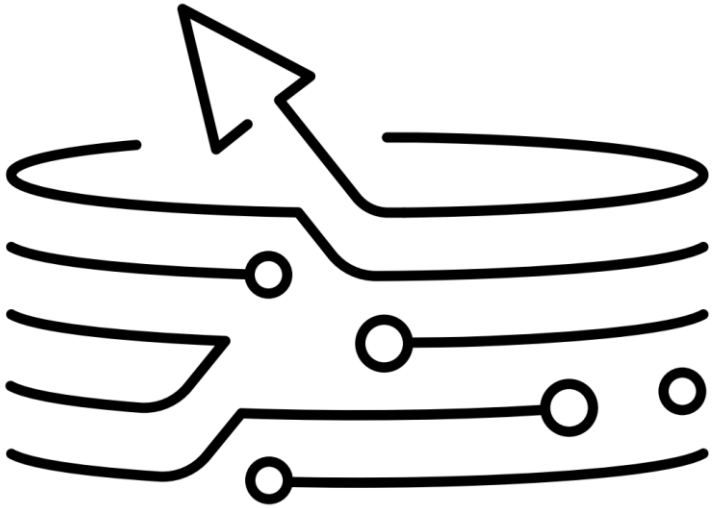
FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ústav telekomunikací



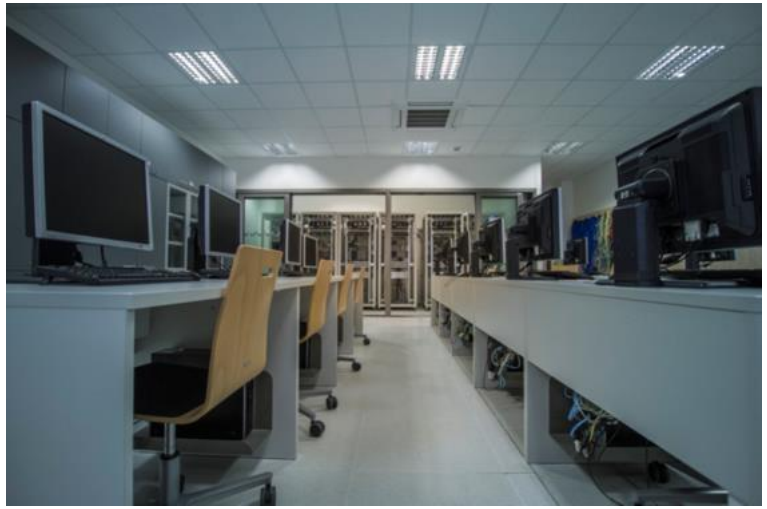
BUTCA

Moderní vzdělávání v kyberbezpečnosti: BUTCA, mikrocertifikáty a profesní trénink

doc. Ing. Jan Hajný, Ph.D.
Bc. Willi Lazarov

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

- **Fakulta elektrotechniky a komunikačních technologií**
  - Ústav telekomunikací
  - Applied Cryptography & Security Engineering Group
  - https://www.utko.fekt.vut.cz/
  - https://axe.vut.cz
- **R&D činnosti v kyberbezpečnosti**
  - Moderní kryptografie
  - Kvantové a postkvantové technologie
  - Průmyslové sítě, KII, energetika
- **Služby v kyberbezpečnosti**
  - Zátěžové testování, DDoS testy, digitální dvojčata, …
- **Vzdělávání a profesní trénink**



Vzdělávání v oblasti kyberbezpečnosti

- **Současné studijní programy**
  - Informační bezpečnost (Bakalářský stupeň)
    - zhruba 100 studentů v ročníku, > 200 zájemců
    - akreditace od roku 2015
    - https://www.vut.cz/studenti/programy/program/8431
  - Informační bezpečnost (Magisterský stupeň)
    - zhruba 50 studentů v ročníku
    - akreditace od roku 2018
    - https://www.vut.cz/studenti/programy/program/8369
  - Informační bezpečnost (Doktorský stupeň)
    - méně než 10 studentů v ročníku
    - akreditace od roku 2020
    - https://www.vut.cz/studenti/programy/program/8398
- **Specifika studia na FEKT VUT**
  - Kombinace technického a netechnického vzdělávání (IT, vývoj, sítě, právo, ekonomie), silně prakticky zaměřené s využitím moderních technologií (virtualizace, cyber range, HW vybavení laboratoří).

Spolupráce, projekty

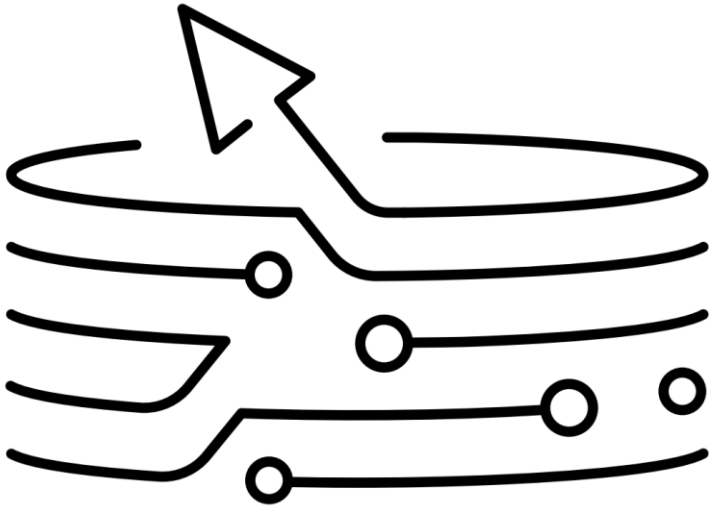
- **Partneři v rozvoji vzdělávání**
  - European Union Agency for Cybersecurity (ENISA) – rámec ECSF
  - Národní úřad pro kybernetickou a informační bezpečnost (NUKIB) – koordinace programů
  - Národní kvalifikační rámec (CyQUAL) – harmonizace s ostatními univerzitami, prac. trhem
  - Pracovní skupiny NIST NICE (USA), CyBoK (VB)
  - Další univerzity, instituce, firmy, spolky, školy…

- **Flagship projekt SPARTA**
  - Velký Horizon 2020 projekt s 44 partnery a 16 mil. EUR rozpočtem
  - VUT vedlo WP9: Cybersecurity training and awareness
  - Doba realizace: 2019 – 2022

- **Výsledky**:
  - Education Map: https://www.sparta.eu/study-programs/
  - Curricula Designer: https://www.sparta.eu/curricula-designer/
  - Články: https://www.sparta.eu/papers/

Vybavení – ukázka

- **Laboratoř kvantové bezpečnosti**
  - Zahrnuje zařízení kvantové a postkvantové kryptografie
  - Unikátní sada v rámci ČR
  - Vznik na základě projektu Network security in post-quantum era (NESPOQ, MVČR)
  - Součástí infrastruktury pro výuku v oborech Informační bezpečnost
  - Jeden z prvních prvků Národní kvantové sítě
- Další infrastruktura:
  - CyberGrid, 5G+ Lab, IoT Lab, Palo Alto, …
  - Kyber-fyzický polygon (průmysl a energetika)



BUTCA

Profesní vzdělávání

Profesní vzdělávání – současný stav

Aktuální problémy

- Nedostatek odborníků na kybernetickou bezpečnost vs. vysoká poptávka na prac. trhu.
  - Legislativní požadavky na obsazení pozic KB v kritické informační infrastruktuře,
  - zvýšený počet incidentů – nutnost intenzivně řešit KB, tj. přijímat nové zaměstnance, rekvalifikovat či doškolit stávající.
- Omezená možnost poskytnout vzdělání a trénink mimo běžné studijní programy.
  - Programy pro vzdělávání v KB vznikají, mnohdy nekoncepčně a narychlo.
  - Kombinované či dálkové programy jsou na ústupu.

Situace na FEKT VUT v Brně

- Aktuálně je nabízen program Informační bezpečnost na všech stupních, tj. bakalářském, magisterském a doktorském.
- Zájem ca. 200 přihlášek za rok.
- Poptávka na poskytování vzdělávání a tréninku zaměstnanců externích subjektů je řešena individuálně a zakázkově (ČEZ, E.GD, ČTÚ, …).

Profesní vzdělávání – mikrocertifikáty

Návrh programu pro profesní vzdělávání

- Koncepční řešení na základě požadavků komerčního sektoru.
- Propojení požadavků firem na obsah, formu a časový harmonogram s možnostmi VUT.
- Spojení relevantních částí dle vyučované problematiky (ICT, vývoj, netechnické disciplíny, …).
- Silné zaměření na reálné dovednosti, praktický hands-on training a reálné prostředí v ČR (legislativa, ekonomika).
- Využití BUTCA[1] pro lokální i vzdálený trénink.
- Provázání s tzv. skills frameworky (ENISA ECSF[2], NIST NICE[3], CyQUAL[4]).
- Zakončeno tzv. mikrocertifikátem k předmětu, modulu i programu s možností transferu ECTS.
- Možnost pokračování v běžném studiu s uznáním předmětů.

1 https://butca.vut.cz/

2 https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

3 https://www.nist.gov/itl/applied-cybersecurity/nice

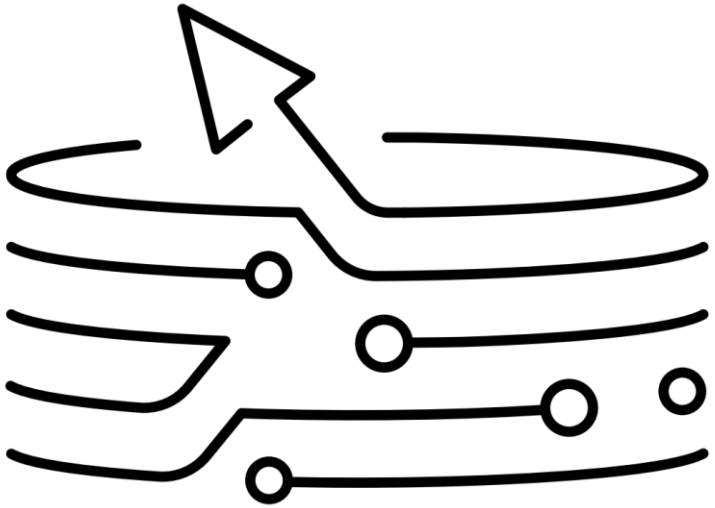
4 https://platform.cyqual.cz

Profesní vzdělávání – mikrocertifikáty

Pracovní parametry programu

- Délka trvání: 1 rok
- Struktura: 3 doporučené průchody, 6 modulů po 3 předmětech
- Harmonogram:
  - Září: zahájení, osobní konzultace
  - Září – Prosinec: přednášky (e-learning/online) + individuální konzultace
  - Leden: Výuka v laboratořích – blokově 1 týden
  - Únor – Květen: přednášky (e-learning/online) + individuální konzultace
  - Červen: Výuka v laboratořích– blokově 1 týden
- Zakončení: mikrocertifikát
- Cena: ~ LLM/MBA

https://forms.gle/GNe82QE11MAskL8PA



BUTCA

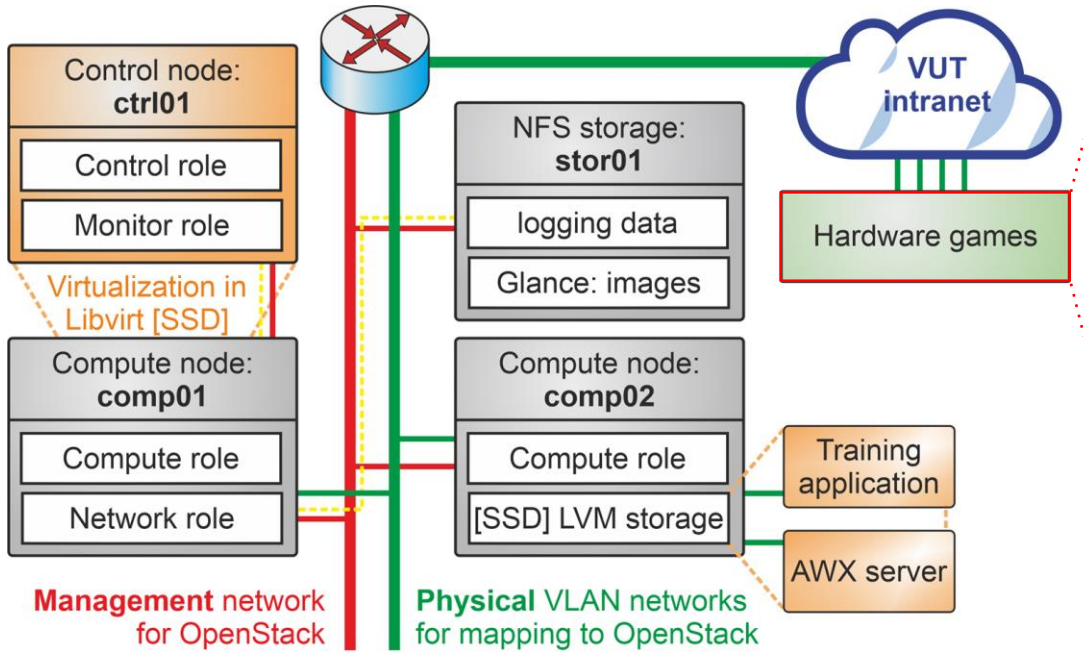
BUTCA: Platforma pro trénink kybernetické bezpečnosti

