- Zachman framework
- FEA (Federal Enterprise Architecture)

TOGAF

- TOGAF je architektonický rámec resp. metodika, ktorý vyvinula Open Group „na poskytovanie metód a nástrojov na pomoc pri akceptovaní, produkcii, používaní a údržbe podnikovej architektúry (všeobecne, nielen IT)“
  - The Open Group je dodávateľsky a technologicky neutrálne konzorcium, ktorého vízia Boundaryless Information Flow™ umožní prístup k integrovaným informáciám v rámci podnikov a medzi nimi na základe otvorených štandardov a globálnej interoperability

- TOGAF je založený na **iteratívnom modeli procesov** podporovanom osvedčenými postupmi a opakovane použiteľným súborom existujúcich aktív architektúry

Vývoj TOGAFu

- TOGAF verzia 1 vznikla v roku 1994
- Na základe rámca technickej architektúry pre správu informácií (TAFIM), ktorý vyvinulo Ministerstvo obrany USA (DoD)
- Z tohto základu The Open Group Architecture Forum vyvinulo v pravidelných intervaloch následné verzie TOGAF
- Fórum architektúry otvorenej skupiny vyvinulo následné verzie TOGAF
- Aktuálna verzia je **TOGAF 10** z roku 2022

Architektúra v kontexte TOGAF

- ISO/IEC/IEEE 42010 definuje „architektúru“ ako **usporiadanie systému, ktorý tvoria komponenty a vzťahy medzi nimi, vrátane vzťahov k prostrediu a princípy, ktoré riadia jeho vývoj a návrh“**

- TOGAF túto definíciu prijíma a rozširuje. V TOGAF má „architektúra“ dva významy v závislosti od kontextu:
  - **Formálny popis** systému alebo podrobný plán systému na úrovni komponentov na usmernenie jeho implementácie
  - **Štruktúra komponentov**, ich vzájomné vzťahy a princípy a usmernenia, ktorými sa riadi ich dizajn a vývoj v čase.

TOGAF – podniková architektúra

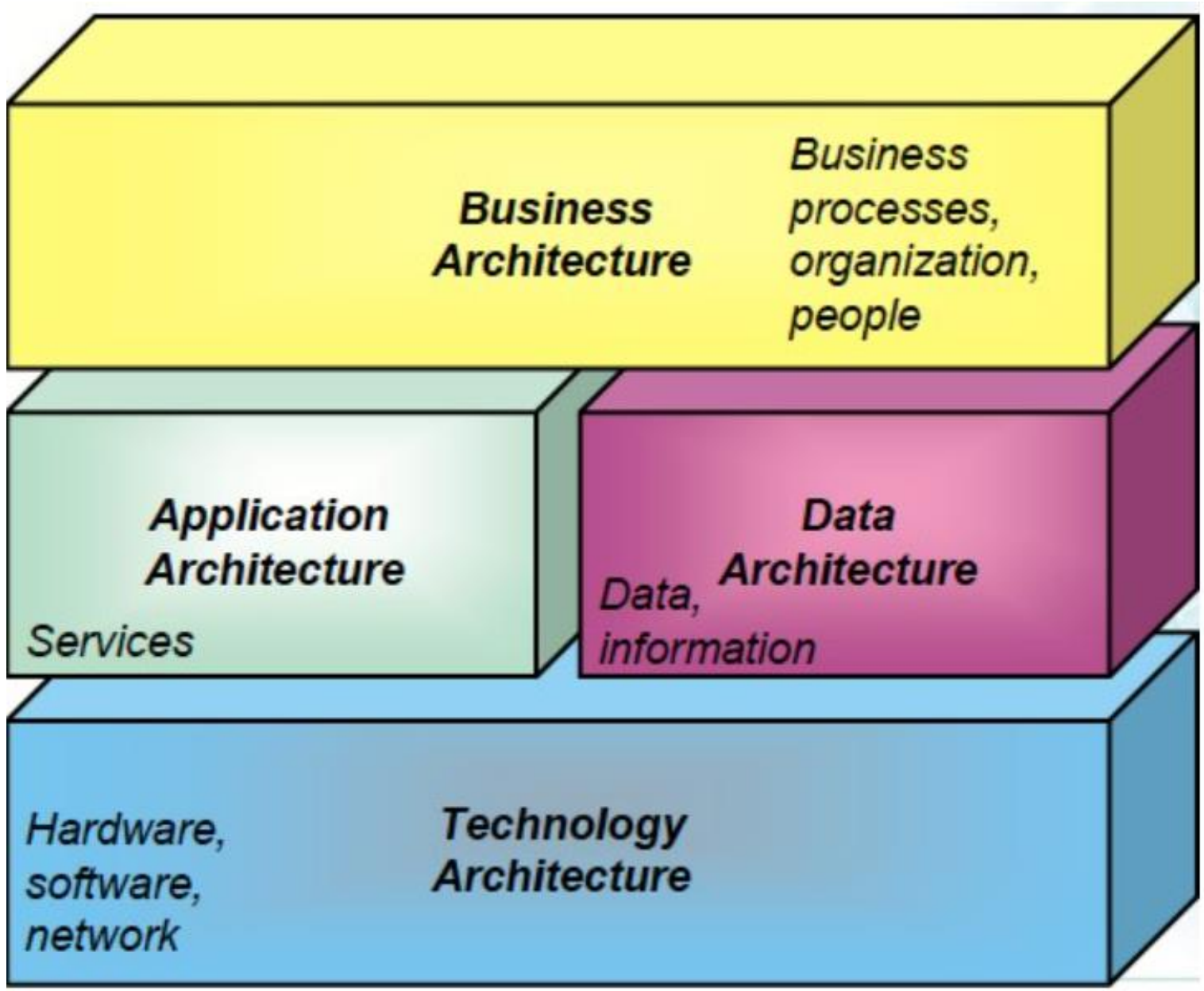
- Obchodná/Business/ architektúra – Obchodná stratégia, riadenie, organizácia a kľúčové obchodné procesy.

