



Nr. 6, maart 2011

www.esat.kuleuven.be**1 Voorwoord****2 Patrick Reynaert****3 ELECTA (1)****4 ELECTA (2)****5 IEEE studenten****6 Stysteembeheer****7 Vincent Rijmen****8 Leuven-ICT****9 Rudi Casteels****10 Triphase****11 Doctoraten (1)****12 Doctoraten (2)**

Voorwoord

Er is weer veel gebeurd in het afgelopen jaar in ons departement en een kleine selectie daarvan hebben we gebundeld in deze nieuwe editie van de ESAT-krant. Naast de vaste rubrieken, hebben we nieuws van het LICT, de IEEE studenten en hadden we een ontmoeting met de systeembeheerders en Rudi Casteels. We nodigen u ook weer van harte uit op onze traditionele inaugurale lezingen.

Veel leesplezier,

Yves Moreau (voorzitter werkgroep PR)

8 april 2011 - Inaugurale Lezingen

Graag nodigen wij u op vrijdag 8 april 2011 uit op de inaugurale lezingen van de docenten die recent op ESAT werden aangesteld. Zij zullen een overzicht geven van hun academische loopbaan en van hun huidige onderzoekswerkzaamheden. De opportuniteit bij uitstek om te polsen naar wat er op het departement Elektrotechniek-ESAT leeft.



C. Diaz



T. Goedemé



L. Meeus

- ▶ **Claudia Diaz**, afdeling SCD/COSIC, *"The challenge of protecting privacy in the information era"*.
- ▶ **Toon Goedemé**, Lessius Mechelen (campus De Nayer) en afdeling PSI, *"Real-time computer vision applications on embedded systems"*.
- ▶ **Leonardo Meeus**, Florence School of Regulation en afdeling ELECTA, *"Electricity sector reforms: inspiration for research and teaching"*.

De deelname is gratis, maar we vragen u wel om zich hiervoor te registreren.

<http://www.esat.kuleuven.be/inauguraal2011>

Bart De Moor wint FWO-Excellentieprijs

De prestigieuze FWO-Excellentieprijsen worden om de vijf jaar uitgereikt in de vijf grote wetenschapsdomeinen. Onderzoekers kunnen zich niet zelf kandidaat stellen, maar moeten voorgedragen worden door collega's. Een onafhankelijke jury van internationale topwetenschappers onderzoekt de voordrachten en selecteert per domein een laureaat. Bart De Moor kreeg de Prijs dr. De Leeuw-Damry-Boullart in de Toegepaste Wetenschappen.



Professor: Patrick Reynaert



Sinds 1 oktober 2007 ben ik als deeltijds docent en sinds 2010 als voltijds docent verbonden aan de onderzoeksgroep MICAS van het departement Elektrotechniek.

Gedreven door een uitgesproken interesse in elektronica behaalde ik in 1998 het diploma industrieel ingenieur aan de Karel-de-Grote Hogeschool te

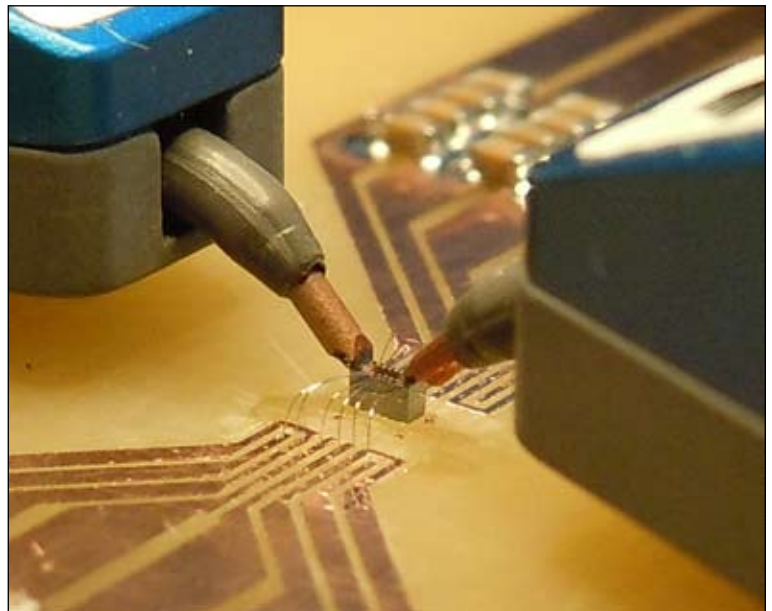
Hoboken. Hierna wilde ik meer weten over analoge geïntegreerde schakelingen en vatte de studies aan van Burgerlijk Elektrotechnische Ingenieur aan de K.U.Leuven. Na het behalen van mijn diploma in 2001 begon ik een doctoraat over CMOS RF vermogenversterkers bij prof. Michiel Steyaert. Met dat onderzoeksonderwerp kwam ik reeds in aanraking tijdens mijn eindwerk. Tijdens mijn doctoraat was ik ook Lector op Groep T. Na het behalen van mijn doctoraat in 2006 verkreeg ik een Francqui Foundation beurs van het B.A.E.F.. Met deze beurs kon ik aan de Universiteit van Berkeley postdoctoraal onderzoek verrichten. Dit onderzoek richtte zich voornamelijk op zeer hoog-frevente schakelingen in een standaard en dus goedkope geïntegreerde technologie (CMOS) en leidde ondermeer tot de realisatie van een 60GHz vermogenversterker in 90nm CMOS. Na een kort verblijf bij Infineon Technologies te Villach, Oostenrijk keerde ik in 2007 terug naar de ESAT-MICAS onderzoeksgroep van de K.U.Leuven om een nieuw onderzoeksdomein uit te bouwen: sub-THz geïntegreerde schakelingen in silicium technologie.

Waarom dit nieuwe onderzoeksdomein? Geïntegreerde schakelingen worden alsmear complexer, wat wil zeggen dat we meer en meer transistoren op één enkele chip kunnen plaatsen. De voornaamste drijfveer hiervoor is een daling van de productiekost. Deze zogenaamde "wet van Moore" heeft ertoe geleid dat we vandaag 1 biljoen transistoren kunnen plaatsen op enkele vierkante centimeter. Uiteraard is dit enkel mogelijk omdat transistoren zeer klein worden, dankzij de nano-technologie. En heel kleine transistoren zijn enorm snel. Zodoende verschijnt er een nieuwe opportuniteit: geïntegreerde elektronische schakelingen die werken op 100,.. 200,..300,.. GHz.

