

Moderní vzdělávání v kyberbezpečnosti: BUTCA, mikrocertifikáty a profesní trénink

doc. Ing. Jan Hajný, Ph.D.

Bc. Willi Lazarov

- **Fakulta elektrotechniky a komunikačních technologií**

- Ústav telekomunikací
- Applied Cryptography & Security Engineering Group
- <https://www.utko.fekt.vut.cz/>
- <https://axe.vut.cz>

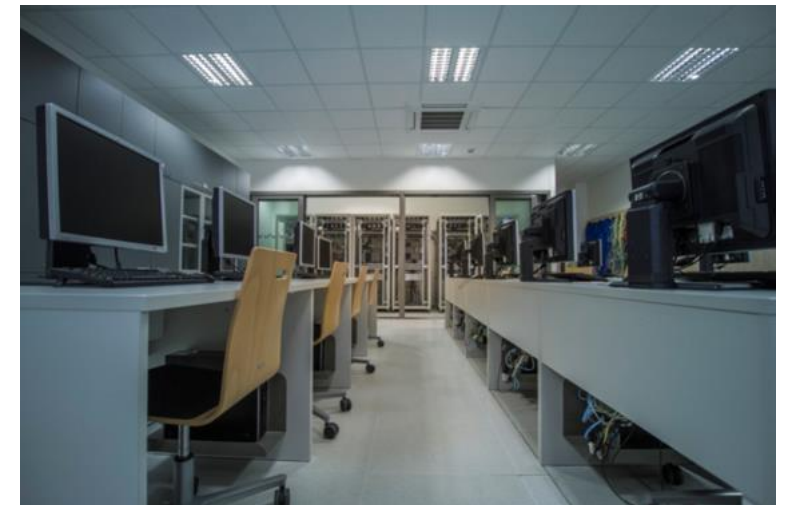
- **R&D činnosti v kyberbezpečnosti**

- 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).

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/>

SPARTA

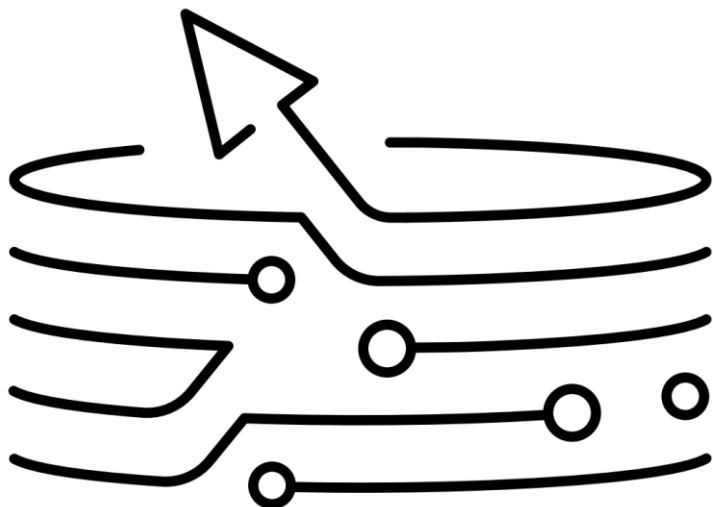
- **Laboratoř kvantové bezpečnosti**
 - Zahrnuje zařízení kvantové a postkvantové kryptografie
 - Unikátní sada v rámci ČR
 - Vznik na základě projektu Network security in post-quantum era (NESPOQ, MVČR)
 - Součástí infrastruktury pro výuku v oborech Informační bezpečnost
 - Jeden z prvních prvků Národní kvantové sítě

- **Další infrastruktura:**
 - CyberGrid, 5G+ Lab, IoT Lab, Palo Alto, ...
 - Kyber-fyzický polygon (průmysl a energetika)





FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH **ústav**
TECHNOLOGIÍ **telekomunikací**



 **BUTCA**

Profesní vzdělávání

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 nekonceptně 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, ...).

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 BUTCA¹ pro lokální i vzdálený trénink.
- Provázání s tzv. skills frameworky (ENISA ECSF², NIST NICE³, CyQUAL⁴).
- 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>

Pracovní parametry programu

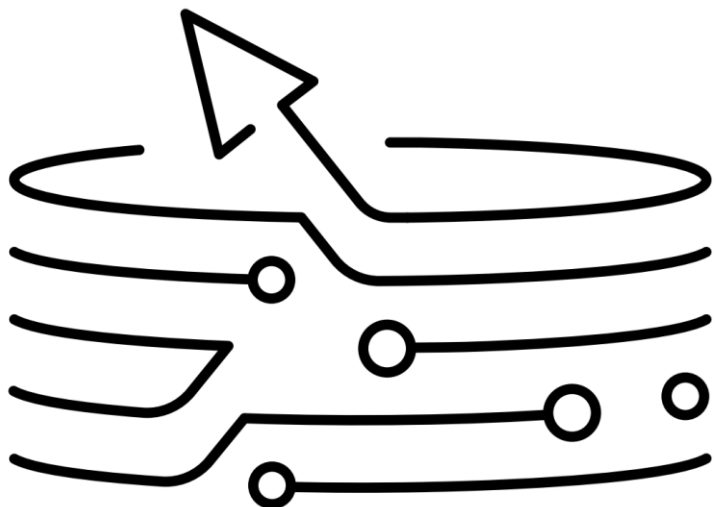
- Délka trvání: 1 rok
- Struktura: 3 doporučené průchody, 6 modulů po 3 předmětech
- Harmonogram:
 - Září: zahájení, osobní konzultace
 - Září – Prosinec: přednášky (e-learning/online) + individuální konzultace
 - Leden: Výuka v laboratořích – blokově 1 týden
 - Únor – Květen: přednášky (e-learning/online)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



<https://forms.gle/GNe82QE11MAskL8PA>



FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH **ústav**
TECHNOLOGIÍ **telekomunikací**



 **BUTCA**

BUTCA: Platforma pro trénink kybernetické bezpečnosti



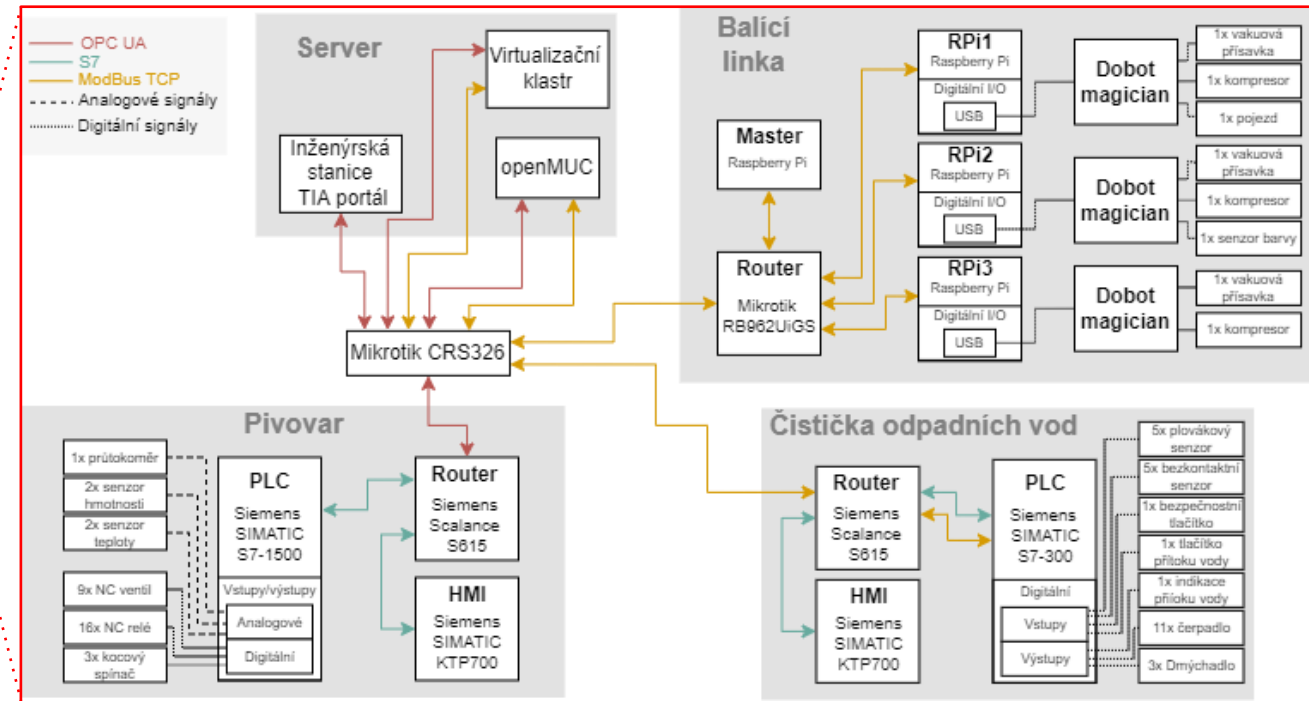
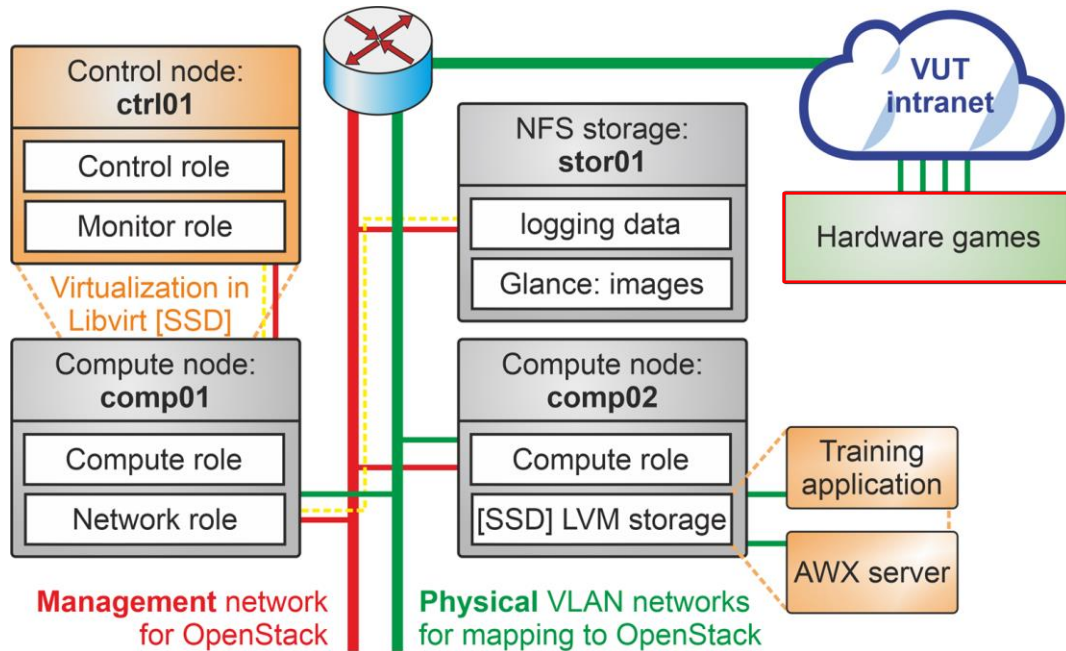
Kybernetická aréna

- 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.