- Dátová architektúra – štruktúra logických a fyzických dátových aktív organizácie a zdrojov na správu dát.

- Aplikačná architektúra – plán pre jednotlivé aplikácie, ktoré sa majú nasadiť, ich interakcie a vzťahy s hlavnými obchodnými procesmi organizácie.

- Technologická architektúra – Logické funkcie softvéru a hardvéru, ktoré sú potrebné na podporu nasadenia obchodných, dátových a aplikačných služieb.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

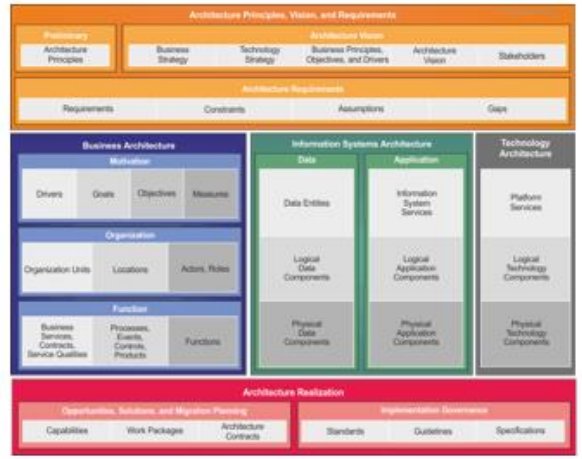

Business Architecture
Business processes, organization, people
Application Architecture
Services
Data Architecture
Data, information
Technology Architecture
Hardware, software, network

TOGAF štruktúra

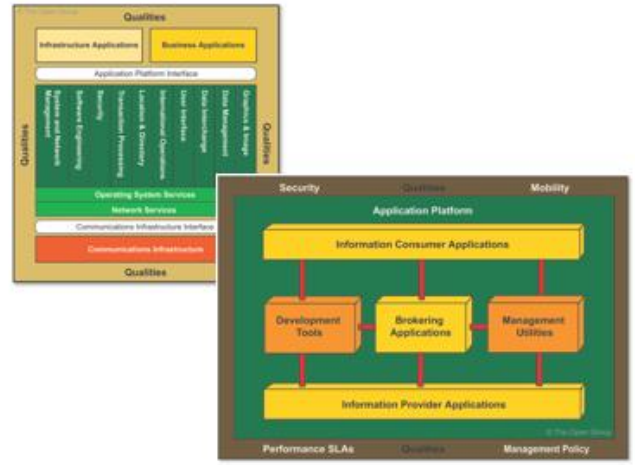
1. Úvod
2. Metóda vývoja architektúry - ADM
3. Pokyny a techniky ADM
4. Rámec obsahu architektúry
5. Enterprise Continuum & Tools
6. Referenčné modely TOGAF
7. Rámec schopností architektúry