Uiteraard zorgen dergelijk hoge frequenties ook voor de nodige fundamentele uitdagingen. Enerzijds op het vlak van modellering en metingen, en anderzijds op het vlak van het ontwerp van de elektronische schakelingen. Het is vooral op dit tweede facet dat mijn onderzoeksfocus

ligt. Maar uiteraard kijken we met de onderzoeksgroep MICAS ook naar de modellering en de uitdagingen bij het opmeten van dergelijke schakelingen. Zodoende heeft MICAS recent geïnvesteerd in meetapparatuur tot 325GHz. Samen met mijn onderzoeksteam, dat momenteel uit 10 doctoraatsstudenten bestaat, hebben we reeds de eerste resultaten bereikt: een 220GHz mixer in 90nm CMOS, een 120GHz 10Gbps draadloze transmitter, en de nodige mm-wave bouwblokken (VCO, delers, vermogenversterkers) werkzaam op 60GHz. Daarnaast zijn we ook actief op "lagere" frequenties en ontwikkelen we nieuwe versterker topologieën voor de volgende generatie smartphones.

Naast onderzoek geef ik ook les aan de K.U.Leuven. Ondermeer de vakken "transistormodellen en elektronische schakelingen" en "basic electronic circuits". En sinds dit academiejaar 2010-2011 coördineer ik ook de helft van het vak P&O3 binnen ESAT. Hierbij ontwikkelen 38 studenten van 2e bachelor in verschillende teams de nodige elektronica, zowel de hardware als de software, voor een "airport shuttle". Dit vraagt een serieuze tijdsinvestering, maar is een uitgelezen middel om bachelorstudenten warm te maken voor elektrotechniek! Tevens zijn ook studenten van de KHK binnen de Associatie hierbij betrokken: zij ontwikkelen een platform dat de positie en status van de trein via het internet kan uitlezen.



▲ Meetopstelling voor de karakterisering van een 100GHz versterker in 40nm CMOS

En tot slot dienstverlening: sinds 2008 ben ik optiecoördinator voor de studierichting geïntegreerde elektronica van de Master Elektrotechniek. Daarnaast ben ik ook lid van de POC Elektrotechniek en de werkgroep studiebegeleiding van ESAT en ben ik diversiteitspromotor van de Faculteit Ingenieurswetenschappen.

Afdeling: ELECTA

Ronnie Belmans, Geert Deconinck, Johan Driesen en Koen Van Reusel

De naam ELECTA staat voor *Elektrische Energie en Computer Architecturen*. De groep bestaat uit een 60-tal mensen, waaronder vier professoren, tien gastprofessoren, drie post-docs, een 40-tal assistenten en een 10-tal ATP-ers.



Electa heeft vele projecten waaruit een goed contact met de industrie, de overheid en de andere universiteiten en hogescholen voortvloeit. Linear, VSGP en EIT-KIC Inno Energy, allemaal projecten rond slimme netten, zijn hier een goed voorbeeld van. Zo bouwen we een sterke band op met onder andere Vito, Belgacom, Telenet, Eandis, SPE-Luminus, Voka, De Vlaamse overheid, KHLim en Infrac om er slechts enkele te noemen.

Het onderzoek van ELECTA bestrijkt de volgende domeinen:

1. Power Systems

Power Systems richt zich voornamelijk op het transport van elektrische energie en de integratie van nieuwe netelementen. Het recent onderzoek omvat verschillende aspecten zoals de aansluiting van windenergie, een gecoördineerde aansturing van nieuwe netelementen zoals faseverschuivende transformatoren en de controle van supergrids.

2. Motoren en aandrijvingen

Dit onderzoeksdomein focust zich op energie-efficiënte optimalisatie van elektrische aandrijfsystemen door implementatie van geavanceerde motor-, vermogenelektronica- en controletechnologieën.

3. Techno-economische aspecten

Sinds de liberalisering van de elektriciteitsmarkt heeft het economische luik van de elektriciteitsvoorziening sterk aan belang gewonnen in Europa. Belangrijke thema's

zijn de ontvlechting van de waardeketen waarbij de netbeheerder onafhankelijk wordt van de generatoren, de veiling van transmissiecapaciteit en de ontwikkeling van elektriciteitsbeurzen, de netwerkplanning, de optimale energiemix, subsidiemechanismen voor hernieuwbare energiebronnen, etc. Al deze onderwerpen hebben duidelijk een economische inslag, maar zijn toch onlosmakelijk verbonden met de technische realiteit.

4. Vermogenelektronica

Huidig onderzoek rond vermogenelektronica focust op het ontwerp en de controle van energiezuinige, compacte vermogenelektronische convertoren.

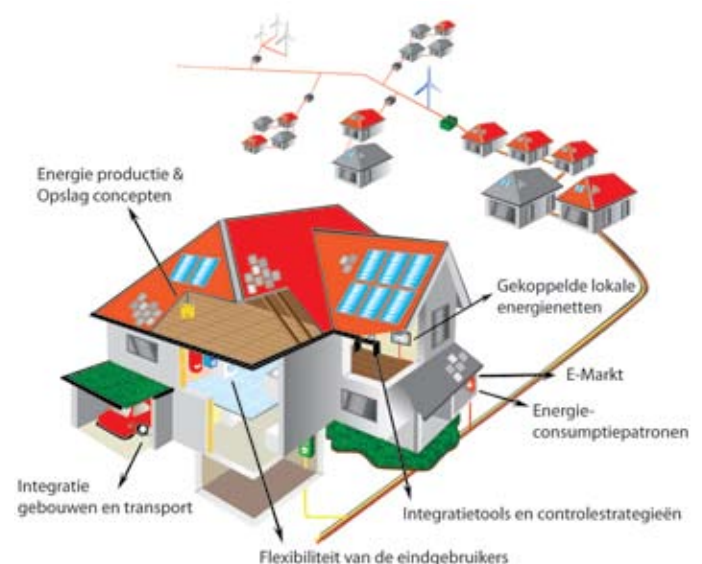
Er wordt nagegaan hoe de introductie van nieuwe, steeds sneller schakelende componenten de topologieën van deze convertoren en hun controle-algoritmes beïnvloedt. In het kader van slimme energienetwerken vinden we vermogenelektronica vooral terug in de vorm van batterijlaadsystemen, koppelingen met het elektriciteitsnet, fotovoltaïsche systemen, e.d.

5. Gedistribueerde energieopwekking

Electa onderzoekt de impact en mogelijkheden van gedistribueerde energieopwekking van fotovoltaïsche zonnepanelen, wind, warmtekrachtkoppeling, biobrandstof, ... en de verspreide opslagmogelijkheden zoals opslag in batterijen (al dan niet ingebouwd in elektrische voertuigen) en supercaps. Zij kunnen het bestaande elektriciteitsnet helpen omvormen naar een "intelligent elektriciteitsnet".

