MESSAGE FROM THE DIRECTOR

2018 was a year in which we pushed the boundaries, in every sense of the word. Our researchers not only trod new scientific ground but also expanded into new industry sectors and countries.

Expanding the scientific frontier is an international endeavour where we team up with top researchers in Europe and beyond. Our presence in the highly competitive EU scientific programmes continues to grow, with 14 new H2020 and European Space Agency projects acquired — a record for SnT. This will double our research activity funded by European sources in 2019. And as all eyes turn towards Horizon Europe (FP9), our place at the table for three of the four EU Cybersecurity Competence Networks being launched puts SnT — the only organisation in Europe to achieve such representation — at the heart of global security efforts.

Beyond Europe, in 2018 we welcomed new international partnerships — including QRA, Canada-based developers of systems and requirements engineering technology — and our first grant from a US research funding agency (ONRG). These are clear signs of the value companies see in tapping into our expertise.

Closer to home, we welcomed nine new partners, beginning collaborations in two new sectors, with our first legal and insurance firms, Linklaters and Foyer. Together with our partners we continue to develop Luxembourg’s reputation as an exciting hub for technology-driven service innovation.

At the heart of our activities, as with any knowledge organisation, is people. Our success lies in attracting and retaining talented, dedicated, and highly motivated individuals committed to SnT and Luxembourg in a competitive market. SnT researchers have now accumulated over 100 prestigious best paper and individual awards. Together with our third ERC Advanced Grant, awarded to Prof. Dr. Jean-Sébastien Coron, these show that we continue to rise to the challenge we set ourselves: bridging the worlds of cutting-edge long-term and demand-driven research.

In pushing the boundaries in 2018, we’ve raised the bar for ourselves in 2019, our 10th anniversary year. Join us on social media to keep track of our celebrations.

Prof. Dr. Björn Ottersten
Director, Interdisciplinary Centre for Security, Reliability and Trust
I spent over four years at SnT, and no matter where I work I will always miss my time there. I was honoured to work alongside inspiring researchers such as Prof. Lionel Briand and Dr. Domenico Bianculli. Problem solving is a big part of my work in industry, and it relies heavily upon the skills I learned at SnT, such as scientific thinking, research, and communication skills, as well as a strong sense of determination and persistence.

IEE puts a big emphasis on staying ahead of the curve in software development techniques. This is especially true in our main domain – sensing solutions for automotive applications. So we were excited to get the opportunity to work with Prof. Lionel Briand and his team. One early project focused on automating testing from use case specifications. This helped us cut costs, improve our release quality, and reduce our time to market. The collaboration’s ongoing success led us to hire one of their PhDs, who now leads the creation of new methods and tools to increase our development and management team’s quality and efficiency.

My first and lasting impression of SnT is the diverse skill sets it brings together – I made a lot of friends from different backgrounds from whom I learned a lot. This cultural and technical diversity is good for fostering collaboration and also crucial for identifying novel problems and challenges. I collaborated with talented students and researchers on a variety of computer vision problems, some theoretical, others highly motivated by practical problems. Such a broad exposure is an enabling experience for pursuing a range of carrier paths.

At SMC, a part of our job is covering new technologies and thinking about their benefits for the public. SnT always helps us discover new possibilities, and also to bring them to life. If SnT is working on a new technology, I want to know all about it, because it’ll be a technology that will be here for good!

My first and lasting impression of SnT is the diverse skill sets it brings together – I made a lot of friends from different backgrounds from whom I learned a lot. This cultural and technical diversity is good for fostering collaboration and also crucial for identifying novel problems and challenges. I collaborated with talented students and researchers on a variety of computer vision problems, some theoretical, others highly motivated by practical problems. Such a broad exposure is an enabling experience for pursuing a range of carrier paths.
OUR RESEARCH

Our scientists conduct research with impact. Whether they are pushing the boundaries of scientific knowledge or tackling clearly defined problems with industry partners, their work is rooted in a thorough understanding of societal and industrial challenges. The result: solutions that are applicable, scalable and provide a genuine long-term competitive advantage for companies in Luxembourg and beyond.

Our work aligns with areas of strategic importance for Luxembourg:

AUTONOMOUS VEHICLES
- Smart Drones for all Seasons ................................................................. 10
- Collective Intelligence Helps Drones Rise above Adversity ............... 12
- Bringing 5G to Europe’s Roads ............................................................ 13
- The 360Lab: a Vehicle for Collaboration ............................................ 14
- Patents on the Radar for Automotive Applications ......................... 15

CYBERSECURITY
- How to Stop Ransomware in its Tracks? Take Away its Tools .......... 16
- SnT at Heart of EU Cybersecurity Push ............................................... 17
- It Wasn’t Me: Deniability in a Post-Quantum World ....................... 18
- Law and Technology: How to Police the Privacy Beat .................... 19
- Saving Lives at the Sharp End of Software Engineering ................. 20
- This Californian Life: Software Solutions in Silicon Valley .......... 22

FINTECH
- How to Catch 42,000 Smart Contract Vulnerabilities ................. 23
- Building Privacy into the Blockchain ................................................. 24
- Your AI Advisor: Wealth Management in the 21st Century ............ 24
- Securing Banks against Digital Heists ............................................. 25
- Setting the Standard for Requirements Engineers ......................... 26

INTERNET OF THINGS
- Print Scheduling Solution Cures Mass Customisation Headache .... 27
- 3D Tech for Stroke Survivors ............................................................ 28

SECURE AND COMPLIANT DATA MANAGEMENT
- Digital Medical Systems: Who’s Accessing Your Data? .................. 29
- Fast but Secure Processing for Your DNA ..................................... 30

SPACE RESOURCES
- Satellite Pre-coding Clears Congested Airwaves ......................... 32

Christof Ferreira Torres and Mathis Steichen research blockchain topics.
On a windy, rainy day last autumn, Dr. Miguel Olivares-Mendez and his colleagues Dr. Jose Luis Sanchez-Lopez, Manuel Castillo-Lopez and Maciej Zurad headed to a bridge over a road just outside of Luxembourg City. Having successfully completed field tests of their airplane inspection drone the week before at Luxembourg Airport, they were ready to explore new challenges and applications for their autonomous technology. This time, they were there to assist a team from the University of Luxembourg’s Physics and Materials Science Research Unit conduct a bridge inspection.

While the rain came down, the drones flew more than 30 autonomous flights around the bridge. They inspected the bridge while it was free from vehicles, again with six loaded trucks on it, and a third time after the trucks were removed. Using a variety of sensors including high-resolution RGB (which shows colours true to the human eye) and LiDAR (which produces a 3D model), they gathered the data needed to search for signs that the bridge had sustained deflection.

Any technology is most useful when it is dependable, simple and unobtrusive. And with the rain pouring down, that was exactly what Miguel’s drones were able to provide. The drones worked with one another perfectly, automatically matching their flight paths and communicating with one another to accomplish this shared mission. The materials scientists, meanwhile, could focus on their own part of the job — interpreting the data.

This unobtrusive dependability will make Olivares-Mendez’s smart, goal-driven drones a good fit for an ever-widening range of applications: from art historians examining a UNESCO monument for preservation purposes, to forest management teams deciding when to close a trail, to film crews who need to replicate a particular shot with precision. “What we do here is make things that really work, in real-world conditions,” says Olivares-Mendez with a smile. “And that includes wind and rain.”

"What we do here is make things that really work, in real-world conditions,” says Olivares-Mendez with a smile. "And that includes wind and rain."
Collective Intelligence Helps Drones Rise above Adversity

Without any central organising mechanism, or indeed any direct communication, ants can outperform computers at scouting an area. Using nothing but passive pheromones to communicate, ants are, in fact, so efficient that Prof. Dr. Pascal Bouvry and Dr. Grégoire Danoy have made them the algorithmic model behind their autonomous drones.

Like the ants, these drones explore independently while automatically informing the swarm of their path. Together they can quickly determine whether an area has been completely explored or whether a given path is efficient. But while insects rely on pheromones, the drones use peer-to-peer communication. The algorithms behind this process don’t rely on consensus or a leader. Rather, through a mechanism analogous to how prices emerge in a free market, individual decisions affect the whole group, without the need for explicit plans or directions.

The great advantage this approach has over its insect role model is that it enables collective intelligence not only within a single swarm but also across multiple swarms. Excitingly, it even opens up the possibility of cooperation between different “species” of drones with different capabilities — working on land, water and in the air.

Multi-swarms, unlike choreographed fleet formations, are resilient in complicated, even adversarial conditions. The loss of any individual drone would not cripple the rest of the multi-swarm because the remaining drones would seamlessly adapt. This makes multi-swarms ideal for use, for example, on the heals of natural disasters, where time is of the essence and drones are likely to fall foul of hazards such as falling trees, debris and bad weather. Using a multi-swarm for search-and-rescue operations following a hurricane, earthquake, or tsunami could therefore help responders find victims faster, saving lives.

While ants have been swarming on earth for 92 million years, the multi-swarm drone model is now just entering its proof-of-concept phase. With funding from an FNR Jump Grant and a two million euro investment in the hardware muscle needed for the high-performance computing that powers the algorithms behind the drones, Bouvry and Danoy look forward to pushing their multi-swarms to the limit. “Right now we are finding a balance between maximising the area covered and ensuring connectivity,” says Bouvry, “but I am personally most looking forward to multi-species cooperation.”

Bringing 5G to Europe’s Roads

It has happened to all of us: on New Year’s Eve shortly after midnight, we pick up our mobile phones and try to call or write a loved one. And then, nothing. The network is too crowded and we start the new year offline. Crowds, data-guzzling apps, and an ever-increasing number of connected devices keep pushing modern cellular networks to the limit. While the consequences of an overcrowded network can be irksome, and even downright inconvenient, the stakes are about to rise significantly as automotive companies develop increasingly connected cars.

Connected cars promise to be safer, to reduce traffic, and to be more fuel efficient. They’ll do this by communicating constantly with one another and their environments, sending messages warning of slowdowns, informing one another of the need to form a rescue lane on the highway, or moving in coordinated platoons to reduce wind resistance. But the foundation of all this communication needs to be more robust and dependable than the networks we live with today. Connected cars need to communicate without delays, without dropped messages, and without service holes.

What connected cars need is 5G — the next generation of mobile connectivity — and Dr. Ion Turcanu and his colleagues at SIT are laying the foundations for just that. They have teamed up with more than 30 partners within the H2020 5G-MOBIX and 5G-DRIVE projects to test potential use cases for 5G in connected cars. Results from trials across Europe, China and Korea, will then contribute to the standardisation of the global 5G network.

Dr. Ion Turcanu explains that “connected cars will use a heterogeneous network to communicate with each other.” This means that the car will switch between different communication methods according to current conditions — their speed, weather, location, etc. For example, in a remote region that might mean communicating via satellite, while in dense urban traffic, Bluetooth or a modified form of short-range WiFi might be more appropriate.

This ability to switch seamlessly between communication technologies will ensure that important messages arrive in real-time and that no information gets dropped. Ion and his fellow researchers are developing technologies and requirements that not only meet the already obvious needs of connected cars in the near future but that also anticipate potential future needs, leaving room for even more innovation.
The 360Lab
— A VEHICLE FOR COLLABORATION

“I see myself as an entrepreneur in research,” Dr. Raphaël Frank explains, sat in front of a colorful display of visual data collected by the newly built heart of SnT’s 360Lab: a self-driving car.

“We finished the car in mid-2018 and next we will be building a simulation of it,” Frank continues, outlining the development of the new lab. The simulation will drive the thousands of virtual kilometres required to build a robust dataset before the real car can undertake longer driving trials on public roads.

With industry giants such as IEE, Delphi and CEBI based in Luxembourg, there is a growing need for local graduates with a background in automated driving. So beyond testing the self-driving car — the first of its kind in Luxembourg — Frank looks forward to using the 360Lab to introduce a younger generation to the new field of smart mobility.

Reflecting on his motivation for founding the 360Lab, Frank emphasises that his job is to “bring people together and motivate them to organise.” The goal is to maximise the potential of SnT’s talented researchers, through connection and collaboration. It is the embodiment of the interdisciplinary model at SnT.

Even closer to home, the lab will continue to help researchers at SnT to broaden their horizons, working with colleagues from across disciplines and backgrounds to develop secure solutions for smart mobility.

In the short-term, automotive radar needs to be made affordable, reliable, and robust. It also needs to detect a wider range of objects more reliably. For example, without an adequate system for coping with clutter, a building or a truck will send back a stronger signal than a pedestrian or cyclist — leaving the most vulnerable road users undetected.

This is where the team’s adaptation of Multiple Input-Multiple Output, or MIMO, radar excels. By placing sensors at different locations on the car and programming specific patterns in how they transmit, the MIMO radar can detect the objects that matter most, more reliably. It is a solution for the car of tomorrow, already making us safer today.

In 1904, the German patent office awarded the first patent for radar technology. It took forty years and two World Wars, however, before radar was adopted for submarines, ships, and airplanes. And it is only now that radar is finally being incorporated into automobiles for situational awareness.

Radar still has someway to go before it will be adopted as an automotive standard. First, it must be adapted for interference (irrelevant radio waves from other cars equipped with radar) and clutter (irrelevant objects). Then, radar needs to fit into the restricted space and power limitations of cars. Finally, automotive radar operates at a much closer range than aviation and marine radar.

At SnT, Dr. Bhavani Shankar and his team are working hard to meet these challenges. Their close cooperation with leading sensor manufacturer IEE to develop new automotive radar systems has resulted in no fewer than five patents in the last two years. And this steady output shows no sign of slowing down. “Once radar is standard in cars, we might for example be able to use it to send short emergency messages,” says Shankar as he reflects on future developments.

In 1904, the German patent office awarded the first patent for radar technology. It took forty years and two World Wars, however, before radar was adopted for submarines, ships, and airplanes. And it is only now that radar is finally being incorporated into automobiles for situational awareness.

Radar still has someway to go before it will be adopted as an automotive standard. First, it must be adapted for interference (irrelevant radio waves from other cars equipped with radar) and clutter (irrelevant objects). Then, radar needs to fit into the restricted space and power limitations of cars. Finally, automotive radar operates at a much closer range than aviation and marine radar.

At SnT, Dr. Bhavani Shankar and his team are working hard to meet these challenges. Their close cooperation with leading sensor manufacturer IEE to develop new automotive radar systems has resulted in no fewer than five patents in the last two years. And this steady output shows no sign of slowing down. “Once radar is standard in cars, we might for example be able to use it to send short emergency messages,” says Shankar as he reflects on future developments.