ADM

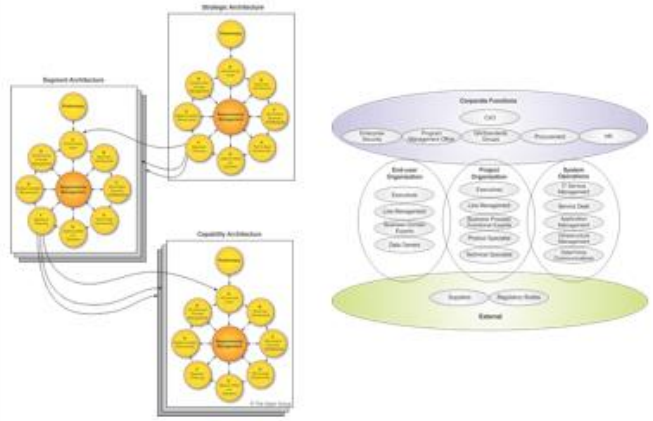
Architecture Content Framework



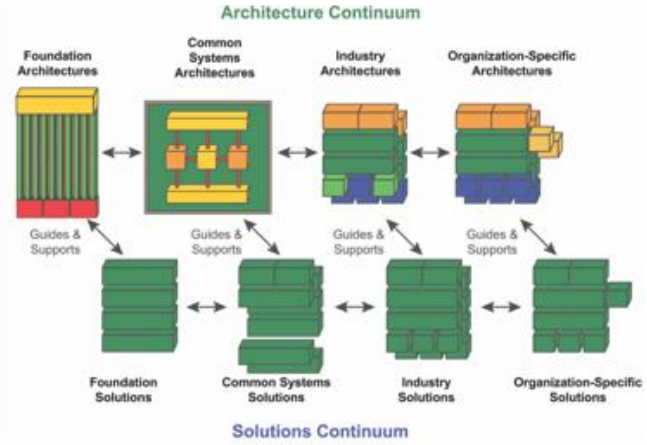
Reference Models



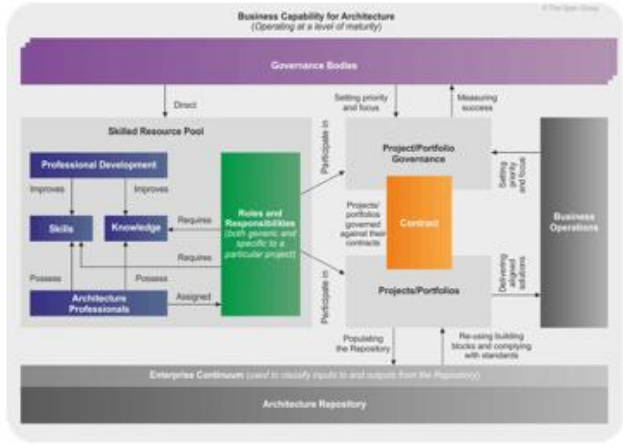
ADM Guidelines & Techniques



Enterprise Continuum



Architecture Capability Framework