6. Smart Grids

De meeste hernieuwbare bronnen (zoals zonnecellen, zonneboiler, windmolen,...) hebben de eigenschap niet stuurbaar en slechts in beperkte mate voorspelbaar te zijn. De energie die op deze manier geproduceerd wordt valt niet af te stemmen op de vraag. Om deze bronnen



optimaal te integreren in het systeem zonder kwaliteitsverlies te lijden in onze energievoorziening zijn intelligente netten of 'smart grids' een vereiste. Hierbij kijken we naar de nodige intelligentie in het net, de eisen voor een robuuste communicatie –en informatieinfrastructuur en de algoritmes voor de hoogniveautoepassingen. Ook de optimalisatie komt aan bod.

7. Elektrowarmte

Veel verschillende materialen zijn in de afgelopen jaren verwerkt via het gebruik van elektrische energie. Zij omvatten belangrijke gebieden van de materiaalclassificatie, variërend van metalen tot keramiek en van natuurlijke vezels tot polymeren, waarbij levensmiddelen een zeer belangrijk gebied vormen voor een aantal elektrowarmte processen. Specifieke voorbeelden hiervan zijn ondermeer het snijden van stalen platen met een plasmatoorts, het drogen van textiel met radiofrequenties, het temperen van bevroren vlees met microgolven, het lassen van metalen met behulp van CO₂-lasers, de hogetemperatuur-korte-tijdsterilisatie van voedsel met behulp van ohmse verwarming, het smeden van stalen halffabricaten met behulp van inductieverwarming, enz. Al deze processen worden omvat door het onderwerp elektrowarmte.

De labo-infrastructuur

Het hoogspanningslaboratorium biedt de mogelijkheid verschillende spanningsvormen te genereren, tot meerdere honderden kilovolt. Bliksemstootspanningen, bijvoorbeeld, worden vaak gebruikt om middenspanningscomponenten en schakelapparatuur aan genormeerde testen te onderwerpen. Naast standaard DC en 50 Hz AC golfvormen, produceert het labo ook hoogfrequente sinusoidale spanningen (tot 1 MHz) met hoge amplitude, die vooral voor onderzoek naar de ontstekings-eigenschappen van hogedrukgasontladingslampen worden ingezet. Ook voor vermogenelektronica, smartgrids en elektrowarmte is een belangrijke labo-infrastructuur ter beschikking. Voor meer informatie:



<http://www.kuleuven.be/electa>

EnergyVille



Electa gaat samen met VITO uitbreiden. Op het voormalig mijnterrein van Waterschei in Genk wordt 'EnergyVille' opgericht, een kenniscentrum rond groene energie en energietechnologie dat aanvankelijk plaats zal bieden aan een 200-tal onderzoekers van K.U.Leuven en VITO. Dit kenniscentrum zal in de zomer van 2012 gevestigd worden op het Wetenschapspark Waterschei in daarvoor speciaal ontworpen gebouwen en laboratoria.

EnergyVille vormt een belangrijke bundeling van krachten en expertises binnen de Vlaamse energietechnologie en heeft als doelstelling een plaats binnen de top vijf van Europa op het vlak van innovatief energie-onderzoek te bereiken. EnergyVille brengt spelers uit onderzoek, business, industrie en onderwijs bij elkaar. Medewerkers van de ingenieursafdelingen van Limburgse hogescholen, van de K.U.Leuven, VITO en IMEC werken hier nauw samen. Ook een deel van het KIC (Knowledge and Innovation Community) InnoEnergy, gesteund door het EIT (European Institute for Innovation and Technology) zal in Waterschei worden geherbergd en zich specifiek richten op de ontwikkeling van intelligente en energie-efficiënte gebouwen en steden. Energyville wordt de uitvalsbasis van het VSGP (Vlaams Smart Grid Platform), een vzw die bedrijven en kennisinstellingen samenbrengt om van smart grids of intelligente energienetten een realiteit te maken. De technologische ontwikkelingen binnen EnergyVille zullen leiden tot daaraan verbonden business development en de creatie van spin-offs en andere economische activiteiten. EnergyVille zal zo een belangrijke bijdrage leveren aan de energietechnologie van morgen, zal ondersteuning leveren bij het beantwoorden van belangrijke ecologische en energie-gerelateerde vraagstukken en innovatie en economische ontwikkeling bevorderen op een voor Vlaanderen en de wereld cruciaal terrein.



IEEE Student Branch Leuven



Afgelopen jaar vierde onze IEEE Student Branch zijn 50ste verjaardag, een gelegenheid die we niet onopgemerkt voorbij konden laten gaan. Zo kregen we in augustus de kans om het IEEE Region 8 Student Branch & GOLD Congress te organiseren. Gedurende vijf drukke dagen overrompelden 300 IEEE- en Student Branch afgevaardigden van over de hele wereld onze universiteitsstad. Naast het aanbod van plenaire sessies en een brede waaier aan technische en soft-skill gerelateerde workshops, maakten ze ook kennis met het onderzoek binnen dit departement. Een van de hoogtepunten was het 'Elect the president' debat, waarbij studenten de mogelijkheid kregen om in discussie te gaan met de IEEE presidents-

kandidaten. Ook de explosieve sessie van 'mad scientist' John Cohn over de motivering van jongeren voor technologie kon op veel bijval rekenen. Daags na het congres kreeg ook ESAT de unieke gelegenheid om van zijn show te genieten. In het goedgevulde avondprogramma met een meer dan geslaagde BBQ en galadiner vormde de afsluitende multiculturele avond het absolute orgelpunt. Gedurende deze laatste avond kregen alle deelnemers de kans om hun eigen cultuur voor te stellen bij de andere congresgangers.

Ook gedurende de rest van het jaar was het programma van onze Student Branch goed gevuld. Naast onze jaarlijkse job fair, ESAT BBQ, symposia en andere activiteiten, organiseerden we samen met het departement een eerste geslaagde ESAT reünie. Op een warme dag in juni zakten zo'n 200 ESATers en oud-getrouwen af naar het Kasteelpark om elkaar weer te zien en herinneringen op te halen

onder muzikale begeleiding van enkele ESAT-bands. Naast een succesvolle lancering van de Women In Engineering Kookavonden, bouwden we ook verder aan onze 'Soirée Technique' lezingen, waarbij we een actuele technologie gedurende een avondlezing in de kijker plaatsen. Zeer binnenkort vult de 'Soirée Pratique' het rijtje van activiteiten aan...

Ben je geïnteresseerd in de IEEE Student Branch Leuven? Neem dan zeker een kijkje op onze website (www.ieee-sb-leuven.be) en aarzel niet om je in te schrijven op onze mailinglijst om op de hoogte te blijven van toekomstige activiteiten. Je vindt ons ook op facebook en linked in!



