# Projekt TraceXpert

Projekt *Nástroje pro verifikaci bezpečnosti kryptografických zařízení s využitím AI* podpořený *Ministerstvem vnitra České republiky* (výzva IMPAKT)

ČVUT ve spolupráci s VUT a MUNI

Petr Socha, Vojtěch Miškovský
1. července 2022, Horoměřice

# Cíle

- Měření postranních kanálů
- Práce s různými komunikačními rozhraními a protokoly, kryptografickými zařízeními, osciloskopy, měřícími scénáři
- Uživatelsky přívětivé grafické rozhraní
- Multiplatformní, vícejazyčné (česky, anglicky)
- Výpočetně nenáročné
- Koncoví uživatelé: Policie České republiky (PČR), Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), Certifikační laboratoře, Univerzity,…

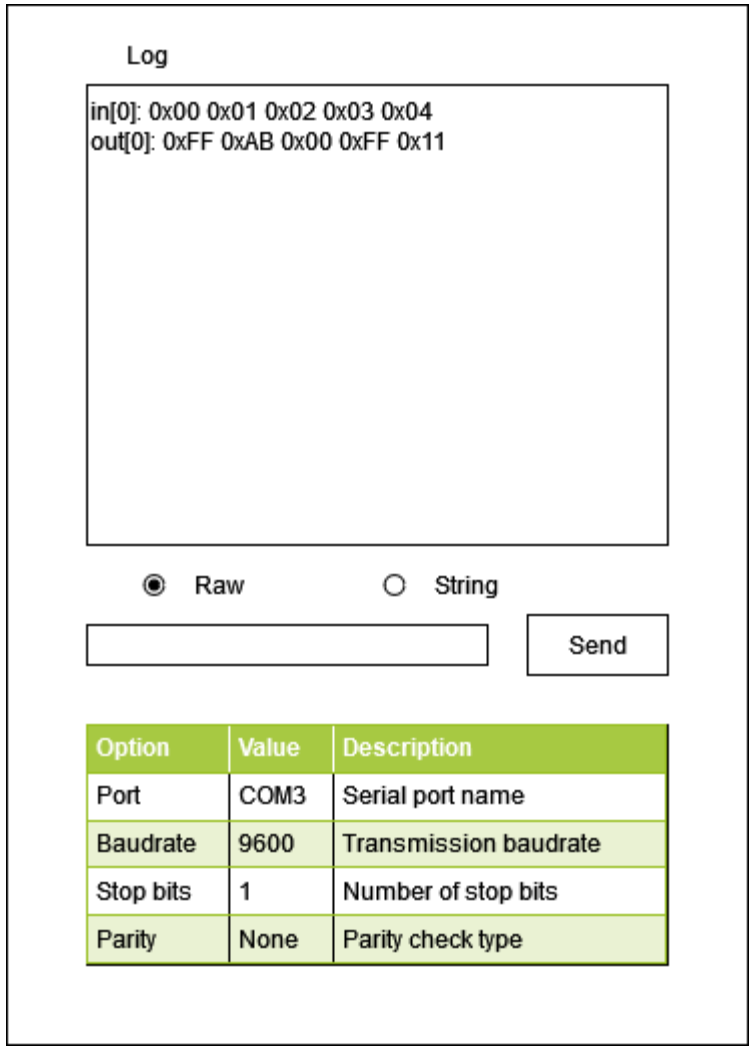
# Klíčové osoby

- Petr Socha – koordinátor prací, vývojář
- Vojtěch Miškovský – vývojář
- Tomáš Přeučil – vývojář