Games overview

Name	Duration	Maximum players	Status	Control panel
Smart Meter Infrastructure	10 h	0 / 10	Online	
Dream Vacation (ENG)	2 h 30 m	0 / 15	Online	
Introduction to the Cyber Arena (ENG)	2 h	0 / 30	Online	
Net packet delivery (ENG)	Unlimited	0 / 30	Offline	
(Un)usual Monday morning (ENG)	2 h	0 / 15	Online	
Stress test	1 h	0 / 72	Offline	
Čistička odpadních vod	24 h	0 / 4	Offline	
Net packet delivery (CZ)	10 h	0 / 30	Offline	
Představení protokolu IEC104	2 h	0 / 26	Offline	
Takové normální čtvrteční ráno... Nebo ne?	2 h	0 / 15	Offline	

Introduction to the Cyber Arena 2 h 0 / 30 Start

(Un)usual Monday morning 2 h 0 / 15 Start

Dream Vacation 2 h 30 m 0 / 15 Start

Net packet delivery Unlimited 0 / 30 Start

Smart Meter Infrastructure 10 h 0 / 10 Finished

Mars Rover Death Escape 8 h 0 / 10 Start

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ ústav telekomunikací



Správa a realizace scénářů

Menu

- Prologue ●
- Task 1 ●
- Task 2 ●
- Task 3 ●
- Task 4 ●
- Task 5 ●
- Task 6 ●
- Task 7 ●
- Task 8 ●
- Task 9 ●
- Epilogue ●

Dream Vacation (ENG)

My argument that Syria would not be the safest place on the planet was not considered – it rather boosted my girlfriend's enthusiasm. She had already bought the plane tickets for both of us.

We flew to Cyprus and took a boat to Syria. She did not book a hotel, but only a room through Airbnb. There were other roommates – one nice couple and probably some stranger who probably never leaves the room. He didn't even come to introduce himself. We unpacked our things and went to a shop to buy some snacks and beers. When we got back a couple invited us to play some board games, so we joined them.

About two hours later, a door to a mystery room opened suddenly and a robust man stood there. He looked mad, pointed at the WiFi router and shook his head. Understanding that I had to do something about the broken/lost internet connection, I went to get my laptop. Everyone was looking at me excitedly at that moment. I revealed to them that I was studying information security, so this wouldn't be a problem for me. Within 10 minutes everything was working as it should and I was a hero. We said goodbye to the nice couple and went to sleep.

Some noise wakes me up at night. I sit up and squint into the darkness. I try to touch my girlfriend, but I only squeeze a blanket. Hmm, she probably went to the toilet and that was probably the noise I heard earlier, I think...

In the morning, the sunshine wakes me up. I turn my head and my girlfriend is nowhere to be found. There is a crumpled piece of paper on the bed. She probably went shopping... I open it and find some letters, is it...

Časový limit 2:25:39

[Download attachment here](#)

Enter answer.

By this task, you can obtain **5 points**

? Take a hint (penalization 25 %) Nápovědy

Use the Refresh button, if the console is not responding.

The code for virtual machine connection: 470896

Poznámky

Lineární průchod

Zadání úkolu

Konzole

```

kali@kali:~$ ptwebdiscover -u www.vutbr.cz -bo
[!] Settings overview
[!] URL.....: www.vutbr.cz
[!] Discovery-type.....: Complete backups only
[!] Extensions.....: ['']
[!] Method.....: HEAD
[!] Charset.....: abcdefghijklmnopqrstuvwxyz
[!] Length-min.....: 1
[!] Length-max.....: 6
[!] Keyspace.....: 321272406
[!] Delay.....: 0.0s
[!] Threads.....: 20
[!] Recurse.....: False
[!] Parse content.....: False
[!] Search for backups.: False

[!] Check http://www.vutbr.cz/
[+] [301] [R] http://www.vutbr.cz/ →
[+] [301] [R] https://www.vutbr.cz/ →
[+] [200] [D] https://www.vutbr.cz/

```

Přílohy





Správa a realizace scénářů

penterepMail - vulnerable webmail (v1.4)

Vulnerable webmail

Welcome in application for demonstration vulnerabilities in web apps. The application is suitable for demonstration of individual attacks or for teaching IT security and penetration testing. List of included vulnerabilities is public on <https://www.penterep.com>.

Challenges for you

There are prepared many challenges for you on web <https://www.penterep.com> Sign up and compare your knowledge with others.

© 2023 penterep.com Mobile app Help Competition E-Shop Contact

Report a cybercrime

Enter full name

Enter email address

Enter phone number

Give us detailed description of the cybercrime

+ Upload photo



Správa a realizace scénářů

- Automatizované nasazení virtualizovaných klientů, serverů, databází atd.

The image displays a Kali Linux desktop environment with a terminal window showing a shell prompt. A settings panel is visible, and a file system view shows a file named '(Un)usual Monday morning'. A control panel is also present, showing a list of challenges:

- (Un)usual Monday morning
- Stress test
- Čistička odpadních vod
- Net packet delivery (CZ)
- Představení protokolu IEC10
- Takové normální čtvrtěční rá

The main dashboard features several challenge cards:

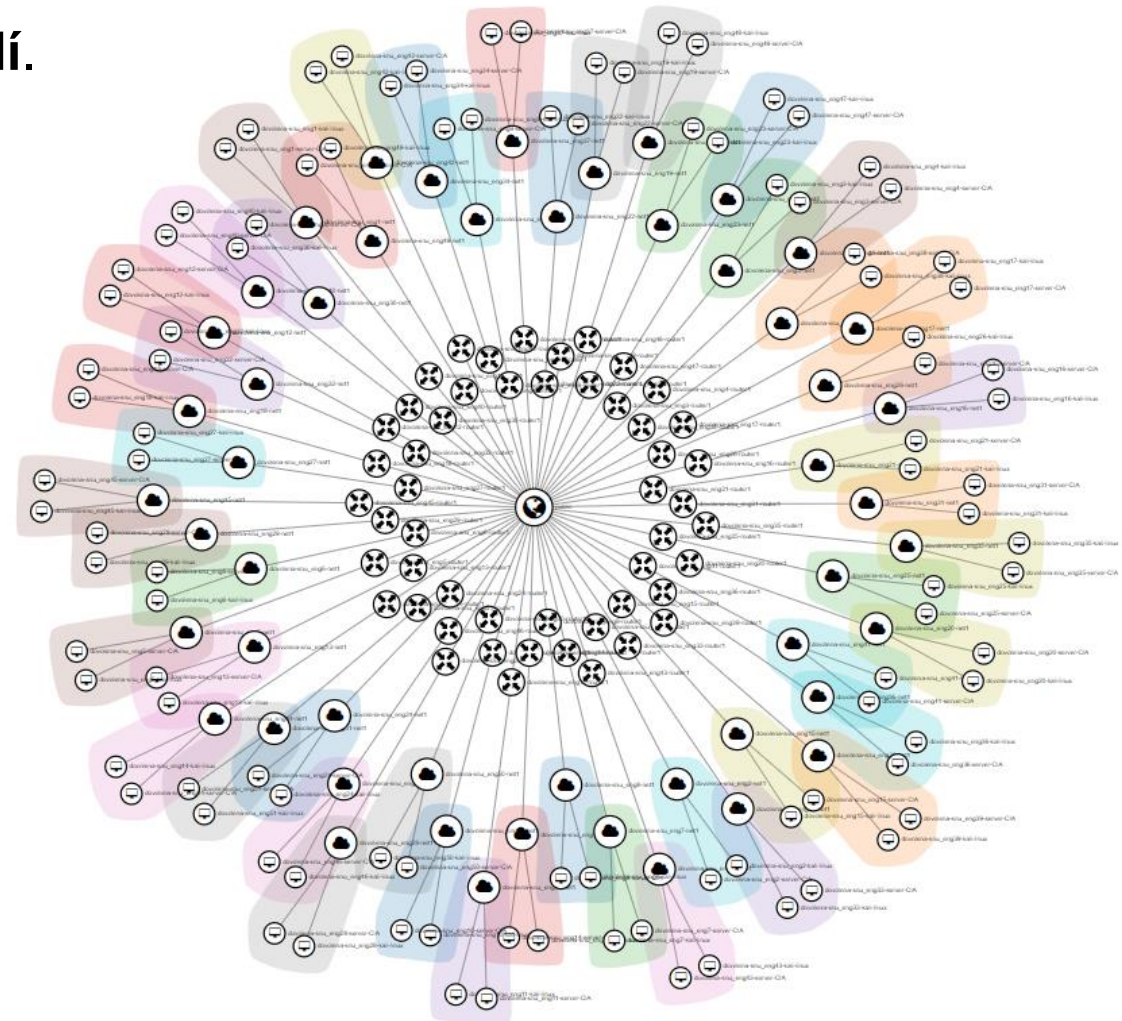
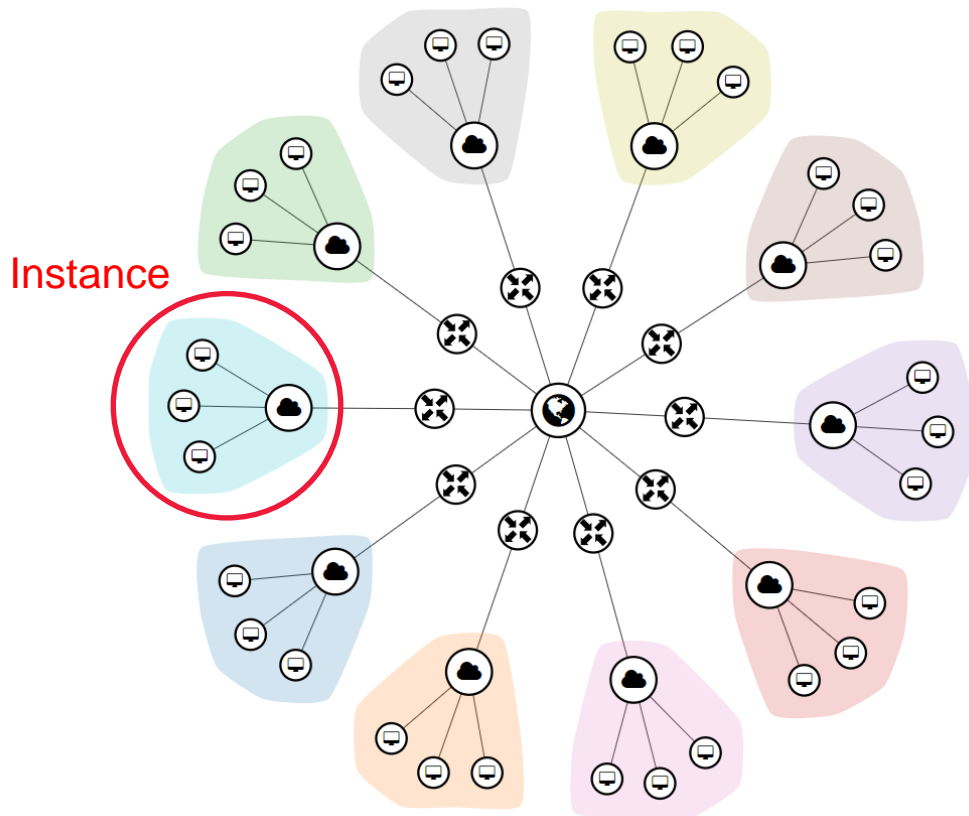
- Introduction to the Cyber Arena (2 h, 0/30)
- (Un)usual Monday morning (2 h, 0/15)
- Dream Vacation (2 h 30 m, 0/15)
- Net packet delivery (Unlimited, 0/30)
- Smart Meter Infrastructure (10 h, 0/10) - Finished
- Mars Rover Death Escape (8 h, 0/10)