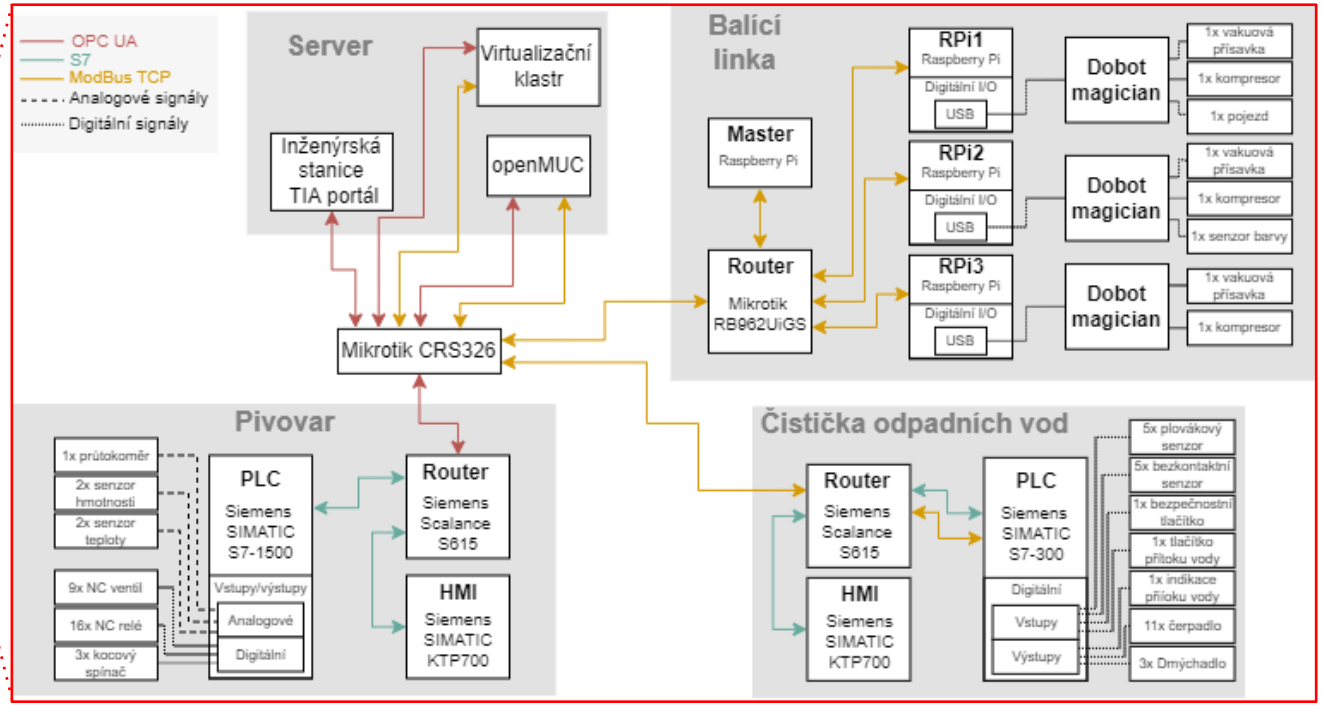
Kybernetická aréna

- Platforma BUTCA (Brno University of Technology Cyber Arena) byla vytvořena s primárním cílením na **výzkum**, **trénink** a **výuku** kybernetické bezpečnosti.
- Platforma cílí na **vzdělávání na více stupních (SŠ, VŠ)** a **školení v komerční sféře**.
- Klíčové parametry:
  - **Uživatelské rozhraní** – webová aplikace (FE, BE a DB).
  - **Scénáře** – vlastní edukační scénáře a trénink formou CTF.
  - **Automatizace** – Ansible AWX (nasazení, obnova prostředí, …).
  - **Cloudová platforma** – OpenStack (virtuální stroje, orchestrace, …).
- Výhoda našeho řešení:
  - jednoduchost ve vytváření scénářů,
  - zaměření na bezpečnost průmyslu a energetiky,
  - využití gamifikace pro podpoření edukace.

Kyber-fyzický polygon

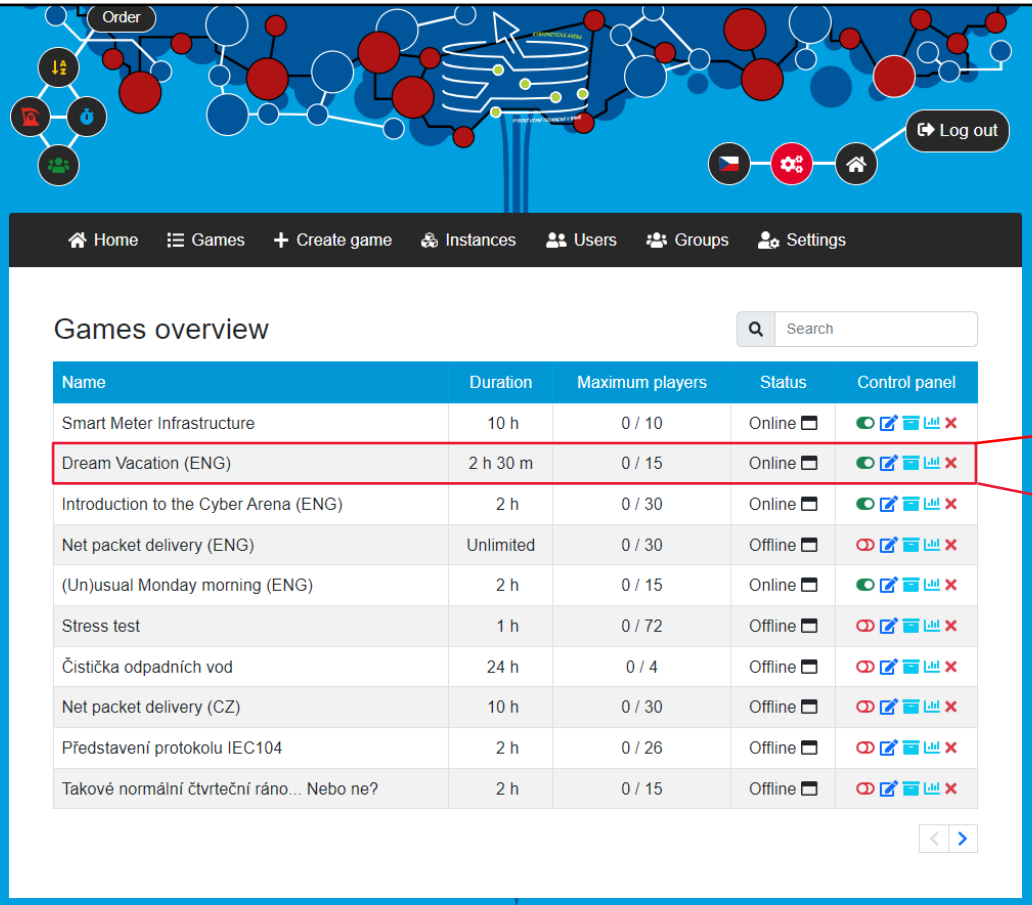
- Kyber-fyzický polygon se skládá z reálných zařízení připojených do IT a OT sítě.
- Momentálně 3 hlavní oblasti: **průmysl**, **energetika** a **voda**.
- Polygony: **fyzické**, **virtuální** a **hybridní**.