In the short-term, automotive radar needs to be made affordable, reliable, and robust. It also needs to detect a wider range of objects more reliably. For example, without an adequate system for coping with clutter, a building or a truck will send back a stronger signal than a pedestrian or cyclist — leaving the most vulnerable road users undetected.

This is where the team’s adaptation of Multiple Input-Multiple Output, or MIMO, radar excels. By placing sensors at different locations on the car and programming specific patterns in how they transmit, the MIMO radar can detect the objects that matter most, more reliably. It is a solution for the car of tomorrow, already making us safer today.
How to Stop Ransomware in its Tracks?

— TAKE AWAY ITS TOOLS

Right around the time that the WannaCry ransomware began to wreak havoc globally, SnT’s Ziya Alper Genç, had a big idea. “It became my obsession,” says Genç. “I had this idea that I just couldn’t let go.” What Genç dreamt up was a method for preventing ransomware from encrypting files in the first place — a method that would make ransomware viruses like WannaCry harmless.

Ransomware gets onto our devices the same way all malware does — through infected emails, downloads, or unprotected internet connections. Once on a device, the malware’s first step is to produce the cryptographic tools it needs to lock your computer. “When we create basically a whitelist of the programs that are allowed to ask for such tools and then just deny programs not on the list. So ransomware would be denied access to the instruments they need to lock your computer.” By cutting off ransomware’s ability to do its job, the encryption process, you render modern ransomware effectively impotent.

Up to now, there have been just three levels of malware protection. Users can regularly backup their data, anti-malware programs can analyse program behaviour, or anti-malware programs can analyse a program file’s unique signature. Genç’s innovative approach is an additional fourth level of malware protection, a potential game-changer in the anti-malware business. With the support of an FNR Pathfinder grant, Genç has already tested his research’s marketability — the first step to bring a new product to market. Having gathered extensive evidence that his idea works under real-world conditions and against actual ransomware, in 2019 he will follow up with another FNR grant, this time to develop a proof-of-concept.

Anticipating the evolution of ransomware is a must, not a luxury,” adds Dr. Gabriele Lenzini, Genç’s thesis supervisor. So while we will all soon be a little more secure, the fight will go on. But it is comforting to know that by the time the world is again gripped with panic at the next round of hacks, researchers such as Genç will almost certainly have another big idea that they just can’t let go.

SnT at Heart of EU Cybersecurity Push

“I was always an interdisciplinary guy,” begins Prof. Dr. Paulo Esteves-Veríssimo, FNR PEARL Chair. “Electrical engineers, computer scientists and data scientists… they all have promising contributions to make to common problems. The same with dependability and security — it is always a two-way street, where we learn from each other.”

Esteves-Veríssimo’s team has been applying this interdisciplinary perspective to develop trustworthy cutting-edge technologies, from computer multi-cores to biomedical data analysis systems. They build software that is not only dependable (which is to say, safe from accidental malfunctions), but also secure (resistant to intentional hacks).

“We create basically a whitelist of the programs that are allowed to ask for such tools and then just deny programs not on the list. So ransomware would be denied access to the instruments they need to lock your computer.” By cutting off ransomware’s ability to do its job, the encryption process, you render modern ransomware effectively impotent.

Up to now, there have been just three levels of malware protection. Users can regularly backup their data, anti-malware programs can analyse program behaviour, or anti-malware programs can analyse a program file’s unique signature. Genç’s innovative approach is an additional fourth level of malware protection, a potential game-changer in the anti-malware business. With the support of an FNR Pathfinder grant, Genç has already tested his research’s marketability — the first step to bring a new product to market. Having gathered extensive evidence that his idea works under real-world conditions and against actual ransomware, in 2019 he will follow up with another FNR grant, this time to develop a proof-of-concept.

“Anticipating the evolution of ransomware is a must, not a luxury,” adds Dr. Gabriele Lenzini, Genç’s thesis supervisor. So while we will all soon be a little more secure, the fight will go on. But it is comforting to know that by the time the world is again gripped with panic at the next round of hacks, researchers such as Genç will almost certainly have another big idea that they just can’t let go.
IT WASN'T ME:

Deniability in a Post-Quantum World

The quantum supremacy — the point at which quantum computers will begin to outperform traditional computers — is just around the corner. Quantum supercomputers will be able to execute ultra-complex calculations so fast, it will leave our laptops looking like abaci and their processing power will drive dramatic advances in fields such as pharmaceutical, AI research, and much, much more. But when the quantum supremacy comes, one of the first changes it will bring will be to the field of cryptography. Because quantum computing will break it.

The threat to modern cryptography is a threat to everything for which we use cryptography, from securing national, critical infrastructures to everything that enables the original author, receiver, and content of the message all to remain uncertain, so everyone involved can plausibly claim, “it wasn’t me.” Building deniability into computer security is an insurance policy against hacks and leaks, ensuring messages can’t be pinned on you even if the unthinkable happens and somehow your encryption is broken. One way the team has been able to achieve this is by hiding messages in the noise that is inherent in quantum communication itself.

Their strategy, called ‘covert communication’, can help ensure that your communication remains safe even after quantum computers change our technological realities. So, by the time quantum computing is accessible, we will have the tools we need to stay one step ahead of the next challenge to our digital privacy.

...Continued...
Saving Lives at the Sharp End of Software Engineering

According to the last major study in IT project failures, conducted by McKinsey and the University of Oxford, half of all large IT projects “massively blow” their budgets. These large projects (defined as IT projects starting out with a budget of over $15 million) on average exceed their budgets by about 45%. In fact, the 5,400 IT projects studied had a collective cost overrun of $66 billion — more than the GDP of Luxembourg.

In many cases, the report suggests, these failures boil down to a lack of focus and clarity. In other words, they boil down to inadequate requirements. And while the prospect of inadequate requirements leading to project overruns is one thing, the prospect of them resulting in software defects that could cause deaths is quite another.

This is the reality faced by software engineers working in the field of cyber-physical systems, where complex software is deeply intertwined with a physical system in order to perform a vital function. From travelling in airplanes equipped with autopilot, to depending on the anti-lock braking system in our cars, we rely almost every day on these complex, intelligent technologies.

The safety of the people interacting with cyber-physical systems often depends on the embedded software working reliably. Because while a “blue screen of death” on our desktop computers can ruin a day, that sort of a failure in an autopilot could ruin lives. But SnT’s Dr. Sallam Abualhaija and Dr. Shiva Nejati are giving software engineers the tools to make our increasingly cyber-physical world safer.

Dr. Abualhaija is developing a tool for examining software requirements documents written for cyber-physical systems. Her tool lets project managers, software engineers, and government regulators alike comb software requirements documents to check for ambiguity, vagueness, and inconsistencies. What makes her tool particularly useful is that it seeks out only legally binding requirements. This lets all the parties really focus on what matters most.

Dr. Nejati and her team, meanwhile, are building a technology that takes a completed requirements document and turns it into a mathematical representation. By translating English sentences into logical equations, defects in the system can be spotted systematically. With cyber-physical systems, the software can then be checked to ensure it respects all of the systems’ physical limitations as well.

Their projects, conducted in collaboration with Canada-based QRA Corp., a company specializing in the development of enterprise tools for software quality assurance, will help make the cyber-physical systems we interact with every day a whole lot safer.

While a “blue screen of death” on our desktop can ruin a day, that sort of a failure in an autopilot could ruin a life.

“Working with QRA helps us to see beyond the research horizon, all the way to application. It’s like a compass that orients our research efforts towards the problems their customers and engineers have to deal with. It’s fun!”

DR. SALLAM ABUALHAIJA

Research
THIS CALIFORNIAN LIFE:

Software Solutions in Silicon Valley

Decompress. Focus your attention. Expand your perspective. That, Prof. Dr. Yves Le Traon explains, is the aim while on sabbatical. While at the University of California, Berkeley, however, Le Traon did one more thing: he connected.

“I had the opportunity to work not only with Prof. Koushik Sen at UC Berkeley, but also to go to Google and PayPal at least once every week.” Working so closely with industry means keeping your research relevant. “We can work on real solutions for real problems,” says Le Traon. At both Google and PayPal, Le Traon discussed methods for testing code and hunting for bugs in both of their continuous integration processes. The two companies, Le Traon explains, are so different that while you can take inspiration from one project to the other, they need specific solutions.

Google’s Test Automation Process (TAP) ensures that any updates to their vast software do not contain bugs or break existing software functionality. But the process of deciding which software tests to run and when to run them needs optimisation. On top of that, Google needs to understand which tests aren’t working reliably and why — a problem known in software engineering as “flakiness”. Together with Google, Le Traon hopes to develop machine-learning algorithms that will ultimately help engineers select just the best tests to run.

His time at PayPal was different. “PayPal has a different software architecture and therefore different problems.” Like Google, PayPal needs to guarantee the reliability of their software. But while PayPal’s flexible service-oriented architecture is less diverse than Google’s, the potential configurations are more complicated. On top of this, at PayPal software incidents lead to crisis situations that have to be managed urgently. Their engineers need to be able to locate the root cause of an incident, the buggy code, very quickly. Add in the huge flow of real-time data and the task resembles a race to find a needle in a haystack. The collaboration with PayPal focuses, therefore, not only on bug prevention done through improvements in the continuous integration process, similar to Google’s, but also on rapid incident response.

In the coming year, Le Traon will recruit a team of researchers, including two PhD students, to investigate this two-pronged project.

Le Traon describes his research as “multi-core.” It is an interdisciplinary model that consists of exploring diverse real-world contexts. But the common denominator is always people: “Humans are gifted at creating a mess. The challenge in software quality is, therefore, to cope with human nature. That’s what I like about working in software engineering. There is never perfect certainty in software testing; there is always a human element. Therefore, you can never fully formalise or automate it, because you have to face the imaginative way humans tend to act.”

How to Catch 42,000 Smart Contract Vulnerabilities

“In some ways with Blockchain it is like we went 30 years back in time,” explains doctoral researcher Christof Ferreira Torres. “Lessons from 30 years ago ought to apply to blockchain programming, but people have moved so fast they didn’t think of it.” Remember, for example, the panic around the turn of the millennium? Because storage was expensive, computers were only programmed to work with the last two digits of the date, e.g. “99” instead of “1989”. Computers then needed to be updated en masse to ensure that on 1 January 2000 they wouldn’t believe we had time traveled back to 1900.

Jump forward 19 years to today’s Ethereum blockchain system. Its primary programming language, Solidity, suffers from a similar error. It has failed to account for “integer overflows” — incidents where the number of digits the computer can store is not adequate for representing the true sum. Within Ethereum’s smart contract ecosystem, this is a potentially dire problem. A malicious actor could exploit an integer overflow to leave an account empty. That would be as simple as sending a target account the exact number of coins needed to “overflow” their balance back to “10000”. The other direction is, however, also possible; a malicious actor could subtract a coin from their empty account, leaving themselves with “9999” coins after the “10000” counter is wound back by one.

Today, most computer programming languages have built-in guard rails against integer overflow and underflow. And indeed, the next generation of Ethereum’s programming language — Vyper — will too. But the development of that language is still ongoing and some programmers might prefer to stick with Solidity anyway. Moreover, the contracts already deployed in Solidity will, by the very nature of the blockchain, continue to exist forever.

This is where Torroes can help. Working with industry partner Banque et Caisse d’Epargne de l’État, he has developed a tool that works with Solidity — the most widely used programming language on the Ethereum blockchain — to check for integer over- and underflows. It does this by producing a control flow graph of the program, and when the tool detects a problem it can follow it back along its branch to its source. This allows Solidity programmers — and those inheriting or acquiring older contracts — to deal with errors in their coding much more efficiently.

The program has, in fact, already found 42,000 contracts with integer over- and underflow bugs — in one case even identifying a potential $30,000 error. “We were floored when we found that,” says Torres, laughing. “It really highlights what a big impact our tool could have in the real-world.”

Christof Ferreira Torres

---

Contract Vulnerabilities

How to Catch 42,000 Smart Contract Vulnerabilities

---
Building Privacy into the Blockchain

On 20 January 2018, two computer scientists boarded a propeller plane in Wisconsin with an air-gapped laptop, a digital counter, and some radioactive material from Chernobyl. They were just one small part of what the developers of Zcash call “the ceremony” — an elaborate procedure to produce a completely random and secret cryptographic key. This key is the backbone of Zcash cryptography, which promises to provide the same functionality as Bitcoin but with significantly improved privacy.

The thing is: despite the elaborate ceremony, even Zcash fails to live up to its promise of privacy. “Cryptocurrencies look anonymous, but they are not,” explains doctoral researcher Sergei Tikhomirov. That’s because the very way transactions occur on their networks can provide a savvy observer with potentially identifying information.

Which isn’t to say that cryptocurrencies cannot ever fulfill their promise of anonymity for all. Rather, as Tikhomirov points out, achieving anonymity is a “gradual process” that needs to be built into technological foundations.

So Tikhomirov, with funding first through a Zcash Foundation Grant and an ERC Grant, spends many of his days working as a white-hat hacker. He searches for ways to exploit information on the blockchain at the network level (for example: how, where, and when a transaction is conducted). He is on the lookout for patterns in blockchain network traffic that would allow him to unmask users, many of whom believe their transactions are totally anonymous.

Once he has found a vulnerability, he suggests countermeasures at the level of the “wallet” and the end user, leading to better privacy in blockchain transactions. But he also makes suggestions to improve the foundations of the blockchain system (called the “core”), moving the entire system closer to offering true anonymity.

Someday, when blockchain-powered currencies are more seamlessly incorporated into our everyday lives, Tikhomirov’s work will help make privacy a real option. “Solutions like the GDPR apply old frameworks to new problems,” points out Tikhomirov. Rather, by building privacy into the technological foundations of the blockchain, maybe we can all look forward to a future where we can make genuinely empowered choices about retaining or waiving our anonymity.

Securing Banks against Digital Heists

On the evening of 10 July 2016, two men made their way through Typhoon Karen to an ATM in Taipei. After the men listened for a few minutes, the machines began to spit out cash. Hundreds of euros worth in cash. Quickly, the men picked up the money, stuffed it into a bag, and took off. They were two of fifteen “money mules” completing the final step in one of the Carbanak gang’s high-tech bank heists.

So forget Ocean’s Eleven. Forget Bonnie and Clyde. Today’s most successful bank robbers work with software code, not a pick lock. And to protect themselves, banks rely on security requirements engineers to draw up the digital equivalent of super-secure bank vaults. These engineers determine the who, where, and how of data accessibility. They need to make sure that hackers cannot access their internal systems to siphon bank balances, transfer money or take control of ATMs. Before a security requirements engineer’s job is done, they have considered hundreds of different parameters and developed a holistic security strategy.