▲ IEEE Region 8 Student Branch & GOLD Congress

Cultureel Erfgoed in de kijker

Het onderzoek naar de visualisatie van cultureel erfgoed door PSI, kreeg de afgelopen tijd extra aandacht in de media. De samenwerking met het Louvre en het Victoria & Albert museum, in het kader van het EC project 3D-COFORM, was te zien op de zender Euro News in het programma Futuris en in de Griekse krant Kathimerini. Ook kreeg het project een speciale stand op de door de Europese Commissie georganiseerde ICT conferentie in Brussel in september 2010. Prof. Luc Van Gool werd uitgenodigd om een presentatie te geven over cultureel erfgoed in ICT in de Nationale Bibliotheek in Brussel in het kader van het Belgische voorzitterschap van de Europese Unie.

De Mexicaanse televisie en kranten hadden vooral aandacht voor de digitalisatie van de indiaanse archeologische nederzetting 'Calakmul', waar PSI samenwerkt met het GIM en de universiteit van Gent in het kader van een UNESCO project tot behoud van het werelderfgoed. Het belang van Limburg tenslotte, richtte zijn focus op de samenwerking met het Gallo-Romeins museum, waar frescofragmenten via een computerprogramma terug in elkaar gepuzzeld worden.



De Systeembeheerders

Evelyn Dehertoghe

Als we onze computer aanzetten en zonder problemen ons vertrouwde scherm zien opkomen, staan we er meestal niet bij stil hoeveel hierbij komt kijken. We zien boodschappen binnenlopen over een 'scheduled maintenance weekend', het vrijgeven van Matlablicenties, wijzigen van je wachtwoord, enzovoort, maar besteden daar in alle drukte nogal weinig aandacht aan. Vandaar dat ik eens binnenloop bij Frank, Piet, Marc, Rik en Stef om te horen wat er zich eigenlijk afspeelt achter de schermen van het systeembeheer.



▲ vlnr: Frank, Piet, Marc, Rik en Stef

Wist je bijvoorbeeld dat er een beurtrol is onder deze heren om een 24u/24u wachtdienst te voorzien en dat zij in het holst van de nacht gewekt kunnen worden wanneer er iets aan de koeling van onze serverruimte schort of wanneer er een stroompanne is?

Ik vroeg mij af hoeveel mensen zij hier eigenlijk ondersteunen en sta even verstomd wanneer Piet me voor 2010 de aantallen meegeeft; 628 personeelsleden en 796 studenten hadden een ESAT computeraccount. Geen wonder dat in 2003 de online IT helpdesk werd ingevoerd. Dit systeem is onmisbaar om al deze gebruikers op een georganiseerde manier vragen en problemen te laten melden. De systeembeheerders bewaren statistieken van de gelogde oproepen en richtten een database op waar je de oplossing voor je probleem waarschijnlijk al kan terugvinden. Intussen staat de teller al op meer dan 14.000 calls! Wees dus begripvol wanneer bijvoorbeeld jouw printprobleem een prioriteit "laag" toebedeeld krijgt en weet dat 95% van de topprioriteitgevallen binnen 2-4 uur zijn opgelost.

Deze ondersteuning is overigens zeer uitzonderlijk binnen de universiteit. Waar de meeste departementen het onderhoud van hun computerinfrastructuur uitbesteden aan de dienst ICTS, heeft ESAT dit in eigen beheer. Met IT als 'core business' zijn ESAT gebruikers immers heel onderlegd en veeleisend. Op deze manier krijgen zij een dienstverlening op maat die overigens veel sneller werkt.

Ondanks deze erg kundige 'users' weten de systeembe-

heerders op mijn aanvraag toch een aantal grappige interventies op te sommen. Adviezen als "probeer de stekker eens in te steken" of "ga nooit meer in op phishing mails" zijn toch niet zo zeldzaam. Ook was een werknemer eens zo creatief om een netwerkkabel onoordeelkundig te verstoppen en zo zijn hele afdeling zonder netwerk te zetten.

Voor een goed en veilig computergebruik geven zij ons dus graag het volgend advies mee:

- Geef nooit je wachtwoord door aan anderen.
- Lees de aankondigingen (dan kom je niet voor verrassingen te staan)
- Versteek niet zomaar kabels en berg ongebruikte kabels netjes weg
- Verander je wachtwoord op tijd (Je account sluit écht na dertig keer 'later' kiezen)
- Geef matlablicenties vrij indien je ze niet meer nodig hebt (deze kosten geld aan je groep)

Een systeembeheerder moet constant mee met de snellende technologische ontwikkelingen. Zij bevestigen mij dan ook wat je meer en meer waarneemt; het belang van de eigen PC wordt steeds kleiner en de centrale server wordt steeds belangrijker. Door deze toenemende virtualisatie kunnen mensen gemakkelijker van thuis werken, mails lezen op hun PDA en de informatie uit de 'cloud' halen.

Het systeembeheer blijkt tenslotte ook een teamwerk te zijn, waarbij iedereen zijn eigen specialisatie heeft, maar ook voor een ander kan inspringen. De belangrijkste taken zijn als volgt verdeeld:

Frank: Beheer van eigen software. UNIX operating systems, externe communicatie, lid van de systeembeheerdersraad en K.U.Leuven ICTS.

Rik: Onderhoud en installatie van Linux systemen, netwerkbeheer en ondersteuning van eindgebruikers.

Marc: Windows installatie, onderhoud en alle services daar rond.

Stef: eerstelijns-ondersteuning voor Linux (soms Windows) en herstellingen.

Piet: eerstelijns-ondersteuning (vooral Windows), de PC-classes controleren, hardware, netwerk en herstellingen uitvoeren samen met Stef.

Gelukkig houden ze nog wat vrije tijd over en blijken buiten de IT ook van aanpakken te weten. Drie van hen zijn momenteel aan het verbouwen. Frank is een verwoed zweefvlieger en kajakker. Stef volgt het rugby op de voet en houdt van lezen. Piet sleutelt aan zijn MG65 en Fiat Bertone. Marc is actief in een volleybalclub, doet aan spinning en tekent graag. Rik is recent papa geworden en heeft hier samen met de verbouwingen zijn handen mee vol.

Toen mijn computer vanmorgen weer heel normaal deed, heb ik alleszins toch even aan hen gedacht. Bedankt voor het goede werk.

IEEE prijzen voor MICAS

Willy Sansen werd onderscheiden met de 'Donald O. Pedersen Award in Solid State Circuits' voor zijn belangrijke bijdrage voor de maatschappij, technologische vooruitgang en professioneel leiderschap in het onderzoek naar 'solid state circuits'.

Bob Puers werd geëerd met de titel IEEE Fellow. Dit is een eer die na een streng evaluatieproces toegekend wordt aan een selecte groep leden van IEEE, die zich uitzonderlijk verdienstelijk hebben gemaakt in hun domein. Bob Puers kreeg de prijs voor "Contributions to implantable micromechanical systems".