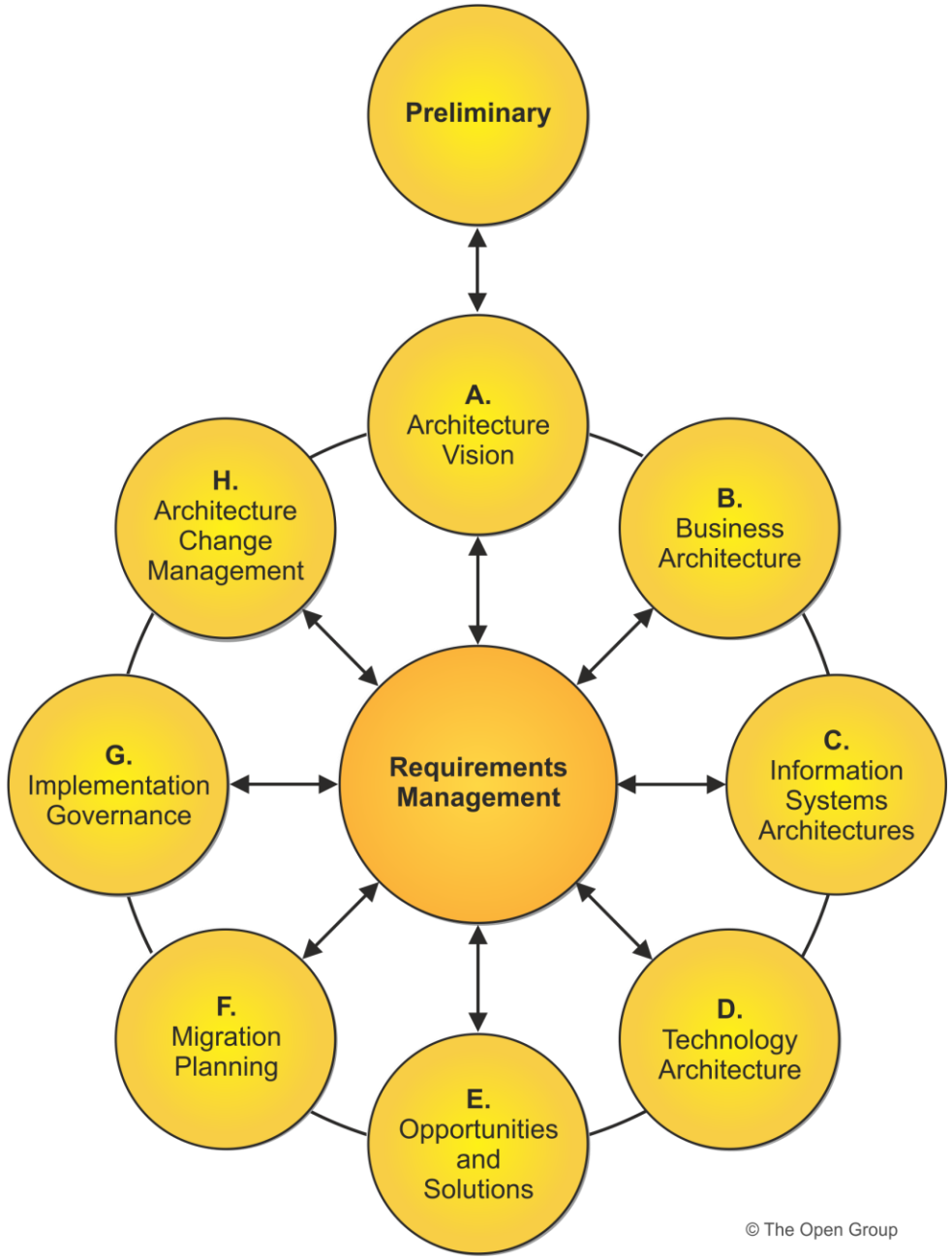


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Architecture development method = ADM

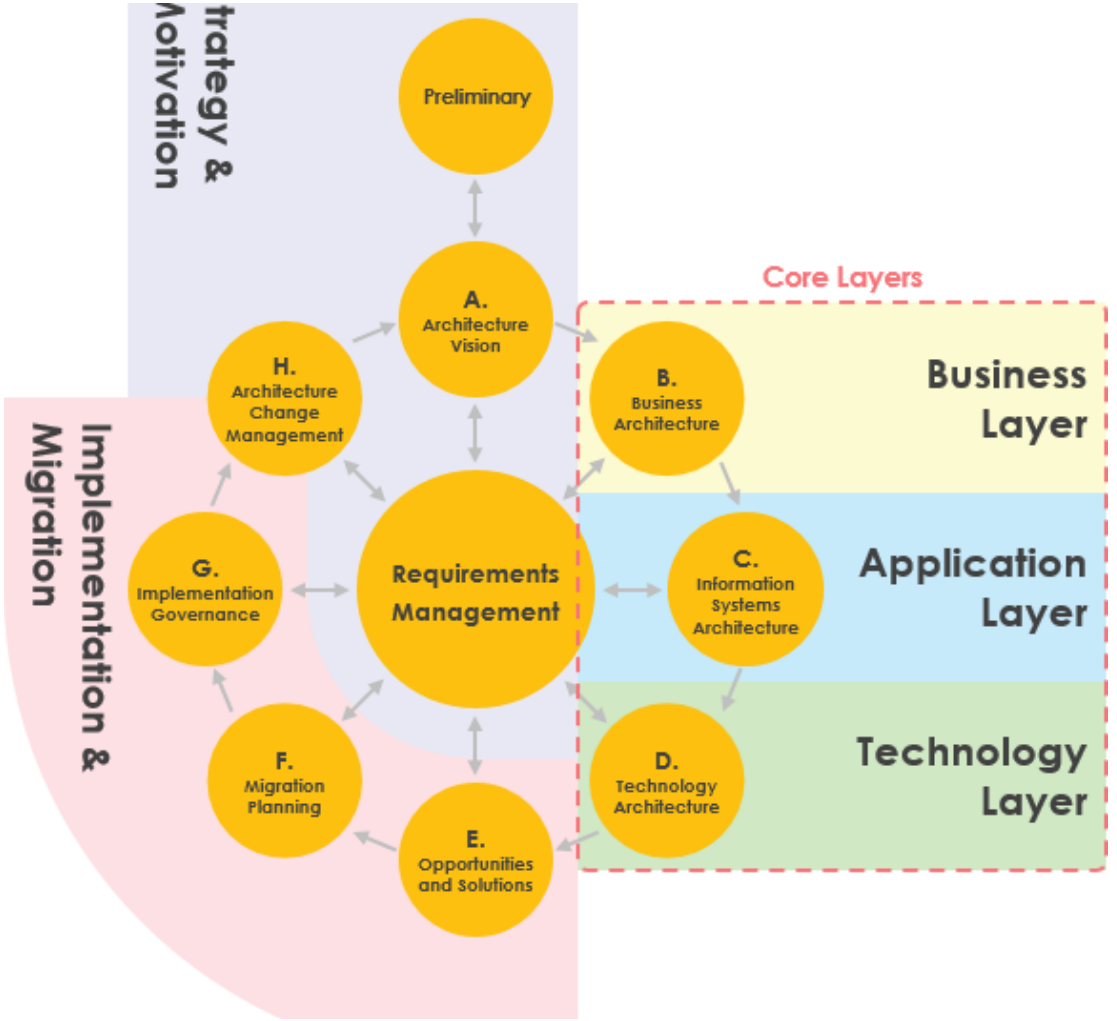
- Metóda vývoja architektúry poskytuje testovaný a opakovateľný proces vývoja podnikových architektúr

