TECNICALL®

ČTVRTLETNÍK **ČESKÉHO VYSOKÉHO UČENÍ TECHNICKÉHO V PRAZE** I 2019

ČVUT

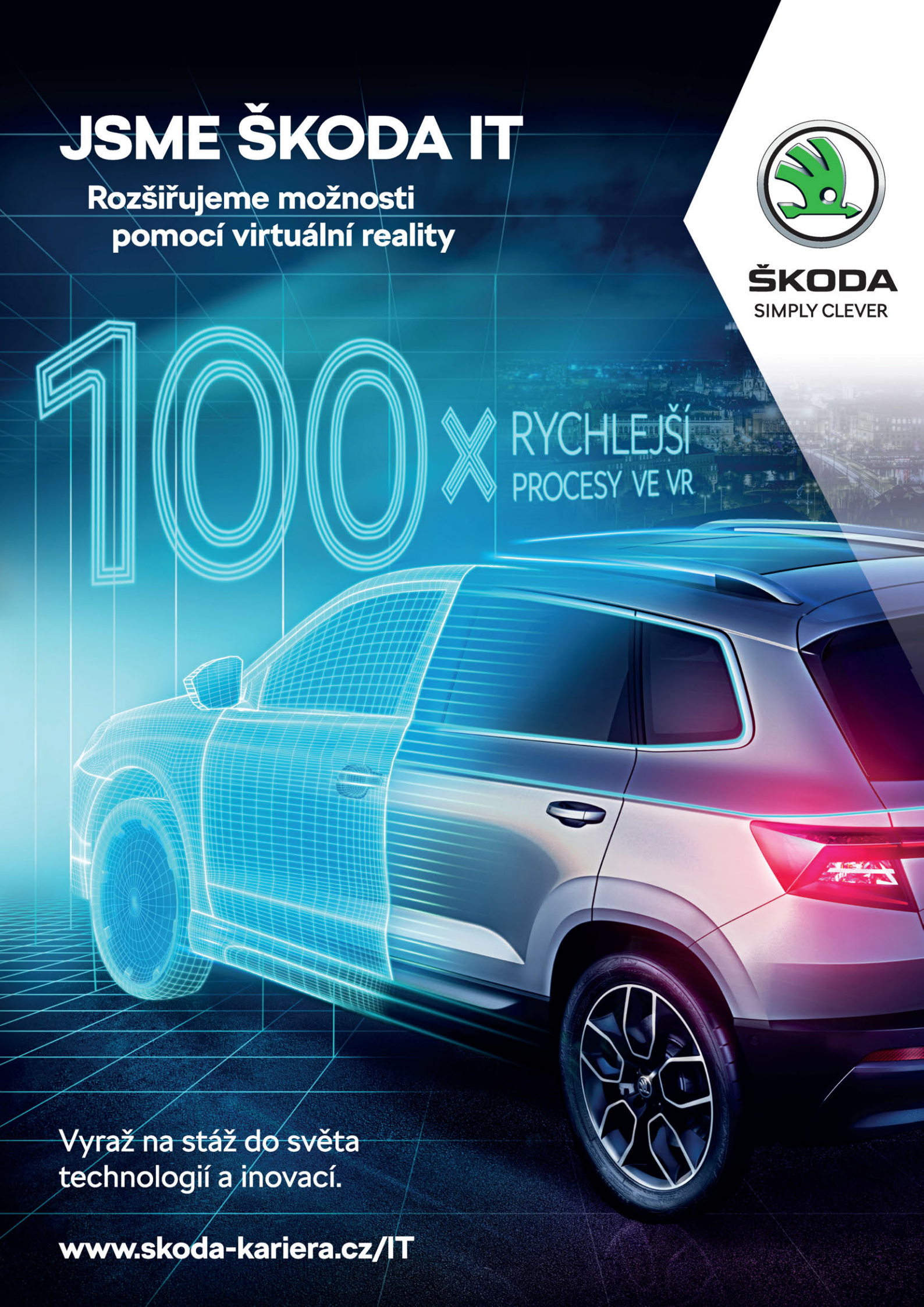
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

JSME ŠKODA IT

Rozšiřujeme možnosti pomocí virtuální reality

ŠKODA
SIMPLY CLEVER

100 X RYCHLEJŠÍ PROCESY VE VR



Vyraž na stáž do světa technologií a inovací.

www.skoda-kariera.cz/IT

prof. Ing. ZBYNĚK ŠKVOR, CSc.
Zbynek.Skvor@cvut.cz

Vážené čtenářky, vážení čtenáři,

vítejte na prvé straně jarního TecniCallu.

Číslo, které právě otvíráte, je věnováno tématu velmi aktuálnímu. Bezpečnost je slovo, které slýcháme stále častěji.

S rychlým rozvojem techniky, zvláště pak informatiky, se objevují dříve nepředstavitelné možnosti a s nimi i zcela nová nebezpečí a hrozby. Mnohé z nich si ještě v době našeho dětství uměli i ti nejnápaditější autoři science-fiction sotva představit. Celé týmy dnes pracují na tom, abychom jim i zítra byli schopni čelit. Jiné týmy je žel vytvářejí. „Kyberbezpečnost" jako obor již dávno opustila science-fiction a stává se důležitým pojmem, laikům jen obtížně pochopitelným. České vysoké učení technické v Praze má v oblasti kybernetické bezpečnosti řadu odborníků a týmů s vynikajícími výsledky. O některých z nich si v tomto čísle můžete přečíst.

K nárůstu mnohých dalších hrozeb vedly změny společnosti (v případě příklonu k terorismu se slovu „rozvoj" pero brání). Pokročilá technika může i zde pomoci rizika a hrozby omezit. Pokročilé materiály mohou ochránit před střelbou nebo účinky explozí, co nejrychlejší automatická detekce může zmírnit následky. Některé z našich výsledků popisujeme v textu.

Celá řada rizik je naopak starší než civilizace sama. Oheň, dobrý služebník, ale zlý pán, již má na svědomí mnoho životů a hodnot. Čím lépe rozumíme vzniku a dalšímu vývoji požáru, tím lépe můžeme oheň odkázat tam, kde nám jen slouží. I o tom si můžete přečíst v novém TecniCallu, který právě držíte v rukou.

Začátek roku na Českém vysokém učení technickém v Praze pravidelně znamená i začátek stovek nových projektů a výzkumných grantů. Každý z nich je něčím originální a zajímavý, alespoň o některých z nich se opět dočtete v pravidelných rubrikách tohoto čísla. V loňském roce jsme byli v získávání velkých projektů opravdu úspěšní, je o čem psát i číst.

Přeji krásné jaro a především bezpečné a zajímavé čtení.

Zbyněk Škvor,
prorektor ČVUT pro vědu, tvůrčí činnost a doktorské studium

Z obsahu

TecniCall 1/2019
Časopis pro spolupráci vědy a praxe

Vydavatel:
Rektorát ČVUT
Jugoslávských partyzánů 1580/3,
166 36 Praha 6
IČ: 68407700

www.tecnicall.cz / tecnicall@cvut.cz

Vydání: jaro 2019

Periodicita: čtvrtletník
Náklad: 5 000 ks / cena: zdarma
Evidenční číslo: MK ČR E 17564
ISSN 1805-1030

Šéfredaktorka
Mgr. Andrea Vondráková

Editorka
PhDr. Vladimíra Kučerová

Spolupracovníci z ČVUT
Fakulta stavební
Ing. Marie Gallová
marie.gallova@fsv.cvut.cz

Fakulta strojní
PhDr. Ladislav Lašek
Ladislav.Lasek@fs.cvut.cz

Fakulta elektrotechnická
Ing. Jan Sláma / slamajan@fel.cvut.cz

Fakulta jaderná a fyzikálně inženýrská
Eva Prostějovská
eva.prostejovska@fjfi.cvut.cz

Fakulta architektury
Ing. arch. Jan Jakub Tesař, Ph.D.
tesarjan@fa.cvut.cz

Fakulta dopravní
Ing. Petra Skolilová
skolilova@fd.cvut.cz

Fakulta biomedicínského inženýrství
Ing. Ida Skopalová
skopalova@fbmi.cvut.cz

Fakulta informačních technologií
Bc. Veronika Dvořáková
veronika.dvorakova@fit.cvut.cz

Design
Michaela Kubátová Petrová,
Lenka Klimtová / Nakladatelství ČVUT

Inzerce
Ing. Ilona Prausová
ilona.prausova@cvut.cz

Distribuce
ČVUT v Praze

Fotograf
Bc. Jiří Ryszawy,
Výpočetní a informační centrum ČVUT
jiri.ryszawy@cvut.cz

Tisk
Grafotechna Plus, s. r. o.

Ilustrační foto na titulu:
Bc. Jiří Ryszawy

Toto číslo bylo připraveno ve spolupráci s Nakladatelstvím ČVUT.

Zvon Zikmund

Největší český zvon a národní kulturní památka – zvon Zikmund v katedrále sv. Víta – letos oslavil 470. výročí od svého odlití zvonařem Tomášem Jarošem z Brna. Toto výročí bylo připomenuto i během osmého ročníku slavnostní akce Den zvoníků Arcidiecéze pražské, která se konala 30. dubna pod patronací J. Em. Dominika kardinála Duky OP, arcibiskupa pražského a Primase českého. Součástí akce byl také seminář, v jehož průběhu přednesli zástupci Fakulty jaderné a fyzikálně inženýrské ČVUT v Praze doc. Jan Siegl a Ondřej Kovářík výsledky získané při zkoumání stavu zvonu Zikmund v rámci spolupráce mezi Metropolitní kapitulou u sv. Víta v Praze a FJFI. Odborníci materiálového inženýrství potvrdili, že ke zlomení srdce zvonu v roce 2002 došlo únavou materiálu. Současně však došli k závěru, že je nezbytné realizovat další práce zaměřené nejen na hodnocení stavu zvonu, ale také jeho interakcí se srdcem při zvonění. Cílem je navrhnout opatření, aby zvon mohl i nadále zvonit, ale přitom aby bylo minimalizováno riziko jeho poškození a mohl být zachován pro budoucí generace.

Výsledky získané v průběhu let 2016 až 2018 vedly k závěru, že pro další bezpečný provoz zvonu Zikmund bude vyžadovat kontrolu srdce a jeho závěsu na zvonu. Pro ověření těchto závěru byli k posuzování stavu zvonu Zikmund přizváni i specialisté z „European Competence Center for Bells ECC – ProBell" při univerzitě v Kemptenu v Německu. Výsledky jejich měření z prosince 2018 zcela jednoznačně potvrdily závěry získané pracovníky FJFI.

Tým docenta Jana Siegla se dlouhodobě věnuje studiu degradačních procesů materiálů a analýzám poruch strojů a zařízení. Získané výsledky jsou nejen publikovány v odborných časopisech, ale slouží i pro praktické využití v průmyslu. Mezi dlouhodobé průmyslové partnery patří například ČEZ, a.s., Aero Vodochody AEROSPACE a.s., ČZ a.s. Strakonice.

(red) foto: archiv

Centrum pro řízení typu drive by wire

Nové výzkumné centrum Smart Driving Solutions vzniklo na Katedře řídicí techniky Fakulty elektrotechnické ČVUT. Tým třinácti vědců pod vedením Ing. Tomáše Haniše, Ph.D., si bere za cíl změnit zaběhlé uvažování a připravit půdu pro novou technologii aktivního dynamického řízení aut, jejíž obdoba se již delší dobu používá u letadel. Odborníci z katedry se dlouhodobě zaměřují na dosud neprosazený koncept řízení aut zvaný drive by wire, při němž řidič neovládá kola či motor vozu přímo, ale prostřednictvím elektronické řídicí jednotky, která má plnou kontrolu nad podvozkem. Jde o technologickou revoluci, kterou již prošel letecký průmysl (tzv. fly by wire systémy jsou u dopravních letadel běžné a u stíhaček nezbytné), v automobilovém průmyslu však na ni kvůli konzervativnímu přístupu automobilek ještě nedošlo. Ing. Tomáš Haniš, Ph.D., je výzkumník a vývojář, který přichází na ČVUT se zkušenostmi z firem Porsche Engineering Services a Rolls-Royce (divize aerospace).

Motivací pro vznik výzkumného centra byla situace v současném automobilovém průmyslu. Zatímco konstruktéři podvozků postupně přidávají do aut systémy typu ABS, ESP, ASR a další, z druhé strany automobilky investují nemalé peníze do vývoje plně autonomního řízení.

Centrum Smart Driving Solutions má pro rok 2019 rozpočet s alokací 8,5 milionů Kč určených převážně na personální výdaje, centrum se dále chystá se navazovat partnerství s významnými komerčními partnery v oblasti automobilového a leteckého průmyslu a usilovat o grantovou podporu z veřejných zdrojů ČR a EU.

(red) foto: FEL

Profesor Vladimír Mařík získal prestižní cenu Manažer roku 2018

Nejlepšími manažery v České republice za rok 2018 se stali prof. Ing. Vladimír Mařík, DrSc., dr. h. c., vědecký ředitel Českého institutu informatiky, robotiky a kybernetiky ČVUT (CIIRC), a Tanja Vainio, generální ředitelka společnosti ABB pro Českou republiku a Slovenskou republiku. Cenu Manažer roku vyhlašuje Česká manažerská asociace, letos se uskutečnil už 26. ročník této prestižní aktivity. Oba vítězní Manažeři roku zastupují oblast moderních technologií.

Na slavnostním galavečeru v paláci Žofín 25. dubna, při němž se sešly tři stovky manažerských osobností a hostů, získal profesor Mařík kromě hlavní kategorie také ocenění Smart manažer roku. Titul Manažer roku 2018 získal zejména za své úsilí prosadit moderní metody organizace a řízení. „Šlo a jde mi o vybudování vysokoškolského ústavu nového typu, uznávaného v mezinárodní vědecké aréně a přínosného pro rozvoj české ekonomiky," uvedl k důvodům, proč CIIRC vznikal.

(red)

foto: BusinessInfo.cz

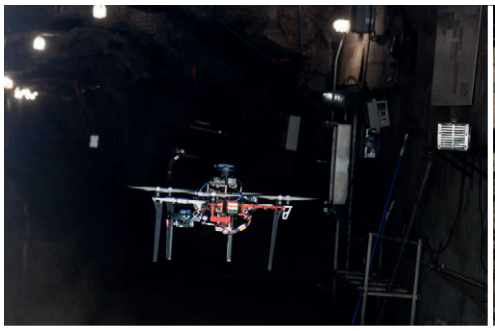
Drony hledaly „zavalené horníky"

Vědci z Katedry kybernetiky a z Katedry počítačů Fakulty elektrotechnické ČVUT v Praze se v dubnu úspěšně účastnili přípravného kempu soutěže DARPA (Defense Advanced Research Projects Agency), který se konal v horách nedaleko města Denver v USA. Cílem DARPA Subterranean Challenge, která má celkový rozpočet převyšující v přepočtu 250 milionů Kč, je vyvinout systém autonomních spolupracujících pozemních robotů a dronů, kteří bez lidské asistence dokáží prozkoumat důl v případě důlního neštěstí a najít v něm známky přítomnosti zavalených horníků.

Tým ČVUT CTU-CRAS v rámci simulované soutěže dosáhl nejlepšího výsledku ve své skupině a jeho roboty dokázaly v prostředí skutečného dolu nalézt několik předmětů potvrzujících existenci přeživších horníků. Přístroje se dokonce dostaly do oblasti, kde byla jedna z figurín reprezentujících zraněnou oběť neštěstí.

Velkým příslibem do finálového kola soutěže, které se bude konat v srpnu v dosud neznámém dole v USA, bylo překonání domácího týmu složeného z univerzit v Denveru a Boulderu a také několika amerických firem specializujících se na vývoj robotických záchranných systémů v dolech a lomech. Dosažené výsledky a možnost dále testovat systém v experimentálním dole ČVUT dává týmu CTU-CRAS velmi reálnou šanci v soutěži uspět, získat jednu z cen v celkové výši 3 miliony amerických dolarů a hlavně se výrazně prosadit v oblasti světového výzkumu robotických systémů a jejich reálného nasazení v záchranných misích, ale i inspekčních a monitorovacích prací v libovolných komplexech tunelů a podzemních prostor.

(red) foto: FEL



Laboratoř otevřených dat

Fakulta informačních technologií ČVUT v Praze ve spolupráci s firmou Profinit EU představila 20. února nově vzniklou Laboratoř otevřených dat (OpenDataLab), ve které si studenti mohou vyzkoušet práci s otevřenými zdroji dat. Naskýtá se jim tak jedinečná příležitost zkoumat data o dopravní obslužnosti, hospodaření státu, životním prostředí a mnoha dalších oblastech, a to formou semestrálních a závěrečných prací.

Open data, smart city a IOT je, podobně jako informační bezpečnost, skloňována ve všech směrech. Mnozí v datech vidí příležitost, jak ušetřit nebo zefektivnit stávající procesy a zlepšit život obyvatel. Chytré odpadkové koše, které si řeknou o vyvezení, chytrá parkovací místa nebo lampy s detekcí znečištění ovzduší znějí jako sci-fi. Například v Praze však již několik takovýchto chytrých lamp je.

„Dostupných dat je velké množství a jejich využití pokulhává. Ve společné laboratoři budou vznikat nové aplikace, analýzy a závěry usnadňující každodenní život. Nejvyšší kontrolní úřad pravidelně pořádá hackathon státní správy, ale to nestačí. Představte si, že máte informace o množství aut aktuálně vjíždějících do Prahy, znáte množství parkovacích míst v centru a jejich obsazenost a máte data o znečištění. Pak dokážete spočítat, že se dostáváte za hranu, kdy město již není schopné množství provozu zvládnout a můžete dopravu začít dynamicky regulovat. Nemá význam auta pouštět do centra, pokud tam není dostatek míst k zaparkování nebo je město naprosto ucpané," říká Ing. Marek Sušický, který má Laboratoř otevřených dat za firmu Profinit na starosti. V rámci OpenDataLab budou studenti FIT ČVUT zapojeni i do výzkumu v oblasti otevřených a propojených dat, jenž pomůže lépe řešit praktické úkoly, například v oblasti datové žurnalistiky. Zároveň se tím vytváří poptávka po otevírání a propojování dalších zajímavých datových zdrojů veřejné správy.

(red)

foto: Jiří Ryszawy

prof. Ing. VLADIMÍR MAŘÍK, DrSc., dr. h. c.
Vladimir.Marik@cvut.cz

RICAIP | Základ ekosystému pro umělou inteligenci

Český institut informatiky, robotiky a kybernetiky ČVUT (CIIRC) získal z EU významnou podporu pro vybudování a rozvoj centra RICAIP (Research and Innovation Centre on Advanced Industrial Production), které je vytvářeno od roku 2017 ve spolupráci s CEITEC VUT Brno, DFKI a ZeMA (oba ze SRN, Saarbrücken). DFKI je největším německým výzkumným centrem pro umělou inteligenci (AI) s více než tisícovkou výzkumníků a jeho klíčovou postavou je prof. Wolfgang Wahlster, autor koncepce Industrie 4.0 a vůdčí osobnost německého výzkumu. ZeMA je významným experimentálním centrem pro průmyslovou automatizaci.