Willy Sansen ►

Bob Puers ►►



Professor: Vincent Rijmen



In 1993 studeerde ik af als burgerlijk ingenieur elektrotechniek. Als aspirant van het FWO begon ik aan een doctoraat in de cryptografie bij COSIC, onder leiding van de professoren René Govaerts en Joos Vandewalle. Dit leidde tot een doctoraat in 1997, gevolgd door een jaar als postdoctoraal onderzoeker van de K.U.Leuven en tenslotte een postdoctoraal

mandaat bij het FWO. Na een korte periode bij de Belgische tak van het Deense bedrijf Cryptomathic en een iets langere periode in de leerstoel Toegepaste Cryptografie aan de Technische Universität Graz (Oostenrijk), keerde ik in 2007 terug in de schoot van de Alma Mater als hoofd-docent met een BOF-mandaat.

Het vercijferen en ontcijferen van boodschappen is een van de oudste bezigheden van de mens, maar als open onderzoeksdiscipline wordt cryptografie pas bedreven sinds de jaren '70. Vooral de doorgedreven automatisering, digitalisering en informatisering van de laatste jaren hebben geleid tot een sterke toename van de publieke belangstelling voor onze branche. Naast de tot de verbeelding sprekende geheimhouding van gevoelige informatie, wordt cryptografie tegenwoordig ook gebruikt om de privacy van consumenten te beschermen, om betalingen met een kaart of over het Internet mogelijk te maken, om films en muziek te beschermen tegen onge-



oorloofd kopiëren, enz.

De onderzoeksgroep COSIC is binnen ons gebied één van de grootste in Europa en is ook bekend ver daarbuiten. Onze expertise strekt zich uit van veilige implementaties voor ingebedde systemen over protocols voor beveiliging van ad-hoc netwerken, tot formeel wiskundig bewijsbare veiligheid.

We ontwikkelen toepassingen zoals privacy-bevorderende browser plugins, elektronische verkiezingen, en de Belgische elektronische identiteitskaart.

Mijn persoonlijke interesse gaat vooral uit naar de ontwikkeling van nieuwe encryptiemethoden met een nieuwe theorie voor de bewijsbare veiligheid ervan, en daarnaast de ontwikkeling van technieken om bewijsbaar veilige implementaties van deze methoden te maken. Tegenover klassieke testmethodes wint bewijsbaarheid aan belang (ook buiten strikt cryptografische toepassingen) omdat door de toenemende complexiteit van systemen het moeilijker en moeilijker wordt om goede tests op te stellen en door te voeren. Het bijzondere aan cryptografische toepassingen is dat we meestal niet kunnen steunen op de wetten van de statistiek om tot een redelijke zekerheid te komen. Waar in sommige toepassingen een faalkans van 0.01% aanvaardbaar is, zal een beveiligingstoepassing die voor 99.99% foutvrij is, door hackers steeds gestuurd worden naar die toestand waarin een fout optreedt en kan uitgebuit worden. Daarenboven wordt cryptografie tegenwoordig vaak gebruikt in toepassingen waar de gebruiker niet noodzakelijk geïnteresseerd is in een correcte werking. Denken we bijvoorbeeld maar aan een bankkaart, waar de gebruiker enkel bezorgd is dat er niet teveel geld van zijn rekening gaat, maar te weinig is voor hem best okee. De ontwikkelaars van een elektronisch betaalsysteem moeten hiermee rekening mee houden bij het ontwerp van de beveiligingsmaatregelen.

Een belangrijk deel van mijn onderzoek verloopt in nauwe samenwerking met dr. Joan Daemen van ProtonWorld, tegenwoordig deel van ST MicroElectronics. We ontwikkelden samen het encryptie-algoritme Rijndael, dat gekozen werd als Advanced Encryption Standard (AES) en ons de eerste CaStaR trofee opleverde. Tegenwoordig vind je AES onder andere in het https protocol, in het WPA2 protocol ter beveiliging van WLAN netwerken, en ook als optie in het EMV protocol ter beveiliging van elektronische betalingen. Sinds 2010 bevatten alle nieuwe Intel processoren extra hardware en ondersteunen ze speciale assembler instructies om software-implementaties van AES nog sneller te maken.

Leuven ICT Centre (LICT)



Het LICT (Leuven Information and Communication Technology Centre) is één van de 12 onderzoekscentra die sinds 2007 binnen de groep Wetenschap en Technologie van de Katholieke Universiteit Leuven werden opgericht. Onderzoekscentra zijn flexibele en dynamische structuren die als doel hebben de kennis en expertise binnen geselecteerde onderzoeksdomeinen te bundelen over de grenzen van de departementen en faculteiten heen, om aldus grensverleggend multidisciplinair onderzoek te stimuleren en om als centraal aanspreekpunt te fungeren voor de overheid en de industrie. In deze context focust het LICT zijn activiteiten op alle aspecten van ICT (Informatie- en Communicatietechnologie), met aandacht voor zowel de technische, de gebruikers- als de legale aspecten.



▲ Leden van LICT in 2010

De missie van het LICT-centrum bestaat uit het coördineren en promoten van top-niveau onderzoek voor het ontwerpen en toepassen van ICT-systemen, zowel hardware als software, met als maatschappelijk doel om (1) samenlevings- en industriële noden aan te pakken, (2) ons leven comfortabeler en veiliger te maken, (3) onze gezondheid te verbeteren en (4) ons milieu in stand te houden.

In 2010 vertegenwoordigde het centrum zo'n 50 professoren en meer dan 350 onderzoekers. Het LICT centrum wordt momenteel geleid door Prof. Georges Gielen, die wordt bijgestaan door de valorisatie-coördinator Greet Bilsen.

Het onderzoek binnen LICT is georganiseerd rond zeven speerpuntpijlers, waarvan de expertise kan ingezet worden in verschillende applicatiedomeinen zoals communicatie, gezondheidszorg, multimedia, transport en logistiek en in het kader van groene ICT, en dit in allerlei onderzoeksprogramma's (EU, IWT, bilateraal met bedrijven, IBBT, enz.). De speerpuntpijlers zijn :

- **Wireless Communication Systems** richt zich op het modelleren, ontwerpen en opmeten van circuits en antennes voor RF, microgolf en mmgolf telecommunicatiesystemen, op draadloze sensornetwerken, en op digitale signaalverwerking voor draadloze communicatie.