And yet, the process is highly individual. Two engineers might do the same job in slightly different ways. Often even a very capable security requirements engineer might not be able to explain why an existing system is like it is — it seems almost impossible to reverse-engineer the logic behind a set of security requirements. But Dr. Mehrdad Sabatzedeh and his colleagues have begun to change that. Together with their partners at BGL BNP Paribas, they are building a tool that provides automated decision-support on specifying security requirements from beginning to end. The aim: to standardise and streamline the security requirements engineering process.

The resulting standardisation will not only make it easier for new team members to understand the security concerns and build upon the existing groundwork more quickly. It will also help ensure that security decisions are applied consistently across whole organisations. All of this is achieved in three broad stages. The tool will first help to define the existing security architecture and indicate what features are desirable according to its logic. Second, using machine learning, it will identify complementary techniques and recommend how to implement them. Finally, it will use natural language processing to extract information from related textual sources, identifying further relevant security measures.

The project is an example of modern artificial intelligence applied to an ultra-complex application environment — made possible by BGL BNP Paribas Bank, who granted unprecedented access to their expert security team. It is a unique partnership that has enabled computer-supported security assessment at a level previously unseen in research.

### Your AI Advisor: Wealth Management in the 21st Century

In collaboration with BGL BNP Paribas, he is developing a tool that will use existing market conditions to suggest relevant products, advise on courses of action and even warn about risk in a portfolio. But this isn’t a recommendation engine like you might know from Amazon. That’s because in finance, the products themselves are not static, and customer preference is influenced just as much by external economic and political factors as by previous customer choices or profile. Bhadauria’s algorithms, he explains, therefore look at customer portfolios “as if they were texts and use natural language processing to then identify how other investors have invested their own portfolios based on external contextual input, like stock-market conditions.” This system therefore takes into account the historical actions of an investor as well as the market situation at the time of those actions to learn their preferences and needs.

“Another thing that is great about our system is that ‘fairness’ is built in,” says Anne Goujon, project supervisor and Director of BGL BNP Paribas’s Data Science Lab. “Because we look only at the contents of the portfolio and the situation in markets, we make suggestions without considering customer demographic profile.” Which is a good news because in the end our needs are all a lot more alike than we sometimes realise, and we all deserve the best possible decision-making support in our financial lives.

Anne Goujon, Anshuman Bhadauria

In 2011, shortly after a new no-frills budget bank was founded in the UK, the CEO found himself in an unexpected situation. Customers were pouring in, but not just for no-cost checking accounts. Hundreds of high-net-worth individuals were leaving prestigious private banks to free themselves from unhelpful advice.

The heart of private banking has always been personalised customer service. But times are changing and private banking must too. SnT’s Anshuman Bhadauria has built his PhD research around bringing the customer service ethos of traditional private banking into the 21st century.

In collaboration with BGL BNP Paribas, he is developing a tool that will use existing market conditions to suggest relevant products, advise on courses of action and even warn about risk in a portfolio. But this isn’t a recommendation engine like you might know from Amazon. That’s because in finance, the products themselves are not static, and customer preference is influenced just as much by external economic and political factors as by previous customer choices or profile. Bhadauria’s algorithms, he explains, therefore look at customer portfolios “as if they were texts and use natural language processing to then identify how other investors have invested their own portfolios based on external contextual input, like stock-market conditions.” This system therefore takes into account the historical actions of an investor as well as the market situation at the time of those actions to learn their preferences and needs.

“Another thing that is great about our system is that ‘fairness’ is built in,” says Anne Goujon, project supervisor and Director of BGL BNP Paribas’s Data Science Lab. “Because we look only at the contents of the portfolio and the situation in markets, we make suggestions without considering customer demographic profile.” Which is a good news because in the end our needs are all a lot more alike than we sometimes realise, and we all deserve the best possible decision-making support in our financial lives.

Anne Goujon, Anshuman Bhadauria

In 2011, shortly after a new no-frills budget bank was founded in the UK, the CEO found himself in an unexpected situation. Customers were pouring in, but not just for no-cost checking accounts. Hundreds of high-net-worth individuals were leaving prestigious private banks to free themselves from unhelpful advice.

The heart of private banking has always been personalised customer service. But times are changing and private banking must too. SnT’s Anshuman Bhadauria has built his PhD research around bringing the customer service ethos of traditional private banking into the 21st century.

In collaboration with BGL BNP Paribas, he is developing a tool that will use existing market conditions to suggest relevant products, advise on courses of action and even warn about risk in a portfolio. But this isn’t a recommendation engine like you might know from Amazon. That’s because in finance, the products themselves are not static, and customer preference is influenced just as much by external economic and political factors as by previous customer choices or profile. Bhadauria’s algorithms, he explains, therefore look at customer portfolios “as if they were texts and use natural language processing to then identify how other investors have invested their own portfolios based on external contextual input, like stock-market conditions.” This system therefore takes into account the historical actions of an investor as well as the market situation at the time of those actions to learn their preferences and needs.

“Another thing that is great about our system is that ‘fairness’ is built in,” says Anne Goujon, project supervisor and Director of BGL BNP Paribas’s Data Science Lab. “Because we look only at the contents of the portfolio and the situation in markets, we make suggestions without considering customer demographic profile.” Which is a good news because in the end our needs are all a lot more alike than we sometimes realise, and we all deserve the best possible decision-making support in our financial lives.

Anne Goujon, Anshuman Bhadauria

In 2011, shortly after a new no-frills budget bank was founded in the UK, the CEO found himself in an unexpected situation. Customers were pouring in, but not just for no-cost checking accounts. Hundreds of high-net-worth individuals were leaving prestigious private banks to free themselves from unhelpful advice.

The heart of private banking has always been personalised customer service. But times are changing and private banking must too. SnT’s Anshuman Bhadauria has built his PhD research around bringing the customer service ethos of traditional private banking into the 21st century.
Setting the Standard for Requirements Engineers

The first step towards good software is good communication. Requirements engineers, who work at the earliest stage of software development, work closely with clients to develop ‘what’ software should do before it is passed on to developers to work out the ‘how’. Like architects creating blueprints before construction, requirements engineers create outlines that software developers then turn into the code.

While architects, however, have universal standards for blueprints — nobody, after all, wants to get feet and metres confused — requirements engineers do not. Most requirements engineering processes are bespoke. On top of this, business-oriented clients and computer-science-oriented software professionals can miscommunicate, making the requirements writing process even more complicated. When all is done, there is a good chance that some requirements may end up being unclear, incomplete or even contradictory. Errors in requirements engineering have a ripple effect on the software development process. These errors can make multiple, unplanned project iterations necessary and result in significant headaches. This ultimately puts projects in danger of being over budget, below expectations, or even completely abandoned.

But what if requirements could be made more consistent? More complete? What if there were a “blueprints” standard that requirements analysts could follow?

This is exactly what SnT researchers in the field of software verification and validation, including Dr Mauricio Alferrez, Alvaro Veizaga, Dr Mike Sabetzadeh and Prof. Dr. Lionel Briand are working to achieve. Together with financial firm Clearstream and IT coaching company, Escent, they are putting together a tool that guides requirements engineers through the process of developing and testing software requirements for the financial and insurance sectors. This will help identify unclear text, contradictory requirements, and inefficient workflows. Their tool will employ artificial intelligence techniques to derive a model of how the envisioned software will work. This model provides an ideal mechanism for uncovering potential errors and omissions through such means as automated testing. The resulting technologies can be used from the very beginning of the requirements gathering and documentation process to guide requirements engineers in consistently following best practices and planning for later software verification and validation activities.

By ensuring that requirements are complete, clear and verifiable before they are handed down to software developers, the whole development process can be streamlined — and latent problems in the software can be fixed early so software turns out as correct and complete as possible the first time around.

Print Scheduling Solution Cures Mass Customisation Headache

We increasingly choose to print only our most important documents — documents that we hope will stand out, like colourful posters; that have a strong emotional significance, like wedding invitations; or that mark major personal achievements, like thesis dissertations. That’s because paper can break through electronic distractions and hold someone’s full attention. Indeed, as it turns out, the digital revolution is already so complicated that it can be adjusted to reflect the actual situation on the factory floor. It can accept changes in priorities, such as the arrival of rush orders, or even a shift in emphasis from quality to cost minimisation. Once adjusted, it performs a rapid search for an optimised workflow. It is the flexible tool printing factories need to execute the mass customisation of products.

As Prof. Dr. Holger Voos explains, while “printing production planning works well when it is formalised as an abstract numerical problem, managers have found that these abstract models just don’t work well with the actual chaos on the ground.” With some factories turning to conventional forms of more or less manual scheduling, the industry needed a tool that could handle high volumes of orders and execute remodelling. And they needed it soon, because, as Voos continues, “a perfect solution is not helpful if it comes too late. What printing factories needed was a very good solution, fast.”

They needed an algorithm that was well, more down-to-earth. So that’s just what Voos and his team at SnT have built for them. Unlike some other approaches, their algorithm reasons based on practical constraints that can be adjusted to reflect the actual situation on the factory floor. It can accept changes in priorities, such as the arrival of rush orders, or even a shift in emphasis from quality to cost minimisation. Once adjusted, it performs a rapid search for an optimised workflow. It is the flexible tool printing factories need to execute the mass customisation of products.

Working in close cooperation with their partners at Rogier — a developer of print management systems — Voos and his team have developed an algorithmic solution so flexible that it can be applied broadly to other industries in need of a flexible solution for mass-market customisation. It is a high-tech solution with its feet on the ground.
3D Tech for Stroke Survivors

Walking into the 4th floor conference room at St.T, I was expecting to see something big and unusual. I was on my way to participate in a trial of 3D motion detection and body representation for a piece of software that promises to improve the recovery process for stroke patients in Europe. But opening the door, all I saw was a small black box like a DVD player and a big screen monitor; it all seemed rather ordinary.

The fact that the hardware setup for the STARR project’s software is so economical is part of its brilliance. Through the HI2020 STARR project (short for Decision Support and self-mAnage- ment system for otRke survivoRs), St.T is developing a home-support system for stroke patients and their doctors. It provides real-time feedback as the patient performs physical therapy exercises in the comfort of their home, and it gives doctors the data they need to ensure patient safety. Should the patient fall down or deviate wildly from their regular motion, their doctor or therapist can be notified immediately. They can check in on patients personally or even send an ambulance to address the situation.

“The whole process is always driven by the patients first and foremost. That’s what is really important to us in this project,” says Dr. Aoua- da. Take the posture feedback, for example: “That was something patients explicitly wanted, so we made it happen. And in the end, we turned that work into an award-winning paper.” It is a human-centred approach to academic excellence in computer science.

It isn’t just the equipment that resembles a video game. What patients see on the screen is reminiscent of a game too: a stick person mirrors their movements, moving as they move, with limbs turning green, yellow, and red. This cartoon avatar tells patients if they are performing their exercises correctly; lean too far to one side and the spine turns yellow. Bend over and the spine turns red.

What is especially innovative about this system is that the “ideal” motion the patient should perform is not only measured against a physical therapist’s example, but also against the start of their program, patients perform their physical therapy exercises with the unaffected side of their body. Their own dexterity is then taken as the baseline that they are working to achieve with the affected side. This process is powered by the team’s movement optimisation feedback algorithm. “That has been the main building block” says Dr. Djamila Aouada, the project leader.

Beyond guiding patients in their exercises, the setup ensures patient safety. Should the patient fall down or deviate wildly from their program, patients perform their physical therapy exercises with the unaffected side of their body. Their own dexterity is then taken as the baseline that they are working to achieve with the affected side. This process is powered by the team’s movement optimisation feedback algorithm. “That has been the main building block” says Dr. Djamila Aouada, the project leader.

Beyond guiding patients in their exercises, the setup ensures patient safety. Should the patient fall down or deviate wildly from their regular motion, their doctor or therapist can be notified immediately. They can check in on patients personally or even send an ambulance to address the situation.

“The whole process is always driven by the patients first and foremost. That’s what is really important to us in this project,” says Dr. Aoua- da. Take the posture feedback, for example: “That was something patients explicitly wanted, so we made it happen. And in the end, we turned that work into an award-winning paper.” It is a human-centred approach to academic excellence in computer science.

In June of 2018 security researchers disco- vered that the American marketing company Exactis had inadvertently leaked the private information of over 218 million people. Not only was the data leak massive, but for the vast majority of people, the first time they heard of Exactis was when they found out the company had leaked their personal information to the world.

Data breaches increasingly affect people who had no idea that the company in question ever had their data. This is because data is often passed along channels that we as consumers — who pay for the services we love with our data — are not made aware of. While this sort of surprise is bad enough when just your email address is leaked, what if it were part of your health records? Your pregnancy results? HIV status? Prescription records?

While digitalising medical records can be a tool to empower patients, it is essential that patients understand (and ultimately control) who then gets to access that data. Even with this transparent handling of data, as required by the new European GDPR law, we might not be able to exclude the possibility of accidents, but we can preclude the possibility of unplea- sant surprises.

But what exactly counts as “transparent” anyway? Is the usual fine print, supposedly defining what data is being collected, why and by whom, good enough? While researchers have been examining standards of data privacy (including concepts of transparency) for years, they have not all been using a common vocabulary, let alone a common framework. And that’s where doctoral candidate Dayana Spagnuelo comes in.

In her research — conducted under the super- vision of Dr. Gabriele Lenzini and in collaborati- on with researchers in Luxembourg, Brazil, and Portugal — she examined the various ways transparency has been defined and assessed. She also clarified the building blocks of trans- parency, such as the availability, portability, and readability of information, the verifiability of a system, and the auditability of privacy policy compliance.

Using her definition of transparency and outline of its building blocks, Spagnuelo developed a checklist of requirements that developers can reference when creating transparent-by-design digital medical systems. She also developed metrics by which they can evaluate transparency in existing systems. This means that we can look forward to a future where we know exactly where, how, and by whom our medical data is processed. While we might never have control over all contingencies, we can expect fewer surprises and will be able to hold the individuals and corporations who do have our most valuable data to account.

Dr. Enjie Ghorbel, Dr. Abd El Rahman Shabayek, Renato Baptista, Dr. Djamila Aouada

Dr. Dayana Spagnuelo

Digital Medical Systems: Who’s Accessing Your Data?
Fast but Secure Processing for Your DNA

Because sequencing your genome should empower you as an individual, our researchers are putting control over the data where it belongs — in your hands.