Cílem RICAIP je vybudovat evropské centrum excelence pro umělou inteligenci a průmyslovou robotiku a tím přispívat k základnímu a aplikovanému výzkumu ve všech dotčených oblastech umělé inteligence a potřebných počítačových disciplín pro podporu moderního průmyslu (zejm. strojového učení, robotiky, plánování a rozvrhování, vyvozování apod.). Ambicí je též vytvořit ekosystém spolupráce akademických institucí, malých a středních podniků, globálních průmyslových firem, start-upů, inkubátorů, organizací pro podporu regionů (jako např. Středočeské inovační centrum, Jihomoravské inovační centrum) a sdružení (Svaz průmyslu a dopravy ČR, Hospodářská komora), zaměřený na konkrétní výsledky při řešení současných technologických a ekonomických výzev v průmyslu. Centrum má v úmyslu podporovat interdisciplinární výzkum a spolupráci s netechnickými obory tak, aby pomáhalo řešit složité problémy a potřeby společnosti. Samozřejmě chce též propojovat výzkum s výukou a výchovou nových odborníků pro potřeby výzkumu, průmyslu i veřejné sféry. Těžištěm je rozvoj výzkumné infrastruktury pro podporu průmyslové výroby (RICAIP Industrial Testbed Core), a to jako základ budoucí evropské výzkumné infrastruktury v předmětné oblasti.

Průmyslový testbed RICAIP bude první svého druhu v České republice a jako první bude geograficky distribuovaný nejen napříč naší zemí (v úvodní fázi Praha–Brno), ale též napojený na testbed německých partnerů v Saarbrückenu. Průmyslový testbed je budován kromě podpory z veřejných zdrojů i díky přispění takových firem, jako je Siemens, Škoda Auto, Kuka, Festo a SAP i českých společností DEL, SIDAT či ABRA. První část testbedu, tedy pružného experimentálního výrobního úseku s možností nasadit až osm robotů, je již v provozu a byla v ní vyvinuta zajímavá technická řešení např. pro LEGO či pro Škoda Auto. Několikrát testbed pracoval v módu propojení a integrace s roboty umístěnými fyzicky jinde (např. v suterénu budovy nebo v Saarbrückenu s využitím principů virtuální a rozšířené reality). Cílem veškerého výzkumu, vývoje a experimentálních prací kolem testbedu je vybudovat geograficky distribuovabnou infrastrukturu pro rychlý vývoj nových výrobních linek a zkrácení doby jejich náběhu. Neméně důležitou roli bude testbed sehrávat při retrofittingu a inovacích stávajícího výrobního zařízení či při zavádění principů Průmyslu 4.0 do stávajících výrobních linek při krátkodobě přerušené či nepřerušené výrobě. Novou či inovovanou linku bude možné odladit, odzkoušet a optimalizovat na strojích umístěných na libovolném místě na světě a integrovaných za využití principů znalostní integrace a virtuální reality bez nutnosti linku napřed sestavit na jednom místě. Očekávané úspory jsou v takovém případě pochopitelně velmi vysoké, přínos umělé inteligence zcela nesporný.

Jádrem integrovaného řešení je systém PLM obsahující veškerá zdrojová data k životnímu cyklu výrobku, což umožňuje efektivní spolupráci různých týmů na vývoji výrobku (CAD/CAM, Simulations), při přípravě výroby či aktualizací výrobních dat na základě informací z již běžící výroby. Dlouhodobým cílem je vytvořit v testbedu jakýsi showroom, který se bude přizpůsobovat cílové skupině, kterou je např. veřejnost, školy, výrobci strojů, provozovatelé automatizované výroby se zájmem o inovaci dle Průmyslu 4.0. Uživatelské scénáře včetně popisu použitých technologií a řešení budou prezentovány odpovídajícím způsobem.

RICAIP získal podporu pro první fázi stejnojmenného projektu v rámci EU program TEAMING I. v období září 2017 až srpen 2018 jednak od EU (400 tis. EUR), jednak od německé vlády (1 mil. EUR). V rámci první fáze nejenže proběhly prvotní experimenty, ale zejména byla připravena zcela unikátní koncepce navazující druhé fáze projektu pod názvem RICAIP II. Ten se ve velmi náročné evropské soutěži 120 projektů umístil na druhém místě ze všech a v dubnu 2019 bylo potvrzeno jeho financování v požadovaném rozsahu. V příštích téměř sedmi letech bude projekt podpořen 49 miliony EUR, z čehož téměř 27 milionů EUR poputuje do CIIRC ČVUT. Na celkové částce 49 milionů EUR se EU (H2020) podílí 15 miliony EUR a operační program OP VVV pak částkou 34 milionů EUR. Prostředky jsou určeny především na budování a údržbu nákladné infrastruktury, v menším rozsahu pak na pilotní výzkumné a vývojové práce, kde se předpokládá synergie s dalšími evropskými a národními projekty.

Velmi významné je, že přijatý projekt RICAIP II počítá s formováním Centra do podoby Evropského centra excelence a s budováním jádra evropské výzkumné infrastruktury, k níž se budou připojovat další laboratoře a výzkumná pracoviště v Evropě i mimo ni. Již dnes např. konkrétně jednáme o propojení s jedním z předních korejských výzkumných center. Projekt předpokládá značnou autonomii Centra jako pilotního řešení v evropském prostoru. Ředitel Centra bude vybrán v mezinárodním výběrovém řízení a bude mít dostatek pravomocí pro rozhodování a řízení. Budou vytvořeny tři adekvátně financované výzkumné pozice typu „tenure", pro něž bychom chtěli získat opravdu špičkové odborníky ze světa.

Centrum RICAIP je klíčovou součástí celého ekosystému pro umělou inteligenci v rámci CIIRC, systémově budovaného po řadu let, a to ekosystému s celoevropským přesahem. Patří do něj nejen Centrum RICAIP, ale i testbed dále budovaný a rozšiřovaný o těžké výrobní stroje ve spolupráci s Fakultou strojní ČVUT, Národní centrum kompetence Kybernetika a umělá inteligence (program TA ČR), na němž se podílejí i FS, FD a FBMI. Velmi významnou roli zde hraje Národní centrum pro Průmysl 4.0 a též evropský Digital Innovation Hub (DIH) pro umělou inteligenci, který CIIRC získal v březnu 2019. Jedná se o jediný DIH pro umělou inteligenci, který se podařilo získat do České republiky a který bude sehrávat významnou roli při integraci českého a evropského výzkumu a transferu know-how v oblasti umělé inteligence. Jsme důležitými partnery rozsáhlého evropského projektu EIT „Manufacturing" (celkové financování 330 mil. EUR), od nějž očekáváme zajištění výzkumných aktivit v rámci testbedu s vysokým komerčním potenciálem. Pozornost je věnována i eClubu jako inkubátoru startupových firem. V neposlední řadě je třeba zmínit i rozhodnutí CLAIRE (panevropské sítě AI komunity) vytvořit na CIIRC ČVUT svou kancelář – teprve čtvrtou v Evropě (po ústředí v Haagu a kancelářích v Saarbrückenu, Oslu a Římě).

O umělé inteligenci se v posledním roce mluví na všech úrovních a snad na všech konferencích. Umělá inteligence se stala klíčovou součástí Národní inovační strategie, má svůj národní akční plán. CIIRC o dané oblasti nejen hovoří, ale zejména koná a systémově po řadu let realizuje výzkum s konkrétními výsledky mezinárodního významu. Současně se snaží být užitečným centrem pro podporu průmyslu v České republice, protože efektivně propojuje evropský výzkum s potřebami malých a středních českých podniků v návaznosti na výzkumnou kooperaci se světovými lídry. Snaží se připravovat českou ekonomiku, zejména sektor průmyslové výroby na nadcházející změny, bez nichž by tento segment české ekonomiky ztratil konkurenceschopnost.

Cílem RICAIP je vybudovat evropské centrum excelence pro umělou inteligenci a průmyslovou robotiku a tím přispívat k základnímu a aplikovanému výzkumu ve všech dotčených oblastech umělé inteligence a potřebných počítačových disciplín pro podporu moderního průmyslu (zejm. strojového učení, robotiky, plánování a rozvrhování, vyvozování apod.). Ambicí je též vytvořit ekosystém spolupráce akademických institucí, malých a středních podniků, globálních průmyslových firem, start-upů, inkubátorů, organizací pro podporu regionů a sdružení zaměřený na konkrétní výsledky při řešení technologických a ekonomických výzev v průmyslu.

autor: Vladimír Mařík
foto: archiv CIIRC

PhDr. MONIKA DOBIÁŠOVÁ, Ph.D.
Monika.Dobiasova@cvut.cz

„Je pro nás mimořádně důležité, abychom na ČVUT podporovali inovační potenciál talentovaných studentů. Právě projekt CIPA je unikátní příležitostí a věřím, že získáme celou řadu nových zkušeností a příležitostí," uvedl k novému programu rektor ČVUT doc. Vojtěch Petráček.

Nápady pro firmy

Prezentace prvních výsledků Česko-izraelského akcelerátoru

Myšlenka programu česko-izraelského akcelerátoru (CIPA) vznikla jako reakce na současné trendy ve vysokoškolském vzdělávání přiblížit studentům co nejvíce již během studia praxi a reálné požadavky současného byznysu. Týmy studentů dvou technických univerzit, ČVUT v Praze a Technionu, představily na konci dubna své výsledky v Haifě. Tématem prvního ročníku bylo Smart City.

Přestože součástí běžné univerzitní výuky se stále více stávají různé případové studie, které by měly simulovat skutečné úkoly, se kterými se úspěšní absolventi budou setkávat během své profesionální dráhy, je jasné, že často mají do reálné praxe daleko a jejich přínos pro studenty má své limity.

Pro ČVUT je mimořádně důležité podporovat studenty v kreativitě, inovačním přístupu a v osvojování podnikatelských dovedností. „Jsem rád, že na půdě ČVUT vznikají nové příležitosti k propojování vědy a průmyslu za aktivní účasti studentů i zkušených odborníků z praxe. Je pro nás mimořádně důležité, abychom na ČVUT podporovali inovační potenciál talentovaných studentů. Právě projekt CIPA je unikátní příležitostí a věřím, že získáme celou řadu nových zkušeností a příležitostí," uvedl k novému programu rektor ČVUT doc. Vojtěch Petráček.

Požadavkem, na který je nutné absolventy technických vysokých škol mnohem více připravovat, je efektivní multidisciplinární kooperace. Mezinárodní spolupráce ve virtuálních týmech je již dlouhou dobu samozřejmostí v komerční sféře, do systému výuky se tyto požadavky však promítají pozvolna. Existují sice různé studentské výměnné a pobytové programy, ale v komerční sféře probíhá řešení úkolů většinou jako spolupráce lokálních týmů prostřednictvím pravidelné elektronické komunikace napříč zeměmi a kontinenty.

Důležitým trendem moderního vzdělávání je přímá účast zkušených odborníků v roli mentorů z komerční praxe, kteří přinášejí studentům reálnou zkušenost s přístupem i postupy, které jsou běžné v byznysu.

Česko-izraelský akcelerátor CIPA je výsledkem dlouhodobé spolupráce mezi Českou republikou a Izraelem v oblasti podpory inovací. „První ročník projektu CIPA je pouze začátkem česko-izraelské spolupráce v oblasti inovací. Jsem velmi potěšen, že se studenti zabývali oblastí Smart City. Tomuto oboru se totiž v Izraeli věnuje okolo 250 startupů, které vyvíjejí přední světové technologie. Věřím, že spolupráce v mezinárodních týmech na konkrétních inovativních řešeních bude přínosem pro všechny účastníky a u studentů podpoří jejich podnikatelského ducha," řekl k programu Daniel Meron, velvyslanec Státu Izrael v ČR.

Program CIPA byl proto od samého počátku koncipován jako práce mezinárodních česko-izraelských studentských týmů na řešení skutečných zadání od komerčních firem pod vedením seniorních externích mentorů. Mezi vybrané projekty, na které se studentské týmy v rámci osmitýdenního cyklu zaměřily, patřila elektromobilita a řízení životního cyklu elektrobaterií od společnosti ČEZ ESCO, provoz dedikované mobilní sítě pro kritické aplikace od společnosti Nordic Telecom, budoucnost dopravy v rámci autonomní mobility ve velkých městech společnosti Eletodo a systém

TE-VOGS ke zvýšení bezpečnosti pozemního provozu od Aero4TE.

Firmy vidí v této spolupráci skvělou příležitost podívat se na své problémy nezatíženýma očima a dát tak studentským týmům příležitost přinést nové pohledy na svou strategii. „Mladí lidé dokáží ještě snít, nejsou zatíženi negativní zkušeností, jsou odvážní a jejich tvořivost a fantazie není ničím omezená", říká Marat Saber, člen představenstva společnosti Eltodo.

Důležitou součástí celého procesu byl výběr studentů. Za ČVUT se projektu zúčastnilo osm studentů z různých ročníků i fakult, kteří se zavázali na programu pracovat mimo své běžné školní aktivity. Stejný počet studentů byl i na straně izraelského Technionu. Studenti dopředu neznali zadání firem a zůstalo pro ně dočasným tajemstvím i to, v jakých týmech budou pracovat. To se dozvěděli až druhý den úvodního týdenního programu v Praze, kde se studenti ČVUT setkali s dalšími osmi studenty z Technionu. Tento přístup je konkrétní ukázkou situace z praxe, kdy je nějaký úkol přidělen ad-hoc vytvořenému týmu s mezinárodní působností.

První týden programu studenti strávili společně na ČVUT v Praze. To jim dalo možnost osobně se seznámit nejen mezi sebou, ale i s mentory a se zástupci firem, pro které pracovali na projektu. Absolvovali celou řadu zajímavých workshopů, při nichž získali mnoho nových nástrojů pro řešení budoucích úkolů. Studenti měli možnost „osahat si" prostředí firem i při půldenní návštěvě a zjistit tak další detaily zadání. Na konci společného týdne vypracoval každý tým své prohlášení o spolupráci „Team Manifesto", ve kterém studenti zástupcům firem prezentovali své porozumění zadání a cesty, kterými se chtějí vydat při řešení svěřeného projektu. Nechybělo ani setkání v rezidenci ambasadora Státu Izrael v České republice Daniela Merona.

Poté následovala druhá, virtuální fáze programu, kdy týmy spolupracovaly na dálku, a to jak mezi sebou, tak i se zástupci firem. Toto bylo určitě nejnáročnějších sedm týdnů programu, kdy opadlo počáteční nadšení a dostavila se realita. Nutnost práce na zadáních, kombinovaná s plněním běžných povinností, jiné časové pásmo, nutnost respektovat množství různých svátků a kulturních zvyklostí obou zemí prověřily týmovou spolupráci a staly ze zřejmě největším přínosem pro studenty. Tato fáze probíhala pod dohledem zkušených mentorů, kteří práci v týmu usměrňovali a někdy i povzbuzovali, pokud si tým nebyl jistý, jak pokračovat dál. Některé týmy byly v užším kontaktu s firmami, jiné zvolily samostatnější postup, což samo o sobě bylo další cennou zkušeností.

Zhruba v polovině virtuální fáze týmy dokončily část věnovanou průzkumu (research) a po konzultaci s firmami se zaměřily na vybrané konkrétní oblasti svého projektu. Některé došly společně s firmami k závěru, že původní zadání je potřeba upřesnit, neboť dosavadní zjištění týmů vedla jiným směrem, než původně předpokládaly. Poslední týdny věnovali studenti finalizaci svých zjištění a doporučení, které prezentovali zástupcům firem. Velmi zajímavým výsledkem bylo, že by mohl existovat prostor i pro účelnou vzájemnou spolupráci firem, které challenge zadávaly. Propojením dedikované bezpečné sítě s prostředky autonomní dopravy nebo systému dohledu na letištích mohou vzniknout zajímavé synergie, které původně ani nebyly očekávány.

Závěrečnou etapou projektu byla osobní prezentace výsledků týmů zástupcům firem na univerzitě Technion v Haifě. Slavnostního ukončení pilotní fáze CIPA se zúčastnil i velvyslanec České republiky v Izraeli Martin Stropnický, jenž uvedl: „Mám za to, že inovativní síla Izraelců spočívá také v tom, že jdou i do nekonvenčních, a tedy i riskantních projektů. Nebojí se chyby, nejdou na jistotu. V tom bychom se měli nechat inspirovat. Kdo nic nezkusí, nic nezkazí. Jistě. Ale také nic nového nepřinese".

Účastníci prvního kola programu CIPA získali nejen řadu nových dovedností, ale také kontakty a přátelství, která mohou využít i v budoucnosti. „Ráda potkávám lidi z jiných kultur, byla to pro mě skvělá zkušenost naučit se něco nového. Elektromobilita je blízká mému srdci, je vždy dobré pracovat na projektu, který udělá svět o trochu zelenějším," uvedla ke své účasti v projektu Shani Adadi, studentka univerzity Technion v Haifě.

„Jsem otevřený novým nápadům, novým věcem a rád poznám nové kontakty, chtěl jsem se účastnit projektu s mezinárodní spoluprací, využít univerzitu na maximum. Jsem strojař, takže mě zajímá, jak se bude vyvíjet technika v budoucnu, na téma chytrých měst píšu i bakalářskou práci," dodává Jan Zaoral z ČVUT.

Delegace ČVUT vedená Ivo Stančekem (odbor pro řízení projektů a transfer technologií) současně ve spolupráci se zástupci Technionu zahájila přípravu dalšího pokračování projektu CIPA.

autorka: Monika Dobiášová
foto: Petr Neugebauer, ČVUT
Itzhar Vardi, Technion,
Jan Zaoral, student FS ČVUT

Závěrečnou etapou projektu byla prezentace výsledků zástupcům firem ČEZ ESCO, Nordic Telecom, Eltodo a Aero4TE 29. dubna na univerzitě Technion v Haifě.
Studenti navázali nové kontakty a přátelství, která mohou využít i v budoucnosti.

> Více na www.cip-accelerator.cvut.cz

BEZPEČNĚ
na každém kroku

Napadení počítače, jenž propojuje naše inteligentní domácí přístroje, ohrožení cesty letadlem kvůli výskytu dronů či dokonce útok teroristů, to vše nám bohužel hrozí v dnešním světě. Abychom se mohli cítit bezpečně, o to se starají i vědci z ČVUT. Představujeme alespoň několik projektů, zacílených na bezpečnostní a obranné technologie.