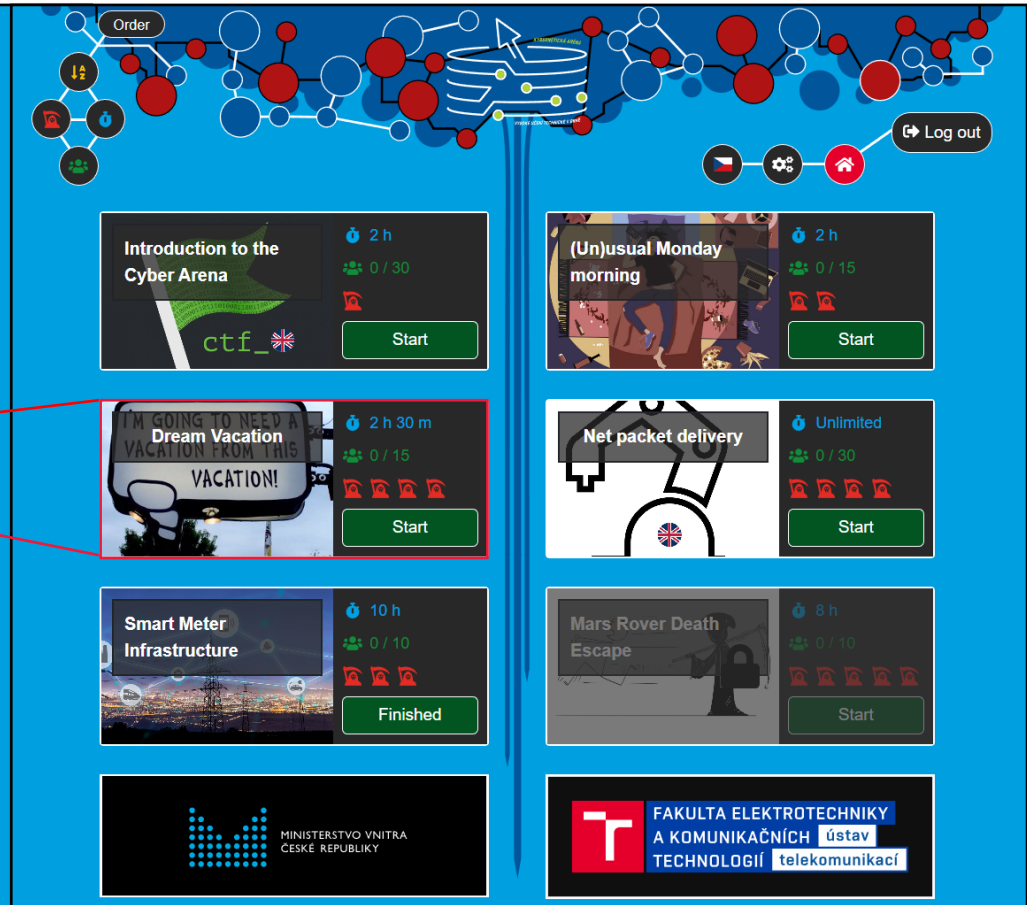




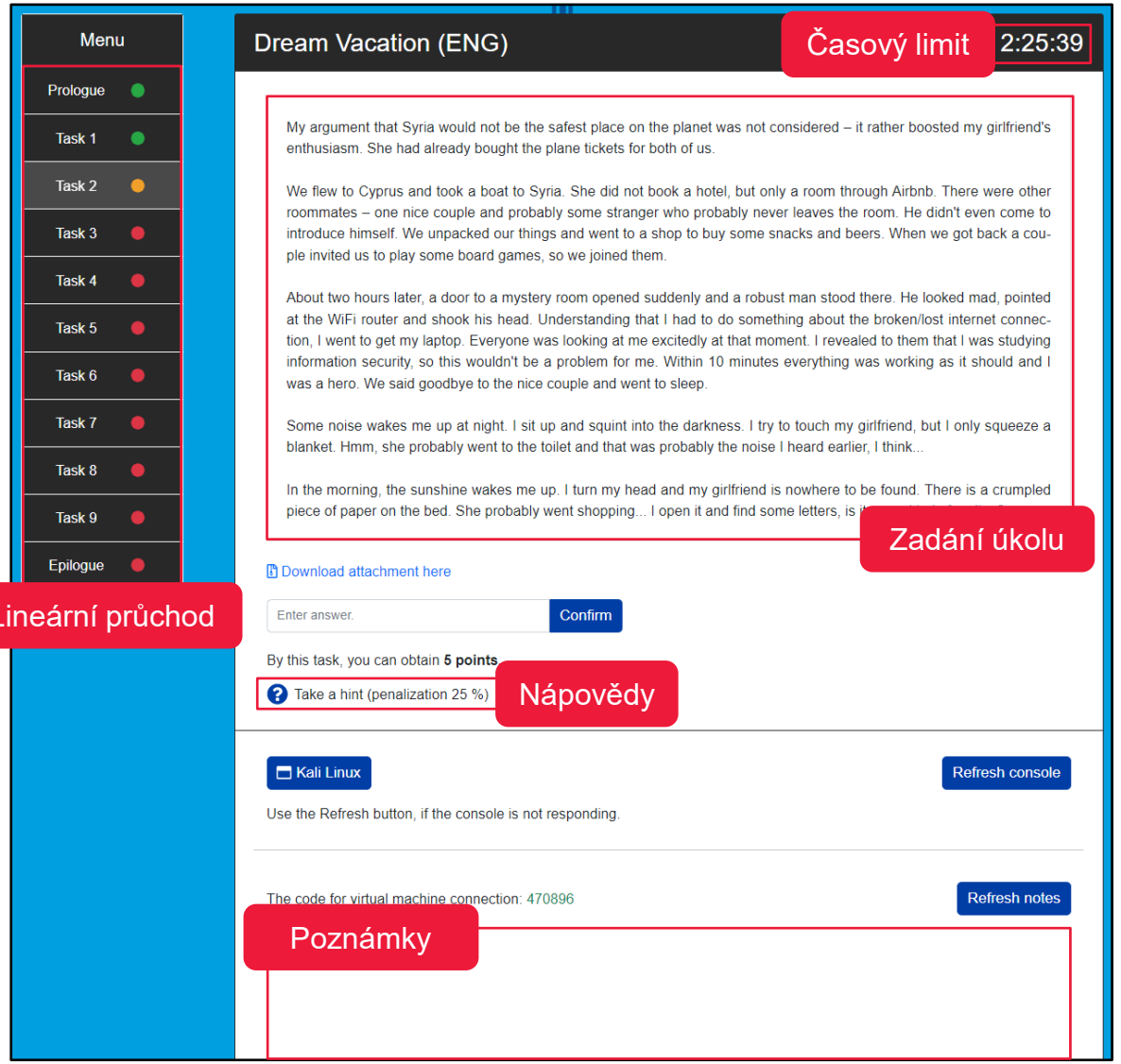
Správa a realizace scénářů

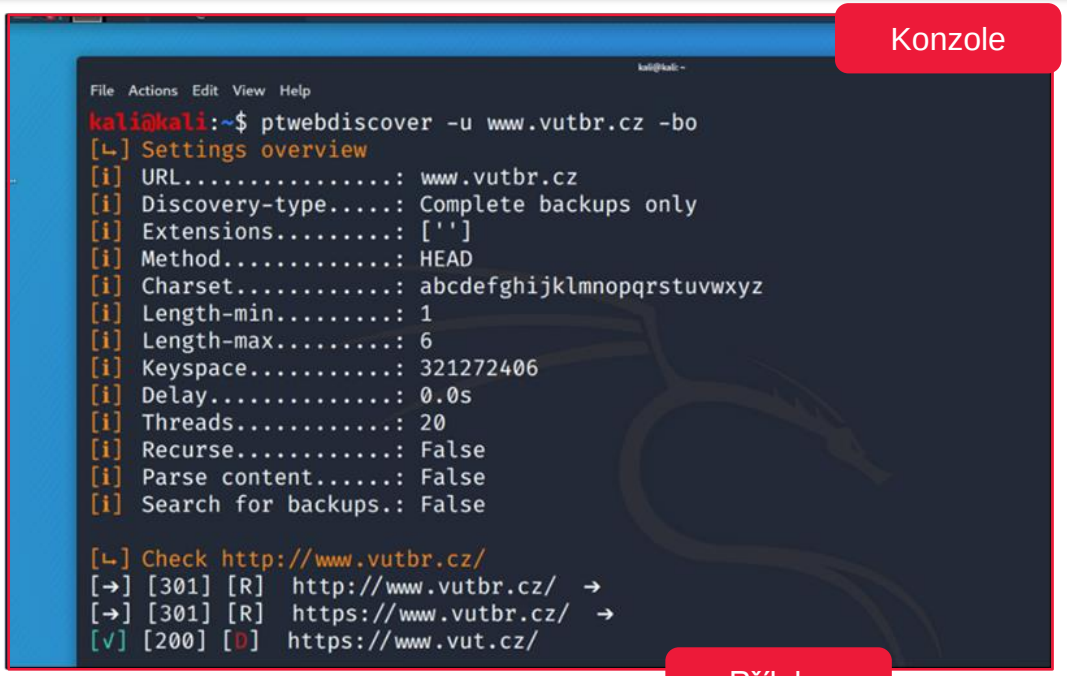
- Vlastní administrace bez nutnosti přihlášení do cloudové platformy OpenStack.



