Defence Research Day 2026: FEL ČVUT ukázala technologie pro moderní obranu: od autonomních robotů přes AI až po rozšířenou realitu a zabezpečení sítí

28.4.2026 - | Fakulta elektrotechnická ČVUT v Praze

Fakulta elektrotechnická ČVUT představila na akci Defence Research Day široké portfolio technologií a výzkumných projektů, které reagují na aktuální potřeby obrany, bezpečnosti a odolnosti státu. Návštěvníci měli možnost vidět autonomní robotické systémy, drony operující bez GNSS, nástroje využívající umělou inteligenci pro analýzu informačního prostoru, rozšířenou realitu pro zásahové jednotky i technologie pro testování a zabezpečení komunikačních sítí.

„Naší ambicí je vyvíjet technologie, které mají reálný dopad – ať už v oblasti obrany, bezpečnosti nebo kritické infrastruktury. Defence Research Day ukázal, že univerzitní výzkum může přinášet konkrétní řešení využitelná v praxi a zároveň posilovat technologickou suverenitu České republiky. Investice do výzkumu mají navíc prokazatelný multiplikační efekt – vracejí se nejen v podobě bezpečnosti, ale i ekonomického růstu, inovací a konkurenceschopnosti," uvedl děkan Fakulty elektrotechnické ČVUT prof. Petr Páta.

Autonomie pro bezosádkové platformy: spolupráce výzkumu a průmyslu

Na akci Defence Research Day na FEL ČVUT byly prezentovány výzkumné aktivity v oblasti autonomních systémů pro bezosádkové pozemní prostředky, zaměřené na jejich nasazení v náročných podmínkách obranného i civilního sektoru. FEL ČVUT se této oblasti věnuje prostřednictvím výzkumu, který na katedře počítačů v Laboratoři výpočetní robotiky (CRL) vede prof. Jan Faigl. Výzkumné aktivity se zaměřují zejména na autonomní řízení, navigaci a rozhodovací algoritmy, a to i v kontextu národních a evropských projektů.

Významnou roli v tomto směru hraje spolupráce se státním podnikem VOP CZ, která umožňuje ověřování a další rozvoj těchto metod na pokročilých bezosádkových platformách určených pro nasazení v náročných podmínkách. Tyto prostředky slouží jako testovací a validační základ pro přenos výzkumných výsledků do praxe. Platformy, jako je TAROS 6×6 vyvíjený VOP CZ, představují modulární víceúčelové prostředky využitelné pro široké spektrum úloh – od průzkumu a monitoringu přes logistickou podporu až po nasazení v krizových situacích. Spolupráce s VOP CZ přispívá k rozšiřování aplikačního potenciálu vyvíjených metod autonomie a jejich uplatnění v širším spektru scénářů. TAROS zapadá do rychle se rozvíjejícího evropského trendu bezosádkových systémů a ukazuje, že český výzkum a průmysl v této oblasti drží krok a že společně dokáží vyvíjet technologie s přímým dopadem na bezpečnost.

Od simulace po velení: virtuální realita v bezpečnostních operacích

Výzkumníci z katedry počítačové grafiky a interakce vyvíjejí technologie, které zásadně proměňují přípravu i řízení operací v bezpečnostních a obranných scénářích. Tým prof. Jiřího Žáry a dr. Davida Sedláčka pracuje na využití virtuální reality pro výcvik pyrotechniků (EOD), kde lze bezpečně simulovat komplexní situace spojené s identifikací a zneškodňováním nevybuchlé munice. Virtuální

prostředí umožňuje trénovat rozhodovací procesy, práci s detekčními nástroji i ovládání specializovaných robotů, a to v rozsahu, který by byl v reálných podmínkách časově, finančně i bezpečnostně obtížně realizovatelný.

Druhý projekt HOLO-Swarm, vznikající ve spolupráci se Skupinou multirobotických systémů FEL ČVUT a firmou QuaternAR, přináší nový koncept tzv. holografického velína. Pomocí rozšířené reality umožňuje zobrazit situaci v terénu jako interaktivní 3D model, do kterého se promítají data o pohybu jednotek, například rojů dronů, jejich stavu či plánovaných trasách. Uživatelé mohou tato data sdílet, analyzovat i přímo ovlivňovat průběh operace v reálném čase.