>>>

foto: Jiří Ryszawy

doc. RNDr. VOJTĚCH PETRÁČEK, CSc.
Vojtech.Petracek@cvut.cz

Přispíváme ke zlepšení bezpečnosti nás všech

O univerzitním výzkumu s rektorem ČVUT docentem Vojtěchem Petráčkem

Bezpečnost na každém kroku, to si jistě všichni přejeme, byť příroda či technika (teroristické útoky raději ani nezmiňujme) je někdy proti nám. Médii čím dál víc rezonují témata jako kyberbezpečnost, či spíše se mluví o kyberútocích, o ochraně lidí v dopravě i dalším veřejném prostoru… Vylepšovat bezpečí kolem nás se výrazně snaží i vědci na ČVUT. Které projekty v tomto směru vás v poslední době zaujaly?
S tím, jak postupuje moderní doba a jak nás stále víc obklopují moderní informační technologie a stále dokonalejší modely umělé inteligence, roste stále více zranitelnost naší společnosti. Závislost na tom, aby vše nové spolehlivě a bezpečně komunikovalo a spolupracovalo, bude stále větší. Proto je pro nás tak důležitá bezpečnost funkce našich technologií i to, abychom dokázali odvrátit jejich zneužití někým, kdo nemá s naší společností pozitivní záměry. Neméně důležité je to, abychom dokázali chránit naše myšlenky a výtvory před odcizením. V oblasti jaderné bezpečnosti, ochrany před zářením a dalších rizik při práci s atomovou energií můžeme přispět, protože ČVUT má rozvinuté jaderné technologie.
Ve všech uvedených směrech, které jsou pro ČVUT důležité, se rozvíjí řada projektů a výzkumů. Myslím, že jako příklad lze uvést rozvoj v oblasti umělé inteligence, informatiky a robotiky, kde se velká část nastíněných problémů snoubí a propojuje. Stejně tak se u nás rozvíjí i viditelnější bezpečnostní projekty, které jsou zaměřeny například na průzkum s pomocí dronů nebo na ochranu osob mobilními bariérami. Úspěšná je naše spolupráce na projektech autonomních prostředků pro armádu. Budujeme teď vlastně celý bezpečnostní sektor, který bude propojený a bude se vzájemně doplňovat. Jak je zřejmé, otázky bezpečnosti vyžadují komplexní řešení, a to bez interdisciplinárního přístupu nelze docílit.

Jménem ČVUT jste podepsal už několik partnerství s firmami působícími v tomto oboru, loni na podzim se škola stala členem Asociace obranného a bezpečnostního průmyslu. Která témata jsou podle vás klíčová? Daří se záměr, aby tato spolupráce napomáhala nejen pozvednutí technické a technologické úrovně obranného a bezpečnostního průmyslu v České republice, ale také vychovávání špičkových odborníků, kteří se již v době studia připravují na působení v této průmyslové oblasti?
V minulém roce jsme podepsali memoranda jak s AOBP, kde se ČVUT stala členem, tak se státními podniky VOP a VTÚ, rovněž tak s Armádou ČR. V mezinárodním kontextu jsme navázali partnerství například s BAE a právě nyní finalizujeme partnerské memorandum s General Dynamics Land Systems. Obecně bychom v těchto partnerstvích byli rádi výzkumným segmentem, který může přispět řešením pokročilých obranných problémů díky vysoké kvalitě našich výzkumníků. Je samozřejmé, že takto se zvyšuje i personální kapacita dostupná pro řešení obranně bezpečnostních témat v České republice. Považujeme to za jeden z příspěvků univerzity k tomu, aby náš stát mohl lépe fungovat.

Oblast obranných a bezpečnostních technologií je velmi citlivá, ne vše se může zveřejnit… Je takto „utajených" projektů na univerzitě hodně? Či jsou to spíše jednotlivé příklady, kde vědci ČVUT, specialisté civilního „sektoru", využívají svůj velký potenciál právě ve prospěch pokroku v oblasti bezpečnosti či armády?
Samozřejmě, že v této oblasti existují témata citlivá a témata v otevřené zóně. Univerzita je otevřeným celkem, na kterém se citlivé projekty a aktivity odehrávají pouze v malé míře. Mezi oblasti, které jsou citlivé, nikoli však utajené, patří například naše jaderná zařízení, která provozujeme podle striktních pravidel atomového zákona. Realizace citlivých projektů vyžaduje precizní řízení bezpečnosti, které právě zavádíme.

Buďme konkrétní. Jedním z partnerů ČVUT je i švédská zbrojařská firma BAE Systems, kde jste na konci listopadu se zástupci její české pobočky podepsali memorandum o spolupráci, které se bude týkat kybernetické ochrany bojových vozidel pěchoty. Prvním krokem spolupráce má být vypracování studie zranitelnosti elektronických systémů existujících vozidel. Jedná se o produkty firmy, která je potenciálním dodavatelem pásových bojových vozidel pro ministerstvo obrany. Můžeme takových spoluprací s firmami, či spíše s ministerstvem obrany, uvést víc?
Naše spolupráce s BAE se rozvíjí na širší bázi a není vázána na procesy spojené s akvizicí bojových vozidel. Pracujeme na rozvoji podobné platformy i s GDLS a jsme připraveni na společné projekty například s VOP či VTÚ. S ministerstvem obrany diskutujeme nové možnosti a formy spolupráce.

Mezi aktuální mezinárodní projekty, které se velmi úspěšně roz-

víjejí, patří i spolupráce s Izraelem. Průřezovým tématem prvního ročníku Česko-izraelského akcelerátoru CIPA je Smart city. Mezinárodní studentské týmy z ČVUT v Praze a izraelské univerzity Technion v Haifě pod vedením zkušených mentorů navrhují inovativní řešení konkrétních zadání průmyslových partnerů. Mezi témata patří elektromobilita, mobilní sítě či systém TE-VOGS ke zvýšení bezpečnosti pozemního provozu. Chystáte obdobnou spolupráci i s dalšími partnery?
Pokud jde o projekt CIPA, mám velikou radost z toho, jak probíhá jeho pilotní fáze. Myslím, že odezva ze všech zúčastněných stran je velmi pozitivní a již začínáme chystat další běh. Směrem k Izraeli vede i naše další nová spolupráce – tentokráte s externím partnerským akcelerátorem PATRIC. Ten by měl být fokusován právě do oblasti obranně bezpečnostních projektů či směrem k ochraně kritické infrastruktury. V tomto případě chceme vyzkoušet v Izraeli velmi osvědčenou formu spolupráce veřejného a soukromého sektoru. V podmínkách České republiky se jedná myslím o pionýrský pilotní pokus a my se těšíme na jeho výsledky. Našimi blízkými partnery jsou rovněž DEFSEC hub a DEFSEC lab, se kterými rozvíjíme například kontakt s NATO – například v rámci NATO innovation challenge, jejíž výsledky budou v rámci veletrhu IDET prezentovány.

Jedním z příkladů podpory nadějných inovací v této oblasti může být podpis licenční smlouvy ČVUT se startupem AKAENE Partners, s.r.o. Výsledkem výzkumné činnosti na projektu, jenž byl v úvodní fázi podpořen z fondů TAČR jako mezifakultní spolupráce Fakulty elektrotechnické a Fakulty dopravní, je systém pro správu znalostí o provozní bezpečnosti, založený na sběru a zpracování bezpečnostních dat. Jeho význam je zásadní při vyhodnocování a vytváření systémových opatření v rámci zvyšování bezpečnosti v letecké dopravě. Chystáte i další obdobné kroky, které podpoří výzkum v oboru?
Pro nás je velice důležité, aby vznikaly nové startup či spin-off firmy, které budou realizovat nápady našich akademiků a přispějí k rozvoji inovací v naší zemi. Proto budeme vznik takových firem podporovat. Je nutné zjednodušit procesy jejich vzniku, podporovat je a obecně vytvořit kolem školy klastr partnerských firem, které budou s univerzitou vzájemně prospěšně spolupracovat. Doufám, že počet takových firem bude rychle narůstat. Snad už končí doba, kdy byly spíše Popelkou.

V tématu tohoto vydání časopisu TecniCall představujeme velmi zajímavé a užitečné projekty napříč fakultami ČVUT, především z Fakulty elektrotechnické a Fakulty stavební, ať už se týká kyberbezpečnosti, detekce střelby, vývoje materiálů odolných vůči nárazu vozidel či účinkům střelných zbraní, využití dronů pro bezpečnost a mnoho dalších, které dokazují, že v tomto oboru jde pokrok výrazně dopředu a můžeme se do budoucna dívat na naši bezpečnost přece jen optimističtěji... Cítíte to taky tak?
Ano, myslím, že pokrok ve všech těchto oblastech jde kupředu a že přispíváme svým dílem ke zlepšení bezpečnosti nás všech v mnoha směrech. Jsem rád, že ČVUT využívá svou kapacitu ke zlepšení bezpečnosti a doufám, že se nám to bude dařit stále více. Myslím, že dosud nevyužitý potenciál je skutečně velký a těším se na jeho odkrytí a rozvoj.

Vladimíra Kučerová
foto: Jiří Ryszawy

Ing. SEBASTIÁN GARCÍA, Ph.D.
garciseb@fel.cvut.cz

prof. Dr. MICHAL PĚCHOUČEK, MSc.
pechoucek@fel.cvut.cz

Bezpečný internet věcí

Projekt Aposemat nás chrání před kyberútoky

Kolem sebe máme stále více zařízení tzv. internetu věcí, která nás v případě útoku vystavují nebezpečí. Proto se Katedra počítačů Fakulty elektrotechnické ČVUT spojila se společností Avast a vytvořila sdílenou laboratoř s názvem Aposemat. Jejím cílem je vyhodnocovat, jakým způsobem se útočníci a malware (škodlivý software) dostávají do našich zařízení a zneužívají je. Tento výzkumný projekt řídí Sebastián García, který na katedře vede výzkum kyberbezpečnosti v rámci Centra umělé inteligence. Aposemat přinese nové metody pro odhalení a následnou ochranu, aby bylo naše soužití s internetem věcí bezpečnější.

Termín internet věcí (z angl. internet of things, zkráceně IoT) označuje technologie, ve kterých se jednotlivá zařízení mohou připojit k ostatním a nejsou snadno modifikovatelné jako třeba počítač. Od chytrých telefonů, televizí, automobilů, kávovarů a bezpečnostních kamer až po routery a dokonce i letadla – stále více jsme obklopeni IoT zařízeními. Ta mohou naše životy zlepšit, jako v případě kardiostimulátorů, ochrany našich domovů, snazšího ovládání v průmyslu a dokonce i v případě umístění této technologie do sportovních míčů, kde pomáhají analyzovat zápas. IoT už nás nejspíš neopustí.

Protipólem těchto benefitů je fakt, že IoT zařízení obecně nejsou dobře zabezpečena a jsou implementována v masivním rozsahu, takže se otevírá nové pole působnosti pro útoky, monitorování, sledování a infikování. Zajistit jejich bezpečnost je náročné a velmi nákladné kvůli velkému množství způsobů, jakými mohou být napadena. Tato zařízení totiž fungují jako velmi komplexní počítače, které nabízejí spoustu funkcí. Jedním z hlavních omezení je navíc to, že náklady na zabezpečení jsou ve srovnání se samotnou výrobou příliš vysoké. Nejsou tudíž navržena s ohledem na bezpečnost, a tím pro společnost představují zásadní problém.

K vyřešení tohoto problému se Katedra počítačů Fakulty elektrotechnické, konkrétně její výzkumné Centrum umělé inteligence, spojila se společností Avast. Společná laboratoř s názvem Aposemat (https://www.stratosphereips.org/aposemat) si klade za cíl lépe porozumět bezpečnostním problémům IoT zařízení s důrazem na to, jakým způsobem jsou napadena z internetu a jak přesně jsou tlačena k útoku na ostatní zařízení v síti. Projekt má několik výzkumných linií a poskytuje cenné informace o skutečném stavu útoků na internet věcí v celé jeho šíři. Výzkum se zaměří na čtyři klíčové oblasti: infikování IoT zařízení malwarem; analýzu IoT honeypotů (pastí na útočníky) na internetu; analýzu externích útoků na skutečná IoT zařízení a vývoj nových metod rozpoznávání pomocí strojového učení.

Infikování malwarem

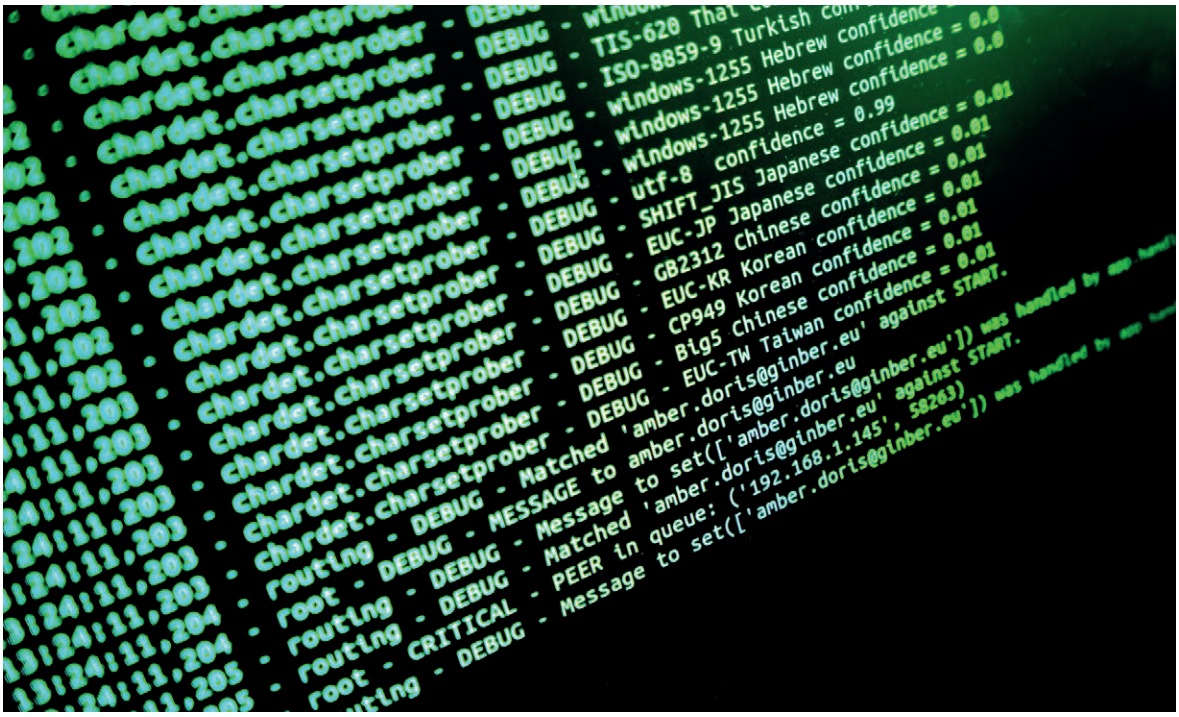
Abychom pochopili, jak útočníci zneužívají internet věcí, dostane projekt Aposemat skutečný malware do IoT zařízení. Prostřednictvím těchto aktivit je možné se od malwaru naučit, jak přesně nakazí jiná zařízení, jak komunikuje s útočníkem, který je ovládá, a jak využívá dostupné prostředky pro útoky jako například těžbu kryptoměn.

Malwarem infikujeme malé počítače (např. Raspberry Pi) uvnitř speciální laboratorní sítě s přístupem k internetu. Typ vybíráme podle aktuálních internetových hrozeb, abychom zachytili ty nejdůležitější útoky na internet věcí, které nás v současnosti ohrožují. Druhotným cílem je získání kvalitních dat o síťovém provozu, které pak soukromě sdílíme s týmem v Avastu.

Aposemat má za sebou už více než 400 útoků na IoT zařízení pomocí škodlivého softwaru, a to zejména malwaru Mirai, IRCBot a dalšího malwaru, jenž je využíván pro těžbu kryptoměn. Mirai se řadí k běžným a velmi známým typům, dosud infikoval už milion IoT zařízení. Funguje tak, že každá z nakažených jednotek dál útočí na ostatní, aby se hrozba šířila dál. Přístup získá Mirai technikou „brute force" na uhodnutí hesla (dle seznamu nejčastěji používaných) a vzdálenými útoky. V případě IRCBotu zas infikované zařízení kontaktuje vzdálený řídicí server IRC, který zadá příkaz k provedení konkrétních akcí. Nejběžnějším je tzv. DoS útok (Denial of Service, odepření služby), který oběť zahltí obrovským množstvím informací, takže systém přestane fungovat. Třetí typ malwaru využívá hardware zařízení jako například procesor nebo grafickou kartu ke generování kryptoměny.

Metodika je po celou dobu pečlivě sledována, abychom získali kvalitní data pro výzkumné účely. Každý experiment nabízí všechny informace, které bezpečnostní laboratoř potřebuje. Poté je síťový provoz analyzován pomocí automatických nástrojů, jako je např. Zeek, který vytváří logovací soubory vysvětlující provoz. Nakonec všechny soubory sdílíme s celým naším týmem Aposemat za účelem analýzy.

Projekt Aposemat si klade za cíl porozumět chování různých zařízení na internetu. Proto je nutné zaznamenávat a analyzovat internetovou komunikaci. V naší laboratoři pro tyto účely používáme různá zařízení, jako například počítače Raspberry Pi, různé síťové kamery i osobní asistentku Alexu od společnosti Amazon.



Pasti na internetu

Honeypot je systém speciálně navržený tak, aby byl napaden. Mezi jeho hlavní přínosy patří to, že nám pomáhá studovat chování útočníka. Jedná se tedy o past, návnadu (v doslovném překladu hrnec medu). Honeypot chrání firmy a organizace před kompromitací tak, že útočníkům zpřístupní falešná data a systémy místo těch skutečných.

Existují dva typy honeypotů, které lze implementovat – skutečná zařízení (fyzická IoT zařízení, která zůstávají otevřená pro útočníky) a softwarové simulace (programy, které vypadají jako IoT zařízení). V Aposematu využíváme oba typy.

Příkladem softwarové simulace je model čerpací stanice. Útoky na tyto provozy jsou detekovány ve chvíli, kdy jsou útočníci schopni ovládat elektronické funkce, jako je poplašný systém nebo odstávka. V naší laboratoři jsme navrhli falešný systém Guardian AST, který sleduje, jak se útočníci snaží ovládnout tento typ softwaru. Získané informace pak můžeme použít k návrhu softwaru, který tyto útoky blokuje.

Dalším dobrým příkladem je náš e-mailový server. Na tomto systému simulujeme server, který přijímá nevyžádanou poštu od skutečných útočníků. Tyto spamové e-maily v sobě skrývají velmi cenné informace o aktuálních trendech útoků. Pozorně sledujeme všechny tyto e-maily, a to včetně příloh. Později je analyzujeme a snažíme se pochopit, zda jsou nějakým způsobem nebezpečné. Na základě těchto poznatků můžeme vytvořit lepší spamové filtry a chránit koncového uživatele.

Ochrana domácího bezpečí

Důležitou část výzkumu tvoří pochopení toho, co IoT zařízení dělají, jaké informace posílají svým domácím serverům a jak řeší svou bezpečnost. Je pravděpodobné, že i pouhým připojením přístroje k domácí síti otevřete útočníkovi nový způsob, jak se k vám dostat a poslouchat, co děláte. Jen si představte, co by se mohlo stát, kdybyste měli dětskou chůvičku s monitorem a bezpečnostní vada v přístroji by komukoli umožnila, aby vaše dítě viděl a poslouchal. Tato představa je jistě vysoce znepokojující a potvrzuje, proč je náš výzkum tak důležitý.

IoT zařízení nejsou navržena s ohledem na bezpečnost, a tím pro společnost představují zásadní problém.