- In de **Mixed-Signal Interface Systems** onderzoekslijn wordt onderzoek verricht naar nieuwe circuittechnieken en -architecturen voor analoge en mixed-signal interfaceschakelingen, de bijhorende modellering, CAD tools en testmethodes, alsook rond MEMS/NEMS en circuits in post-CMOS nanotechnologieën. Toepassingen vinden we in verschillende bedrijfstakken, zoals o.a. de communicatie-, biomedische-, auto-, instrumenten- en multimediatechnologieën.

- **Embedded Systems and Software** richt zich op het ontwerp van (goedkope) laagvermogen, hoogperformante ingebedde systemen en op de software ingebed op dergelijke in mogelijkheden beperkte systemen. Dit laatste met bijzondere aandacht voor de niet-functionele vereisten zoals samenstelbaarheid, voorspelbaarheid, flexibiliteit, schaalbaarheid, betrouwbaarheid, enz. Ook aan de incorporatie van privacy en authenticatie wordt aandacht besteed.

- **Distributed Software** kijkt naar architecturen voor gedistribueerde software, middleware technologieën, oplossingen voor het uitrollen en beheren van gedistribueerde

software, en ontwikkelmethodes voor gedistribueerde software.

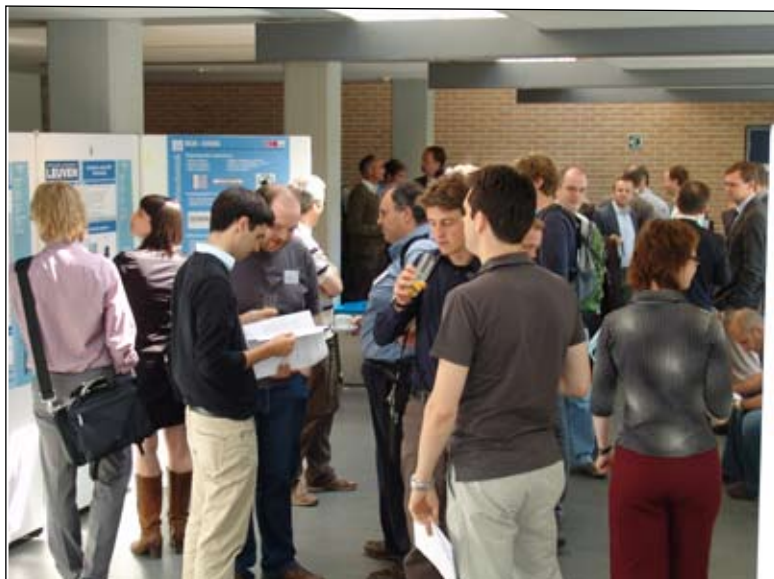
- **ICT Security** omvat zowel de technische als de legale aspecten van ICT beveiliging en privacy, m.i.v. onderzoek naar cryptografische algoritmes en protocollen, veilige software en software-ontwikkeling, en efficiënte en veilige hardware implementaties.

- De interactie tussen de technologie en de eindgebruiker komt aan bod in de **Human-Machine Interaction** onderzoekspijler. Een eerste lijn binnen deze pijler heeft betrekking op gebruiksvriendelijke interfaces en gebruikersgeoriënteerde ontwerpmethodes. Daarnaast omvat de pijler ook onderzoeksactiviteiten met betrekking tot computervisie, computer graphics, spraakverwerking, data- en informatievisualisatie en educatieve computerspellen.

- De **Knowledge Technologies** pijler omvat onderzoeksthema's als artificiële intelligentie, machine lear-

ning, data/tekst/beeld/web mining, kennisrepresentatie en declaratieve talen.

Als overkoepelende structuur biedt LICT een belangrijke toegevoegde waarde bij het promoten en valoriseren van dit onderzoek en het samenbrengen van interne en externe partijen. In dit opzicht biedt het centrum, bij hoofde van de valorisatiecoördinator Greet Bilsen, onder andere een brugfunctie aan tussen de interne LICT leden enerzijds en de buitenwereld (industrie, overheid) anderzijds. De leden zien zich vertegenwoordigd bij de overheid, op externe events, in externe consortia en netwerkorganisaties, grote Europese programma's, enz. Er is ook een gerichte doorstroming van informatie aangaande onderzoeksopportunities naar de leden toe. Naar de industrie toe vervult het LICT dan weer een waardevolle rol in het aanbieden van een eenduidig aanspreekpunt voor alle ICT-gerelateerde onderzoeksvragen. Hiernaast draagt het LICT ook actief bij aan de verspreiding van kennis en informatie over toekomstige evoluties in het ICT domein, ondermeer door het organiseren van workshops en seminars en een "distinguished lectures" programma, steeds vergezeld van uitgebreide mogelijkheden tot netwerking.



▲ LICT Industrial Affiliation day

Firma's kunnen van deze opportuniteiten gebruik maken door lid te worden van het LICT industrieel affiliatieprogramma.

Voor meer informatie zie www.kuleuven.be/LICT of contacteer Greet Bilsen op LICTcoordinator@kuleuven.be.

Personeelslid in de kijker: Rudi Casteels

Reeds 31 jaar werkt Rudi in de Centraal Mechanische Werkplaats in de kelder. Toch weten heel wat ESATers niet eens wie Rudi is. Hoog tijd om daar verandering in te brengen en hem aan u voor te stellen.

Zijn verhaal begon in 1979 toen de laatstejaars Elektromechanica van het Don Bosco College te Haacht de vraag kregen wie interesse had om voor de K.U.Leuven te gaan werken. In juli viel er om 7 uur 's morgens een telegram in de bus bij de familie Casteels. Rudi, aan het genieten van de pas begonnen vakantie, was nog maar een paar uur thuis na een nachtje stappen op de Parkfeesten van Kampenhout. In het telegram stond dat hij nog diezelfde ochtend om 9 uur op gesprek verwacht werd bij professor Luypaert. Het ging goed want een dag later al begon Rudi aan zijn trouwe carrière bij ESAT.

Eerst werkte hij voor afdeling MILO3 (het huidige TELEMIC) dat onderzoek verrichtte naar microgolven en lasers. In die tijd werkten er zeven mensen in de Centraal Mechanische Werkplaats en werden er stukken gefreesd, geboord, gezaagd en gekapt voor studenten, onderzoeksassistenten en professoren van binnen en buiten ESAT. Rudi maakte toen vooral golfgeleiders voor industriële microgolfovens.

Over de jaren heen is er natuurlijk wel wat veranderd. Intussen werken er minder mensen in de werkplaats. Er gebeurt nu immers veel meer op computer. Rudi werkt ook al lang niet meer uitsluitend voor één onderzoeksafdeling. 12 jaar geleden werd hij hoofd van de werkplaats en nu verricht hij werk voor het ganse departement. Het machinepark zelf heeft ook wat veranderingen ondergaan. De toestellen zijn moderner, computergestuurd en hebben een digitale aflezing.