The dashboard also includes a 'Log out' button and a 'Control panel' section. The footer of the dashboard displays the logo of the Faculty of Electrical Engineering and Communication Technology (FEKT) and the text: 'FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ ústav telekomunikací'.



Správa a realizace scénářů

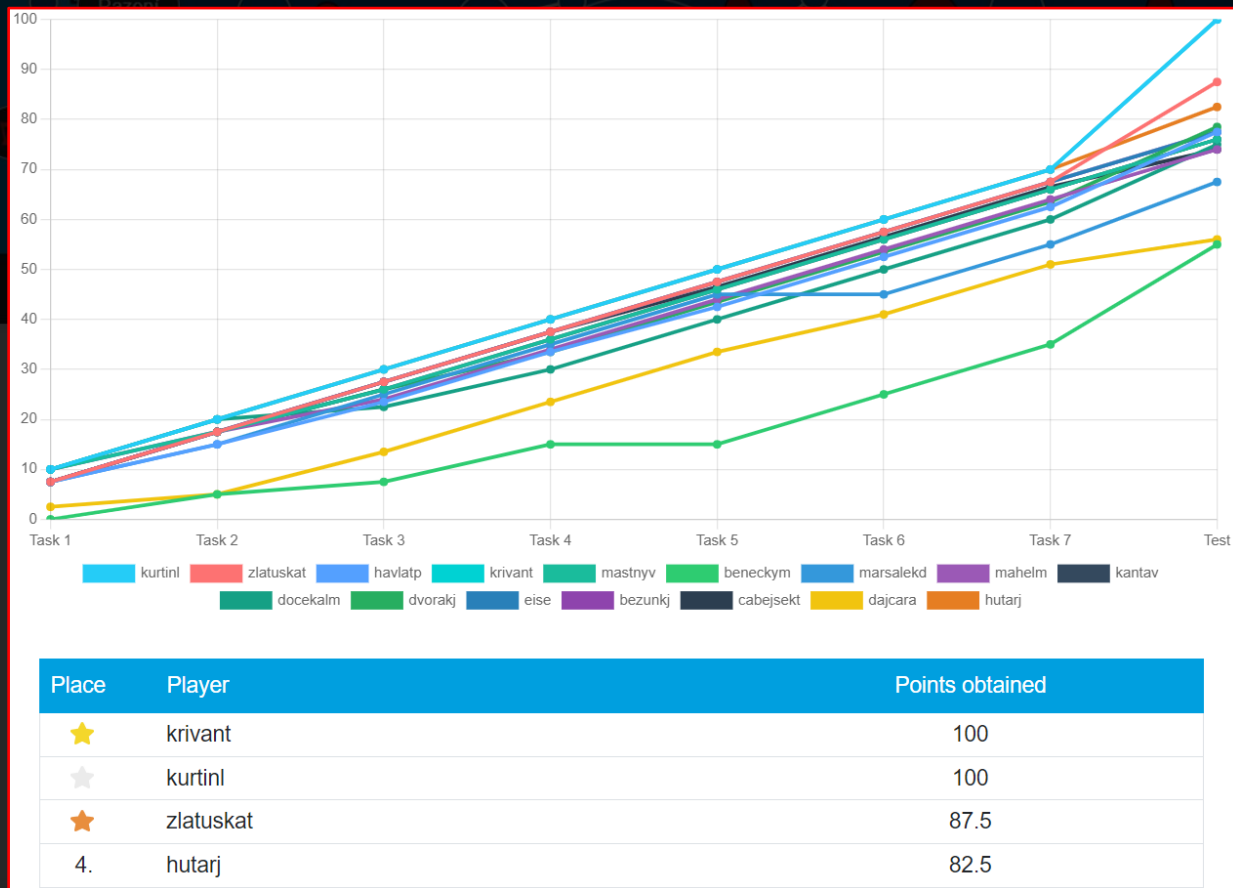
- Instance = **bezpečné a izolované prostředí.**





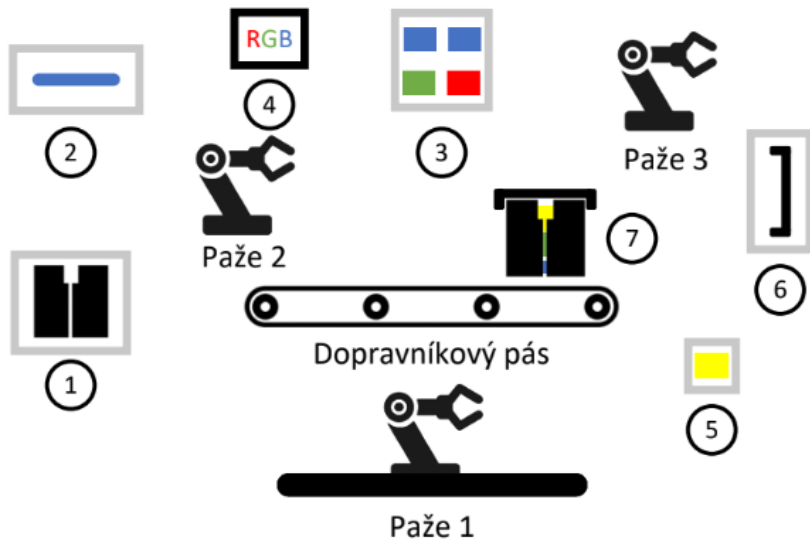
Správa a realizace scénářů

- Bodované a kompetitivní herní scénáře.



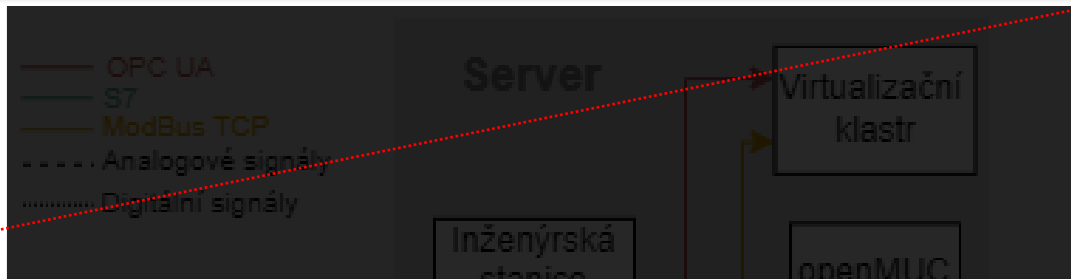
- **Průmyslová balící linka:**

- vlastní linuxový controller,
- protokol Modbus TCP a 5G,
- simulace útoků na procesy.