V laboratoři máme zapojené tři různé typy kamer se vzdáleným přístupem, hlasovou asistentku Alexa od společnosti Amazon, chytré žárovky Philips, síťová úložiště značky Synology a mnoho dalších. Tato zařízení byla nastavena s jednoduchými přístupovými údaji (přihlašovací jméno a heslo), aby je útočníci našli a jednoduše napadli. Jelikož jdou velmi snadno uhodnout, můžeme analyzovat, co útočníci v IoT zařízeních dělají, a následně se naučit, jak uživatele lépe chránit.

Analýza dat získaných z honeypotů je velmi důležitá pro pochopení chování malwaru. Ačkoliv lze pochopit útoky infikováním našich vlastních zařízení, tato metoda má jen velmi omezené využití, neboť hlavní příčinou všech útoků jsou lidé-útočníci. Ti jsou schopni změnit metody útoku stejně dynamicky, jako se jim my přizpůsobujeme, a tak neustále vyvíjí nový a výkonnější malware. Nejlepším způsobem obrany je proto zmatení útočníků, aby si mysleli, že jsou v bezpečí a odhalili nám tak své metody. To pak společnosti mohou využít k vytvoření úspěšného obranného mechanismu proti různým typům útoků a k identifikaci potenciálních nedokonalostí systému, které mohou být napraveny.

Důležitou část výzkumu tvoří pochopení toho, co IoT zařízení dělají, jaké informace posílají svým domácím serverům a jak řeší svou bezpečnost. Je pravděpodobné, že i pouhým připojením přístroje k domácí síti otevřete útočníkovi nový způsob, jak se k vám dostat a poslouchat, co děláte. Jen si představte, co by se mohlo stát, kdybyste měli dětskou chůvičku s monitorem a bezpečnostní vada v přístroji by komukoli umožnila, aby vaše dítě viděl a poslouchal. Tato představa je jistě vysoce znepokojující a potvrzuje, proč je náš výzkum tak důležitý.

Vývoj nových metod rozpoznávání pomocí strojového učení

Jedním z nejdůležitějších cílů projektu Aposemat je ochránit uživatele před budoucími útoky skrze učení se z rozpoznaných útoků a chování malwaru v síti. Tyto znalosti nám pomáhají vytvářet automatické detekční systémy založené na strojovém učení. Například pokud vlastníte bezpečnostní kameru, je možné se automaticky učit, jak se zařízení chová během každodenního provozu. Pokud v určitém okamžiku začne například navštěvovat spoustu webových stránek na internetu, mohlo by to znamenat, že byla kamera infikována nějakým škodlivým softwarem a nyní se účastní dalšího útoku.

Použití strojového učení nám umožňuje budovat modely chování malwarových útoků a matematické modely k odhalení anomálií. Tyto nástroje strojového učení budete nakonec moci využít i pro zabezpečení své sítě a hlavně pro vaši vlastní ochranu.

autoři: Sebastián García, Maria Jose Erquiaga, Yury Kasimov, Simona Musilová, Thomas O'Hara, Anna Shirokova
foto: Jiří Ryszawy

Projekt Aposemat vznikl v Centru umělé inteligence Katedry počítačů FEL ČVUT v Praze. Výzkum provádí mezinárodní tým spolupracující se studenty např. ze Slovenska, Ruska, USA nebo Argentiny.

Ing. MICHAL MÁRA
michal.mara@fsv.cvut.cz

doc. Ing. RADOSLAV SOVJÁK, Ph.D.
sovjak@fsv.cvut.cz

Odolné bariéry pro nebezpečnou dobu

V současné době se bezpečnostní situace napříč světem výrazně (místy jen mírně) zhoršuje. Evropa se v posledních deseti letech učí vzdorovat vzrůstajícím tendencím extrémistických jevů a teroristických útoků i dalším bezpečnostním hrozbám. Útoky nutí bezpečnostní složky v celé Evropě hledat a vyvíjet nové metody a systémy, které by jim pomohly na tyto hrozby reagovat. V Experimentálním centru Fakulty stavební ČVUT se již osm let zabýváme výzkumem a vývojem materiálů a konstrukcí se zvýšenou odolností vůči extrémním zatížením. Nejvíce se zaměřujeme na ochranu před účinky palných zbraní, výbuchu a sekundárních fragmentů. V neposlední řadě jsme vyvinuli i několik systémů schopných zpomalit nebo zcela zastavit osobní či nákladní vozidla, což je v poslední době jeden z často používaných druhů útoku.

V začátcích našeho bezpečnostního výzkumu jsme se zabývali vývojem kompozitního materiálu na bázi cementu, který by našel využití hlavně ve výstavbě nových konstrukcí a budov se strategickým významem nebo při jejich rekonstrukcích a úpravách. Primárně se jedná o objekty energetické infrastruktury, letiště, nádraží, vojenské a policejní objekty. Jinými slovy se jedná o stavby, kde se vyskytuje velké množství osob anebo jsou zcela zásadní pro fungování státu. Po několikaletém výzkumu jsme vyvinuli kompozitní materiál, který by se dal přirovnat k dobře známému betonu, nicméně jeho vlastnosti jsou mnohonásobně lepší. Vyznačuje se velkou schopností absorbovat energii – lomovou energií, jejíž hodnota se pohybuje mezi 20 až 30 KJ/m^2, což je přibližně 500krát více než hodnota lomové energie běžného betonu. Úzce s tím souvisí i vysoká tahová pevnost a smyková odolnost, díky které je tento materiál ideální pro stavební konstrukce namáhané extrémním zatížením. Pevnost tohoto kompozitu v tlaku se pohybuje kolem 150 MPa, zatímco pevnost běžného betonu, který je použit u většiny stojících konstrukcí, se pohybuje okolo 30 MPa.

Na sklonku roku 2014 a v návaznosti na tragické útoky v Paříži jsme poprvé představili myšlenku systému mobilních balistických bariér, který reaguje na nové bezpečnostní hrozby. Tento systém slouží především pro ochranu objektů, budov a staveb strategického významu. Lze jej také využít pro vybudování speciálních kontrolních bodů, zabezpečených vjezdů a v neposlední řadě i jako mobilní městské bariéry a zátarasy. Mobilní bariéry mohou být vyrobeny z námi vyvinutého kompozitního materiálu, který jim propůjčí potřebnou odolnost vůči průstřelu, výbuchu a nárazu vozidla. Celý systém je založen na velké mobilitě a univerzálnosti všech prvků, což umožňuje velice jednoduché a rychlé nasazení v reálných podmínkách bez potřeby těžké techniky, a to pouze za pomoci lidské síly. Jeden základní prvek, plná deska, má rozměry 1,5 × 0,4 m, tloušťku 4 cm a jeho hmotnost nepřesahuje 55 kg. Postupným sestavováním těchto základních prvků lze pak docílit různých konstrukcí s téměř neomezenými rozměry. Mezi základní typy patří stěna s půdorysem ve tvaru písmene „V", kterou lze sestavit bez nutnosti jakýchkoli základů. Další variantou je čtyřhran, který primárně slouží jako malé strážní stanoviště pro vizuální kontrolu hlídané oblasti či

Po několikaletém výzkumu jsme vyvinuli kompozitní materiál, který by se dal přirovnat k dobře známému betonu, nicméně jeho vlastnosti jsou mnohonásobně lepší. Vyznačuje se velkou lomovou energií, která se pohybuje mezi 20 až 30 KJ/m², což je přibližně 500krát více než hodnota lomové energie běžného betonu.

jako dočasné zázemí. Třetím základním modulem je šestihran, který plní účel velkého hlídkovacího stanoviště, hlídkové věže, dočasného skladu či cely předběžného zadržení. Kombinací těchto základních typů lze poskytnout adekvátní ochranu na velké množství hrozeb, se kterými se bezpečnostní složky dnes setkávají a na které musí bezprostředně reagovat.

Celý vývoj, jenž realizoval tým Experimentálního centra ve složení prof. Ing. Petr Konvalinka, CSc., FEng., Ing. Jindřich Fornůsek, Ph.D., Ing. Michal Mára, doc. Ing. Radoslav Sovják, Ph.D., a Ing. Jan Zatloukal, Ph.D., byl hned od počátku zaměřen na úzkou spolupráci s koncovými uživateli. I proto byla k vývoji a připomínkám přizvána Policie ČR, Armáda ČR a další státní složky. Cílem bylo vyvinout systém dle jejich potřeb, jenž by splňoval co nejvíce takticko-bezpečnostních podmínek a tím bylo umožněno jeho nasazení v co nejkratší době. Během výzkumu proběhlo mnoho testů a cvičení s Policií ČR i s Armádou ČR, ale například i dvě cvičení s německou spolkovou policií. Testovala se jak balistická odolnost na krátké ruční zbraně, tak i na puškové ráže včetně armádních zbraní běžně používaných například pro obrněné transportéry. Velkou odolnost projevily bariéry rovněž při výbuchu plastických trhavin a proti účinkům tlakové vlny, kdy například stěna o délce 6 m a výšce 1,8 m zůstala po výbuchu nálože ekvivalentu 3,6 kg TNT téměř bez porušení.

Důležitým momentem tohoto výzkumu byl vznik start-up MOB-Bars (z anglického „mobile barriers") na ČVUT, který získal licenci a dnes se zabývá dalším vývojem a prodejem těchto ochranných konstrukcí. Díky této spolupráci ČVUT v Praze a MOB-Bars bylo možné mobilní balistické bariéry, ale i další výsledky technické univerzity prezentovat nejen na domácí scéně, ale i ve světě. Výsledky našeho výzkumu dosud zaujaly bezpečnostní a státní složky mnoha zemí včetně Německa, Portugalska, Izraele nebo Jihoafrické republiky.

Velkou odolnost projevily bariéry rovněž při výbuchu plastických trhavin a proti účinkům tlakové vlny, kdy například stěna o délce 6 m a výšce 1,8 m zůstala po výbuchu nálože ekvivalentu 3,6 kg TNT téměř bez porušení.

Během mezinárodního veletrhu IDET 2019, který se již pravidelně koná na výstavišti v Brně, představíme spolupráci Experimentálního centra ČVUT s MOB-Bars a se státním podnikem VOP s.p. hned několik prvků mobilních bariér. Konkrétně se bude jednat o šestihran se dvěma podlažími, který lze využít jako součást kontrolního bodu, strážní věž nebo dočasné skladiště pro zabezpečení nebezpečného materiálu. Na stánku ČVUT bude vystavena nová a odolnější varianta mobilní bariéry v podobě liniového zátarasu s odolností vůči všem běžně používaným puškovým rážím. V neposlední řadě budou mobilní bariéry k vidění i v rámci venkovní expozice, kdy se MOB-Bars ve spolupráci s VOP s.p. bude podílet na prezentaci cvičného polygonu. Součástí expozice bude virtuální realita, se kterou mohou všichni nahlédnout do praktických situací a zjistit, jak lze mobilní bariéry využít k ochraně obyvatelstva nebo bezpečnostních složek.

autoři: Michal Mára
a Radoslav Sovják
foto: Experimentální centrum FSv
a MOB-Bars

Ing. MARTIN SASKA, Dr. rer. nat.
martin.saska@fel.cvut.cz

Eagle.one | Autonomní helikoptéra chytá nežádoucí drony

Je prakticky nemožné nevšimnout si extrémního nárůstu počtu bezpilotních helikoptér kolem nás v posledních několika letech. Nepochybně se bezpilotní helikoptéry, často označované jako drony, staly užitečným nástrojem v bezpočtu aplikací, nicméně existuje i stinná stránka zvýšení dostupnosti bezpilotních prostředků. Již v současné době se množí případy použití takzvaných paparazzi dronů pro sledování a nezákonné fotografování veřejně známých osobností a pro průmyslovou špionáž. Ještě mnohem nebezpečnější je možnost použití bezpilotních helikoptér pro teroristické útoky. Z nejvíce medializovaných příkladů lze zmínit nedávnou situaci kolem londýnského letiště Gatwick, které bylo po několik dní kompletně paralyzováno kvůli nelegálnímu výskytu dronu v jeho blízkosti. Dalším veřejně známým případem byl pokus o atentát helikoptérou na venezuelského prezidenta.

Zmíněná rizika ohrožení soukromí a bezpečnosti se týkají každého z nás a společnost na ně musí razantně reagovat. Existuje několik způsobů prevence výskytu neautorizovaných dronů v oblastech s omezením jejich výskytu. Nicméně, ať už jde o elektromagnetické pulzy, rušení komunikace a GPS signálu, nebo dokonce palné zbraně, všechny dosud dostupné techniky postrádají bezpečnost a většina z nich má omezené použití. Nelze si dost dobře představit možnost zrušení GPS signálu v oblasti letiště nebo střelbu z brokovnice po letících helikoptérách nad hlavami turistů na Pražském hradě. Vědci z ČVUT spolu s firmou Drone Defense Solutions s.r.o. přicházejí s řešením, které umožňuje bezpečný odchyt nežádoucího dronu do sítě vystřelené z paluby autonomní helikoptéry a následný transport dronu do dostatečné vzdálenosti od potencionálního cíle. Tento způsob je jediný možný, pokud vyžadujeme kompletní ochranu proti všem typům dronů a v aplikacích, které nedovolují riskovat neřízený pád odstraňované helikoptéry.

Systém Eagle.one vyvinutý pro tuto aplikaci sestává z detekčního zařízení Dedrone a plně autonomního vzdušného robotu vybaveného podvěsenou vystřelovací sítí. Vlastní mise helikoptéry Eagle.one začíná okamžikem detekce neautorizovaného dronu letícího v hlídané oblasti. Dedrone jej zaznamená pomocí instalovaných kamer pokrývajících příslušnou bezletovou zónu. Na základě rádiových signálů komunikace mezi dronem a pilotem a s pomocí algoritmů počítačového vidění zpracovávajících obrazy z kamer v reálném čase, dokáže systém rozlišit helikoptéry od ostatních objektů, například ptáků. Pokud cizí helikoptéra vlétne do zakázané oblasti, systém Dedrone ji detekuje a vydá povel ke startu helikoptéře Eagle.one se záchytnou sítí.

Prakticky okamžitě Eagle.one autonomně odstartuje a doletí do oblasti, kde je odhadována pozici cíle, která je průběžně aktualizovaná systémem Dedrone. Eagle následně použije své palubní kamery pro přesné zaměření cíle. Z tohoto měření určí jeho trajektorii, predikuje jeho pohyb a naplánuje vhodný útočný manévr. Když je cíl zaměřen a potvrzen, Eagle sám vystřelí síť, do které se cizí dron zachytí. Po zasažení dronu zůstává vystřelená síť připojena pomocí lanka k Eaglu, takže sestřelený dron nespadne na zem, kde by mohl způsobit újmu náhodně se vyskytujícím osobám a škody na majetku. Eagle zachycený cíl bezpečně odnese a přistane s ním na určeném místě. Tato možnost je extrémně důležitá v případech, kdy je podezření, že útočící dron může nést výbušninu a je nutné jej co možná nejrychleji dopravit do bezpečné vzdálenosti od hlídaného objektu nebo osoby.

Ačkoliv celá mise od detekce dronu po jeho bezpečnou eliminaci může být provedena v bezpečnostně kritických aplikací zcela autonomně bez jakékoliv intervence s operátorem, systém umožňuje i zapojení lidského faktoru, pokud je to vyžadováno. Povelu k vystřelení sítě, který helikoptéře dává palubní počítač na základě informace z palubních senzorů a výsledků rozhodování umělé inteligence Eaglu, může předcházet dálkové potvrzení od operátora systému. Ten také může misi v kterékoliv fázi přerušit a navést platformu Eagle na bezpečné přistání, pokud to operační situace vyžaduje.

Autonomní chování systému Eagle.one umožňuje použití metod umělé inteligence vyvíjených vědci Fakulty elektrotechnické ČVUT, které jsou na hranici stavu současného světového výzkumu autonomních bezpilotních prostředků. Eagle je vybaven dvěma palubními počítači. Jeden z nich je určen pouze pro přesnou detekci a lokalizaci cíle v reálném čase s využitím vysokorychlostních palubních kamer sledujících okolí. Systém využívá kombinaci 3D vidění a detekce pohybujícího se objektu konvolučními neuronovými sítěmi. Pro nasazení při snížené viditelnosti je možné platformu Eagle.one dovybavit termokamerou detekující motory nepřátelského dronu a leteckým radarem. Druhý počítač je určen pro reprezentaci výsledků počítačového vidění a pro optimální prediktivní řízení Eaglu tak, aby se vyskytoval v místě a čase optimálním pro výstřel sítě vzhledem k predikci pohybu cíle. Tato předpověď je realizována pomocí Extended Kalman filtru a datové fúze palubních senzorů. Dalším důležitým prvkem palubní inteligence je systém logického uvažování, který vyhodnotí situaci a dostupné senzorické údaje a rozhodne o konečném potvrzení povelu pro vypuštění odchytové sítě. Následně Eagle porovná aktuální stav chování svého letového systému s předem naučenými modely a sám rozhodne, zda byla mise úspěšná a zda je fyzicky schopen transportu cíle do určené oblasti. V případě, že je odchycený dron příliš těžký, je vystřelen záchranný padák a obě helikoptéry se bezpečně snesou na zem. Maximální přípustná váha objektu zavěšeného na laně pod Eaglem je přibližně 5 kg, což výrazně přesahuje parametry většiny běžně používaných dronů. Pokud Eagle vyhodnotil pokus jako neúspěšný a jiná platforma Eagle není připravena v záloze, je možné využít kamikaze postupu a nepřátelský dron zneškodnit přímým nárazem, který je okamžitě následován vystřelením padáku. Nicméně nabízené řešení přímo podporuje nasazení více spolupracujících platforem Eagle pro zvýšení spolehlivosti a rozsahu hlídané operační oblasti.

Eagle je dodáván ve dvou variantách. První je primárně určena pro ochranu bezpečnostně kritické infrastruktury, jako jsou letiště, elektrárny, vládní úřady, stadiony nebo věznice, a využívá staticky rozmístěný detekční systém Dedrone pro inicializaci první fáze mise. Ve druhé variantě je platforma Eagle kombinována s mobilní aplikací a je cílena pro ochranu soukromých sídel a dočasných akcí, jako jsou koncerty, mítinky politických stran, vystoupení veřejně aktivních osob a podobně. V této mobilní variantě systém Dedrone nahrazuje vyškolený personál, který povel ke vzletu Eagla a prvotní zaměření cíle realizuje s pomocí senzorů mobilního telefonu vybaveného aplikací Eagle.one. Právě tato verze Eagle.one bude oficiálně představena na bezpečnostním veletrhu IDET v Brně, kde se tento produkt utká v soutěži o ZLATÝ IDET 2019. Kromě stánku Eagle.one se návštěvníci veletrhu budou moci seznámit i s dalšími technologiemi autonomních bezpilotních prostředků na stánku ČVUT.