AR RESCUE: rozšířená realita a biomonitoring pro zásahy v CBRN prostředí

Pozornost na akci vzbudil také projekt AR RESCUE, který propojuje senzory vitálních funkcí, detekci nebezpečných látek a rozšířenou realitu pro podporu zásahových jednotek. Systém je určen pro hasiče, armádní jednotky i další složky zasahující v CBRN prostředí, tedy v situacích spojených s chemickými, biologickými, radiologickými nebo jadernými hrozbami. Jeho cílem je poskytovat zasahujícím v reálném čase klíčové informace o vlastním stavu, stavu kolegů i o nebezpečích v okolí, a to bez zbytečného zahlcení nebo odvádění pozornosti. Důležitá varování se zobrazují ve vizoru rozšířené reality na přilbě, zatímco velitel zásahu může sledovat detailnější data ve specializované aplikaci. Systém byl navržen tak, aby fungoval i při špatné konektivitě a co nejméně rozptyloval své uživatele.

Na Defence Research Day tým kolem prof. Miroslava Bureše z Laboratoře inteligentního testování systémů na katedře počítačů představil pracovní verze jednotlivých hardwarových komponent systému, včetně senzorů a vizoru. Projekt tak názorně ilustroval, že bezpečnostní technologie nevznikají jen pro „bojové“ scénáře v úzkém slova smyslu, ale i pro ochranu lidí v extrémně nebezpečných zásazích, kde rozhoduje čas, přesná informace a schopnost fungovat i v prostředí s omezenou komunikací. AR RESCUE zároveň dobře reprezentoval jednu z dlouhodobých silných stránek FEL ČVUT: schopnost propojit informatiku, elektroniku, senzory, uživatelské rozhraní a potřeby koncových uživatelů do funkčního systému s reálným aplikačním potenciálem.

Když systémy degradují: jak zabránit překvapivým narušením nebo selháním

Další prezentace z okruhu kolem prof. Miroslava Bureše se věnovala spolehlivosti a bezpečnosti systémů ve stavu degradace. Výzkumníci se zaměřují na situace, kdy komplexní systémy používané v oblasti kritické infrastruktury, IZS nebo obrany čelí výpadkům, rušení, částečnému poškození nebo kyberútoku. V takových chvílích nestačí spoléhat na ideální model provozu – je třeba umět dopředu identifikovat scénáře, v nichž mohou nastat nečekaná selhání nebo narušení, a připravit se na ně. Představená metoda využívá úmyslně jednoduché, vysvětlitelné modely a transparentní AI algoritmy, aby bylo možné rizikové situace nejen detekovat, ale také jim rozumět a vysvětlit je obsluze.

Právě tato srozumitelnost je v bezpečnostní a obranné praxi zásadní. Operátor nebo velitel nepotřebuje jen „výstup z černé skříňky“, ale musí vědět, proč je určitý stav rizikový a jaké důsledky může mít. Demonstrace se soustředila na dva reálné příklady s anonymizovanými modely situace, které ilustrovaly, jak lze pomocí této metody odhalit možná překvapení, která by mohla mít v ostrém provozu systému nepříjemné nebo i fatální důsledky. Tento směr ukázal další důležitou rovinu výzkumu FEL: ne jen vývoj jednotlivých zařízení, ale i analýzu chování celých systémů v krizových podmínkách.

ALICE: mapování informačního prostoru

Vědci z Fakulty elektrotechnické ČVUT vyvíjejí nástroje založené na umělé inteligenci, které

umožňují analyzovat informační prostor jako plnohodnotné operační prostředí. Projekt ALICE, vedený doc. Tomášem Pevným z katedry počítačů, se zaměřuje na mapování šíření informací na sociálních sítích, identifikaci jejich zdrojů a detekci koordinovaných či automatizovaných kampaní. Využívá kombinaci strojového učení, jazykových modelů a statistických metod k tomu, aby dokázal sledovat, jak informace vznikají, jak se šíří mezi jednotlivými účty a jak se v čase proměňují. Výsledkem je strukturovaný pohled na informační prostředí, který umožňuje identifikovat vlivné aktéry a porozumět dynamice šíření konkrétních narativů napříč platformami.

Projekt propojuje akademický výzkum s praktickým využitím – vzniká ve spolupráci s firmou Gerulata, která vyvíjené metody integruje do nástrojů pro bezpečnostní instituce. Ty umožňují převést velké objemy dat do přehledné podoby a výrazně zrychlit analýzu informačního prostoru, která by jinak trvala týdny až měsíce. ALICE tak ukazuje, že informační prostor lze pomocí moderních AI metod systematicky „číst“ a že schopnost porozumět tomu, jak se informace šíří a kdo je ovlivňuje, se stává klíčovou součástí současné bezpečnosti i odolnosti společnosti.