Rudi is in '83 getrouwd met Ingrid. Zij gaan in hun vrije tijd graag al wandelend steden of markten bezoeken en onze Vlaamse kust behoort eveneens tot de favoriete uitstappen. Eens per jaar trekken ze er binnen Europa ook op uit met de wagen.



▲ Rudi Casteels in zijn natuurlijke omgeving, de Centraal Mechanische Werkplaats

SPIN-OFF: Triphase



Vanuit de ELECTA groep werd op 6 oktober 2006 Triphase opgericht. Deze spin-off focust op stuursystemen voor conversie en management van elektrische energie. Toepassingen gaan van elektrische of hybride voertuigen tot zogenaamde 'slimme energienetwerken van de toekomst' of smartgrids.

De basistechnologie werd ontwikkeld door Jeroen Van den Keybus, in zijn doctoraat onder supervisie van prof. Ronnie Belmans. Deze belangrijke link met de universiteit uit zich verder in een dagelijkse samenwerking in verschillende onderzoeks- en onderwijsprojecten.

Het hart van de Triphase oplossingen wordt gevormd door een ontwikkelmethodologie die onderzoekers toelaat om snel de brug te slaan tussen simulatie en implementatie.

Deze methodologie, die een combinatie is van model-gebaseerd ontwerpen en client-server architectuur, werd aangevuld met de nodige integratie-hardware om snel vermogenelektronische componenten en metingen te kunnen integreren.

Na vier jaar ontwikkeling vormt deze basistechnologie nog altijd het fundament van de onderneming. Hiermee worden 'out-of-the-box' systemen gerealiseerd waarbij, onder het motto 'unpack, connect, get creative', iemand zich onmiddellijk kan concentreren op het aanleggen van schakelpatronen en geen rekening moet houden met vermogenelektronische integratievraagstukken.



Momenteel wordt ook een belangrijke tak rond elektrisch/hybride rijden uitgebouwd. Deze activiteiten vallen onder de vlag van 3PMotive. In het verleden werden op projectbasis aandrijvingen ontwikkeld voor een waterstofaangedreven kart en een prototype-aandrijving voor een Engelse taxi.

Deze ontwikkelingen worden nu opgeschaald naar hogere vermogens en Triphase voorziet tegen eind 2011 de aandrijflijn uit te leveren voor een aantal prototype-voertuigen voor gebruik op de openbare weg.

Dit vergt telkens een samenwerking met specifieke voertuigombouwers waarbij Triphase zich focust op het vraagstuk rond elektrische aandrijving en energiemangement.

De toekomst

Na de eerste vier jaar is Triphase gegroeid van vier naar tien mensen. Alle winsten worden hierbij maximaal geherinvesteerd in de verdere uitbouw van de onderneming. Deze gestage groei wordt ook voor de volgende jaren voorzien. Enerzijds wordt er gewerkt aan de uitbreiding van het productgamma en verdere integratie met mogelijke eindapplicaties. Binnen 3PMotive ligt de nadruk op het afwerken van de eerste voertuigen om op termijn een standaard gamma aan aandrijflijnen te realiseren.

En natuurlijk wordt de eerstkomende jaren ook een verdere uitbouw van de samenwerking met onze Alma Mater voorzien.

Voor meer informatie: <http://www.triphase.com>

ESAT sportdag

Op vrijdag 17 december vond de jaarlijkse ESAT-sportdag plaats in De Borre in Bierbeek. In een vriendschappelijke maar competitieve sfeer werd onder het personeel van ESAT uitgemaakt, wie zich de kampioen zaalvoetbal, volleybal en badminton mag noemen. Voor minder competitief ingestelde collega's werd er ook een mountainbike fietstocht en een wandeltocht georganiseerd. De traditioneel aanwezige mandarijnen zorgden voor de broodnodige energie tijdens de spelen, terwijl de cafetaria opgezocht werd om het verloren zweet terug aan te vullen en na te kaarten over de gebeurtenissen van de dag.



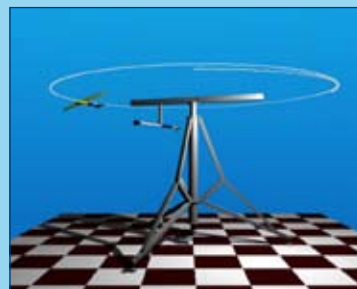
Wetenschapsweek

In het kader van de Wetenschapsweek streken in november meer dan 300 middelbare scholieren neer in ESAT. Aan de hand van 12 uiteenlopende demonstraties, die varieerden van elektrische wagen tot inslikbare camera, konden ze kennis maken met wat de wetenschap te bieden heeft in ons departement. Het was tevens een speciale editie van dit wetenschapsfeest, aangezien organisator Jan Engelen na jarenlange dienst en tomeloze inzet het stokje doorgaf aan Vincent Rijmen.



Moritz Diehl wint ERC starting Grant

OPTECs Moritz Diehl kreeg van de EU een 'ERC Starting Grant' voor zijn project *HIGHWIND - Simulation, Optimization and Control of High-Altitude Wind Power Generators*. Deze beurs zal het reeds aan de gang zijnde onderzoek van OPTEC naar het modelleren van opwekken van windenergie uit megavliegers in de komende vijf jaar aanzienlijk kunnen versterken.



(zie ook artikel over Moritz Diehl en ERC grants in de vorige editie van de ESAT-krant).