- David Pokorný – tester
- Martin Novotný – tester

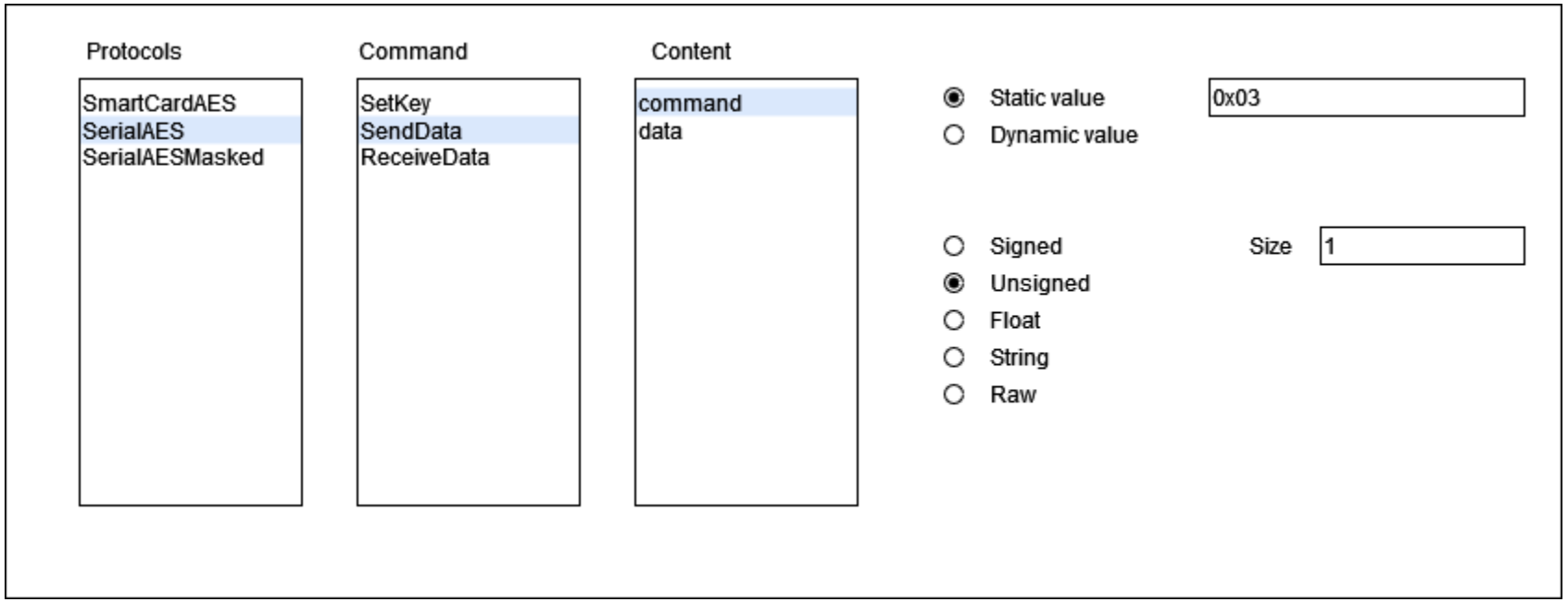
# Funkcionalita I

- Projekty
  - Uložitelné a znovu otevíratelné projekty
- Vstupně/výstupní zařízení
  - Soubory, generátory náhodných dat, sériový port, smartcard, lokální/síťový socket,…
  - Implementováno jako plug-iny se společným rozhraním
  - Plně nastavitelné a ovladatelné skrze grafické rozhraní