Drony bez GPS, bezpečná komunikace a evropské platformy nové generace

Výraznou oblastí prezentace byly autonomní drony, které na FEL ČVUT rozvíjí zejména Skupina multirobotických systémů (MRS) z katedry kybernetiky. Návštěvníci se seznámili s technologiemi umožňujícími let dronů v prostředí bez GNSS, se systémy pro koordinaci rojů a s přístupy, které zvyšují bezpečnost komunikace i důvěryhodnost použitých komponent. Výzkumníci ukázali, že v podmínkách moderního konfliktu už nelze spoléhat na nepřetržitou dostupnost satelitní navigace ani na nerušenou komunikaci s operátorem, a proto se vývoj posouvá směrem k vyšší autonomii, rychlejší reakci na změny v prostředí a zabezpečení robotických platforem proti převzetí nebo zneužití. Nedávná dynamická letová ukázka roje dronů zdůraznila, že skupina MRS pod vedením prof. Martina Sasky pracuje jak na bezpečných evropských dronech pro ochranu kritické infrastruktury, tak na dynamických rojích inspirovaných kolektivním chováním ptáků.

Výzkum v této oblasti se soustředí nejen na samotný let a koordinaci více strojů, ale také na zero trust principy, zabezpečené palubní počítače, flight control unity a bezpečnou komunikaci, stejně jako na vývoj platforem, které nejsou závislé na rizikových dodavatelských řetězcích. Významnou roli hraje i problematika ochrany proti dronům a droním rojům. Kombinace autonomie bez GNSS, kyberbezpečnosti a důvěryhodného hardwaru tvoří jednu z nejsilnějších obranných domén FEL ČVUT. Výsledkem nejsou jen laboratorní demonstrace, ale také technologie s přímým dopadem na schopnost českých ozbrojených sil a bezpečnostních složek fungovat v prostředí silného rušení nebo elektronického boje.

Katedra měření: výstřely, rušení GPS, lokalizace i bezpečná autentizace

Silné a velmi pestré stanoviště připravila katedra měření, která dlouhodobě rozvíjí senzory, měřicí techniku, diagnostiku a systémy přenosu dat pro bezpečnostní a obranné aplikace. Klíčovým exponátem byl systém pro akustickou detekci a lokalizaci výstřelů, který využívá autonomní senzorové jednotky osazené mikrofony a centrální vyhodnocovací jednotku se softwarovou aplikací. Měřený signál je zpracováván pokročilými algoritmy a klasifikátory s využitím AI tak, aby bylo možné odlišit výstřely od okolního hluku a minimalizovat falešné poplachy. Na místě byl představen demonstrátor bezpečnostního akustického čidla do vnitřního prostředí i zařízení pro bezpečný a automatický sběr akustických signálů bez nutnosti přítomnosti obsluhy.

Vedle akustické detekce katedra ukázala také ruční detektor rušení GPS, který umožňuje odhalit lokální rušení v pásmu L1 GPS a Galileo E1, a to jak ve všesměrovém, tak ve směrovém režimu. Dále byly představeny systémy pro lokalizaci členů IZS a bezpečnostních složek v komplexních prostorech s nebo bez GNSS, včetně nositelných komponent, bot s inerciálním systémem, radiolokačních

a komunikačních modulů a základnové stanice. Praktické portfolio doplnilo zařízení pro potlačení zvukového záznamu na mobilních telefonech a hardware Lion Key založený na FIDO2 pro bezpečnou autentizaci. Stanoviště ukázalo, jak široce lze moderní měření a zpracování signálu využít od bojiště po kritickou infrastrukturu a veřejnou bezpečnost.

Výzkum katedry měření doplňuje také projekt prof. Jana Holuba podpořený grantem NATO Chief Scientist Grants, který se zaměřuje na kvalitu a spolehlivost hlasové komunikace v zabezpečených nízkobitových kanálech. Ukazuje, že i zdánlivé detaily – například rozdíly v přenosu ženských a mužských hlasů – mohou mít v bezpečnostních a obranných aplikacích přímý dopad na srozumitelnost komunikace, únavu operátorů i riziko chyb.