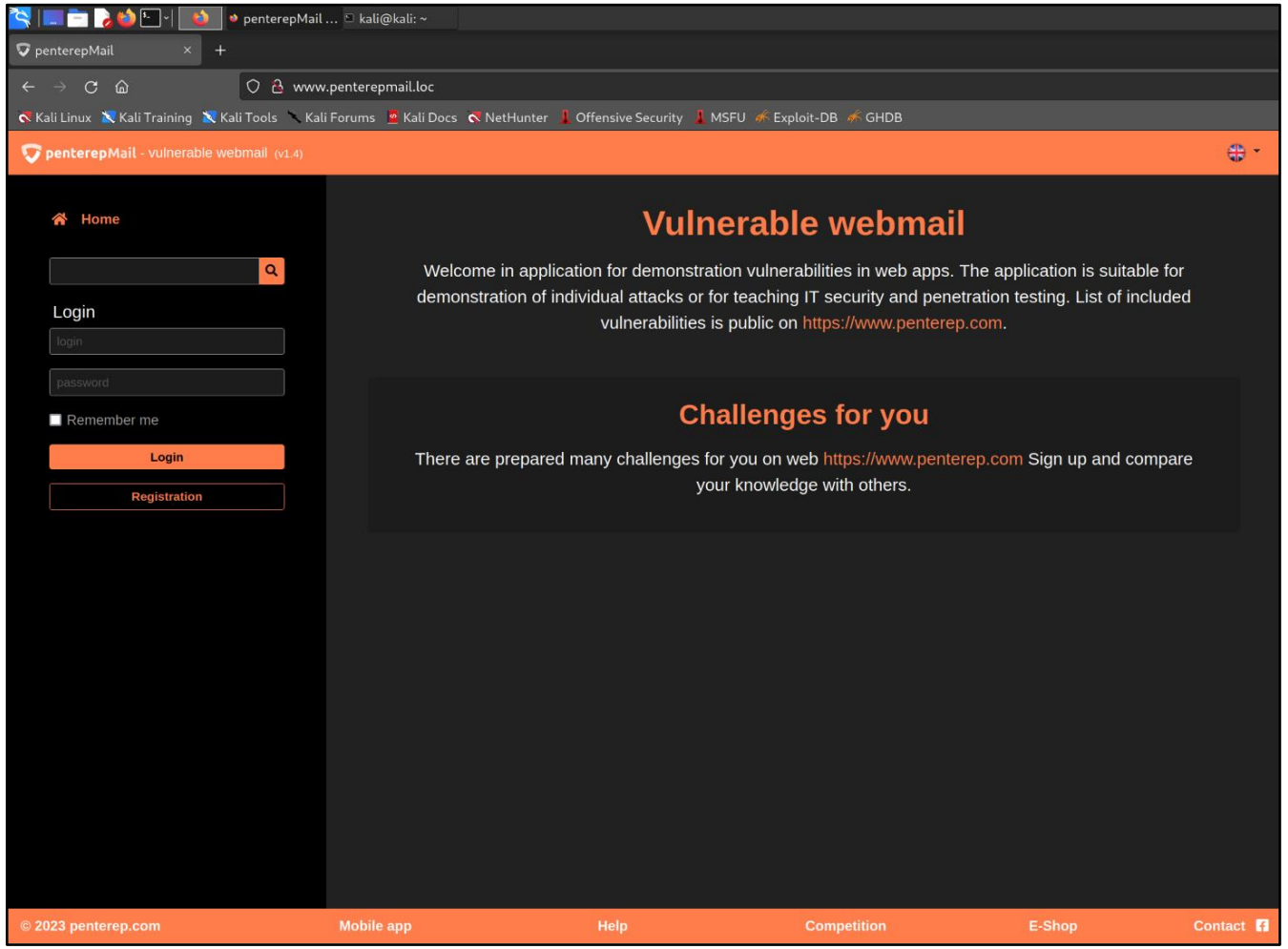


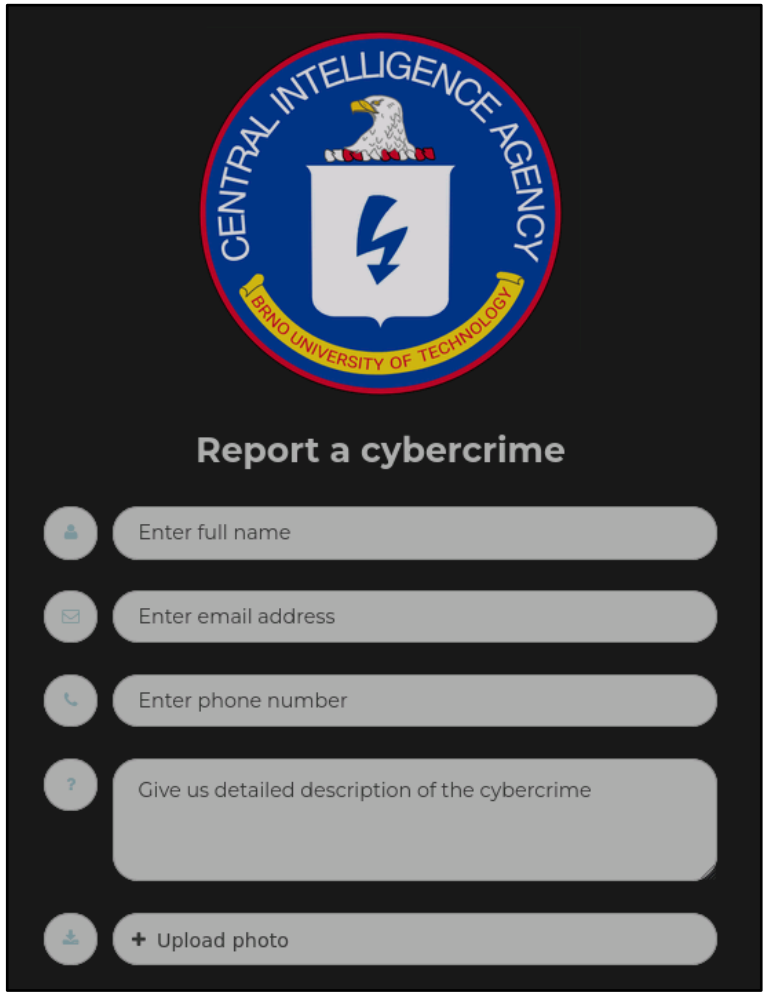
Správa a realizace scénářů





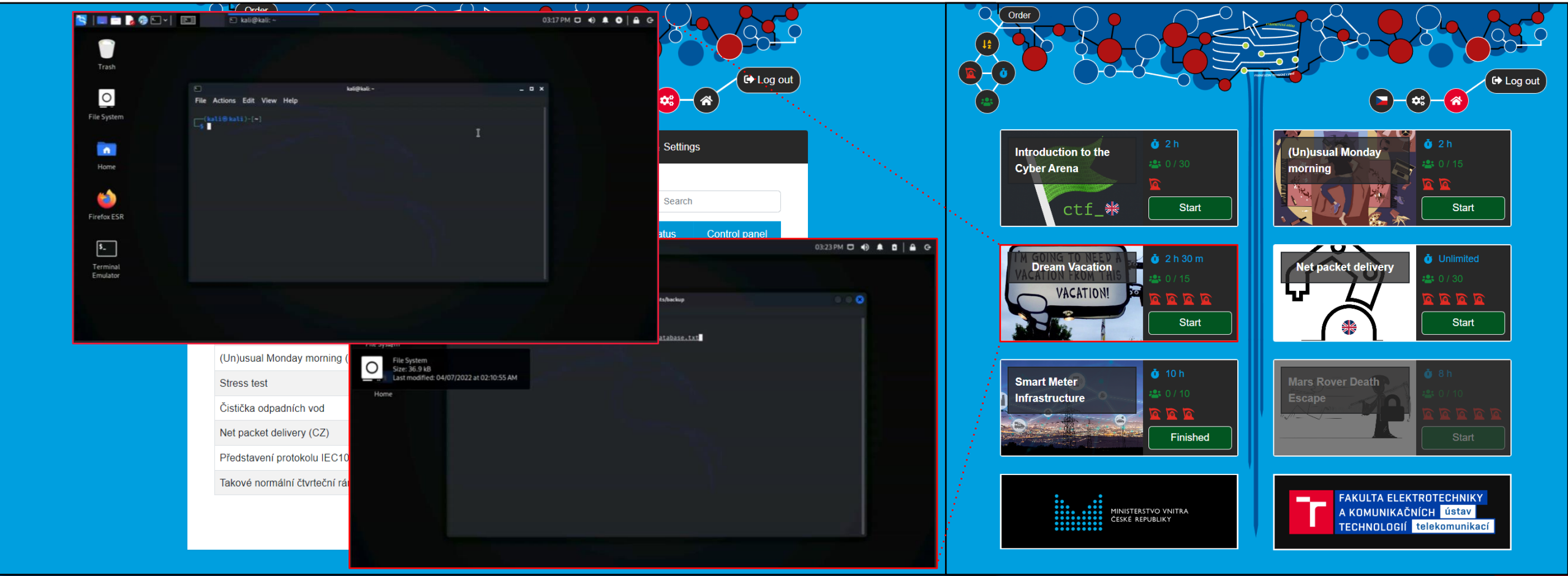
Správa a realizace scénářů





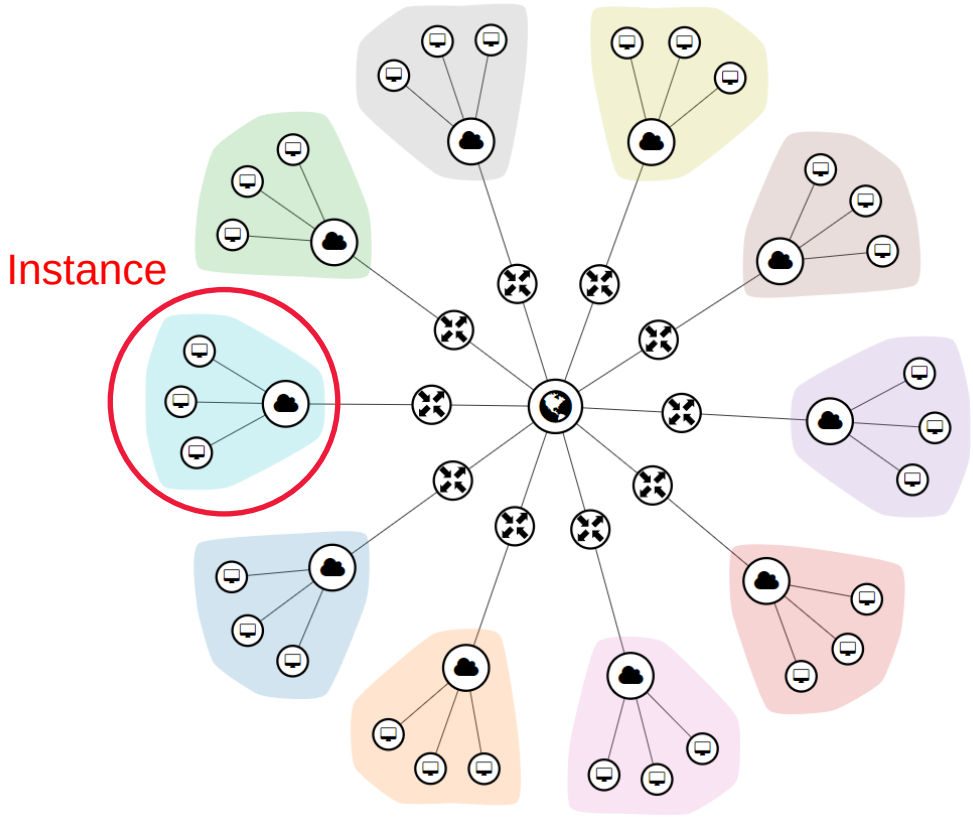
Správa a realizace scénářů

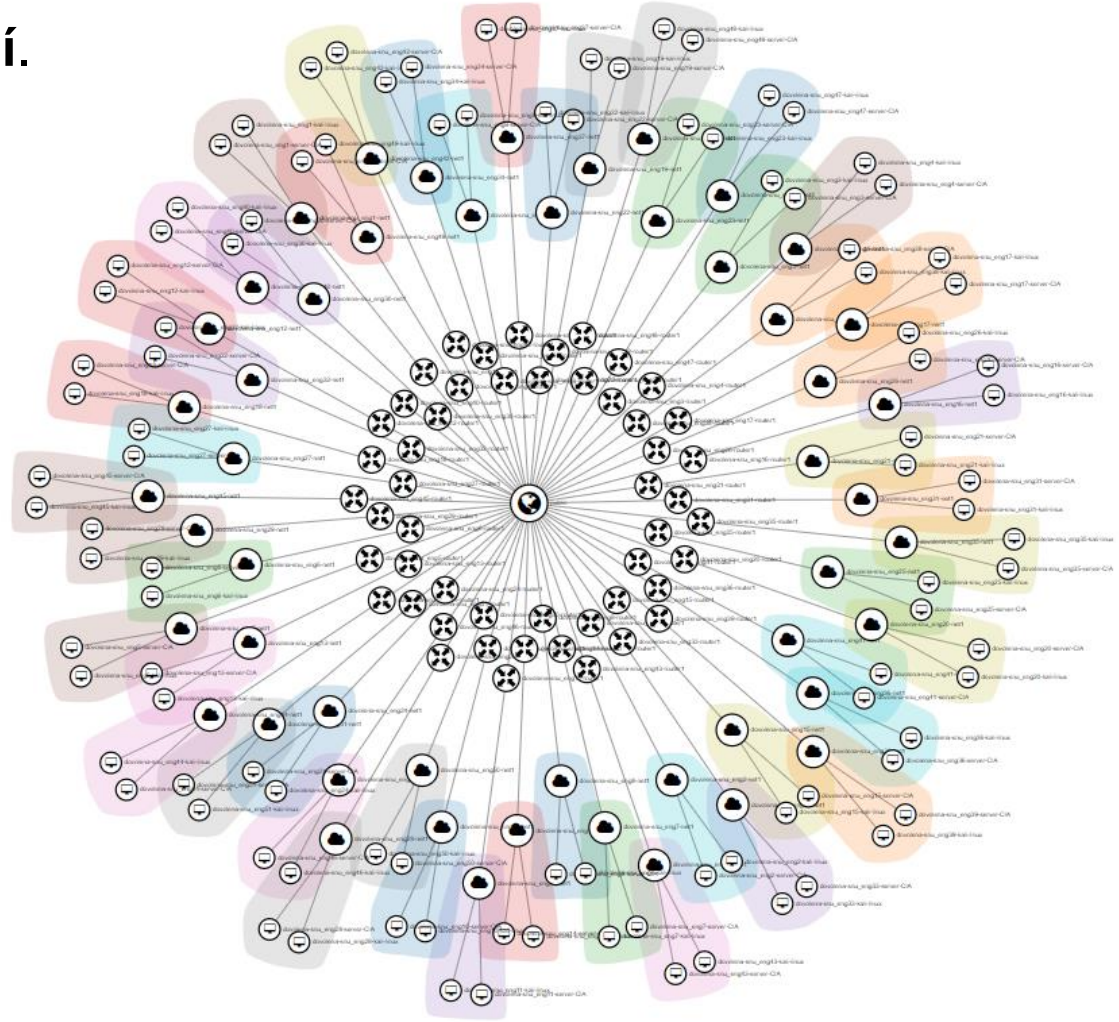
- Automatizované nasazení virtualizovaných klientů, serverů, databází atd.



Správa a realizace scénářů

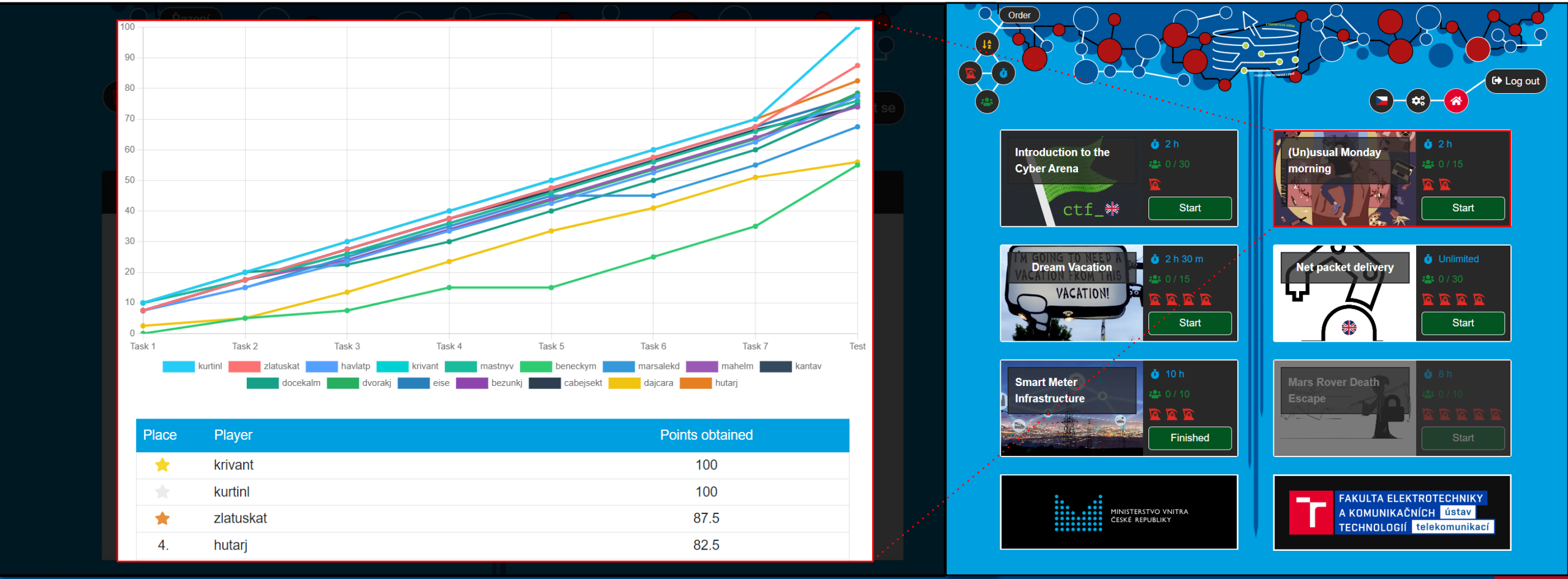
- Instance = **bezpečné** a **izolované prostředí**.





Správa a realizace scénářů

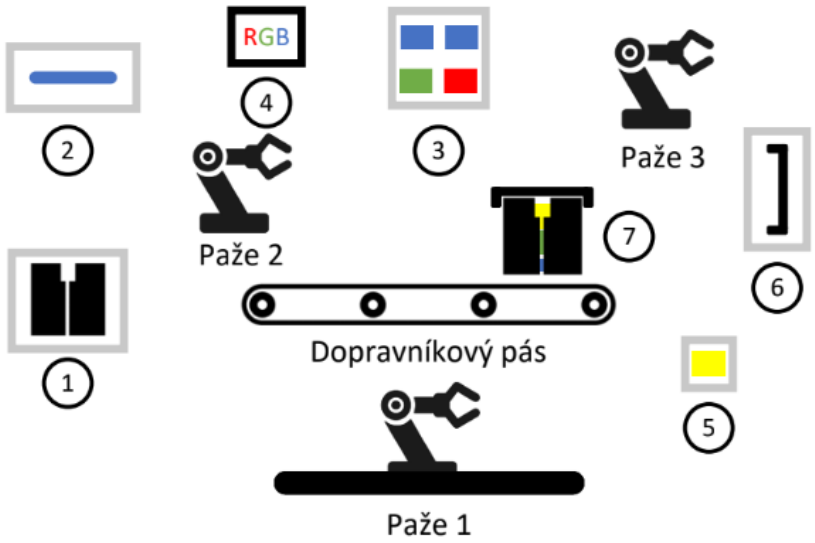
- Bodované a kompetetivní herní scénáře.



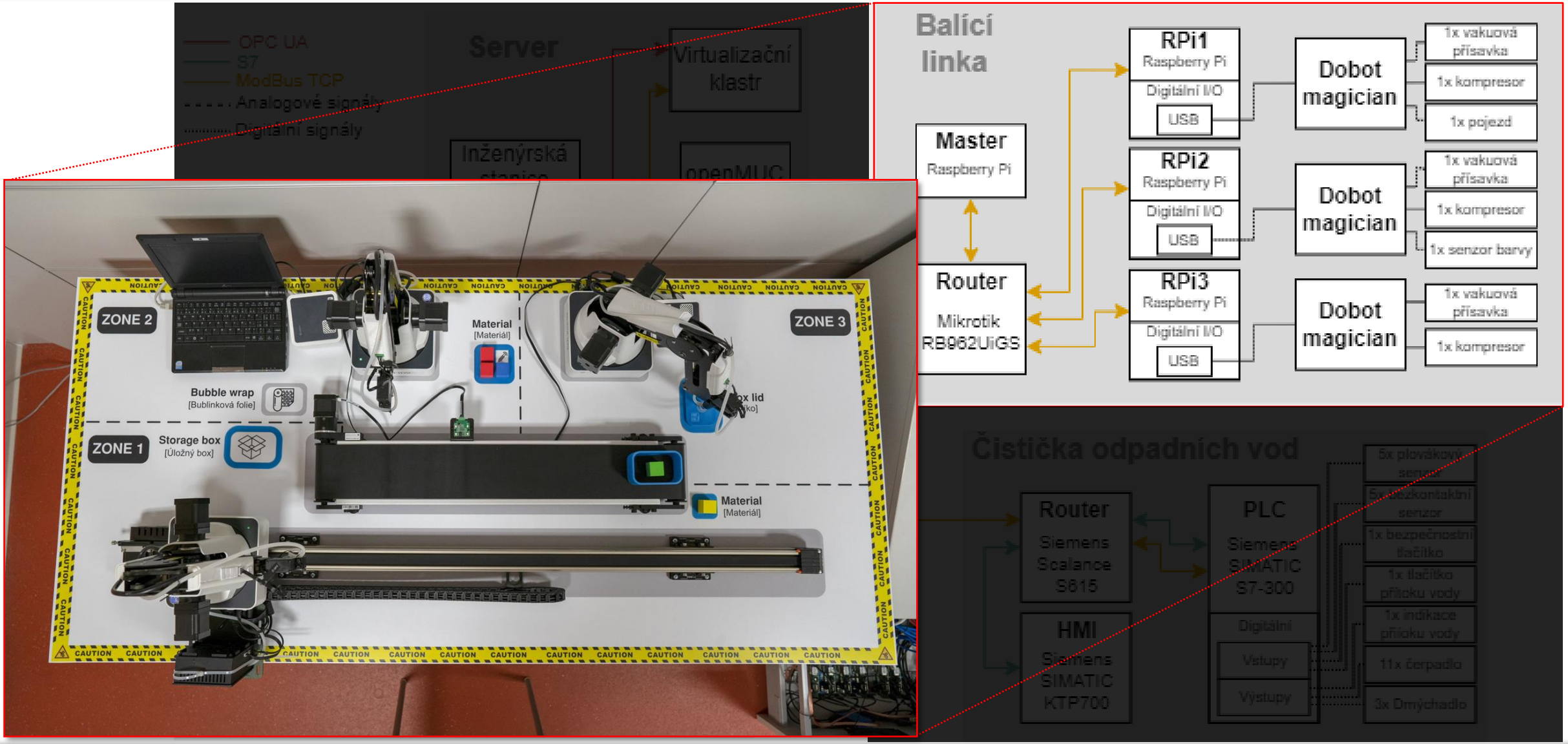
Place	Player	Points obtained
★	krivant	100
★	kurtinl	100
★	zlatuskat	87.5
4.	hutarj	82.5

Bezpečnost průmyslových zařízení

- **Průmyslová balící linka**:
  - vlastní linuxový controller,
  - protokol Modbus TCP a 5G,
  - simulace útoků na procesy.