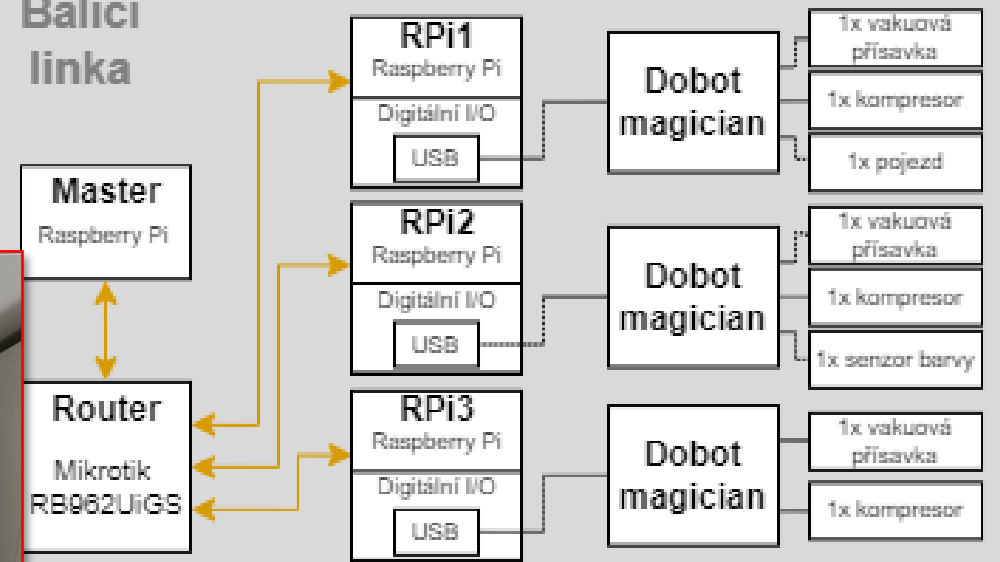




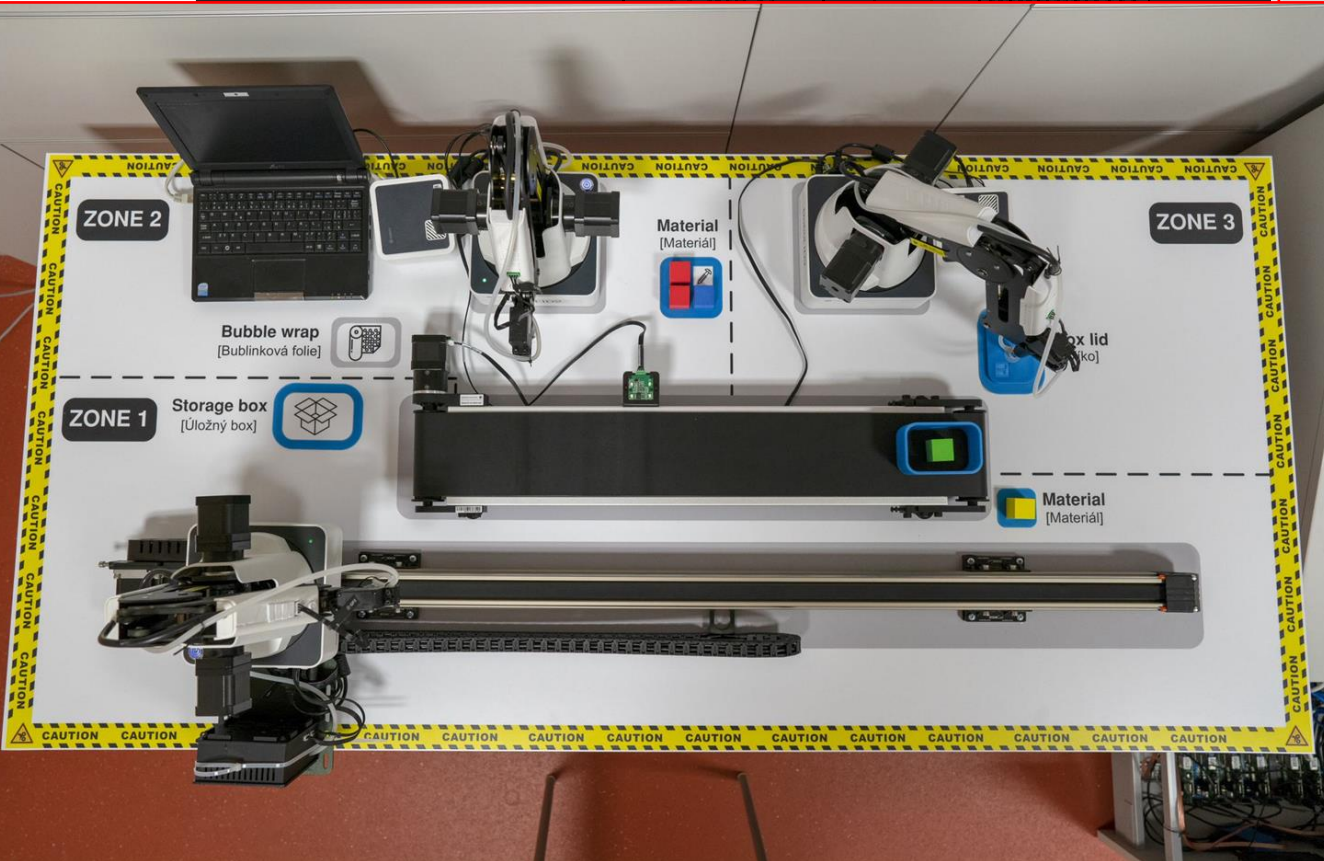
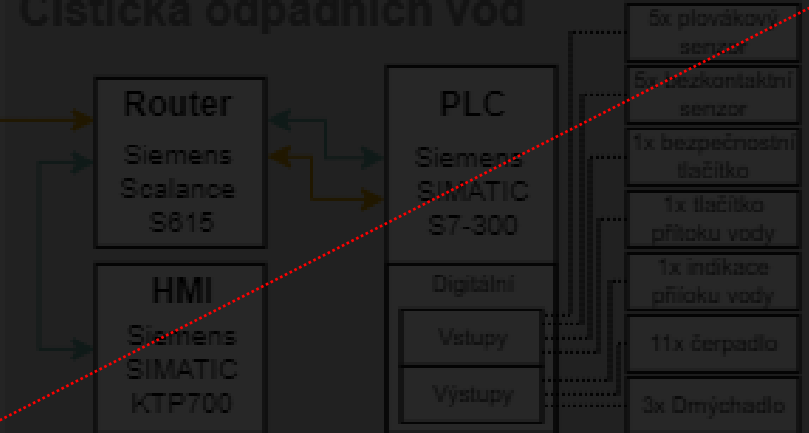
Bezpečnost průmyslových zařízení



Balící linka



Čistička odpadních vod





Bezpečnost průmyslových zařízení

- Plně virtualizovaná verze balící linky se 3 robotickými pažemi.

```
student@ubuntu:~/Desktop/balici_smycka$ sudo python3 master-client.py
* * * * * Balici smycka * * * * *
*** Balici proces spusten ***
      Spusteno kolo: 1/10
Pripojeni rukou:

Navazuji spojeni s IP: 192.168.16.133
      Spojeni bylo uspesne navazano
Navazuji spojeni s IP: 192.168.16.134
      Spojeni bylo uspesne navazano
Navazuji spojeni s IP: 192.168.16.135
      Spojeni bylo uspesne navazano
Ruka - bezpecna pozice, zmana coilu 6 na TRUE
Ruka - bezpecna pozice, zmana coilu 6 na TRUE
Ruka - bezpecna pozice, zmana coilu 6 na TRUE

      Provadim aktualizace hodnot okolnich rukou

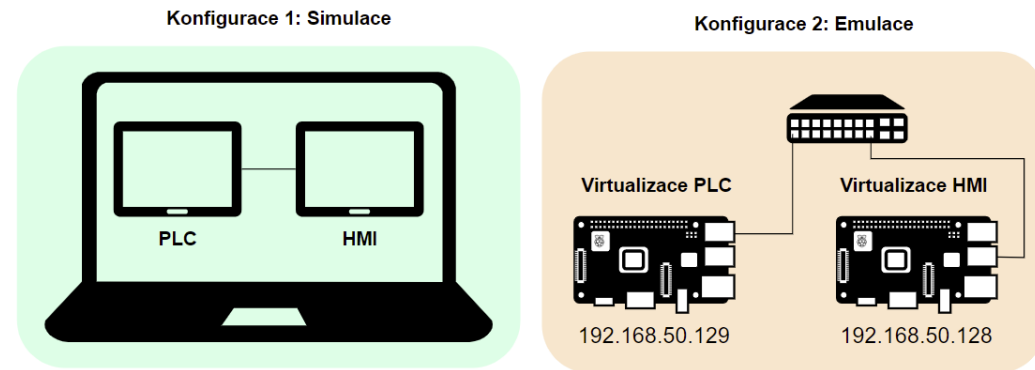
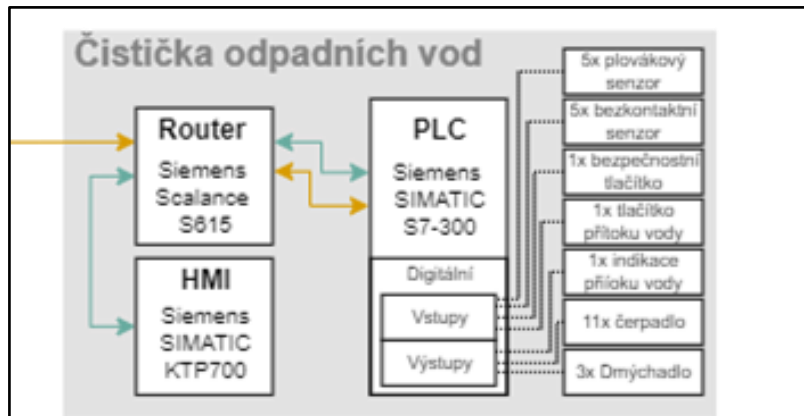
Ruka2 - bezpecna pozice
[x] Cekani na dokonzeni predchoziho kroku.
HOTOVO
Ruka3 - bezpecna pozice
[x] Cekani na dokonzeni predchoziho kroku.
```

The screenshot shows a virtual CTF interface with a blue background and a network diagram at the top. The interface includes a 'Log out' button and several challenge cards:

- Introduction to the Cyber Arena**: 2 h, 0/30, Start button.
- (Un)usual Monday morning**: 2 h, 0/15, Start button.
- Dream Vacation**: 2 h 30 m, 0/15, Start button.
- Net packet delivery**: Unlimited, 0/30, Start button.
- Smart Meter Infrastructure**: 10 h, 0/10, Finished button.
- Mars Rover Death Escape**: 8 h, 0/10, Start button.