VRAS: Helhest a roboty do složitého terénu

Výzkumníci prof. Tomáš Svoboda a doc. Karel Zimmermann ze skupiny Vidění pro roboty a autonomní systémy (VRAS) představili svůj výzkum zaměřený na odhad chování robotů v netriviálním prostředí na základě kamerových snímků a lidarových dat. U pozemních robotů se soustředí na predikci trajektorie a vlastností terénu v prostředí s vegetací, pískem, bahnem nebo částečně poddajným povrchem; u dronů na predikci trajektorie a větru v okolí překážek. Tyto schopnosti jsou zásadní v situacích, kdy je teleoperace rušena a GNSS není k dispozici. V takovém prostředí musí robot sám odhadnout, co si může dovolit, jak se bezpečně pohybovat a jak reagovat na terén nebo proudění, které nelze jednoduše popsat předem.

Z výzkumného zázemí skupiny VRAS na katedře kybernetiky vzešel i autonomní robot pro náročný terén Helhest, který vznikl jako první robotický spin off ČVUT. Odolný Helhest dokáže fungovat i po převrácení, pohybovat se bez GPS pouze na základě pasivních senzorů a cílí na využití v civilních i vojenských scénářích. Zároveň ukazuje, že některé výsledky univerzitního výzkumu už přecházejí z laboratorní fáze do komerčního prostředí. Defence Research Day tak nabídl nejen pohled na současný výzkum, ale i na to, jak se z něj může stát tržně uplatnitelný produkt.

E-Shaper a F-Tester: jak testovat sítě v podmínkách rušení

Katedra telekomunikační techniky prezentovala dvě technologie zaměřené na síťovou odolnost: měření a diagnostiku TCP/IP sítí včetně hlasu a emulaci TCP/IP sítí pomocí systému E-Shaper. Systém F-Tester umožňuje kvalitativní měření sítí v pásmech pod 6 GHz i nad 20 GHz a nově i vyhodnocování vhodnosti sítí pro hlas a aplikace v reálném čase. To je významné zejména proto, že stále více obranných technologií spoléhá na mobilní 5G sítě nebo satelitní komunikaci typu Starlink. Dr. Zbyněk Kocur jako hlavní vývojář zároveň zdůraznil, že jde o reálně nasaditelná zařízení, která jsou připravena nejen k měření, ale i k integraci a školení obsluhy.

Druhý pilíř stanoviště tvořil E-Shaper, tedy nástroj pro emulaci chování různých přenosových technologií a komunikačních systémů. V praxi je často nemožné testovat vše v reálném prostředí, a právě zde má emulace zásadní hodnotu: dokáže simulovat fyzické překážky, rušení, hardwarové i softwarové problémy a další faktory, které ovlivňují komunikaci v obranném provozu. Technologie byla podle podkladů upravena i pro nasazení v projektu Little Moon City Prague a na stánku byla doplněna o Edu BOX, který kombinuje emulaci s aktivním testováním sítí. Celé stanoviště ukázalo, že odolnost komunikace není jen otázkou infrastruktury, ale i schopnosti věrohodně simulovat krizové podmínky a připravit na ně technologie i lidi.

Centrum kybernetické bezpečnosti: od auditu po výcvik a certifikace

Na akci bylo výrazně zastoupeno také Centrum kybernetické bezpečnosti FEL ČVUT, které prezentovalo své komplexní služby. Ty sahají od expertního poradenství a analýzy odolnosti IT

systémů přes doporučení pro splnění regulatorních požadavků, například NIS2, až po systematické vzdělávání a přípravu na mezinárodní certifikace. Skupina Netacad dr. Jaroslava Burčíka z katedry telekomunikační techniky je jediným akademickým partnerem CompTIA v České republice a důraz klade na praktický, srozumitelný a česky vedený výcvik. V kontextu obrany a bezpečnosti je to důležité nejen pro státní správu, ale i pro kritickou infrastrukturu a firmy zapojené do obranného sektoru.

FEL ČVUT už dříve informovala například o strategické spolupráci Centra kybernetické bezpečnosti s Úřadem vlády ČR, která zahrnovala analýzu bezpečnostního stavu, školení zaměstnanců i pilotní studentské stáže. Na Defence Research Day tak centrum nepůsobilo jen jako „školitel kyberbezpečnosti“, ale jako partner, který propojuje vzdělávání, audit, zvyšování odolnosti a praktické budování kompetencí. Tím vhodně doplnilo ostatní technické demonstrátory: moderní obrana nestojí jen na robotech a senzorech, ale také na lidech, procesech a schopnosti organizací reagovat na digitální hrozby.

Autor fotografií: Petr Neugebauer

https://fel.cvut.cz/cs/aktualne/novinky/84103-defence-research-day-2026-fel-cvut-ukazala-technologie-pro-moderni-obranu-od-autonomnich-robotu-pres-ai-az-po-rozsirenou-realitu-a-zabezpeceni-siti