Na základě rádiových signálů komunikace mezi dronem a pilotem a s pomocí algoritmů počítačového vidění zpracovávajících obrazy z kamer v reálném čase, dokáže systém rozlišit helikoptéry od ostatních objektů, například ptáků. Pokud cizí helikoptéra vlétne do zakázané oblasti, systém Dedrone ji detekuje a vydá povel ke startu helikoptéře Eagle.one se záchytnou sítí.

autor: Martin Saska
foto: archiv skupiny Multirobotické systémy

prof. Ing. JAN HOLUB, Ph.D.
holubjan@fel.cvut.cz

Ing. JAKUB SVATOŠ, Ph.D.
jakub.svatos@fel.cvut.cz

Akustická detekce a lokalizace zdroje střelby

V současné době jsou techniky detekce akustických impulzních signálů (detekce výstřelů) čím dál více využívány nejen pro vojenské aplikace, ale také pro civilní účely. S přibývajícími útoky ve školách, kampusech, nákupních centrech nebo v nemocnicích vzniká požadavek automatického rozpoznání střelby i jinými metodami než kamerovými systémy ve spojení s operátorem. Lokalizace a klasifikace střelby pomocí akustické detekce je proto z hlediska bezpečnosti obyvatelstva čím dál tím důležitější.

Z historického pohledu jsou systémy pro akustický průzkum předmětem výzkumu od období první světové války. Průkopníkem akustických detekčních systémů byl italský PALS, určený pro rozpoznání činnosti nepřátelského dělostřelectva. Za první moderní nástroj se dá považovat systém Boomerang od společnosti BBN pro akustickou detekci palby vyvíjený v rámci programu DARPA TTO (Counter Sniper Program) ještě před rokem 1997, jenž byl schopen na základě času zachycení pulsní události (TOA – Time of Arrival) odhadnout polohu střelce a z parametrů pulsu zároveň odhadnout možnou ráži střelné zbraně.

Prototyp akustického detektoru, založeného na čtyřech mikrofonech umístěných v tetraedru připojených přes čtyřkanálový zesilovač k 16bitovému digitizéru. foto: Jakub Svatoš

V současné době existuje několik experimentálních, ale i profesionálních komerčních detekčních a lokalizačních akustických systémů. Mezi ty profesionální, určené zejména pro vojenské použití, patří např. QinetiQ, PILAR (Metravib FR), AVISA (Microflown) nebo Shot Spotter, který je využíván zejména pro ochranu VIP objektů (Bílý dům, univerzitní kampusy).

Na základě požadavků současného trhu vyvíjí Katedra měření Fakulty elektrotechnické ČVUT akustický detektor pro lokalizaci zdroje střelby použitelný jak pro speciální vojenské, tak i pro civilní použití např. v rámci koncepce Smart City. Navržený systém rozpoznává akustický ráz způsobný výstřelem pomocí několika samostatných jednotek, rozmístěných uvnitř oblasti, ve které probíhá detekce, a centrálního serveru. Každá samostatná jednotka obsahuje mikrofon, mikroprocesor ARM pro zpracování signálu a obsluhu celé jednotky, špičkový detektor pro rychlé analogové vyhodnocení signálu, zda mohlo k výstřelu dojít a má smysl spustit algoritmus pro detekci, modul pro časovou synchronizaci a přesné určení polohy jednotky (GPS) a modul pro datovou komunikaci (např. LoRa, GPRS) s centrálním serverem. Očekávaná reakční doba systému je v jednotkách sekund a střední přesnost lokalizace v otevřeném terénu lepší než tři procenta střední vzájemné vzdálenosti sousedních samostatných jednotek v mřížce rozložení detektorů. Součástí vyvíjeného systému je i software skládající se z firmware pro ARM mikroprocesor a z obslužného programu pro nadřazený server, kde probíhá výpočet lokalizace zdroje události a jejich pokročilá klasifikace. Lze tak odhadnout pravděpodobný typ a ráži zbraně.

Aby bylo možné výstřel detekovat a dále i správě klasifikovat, je třeba pochopit jeho fyzikální podstatu. Charakteristika výstřelu palné zbraně je popsána třemi jevy. Konvenční střelné zbraně používají zápalku a výbušnou náplň k vymetení projektilu z hlavně. Zvuk výbuchu se šíří ven z hlavně zbraně ve všech směrech, ale většina akustické energie je šířena ve směru vystřeleného projektilu. Tato rázová vlna a její zvuková energie šířící se z hlavně typicky trvá do tří milisekund a šíří se vzduchem rychlostí zvuku (tj. 343 m/s při 20° C). Pokud je náboj vystřelen nadzvukovou rychlostí, produkuje navíc vnější rázovou vlnu. Nadzvuková střela svým průchodem vzduchem vyvolává akustickou rázovou vlnu ve tvaru kužele šířícího se směrem ven od dráhy letu projektilu. Tato vlna se, stejně jako vlna způsobená expanzí spalin z hlavně, šíří vzduchem rychlostí zvuku. Další z akustických projevů výstřelu je způsoben mechanickou akcí samotné zbraně. To zahrnuje zvuk mechanismu spouště a kohoutu v případě vysunutí prázdné nábojnice a umístění nové automatickým nebo ručním nabíjecím systémem zbraně. Tyto mechanické projevy střelby jsou však mnohonásobně tišší, a proto je téměř nemožné je při detekci využít.

Na tvar akustického pulzu, který odpovídá výstřelu, má vliv mnoho faktorů. Nejvíce jej ovlivňuje samozřejmě kalibr hlavně palné zbraně a použitá munice. Závisí však také na několika dalších souborech faktorů, jako je teplota a vlhkost vzduchu, rychlost větru, ale i např. druh a chemické vlastnosti výbušné náplně střeliva. V neposlední řadě tvar pulzu ovlivňuje také prostředí. Jiný průběh bude při střelbě v urbanistické oblasti nebo v otevřeném prostoru, přírodě. Důležité je také znát význam odrazu, absorpce a difrakce zvukové vlny způsobené výstřelem. Měřený signál akustic-

Na základě požadavků současného trhu vyvíjí Katedra měření Fakulty elektrotechnické ČVUT akustický detektor pro lokalizaci zdroje střelby použitelný jak pro speciální vojenské, tak i pro civilní použití např. v rámci koncepce Smart City.

kého rázu tedy neobsahuje jen signaturu střelby, ale je ovlivněn též okolním prostředím.

Tým vědců z Katedry měření FEL ČVUT má s detekcí a lokalizací střelby již zkušenosti. V rámci spolupráce s brněnskou Univerzitou obrany vyvinul prototyp akustického detektoru, založený na čtyřech mikrofonech umístěných v tetraedru připojených přes čtyřkanálový zesilovač k 16bitovému digitizéru. Digitalizovaná data ze všech čtyř kanálů jsou následně zpracovávána pomocí detekčního algoritmu pracujícího na principu mediánového filtru a dělení signálu do energetických oken.

Hlavním uživatelem vyvíjeného akustického detektoru pro lokalizaci zdroje střelby by mohly být primárně bezpečnostní složky státu, jako je Policie ČR a další spadající pod Ministerstvo vnitra ČR. Použití střelné zbraně na veřejnosti je vždy riskantní záležitost, ať jsou důvody střelby jakékoli. Je proto nanejvýš vhodné, aby o takovém incidentu byly bezpečnostní složky a případně další orgány městské správy informovány okamžitě, pokud možno bez zpoždění způsobeného lidským faktorem. Dorazí-li hlídka na místo střelby neprodleně, přispívá to k pozitivnímu vnímání zasahujících bezpečnostních složek občany. Nedostatek informací o času a místě střelby ovšem může pro zasahující policisty představovat hrozbu. Proto je v případě aktivního střelce žádoucí co nejrychlejší zásah bezpečnostních sil s co nejpřesnějšími informacemi.

autoři: Jan Holub a Jakub Svatoš

Pracoviště pro testování srozumitelnosti nízkobitových hlasových kodérů (MELPe) s paralelní psychomotorickou úlohou: sluchátka pro vysoce věrnou reprodukci vzorku (Sennheisser HD600), zbraň upravená pro použití ve střeleckém simulátoru a bezdrátové hlasovací zařízení (jednobodový snímač EEG není na tomto snímku vyobrazen)
foto: Jan Holub

Testování srozumitelnosti řeči při paralelní zátěži

Výzkumný tým vedený prof. Janem Holubem na Katedře měření FEL ČVUT se zabývá měřením srozumitelnosti a kvality přeneseného hlasu a vývojem nových subjektivních i objektivních metod pro tato měření.

Na počátku výzkumu bylo experimentálně prokázané zjištění, že některé zavedené testovací metody neposkytují realistické výsledky, použitelné v denní praxi. Proto byly naším výzkumným týmem vyvinuty testovací postupy, které lépe postihují reálné situace použití telekomunikačních technologií. Vyvrcholením této snahy je nová mezinárodní norma TR 103 503: Procedures for Multimedia Transmission Quality Testing with Parallel Task, navržená pracovníky FEL ČVUT a schválená mezinárodní institucí European Telecommunication Standardization Institution (ETSI). Dalším krokem je harmonizace tohoto doporučení na úrovni NATO, neboli přidělení čísla STANAG.

Výzkum Katedry měření rozšiřuje poznání základních principů lidského vnímání, zejména při paralelní zátěži (např. při fyzické námaze, při sledování kritických dat na monitoru či při řízení vozidla). Zpřesněním testovacích metod a algoritmů lze lépe optimalizovat vývoj komunikačních zařízení (např. sluchátek či tzv. hands-free) či algoritmů (např. hlasových kodérů, řečových syntezátorů, algoritmů pro potlačení šumu či zvýraznění řeči) tak, aby co nejlépe vyhovovaly praktickým potřebám vojáků či záchranných složek IZS, ale také uživatelům mobilních telefonů.

Při subjektivních experimentech s paralelní zátěží byl identifikován překvapivý fenomén – pro určité typy zátěže se srozumitelnost určitých vzorků neočekávaně (statisticky významně) zvýšila. O vysvětlení toho jevu se tým pokouší ve spolupráci s FTVS UK s využitím elektroencefalografického monitorování (EEG) probandů během testování. Využívá se jak klasické 32elektrodové „čepice", tak zjednodušeného bezdrátového provedení snímače s jednou aktivní elektrodou.

Ve spolupráci s Katedrou počítačové grafiky a interakce FEL také probíhá výzkum v oblasti implementace výše uvedených testovacích metod pomocí virtuální reality. Ta totiž umožňuje např. efektivně zkombinovat proces testování srozumitelnosti a proces paralelní úlohy do jedné testovací platformy, čímž se zvýší opakovatelnost testu a sníží nároky na vybavení testovací laboratoře, týkající se např. parametrů prostorové akustiky.

autor: Jan Holub

doc. Ing. MARTIN LIDMILA, Ph.D.
martin.lidmila@fsv.cvut.cz

doc. Ing. PAVEL TESÁREK, Ph.D.
pavel.tesarek@fsv.cvut.cz

Ing. ONDŘEJ SEDLÁČEK
sedlacek@prefa.cz

DUŠAN DUFKA
dufka@strixchomutov.cz

BALBAR

Ochranná a balistická bariéra s vysokým stupněm mobility

Především pro potřeby jednotek požární ochrany České republiky a dalších složek Integrovaného záchranného systému zasahujících v budovách a průmyslových objektech, v městském prostředí nebo v otevřeném terénu byla vyvinuta ochranná a balistická bariéra s označením BALBAR. Skládá se z nosné nafukovací konstrukce, vodního vaku a dvou balisticky odolných kompozitních desek. Konstrukce bariéry byla navržena tak, aby umožňovala aplikaci v modulárním režimu.

Ochranná a balistická bariéra BALBAR byla vyvinuta v letech 2016 až 2019 v rámci řešení projektu MPO Trio č. FV10506 Výzkum a vývoj mobilní ochranné a balistické bariéry tvořené kompozitní deskou a vodní náplní. Řešitelským tým projektu pracoval ve složení: Fakulta stavební ČVUT v Praze, firma Strix Chomutov, a. s., se sídlem v Chomutově (dále jen STRIX Chomutov) a firma Prefa Kompozity, a. s., se sídlem v Brně (dále jen Prefa Kompozity).

Hlavním cílem projektu byl vývoj takové konstrukce bariéry, která umožní extrémně rychlé a technicky jednoduché nasazení především v městském prostředí, uvnitř budov a průmyslových areálů nebo v otevřeném terénu. Na začátku řešení projektu byly ve spolupráci s odborníky z oblasti požární ochrany, policie a armády vytipovány modelové krizové situace, pro které má být bariéra navržena. Z několika desítek možných scénářů krizových situací byly vybrány tyto čtyři základní:

– požár objektu s tlakovými lahvemi s obsahem libovolného stlačeného technického plynu,
– improvizovaný nástražný systém umístěný v otevřeném městském prostoru charakteru náměstí,
– střelec vybavený krátkou nebo dlouhou palnou zbraní,
– požár v chemickém průmyslovém areálu nebo ve velké průmyslové hale s nutností realizace dočasného krytu před účinky zášlehu plamene.

Podrobnou analýzou vytipovaných krizových situací byla navržena základní koncepce bariéry, která vychází z principu interakce kompozitní ochranné a balistické desky s vodní náplní. Kompozitní desky plní v systému bariéry BALBAR první stupeň ochrany, tzv. přímou nebo primární ochranu. Nepřímou sekundární ochranu osob tvoří vodní náplň. Její hlavní funkcí je pomocí své hmotnosti zvýšit stabilitu bariéry při působení energie výbuchu. Současně vodní náplň plní funkci pohlcování kinematické energie střepin a fragmentů střel, které pronikly přes primární ochranu. Ochranná a balistická bariéra BALBAR je tedy dvoustupňový ochranný systém skládající se ze dvou základních prvků – balisticky odolných desek a nosiče, který dále umožňuje integraci vaku pro vodní náplň.

Základním balisticky odolným prvkem jsou tedy kompozitní desky typu GFRP (Glass Fiber Reinforced Polymer). Desky byly vyvinuty firmou Prefa Kompozity a svými balistickými vlastnostmi chrání proti projektilům krátkých palných zbraní a střepinám ručních a dělostřeleckých granátů malých a středních ráží.

Kompozitní desky jsou výrobkem připraveným metodou lisování z materiálů na bázi polymerní pryskyřice a skelné výztuže ve formě tkaniny. Jejich stupeň balistické odolnosti závisí stejně jako u jiných materiálů na jejich tloušťce a plošné hmotnosti. V současnosti jsou testovány GFRP desky určené především pro ochranu před pistolovými projektily a střepinami z granátů malých a středních ráží.

Současně s vývojem balistických kompozitních desek probíhalo navrhování konstrukce bariéry, která má funkci nosiče desek. Technické požadavky na nosnou konstrukci byly omezeny maximální požadovanou hmotností do 30 kg (včetně prázdného integrovaného vodního vaku) a co nejmenšími skladebnými rozměry. Současně – s cílem minimalizace možného vzniku sekundárních úlomků a střepin při destrukci bariéry, které by mohly ohrozit zasahující hasiče – nesměla být konstrukce nosiče na bázi kovu ani kompozitních materiálů. Dalšími požadavky bylo snadné a rychlé postavení (aktivace) včetně kompatibility s prostředky běžně užívanými jednotkami HZS ČR, případně jednotkami HZS Armády České republiky.

Na základě výše uvedených požadavků byla nosná část bariéry (nosič desek) navržena jako gumotextilní nafukovací nízkotlaká konstrukce. Vývoj probíhal ve spolupráci s firmou Gumotex a.s. Břeclav, která je tradičním producentem výrobků a systémů v oblasti „rescue systems" včetně dodávek pro potřeby Hasičského záchranného sboru ČR. Základní geometrie bariéry kopíruje svým tvarem písmeno „A" o rozměrech 1,90 × 0,90 × 1,80 m. Strana nosné nafukovací konstrukce vystavená zásahu byla navržena pod úhlem 70° od horizontu, tento sklon zajišťuje lepší odolnost proti účinkům tlakové vlny a současně přispívá ke zvýšení celkové balistické odolnosti bariéry BALBAR. Obsah nafukovací části nosné konstrukce je cca 220 litrů vzduchu. Plnění nosné nafukovací konstrukce bylo navrženo tak, aby bylo možné použít stlačený vzduch obsažený v tlakové lahvi, která je součástí sestavy vzduchového izolačního přístroje, laicky řečeno dýchacího přístroje hasiče. Z láhve je možné nafouknout bariéru do jedné minuty. Po aktivaci nafuko-


[1]


[2]


[3]


[4]

[1] Testování sestavy bariér BALBAR při krizovém scénáři „sebevražedný atentátník" (figurína postavená zády k objektivu). Figuríny modelující členy bezpečnostních složek jsou označeny žlutými přilbami a stojí za sestavou bariér.
[2] Testování sestavy bariér při krizovém scénáři „velký zášleh plamenem", jehož zdrojem je výbuch směsi benzínu a nafty před experimentem.
[3] Záběr při výbuchu.
[4] Pohled na výbuchový děj s viditelnými fragmenty, které letí proti bariéře.

vací nosné konstrukce je možné osadit balisticky odolné kompozitní desky a zajistit je v „pracovní poloze" systémem suchých zipů.

Sekundárním stupeň balistické ochrany je tvořen vodním vakem, který je vyroben z materiálu na bázi polyesterové tkaniny (80 %), která je oboustranně nánosovaná polyvinylchloridem (20 %). Barva vodního vaku je červená (RAL 3000). Je opatřen koncovkou pro nasazení požární hadice typu „D" a je tedy kompatibilní s vybavením jednotek HZS. Maximální obsah vaku je cca 1,0 m^3. Konstrukce umožňuje i částečné naplnění, které je regulováno pomocí vypouštěcích ventilů umístěných v cca ½ a ještě mezi 3/4 a plnou, což je cca 7/8 výšky. Při částečném naplnění lze bariéry BALBAR nasadit i ve sklonitém terénu (do 10 stupňů).

Při řešení grantového projektu byly na některých vývojových variantách konstrukce bariéry BALBAR experimentálně ověřeny vybrané krizové scénáře, např. výbuch obranného granátu, improvizovaného výbušného systému či plastické trhaviny. V rámci výcviku jednotek HZS ČR při požárním cvičení s lahvemi s technickým plynem, které byly zahřívány až do samovolného výbuchu, byla poprvé nasazena sestava, kterou tvořily dva rozměrově stejné moduly bariéry. Při tomto experimentu roztržený plášť vybuchlé tlakové láhve zasáhl horní okraj sestavy bariéry, která jej odklonila a sama zůstala v zásadě nepoškozena. Zkouška byla celkově hodnocena jako úspěšná.