Humans have much more in common with one another than we sometimes imagine. Indeed, only 3% of DNA is unique to a person, while the balance is shared with the rest of humanity. But that 3% is powerful. It determines eye color, height, and bone structure. It can make you smarter and healthier than your neighbours. Or it could give you a tendency to put on weight, an inability to digest lactose, or a predisposition to developing a number of life-threatening diseases. As our understanding of the genome develops, medicine is searching for treatment options guided by the patient’s genetic makeup. Already companies sell kits to map your genome in the comfort of your own home, using equipment smaller than a loaf of bread. Other “mail-order” services map your genome in the lab.

To date, the process has focused on complete, accurate results. But an important question remains: what happens to those results? Who controls the data? How should it be stored? These privacy and security driven questions have hardly been considered. As researcher Dr. Jérémie Decouchant puts it, “I would like info on my DNA, but I, as a computer scientist, don’t trust the stakeholders or their computing infrastructures.” There is, after all, no data more sensitive than that 3% of your genome.

That’s why Decouchant and doctoral researcher Maria Fernandes have developed a new methodology for human genome analysis that keeps 10% of the information produced truly secure. 90% of the genome can be processed as usual — it is, after all, information that is common to all humans. The remaining 10% (including that discriminating 3%) can then be processed either locally or in a secure enclave in the cloud. This system has the important advantage of leaving private data in the owner’s control, and crucially, it is only marginally slower than the standard way of processing the human genome.

With this control, you decide who gets to see your data and when. You could take any information that might be relevant to a nutritionist, for example, with you to your appointment and would not have to reveal unrelated details. And you could ensure that insurance companies, hospitals or even employers cannot use your data to make decisions about your premium, eligibility or treatment options.

Because sequencing your genome should empower you as an individual, Decouchant and Fernandes are putting control over the data where it belongs — in your hands. And having filed a patent last year and recently launched a Proof of Concept funded by FNR, they are looking forward to taking their work another step nearer to application. So consider waiting just a bit longer before you get your genome sequenced. A better approach is just a short way off.
Satellite Pre-coding Clears Congested Airwaves

Access the Internet wherever and whenever you need to, whether in a plane or out at sea.

"Buy land, they’re not making any more of it." Mark Twain’s famous advice was probably sound for the generation that came after him. But then, things changed. While land remains a finite resource, the way we use it would hardly be recognisable to Twain. We work and live, for example, in buildings hundreds of metres taller than anything he could have imagined. Yes, physical space remains finite. It is the way we relate to that space and use it that has changed dramatically.

Like land, the radio frequency spectrum, including the frequencies used for satellite communications, is also a finite resource. And each year, the demands we put on it have been increasing; telecommunications companies have been preparing for a coming frequency crunch. But thanks to SnT’s SERENADE project, they might not need to look quite as far to find the satellite bandwidth they need — because the way they utilise frequencies they already have is about to change.

Up to now, telecoms have had to minimise interference by leaving dedicated buffer frequencies empty and then sending only one signal on a frequency at a time. Last year, however, the FNR-funded project SERENADE, led by Dr. Symeon Chatzinotas with Dr. Juan Carlos Merlano Duncan, developed a method of altering wavelengths to cancel out the anticipated inference, leaving simultaneous messages crystal clear.

These precise alterations, called “pre-coding”, are calculated based on interference information received along with test signals already being sent for synchronisation purposes. Moreover, this pre-coding does not require any alterations to existing satellites — it can be accomplished with simple processing power upgrades at the earthbound transmitter.

Pre-coding transmissions in this way allows multiple transmissions to be sent simultaneously on the same frequency. The end effect for frequencies is like that of the skyscraper for land: you can layer multiple transmissions on top of each other. Just as skyscrapers have elevators with buttons to reach the floor you need, these layered transmissions arrive with the keys needed to clean up the signal to focus on any given one. This means telecoms can make significantly better use of their allocated frequencies.

Together with SES and Airbus, and with funding from the European Space Agency, SnT’s LiveSatPreDem project is implementing the theoretical framework produced by SERENADE. So perhaps very soon we can expect a significant improvement in the quality of Internet on airplanes, boats and in remote regions — or more prosaically, as Dr. Nicola Maturo, researcher on the LiveSat project said with a smile, “with these data-capacity improvements, before long we will be able to receive a lot more channels on Ultra-HD satellite TV.”

“Buy land, they’re not making any more of it.” — Mark Twain
SnT has a broad range of vehicles for ensuring that we play a central role in Luxembourg’s innovation ecosystem. Whether we are putting our researchers in direct contact with industry through our Partnership Program and business network, or encouraging entrepreneurial activity all the way through from patenting to spin-offs, we ensure that our research has socio-economic impact.

Jacek Plucinski and Jose Soares bridge the gap between research and industry.
SnT Partners 2018

In 2018 SnT's Partnership Program counted 43 industry and public partners. In addition to collaborating on projects with our research partners, we also foster communication and knowledge sharing between the key players in Luxembourg's innovation ecosystem with our networking partners.

In 2018, nine new partners joined the SnT Partnership Program. Meet the latest companies to join the program:

**Cebi** is a global developer and manufacturer of electromechanical components for the automotive and household appliance industries. SnT researchers will work with Cebi Luxembourg S. A. to make Industry 4.0 a reality at their flagship factory in Luxembourg.

**Foyer S.A.** is a leading player in Luxembourg in the local life and non-life insurance market, with activities in several European countries through insurance, benefit protection insurance and wealth management. In two projects, SnT will work on data analytics for personalised insurance, and risk assessments based on driving data fused from multiple sources while maintaining user privacy.

**Linklaters** is a leading global law firm, supporting clients in achieving their strategies wherever they do business. This project will help organisations come to terms with the implications of the new GDPR regulation by converting the legal texts into an intuitive and machine-analysable format, opening the way for computer-assisted compliance analysis.

**VNX Exchange** is a marketplace and trading platform for tokenised venture capital assets, aiming to unlock liquidity for the venture capital industry. Through this partnership, SnT researchers will design new IT frameworks facilitating the secure exchange of digital assets on blockchain networks.

**Huawei** is a leading global provider of ICT infrastructure and smart devices. In this project, SnT researchers will develop automated tools for testing Android smartphone updates, replacing the painstaking manual process of identifying “regression faults” in Android OS updates.

**The LHoFT Foundation** is a public-private sector incubator initiative that drives technology innovation for Luxembourg’s financial services industry, connecting the domestic and international FinTech community to develop solutions that shape the world of tomorrow. This networking partnership will enable SnT researchers to interact with the start-ups and institutions making use of the FinTech innovation hub.
**Partnership Program**

Public and private organisations collaborate with SnT to open up new possibilities using cutting-edge concepts in computer science and ICT. Guided by a partner’s domain knowledge, SnT researchers bring their expertise to bear on specific industry pain points, from the need to improve efficiency in software testing to challenges in making smart manufacturing a reality.

**WHY COLLABORATE WITH SNT?**
This combination of scientific excellence and domain knowledge results in technological solutions that are applicable and scalable in real contexts, providing a long-lasting competitive advantage for companies in Luxembourg and beyond.

**MORE PRECISELY, PARTNERS BENEFIT FROM:**
- Joint research results and Intellectual Property (IP) commercialisation rights
- Leveraging of public research funding
- Scientific knowledge and research excellence
- Access to research equipment
- Highly specialised talent for future hiring needs
- IP management expertise
- Networking across Luxembourg’s innovation ecosystem

**HOW DOES A PARTNERSHIP WORK?**
The Partnership Program provides an attractive form of collaboration with SnT. Project costs are split 50/50, and the Program leverages European and national public research funding.

1. SnT and the partner define a three-to-four-year project, addressing a specific industry challenge and targeting results of long-term scientific value
2. SnT recruits an Industrial PhD candidate for the project. S/he will conduct applied research within a team of experienced SnT scientists
3. A steering committee monitors and evaluates the project, ensuring that activities remain in line with project goals
4. Experts in Intellectual Property at SnT work with the partner to identify and protect research results with potential commercial value

**A KEY PART OF OUR RESEARCH MODEL**
Our scientists are inspired by the challenge of conducting academic research in the face of industry realities. These collaborations provide a different perspective, allowing them to tackle well-defined problems within well-understood domains. The results? IP for licensing and commercialisation, and award-winning papers and theses.

Jacek Plucinski, Isabelle Chesnay, Dr. Marc Lemmer and Jose Soares work on technology transfer and partnership development.

---

**Boosting the Innovation Ecosystem**

**CULTIVATING ENTREPRENEURSHIP**
Our researchers are encouraged to be entrepreneurs. Regular training sessions on IP commercialisation together with ideation camps at the University of Luxembourg Incubator help them to develop the skills they need to build a business from an idea.

On the practical side, IP experts are always on hand to help researchers navigate the winding road from research results and invention disclosures through to proof of concepts and spin-offs.

**OUR SPIN-OFFS**

**A STRONG NETWORK**
Innovations don’t make it all the way from discovery to commercialisation by chance – the transition requires a robust network of players from across the research and innovation ecosystem.

To make this network a reality, SnT works closely with government, trade offices, SMEs, large corporates, and entrepreneurs and investors, organising events and other platforms to share knowledge (see all events on pages 46-47).

In 2018, SnT was delighted to launch a new collaboration with The Luxembourg House of Financial Technology (LHoFT), bringing our researchers into daily contact with the firms and institutions making use of Luxembourg’s FinTech incubator.

> www.motion-s.com

**SPOTLIGHT ON MOTION-S**
2018 was a landmark year for SnT spin-off Motion-S, which closed its first round of investment with one million euros from FEBIAC, the federation of automotive manufacturers and importers in Belgium and Luxembourg.

Motion-S collects, augments and analyses mobility data for the insurance market. The spin-off will now take the next step in its journey, expanding its data services to encompass the full range of modern mobility, from car sharing to fleet management and predictive maintenance.

> www.motion-s.com
The University of Luxembourg launched its Interdisciplinary Centre for Security, Reliability and Trust (SnT) in 2009. SnT has a two-fold approach focusing on both collaborative demand-driven research and high-risk, long-term research projects. The Centre brings 290 staff, from some 40 nationalities, together in Luxembourg. Nine research groups with complementary expertise tackle the biggest problems facing industry and society in Luxembourg and beyond.
Organisation

The SnT Advisory Board advises the President of the University of Luxembourg on the Centre’s activities. The SnT Director, supported by the Management Board (see pages 44–45), is responsible for the day-to-day management of the Centre.

For me, SnT is one of the strongest arguments for Luxembourg’s achievements in terms of research excellence. The list of international players that have chosen SnT as a research institute is truly impressive and because of SnT, I can tell our international partners: “Yes, we have innovation in Luxembourg, we’re even a technology exporter!”

Location and Labs

SnT is strategically located on two sites – one in the centre of Luxembourg’s Kirchberg financial district and one on the University’s vibrant Belval Campus.

When SnT researchers are refining their work for real-world application, they can test and validate their ideas on state of the art hardware and software in SnT’s laboratory infrastructure. To date, we count some 10 labs that offer unique environments for work relating to computer vision, satellite communications, autonomous driving, aerial robotics, server networks, cybersecurity and safety and Artificial Intelligence.
Leadership

SnT’s Management Board consists of internationally renowned experts from across the ICT landscape. We provide them with a platform to do research that matters.

Under their leadership, computer scientists at SnT conduct outstanding research driven by industry needs, collaborate on interdisciplinary solutions to complex problems, and nurture the next generation of specialists in ICT.

**SnT’s Management Board**

- **PROF. DR. BJÖRN OTTERSTEN, SNT DIRECTOR**
  Signal Processing and Communications Research Group (SIGCOM)
  SIGCOM focuses on signal processing in wireless communications, radar and computer vision. Applications range from satellite systems to vehicular sensors and 3D body modelling.

- **PROF. DR. LIONEL BRIAND, SNT VICE-DIRECTOR**
  Software Verification and Validation Research Group (SVV)
  SVV develops novel and effective techniques to ensure that software systems are reliable, safe, secure, and compliant. Their work heavily relies on artificial intelligence and is done in collaboration with partners in domains such as satellite, automotive, finance, public service, and legal.

- **PROF. DR. ALEX BIRYUKOV**
  CryptoLux Research Group
  CryptoLux strives for a greater understanding of how cryptosystems get broken in the real world, how they can be designed and implemented to better resist attacks, and how they should be used to build secure systems and networks.

- **PROF. DR. THOMAS ENGEL**
  Networking Research Group (NetLab)
  NetLab works on privacy by distribution, network and system security, Supervisory Control and Data Acquisition and cybersecurity, IoT, vehicular communication and multimodal traffic management, and wireless networks and mobile security.

- **PROF. DR. PAULO ESTEVES-VERÍSSIMO**
  Critical and Extreme Security and Dependability Research Group (CritiX)
  CritiX investigates methods and architectures to ensure systems resilience in an automated way, keeping them safe, secure and operational even in the face of unexpected threats, like when compromised by highly skilled and well-equipped hacker attacks. Such systems include autonomous driving, e-health, blockchains, or powergrids.

- **PROF. DR. YVES LE TRAON**
  Security, Reasoning and Validation Research Group (SERVAL)
  SERVAL focuses on three areas: testing, debugging and repair techniques; mobile security and reliability using static code analysis and machine learning; and model-driven engineering with a focus on analytics and artificial intelligence. They work on applications ranging from automated Android app debugging to IoT data analytics with decision making capabilities.

- **PROF. DR. PETER Y. A. RYAN**
  Applied Security and Information Assurance Research Group (APSIA)
  APSIA specialises in the mathematical foundations of cybersecurity and the design and modelling of security protocols (classical and quantum). Applications range from electronic voting systems to privacy enhancing technologies. The group also performs interdisciplinary research in cybersecurity, with close collaborations with social sciences, physics and law.

- **DR. RADU STATE**
  Service and Data Management in Distributed Systems Research Group (SEDAN)
  SEDAN works on blockchain, cloud computing, and data analytics, developing new architectures, algorithms and approaches for dealing with ever-increasing volumes of data. Applications range from blockchain infrastructures for KYC and digital trading to analysis and visualisation of big data for public utilities.

- **PROF. DR. HOLGER VOOS**
  Automation and Robotics Research Group
  Automation and Robotics investigates approaches to perception, control, adaptation and learning for networked autonomous cars, service robots, drones and space robots. In large-scale distributed systems it works on novel distributed estimation, control and optimisation algorithms.

**Operations**

- **ISABELLE CHESNAY**
  Administration
  As Head of Office, Isabelle Chesnay guarantees the efficient support of SnT’s researchers from an administrative perspective, while also complying with University policies and procedures.