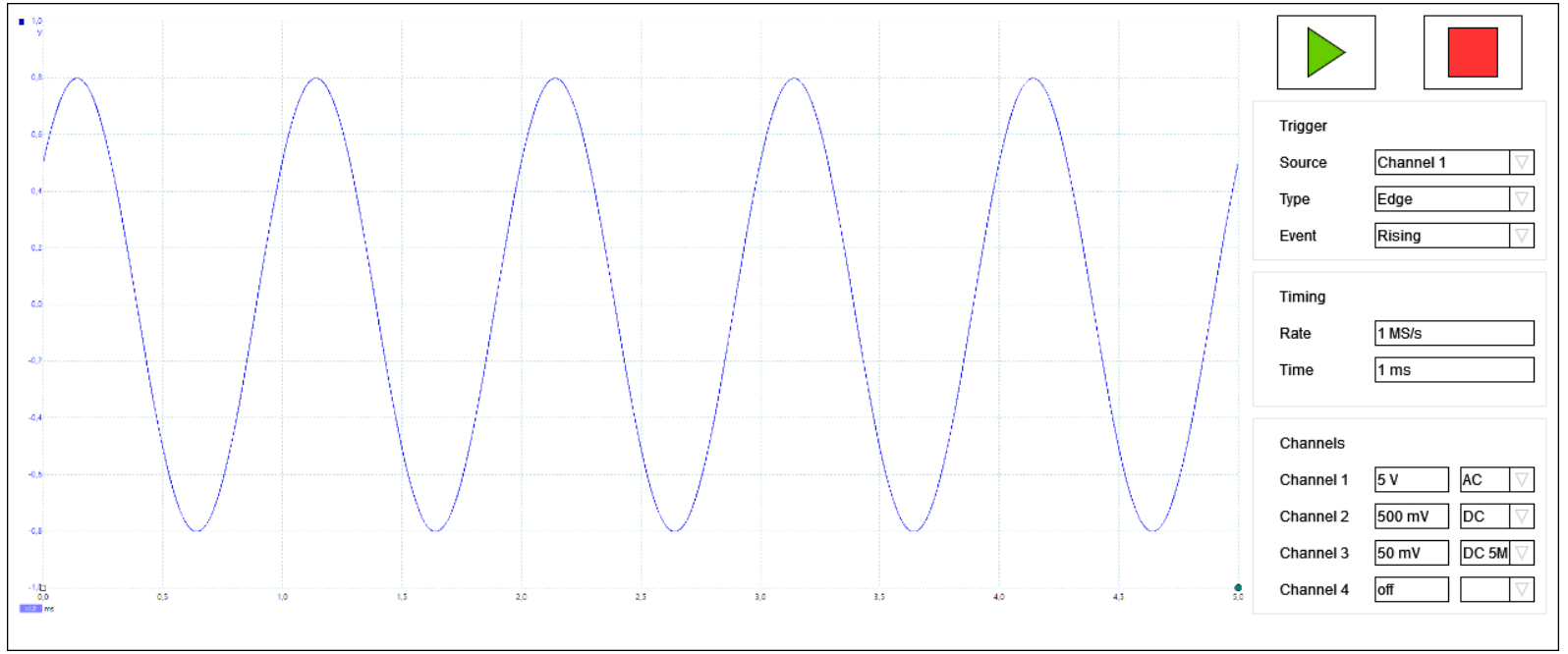
# Funkcionalita II

- Protokoly
  - Předdefinované parametrizovatelné zprávy
  - Odesílané nebo obdržené ze vstupně/výstupního zařízení
  - Konfigurovatelné skrze grafické rozhraní



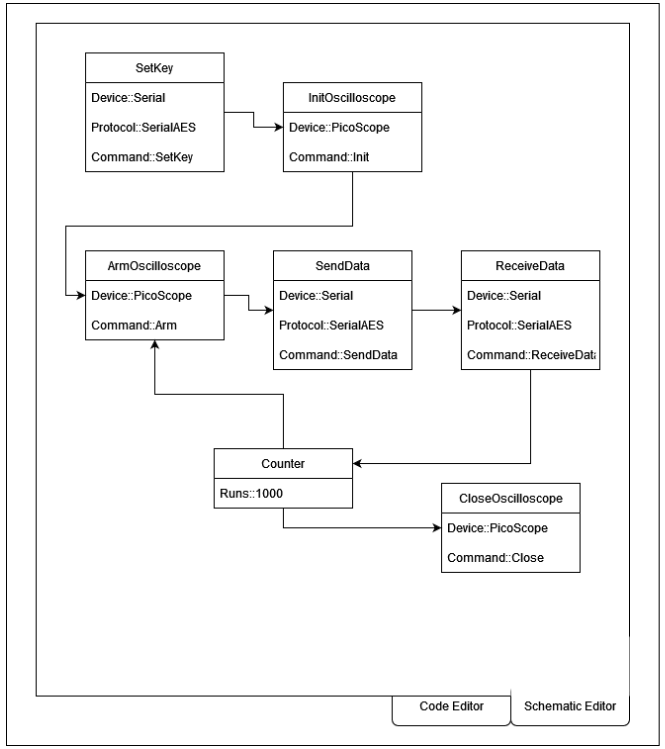
# Funcionalita III

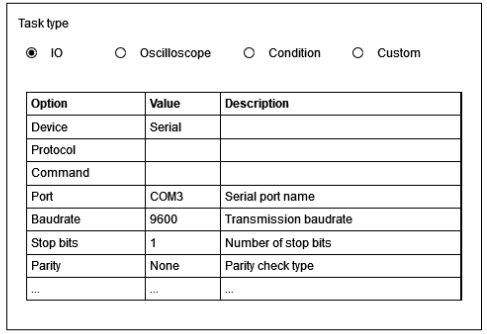
- Osciloskopy
  - Implementovány jako plug-iny se společným API
  - Plně konfiguratelné a ovladatelné skrze grafické rozhraní
  - Výstupní data (traces) snadno vizualizovatelné



# Funkcionalita IV

- Měřící scénáře
  - Automatizace ovládání vstupně/výstupních zařízení a osciloskopů
  - Plně konfigurovatelné a ovladatelné skrze grafické rozhraní
- Průvodci a vyčerpávající dokumentace




# To je vše.

Otázky?

Děkuji za Vaši pozornost.