Mobilní ochranná a balistická bariéra je v současné době navržená ve dvou modulových variantách, které se od sebe výškově liší a od toho se odvíjí i způsob a taktika nasazení a použití celého systému BALBAR. V článku popsaný modul bariéry slouží k ochraně stojící postavy, která se připravuje na zásah. Výška je přibližně 1,9 m. Druhý modul bariéry je nižší (cca 1,4 m) a slouží jako pracovní část, za kterou je možné provádět zásah. K bariéře je navrženo i několik doplňků, které by měly prodloužit její životnost a zvýšit ochranu zasahujících jednotek IZS. Nyní probíhá patentová ochrana finálních variant mobilní a ochranné balistické bariéry.

autoři: Martin Lidmila, Pavel Tesárek, Ondřej Sedláček a Dušan Dufka
foto: archiv autorů


[5]

[6]


[7]


[8]


[9]

[5] Pro potřeby projektu byl upraven „balistický" přívěs, pomocí kterého je možné převážet až čtyři sestavy složených bariér BALBAR a až šestnáct balisticky odolných kompozitních desek včetně dalšího příslušenství.
[6] Mobilní ochranné a balistické bariéry při předvádění hlavním složkám IZS, v tomto případě hasičské jednotce HZS Petřiny (Praha). Prezentována byla sestava BALBAR tvořená malým a velkým modulem bariéry, která takto umožňuje ochranu základní dvojici zasahujících hasičů. [7] Testování balistické odolnosti kompozitních desek, ve stojanech jsou umístěny vzorky desek. Pro testování bylo použito několik krátkých a dlouhých palných zbraní včetně odstřelovací pušky. [8] Nácvik osazování balistických desek v pyrotechnickém obleku na nafouknutou (aktivovanou) nosnou konstrukci. Test dokazuje snadnou práci s celým systémem i při použití ochranných pomůcek při zásahu.
[9] Manipulace s aktivovanou balistickou bariérou pomocí policejního pyrotechnického robota na dálkové ovládání. Uvedeným způsobem by mohla být balistická bariéra dopravena k rizikovému místu, aby byla maximálně zajištěna ochrana osob při zásahu.

prof. Ing. FRANTIŠEK VEJRAŽKA, CSc.
vejrazka@fel.cvut.cz

Družicová navigace

Koncem března letošního roku proběhly médii poplašné zprávy o špatné funkci systému družicové navigace GPS. Dále jsme se mohli dočíst o testech přijímačů GNSS (GNSS je obecný termín pro existující a sobě podobné družicové systémy GPS, Galileo, GLONASS a BeiDou) na pražských tramvajových linkách.

Především šlo o tzv. „rollover", který nastal o půlnoci ze soboty 6. na neděli 7. dubna. Souvisí se způsobem měření času na družicích. Přesný čas je podstatný pro určování polohy. Dobou zpoždění signálu na dráze družice–uživatel měříme vzdálenost uživatele od družice a z ní určujeme polohu. Nároky na přesnost měření času jsou vysoké, uvědomme si, že jedna mikrosekunda odpovídá vzdálenosti 300 m a dnešní uživatelé GPS by chtěli znát polohu na centimetry.

Čas na palubě družice GPS je měřen tzv. Z-countem (čítačem), slovem o 29 bitech, které se zvětšuje o jedničku každé 1,5 s a je dostupné z přijímače uživatele. Na základě jeho bitů 3–19 se dozvíme čas v týdnu (TOW – Time of Week) a bity 20–29 informují o číslu týdne. Po dosažení hodnoty 403 199 a po příchodu další jedničky přejde TOW na hodnotu nula. Načtených 403 200 jeden a půl sekundových intervalů odpovídá času 604 800 sekund a tedy právě sedmi dnům uplynulého týdne. Přechod TOW na nulu nastane vždy o půlnoci ze soboty na neděli.

Podobně tomu je s horními (nejvýznamnějšími) 10 bity Z-countu. Ty jsou počítadlem týdnů, které uplynuly od 6. ledna 1980, kdy bylo počítadlo vynulováno. Největší číslo týdne (číslujeme od nuly) může být 2^{10}-1 = 1023. Pokud zvýšíme jeho hodnotu ještě o jednotku, přejde nikoli na hodnotu 1024, ale na nulu, čítač už dosáhl své nejvyšší kapacity a další (11.) dvojkový řád už není k dispozici. Tento jev označujeme jako přetečení čítače týdnů, anglicky rollover. To znamená, že datum uvnitř přijímače se, pokud neuděláme další opatření, vrátí na 6. ledna 1980. Opatření spočívá v tom, že si zapamatujeme, že už nastal 1024. týden a při určování data k horním bitům Z-countu připočteme 1024. Neošetřený rollover neznamená jen potíže s identifikací okamžiku (např. banky využívají GPS čas k rozhodnutí o včasnosti plateb ap.), ale např. i nesprávnou činnost některých modelů šíření signálů a dalších funkcí, správný chod přijímače je často zcela narušen.

Poprvé došlo k rollover o půlnoci 21. srpna 1999 a letošní událost nastala po naplnění dalších 1024 týdnů o půlnoci z 6. na 7. dubna. Rollover je u většiny přijímačů na trhu ošetřen, ale některé starší přístroje měly obtíže, např. pulty centrální ochrany hlídající automobily vyhlašovaly poplachy, nefungovaly záznamníky jízd, dodávaly nesmyslná data apod. A to přesto, že provozovatel GPS vydal varování a že ve standardu GPS, tzv. ICD dokumentu, je na rollover pamatováno výraznou výstrahou.

Několik provozovatelů přijímačů GPS se obrátilo na katedru radioelektroniky FEL s žádostí o radu a pomoc. Protože disponujeme generátorem signálu GPS, mohli jsme předem nasimulovat signály, které měly družice vysílat 6. dubna a vyzkoušet přijímače zájemců. Byli jsme překvapeni rozsahem neošetřených zařízení a bylo nám potěšením, že jsme mohli zabránit mnoha nepříjemnostem. Třetí perioda přetečení čítače týdnů nastane 20. 11. 2038. Snad si naši následníci včas vzpomenou na potřebná opatření.

Použití GNSS systémů v systému dopravy města je samozřejmě lákavé, protože se zdá být snazší, než např. umisťování RFID čipů do kolejí. Jenže družicové systémy pracují bez nejmenších potíží, pokud přijímač vidí celou oblohu a pokud v okolí nejsou budovy a předměty, které by odrážely signály družic. Signál, který doputuje na anténu přijímače odrazem, urazil delší cestu, neodpovídá vzdálenosti družice–uživatel a údaj o poloze může být změřen chybně. Rovněž zastínění oblohy okolními domy podstatně zhorší přesnost měření, nemluvě o podjezdech, příp. tunelech, kde GNSS přijímač na nějaký čas vypadne zcela.

Při použití družicové navigace v městské zástavbě může být pomocí příjem několika systémů a vhodné sloučení jejich informace, protože využití většího počtu družic na obloze vede k lepším výsledkům měření. Dále lze družicové přijímače podporovat korekčními signály z tzv. referenčních stanic, čímž se podstatně zlepší přesnost, ale stále vadí výpadky a odrazy. Ty lze překlenout podporou signály nezávislého zdroje, např. inerciálního čidla, které je schopné dodávat parametry pohybu přijímače. Pokud známe velikost a směr rychlosti pohybu, můžeme překonat krátký výpadek signálu z družic. To samozřejmě vyžaduje provést tzv. fúzi dat z družic a z čidla ne zcela triviálním algoritmem. Ten můžeme vybavit i informací o statistice signálů, tj. např. umožnit mu považovat velké odchylky družicových měření za málo pravděpodobné, dát jim malou váhu a dát přednost např. signálům inerciálního čidla. Takováto podpora nejen že umožní určovat polohu vozidla např. při průjezdu tunelem, pod vegetací či v terénním zářezu, ale může vést i ke zpřesnění nerušených měření.

Všechno něco stojí. A tak samozřejmě multikonstelační GNSS přijímač, který přijímá signály několika systémů, bude vidět hodně družic a bude mít vyšší přesnost, ale bude řádově dražší než přijímač pro turistu nebo hráče geocachingu. V současné době se zabýváme studií vybavení přijímačů GNSS, aby vyhověly požadavkům provozovatelů dopravních služeb v městském prostředí.

autor: František Vejražka
ilustrační foto: FEL

Ing. JAN CHUDOBA
Jan.Chudoba@cvut.cz

Autonomní navigace vozidla

Taros (Taktický robotický systém) je vozidlo bez řidiče vyvíjené společností VOP CZ, s. p., určené pro širokou škálu použití zahrnující průzkum, dohled nad oblastí či transport materiálu nebo osob. Výzkumná skupina Inteligentní mobilní robotiky v rámci Českého institutu informatiky, robotiky a kybernetiky ČVUT pro něj implementuje funkce pro autonomní navigaci.

Vozidlo Taros je možné používat v režimu dálkového ovládání na základě rádiového přenosu obrazu z palubní kamery. Pro mnoho aplikací je však vyžadována určitá míra autonomie vozidla, aby bylo schopné se pohybovat a plnit požadované úkoly i bez přímého řízení v případech, kdy operátor nemá dostatečný přehled o situaci v okolí vozidla nebo ztratí spojení s vozidlem úplně. Proto byly osloveny týmy robotických laboratoří na ČVUT v Praze a VUT v Brně, aby spolupracovaly na vývoji funkcí autonomního řízení vozidla.

Zatímco tým Laboratoře teleprezence a robotiky VUT se věnoval především navigačním metodám využívajícím přesný satelitní navigační systém RTK GNSS, pracovníci skupiny Inteligentní mobilní robotiky ČVUT (IMR) se zaměřili na metody navigace využívající palubní senzory snímající okolí robotu. Tyto senzory zahrnují soustavu rozmítaných laserových dálkoměrů pokrývajících prostor před vozidlem tak, aby byly bezpečně detekovány různé překážky v cestě robotu.

Aktuální konfigurace vozidla obsahuje tři dálkoměry rozmítané v jedné rovině. Jeden senzor je instalován v horizontální orientaci ve středu čelní masky vozidla a umožňuje detekovat překážky ve výšce jeho instalace do vzdálenosti 50–70 m. Pro detekci nižších překážek jsou instalovány dva další senzory stejného typu na rozích vozidla pod sklonem blízkém 45 stupňům. Tyto skloněné senzory při jízdě vozidla poskytují data pro vytváření 3D reliéfu terénu a následnou detekci objektů, které by představovaly překážku v bezpečné jízdě. Nad systémem detekce překážek může pracovat modul pro předcházení kolizí, který koriguje trajektorii robotu tak, aby se robot překážkám vyhnul nebo zastavil pohyb v případě, že není možné se překážce vyhnout jednoduchým manévrem.

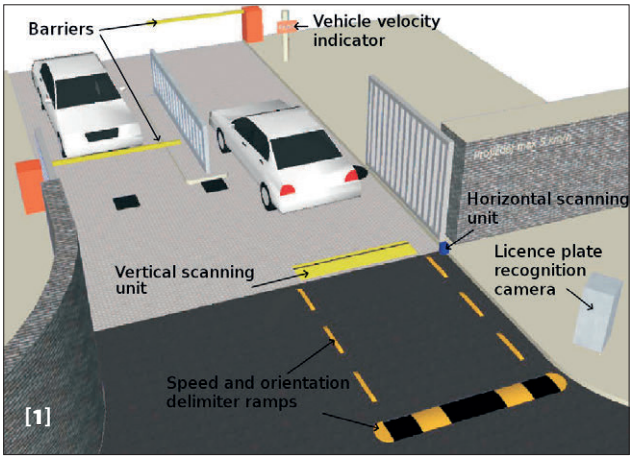
Pro plnění úkolů bez trvalého ovládání operátorem je zapotřebí autonomního navigačního modulu, řídícího vozidlo na základě stanoveného cíle a dostupných senzorických měření. Skupina IMR implementovala lokalizační systém vozidla využívající 3D laserový dálkoměr, umožňující určit přesnou polohu vozidla ve známém a předem zmapovaném prostředí. Zmíněný 3D dálkoměr poskytuje desetkrát za sekundu měření obsahující asi půl miliónu bodů věrně reprezentujících objekty v okolí robotu. Lokalizace je realizována metodami registrace bodů (např. „iterative closest points") na předem vytvořenou mapu. V kombinaci s metodou plánování trajektorie umožňuje samostatnou navigaci vozidla např. v průmyslovém areálu, kde by vozidlo operovalo.

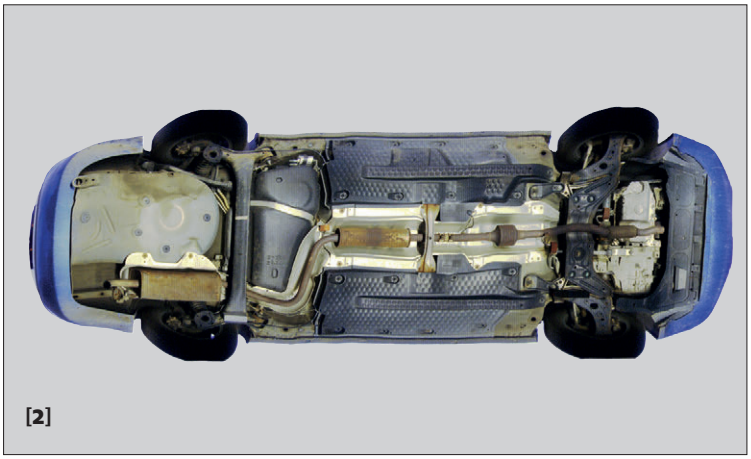
Dalším směrem výzkumu jsou navigační metody typu „record and replay" určené k projíždění trajektorií dříve naučených při ovládání operátorem. Využití těchto metod je např. pro opakované průjezdy hlídaného prostoru nebo pro automatický návrat vozidla do výchozí pozice. Byly testovány metody vyvíjené několika robotickými skupinami na ČVUT, využívající obraz z kamery na vozidle, založené na detekci stabilních obrazových příznaků, které jsou rozpoznatelné a identifikovatelné při opakovaných průjezdech stejným místem. Poloha těchto příznaků ovlivňuje řízení zatáčení po požadované trajektorii. Metoda umožňuje i přenos naučené mapy mezi jednotlivými vozidly, což bylo testováno v experimentu, kdy byla učící fáze provedena s menším průzkumným robotem Orpheus a mapa byla následně bezdrátově přenesena na vozidlo Taros, které poté bylo schopno samostatně dojet až na místo určené druhým robotem.

Vozidlo Taros s 3D laserovým dálkoměrem Velodyne.

autor: Jan Chudoba
foto: archiv pracoviště

Ing. KAREL KOŠNAR, Ph.D.
Karel.Kosnar@cvut.cz





Bezpečnostní kontrola podvozků aut

[1] Systém Kerberos – schématické zobrazení (zdroj: VOP CZ, s. p.)
[2] Rekonstrukce obrazu podvozku systémem Kerberos 2D

Skupina Inteligentní a mobilní robotiky (IMR) Českého institutu informatiky, robotiky a kybernetiky ČVUT v Praze dlouhodobě spolupracuje s firmou VOP CZ, s. p. na vývoji systémů pro rutinní bezpečnostní kontrolu podvozků vozidel při vjezdu do chráněných objektů.

Vyvíjené a nabízené skenery jsou navrhované jako přejezdové, kdy podvozek je snímán v průběhu přejezdu vozidla přes skener. Zároveň se snaží o co nejrychlejší zpracování dat tak, aby bylo možné co nejplynuleji odbavovat projíždějící vozidla.

První verze skeneru Kerberos 3D využívala sestavu tří laserových dálkoměrů pro rekonstrukci 3D reliéfu podvozku vozidla. V součinnosti s externím systémem pro evidenci vjezdu vozidel, který rozpoznává registrační značky vozidel, byl model podvozku přiřazen ke konkrétnímu vozidlu. Následně, při opakovaném průjezdu vozidla přes skener, je uložený model podvozku porovnán s aktuálním a jsou vyhodnoceny rozdíly ve tvaru a odrazivosti. Na základě těchto rozdílů jsou ohodnoceny významnosti odlišností jednotlivých oblastí podvozku. Získaný 3D model, doplněný o reflektivitu povrchu a ohodnocení významnosti změny ve formě barevné škály, je pak prezentován obsluze k finálnímu vyhodnocení hrozby.

Druhá verze skeneru poskytuje pouze 2D barevný snímek podvozku. Jedná se o náhradu vizuální kontroly podvozku s použitím ručního zrcadla. Kerberos 2D pracuje s jedinou kamerou a je možné ho provozovat dokonce i v mobilní verzi. Tu je možné nainstalovat během několika minut a kontrolovat projíždějící vozidla prakticky na libovolném místě. Výsledný obraz má rozlišení vyšší než 1 pixel/mm a umožňuje tak obsluze vidět detaily, jako jsou šrouby uchycující krycí plechy či nápisy na dílech podvozku.

Je také možné provozovat obě verze současně v jedné zástavbě. To umožňuje využívat automatické porovnání 3D modelu a současně mít podrobnou vizuální kontrolu ve formě detailního barevného obrazu podvozku.

V současnosti je v řešení projekt Ministerstva vnitra č. VI2VS/461 Kassandra – mnohokamerový bezpečnostní skener podvozků vozidel. Ten jde v integraci ještě dále a kombinuje vlastnosti všech verzí systému Kerberos (2D, 3D a mobilní). Zejména se jedná o malou hloubku zástavby skeneru a o tvorbu 3D modelu podvozku současně s 2D barevným obrazem, resp. tvorbu 3D modelu s podrobnou texturou.

Pro dosažení požadovaných vlastností jsou laserové dálkoměry nahrazeny rychloběžnými kamerami s širokým zorným polem a globální závěrkou. Pro rekonstrukci 3D modelu jsou využívány metody kombinující výpočet husté disparitní mapy a vizuální odometrie. To umožní složit obarvený 3D model celého podvozku ze sekvence snímků.

Systém zrcadel umožňuje snížit hloubku zástavby při zachování dostatečné optické vzdálenosti od podvozku. Zároveň je integrováno i osvětlení podvozku pro dosažení krátké expozice. To nabízí dosažení vyšších rychlostí přejezdu skeneru při zachování dostatečné ostrosti obrazu.

Výzkum se dále zaměřuje na zvýšení robustnosti rozpoznání změn a ohodnocování jejich významnosti či nebezpečnosti využitím technik strojového učení. Dalším směrem je snížení kognitivní zátěže operátora tak, aby mohl jeden pracovník obsluhovat více kontrolních stanovišť bez zvýšeného úsilí a stresu.

autor: Karel Košnar

> Více na http://imr.ciirc.cvut.cz

prof. Ing. FRANTIŠEK WALD, CSc.
frantisek.wald@fsv.cvut.cz

Ing. KAMILA CÁBOVÁ, Ph.D.
kamila.cabova@fsv.cvut.cz

Ing. FILIP ZEMAN
filip.zeman@fsv.cvut.cz

Virtuální požární zkoušky

Pro zkoušení požární odolnosti konstrukcí byl na Katedře ocelových a dřevěných konstrukcí Fakulty stavební ČVUT připraven virtuální model vodorovné pece. Je založen na analýze dynamiky plynů v otevřeném nástroji Fire Dynamics Simulator. Přesnost modelu byla potvrzena několika požárními zkouškami na vodorovné peci v požární laboratoři PAVUS, a.s. Výsledky teplot plynu uvnitř pece vykazují dobrou shodu s experimenty, a to i v případě přítomnosti hořícího zkušebního vzorku. Využití numerického modelování na základě analýzy dynamiky plynů se ukázalo jako vhodná metoda pro zkoušky požární odolnosti.

Model byl připraven a rozvinut při práci na grantech VirFur GAČR 16-18448S a 19-22435S, které jsou zaměřeny na spojování modelů dynamické analýzy plynů, přestupu tepla a mechanického chování konstrukcí. Pro validaci bylo připraveno šest zkoušek v požární zkušebně PAVUS, a.s. ve Veselí nad Lužnicí v nově zaváděné horizontální peci 3,0 m x 4,0 m s výškou 2,16 m. Stropní pec je ohřívána osmi plynovými hořáky na zemní plyn, vždy čtyřmi na obou delších stranách.