- **DR. MARC LEMMER**
  Technology Transfer
  Marc Lemmer’s team shapes the Centre’s interaction with industry, enables IP commercialisation and fosters entrepreneurship throughout the country and at international level.
Events

Distinguished Lectures

- Prof. Stephen Boyd (Stanford University, USA): Convex Optimisation, July 2018
- Prof. Bryan Ford (Swiss Federal Institute of Technology in Lausanne, Switzerland): Coins, Clubs, and Crowds: Scaling and Decentralisation in Next-Generation Blockchains and Cryptocurrencies, December 2018
- Prof. Francois Coallier (École de technologie supérieure, Canada): Engineering Challenges in IoT based Systems, December 2018

Scientific Events

- Flysec: Proof of Concept at lux-Airport by Aurel Machalek, February 2018
- SatNEx IV Summer School 2018 by Dr. Bhavani Shankar, Dr. Symeon Chatzinotas and Prof. Dr. Björn Ottersten. In collaboration with SES, May 2018
- International Conference on Dependable Systems and Networks (DSN 2018) by Prof. Dr. Paulo Esteves-Veríssimo, June 2018
- 74th Meeting of IFIP Working Group 10.4 by Prof. Dr. Paulo Esteves-Veríssimo, June 2018
- ATENA H2020 Workshop by Dr. Florian Adamsky, October 2018

Business

- GDPR Roundtable Session 1: Legal Solutions: How to Accommodate the GDPR Challenges in Your IT Contracts by Dr. Andra Giurgiu. In collaboration with Stibbe and FDEF, December 2017
- GDPR Roundtable Session 2: Big Data Projects: How to Draft Efficient and Pragmatic Privacy Policies? by Dr. Andra Giurgiu. In collaboration with Stibbe and FDEF, January 2018
- GDPR Roundtable Session 3: Help Me, I’m Hacked – Incident Management and GDPR Governance by Dr. Andra Giurgiu. In collaboration with Stibbe and FDEF, February 2018
- GDPR Roundtable Session 4: International Data Transfers by Dr. Andra Giurgiu. In collaboration with Stibbe and FDEF, March 2018

Public

- Shapify 3D Scanning at Belle Étoile by Dr. Djamila Aouada, August 2018
- Aerial Robotics Lab Open House by Dr. Miguel A. Olivares-Mendez. Part of European Robotics Week 2018, November 2018

Trainings

- A New Awareness of the GDPR by Dr. Sandrine Munoz and Christian Hutter, March 2018
- Turning Your Research into a Proof-Of-Concept Proposal Worth Funding by Dr. Jeff Skinner, October 2018

Spotlight On:

- GDPR Roundtable Series

The European General Data Protection Regulation (GDPR) came into play on 25 May 2018. In the lead up, professionals from across industries were struggling to come to terms with its implications. SnT legal expert, Dr. Andra Giurgiu took the opportunity to lead the discussion in a popular series of five monthly GDPR roundtables. Stakeholders and experts gathered to tackle subjects ranging from IT contracts and privacy policies for big data projects to applying the law to new disruptive technologies.
Advancement of Heterogeneous Networks
Dr. Shree Krishna Sharma, Dr. Symeon Chatsiotis and Prof. Dr. Björn Ottersten
European Association for Signal Processing (EURASIP) 2018 Best Paper Award
Presented during the 28th European Signal Processing Conference (EUSIPCO 2018)
3-7 September 2018, Rome, Italy

Code Design for Non-Coherent Detection of Frame Headers in Precoded Satellite Systems
Dr. Farbod Kayhan and Prof. Guido Montorsi
9th Advanced Satellite Multimedia Systems Conference (ASMS) and Signal Processing for Space Communications Workshop (SPSC)
10-12 September 2018, Berlin, Germany

Enabling Model Testing of Cyber-Physical Systems
Dr. Carlos A. González, Mojtaba Varmazyar, Dr. Shiva Nejati, Prof. Dr. Lionel C. Briand and Yago Izaï
ACM/SIGBED 21st International Conference on Model Driven Engineering Languages and Systems (MODELS 2018)
14-19 October 2018, Copenhagen, Denmark

Live Search of Fix Ingredients for Automated Program Repair
Kui Liu, Anil Koyuncu, Kusab Kim, Dongsun Kim and Dr. Tegawendé F. Bissyandé
Best EDA Paper Award, 29th Asia-Pacific Software Engineering Conference (APSEC 2018)
4-7 December 2018, Nara, Japan

INDIVIDUAL AWARDS

Prof. Dr. Pascal Bouyer and Dr. Grégoire Dany received a US Navy Office of Naval Research three-year grant in recognition of their research into drone swarming. The US Navy funded project will allow them to combine their work on three distinct areas of swarm mobility — chaos theory, clustering techniques and nature-inspired approaches — to optimise the behaviour of autonomous vehicles in a completely distributed way.

Dr. Jean-Sébastien Corin received the European Research Council’s prestigious Advanced Grant. Corin and his team will receive up to €2.5 million over a period of five years to make cryptographic tasks usable in practice, so that citizens do not have to compromise on the privacy and security of their data. Corin is the third researcher at SnT (and in Luxembourg) to receive an ERC Advanced Grant.

Dr. Birgir Hafstein received the European Association for Biometrics Research Award 2018. The prestigious award recognises individuals who have made a significant contribution to the field of biometrics research in Europe; in this case, Dag’s work on facial recognition and finger vein-based identification.

Dr. Shiva Nojaji was named a Distinguished Reviewer at the 42nd International Conference on Software Engineering (ICSE 2018), 27 May-3 June, Gothenburg, Sweden.

Prof. Dr. Björn Ottersten, Director of SnT, is the 2018 recipient of the prestigious European Association for Signal Processing (EURASIP) Group Technical Achievement Award. The award recognises Ottersten’s scientific leadership in building research groups, most recently as head of SnT’s Signal Processing and Communications Research Group (SIG-COM) at SnT.

Dr. Léo Perrin won the Amis de l’Université du Luxembourg’s annual best thesis award — the Rolf Tarrach Prize — to SnT’s Léo Perrin. Dr. Perrin completed his thesis, “Cryptanalysis, Reverse-Engineering and Design of Symmetric Cryptographic Algorithms”, under the supervision of Prof. Dr. Alex Biryukov, and is now a postdoctoral researcher at Inria, Paris. We caught up with him to learn more about his pioneering work in cryptography.

Dr. Léo Perrin gives the keynote speech at the graduation ceremony of the University of Luxembourg held in December 2018.

On 5 July 2018, the Amis de l’Université du Luxembourg awarded their annual best thesis award — the Rolf Tarrach Prize — to SnT’s Léo Perrin. Dr. Perrin completed his thesis, “Cryptanalysis, Reverse-Engineering and Design of Symmetric Cryptographic Algorithms”, under the supervision of Prof. Dr. Alex Biryukov, and is now a postdoctoral researcher at Inria, Paris. We caught up with him to learn more about his pioneering work in cryptography. What first drew you to cryptography? I discovered cryptography when I was still in middle school. I used to read a lot of books by Jules Verne, and in one of them the decryption of an encrypted message is a key plot point – that got me curious.
I also consider strong cryptography crucial for society to work. When we exchange messages, we want to ensure that nobody can read them but their recipient, that they have been written by the right person, and that they have not been modified along the way. Cryptography is the science that ensures that these three properties are present.
This interest for cryptography, my love for mathematics, and a sense of purpose nudged me toward research in this field. Plus, I find cryptography fun!
Can you tell us about your PhD thesis? The first of my two main topics was “lightweight cryptography.” With the advent of the Internet of Things, we are going to have a myriad of tiny devices with very little computing power but which still need to communicate securely.
To meet this need for “lightweight algorithms”, I co-designed a block cipher (a type of cryptographic algorithm) called SPARX. Block ciphers use one of two types of substitution: “S-boxes”, which allow security proofs, or modular additions, which are lighter weight. For SPARX, I invented a new design approach that bridges the gap between the good performance of modular additions and the security guarantees of S-boxes. This opened a new avenue for designing the algorithm to secure the IoT.
The second axis of my PhD was on “S-box reverse-engineering”. The security of a cipher using a S-box hinges on its mathematical properties, so cipher designers always describe the design process for their S-box in great detail, except when they don’t... Russian and American secret services have designed algorithms without describing them, and these have gone on to be used widely, without anyone knowing if they contain hidden flaws.
I co-invented techniques that can recover the structure or the design process of such S-boxes using very limited information. In fact, we found a hidden structure in the S-box used by the last Russian standard!
What are you working on now? In Paris, I’m continuing my work on S-box reverse-engineering, while with my former colleagues from Luxembourg we’re submitting an algorithm, based on my design strategy for SPARX, to a National Institute of Standards and Technology (USA) competition for choosing a new standard.
<table>
<thead>
<tr>
<th>Project</th>
<th>PhD Student</th>
<th>Supervisor</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure and Compliant Data Management</td>
<td>Amin Sleimi</td>
<td>Dr. Mehrdad Saberzadeh</td>
<td>Service Central de Législation (Public)</td>
</tr>
<tr>
<td>Automated Extraction of Metadata and Compliance Rules from Legal Texts</td>
<td>Iago Vázquez Sanchez</td>
<td>Dr. Gabriele Lensini</td>
<td>pEp Security</td>
</tr>
<tr>
<td>Implementation of Securely Proxied Protocols for Private Communications</td>
<td>Ziya Alper Genc</td>
<td>Dr. Gabriele Lensini</td>
<td>pEp Security</td>
</tr>
<tr>
<td>Protocols for Privacy Security Analysis</td>
<td>Laurent Leusage</td>
<td>Dr. Rado State</td>
<td>Foyer</td>
</tr>
<tr>
<td>Personalized Insurance with Data Analytics</td>
<td>Amin Sleimi</td>
<td>Dr. Mehrdad Saberzadeh</td>
<td>Service Central de Législation (Public)</td>
</tr>
<tr>
<td>Automated Decision Support for Security Requirements Analysis</td>
<td>Scholastique Botaix</td>
<td>Prof. Dr. Lionel Briand</td>
<td>BGL BNP Paribas</td>
</tr>
<tr>
<td>Anti-Money Laundering with Big Data Analytics</td>
<td>Ramiro Camino</td>
<td>Dr. Rado State</td>
<td>LOGOS (AFR)</td>
</tr>
<tr>
<td>Data Analytics for Personal Finance</td>
<td>Jeremy Charlier</td>
<td>Dr. Rado State</td>
<td>BCEE</td>
</tr>
<tr>
<td>Security of Smart Contracts</td>
<td>Cristof Ferreira Torres</td>
<td>Dr. Rado State</td>
<td>BCEE (IR)</td>
</tr>
<tr>
<td>Data Analytics and Smart Contracts for Traceability in Finance</td>
<td>Nida Khan</td>
<td>Dr. Rado State</td>
<td>Ethiq (AFR)</td>
</tr>
<tr>
<td>Smart Testing in a DevOps and Continuous Integration Process</td>
<td>Renaud Rovemalika</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>BGL BNP Paribas (AFR)</td>
</tr>
<tr>
<td>Distributed Ledger Prototype and Data Analytics for KYC</td>
<td>Robert Narsil</td>
<td>Dr. Rado State</td>
<td>ABIN</td>
</tr>
<tr>
<td>Machine Learning for Client Segmentation</td>
<td>Anshuman Bhadauria</td>
<td>Prof. Dr. Lionel Briand</td>
<td>CLEARSTREAM-ESSENTIAL (AFR)</td>
</tr>
<tr>
<td>A Model-based Framework for Requirements Engineering in the Financial Domain</td>
<td>Alvaro Mario Veizaga Campero</td>
<td>Prof. Dr. Lionel Briand</td>
<td>Clearstream-Escent</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>Software Defined Network Service Chaining through Network Analytics</td>
<td>Beltran Buija Fortinveros</td>
<td>Dr. Rado State</td>
</tr>
<tr>
<td>Smart Grid Deep Search</td>
<td>Nikolaos Antoniadis</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>CReOS</td>
</tr>
<tr>
<td>Hardware/Software Architectures for Deep Packet Inspection and Security Monitoring at Gigabyte Speed</td>
<td>Mathis Steichen</td>
<td>Dr. Rado State</td>
<td>Telindus</td>
</tr>
<tr>
<td>Self-learning Predictive Algorithms: from Design to Scalable Implementation</td>
<td>Marian Du</td>
<td>Dr. Rado State</td>
<td>Clearstream-Escent (AFR)</td>
</tr>
<tr>
<td>Data Analytics for Network Security</td>
<td>Georgios Kalafas</td>
<td>Dr. Rado State</td>
<td>CLEARSTREAM-ESSENTIAL (AFR)</td>
</tr>
<tr>
<td>Big Data Analytics against Electricity Theft</td>
<td>Patrick Glauner</td>
<td>Dr. Rado State</td>
<td>CLEARSTREAM-ESSENTIAL (AFR)</td>
</tr>
<tr>
<td>Risk Monitoring with Intrusion Detection for Industrial control systems</td>
<td>Steve Muller</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>Imtrust (AFR)</td>
</tr>
<tr>
<td>Space Systems and Resources</td>
<td>Satellite Sensor Networks for Spectrum Monitoring</td>
<td>Chaima Boufadi</td>
<td>Prof. Dr. Lionel Briand</td>
</tr>
<tr>
<td>Model-driven Trace Checking</td>
<td>Christoph Potiris</td>
<td>Prof. Dr. Lionel Briand</td>
<td>LuxSpace (IR)</td>
</tr>
<tr>
<td>Advanced Signal Processing Techniques for Satellite Communications</td>
<td>Alberto Mongai</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>SES (CORE)</td>
</tr>
<tr>
<td>Broadband/Broadcast Convergence through Intelligent Caching in 5G Satellite Networks</td>
<td>Danilo Sparsi</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>SES (CORE)</td>
</tr>
<tr>
<td>Autonomous Vehicles</td>
<td>Multimodal Transport Optimization</td>
<td>Thierry Derrmann (graduated in 2018)</td>
<td>Prof. Dr. Thomas Engel</td>
</tr>
<tr>
<td>Scenic flow from Rull-O-D Applications in Human Motion Sensing</td>
<td>Konstantinos Papadopoulus</td>
<td>Dr. Olympti Anaxian</td>
<td>POST (CORE)</td>
</tr>
<tr>
<td>Accurate 3D Human Body Shape Modelling and Fitting under Clothing</td>
<td>Alexandre Saint</td>
<td>Dr. Olympti Anaxian</td>
<td>ARTEC (AFR)</td>
</tr>
<tr>
<td>Deep Learning Based 3D Shape Analysis with Application to Face Recognition</td>
<td>Eman Ahmed</td>
<td>Dr. Olympti Anaxian</td>
<td>ARTEC (CORE-PPP)</td>
</tr>
<tr>
<td>Automated CAD-Re-engineering</td>
<td>Kenjiya Cherenkova</td>
<td>Prof. Dr. Lionel Briand</td>
<td>IEE (AFR)</td>
</tr>
<tr>
<td>Automating Regression Test Selection for Requirements-based Testing in Embedded Systems</td>
<td>Inez Haji</td>
<td>Prof. Dr. Lionel Briand</td>
<td>IEE (AFR)</td>
</tr>
<tr>
<td>Traceability from Requirements to Design to Support Context-driven Testing of Embedded Software Systems</td>
<td>Raja Ben Abdessalem</td>
<td>Prof. Dr. Lionel Briand</td>
<td>IEE (AFR)</td>
</tr>
<tr>
<td>Increased Mission Autonomy for small UAVs</td>
<td>Manuel Castillo Lopez</td>
<td>Prof. Dr. Holger Voss</td>
<td>Lux Army</td>
</tr>
<tr>
<td>Radar Waveform Design for Automotive Applications</td>
<td>Christian Hammers</td>
<td>Dr. Bhavani Shankar</td>
<td>IEE (AFR)</td>
</tr>
<tr>
<td>Coherent Radar Waveform Design for Automotive Applications</td>
<td>Sayed Dashmehri</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>Lux Army</td>
</tr>
<tr>
<td>Future Developments for Flexible Production Processes</td>
<td>Lunard William Tassaro</td>
<td>Prof. Dr. Holger Voss</td>
<td>ROGLER</td>
</tr>
<tr>
<td>VICO - Vision-based Control of Small Unmanned Aerial Vehicles</td>
<td>Jean-Armandian</td>
<td>Graduated in 2018</td>
<td>Prof. Dr. Holger Voss</td>
</tr>
<tr>
<td>Learning of Control Behaviors in Flying Manipulation</td>
<td>Anshul Anand</td>
<td>Prof. Dr. Holger Voss</td>
<td>Lux Army</td>
</tr>
<tr>
<td>Design and Control of a Flying Gripper and Manipulator</td>
<td>Paul Kremer</td>
<td>Prof. Dr. Holger Voss</td>
<td>Lux Army</td>
</tr>
<tr>
<td>Security in ROS Base Systems</td>
<td>Sean Rivera</td>
<td>Dr. Rado State</td>
<td>Lux Army</td>
</tr>
<tr>
<td>Hybrid Verification of CPS Behavioral Design Models</td>
<td>Khoukoua Gaaol</td>
<td>Dr. Shiva Nejati</td>
<td>QRA</td>
</tr>
</tbody>
</table>
### Projects