At the bottom, there are logos for the Ministry of the Interior of the Czech Republic and the Faculty of Electrical Engineering and Communication Technology (FET) at BUTCA.

- **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.

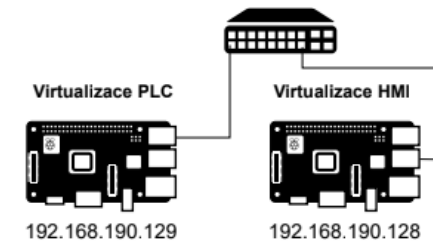




Bezpečnost průmyslových zařízení

- Plně virtualizovaná verze ČOV.

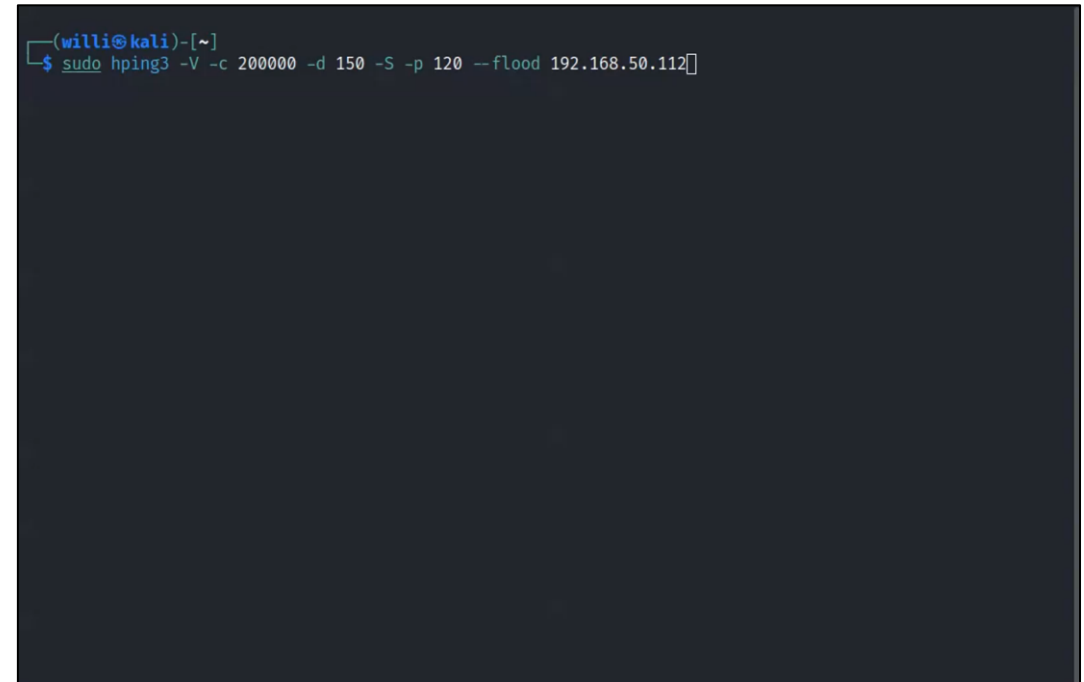
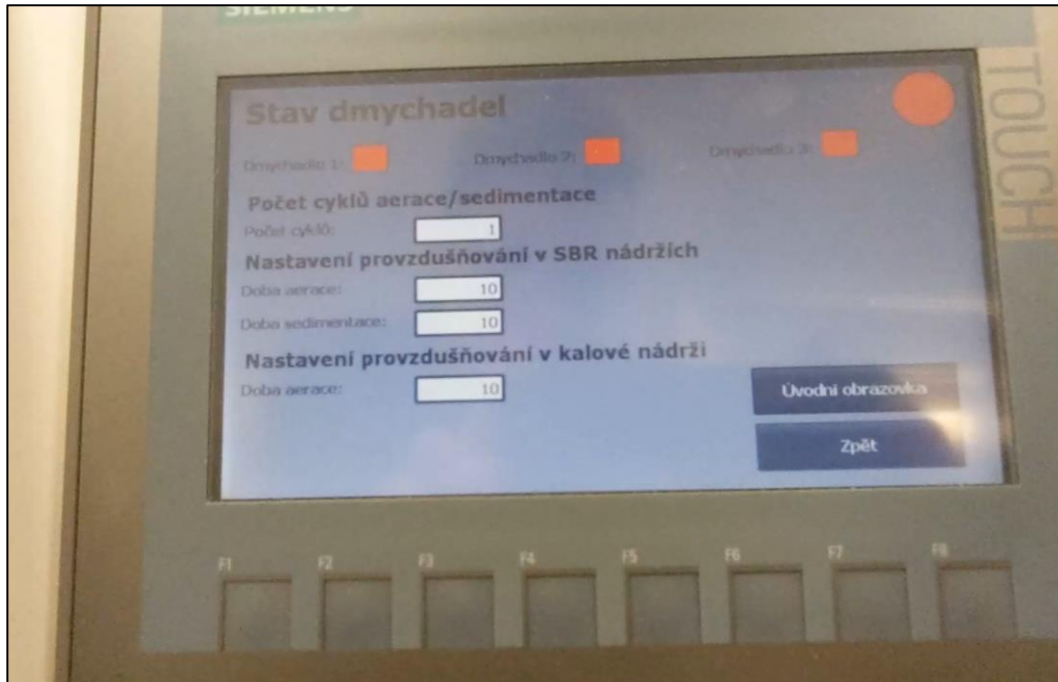
```
IP (vychozi je loopback): 127.0.0.1
2022-07-19 15:55:28 Server started
IP nastavena: 127.0.0.1
2022-07-19 16:13:36 [127.0.0.1] Client added
2022-07-19 16:13:36 [127.0.0.1] Client disconnected by peer
2022-07-19 16:13:36 [127.0.0.1] Client added
2022-07-19 16:13:36 [127.0.0.1] The client requires a PDU size of 480 bytes
2022-07-19 16:13:36 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:13:39 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:13:39 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:13:39 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:13:42 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:13:45 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:13:45 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:13:51 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:13:51 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:13:56 [127.0.0.1] Client disconnected by peer
2022-07-19 16:15:07 [127.0.0.1] Client added
2022-07-19 16:15:07 [127.0.0.1] Client disconnected by peer
2022-07-19 16:15:07 [127.0.0.1] Client added
2022-07-19 16:15:07 [127.0.0.1] The client requires a PDU size of 480 bytes
2022-07-19 16:15:07 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:15:15 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:15:15 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:15:15 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:15:23 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:15:31 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:15:31 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:15:31 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:15:47 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
2022-07-19 16:15:47 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 80 --> OK
```





Bezpečnost průmyslových zařízení

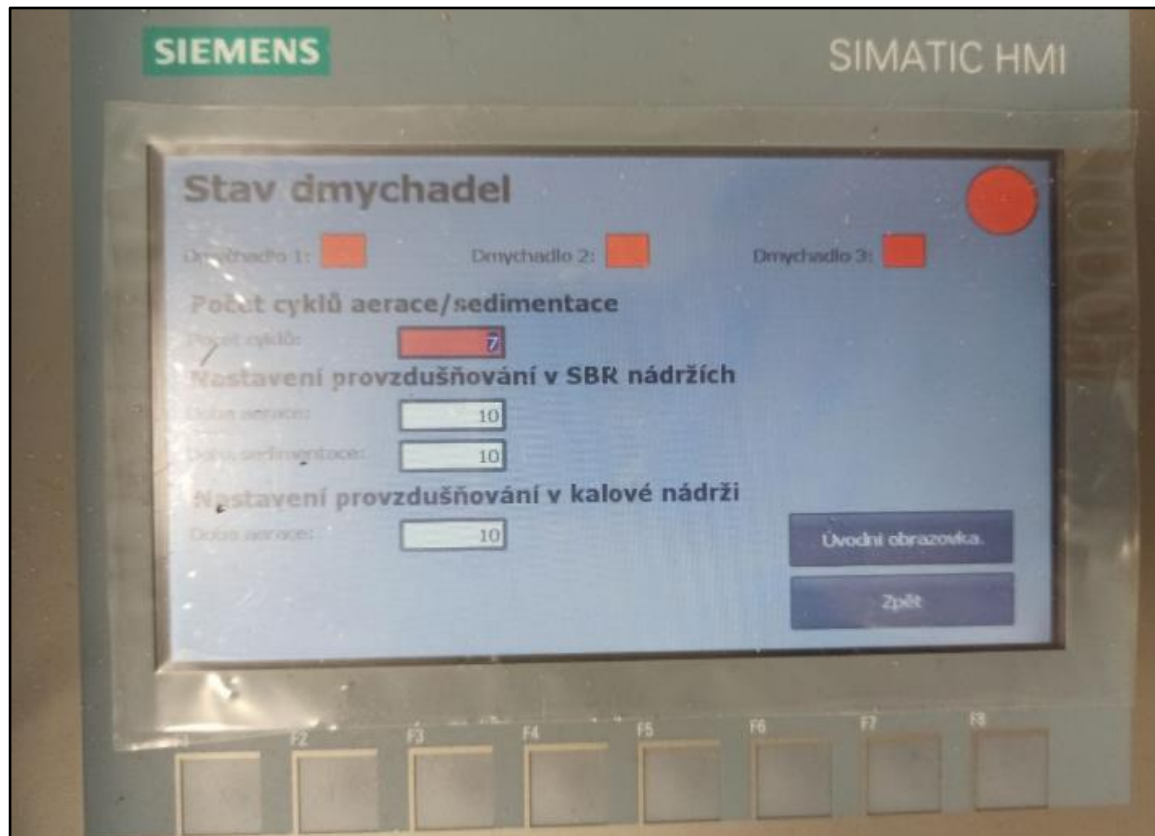
- Ukázka DoS útoku na ČOV.