- ADM zahŕňa:
  - Vytvorenie rámca architektúry
  - Rozvíjanie obsahu architektúry
  - Prechod
  - Riadenie realizácie architektúr
-
- ADM sa vykonáva v rámci iteratívneho cyklu a umožňuje organizáciám transformovať svoje podniky riadeným spôsobom v reakcii na obchodné ciele a príležitosti



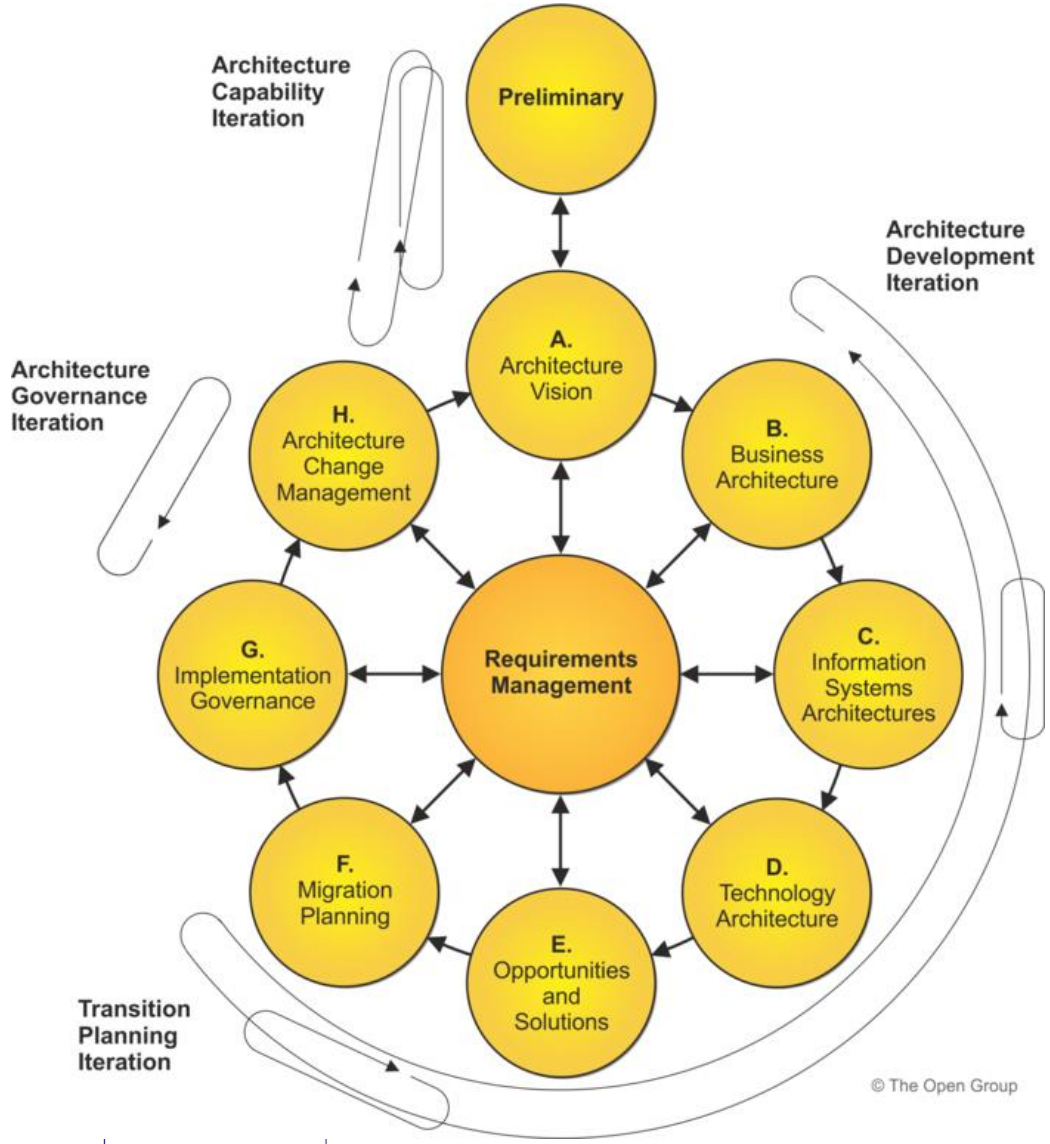
ADM: fáza po fáze

- Prístup krok po kroku
- Metóda pre vývoj EA
- Jadro pre TOGAF
- Pomáha vytvoriť rámec TOGAF



ADM: iterácie

- ADM je iteratívny proces
- Iterácie vznikajú:
  - počas celého procesu
  - medzi jednotlivými fázami
  - v rámci jednotlivých fáz
- Nové rozhodnutia



ADM fázy

- **Predbežná fáza** popisuje prípravné a iniciačné činnosti potrebné na prípravu na splnenie obchodnej smernice pre novú podnikovú architektúru, vrátane definície rámca Organizačno-špecifickej architektúry a definície princípov.
- **Fáza A:** Vízia architektúry opisuje počiatočnú fázu cyklu vývoja architektúry. Zahŕňa informácie o definovaní rozsahu, identifikácii zainteresovaných strán, vytváraní vízie architektúry a získavaní súhlasov.
- **Fáza B:** Business Architecture opisuje vývoj obchodnej architektúry na podporu dohodnutej vízie architektúry.
- **Fáza C:** Architektúra informačných systémov opisuje vývoj architektúr informačných systémov pre projekt architektúry, vrátane vývoja dátových a aplikačných architektúr.

ADM fázy

- **Fáza D:** Technologická architektúra opisuje vývoj technologickej architektúry pre projekt architektúry.
- **Fáza E:** Opportunities & Solutions vykonáva počiatočné plánovanie implementácie a identifikuje dodávacie vozidlá pre architektúru definovanú v predchádzajúcich fázach.
- **Fáza F:** Plánovanie migrácie sa zaoberá formuláciou súboru podrobných sekvencií prechodových architektúr s podporným plánom implementácie a migrácie.