Doctoraten 2010

1. Nick Van Helleputte, "*Low-power analog front-ends for pulsed ultra-wideband receivers with ranging capabilities*", jan. 2010, prom. Georges Gielen en Bob Puers.
2. Wim Van Thillo, "*Continuous phase modulation for 60 GHz high-rate communications*", jan. 2010, prom. Rudy Lauwereins en Emmanuel Van Lil.
3. Maarten Van Segbroeck, "*Robust large vocabulary continuous speech recognition using missing data techniques*", jan. 2010, prom. Hugo Van hamme.
4. Min Li, "*Algorithm/Architecture Co-Design for Energy Aware Signal Processing in Software Defined Radio*", jan. 2010, prom. Francky Catthoor en Diederik Verkest.
5. Jan Luts, "*Classificatie van hersentumoren op basis van Magnetische Resonantie Spectroscopie*", jan. 2010, prom. Sabine Van Huffel en Johan Suykens.
6. Daniel Ruijters, "*Multi-modal image registration during minimally invasive treatment*", feb. 2010, prom. Paul Suetens en Bart Ter Haar Romeny.
7. Mohammad Ali Pourghaderi, "*Carrier Transport in Nanoscale Transistors*", maart 2010, prom. Christina De Meyer.
8. Phillip Ekkels, "*Metal surface micromachining technologies for implementation in RF-MEMS switching devices*", maart 2010, prom. Bob Puers en Robert Mertens.
9. Deepaknath Tandur Krishnagopal, "*Digital compensation of front-end non-idealities in broadband communication systems*", maart 2010, prom. Marc Moonen.
10. Markulf Kohlweiss, "*Cryptographic Protocols for Privacy Enhanced Identity Management*", maart 2010, prom. Bart Preneel.
11. Dagang Li, "*QoS Enabled Mobility in Heterogeneous Networks*", apr. 2010, prom. Antoine Van de Capelle en Emmanuel Van Lil.
12. Christophe Poucet, "*Dynamic Memory Optimisations for Multimedia Applications*", apr. 2010, prom. Francky Catthoor.
13. Peter Karsmakers, "*Sparse Kernel-based Models for Speech Recognition*", mei 2010, prom. Johan Suykens en Hugo Van hamme.
14. Raf Van de Plas, "*Tissue Based Proteomics and Biomarker Discovery - Multivariate Data Mining Strategies for Mass Spectral Imaging*", mei 2010, prom. Bart De Moor.
15. Johan Loeckx, "*Methods for simulating and analyzing the effects of EMC on Integrated Circuits*", mei 2010, prom. Georges Gielen.
16. Izabella Kuzma Filipek, "*Advanced epitaxial silicon solar cells on low - cost silicon substrates by means of porous silicon internal reflector*", mei 2010, prom. Robert Mertens.
17. Sebastiaan Indestege, "*Analysis and design of cryptographic hash functions*", mei 2010, prom. Bart Preneel.
18. Anneleen Daemen, "*Ontwerpen van klinische besluitvormingssystemen voor kanker op basis van klinische en moleculaire*

gegevens”, mei 2010, prom. Bart De Moor en Dirk Timmerman.

19. Yves Vanderperren, “Development of a digital, low power and flexible UWB receiver”, jun. 2010, prom. Wim Dehaene en Gert Leus.

20. Koen Weerts, “Informatie transport in magnetische nanostructuren voor logische toepassingen”, jun. 2010, prom. Robert Mertens en Staf Borghs.

21. Koen Cornelissens, “Delta-Sigma A/D converter design in nanoscale CMOS”, jun. 2010, prom. Michiel Steyaert.

22. Celso José Dias Cavaco, “Hybrid Layered Nanosystems using Ferromagnetic and Piezoelectric Materials for Magnetic Memory Applications”, jun. 2010, prom. Robert Mertens en Staf Borghs.

23. Mina Deng, “Privacy preserving content protection”, jul. 2010, prom. Bart Preneel.

24. David Novo Bruna, “Exploiting Adaptive Precision in Software Defined Radios”, sept. 2010, prom. Francky Catthoor.

25. Wouter Deburchgraeve, “Development of an Automated Neonatal EEG Seizure Monitor”, sept. 2010, prom. Sabine Van Huffel en Lieven De Lathauwer.

26. Toni Barjas Blanco, “De Demer geregeld met MPC”, sept. 2010, prom. Bart De Moor en Jean Berlamont.

27. Stijn Cole, “Steady-State and Dynamic Modelling of VSC HVDC systems for Power System Simulation”, sept. 2010, prom. Ronnie Belmans.

28. Junfeng Zhou, “Digital design techniques for the improvement of EMC in Automotive electronics”, sept. 2010, prom. Wim Dehaene

29. Pieter Slagmolen, “Image registration for the management of organ motion and deformation in image guided radiotherapy”, sept. 2010, prom. Frederik Maes en Karine Hausterman.

30. Oleksandr Vasylychenko, “Towards the Miniaturization of New Ultra Wideband Small Integrated Antenna Topologies”, sept. 2010, prom. Guy Vandenbosch en Robert Mertens.

31. Arno Keppens, “Modelling and Evaluation of High-Power Light-Emitting Diodes for General Lighting”, sept. 2010, prom. Geert Deconinck en Peter Hanselaer.

32. Kristien Clement-Nyns, “Invloed van plug-in hybride elektrische voertuigen op het elektriciteitssysteem”, okt. 2010, prom. Johan Driesen.

33. Steven Vandeput, “Heart rate variability: linear and nonlinear analysis with applications in human physiology”, okt. 2010, prom. Sabine Van Huffel en A. Aubert.

34. Mike Wens, “Monolithic Inductive CMOS DC-DC Converters: Theoretical Study & Implementation”, okt. 2010, prom. Michiel Steyaert.

35. Gerald Moernaut, “The Shorted Annular Patch as a Global Navigation Satellite System Antenna”, okt. 2010, prom. Guy Vandenbosch.

36. Koenraad Van Reusel, “Context and Technology Bound Motives for the Use of Electricity in Industrial Thermal Processing”, okt. 2010, prom. Ronnie Belmans en Daniël Van Dommelen.

37. Sahar Sahhaf, “Electrical defects in high k / Metal gate MOS transistors”, okt. 2010, prom. Guido Groeseneken.

38. Yu Yang, “Process Characterization and Reliability Issues of Three Dimension-Stacked Integrated Circuit (3D-SIC) Structures”, nov. 2010, prom. Chris Van Hoof en Robert Mertens.

39. Piotr Czarnecki, “Impact of Charging Mechanisms on the Reliability of RF MEMS Devices”, nov. 2010, prom. Bob Puers en Chris Van Hoof.

40. Elke De Mulder, “Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices”, nov. 2010, prom. Bart Preneel en Ingrid Verbauwheide.

41. Peter Tant, “Characterization and Modelling of Gas Discharge Lamps Using a High-Voltage Test System”, nov. 2010, prom. Geert Deconinck en Johan Driesen.

42. Sofie Put, “Radiation Tolerance of Advanced CMOS and Bipolar Technologies”, nov. 2010, prom. Corneel Claeys en Paul Leroux.

43. Riccardo Carta, “Wireless Power and Data Transmission for Robotic Capsule Endoscopes”, dec. 2010, prom. Bob Puers

44. Vanya Van Belle, “Non-Linear Survival Models and Their Applications Within Breast Cancer Prognosis”, dec. 2010, prom. Sabine Van Huffel en Johan Suykens.

45. Marie Garcia Bardon, “Modeling, Fabrication and Characterization of Suspended Gate Transistors”, dec. 2010, prom. Bob Puers en Chris Van Hoof.

46. Elena Andreeva, “Domain Extenders for Cryptographic Hash Functions”, dec. 2010, prom. Bart Preneel.

47. Sebastian Faust, “Provable Security at Implementation-Level”, dec. 2010, prom. Bart Preneel.

48. Steve Stoffels, “Extensional Mode SiGe MEM-Resonators: Design, Modelling and Fabrication”, dec. 2010, prom. Bob Puers en Robert Mertens.