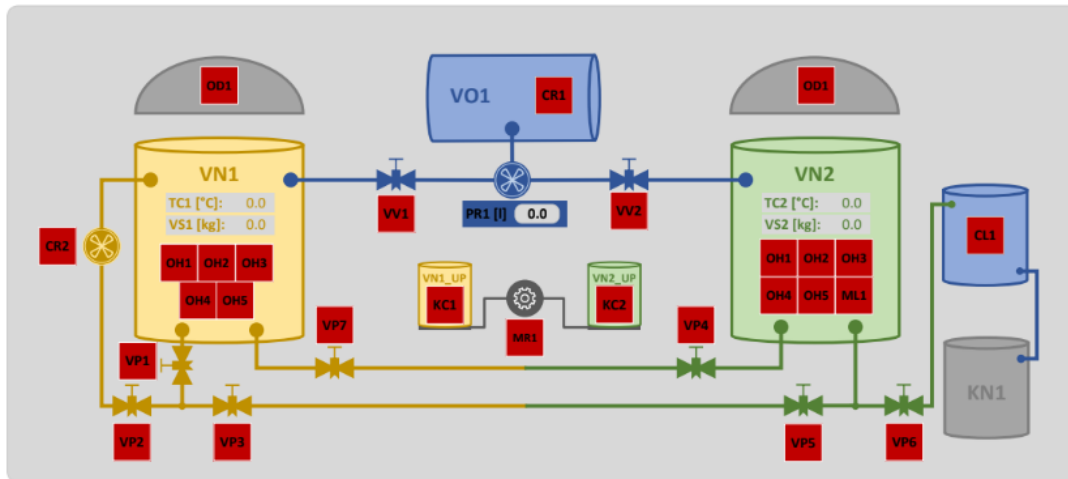


Bezpečnost průmyslových zařízení

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

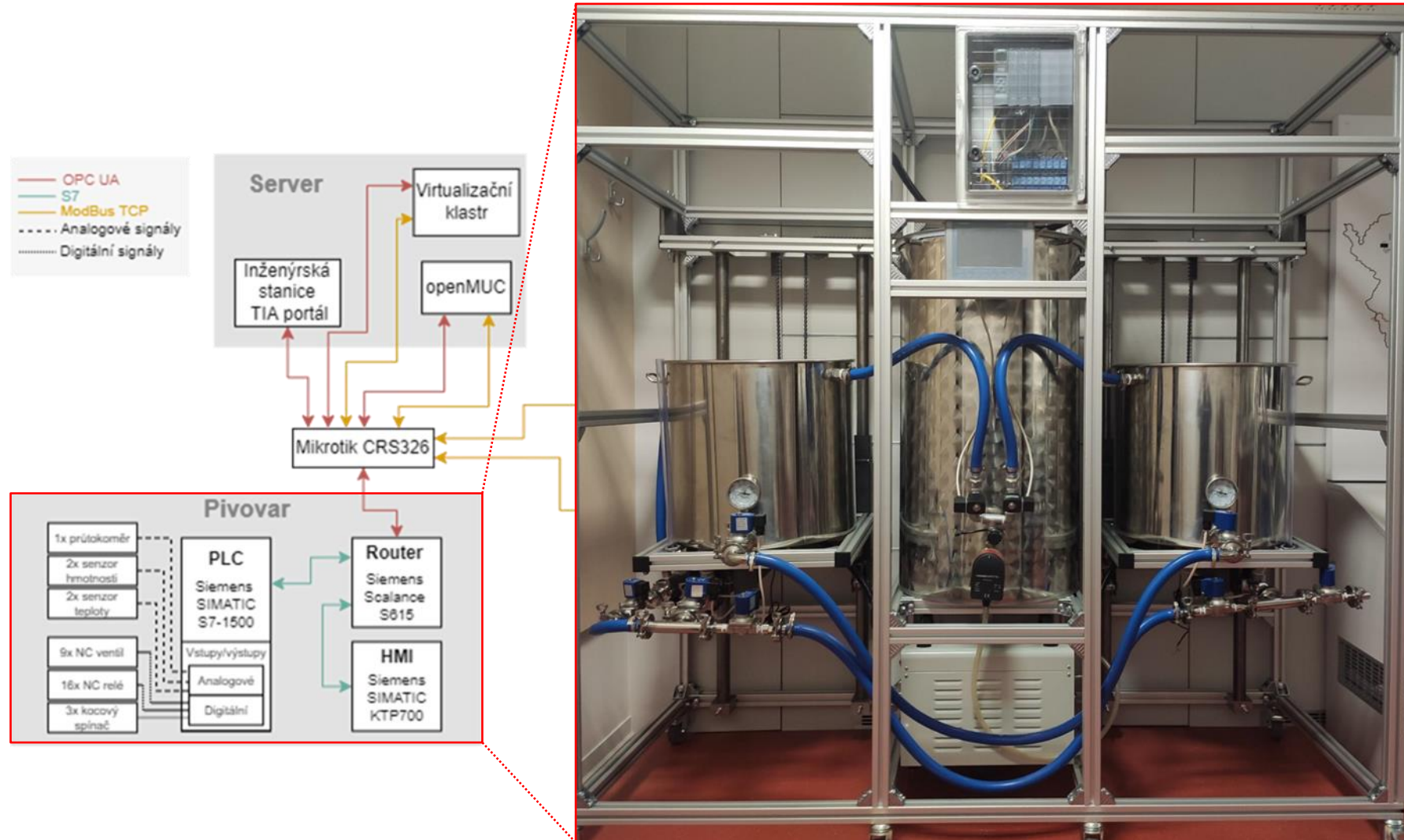


- **Pivovar s plně funkčním procesem vaření:**
 - SIMATIC PLC S7-1500 a HMI KPT700,
 - průmyslové protokoly S7Comm a Modbus TCP,
 - ethernetový přepínač Siemens Scalace XB005,
 - simulace útoků (např.: narušení procesu, DoS).