#### EU AND ESA PROJECTS IN 2018

<table>
<thead>
<tr>
<th>Project</th>
<th>Principal Investigator</th>
<th>Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCD4ITS - Floating Car Data Collection for Intelligent Transportation Systems</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>CONCORDIA - Cyber security Competence Hbr Research and Innovation</td>
<td>Dr. Radu State</td>
<td>H2020</td>
</tr>
<tr>
<td>FlexPodDem - Demonstrator of Precoding Techniques for Flexible Broadband Systems</td>
<td>Dr. Symeon Chatzinotas</td>
<td>ESA</td>
</tr>
<tr>
<td>SPARTA - Special projects for advanced research and technology in Europe</td>
<td>Prof. Dr. Paulo Estevves-Verissimo</td>
<td>H2020</td>
</tr>
<tr>
<td>FIN-TECH - A Financial supervision and TECHomology compliance training programme</td>
<td>Dr. Radu State</td>
<td>H2020</td>
</tr>
<tr>
<td>5G-DRIVE - 5G Harmoni4ized Research and Trials for service Evolution between EU and China</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>5G-MOBIX - 5G for cooperative &amp; connected automated MOBility on X-border corridors</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>NG-HOR - Next Generation High Data Rate Trunking Systems</td>
<td>Dr. Bhavani Shankar</td>
<td>ESA</td>
</tr>
<tr>
<td>CyberSec4Europe - Cyber Security Network of Competence Centres for Europe</td>
<td>Prof. Dr. Paulo Estevves-Verissimo</td>
<td>H2020</td>
</tr>
<tr>
<td>Hi4Elec - Modernisation of Higher Education in Central Asia through new Technologies</td>
<td>Prof. Dr. Thomas Engel</td>
<td>Erasmus plus</td>
</tr>
<tr>
<td>VHTS4DEM - User Terminal Wideband Modern for Very High Throughput Satellite (VHTS)</td>
<td>Dr. Symeon Chatzinotas</td>
<td>ESA</td>
</tr>
<tr>
<td>CLOUDMAP - Cloud Computing via Homomorphic Encryption and Multilinear Maps</td>
<td>Prof. Dr. Jean-Sebastian Coron</td>
<td>ERC</td>
</tr>
<tr>
<td>TERMINAL - Minibus électriques automatisés dans les navettes sous Contrôleurs</td>
<td>Dr. Raphael Frank</td>
<td>Interreg V A</td>
</tr>
<tr>
<td>LAST-JD-RIoE - Law, Science and Technology Joint Doctorate: Rights of the Internet of Everything</td>
<td>Prof. Dr. Leon Van Der Torre</td>
<td>MSCA-ITN</td>
</tr>
</tbody>
</table>

#### EU AND ESA PROJECTS IN 2019

<table>
<thead>
<tr>
<th>Project</th>
<th>Principal Investigator</th>
<th>Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveSatProDemo - Live Satellite Demonstration of Advanced Interference Management Techniques</td>
<td>Dr. Symeon Chatzinotas</td>
<td>ESA</td>
</tr>
<tr>
<td>GRiNe - Grande Region Oblique airnрей</td>
<td>Prof. Dr. Holger Voos</td>
<td>Interreg V A</td>
</tr>
<tr>
<td>MIREL - Mining and Reasoning with Legal Text</td>
<td>Prof. Dr. Leon Van Der Torre</td>
<td>MSCA-RISE</td>
</tr>
<tr>
<td>ATENA - Advanced Tools to Assess and Mitigate the Criticality of ICT Components and their Dependencies over Critical Infrastructures</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>ADIMOSTHIC - Activity Enhanced Cognition based Framework for Design of Complex Systems</td>
<td>Prof. Dr. Bjorn Jansen</td>
<td>ERC</td>
</tr>
<tr>
<td>SANT - Systemic Analyzer In Network Threats</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>STARR - Decision Support and self-management system for sthikes survivoRs</td>
<td>Dr. Djamila Assaoula</td>
<td>H2020</td>
</tr>
<tr>
<td>HTS-DMS - High Throughput Digital Broadcasting Satellite System</td>
<td>Dr. Symeon Chatzinotas</td>
<td>ESA</td>
</tr>
<tr>
<td>FuturePMP - Future Proving the Connected World: A Quantum-Resistant Trusted Platform Module</td>
<td>Prof. Dr. Peter Y. A. Ryan</td>
<td>H2020</td>
</tr>
</tbody>
</table>

#### Projects

<table>
<thead>
<tr>
<th>Project</th>
<th>PhD Student</th>
<th>Supervisor</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using Artificial Intelligence to Support Automated Requirements Quality Assurance</td>
<td>Saad Ezzini</td>
<td>Dr. Mehrdad Sabarasteh</td>
<td>QRA</td>
</tr>
<tr>
<td>Highly Automated Surveillance of Data Centers with Multi-UAV Systems</td>
<td>Claudio Cianelli</td>
<td>Prof. Dr. Holger Voos</td>
<td>Luxconnect</td>
</tr>
<tr>
<td>Privacy Preserving Risk Assessment of Human &amp; Automated Driving using Multi-Fusion Sensor Analytics</td>
<td>Francois Robinet</td>
<td>Dr. Raphael Frank</td>
<td>IE (CORE-PPP)</td>
</tr>
<tr>
<td>mmWave Cognitive Radar: Adaptive Waveform Design and Implementation</td>
<td>Ehsan Raei Dehaghi</td>
<td>Dr. Bhavani Shankar</td>
<td>FNR Bilateral</td>
</tr>
<tr>
<td>Compressive Sensing for Ranging and Detection in Automotive Applications</td>
<td>Saad Sedighi</td>
<td>Prof. Dr. Bjorn Ottersten</td>
<td>POST</td>
</tr>
<tr>
<td>Handling Uncertainties in Design and Analysis of Cyber Physical Systems</td>
<td>Jaekwon Lee</td>
<td>Prof. Dr. Lionel Briand</td>
<td>LuxSpace</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>Ludovic Mouline</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>POST</td>
</tr>
<tr>
<td>Software Engineering and Data Analytics in the Context of Smart Buildings</td>
<td>Danquan Li (graduated in 2018)</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>POST</td>
</tr>
<tr>
<td>Normalisation and IoT</td>
<td>Nader Samir Labib</td>
<td>Dr. Grégoire Danoy</td>
<td>ILNAS</td>
</tr>
<tr>
<td>Normalisation and Cloudcomputing Service Price Models for Optimisation</td>
<td>Chao Liu</td>
<td>Prof. Dr. Pascal Bouvy</td>
<td>ILNAS</td>
</tr>
<tr>
<td>Biotechnological Big Data: Security, Privacy, and Standardisation</td>
<td>Saharnaz Esmaeilzadeh Dimaghani</td>
<td>Dr. Matthias Brust</td>
<td>ILNAS</td>
</tr>
<tr>
<td>Connectivity Framework for the Industry 4.0</td>
<td>Paul-Lou Benedick</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>Cabi</td>
</tr>
<tr>
<td>Security Framework for the Industry 4.0</td>
<td>Julien Polge</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>Cabi</td>
</tr>
</tbody>
</table>

#### EU AND ESA PROJECTS IN 2018

<table>
<thead>
<tr>
<th>Project</th>
<th>Principal Investigator</th>
<th>Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCD4ITS - Floating Car Data Collection for Intelligent Transportation Systems</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>CONCORDIA - Cyber security Competence Hbr Research and Innovation</td>
<td>Dr. Radu State</td>
<td>H2020</td>
</tr>
<tr>
<td>FlexPodDem - Demonstrator of Precoding Techniques for Flexible Broadband Systems</td>
<td>Dr. Symeon Chatzinotas</td>
<td>ESA</td>
</tr>
<tr>
<td>SPARTA - Special projects for advanced research and technology in Europe</td>
<td>Prof. Dr. Paulo Estevves-Verissimo</td>
<td>H2020</td>
</tr>
<tr>
<td>FIN-TECH - A Financial supervision and TECHomology compliance training programme</td>
<td>Dr. Radu State</td>
<td>H2020</td>
</tr>
<tr>
<td>5G-DRIVE - 5G Harmoni4ized Research and Trials for service Evolution between EU and China</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>5G-MOBIX - 5G for cooperative &amp; connected automated MOBility on X-border corridors</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>NG-HOR - Next Generation High Data Rate Trunking Systems</td>
<td>Dr. Bhavani Shankar</td>
<td>ESA</td>
</tr>
<tr>
<td>CyberSec4Europe - Cyber Security Network of Competence Centres for Europe</td>
<td>Prof. Dr. Paulo Estevves-Verissimo</td>
<td>H2020</td>
</tr>
<tr>
<td>Hi4Elec - Modernisation of Higher Education in Central Asia through new Technologies</td>
<td>Prof. Dr. Thomas Engel</td>
<td>Erasmus plus</td>
</tr>
<tr>
<td>VHTS4DEM - User Terminal Wideband Modern for Very High Throughput Satellite (VHTS)</td>
<td>Dr. Symeon Chatzinotas</td>
<td>ESA</td>
</tr>
<tr>
<td>CLOUDMAP - Cloud Computing via Homomorphic Encryption and Multilinear Maps</td>
<td>Prof. Dr. Jean-Sebastian Coron</td>
<td>ERC</td>
</tr>
<tr>
<td>TERMINAL - Minibus électriques automatisés dans les navettes sous Contrôleurs</td>
<td>Dr. Raphael Frank</td>
<td>Interreg V A</td>
</tr>
<tr>
<td>LAST-JD-RIoE - Law, Science and Technology Joint Doctorate: Rights of the Internet of Everything</td>
<td>Prof. Dr. Leon Van Der Torre</td>
<td>MSCA-ITN</td>
</tr>
</tbody>
</table>

#### EU AND ESA PROJECTS IN 2019

<table>
<thead>
<tr>
<th>Project</th>
<th>Principal Investigator</th>
<th>Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveSatProDemo - Live Satellite Demonstration of Advanced Interference Management Techniques</td>
<td>Dr. Symeon Chatzinotas</td>
<td>ESA</td>
</tr>
<tr>
<td>GRiNe - Grande Region Oblique airnрей</td>
<td>Prof. Dr. Holger Voos</td>
<td>Interreg V A</td>
</tr>
<tr>
<td>MIREL - Mining and Reasoning with Legal Text</td>
<td>Prof. Dr. Leon Van Der Torre</td>
<td>MSCA-RISE</td>
</tr>
<tr>
<td>ATENA - Advanced Tools to Assess and Mitigate the Criticality of ICT Components and their Dependencies over Critical Infrastructures</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>ADIMOSTHIC - Activity Enhanced Cognition based Framework for Design of Complex Systems</td>
<td>Prof. Dr. Bjorn Jansen</td>
<td>ERC</td>
</tr>
<tr>
<td>SANT - Systemic Analyzer In Network Threats</td>
<td>Prof. Dr. Thomas Engel</td>
<td>H2020</td>
</tr>
<tr>
<td>STARR - Decision Support and self-management system for sthikes survivoRs</td>
<td>Dr. Djamila Assaoula</td>
<td>H2020</td>
</tr>
<tr>
<td>HTS-DMS - High Throughput Digital Broadcasting Satellite System</td>
<td>Dr. Symeon Chatzinotas</td>
<td>ESA</td>
</tr>
<tr>
<td>FuturePMP - Future Proving the Connected World: A Quantum-Resistant Trusted Platform Module</td>
<td>Prof. Dr. Peter Y. A. Ryan</td>
<td>H2020</td>
</tr>
</tbody>
</table>
CADSAT - Carrier Aggregation in Satellite Communication Networks

Principal Investigator: Dr. Symeon Chatzinotas
Funding: ESA

TUNE - Testing the Untestable: Model Testing of Complex Software-intensive Systems

Principal Investigator: Prof. Dr. Lionel Briand
Funding: ERC

F-INTEROP - FIRE+ Online Interoperability and Performance Test Tools to Support Emerging Technologies from Research to Standardisation and Market Launch: An Accelerator to Develop Standards and Innovations