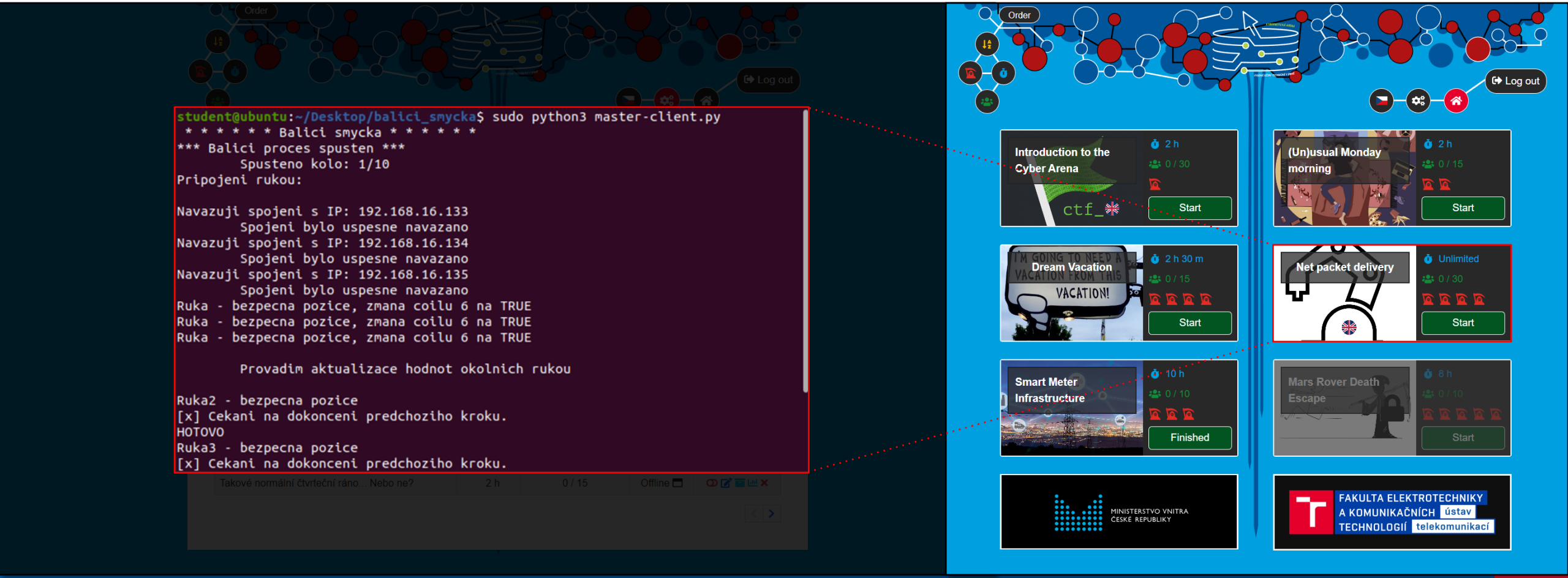


Bezpečnost průmyslových zařízení



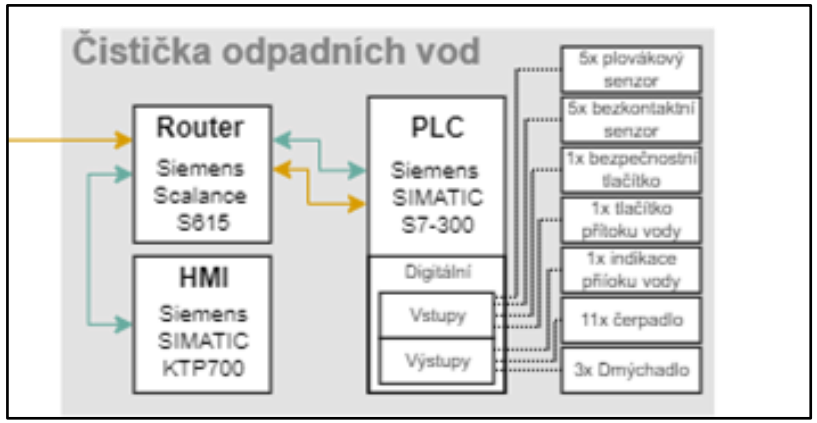
Bezpečnost průmyslových zařízení

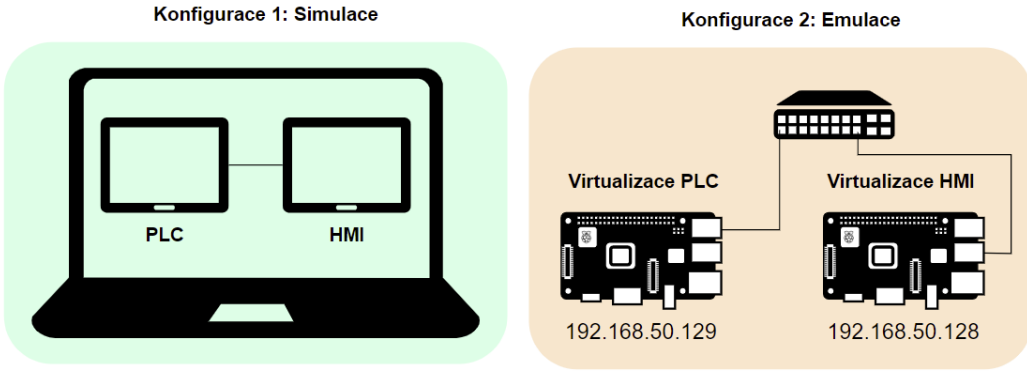
- Plně virtualizovaná verze balící linky se 3 robotickými pažemi.



Bezpečnost průmyslových zařízení

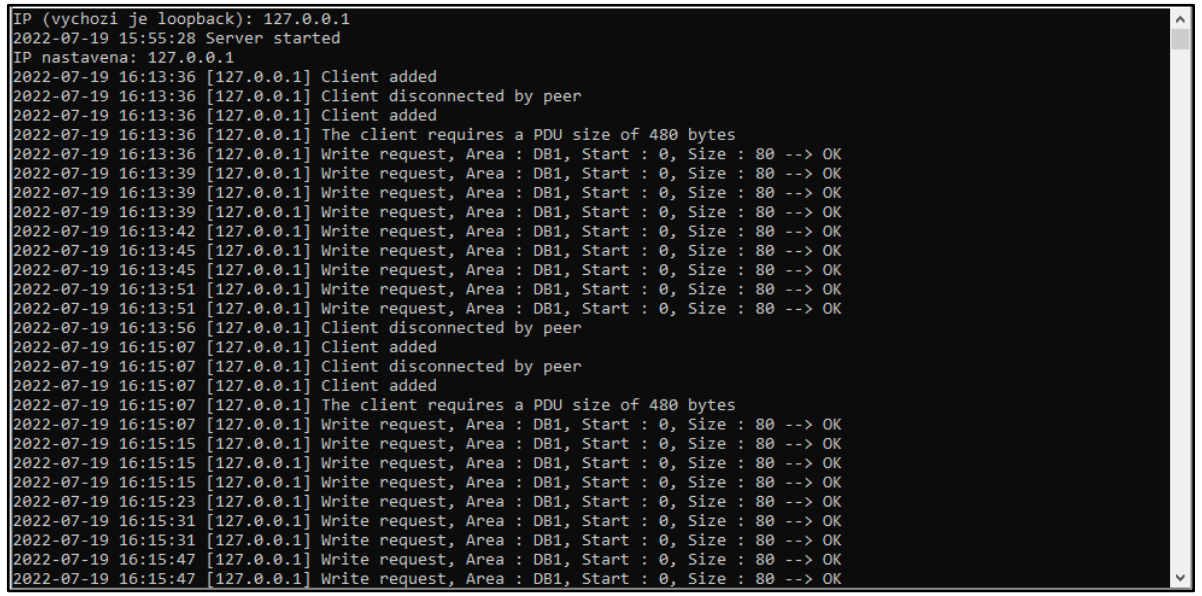
- **Čistírna odpadních vod (ČOV)**:
  - model městské čistírny v měřítku 1:12,
  - SIEMENS PLC controller S7-300 a HMI KPT-700,
  - protokoly OPC-UA, S7Comm a Profinet,
  - vektory útoku, jako např.: aktualizace firmware, konfigurace a S7Comm crypto-imperfections.

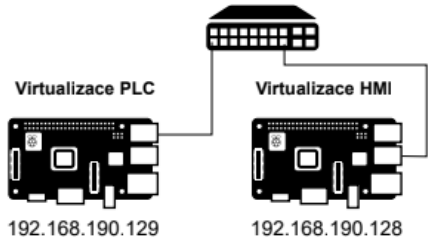




Bezpečnost průmyslových zařízení

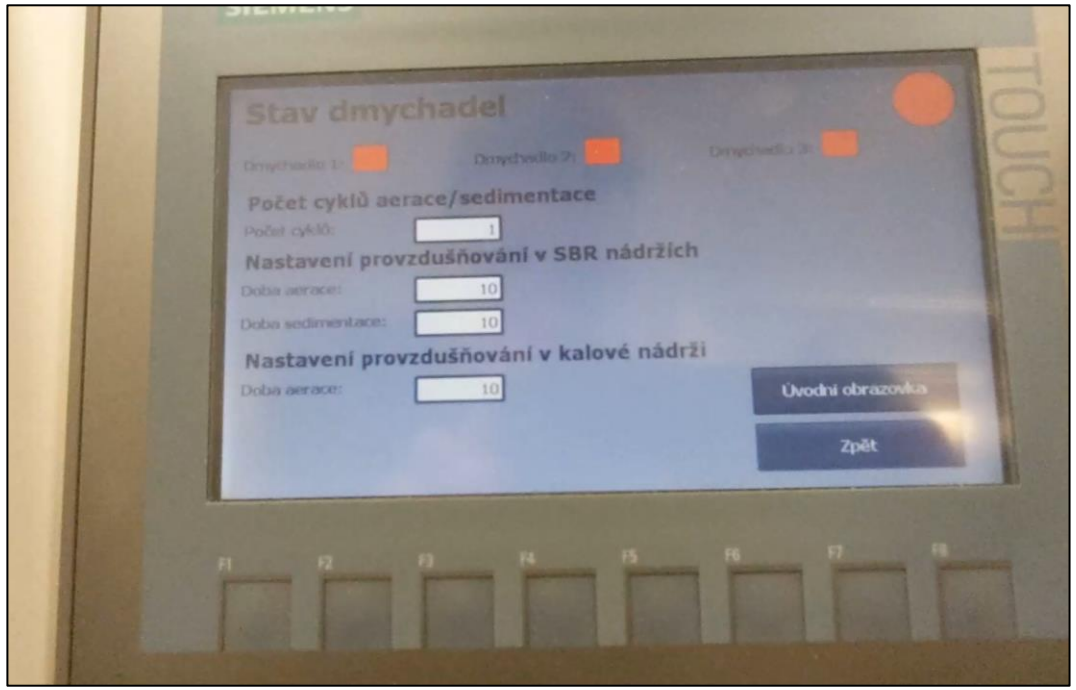
- Plně virtualizovaná verze ČOV.