Pec se nejčastěji ohřívá podle nominální normové teplotní křivky. Řídí se průměrnou teplotou deskových snímačů umístěných 0,1 m pod stropem. Tolerance teploty oproti požadavku se v prvních 30 minutách zkoušky požaduje ±100 °C a přetlak ± 5 Pa do 5 minut a ± 3 Pa od 10 minut testu. Tlak se reguluje nucenou ventilací na dně pece. V modelu je přidána ocelová konstrukce nad ventilačním otvorem jako ve skutečné peci. Konstrukce chrání ventilační otvor před padajícími částmi zkušebních vzorků a usměrňuje proudění odtahovaného plynu ke kraji pece.

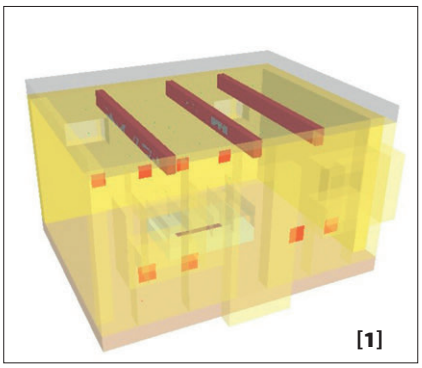
K ověření přesnosti modelu byla provedena série tří experimentů. Prvním byla zkouška v prázdné peci. Experiment sloužil pro získání a následné nastavení hodnot výkonů hořáků pro numerický model. Následovala zkouška s ocelovým nosníkem IPE 400. Zkušební vzorek ovlivnil naměřené průběhy teplot svou polohou a tepelnou jímavostí. Třetím experimentem byla zkouška s třemi lepenými dřevěnými nosníky průřezu 100 mm x 240 mm. Nosníky byly uloženy kolmo na delší strany pece a byly vybaveny ocelovými styčníkovými a výztužnými prvky.

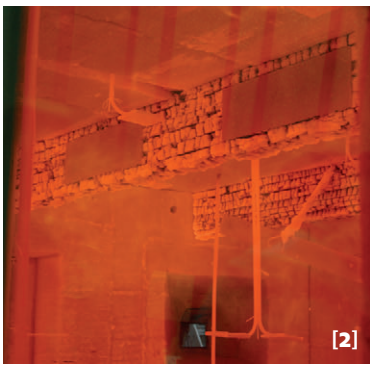
Pro vytvoření numerického modelu byla zvolena verze 6.5.4. programu FDS. Jednotlivé konstrukce v modelu pece jsou vytvořeny z materiálů s vlastnostmi změřenými v peci. Kvalita modelu je validována na výsledcích změřené teploty a přetlaku plynu. Při zkoušce dřevěného nosníku bylo ověřeno, že teplota je v počáteční fázi simulace výrazně vyšší než během samotného experimentu v praxi. Po uplynutí pěti minut dochází ke srovnání obou křivek a model má stejný průběh teploty jako při experimentu. Model přetlaku v peci ukazuje, že vypočítané hodnoty kopírují lokální výkyvy přetlaku uvnitř pece se zpožděním a bez dostatečného tlumení. Na vylepšení modelu hoření dřeva a tlumení přetlaku se dále pracuje.

Virtuální pec prokazuje dobré výsledky především v pokročilé době simulace, kde se teploty plynu téměř shodují s experimenty. Práce s kolegy z Katedry mechaniky Fakulty stavební při propojení dynamické analýzy plynů s tepelnou a mechanickou analýzou metodou konečných prvků umožňuje využít virtuální pec k ověření požární odolnosti konstrukcí. Sdružený model dokáže předpovědět chování, které se na peci již jen ověří. K širšímu využití je potřeba model dále zdokonalovat. Další výzkum je zaměřen na modelování řízení ventilace a hořáku, popis deskových snímačů teploty, hoření zkušebních vzorků v peci a jednostěnného a oboustranného propojení s modely konečnými prvky.

autoři: Kamila Cábová, Filip Zeman, František Wald
ilustrace: archiv pracoviště

[1] Vitruální pec s dřevěnými nosníky
[2] Dřevěný nosník při zkoušce
[3] Stropní pec v požární zkušebně PAVUS, a.s.


[1]


[2]

[3]

Ing. PAVLA BRADÁČOVÁ
bradapa1@fit.cvut.cz

prof. Ing. RÓBERT LÓRENCZ, CSc.
robert.lorencz@fit.cvut.cz

Boj s kybernetickou hrozbou

Výzkum a výuka na Katedře informační bezpečnosti FIT

Kybernetická hrozba. Ještě před pár lety by to mnohým znělo jako termín ze sci-fi filmu. Od té doby jsme již ale pochopili, že scénář k filmu o daleké budoucnosti, kde jsme sami sobě nebezpeční, už je realitou. Někteří z nás se rozhodli postavit této skutečnosti čelem.

V současnosti si lze jen těžko představit práci bez přístupu k internetu. Všichni až moc dobře víme, jaká rizika s sebou přináší moderní pracovní prostředí neodmyslitelně spojené se šířením informací. Citlivé údaje směle i nevědomky sdílíme v jednom obrovském virtuálním světě s křehkými obrannými zdmi. Jak jedinci, tak firmy pracují s daty a citlivými informacemi, což je ve světě hackerských útoků chůze po tenkém ledě.

Kybernetická hrozba má svého hodného sourozence, jímž je kybernetická bezpečnost. Jeden ovlivňuje toho druhého, neustále spolu bojují a snaží se vyhrát. Kybernetická bezpečnost identifikuje a řeší hrozby v kyberprostoru posilováním informační a komunikační infrastruktury. Jejím cílem je ochrana informací a majetku před krádeží, korupcí nebo přírodní katastrofou.

Z toho vyplývá, že informace budou muset být zabezpečeny nejen technicky, ale také dodržováním pracovních postupů a bezpečnostních předpisů. Kybernetické hrozby se stávají sofistikovanějšími. Hackerské útoky jsou důmyslnější a rafinovanější. Logicky tedy musí nastat zesílení zabezpečení dat, která používáme. Jak na to? Musíme být chytřejší a na tyto útoky se připravit, ještě než nastanou. Musíme umět odhadnout jejich životní dráhu a tu korigovat.

Je třeba hledat a vychovávat odborníky na kybernetickou bezpečnost. A začít již u studentů. V roce 2018 Fakulta informačních technologií ČVUT v Praze proto jako první v České republice založila specializované pracoviště pro studium bezpečnosti IT technologií – Katedru informační bezpečnosti. Její vznik je výsledkem několikaletého úsilí v realizaci výzkumu a výuky v oblasti IT bezpečnosti. Katedra nabízí rychlý a dynamický rozvoj aktuálně žádaných bezpečnostních studijních programů a zaměření.

Vedoucím katedry je prof. Ing. Róbert Lórencz, CSc., jeden z nejlepších odborníků na IT bezpečnost a zároveň soudní znalec v této oblasti. „Snažíme se vychovávat absolventy, kteří budou odborníky v oboru informační bezpečnosti a splní náročné požadavky praxe. Katedra informační bezpečnosti rozvíjí oblasti výzkumu, které nabývají v současnosti na důležitosti, jako jsou například detekce hardwarových trojských koňů, bezpečné generování kryptografických klíčů nebo sofistikované analýzy založené na postranních kanálech," říká prof. Lórencz. Studenti se v rámci předmětů vyučovaných katedrou seznamují s kryptologickými principy nebo se způsoby detekce útoků v počítačových sítích.

Vědečtí pracovníci i studenti mají jedinečnou možnost zkoumat principy kybernetiky ve třech laboratořích, které katedra zaštiťuje. Jedná se o Laboratoř etického hackování, Laboratoř RFID a Laboratoř forenzní analýzy. Právě v nejnovější z nich, zaměřené na etické hackování, si studenti mohou vyzkoušet, jak napadnout různé systémy. Fakulta založila toto pracoviště ve spolupráci se společností NN Group, nabízí tak studentům skvělou příležitost vyzkoušet si teoreticky nabyté zkušenosti v praxi. Ze studentů se stanou odborníci na kybernetickou bezpečnost, a to díky praktické výuce v rámci bakalářského oboru Bezpečnost a informační technologie a magisterského oboru Počítačová bezpečnost, které katedra garantuje.

Dnešní společnost potřebuje bezpečnostní analytiky, kteří dokáží zajistit spolehlivý provoz informačních systémů a umí efektivně řešit hackerské útoky. Fakulta informačních technologií ČVUT vychovává odborníky, kteří dokáží řešit problémy bezpečnosti informačních systémů. Díky jejich znalostem bude mnohem jednodušší bojovat s takovým nebezpečím, jakým je kybernetická hrozba.

autorka: Pavla Bradáčová
foto: Jiří Ryszawy

„Snažíme se vychovávat absolventy, kteří budou odborníky v oboru informační bezpečnosti a splní náročné požadavky praxe. Katedra informační bezpečnosti rozvíjí oblasti výzkumu, které nabývají v současnosti na důležitosti, jako jsou například detekce hardwarových trojských koňů, bezpečné generování kryptografických klíčů nebo sofistikované analýzy založené na postranních kanálech," říká prof. Lórencz.

Mgr. KAROLÍNA POLIAKOVÁ
Karolina.poliakova@fel.cvut.cz

prof. Dr. MICHAL PĚCHOUČEK, MSc.
pechoucek@fel.cvut.cz

Superpočítač pro umělou inteligenci | Centrum excelentního výzkumu v informatice

Fakulta elektrotechnická a Fakulta informačních technologií ČVUT v Praze spojily své síly a založily Výzkumné centrum informatiky (Research Center for Informatics – RCI). V rámci projektu byl vybudován nejvýkonnější počítačový klastr pro výzkum umělé inteligence v ČR v hodnotě 41,6 milionu korun. Toto jedinečné zařízení, které se svým výkonem řadí mezi superpočítače, se nachází v podzemí historické budovy Fakulty elektrotechnické ČVUT na Karlově náměstí.

Centrum excelentního výzkumu v informatice RCI je špičkou české vědy v oblasti počítačových věd a umělé inteligence. Jeho cílem je nadále rozvíjet konkurenceschopnou kvalitu výzkumu v mezinárodním měřítku, posílit spolupráci mezi základním a aplikovaným výzkumem, zvát na univerzitní půdu kvalifikované vědce ze zahraničí a propojovat zkušené vědce s mladými studenty. Provoz RCI je financován z Operačního programu Výzkum, vývoj a vzdělávání v rámci výzvy Excelentní výzkum s rozpočtem 580 milionů korun. Díky dotaci, jejímž poskytovatelem je MŠMT, bylo možné vybudovat počítačový klastr pro výzkum v oblasti umělé inteligence, který je svým výkonem v tomto ohledu nejlepším v celé ČR.

Centrum řídí vedoucí Katedry počítačů Fakulty elektrotechnické prof. Dr. Michal Pěchouček, MSc., který o projektu říká: „Dnes máme úžasnou příležitost pracovat na společném výzkumném cíli napříč celou univerzitou a posouvat vývoj informatiky na mezinárodní úroveň. Naši experti přinesou hodnotu ve výzkumu strojového učení, umělé inteligence, teoretické informatiky, bioinformatiky, vysoce výkonných výpočtů, velkých dat, kyberbezpečnosti nebo počítačové grafiky. S nově vybudovaným počítačovým klastrem se nám navíc otevírají možnosti, o kterých se nám dřív ani nezdálo."

I výzkumné týmy Fakulty informačních technologií vítají pořízení tohoto výkonného klastru, který na ČVUT již několik let chyběl. „Výzkum a experimentální vývoj vysoce výkonných a škálovatelných algoritmů probíhá třífázově. Nejdříve na osobních počítačích pro malé instance dat, pak je třeba ověřit korektnost a škálovatelnost algoritmů na dostatečně velkém klastru a následně vyhodnocení efektivnosti a škálovatelnosti na těch největších světových superpočítačích. Špičková architektura nově instalovaného RCI klastru umožní výzkumníkům efektivně zvládnout tuto druhou fázi vývoje vysoce škálovatelných algoritmů," vysvětluje prof. Ing. Pavel Tvrdík, CSc., vedoucí Katedry počítačových systémů z Fakulty informačních technologií ČVUT.

Technické parametry zařízení jsou obdivuhodné. „NVIDIA V100 Tensor Core GPU představuje nejvýkonnější akcelerátor pro tzv. high performance computing a umělou inteligenci. Celkový instalovaný výkon přes šest PetaFLOPS dělá z instalace na ČVUT aktuálně nejvýkonnější superpočítač pro AI aplikace v České republice," uvedl za společnost NVIDIA Rob Evans, ředitel regionu EMEA v oblasti high performance computing (vysoce výkonné výpočty) a umělé inteligence.

V klastru je osazeno 48 akcelerátorů s celkovým počtem 245 760 CUDA jader, 30 720 Tensor Core a celkovým výpočetním výkonem přes 6 Peta-FLOPS v operacích umělé inteligence.

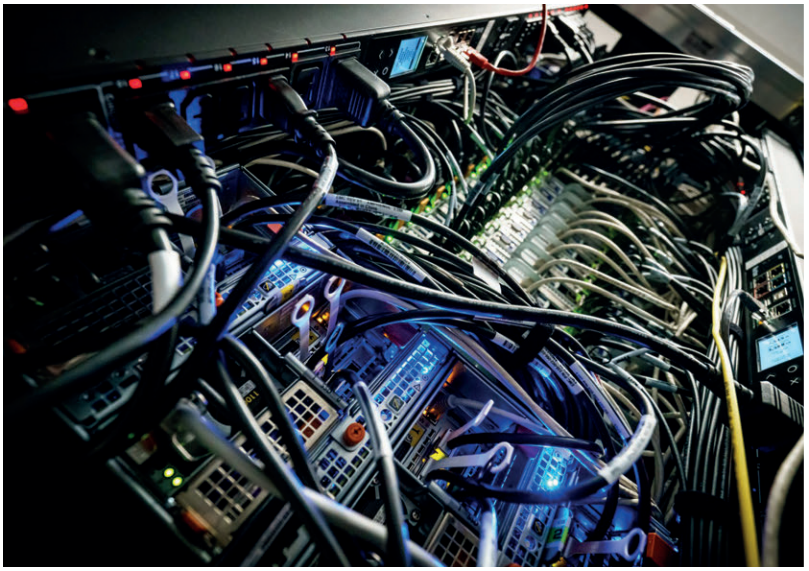
Uvést do provozu takto výkonný superpočítač nebyl jednoduchý úkol. „Celá instalace nám zabrala šest týdnů včetně dodávky všech hardwarových součástí, instalace klimatizace a rozběhnutí softwaru," vysvětluje Petr Plodík z firmy M Computers, která měla implementaci klastru na starost. „Vybudovat takový klastr v centru Prahy je poměrně unikátní. Museli jsme vytvořit nové rozvody pro napájení a chlazení a navíc jsme čelili limitům zdejší trafostanice," upřesňuje Plodík.

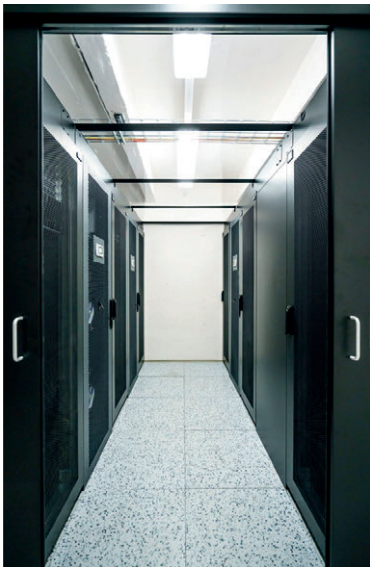
Klastr je složen z 20 CPU výpočetních uzlů Gigabyte s procesory Intel Xeon Gold (celkem 480 procesorových jader), 12 NVIDIA GPU výpočetních uzlů Supermicro, jednoho uzlu Lenovo ThinkSystem SR950 s velkým počtem CPU jader a sdílenou pamětí (192 procesorových jader, 1,5 TB operační paměti), vysokorychlostní propojovací sítě Infiniband EDR (100Gb/s) od firmy Mellanox, rychlých NVMe SSD disků Western Digital a sdíleného škálovatelného diskového pole DELL EMC Isilon. Každý GPU uzel je osazený čtyřmi akcelerátory NVIDIA V100 Tensor Core GPU. V klastru je osazeno 48 akcelerátorů s celkovým počtem 245 760 CUDA jader, 30 720 Tensor Core a celkovým výpočetním výkonem přes 6 PetaFLOPS v operacích umělé inteligence.

S tímto výkonem budou vědci z RCI moci v plné šíři provádět základní výzkum metod hlubokého učení, které je klíčové pro umělou inteligenci, např. pro aplikace v robotice, bioinformatice, vývoji aplikací pro počítačovou bezpečnost nebo řízení autonomních aut. A v těchto oblastech teď díky projektu RCI bude Česká republika moci konkurovat i zahraničním univerzitám a centrům excelence.

autorka: Karolína Poliaková
foto: Jiří Ryszawy

> Více na http://www.rci.cvut.cz





Nový superpočítač byl 16. dubna 2019 představen novinářům. Před prohlídkou výkonného clusteru se nejprve z úst nejpovolanějších – prof. Michala Pěchoučka a prof. Pavla Tvrdíka z ČVUT a Ing. Petra Plodíka z firmy M Computers – dozvěděli detaily technických parametrů i informace o záměrech zdejších vědců, kteří zde pracují v rámci Výzkumného centra informatiky (RCI).

KARIÉRNÍ CENTRUM ČVUT

SEMINÁŘE A WORKSHOPY

PODNIKNI TO!

PERSONÁLNÍ PORADNA PO SKYPU

OSOBNOSTNÍ TESTOVÁNÍ

KARIÉRNÍ PORADNA

KOUČINK

VIDEOINTERVIEW NA ZKOUŠKU

MENTORING

KNIHOVNA A ONLINE INSPIRACE

ZDOLÁVEJ VEJŠKU S KÁCÉČKEM I TY!

Služby Kariérního centra ČVUT jsou pro studenty a absolventy ČVUT ZDARMA!

SPOJ SE S NÁMI!

Jugoslávských partyzánů 1580/3, Praha 6 | Místnost A–921

www.kariernicentrum.cz Kariérní centrum ČVUT kariera@cvut.cz

MgA. IVA PELÁKOVÁ
Iva.Pelakova@cvut.cz

Od nápadu k byznysu

Kariérní centrum ČVUT dokončilo již čtvrtý běh workshopů Podnikni to!, ve kterých se studenti učí, jak objevit nápad pro podnikání a jak postupovat s projektem tak, aby měl šanci na úspěch. Studenti si odnášejí nejen motivaci vyzkoušet si podnikání, ale také velmi přesnou představu, co to bude obnášet.