- **Fáza G:** Riadenie implementácie poskytuje architektonický dohľad nad implementáciou.
- **Fáza H:** Riadenie zmien architektúry stanovuje postupy na riadenie zmien novej architektúry.

THE ZACHMAN FRAMEWORK

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zachman framework

- Zachman Framework je **metodologický rámec** používaný na **modelovanie a organizáciu podnikovej architektúry**.
- Pomáha organizáciám systematicky premýšľať o tom, ako sú ich procesy, systémy, dáta a technológie navzájom prepojené.
- Zachman Framework **matica/mriežka** je vizualizovaný ako tabuľka s **6 radmi** (perspektívy) a **6 stĺpcami** (otázky).
  - Každá bunka (36) je **kombináciou jednej otázky (stĺpec)** a **jednej perspektívy (riadok)**.
  - Bunka predstavuje **konkrétny artefakt alebo model**, ktorý odpovedá na určitú otázku z určitého pohľadu.

ZACHMAN FRAMEWORK

	Data What	Function How	Network Where	People Who	Time When	Motivation Why
Objective /Scope *(Contextual)* **Role:** Planner	List of Things Important in the Business	List of Business Processes	List of Business Locations	List of Important Organizations	List of Events	List of Business Goals & Strategies
Enterprise Model *(Conceptual)* **Role:** Owner	Conceptual Data/Object Model	Business Process Model	Business Logistics System	Workflow Model	Master Schedule	Business Plan
System Model *(Logical)* **Role:** Designer	Logical Data Mode	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Technology Model *(Physical)* **Role:** Builder	Physical Data / Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Detailed Representation *(Out of Context)* **Role:** Programmer	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Speculation
Functioning Enterprise **Role:** User	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