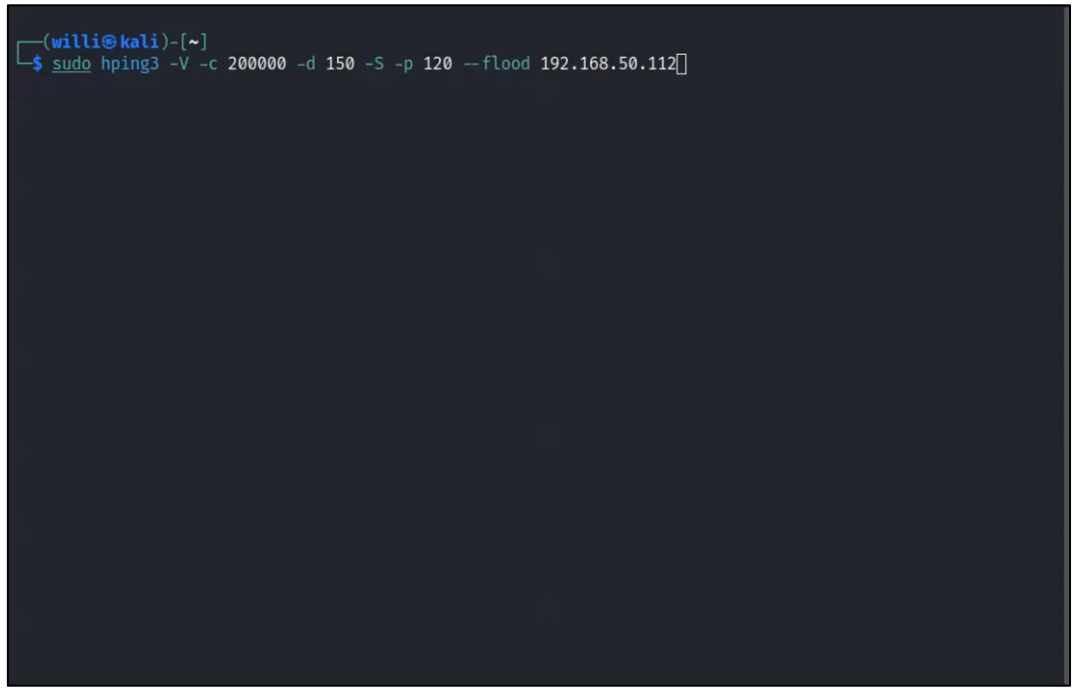




Bezpečnost průmyslových zařízení

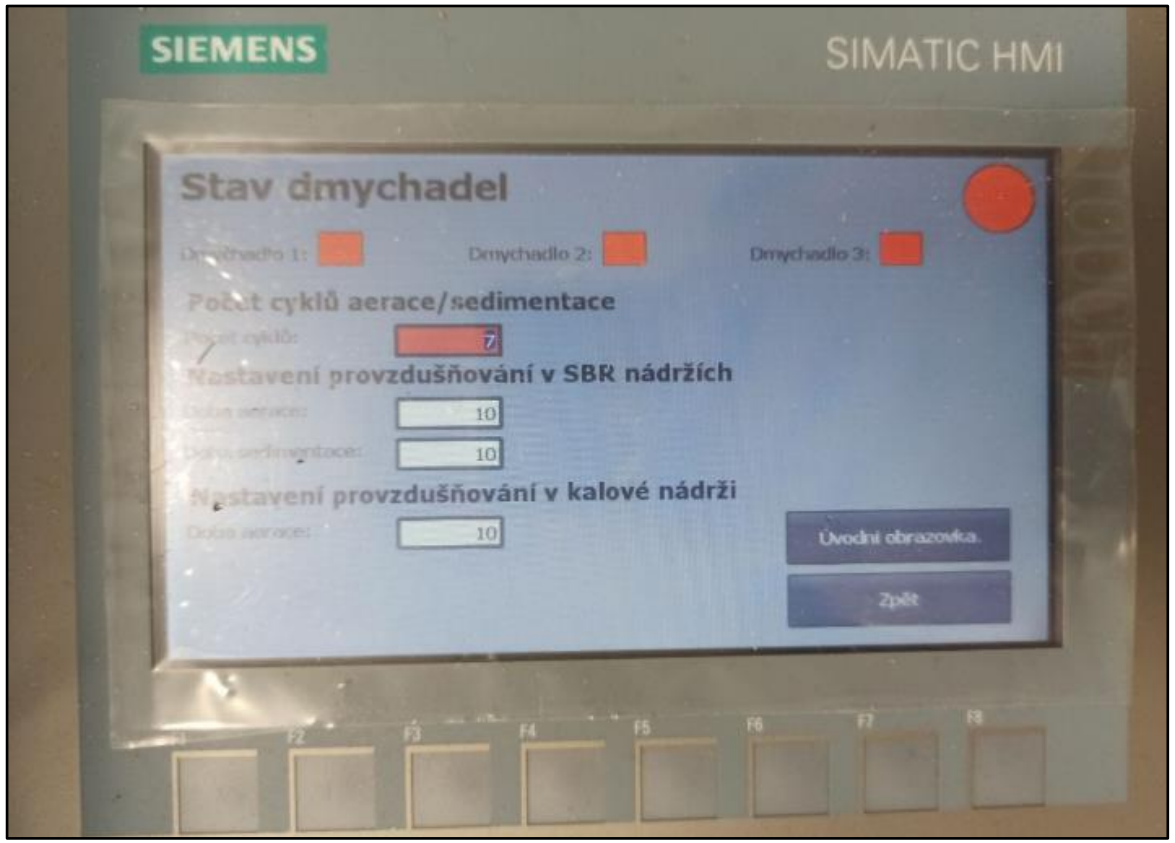
- Ukázka DoS útoku na ČOV.





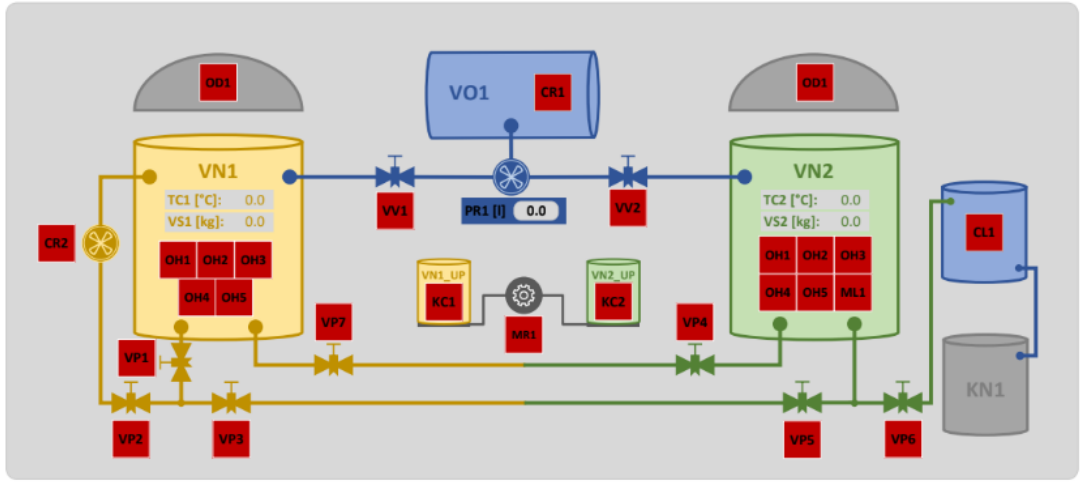
Bezpečnost průmyslových zařízení

- Ukázka zastavení cyklu procesu ČOV přepsáním hodnoty počtu cyklů aerace.

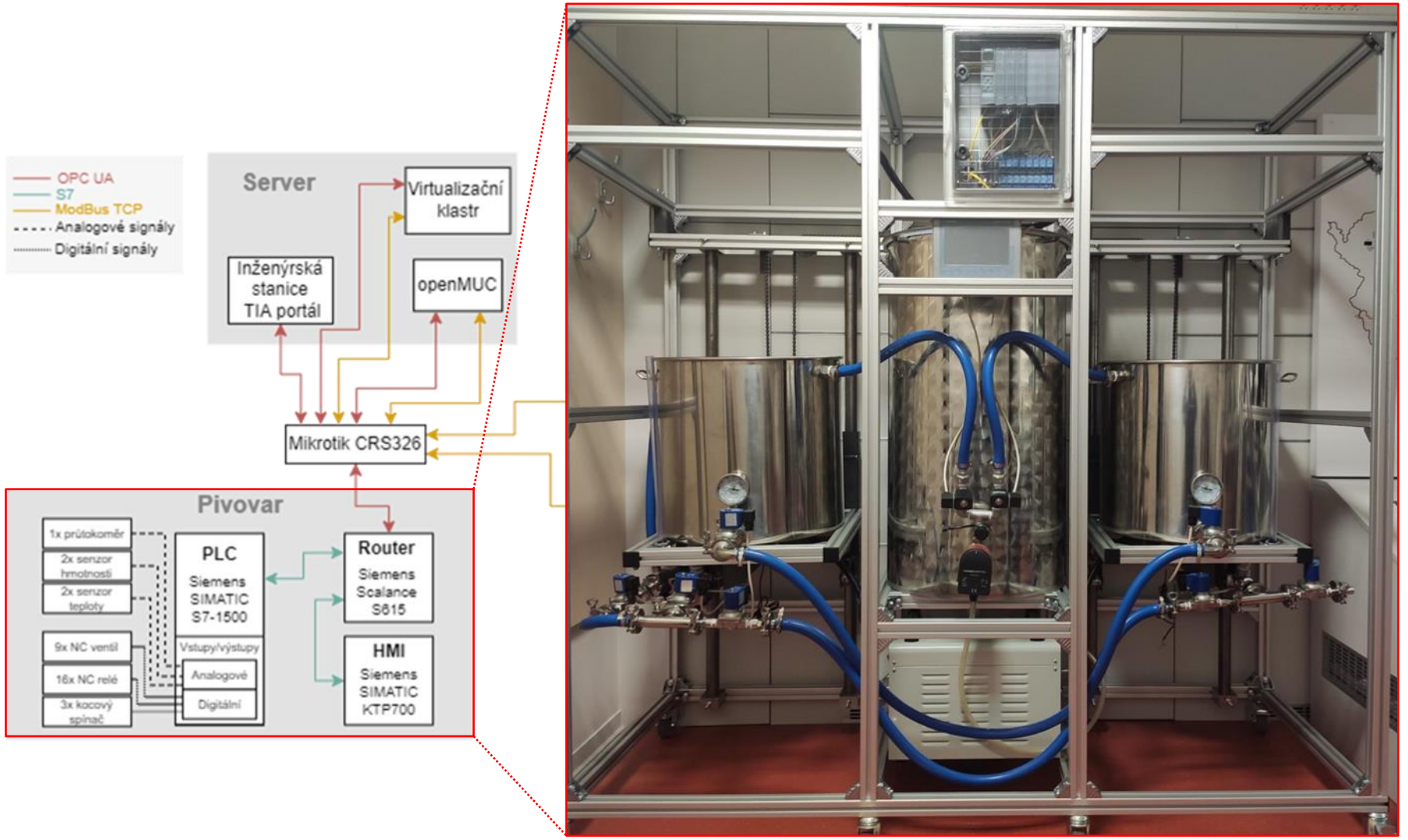


Bezpečnost průmyslových zařízení

- **Pivovar s plně funkčním procesem vaření**:
  - SIMATIC PLC S7-1500 a HMI KPT700,
  - průmyslové protokoly S7Comm a Modbus TCP,
  - ethernetový přepínač Siemens Scalace XB005,
  - simulace útoků (např.: narušení procesu, DoS).

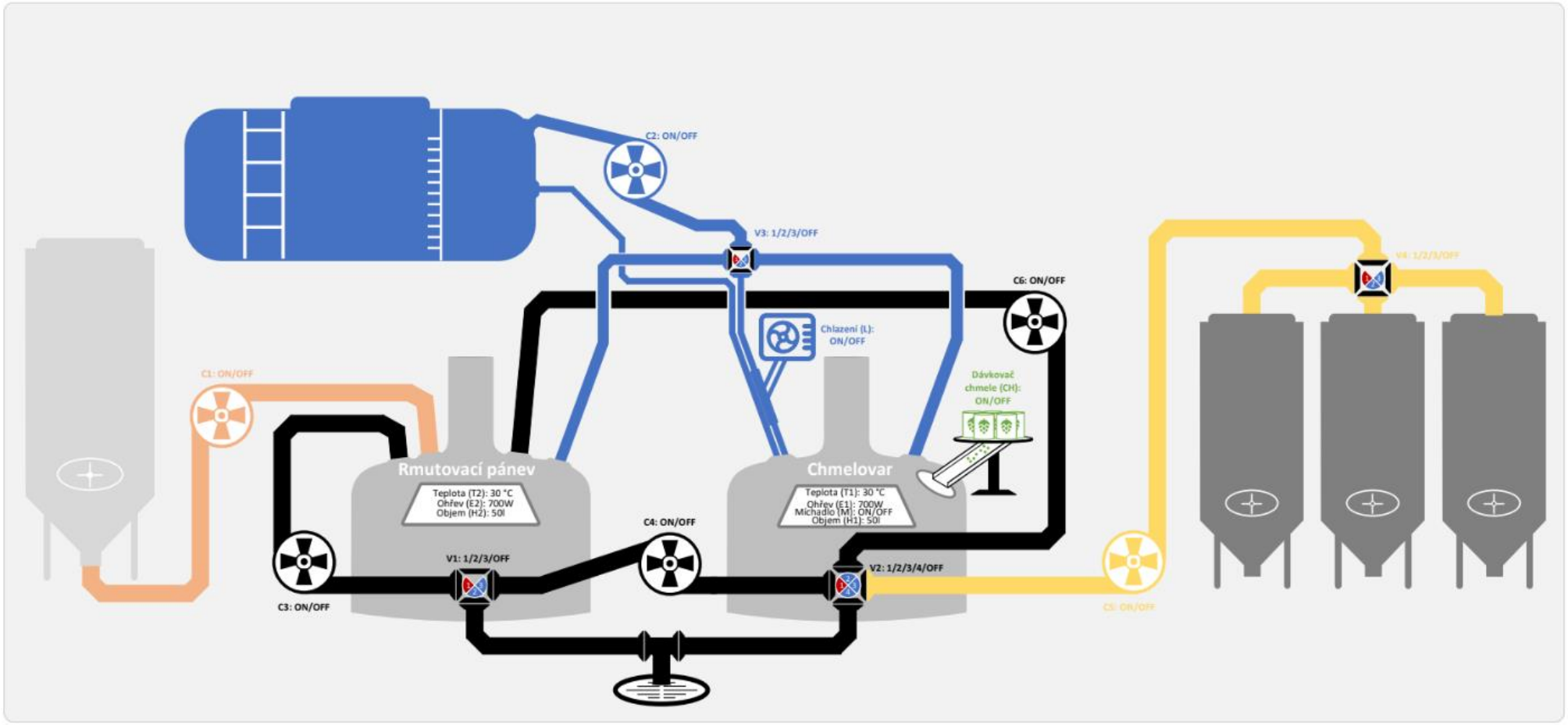


Bezpečnost průmyslových zařízení



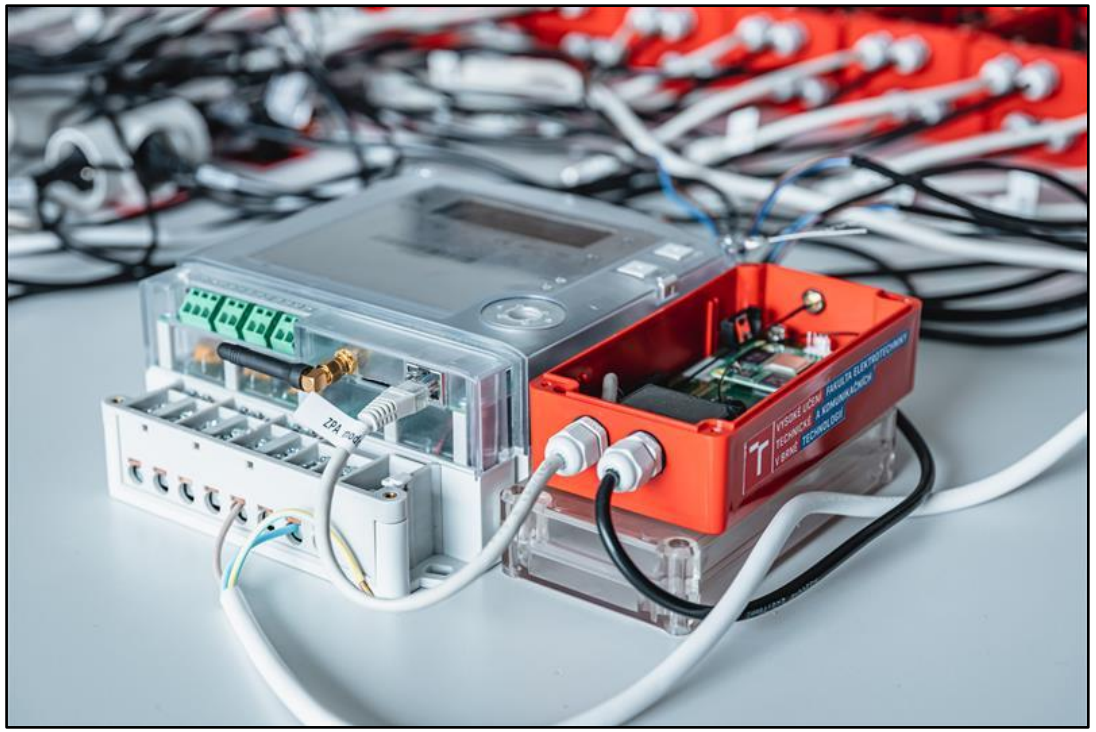
Bezpečnost průmyslových zařízení

- Virtualizovaná verze pivovaru.