„Mladí lidé mají sice nápady, ale netuší, jak začít a jaké praktické kroky vedou k vlastnímu projektu," říká zakladatel Podnikni to! Jakub Tížek a uvádí to jako jeden z hlavních důvodů, proč se rozhodl pozvednout podnikavost právě na školách. Některé projekty se i po ukončení kurzu drží dál, další studenti své nápady na nějakou dobu odloží a vracejí se k nim až později – už je to pro ně ale snazší, protože aplikují poznatky z workshopů. Podnikatelé však doporučují rozjíždění vlastního projektu neodkládat na lepší časy, protože nikdy nepřijdou. „Teď máte nejvíc času, nemusíte zatím platit pojištění státu a máte věk, kdy si můžete dovolit chyby i slepé cesty.... Až budete mít rozjetou kariéru, rodinu a hypotéku, tak už se vám nebude chtít začínat od nuly," předává své zkušenosti lektor Matouš Vinš.

A jaké nápady se na kurzu objevují? Studenti přišli například s vlastním chatbotem, rodinnou online nástěnkou, speed datingem pro studenty, návrhem na přepravu radioaktivních lékařských materiálů pomocí dronů nebo na sprchopračku, která bude šetřit vodu. Autor posledního z projektů Jan Mára si chválí především to, že se naučil, jak si nenabít podnikáním pusu: „Kurz mi rozhodně dodal odvahu. Teď mnohem víc přemýšlím, že opravdu budu podnikat. Bylo naprosto skvělé zjistit, že jsou na ČVUT lidi s podnikavým duchem a konečně jsem viděl i na přednášejícím, že ho to baví a dává to celé velký smysl."

Každý projekt vyrazí studenti ověřit v praxi tak, že mají za úkol ptát se lidí, co si o tom myslí a jestli by jejich nápad využili. Naučí se tedy i umět svůj projekt dobře vysvětlit a prodat. Zároveň vystupují z komfortní zóny, když na ulici oslovují cizí lidi nebo když prezentují svá díla před porotou profíků. V letošním Podnikni to!, které vedl digitální nomád Matouš Vinš, usedl v porotě například zakladatel Rekol Vítek Ježek. Porotci nejdříve zhlédli prezentaci studentů a následně jim dali zpětnou vazbu i vlastní tipy, jak projekt posunout.

„Snažíme se studentům co nejvíce pomoci, aby si toho pro sebe hodně odnesli. I zjištění, že podnikání pro ně není, může být důležité. Většina z nich ale odchází nadšená a odhodlaná to aspoň zkusit. Každopádně u nás mají podporu v podobě předání kontaktů inkubátorů, mentoringu, koučinku nebo knihovny vybavené zajímavými tituly z oblasti podnikání, leadershipu a osobního rozvoje," říká manažerka Kariérního centra ČVUT Iva Peláková.

Účastníci oceňují i možnost potkat se se studenty z jiných fakult, tvořit něco společně a získat pro svůj projekt podobně naladěného člověka s jiným oborem, který může pomoci vyřešit dosud nepřekonatelné zádrhele. Spousta studentů přichází na úvodní setkání ještě bez nápadu a konkrétní představy, ale už po prvním workshopu se jim podnikavost zalíbí a rozhodnou se pokračovat. Někteří už podnikání zkusili, ale nevyšlo to, a tak je zajímají především tipy, jak získat klienty a všechno si správně propočítat dřív, než do projektu investují své peníze. Mnoho studentů se podnikat bojí. To se obvykle ukáže hned na začátku, kdy účastníci jmenují všechna možná rizika a své obavy. Na kurzech však projdou změnou myšlení a pochopí, jak stáhnout rizika na úplné minimum a naopak z podnikání vytěžit to, co je pro ně osobně nejdůležitější, ať už je to často zmiňovaná svoboda, flexibilita, naplnění nebo smysluplnost.

Přihlašování na další běh bude možné opět přes Kariérní centrum ČVUT v září.

autorka: Helena Pechová
foto: Iva Peláková

> Více na www.kariernicentrum.cz

Elektronická dvojčata z Continentalu

Dvojčata mohou být siamská, jednovaječná, elektronická… Nevěříte? Důkazem jsou bratři Petr a Pavel Bařinovi, kteří žijí elektronikou od střední školy a po absolvování Fakulty elektrotechnické ČVUT dnes testují desky plošných spojů palubních přístrojů do automobilů v Continentalu v Brandýse nad Labem.

Přestože spojení ČVUT a Continentalu je velmi pevné, jejich cesta do firmy byla spíš dílem náhody. Mohla za ni i rozbitá pračka jednoho ze zaměstnanců brandýského závodu. Opravoval ji otec Petra a Pavla a díky němu se dozvěděli o tom, že Continental dělá elektroniku. Tehdy studovali SPŠ elektrotechnickou Ječná v Praze a rozhodli se absolvovat povinnou praxi právě v Brandýse.

I další kroky Petra a Pavla byly společné. Oba vystudovali na Fakultě elektrotechnické bakalářský obor Aplikovaná elektronika a následně navazující magisterský program Elektronika. „Na magisterském studiu jsme si uvědomili, že by bylo fajn mít praxi v oboru a už v letním semestru si domluvili v Continentalu stáž," říká Pavel. „Tentokrát jsme se věnovali složitějším problémům, několik týdnů jsme strávili i v laboratořích, kde jsme se poprvé setkali například s rentgenem elektronických součástek, ale poznali jsme i další oddělení firmy."

Po úspěšné stáži dostali oba z Continentalu nabídku na brigádu a tehdy se jejich cesty poprvé „rozdělily". Petr šel do oddělení náběhu nových projektů, které zajišťuje projektovou koordinaci od stavby nové výrobní linky, přes objednávání materiálu až po uvedení projektu do sériové výroby. „Pracoval jsem na projektu palubních přístrojů pro Toyotu a díky tomu poznal celý proces výroby," vzpomíná Petr.

Pavel nastoupil do oddělení kvality, kde se také podílel na projektu přístrojů pro japonskou automobilku. „Hodně jsem spolupracoval s oddělením metrologie, takže jsem se dozvěděl třeba to, jak se ověřuje kvalita plastových dílů," dodává Pavel.

Po celoroční brigádě v brandýském závodě a úspěšném ukončení studia přešli oba do firmy plynule na plný pracovní úvazek. Teď už jsou v Continentalu čtvrtým rokem a postupně se jejich cesty zase sešly. Pavel nastoupil do oddělení Industrial Engineering na pozici Test technik, kde měl na starosti technickou správu testovacích zařízení ve výrobě. Od roku 2016 se posunul na pozici inženýra, nicméně celou dobu se věnuje oblasti ICT (In Circuit Test).

Petr navázal na brigádu v oddělení NPL jako Launch Manager Junior. „Postupně jsem přišel na to, že se nechci vzdát svých znalostí v oblasti elektro, po roce jsem tedy přešel do oddělení Industrial Engineering na pozici Test Engineer Junior pro oblast FCT, tedy Functional Test."

V současné době jsou oba v pozici Test Engineer pro oblast ICT, sedí v jedné kanceláři a, jak sami říkají, „u jednoho kávovaru". Jejich náplní práce je příprava testovacích zařízeních pro sériovou výrobu palubních přístrojů určených pro přední světové automobilky.

Pro tato testovací zařízení navrhují i vlastní hardware a software pro podpůrné elektronické moduly. Právě možnost sebereализace je jednou z věcí, která je na práci hodně baví. „Nové nápady jsou vítány a často dovedeny do zdárného konce, tedy do výroby," pochvaluje si Pavel.

A jaká může být jejich další kariéra? Uplatnit by se mohli třeba v brandýském oddělení výzkumu a vývoje, ale existují i možnosti přesunu do některého ze zahraničních závodů Continentalu. Že by vycestovali zase společně?

autorka: Věra Kubinová
foto: Jan Berghauer

doc. Dr.-Ing. JAN VRBA, MSc.
jan.vrba@fbmi.cvut.cz

Bio-elektromagnetismus vrací zdraví | Vývoj zařízení pro léčbu pacientů se srdeční fibrilací

Mezinárodní konsorcium firem a univerzit ze tří zemí, mezi nimiž je i Fakulta biomedicínského inženýrství ČVUT v Praze, získalo dvouletý grant v prestižním programu Evropské komise - Horizon 2020, Fast track to innovation, ve výši více než jednoho milionu eur na dokončení vývoje systému, který sníží riziko mrtvice a srdečního selhání u pacientů se srdeční fibrilací síní, tedy nepravidelným srdečním tepem způsobeným abnormální elektrickou aktivitou v srdci.

Irská společnost AuriGen Medical navrhla koncept a vyvinula unikátní prototyp minimálně invazivního srdečního implantátu, který trvale elektricky a mechanicky izoluje tzv. ouško levé srdeční síně jednorázovou procedurou. Právě toto místo je u pacientů s chronickými fibrilacemi síní velmi častým místem vzniku krevních sraženin, které mohou způsobit cévní mozkové příhody nebo srdeční selhání. V EU a USA se jedná přibližně o více než 10 milionů pacientů.

Cílem grantu Left Atrial Appendage Electrical Isolation via Bio-photonic Optical Confirmation to Treat Persistent Atrial Fibrillation je dokončit vývoj tohoto systému s následným zavedením do praxe a minimalizovat tak vznik krevních sraženin a tím i fatálního poškození mozku a srdce pacienta.

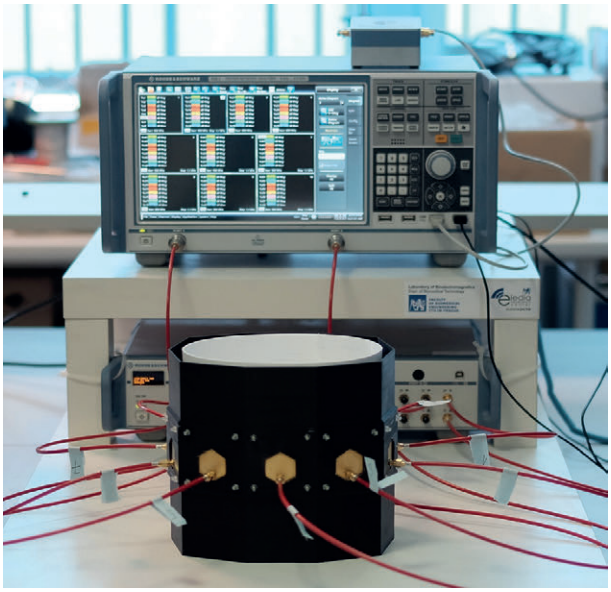
V rámci projektu se doc. Jan Vrba, doc. David Vrba a Dr. Ondřej Fišer z týmu Bio-elektromagnetismu Katedry biomedicínské techniky FBMI podílejí na návrhu a optimalizaci geometrie aplikátoru, který bude v rámci vyvíjeného systému zodpovědný za radiofrekvenční odstranění srdeční arytmie. Tým Bio-elektromagnetismus byl na Fakultě biomedicínského inženýrství založen v roce 2011 a navazuje na výzkumné aktivity prof. Jana Vrby z Fakulty elektrotechnické ČVUT, jednoho z průkopníků tzv. mikrovlnné hypertermie (HT) v bývalém Československu. HT je terapeutická metoda v onkologii, při které se úmyslně zvyšuje teplota nádorové tkáně na 40 až 44 °C. tato metoda se nejčastěji kombinuje s radioterapií pro léčbu rekurentních nádorů, u kterých díky předešlé aplikaci radioterapie v oblasti již není možné aplikovat plnou dávku. U nádorových buněk spouští řízenou buněčnou smrt. Aplikací mikrovlnné hypertermie lze i přes nižší radiační dávku zvýšit celkovou účinnost léčby.

V oblasti mikrovlnné hypertermie je jednou z hlavních aktivit týmu návrh a realizace nových originálních typů aplikátorů pro mikrovlnnou lokální a regionální HT. Pod vedením doc. Davida Vrby probíhá výzkum v oblasti návrhu nových typů aplikátorů na bázi tzv. metamateriálových struktur. Takové aplikátory v porovnání se těmi konvenčními vykazují zcela unikátní vlastnosti. Jedná se o přístroje s vysokou prostorovou variabilitou, kdy rezonanční frekvence je málo závislá na jejich fyzických rozměrech.

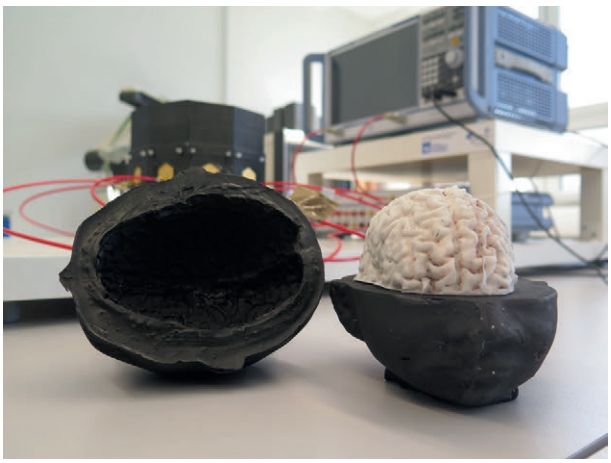
Tým Bio-Elektromagnetismus se kromě mikrovlnné hypertermie soustředí i na různá využití tzv. mikrovlnné diagnostiky v medicíně. Ta je založená na měření elektrických parametrů biologických tkání, které se liší jak pro jednotlivé jejich typy, tak i pro jejich různé stavy. Díky schopnosti mikrovln procházet a interagovat s biologickými tkáněmi je možné takovéto měření, resp. diagnostiku, provádět zcela neinvazivně.

V rámci mikrovlnné diagnostiky se věnuje vývoji vysoce senzitivních mikrovlnných senzorů pro neinvazivní měření koncentrace glukózy v krvi pacientů s diabetem, vývoji systému a algoritmů pro mikrovlnnou detekci a klasifikaci cévních mozkových příhod a v neposlední řadě 3D mikrovlnnému monitorování teploty v oblasti léčené mikrovlnnou HT.

autor: Jan Vrba
foto: archiv pracoviště



Prototyp mikrovlnného zobrazovacího systému umožňující testování nových algoritmů pro klasifikaci cévních mozkových příhod na fantomech.



Elektricky a geometricky věrný fantom lidské hlavy.

Ing. JITKA JENÍKOVÁ
Jitka.Jenikova@fs.cvut.cz

MiniFluid | Malý kotel velkého významu

Jedním ze skleníkových plynů s největším potenciálem globálního oteplování je CO_2. Nejvíce se na jeho produkci podílejí spalovací procesy, které využívají uhlíkatá paliva, jako je uhlí nebo ropa, a řada průmyslových procesů. Na produkci emisí ze spalovacích procesů se zaměřuje několik úkolů aplikovaného výzkumu na Fakultě strojní ČVUT.

V rámci doktorského studia tři studenti fakultního Ústavu energetiky navrhli a postavili experimentální fluidní kotel MiniFluid s výkonem 30 kW, jenž byl součástí výzkumu optimalizace spalování se zaměřením na snížení emisí nejenom CO_2, ale i jiných znečišťujících látek, jako je SO_2 nebo NO_x. Je možné v něm spalovat dřevní biomasu, uhlí a plánuje se i spalování nedřevní biomasy a alternativních paliv. Ve spolupráci s dalšími evropskými univerzitami zkoumají především proces oxy-fuel spalování ve fluidní vrstvě, přestup tepla ve fluidní vrstvě a fluidační vlastnosti různých materiálů.

Současnou prioritou je výzkum oxy-fuel spalování, což je jeden z perspektivních způsobů, jak zachytit CO_2 ze spalin. K okysličení paliva se používá místo vzduchu čistý kyslík. Díky tomu spaliny neobsahují žádný dusík, skládají se převážně jen z CO_2 a vodní páry. Pak je jednodušší tento plyn separovat a dál využít v průmyslu, potravinářství anebo jej uložit do geologických struktur, např. do vytěžených ložisek ropy a zemního plynu. Fluidní vrstvu, kterou prochází plyn a všechny částice nadnáší, tvoří inertní materiál. Částice jsou tak ve stavu silové rovnováhy, to znamená, že součet odporové, tíhové a vztlakové síly je rovný nule a samotná vrstva se chová velice podobně jako kapalina. Ve zkušebním MiniFluidu skutečně vzniká bublinková fluidní vrstva, která připomíná intenzivně vroucí kapalinu.

MiniFluid slouží primárně pro výzkum. Získané výsledky se následně dají ověřit na dalším zkušebním kotli vlastní výroby, zvaném Golem. Ten má patnáctkrát větší výkon, dosahuje 500 kW, a rovněž jej lze provozovat v oxy-fuel režimu. Je jedním z největších výzkumných zařízení svého druhu v Evropě.

Výsledky z měření neslouží pouze vědeckým účelům, ale i dalšímu vzdělávání a firmám, které se podílely na smluvním výzkumu. Ve spolupráci s průmyslem fakulta například ověřovala vlastnosti aditiv pro snižování emisí SO_2, tato spolupráce probíhala s firmou United Energy, a.s.

Kotle MiniFluid a Golem jsou součástí vzdělávání studentů. Malé skupiny se zaměřují zejména na laboratorní měření fluidace, měření procesu spalování a tvorby plynných znečišťujících látek. Samozřejmě nejde jen o pouhé měření, součástí výuky jsou také hodnotné experimenty. Výsledky měření i experimentů využívají studenti ve svých bakalářských, diplomových i doktorských pracích.

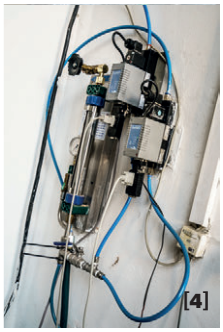
autorka: Jitka Jeníková
foto: Jiří Ryszawy

[1] FBC kotel Golem
[2] Spalovací komora
[3] Teplotní čidla spalovací komory
[4] Regulátory O_2 pro oxy-fuel spalování


[1]


[2]


[3]


[4]

Technická data MiniFluid
Výkon: 30 kW
Průřez ohniště: 22,5 × 15 cm
Výška zařízení: 2,8 m

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

PÍŠŤALY pro ČVUT

Spolek absolventů
a přátel ČVUT
pořádá

veřejnou sbírku na pořízení varhan do Betlémské kaple

Pojďme společně rozeznít Betlémskou kapli!

Dar v jakékoliv výši můžete zasílat na účet veřejné sbírky č. **2100626587/2010** nebo jej složit v hotovosti do zapečetěné pokladničky na akcích Českého vysokého učení technického v Praze.

Tváří sbírky je Eva Jiřičná, architektka a absolventka ČVUT.

Zahájení sbírky: 1. října 2014

Sbírka bude ukončena dnem vybrání maximální potřebné částky.

www.absolventicvut.cz
www.varhany.cvut.cz

Osvědčení o konání sbírky vystavil Magistrát hl. m. Prahy dne 19. 8. 2014.

CSG

CZECHOSLOVAK GROUP

Navštivte nás

Visit us

IDET 2019

29–31/5/2019

Stánek P038

a venkovní plocha

Zveme Vás na mezinárodní veletrh obranné a bezpečnostní techniky IDET BVV Brno, Česká Republika

We invite you to the International Defense and Security Technology Fair IDET BVV Brno, Czech Republic **Stand P038** and outdoor area

www.czechoslovakgroup.cz

TATRA / EXCALIBUR ARMY / msm GROUP / ZVS / TATRA DEFENCE VEHICLE / RETIA / ELDIS / european air services / NST NEW SPACE TECHNOLOGIES / CLS