Zachman framework

- **6 základných otázok (stĺpce):**
  - **What** – Dáta (napr. informácie, ktoré organizácia používa)
  - **How** – Funkcie (procesy, ktoré sa vykonávajú)
  - **Where** – Miesta (lokalizácia, sieťová architektúra)
  - **Who** – Ľudia (účastníci, roly)
  - **When** – Čas (časové aspekty, plánovanie)
  - **Why** – Motivácia (ciele, stratégie)

Zachman framework

- **6 perspektív (rady):**
  - **Planner** – Koncepčný pohľad (napr. podniková vízia)
  - **Owner** – Pohľad vlastníka (napr. požiadavky biznisu)
  - **Designer** – Systémový návrh (napr. logická architektúra)
  - **Builder** – Implementačný pohľad (napr. technická špecifikácia)
  - **Subcontractor** – Detailný pohľad (napr. kód, konfigurácia)
  - **Functioning Enterprise** – Prevádzkový pohľad (reálne fungovanie)

Zachman framework – bunky (príklady)

- **Príklad: Bunka „What“ + „Owner“ (Dáta z pohľadu vlastníka)**
  - **Otázka:** *Čo?* → Aké dáta sú dôležité?
  - **Perspektíva:** *Owner* → Biznis pohľad (napr. manažér)
  - **Obsah bunky:** Biznis entity a ich vzťahy (napr. zákazník, objednávka, produkt)
  - **Forma:** Konceptuálny model dát (napr. ER diagram)

- **Ďalší príklad: Bunka „How“ + „Designer“ (Procesy z pohľadu návrhára)**
  - **Otázka:** *Ako?* → Aké procesy sa vykonávajú?
  - **Perspektíva:** *Designer* → Logický návrh systému
  - **Obsah bunky:** Logické procesné modely (napr. BPMN diagramy)
  - **Forma:** Popis tokov informácií a rozhodnutí

Zachman framework – bunky (príklady)

- **Bunka „Where“ + „Builder“ (Lokalita z pohľadu vývojára)**
  - **Otázka:** *Kde?* → Kde sa veci dejú?
  - **Perspektíva:** *Builder* → Technická implementácia
  - **Obsah bunky:** Sieťová architektúra, servery, uzly
  - **Forma:** Deployment diagram, sieťové mapy

- **Bunka „Why“ + „Planner“ (Motivácia z pohľadu plánovača)**
  - **Otázka:** *Prečo?* → Aké sú ciele?
  - **Perspektíva:** *Planner* → Strategický pohľad
  - **Obsah bunky:** Vízia, misia, strategické ciele
  - **Forma:** Balanced Scorecard, strategické dokumenty

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zachman framework – záver

- Je to **referenčný rámec**, nie konkrétna metodika alebo nástroj – nehovorí *ako* veci robiť, ale *čo* treba zohľadniť.
- **Na čo sa používa?**
  - Na **zlepšenie komunikácie** medzi IT a biznisom
  - Na **analýzu komplexných systémov**
  - Na **plánovanie digitálnej transformácie**
  - Na **dokumentáciu podnikovej architektúry**
- Každá bunka odpovedá na **jednu otázku** z **konkrétneho pohľadu** a vytvára **artefakt**, ktorý je súčasťou celkovej podnikovej architektúry.
- Zachman Framework tak pomáha zabezpečiť, že nič dôležité neunikne – od stratégie až po implementáciu.

FEAF

means

Federal Enterprise Architecture Framework

Federal Enterprise Architecture framework

- Federal Enterprise Architecture Framework (FEAF) je **architektonický rámec vyvinutý vládou USA**, konkrétne **Office of Management and Budget (OMB)**, na podporu **koordinácie a integrácie IT systémov** v rámci federálnych agentúr.
  - FEAF I vznikla v roku 1999 - definovala základné princípy enterprise architektúry pre federálne agentúry
  - FEAF II vznikla v roku 2012 – viac dôrazu na stratégie, segmentovú architektúru a praktické implementačné príklady + doplnený Security Reference Model
- FEAF predstavuje **strategický nástroj** na riadenie a koordináciu IT systémov vo verejnej správe USA.
  - Jeho cieľom je zlepšiť **efektivitu, interoperabilitu a transparentnosť** verejného sektora.
- FEAF je postavený na **konceptoch podnikovej architektúry**, podobne ako Zachman alebo TOGAF, ale je špecificky navrhnutý pre potreby verejnej správy.