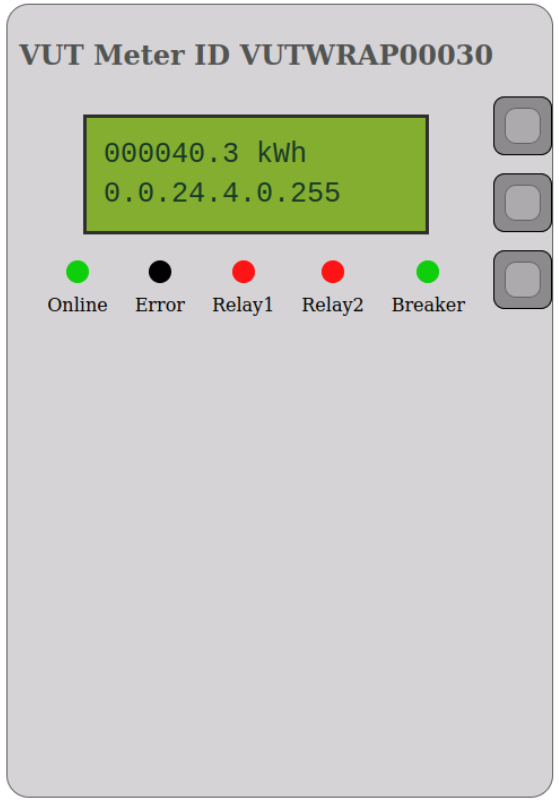
Bezpečnost energetické infrastruktury

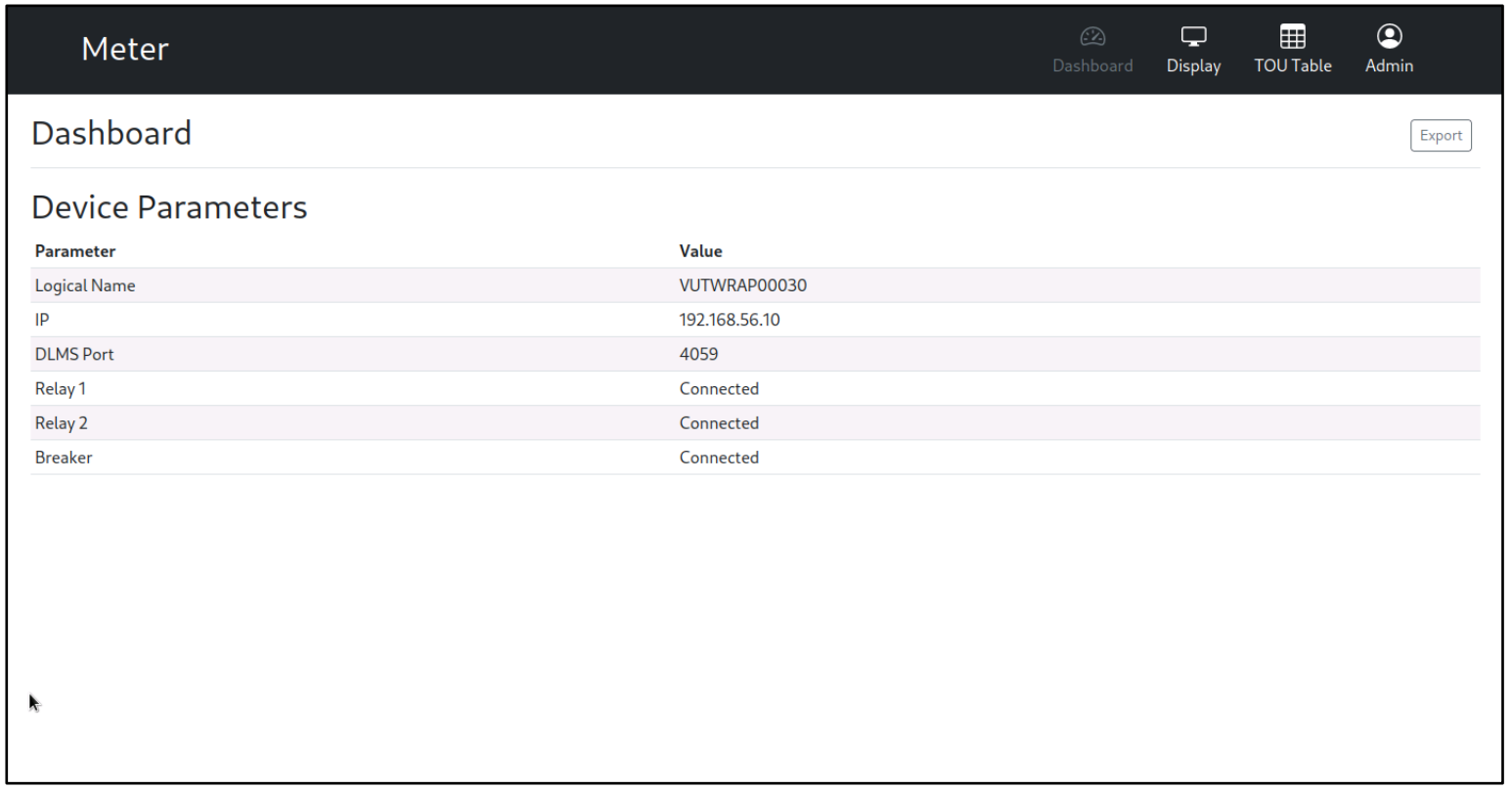
- **Certifikované DLMS/COSEM chytré elektroměry od různých výrobců.**



Bezpečnost energetické infrastruktury

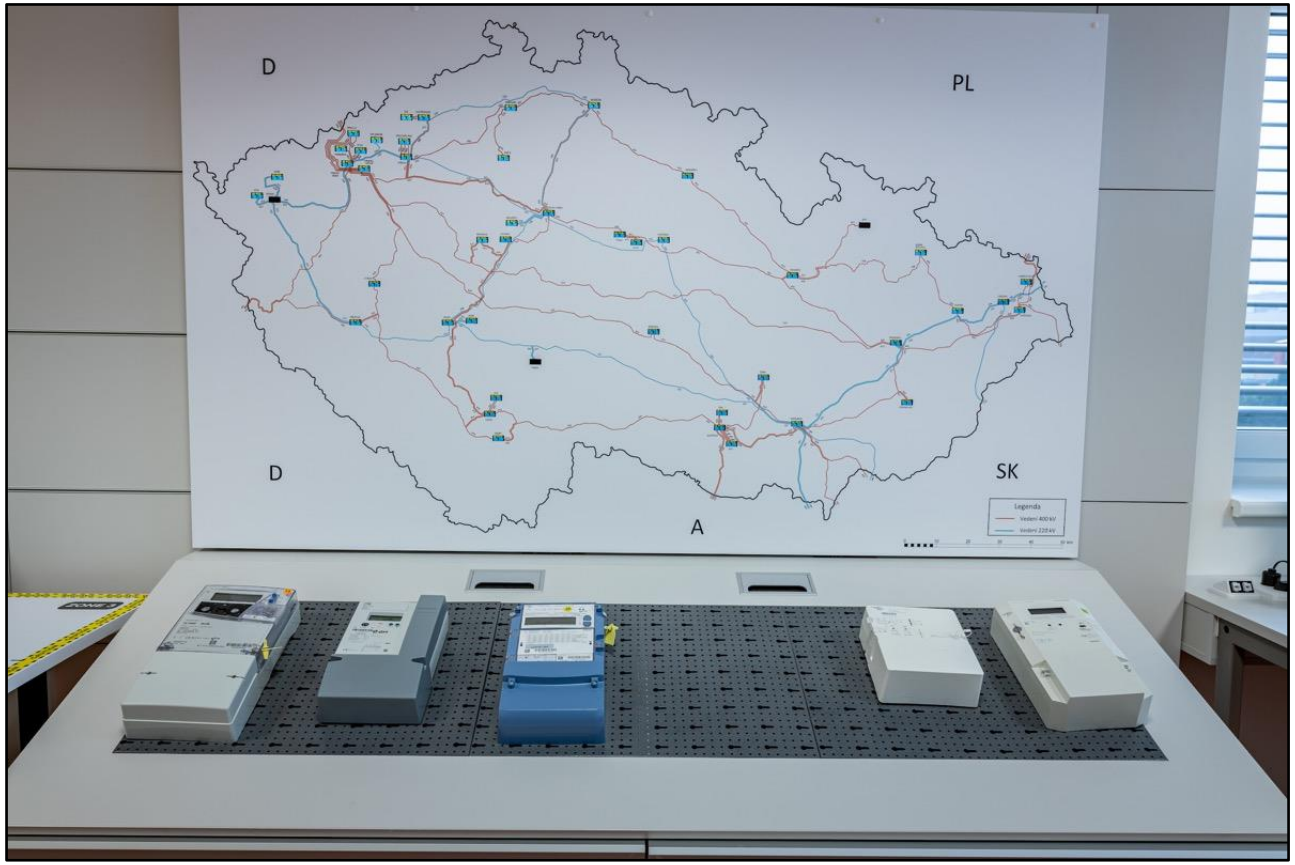
- Plně virtualizovaná verze polygonu s chytrými elektroměry.