Principal Investigator: Prof. Dr. Thomas Engel
Funding: H2020

Flysec - FLY faster through an innovative and robust risk-based SECurity tunnel

Principal Investigator: Prof. Dr. Thomas Engel
Funding: H2020

SATNEX-IV - Satellite Network Of Experts CCN2 W11

Principal Investigator: Dr. Symeon Chatzinotas
Funding: ESA

SATNEX-IV - Satellite Network Of Experts CCN2 W12

Principal Investigator: Dr. Bhavani Shankar
Funding: ESA

Privacy Flag - Enabling Crowd-sourcing based Privacy Protection for Smartphone Applications, Websites and Internet of Things Deployments

Principal Investigator: Prof. Dr. Thomas Engel
Funding: H2020

M2MSAT - Demonstrator of Light-weight Application and Transport Protocols for Future M2M Applications

Principal Investigator: Prof. Dr. Thomas Engel
Funding: ESA

TARGET - Training Augmented Reality Generalized Environment Toolkit

Principal Investigator: Prof. Dr. Thomas Engel
Funding: H2020

ONSET - Optical Feeder Study for Satellite Networks

Principal Investigator: Prof. Dr. Björn Ottersten
Funding: ESA

SANSA - Shared Access Terrestrial-Satellite Backhaul Network enabled by Smart Antennas

Principal Investigator: Prof. Dr. Björn Ottersten
Funding: ESA

ProDem - Preconditioning Demonstrator for broadband system forward links

Principal Investigator: Dr. Symeon Chatzinotas
Funding: ESA

bIoTope - Backbone of future Internet of Thing Open Ecosystems

Principal Investigator: Prof. Dr. Yves Le Traon
Funding: H2020

GHOST - On-Ground EnHanced Non-Intrusive IOT System Protootyping and Testing for Efficient Monitoring Of Wideband Satellite Transponders

Principal Investigator: Dr. Symeon Chatzinotas
Funding: ESA

EnCaVIBS - The EU NIS Directive: Enhancing Cybersecurity across Vital Business Sectors

Principal Investigator: Prof. Dr. Mark Cole
Funding: CORE

Onniva - Automatic Detection and Prevention of Deserialization Vulnerabilities

Principal Investigator: Dr. Alexandre Bartel
Funding: CORE

SPRINGER - Signal Processing for Next Generation Radar

Principal Investigator: Prof. Dr. Björn Ottersten
Funding: CORE

STV - Socio-Technical Verification of Information Security and Trust in Voting Systems

Principal Investigator: Prof. Dr. Peter Y. A. Ryan
Funding: CORE

Flysec - FLY faster through an innovative and robust risk-based SECurity tunnel

Principal Investigator: Prof. Dr. Thomas Engel
Funding: H2020

TargetAdapt - Adaptive Byzantine Fault and Intrusion Tolerance

Principal Investigator: Prof. Dr. Paulo Esteves-Veríssimo
Funding: CORE

SSh - Security in the Shell

Principal Investigator: Prof. Dr. Jan Laguna (co-PI Dr. Gabriele Lenzini)
Funding: CORE

PrivDA - Privacy-preserving Publication of Dynamic Social Network Data in the Presence of Active Adversaries

Principal Investigator: Dr. Yunior Ramirez-Cruz
Funding: CORE Junior

Q-CoDe - Quantum Communication with Deniability

Principal Investigator: Prof. Dr. Peter Y. A. Ryan
Funding: CORE

FESS - Functional Encrypted Secure Systems

Principal Investigator: Dr. Vincenzo Iovino
Funding: CORE Junior

DAPICO - Data Protection-Regulation Compliance

Principal Investigator: Dr. Gabriele Lencini
Funding: CORE

BEST-RPAS - Robust Emergency Sense-and-Avoid Capability for Small Remotely Piloted Aerial Systems

Principal Investigator: Prof. Dr. Holger Voss
Funding: CORE

3D-ACT - 3D Action Recognition Using Refinement and Invariance Strategies for Reliable Surveillance

Principal Investigator: Prof. Dr. Björn Ottersten
Funding: CORE

ESSTIMS - Enhanced Signal Space Optimization for satellite communication Systems

Principal Investigator: Dr. Farbod Kayhan
Funding: CORE Junior

ROSETTA - Resource Optimization for Integrated Satellite-5G Networks with Non-Orthogonal Multiple Access

Principal Investigator: Dr. Lei Lei
Funding: CORE Junior

COHESAT - Cognitive Cohesive Networks of Distributed Units for Active and Passive Space Applications

Principal Investigator: Dr. Juan Morlano Duncan
Funding: CORE Junior

FinCrypt - Security, Scalability, and Privacy in Blockchain Applications and Smart Contracts

Principal Investigator: Prof. Dr. Alex Biryukov
Funding: CORE

EDECTIC - Energy and Complexity Efficient Millimeter-wave Large-Array Communications

Principal Investigator: Dr. Teneo Christos
Funding: CORE Junior

DOOMATES - Continuous Development with Mutation Analysis and Testing

Principal Investigator: Dr. Michal Papadakis
Funding: CORE Junior

PROCAST - Proactive Edge Caching for Content Delivery Networks powered by Hybrid Satellite/Terrestrial Backhauling

Principal Investigator: Prof. Dr. Björn Ottersten
Funding: CORE

RECOMMEND - Automatic Bug Fix Recommendation: Improving Software Repair and Reducing Time-to-Fix Delays in Software Development Projects

Principal Investigator: Dr. Tegawendé Bissyande
Funding: CORE

VoteVerif - Verification of Voter-Verifiable Voting Protocols

Principal Investigator: Prof. Dr. Peter Y. A. Ryan
Funding: CORE
### Projects

**SCASE21** - "Space" as a Catalyst of a Sustainable Smart School
- **Principal Investigator:** Melissa Bellesi
- **Supervisor:** Prof. Dr. Charles Ottersten

**DAAP** - Real Time Prediction and Detection of Malicious Activities
- **Principal Investigator:** Georgios Kailas
- **Supervisor:** Prof. Dr. Radu State

**BODYFIT** - Accurate 3D Human Body Shape Modelling and Fitting under Clothing
- **Principal Investigator:** Alexandre Saint
- **Supervisor:** Dr. Oujama Aouada

**LARKOS** - Learning-Assisted Optimization for Resource and Security Management in Slicing-Based 5G Networks
- **Principal Investigator:** Yanxing Yuan / S. Bommeraweni
- **Supervisor:** Dr. Symeon Chatzinotas

**DYNMOC** - Enhancing Angular Resolution in Radar Through Dynamic Beam Steering and MIMO
- **Principal Investigator:** Christian Hammes
- **Supervisor:** Dr. Bhuvani Shankar

**NAV** - Automatic Feature Selection for Visual Recognition
- **Principal Investigator:** Oyaebade Oyedotun
- **Supervisor:** Prof. Dr. Björn Ottersten

**NAVSY** - Navigation System for a Small Lunar Exploration Rover
- **Principal Investigator:** Philippe Ludwig
- **Supervisor:** Prof. Dr. Holger Voos

**SCASE21** - "Space" as a Catalyst of a Sustainable Smart School
- **Principal Investigator:** Melissa Bellesi
- **Supervisor:** Prof. Dr. Charles Ottersten

**Digital Payload Processing for Next Generation Satellite Systems**
- **Principal Investigator:** Vahid Joroughi
- **Supervisor:** Prof. Dr. Björn Ottersten

**Functionalities**
- **Principal Investigator:** Sajad Mehrizi Rahmat Abadi
- **Supervisor:** Prof. Dr. Björn Ottersten

**SyProSat - End-to-end Signal Processing Algorithms for Precoded Satellite Communications**
- **Principal Investigator:** Jurek Krivochiza
- **Supervisor:** Prof. Dr. Björn Ottersten

**AREG - Automating Regression Test Selection for Requirements-based Testing in Embedded Systems**
- **Principal Investigator:** Ines Hajri
- **Supervisor:** Prof. Dr. Lionel Briand

**ISEG2S** - Machine Learning for Risk Assessment in Semi-autonomous Vehicles
- **Principal Investigator:** François Robinet
- **Supervisor:** Dr. Raphael Frank

**Blockchain for Finance - Secure Blockchain Technologies for Finance**
- **Principal Investigator:** Christin Fomina Torres
- **Supervisor:** Dr. Rado State

**C2ML - Continuously Learning to Meta Learn Using Ensemble and Reinforcement Learning**
- **Principal Investigator:** Dr. Thomas Hartmann
- **Supervisor:** Prof. Dr. Yves Le Traon

**DESSIRA - Development of a Decision Support System for Incorporating Risk Assessments during the System Design of Microsatellites**
- **Principal Investigator:** Raja Pandi Perumal
- **Supervisor:** Prof. Dr. Holger Voos

**LAGLOCM - Learning -Assisted Cross-Layer Optimization of Cognitive Communication Networks**
- **Principal Investigator:** Praween Kumar Kornal
- **Supervisor:** Dr. Symeon Chatzinotas

**AutoGEM - Automatic Generation and Maintenance of functional tests in agile environment**
- **Principal Investigator:** Renaud Raveulka
- **Supervisor:** Prof. Dr. Yves Le Traon

**SAINT - Communication Algorithms for End-to-End Satellite-IoT**
- **Principal Investigator:** Chitin Kodheli
- **Supervisor:** Dr. Symeon Chatzinotas

### FNR CORE PPP, BRIDGES AND PUBLIC2

**Projects**

<table>
<thead>
<tr>
<th>Project</th>
<th>Principal Investigator</th>
<th>Funding Instrument</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobiRoF - Improved Model-based Requirements for Financial Applications</td>
<td>Prof. Dr. Lionel Briand</td>
<td>BRIDGES</td>
</tr>
<tr>
<td>CAFFE PP - Cost-aware Active Feedback &amp; Feature Extraction for Profiling Financial Transactions</td>
<td>Dr. Radu State</td>
<td>BRIDGES</td>
</tr>
<tr>
<td>TESTFAST - Software testing in a Fast, Dover and Effective Way</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>BRIDGES</td>
</tr>
<tr>
<td>EQUAQS - Event-Quality Assurance of Critical Systems</td>
<td>Prof. Dr. Mehrdad Sabzevarian</td>
<td>BRIDGES</td>
</tr>
</tbody>
</table>

**Completed**

**SCARLET - Semantic Metadata and Compliance Rule Extraction**
- **Principal Investigator:** Dr. Andy Pantchenko
- **Supervisor:** CORE Junior

**WITNESS - Multi-Layer Witnessing and Protection Frameworks for Cyber Security**
- **Principal Investigator:** Prof. Dr. Lionel Briand
- **Supervisor:** CORE PPP