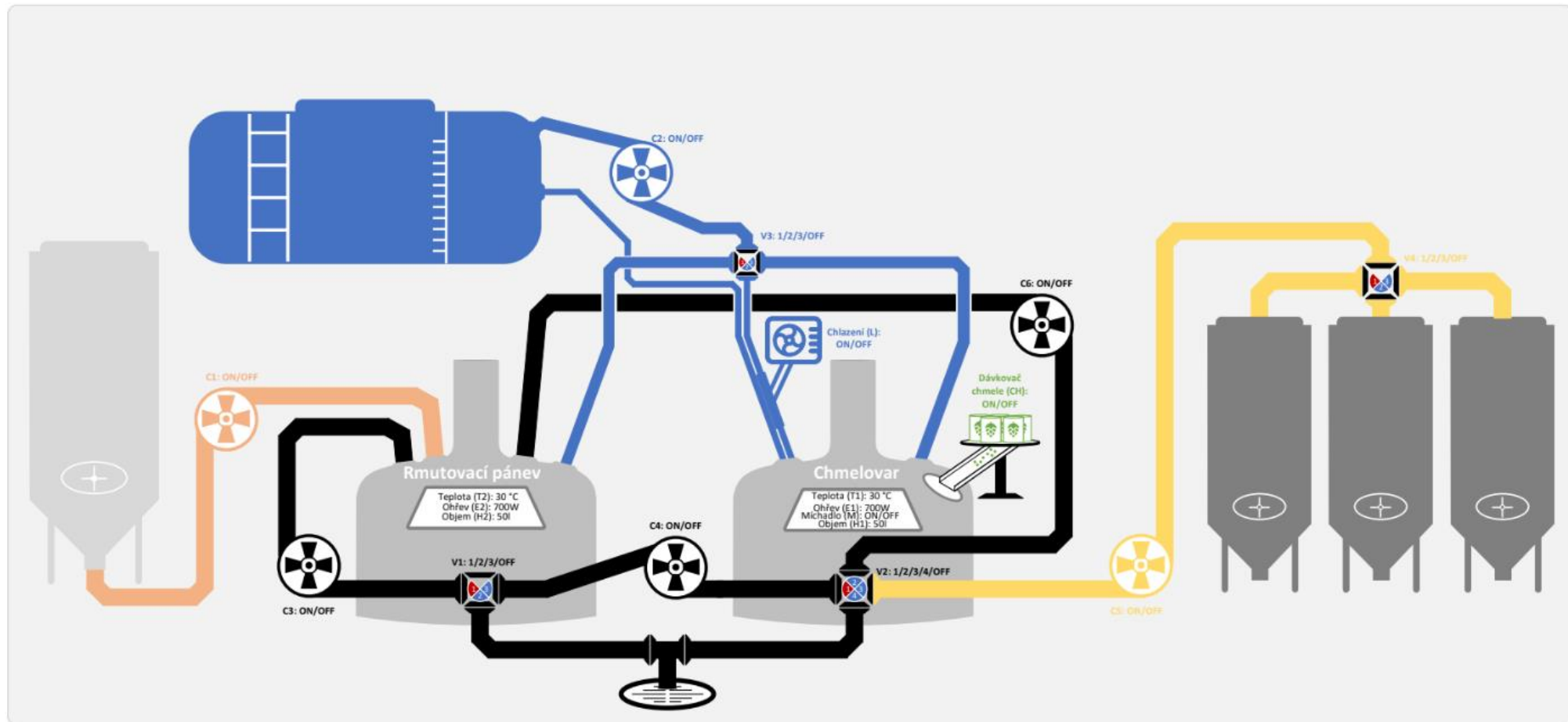




Bezpečnost průmyslových zařízení



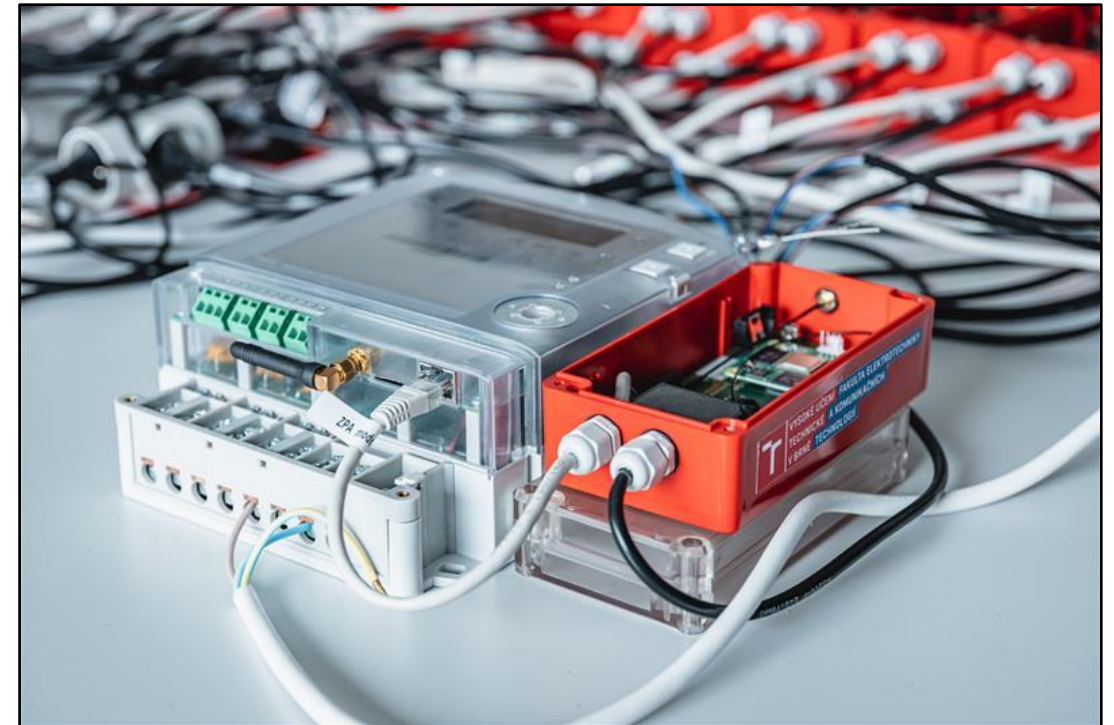
- Virtualizovaná verze pivovaru.





Bezpečnost energetické infrastruktury

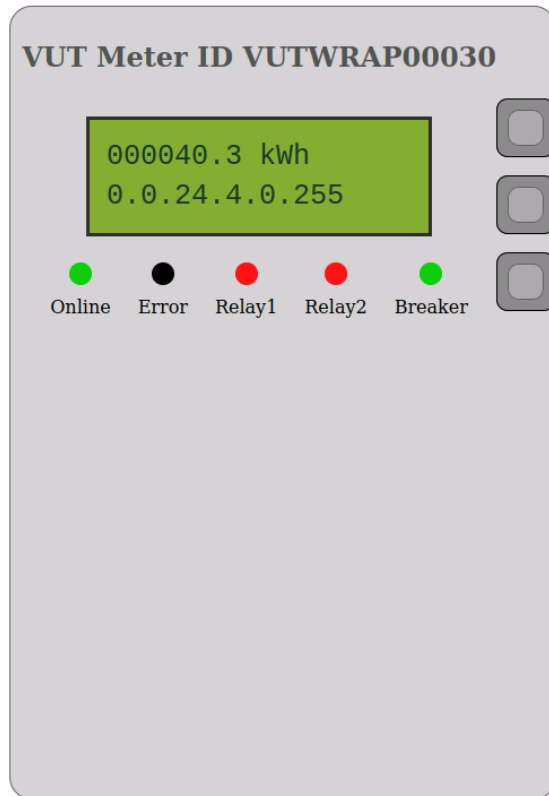
- **Certifikované DLMS/COSEM chytré elektroměry od různých výrobců.**





Bezpečnost energetické infrastruktury

- Plně virtualizovaná verze polygonu s chytrými elektroměry.



Meter

Dashboard Display TOU Table Admin

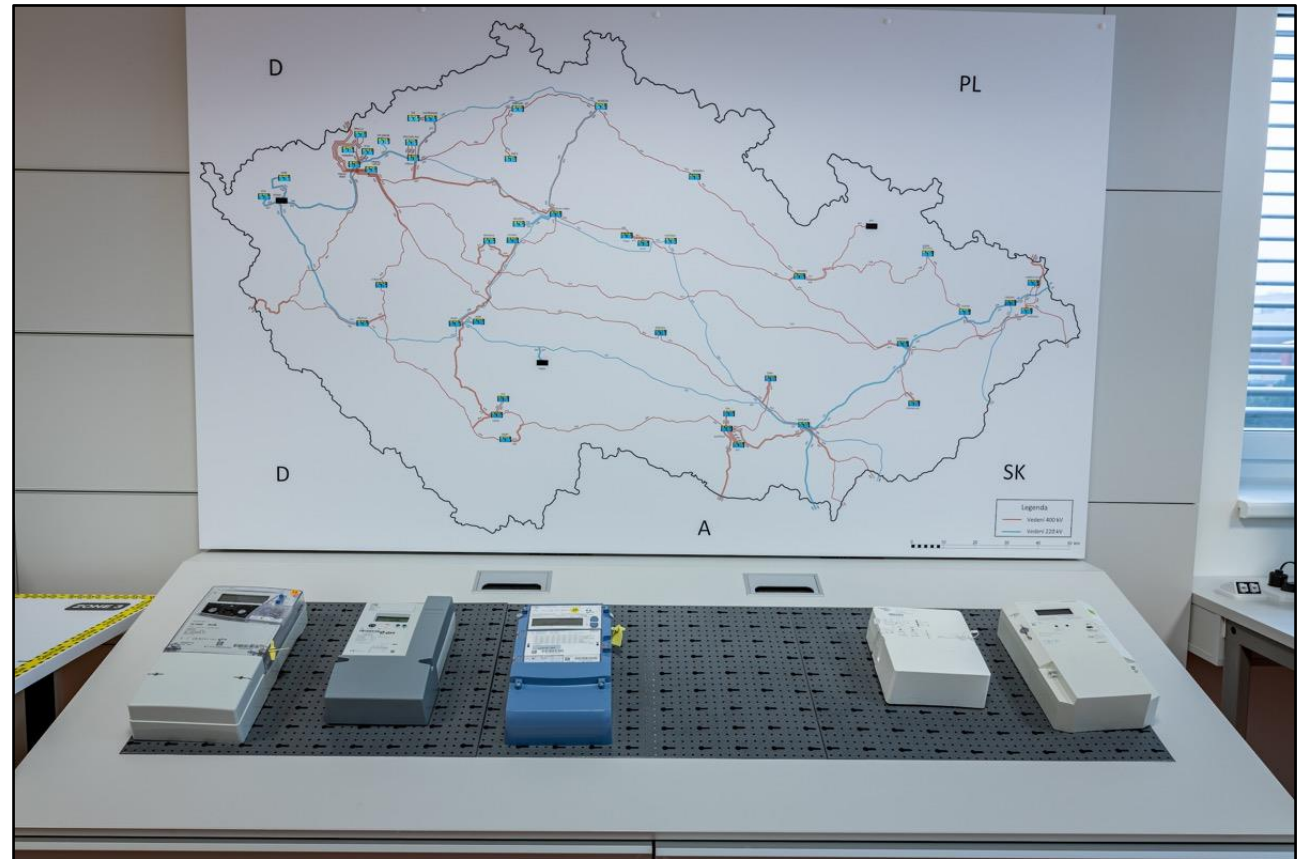
Dashboard Export

Device Parameters

Parameter	Value
Logical Name	VUTWRAP00030
IP	192.168.56.10
DLMS Port	4059
Relay 1	Connected
Relay 2	Connected
Breaker	Connected