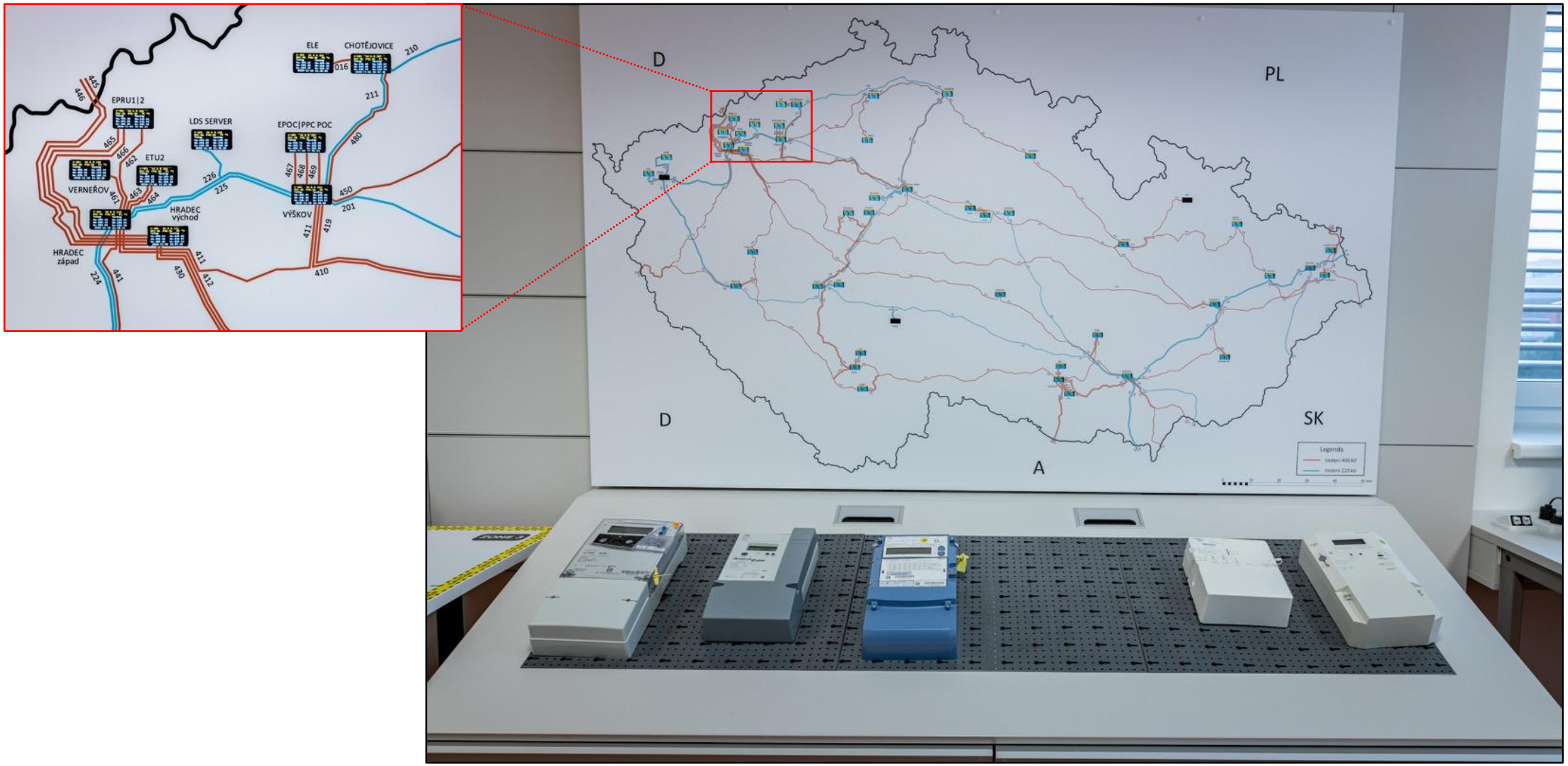


Bezpečnost energetické infrastruktury

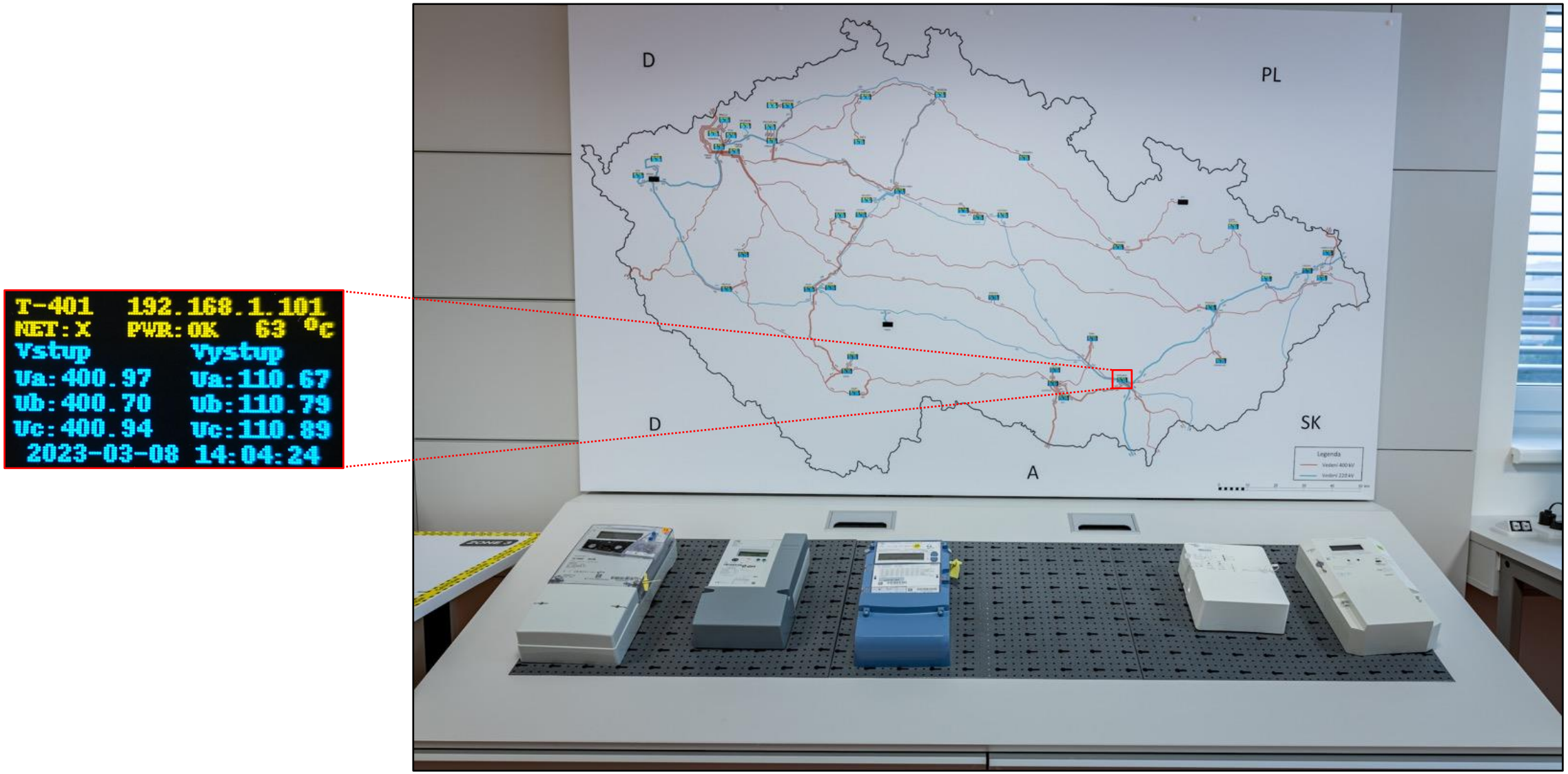
- **Elektrická přenosová soustava České republiky:**
  - vlastní linuxové PLC/RTU,
  - protokoly IEC-61850 a IEC-60870,
  - celkem 47 zařízení Raspberry Pi,
  - 34 rozvoden a 13 elektráren,
  - simulace (např. podpětí a přepětí).



Bezpečnost energetické infrastruktury

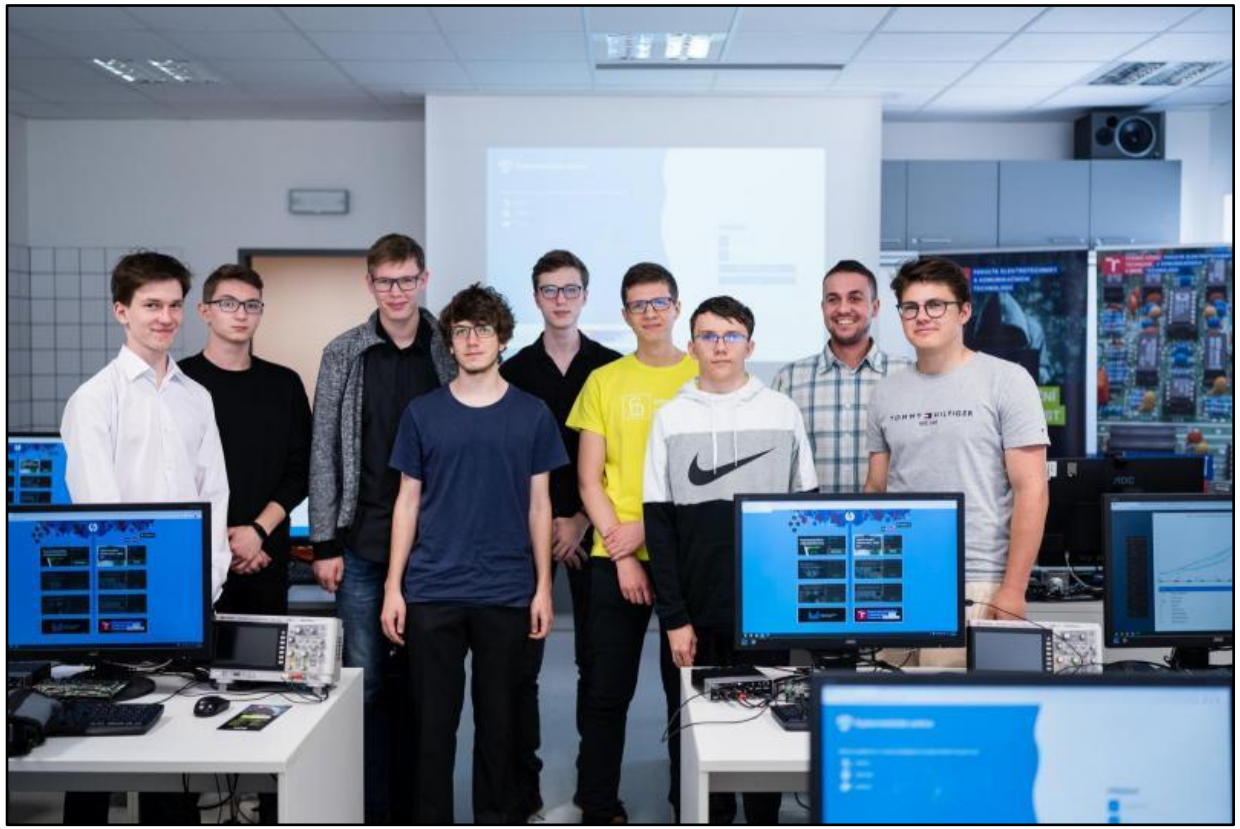


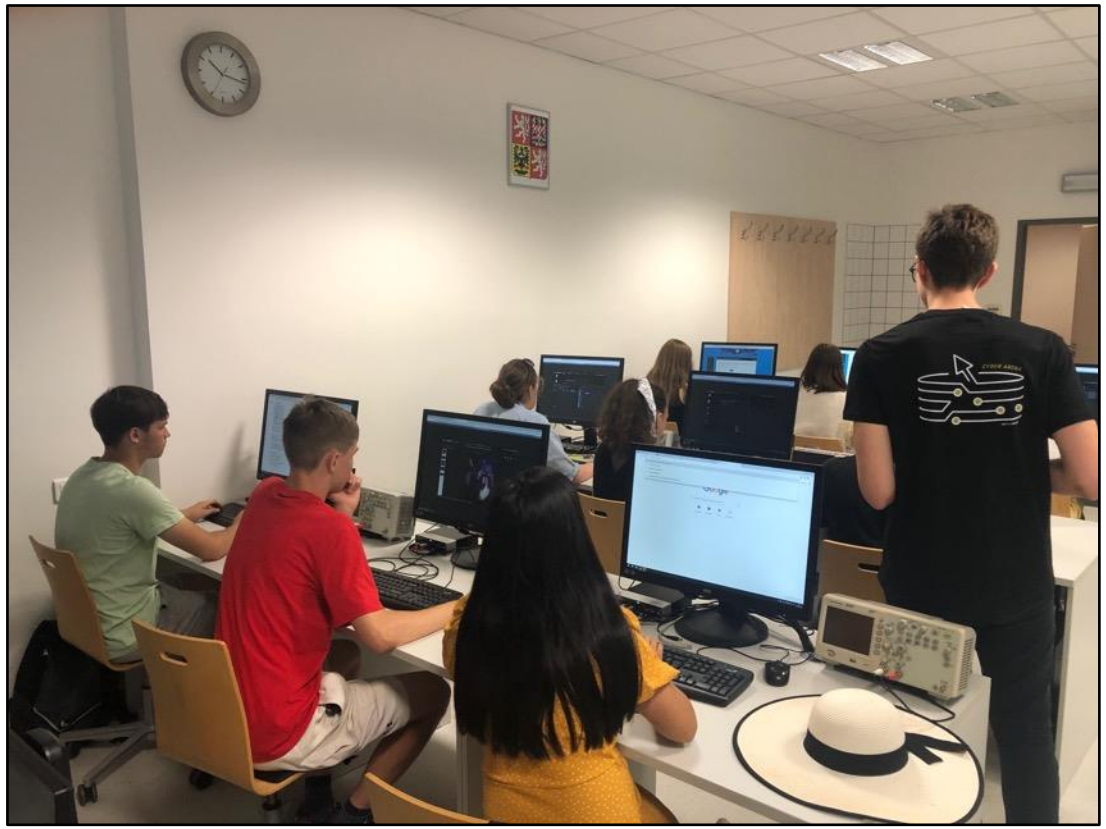
Bezpečnost energetické infrastruktury



Testování v rámci ČR a zahraničí

- Testování se studenty **průmyslových středních škol** a **víceletých gymnázií**.





Testování v rámci ČR a zahraničí

- Testování se studenty **Univerzity obrany**, v zahraničí s finskou **Tampere University**.

BUTCA – jedinečné řešení

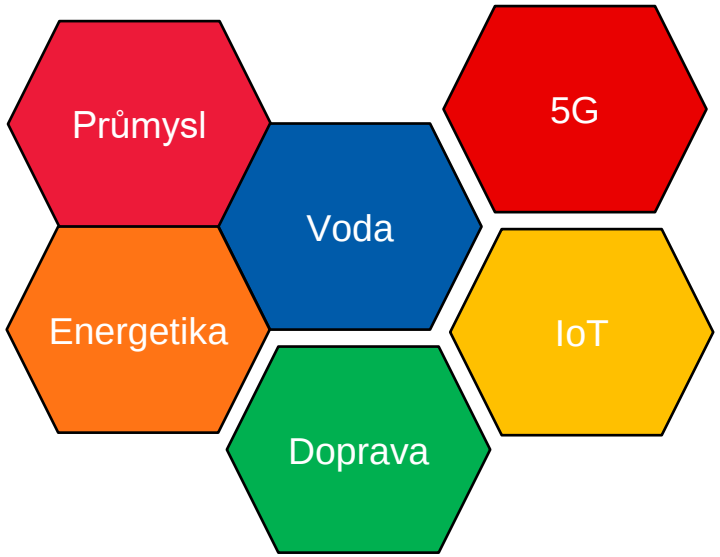
- BUTCA jako **lokální platforma**:
  - Vysoké učení technické v Brně,
  - výuka a trénink studentů,
  - výzkum, vývoj a testování.

- BUTCA jako **školící platforma**:
  - jednorázové nebo opakované školení,
  - fyzické a virtuální polygony,
  - on-demand a ad hoc přístup.

- BUTCA jako **služba na míru**:
  - SaaS (Software as a Service),
  - dostupnost odkudkoliv,
  - minimální požadavky.

Shrnutí

- BUTCA je platforma pro:
  - **výuku** na různých stupních vzdělání (gymnázia, střední školy a univerzity),
  - **trénování** zaměstnanců s/bez počáteční zkušeností v kybernetické bezpečnosti,
  - **výzkum** nad systémy s reálnými daty a možností simulovat komplexní scénáře.
- Kyber-fyzický polygon:
  - **průmyslová balící linka**,
  - **čistírna odpadních vod**,
  - **automatizovaný pivovar**,
  - **el. přenosová soustava**,
  - **chytré elektroměry**.
- V přípravě:
  - **bezpečnost IoT a 5G**,
  - **kooperativní systémy V2V a V2X**,
  - **osvěta kybernetické bezpečnosti**.



Otázky?

Vysoké učení technické v Brně
Fakulta elektrotechniky a komunikačních technologií
Ústav telekomunikací

https://butca.vut.cz