**FNR AFR GRANTS AND INDUSTRIAL FELLOWSHIPS**

**Projects**

<table>
<thead>
<tr>
<th>Project</th>
<th>Applicant</th>
<th>Supervisor</th>
<th>Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAESTRO - Machine Learning for Risk Assessment in Semi-autonomous Vehicles</td>
<td>François Robinet</td>
<td>Dr. Raphael Frank</td>
<td>Industrial Fellowship (Foyer)</td>
</tr>
<tr>
<td>Blockchain for Finance - Secure Blockchain Technologies for Finance</td>
<td>Christin Fomina Torres</td>
<td>Dr. Rado State</td>
<td>Industrial Fellowship (BCB)</td>
</tr>
<tr>
<td>C2ML - Continuously Learning to Meta Learn Using Ensemble and Reinforcement Learning</td>
<td>Dr. Thomas Hartmann</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>Industrial Fellowship (DataThras)</td>
</tr>
<tr>
<td>DESSIRA - Development of a Decision Support System for Incorporating Risk Assessments during the System Design of Microsatellites</td>
<td>Raja Pandi Perumal</td>
<td>Prof. Dr. Holger Voos</td>
<td>Industrial Fellowship (LuxSpace)</td>
</tr>
<tr>
<td>LAGLOCM - Learning -Assisted Cross-Layer Optimization of Cognitive Communication Networks</td>
<td>Praween Kumar Kornal</td>
<td>Dr. Symeon Chatzinotas</td>
<td>AFR PhD</td>
</tr>
<tr>
<td>AutoGEM - Automatic Generation and Maintenance of functional tests in agile environment</td>
<td>Renaud Raveulka</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>AFR PhD</td>
</tr>
<tr>
<td>SAINT - Communication Algorithms for End-to-End Satellite-IoT</td>
<td>Chitin Kodheli</td>
<td>Dr. Symeon Chatzinotas</td>
<td>Industrial Fellowship (ISED)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Awarded</th>
<th><strong>Project</strong></th>
<th><strong>Applicant</strong></th>
<th><strong>Supervisor</strong></th>
<th><strong>Programme</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTEN - online Learning for edge-caching in hybrid Satellite-Terrestrial Networks</td>
<td>Sajad Mehrizi Rahmat Abadi</td>
<td>Prof. Dr. Björn Ottersten</td>
<td>AFR-PPP Phd (IES)</td>
<td></td>
</tr>
<tr>
<td>SPA - Self-learning Predictive Algorithms: From Design to Accurate Implementation</td>
<td>Mating Bu</td>
<td>Prof. Dr. Radu State</td>
<td>AFR-PPP Phd (ElsanMoble)</td>
<td></td>
</tr>
<tr>
<td>SyProSat - End-to-end Signal Processing Algorithms for Precoded Satellite Communications</td>
<td>Jurek Krivochiza</td>
<td>Prof. Dr. Björn Ottersten</td>
<td>AFR-PPP Phd (IES)</td>
<td></td>
</tr>
<tr>
<td>AREG - Automating Regression Test Selection for Requirements-based Testing in Embedded Systems</td>
<td>Ines Hajri</td>
<td>Prof. Dr. Lionel Briand</td>
<td>AFR-PPP Phd (IEI)</td>
<td></td>
</tr>
<tr>
<td>DAP - Real Time Prediction and Detection of Malicious Activities</td>
<td>Georgios Kailas</td>
<td>Prof. Dr. Radu State</td>
<td>AFR-PPP Phd (POSTI)</td>
<td></td>
</tr>
<tr>
<td>BODYFIT - Accurate 3D Human Body Shape Modelling and Fitting under Clothing</td>
<td>Alexandre Saint</td>
<td>Dr. Oujama Aouada</td>
<td>AFR-PPP Phd (Arttec)</td>
<td></td>
</tr>
<tr>
<td>LARKOS - Learning-Assisted Optimization for Resource and Security Management in Slicing-Based 5G Networks</td>
<td>Yanxing Yuan / S. Bommeraweni</td>
<td>Dr. Symeon Chatzinotas</td>
<td>AFR Bilateral Grant</td>
<td></td>
</tr>
<tr>
<td>DiskMod - Systematically Exploring Semantic App-Models for Android</td>
<td>Alexandre Pilgun</td>
<td>Prof. Dr. Spiros Manos</td>
<td>AFR-PhD</td>
<td></td>
</tr>
<tr>
<td>DYNMOC - Enhancing Angular Resolution in Radar Through Dynamic Beam Steering and MIMO</td>
<td>Christian Hammes</td>
<td>Dr. Bhuvani Shankar</td>
<td>AFR-PPP Phd (IEI)</td>
<td></td>
</tr>
<tr>
<td>NAV - Automatic Feature Selection for Visual Recognition</td>
<td>Oyaebade Oyedotun</td>
<td>Prof. Dr. Björn Ottersten</td>
<td>AFR-PhD</td>
<td></td>
</tr>
<tr>
<td>NavSY - Navigation System for a Small Lunar Exploration Rover</td>
<td>Philippe Ludwig</td>
<td>Prof. Dr. Holger Voos</td>
<td>AFR-PPP Phd (Space)</td>
<td></td>
</tr>
<tr>
<td>SCASE21 - &quot;Space&quot; as a Catalyst of a Sustainable Smart School Environment Systems Conceiving and achieving of Conviviality for the School of the 21st Century</td>
<td>Melissa Belli</td>
<td>Prof. Dr. Charles Max</td>
<td>AFR-PhD</td>
<td></td>
</tr>
<tr>
<td>Digital Payload Processing for Next Generation Satellite Systems</td>
<td>Dr. Vahid Joroughi</td>
<td>Prof. Dr. Björn Ottersten</td>
<td>AFR-PPP PDR (IES)</td>
<td></td>
</tr>
<tr>
<td>SemCode - Source Code Search for Semantically Similar Functionalities</td>
<td>Kisub Kim</td>
<td>Dr. Tingawonde Biyavante</td>
<td>AFR-PhD</td>
<td></td>
</tr>
<tr>
<td>Project</td>
<td>Applicant</td>
<td>Supervisor</td>
<td>Programme</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td>------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>SPASAT  - Power Efficient Sparse Signal Processing for Digital Wideband On-board Techniques</td>
<td>Aakash Arora</td>
<td>Prof. Dr. Björn Ottersten</td>
<td>AFR-PPP PND (SES)</td>
<td></td>
</tr>
<tr>
<td>DASD - Data Analytics and Smart Contracts for Traceability in Finance</td>
<td>Nida Khan</td>
<td>Dr. Radu State</td>
<td>AFR-PPP PND (SETHIO)</td>
<td></td>
</tr>
<tr>
<td>STEP1 - Spatio-Temporal Processes for Electricity Theft Detection</td>
<td>Patrick Guazner</td>
<td>Dr. Radu State</td>
<td>AFR-PPP PND (CHICCE)</td>
<td></td>
</tr>
<tr>
<td>OSPNPAP - Optimal Scalability and Performance in Programmatically Advertising Platforms</td>
<td>Georgios Varistras</td>
<td>Dr. Radu State</td>
<td>AFR-PPP PDR (Chamber)</td>
<td></td>
</tr>
<tr>
<td>ANNADA - Advanced Market Abuse Detection with Big Data</td>
<td>Ramin Camirao</td>
<td>Dr. Radu State</td>
<td>AFR-PPP PND (LOGOS)</td>
<td></td>
</tr>
<tr>
<td>UTEMA - Unbiased Temporal Machine for General-purpose Times Series-based Fraud Detection</td>
<td>Eric Antonolo</td>
<td>Dr. Radu State</td>
<td>AFR-PPP PDR (CHICCE)</td>
<td></td>
</tr>
<tr>
<td>TASTRA - Tailoring Automated Software Techniques for Real World and Large Scale Software Applications</td>
<td>Thierry Titchou Chekam</td>
<td>Prof. Dr. Yves Le Traon</td>
<td>AFR Ph.D</td>
<td></td>
</tr>
<tr>
<td>ACCORDION - Compressive Sensing for Ranging and Detection in Automotive Applications</td>
<td>Saed Sedighi</td>
<td>Prof. Dr. Björn Ottersten</td>
<td>AFR Bilateral Grant</td>
<td></td>
</tr>
<tr>
<td>CatchMe - Android Malicious Code Localisation: Catch Me if You Can!</td>
<td>Pingen Kong</td>
<td>Dr. Jacques Klein</td>
<td>AFR Ph.D</td>
<td></td>
</tr>
<tr>
<td>RECONCIS - Reconceiling Natural Language Requirements and Model-based Specification for Effective Development of Critical Infrastructure Systems</td>
<td>Chetan Arora</td>
<td>Prof. Dr. Lionel Briand</td>
<td>AFR-PPP PDR (SES)</td>
<td></td>
</tr>
<tr>
<td>GRAMMAP - Graph Anti-Money Laundering and Market Abuse Framework</td>
<td>Leonardo Montoro</td>
<td>Dr. Radu State</td>
<td>AFR-PPP PDR (LOGOS)</td>
<td></td>
</tr>
<tr>
<td>LSIBT - Large-Scale Blockchain Testbed</td>
<td>Wazen Shbair</td>
<td>Dr. Radu State</td>
<td>AFR-PPP PDR (EETHIQ)</td>
<td></td>
</tr>
<tr>
<td>CARBON - Coevolutionary Hybrid Bi-level Optimization</td>
<td>Emmanuel Kieffer</td>
<td>Prof. Dr. Pascal Boche</td>
<td>AFR Ph.D</td>
<td></td>
</tr>
</tbody>
</table>

**Completed**

<table>
<thead>
<tr>
<th>Project</th>
<th>Principal Investigator</th>
<th>Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMPC - Stochastic Model Predictive Control for Eco-Driving Assistance Systems in Electric Vehicles</td>
<td>Seyed Amin Sajadi Alamdari</td>
<td>Prof. Dr. Holger Voelz</td>
</tr>
<tr>
<td>Broadcast - Multibeam Joint Processing for Broadcast Broad-cast Convergence in Next Generation High Throughput Satellite Communications</td>
<td>Danilo Sparo</td>
<td>Prof. Dr. Björn Ottersten</td>
</tr>
<tr>
<td>RIMER - Risk Monitoring with Intrusion Detection for Industrial control systems</td>
<td>Steve Muller</td>
<td>Prof. Dr. Yves Le Traon</td>
</tr>
<tr>
<td>Hydlan - A Scalable Symbiotic Execution Framework for Detecting Vulnerabilities</td>
<td>Julian Thorne</td>
<td>Prof. Dr. Lionel Briand</td>
</tr>
<tr>
<td>RUCON - Rule Compilation for Software-defined Networks (SDN)</td>
<td>Stefan Hommes</td>
<td>Dr. Radu State</td>
</tr>
<tr>
<td>MOSER - Model-driven Software Engineering for Social Robots</td>
<td>Gary Cornelius</td>
<td>Prof. Dr. Holger Voelz</td>
</tr>
<tr>
<td>ColNav - Collision-free Navigation of Small UAS in Complex Urban Environments Using Prodictive Control</td>
<td>Arun Annaiyan</td>
<td>Prof. Dr. Holger Voelz</td>
</tr>
<tr>
<td>FLYMAN - Controller Design for Cooperative Flying Manipulation Using Small Quadrotors UASs</td>
<td>Jan Erik Dentler</td>
<td>Prof. Dr. Holger Voelz</td>
</tr>
<tr>
<td>TYPAMEO - Transparent yet Private Access to Medical Data</td>
<td>Davide Spagnuolo</td>
<td>Prof. Dr. Peter Y. A. Ryan</td>
</tr>
<tr>
<td>RECONTE - Reliable Communication Techniques for Future Generation Satellite Systems</td>
<td>Alberto Mengali</td>
<td>Prof. Dr. Björn Ottersten</td>
</tr>
</tbody>
</table>

**Ongoing**

<table>
<thead>
<tr>
<th>Project</th>
<th>Principal Investigator</th>
<th>Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>SATOCROSS - Support of Advanced Test Coverage Criteria for Robust and Secure Software</td>
<td>Michael Papadakis</td>
<td>Dr. Michael Papadakis</td>
</tr>
<tr>
<td>SURCVS - Secure, Usable, Robust Cryptographic Voting Systems</td>
<td>Peter Y. A. Ryan</td>
<td>Prof. Dr. Peter Y. A. Ryan</td>
</tr>
<tr>
<td>SODA - Spectral Efficient Receivers and Resource Allocation for Satellite Cognitive Systems</td>
<td>Symeon Chatzinotas</td>
<td>Dr. Symeon Chatzinotas</td>
</tr>
<tr>
<td>D-PHY - Exploiting Interference for Physical Layer Security in 5G Networks</td>
<td>Symeon Chatzinotas</td>
<td>Dr. Symeon Chatzinotas</td>
</tr>
<tr>
<td>ELEAH2 - Enhanced Daily Living and Health 2 - an incentive based service</td>
<td>Lionel Briand</td>
<td>Prof. Dr. Lionel Briand</td>
</tr>
<tr>
<td>IMWPNET - Integrated Wireless Information and Power Networks</td>
<td>Björn Ottersten</td>
<td>Prof. Dr. Björn Ottersten</td>
</tr>
<tr>
<td>CONTACT - Context and content Aware Communications for QoS support in VANETs</td>
<td>Thomas Engel</td>
<td>Prof. Dr. Thomas Engel</td>
</tr>
<tr>
<td>MaDSAV - Maintaining Driving Skills in Semi-Autonomous Vehicles</td>
<td>Thomas Engel</td>
<td>Prof. Dr. Thomas Engel</td>
</tr>
</tbody>
</table>
### OTHER PROJECTS FUNDED BY FNR

<table>
<thead>
<tr>
<th>Project</th>
<th>Principal Investigator</th>
<th>Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIMMS - Swarm Intelligent Mission system</td>
<td>Dr. Grégoire Danoy</td>
<td>POC</td>
</tr>
<tr>
<td>PreMAss - Predictive Maintenance as a Service</td>
<td>Dr. Jorge Augusto Meira</td>
<td>POC</td>
</tr>
<tr>
<td>NoCry Poc - No More Cryptographic Ransomware, Proof of Concept</td>
<td>Dr. Gabriele Lenzini</td>
<td>POC</td>
</tr>
<tr>
<td>GenoMask POC - Early Stage Read Filtering and Masking of Genomic Information</td>
<td>Dr. Marcus Völ</td>
<td>POC</td>
</tr>
<tr>
<td>Luxlog4AI 2018 - Luxembourg Logic for AI Summit</td>
<td>Prof. Dr. Leon Van Der Torre</td>
<td>RESCOM</td>
</tr>
<tr>
<td>AURORA - unpredictable Low-secPins For suPperHawce</td>
<td>Dr. Grégoire Danoy</td>
<td>PATHFINDER</td>
</tr>
<tr>
<td>Smart School 2025 - Smart School 2025: The Future Luxembourg Smart School</td>
<td>Dr. Djamilia Aouada</td>
<td>PSF</td>
</tr>
<tr>
<td>PREMA - Predictive Maintenance Analysis</td>
<td>Dr. Jorge Augusto Meira</td>
<td>PATHFINDER</td>
</tr>
<tr>
<td>QoE WC - Distributed optimization and dynamic programming for wireless edge caching to maximize quality of experience</td>
<td>Dr. Syunen Chatzinotas</td>
<td>INTER MOBILITY</td>
</tr>
<tr>
<td>DIAPOSELF - Data Protection Self-assessment Method For SMEs</td>
<td>Dr. Andra Giurgiu</td>
<td>PATHFINDER</td>
</tr>
<tr>
<td>SIGNUMA - Secure, Interoperable and Global Mobile Money in Sub-Saharan Africa</td>
<td>Dr. Tegawendé Bissyande</td>
<td>PATHFINDER</td>
</tr>
<tr>
<td>Autonomous Driving Demo</td>
<td>Dr. Raphaël Frank</td>
<td>RESEARCHERS NIGHT/DAY</td>
</tr>
<tr>
<td>NoCry - No More Cryptographic Ransomware</td>
<td>Dr. Gabriele Lenzini</td>
<td>PATHFINDER</td>
</tr>
<tr>
<td>GenoMask - Early Stage Read Filtering and Masking of Genomic Information</td>
<td>Dr. Marcus Völ</td>
<td>PATHFINDER</td>
</tr>
</tbody>
</table>

### OTHER PROJECTS

<table>
<thead>
<tr>
<th>Project</th>
<th>Principal Investigator</th>
<th>Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building an In-car Ethernet Testbed System</td>
<td>Prof. Dr. Thomas Engel</td>
<td>Honda Initiation Grant Europe</td>
</tr>
<tr>
<td>HUNTED - Heterogeneous multi-swarm of URFtanned autonomous systems for mission Deployment</td>
<td>Prof. Dr. Pascal Bouvry</td>
<td>US NAVY Research Office</td>
</tr>
</tbody>
</table>

**Completed**

- ARMLET - Automated Retrieval of Metadata from Legal Texts | Dr. Mehrdad Sabetzadeh | POC |
- ProDia3 - PRogramming Cognitive ROBots 3 | Prof. Dr. Leon Van Der Torre | POC |
- SERNASE - Satellite Preceding Hardware Demonstrator | Dr. Syunen Chatzinotas | POC |
- RANFAL - RainFall Estimation Using Signaling Data of Satellite Communication Network | Dr. Bhavani Shankar | POC |
- AIR - Air Frame Inspection | Dr. Miguel Angel Olivares-Mendez | POC |
- VLab Lab - Verification and Validation Laboratory | Prof. Dr. Lionel Briand | PEARL |

**Ongoing**

- TTO2.0-Leader | Prof. Dr. Björn Ottersten | KITS |
- 5G - Strategic RTN on Information Infrastructure Security and Dependability | Prof. Dr. Paulo Esteves-Veríssimo | PEARL |
- IndustPartnership2.0 | Dr. Marc Lemmer | KITS |

**We would like to thank the following organisations for their support:**


64. Ostaszewski, M., Kieffer, E., Danoy, G.,
63. Neveu, E., Popov, P., Hoffmann, A., Migliosi, A.,

57. Martinez, J., Ziadi, T., Papadakis, M., Bissyan-
56. Mazzali, N., Boumard, S., Kinnunen, J., Shan-
54. Bana, G., Chadha, R., & Eeralla, A. (2018). For-
53. Besseron, X., Danoy, G., Bouvry, P., & Grudinin,
51. Andrenacci, S., Duncan, J. C. M., Krivochiza,
50. Wolter, M., Zavala, S., & Schlenk, O. (2018). Near-

86. Symeonidis, I., Biczók, G., Shirazi, F., Pé-