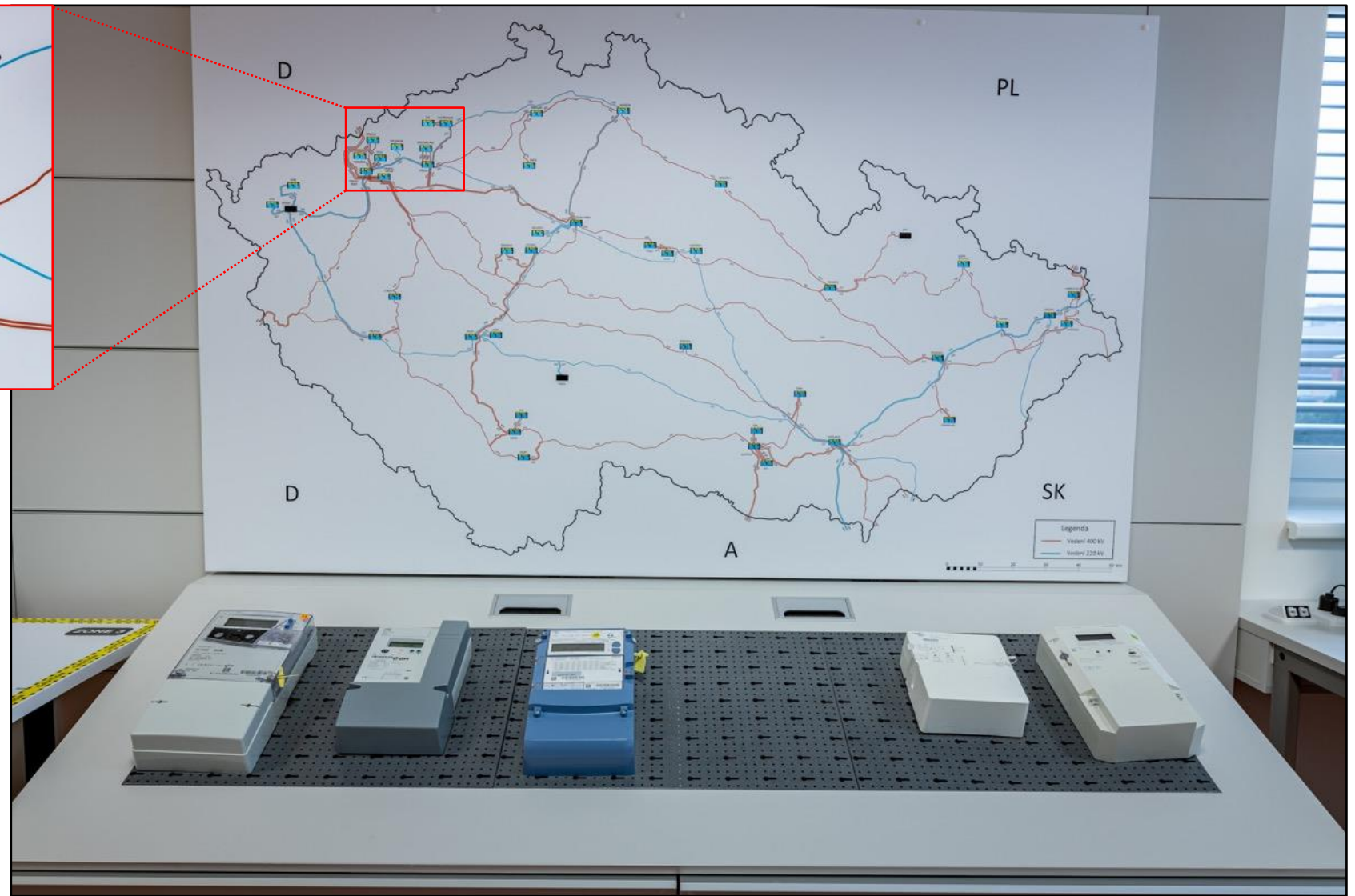
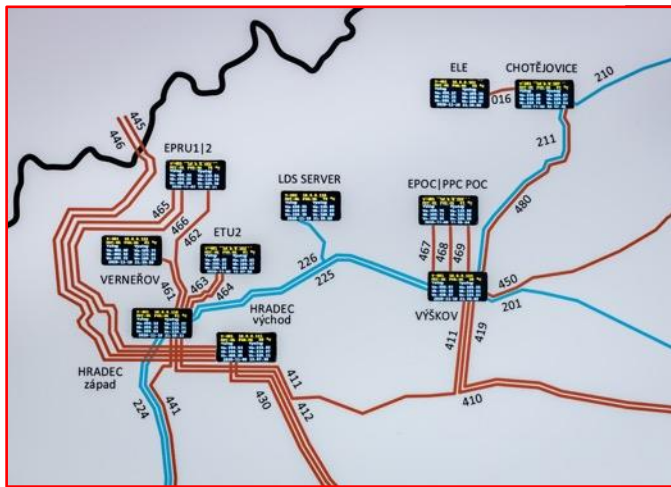
- **Elektrická přenosová soustava České republiky:**

- vlastní linuxové PLC/RTU,
- protokoly IEC-61850 a IEC-60870,
- celkem 47 zařízení Raspberry Pi,
- 34 rozvodn a 13 elektráren,
- simulace (např. podpětí a přepětí).





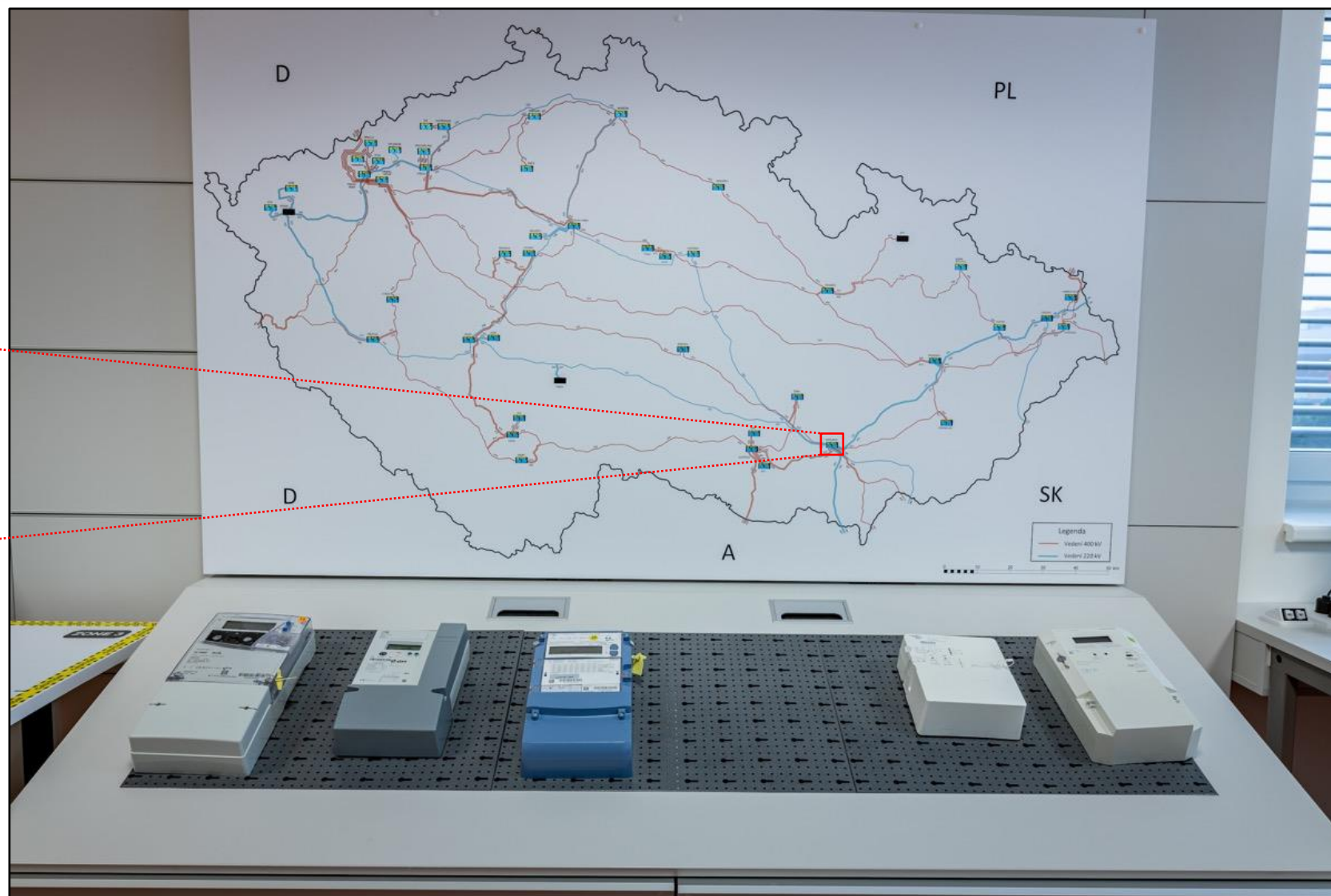
Bezpečnost energetické infrastruktury





Bezpečnost energetické infrastruktury

```
T-401 192.168.1.101
NET: X PWR: OK 63 °C
Vstup Vystup
Va: 400.97 Va: 110.67
Ub: 400.70 Ub: 110.79
Vc: 400.94 Vc: 110.89
2023-03-08 14:04:24
```



T

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 jako **lokální platforma:**

- Vysoké učení technické v Brně,
- výuka a trénink studentů,
- výzkum, vývoj a testování.



- BUTCA jako **školicí platforma:**

- jednorázové nebo opakované školení,
- fyzické a virtuální polygony,
- on-demand a ad hoc přístup.

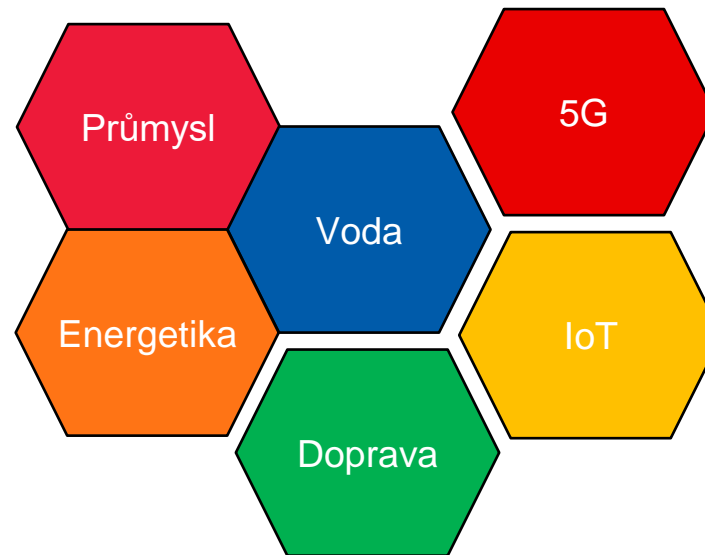


- BUTCA jako **služba na míru:**

- SaaS (Software as a Service),
- dostupnost odkudkoliv,
- minimální požadavky.



- 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>