Základné komponenty FEAF

- **1. Enterprise Architecture (EA) – „celková strecha“**
  - Pokrýva celú organizáciu alebo federálnu agentúru
  - Stanovuje víziu, princípy a štandardy
  - Zabezpečuje jednotnosť medzi jednotlivými segmentmi
- **2. Core Mission Segments (CMS)**
  - Segmenty, ktoré priamo podporujú hlavnú misiu a strategické ciele organizácie.
  - Príklad: u ministerstva zdravotníctva by to mohli byť segmenty „verejné zdravie“ alebo „bezpečnosť potravín“.
- **3. Business Services Segments (BSS)**
  - Podporné segmenty, ktoré poskytujú spoločné biznis služby využívané viacerými organizačnými jednotkami.
  - Príklad: ľudské zdroje, financie, obstarávanie
- **4. Enterprise Services Segments (ESS)**
  - Technické a infraštruktúrne služby, ktoré podporujú všetky ostatné segmenty.
  - Zahŕňajú napr. IT infraštruktúru, dátové služby, komunikačné platformy, bezpečnosť

Reference Models FEAF

- FEAF používa **6 referenčných modelov**
- Referenčné modely spoločne tvoria **Common Approach to Federal Enterprise Architecture**, čo umožňuje federálnym agentúram plánovať, porovnávať a koordinovať IT a biznis riešenia jednotným/spoločným spôsobom.
- **Consolidated Reference Model (CRM)** tvorí **integrovaný pohľad** na všetky referenčné modely, ktorý umožňuje
  - integráciu referenčných modelov - združuje všetky **referenčné modely FEAF** do jedného súdržného rámca.
  - spoločný slovník a klasifikačný systém - definuje, **ako popisovať procesy, služby, údaje, technológie a výkonnosť** rovnakým spôsobom v celej federálnej vláde
  - porovnateľnosť a interoperabilita - umožňuje **porovnávanie architektúr, identifikáciu redundancií a prepojení** medzi agentúrami
  - podpora rozhodovania - uľahčuje **strategické plánovanie a investičné rozhodnutia**

Reference Models FEAF

- 1. Performance Reference Model (PRM) - identifikuje biznis procesy (napr. monitorovanie, reporting..)
  - Zameriava sa na meranie výkonnosti programov a služieb
  - Prepojuje ciele organizácie s výsledkami a umožňuje sledovať efektívnosť a hodnotu pre občanov
- 2. Business Reference Model (BRM) - definuje dátové entity (napr. údaje o znečistení ...)
  - Klasifikuje funkcie a služby, ktoré vláda poskytuje (nie organizačné štruktúry, ale činnosti)
  - Pomáha identifikovať duplicity a zlepšiť koordináciu medzi agentúrami
- 3. Data Reference Model (DRM) - vyberie vhodné aplikácie
  - Popisuje, ako sa dáta zbierajú, spravujú a zdieľajú
  - Podporuje interoperabilitu a štandardizáciu dátových štruktúr

Reference Models FEAF

- 4. Application Reference Model (ARM) - navrhne infraštruktúru (napr. servery, senzory)
  - Rámec pre softvérové aplikácie a služby
  - Pomáha porovnávať, ktoré aplikácie podporujú ktoré obchodné funkcie
- 5. Infrastructure Reference Model (IRM) - zabezpečí ochranu dát
  - Popisuje technologickú infraštruktúru (servery, siete, platformy)
  - Podporuje štandardizáciu technológií a znižovanie redundancie
- 6. Security Reference Model (SRM) - nastaví metriky výkonnosti
  - Zavedený vo FEAF II
  - Poskytuje rámec pre riadenie bezpečnosti a ochrany údajov naprieč architektúrami

Federal Enterprise Architecture framework - záver

- FEAF je vhodný najmä pre **veľké organizácie** s komplexnou štruktúrou, ktoré potrebujú **koordinovať rôzne systémy a služby** v rámci jednej architektúry.
- FEAF je založený na **referenčných modeloch**, ktoré pokrývajú oblasti ako biznis procesy, dáta, aplikácie, infraštruktúra, bezpečnosť a výkonnosť.
  - Tieto modely umožňujú **štandardizované plánovanie, analýzu a rozhodovanie**.

- **Ciele FEAF:**
  - **Zlepšiť spoluprácu** medzi federálnymi agentúrami
  - **Znížiť duplicitu** IT systémov
  - **Zvýšiť transparentnosť** a zodpovednosť
  - **Podporiť strategické rozhodovanie**

Priestor na otázky

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

Milan Kubina

KC KYB UNIZA, https://kc.uniza.sk/

milan.kubina@fri.uniza.sk