Acronym	RAIMo
Project title	A road toward safe artificial intelligence in mobility
Chair candidate	Stéphane Canu – LITIS – INSA Rouen Normandie
Chair participants	Alain Rakotomamonjy & Gilles Gasso – LITIS – INSA & Univ. R N
Requested funding	599 400 €
Project duration	48 months
Scientific field(s) of the project	Machine learning, Deep learning, Optimization, Mixed integer programing, Mobility, Autonomous vehicles

Contents

Project summary

Recent progresses in machine learning in general and especially in deep learning make it possible to include this technology in more and more autonomous vehicles. However, before this possible future becomes reality and our roads are made safer with algorithms replacing human drivers, it is necessary to know how to prove the quality of the decisions made.

This Chair project "A road towards Safe Artificial Intelligence for Mobility" is a research proposal aimed at strengthening local research dynamics about safety issues associated with the use of artificial intelligence in mobility. To achieve this goal, the project will endeavor to formalize the problem, to propose algorithms to solve it and to demonstrate its feasibility on real autonomous vehicles under real driving conditions.

The chair project will intervene, with the INSA and the University of Rouen Normandy as part of Normandy University, in all levels of engineering training and in training through research. To this end we will work with the Normandy University Research Institute (EUR) project MINMACS in the field of safe AI for mobility.

To reach these ambitious goals and to make the Madrillet Campus in Normandy an international reference in the field of AI for mobility, the Chair will benefit from: (i) a team of three professors combining the relevant scientific skills, (ii) financial support provided by INSA and the University of Rouen Normandy, (iii) scientific support from local and national laboratories with research in AI domain, (iv) facilities of the CRIANN (the regional on-site calculation center), and (v) the support of Rouen autonomous lab and its four autonomous vehicles operating on Campus of Madrillet.

Our ultimate goal is to contribute to make learning systems safe for mobility and beneficial to society.

1 Chair candidates presentation

The research program of the RAIMo Chair proposal has been elaborated by a team of three Full Professors, experts in machine learning, working in the same place and with a long and fruitful collaboration record. This team is composed of Stéphane Canu, the Chair holder, Gilles Gasso and Alain Rakotomamonjy. INSA Rouen Normandy is committed to recruiting a *Maitre de Conférence* (Associate Professor) in support of the Chair. The following table summarizes the Chair team.

Partner	Name		PM	Contribution to the project
INSA Rouen Normandy	Stéphane Canu	PU	20.4	Chair manager, Ph.D. advisory
INSA Rouen Normandy	Gilles Gasso	PU	7.2	Ph.D. advisory
Univ. Rouen Normandy	Alain Rakotomonjy	PU	7.2	Ph.D. advisory
INSA Rouen Normandy	MCF to be recruted	MCF	20.4	Investigator

Note that RAIMo also includes explicit partnerships with Vincent T'Kindt (Tour University) in the optimization domain, Laetitia Chapel (Université de Bretagne Sud) regarding optimal transport and Thierry Chateau from Institut Pascal (Clermont Auvergne University) for image processing all three through the joint advising of a RAIMo Ph.D. thesis.

Stéphane Canu[1] is Professor at INSA Rouen Normandy and a member of the LITIS Research Laboratory. He received a Ph.D. degree in applied mathematics from Compiegne University of Technology in 1986. He joined the faculty department of Computer Science at Compiegne University of Technology in 1987. He received the French habilitation degree from Paris 6 University. In 1997, He joined the INSA Rouen as a Full Professor, where he created the computer science department. In 2004 he joined for one sabbatical year the machine learning group at ANU/NICTA (Canberra) with Alex Smola and Bob Williamson. From 2006 to 2012 he has been the former executive director of the LITIS, an information technology research laboratory in Normandy. He is also a lecturer in machine learning at École Polytechnique since 2017.

He has been doing research for 35 years in the field of artificial intelligence, deep learning, machine learning and data science. He published its first research paper in the neural network domain in 1990. In the last five years, he has published approximately thirty papers in refereed conference proceedings or journals in the areas of kernels machines, regularization, optimization issues in machine learning, pattern classification and deep learning with a h-index of 34 according to Google Scholar. He was coordinator of a node of the Pascal excellence network. He is reviewer (JMLR, NIPS, ICML, ECML, KDD) and ERC referee. He has been an elected member of the IEEE Technical Committee for machine learning and signal processing from 2008 to 2012. He coordinated the ANR-funded KernSig and Deep in France program on the crucial issue of the energetic sobriety of deep learning. He is a member of the Normandy French Tech Board of Directors. He is also the scientific advisor of the startup Saagie. He was nominated by the "Usine Nouvelle" magazine among "the 100 Frenchmen who count in AI".

Gilles Gasso[2] has received a Ph.D. in Automatic Control and Signal Processing from Lorraine National Institute of Technology. From 2002 to 2012, he held a position of Associate Professor at INSA Rouen, affiliated to Computer Science Department. From thereon he held a Full Professor position at INSA Rouen Normandy. In 2008 he joined for one sabbatical year the machine learning group at NEC Labs (USA) with Léon Bottou. His research interests include machine learning and deep learning, non-convex optimization, with applications to signal and image processing.

Alain Rakotomamonjy[3] received the Ph.D. degree in signal processing from the University of Orléans, France, in 1997. He has been a Professor in the Department of Physics, University of Rouen Normandy, since 2006. His research interests include machine & deep learning, optimization, optimal transport and signal processing with applications to brain–computer interfaces and audio applications. He is area chair of NeurIPS and IJCAI.

[1] asi.insa-rouen.fr/enseignants/~scanu/
[2] asi.insa-rouen.fr/enseignants/~gasso/
[3] sites.google.com/site/alainrakotomamonjy/

2 Chair description

2.1 Originality, perspective, methodology

As noticed in a recent report from France Stratégie on Artificial Intelligence (AI) and work "the major innovation brought about by development of AI in the field of transport will undoubtedly be the autonomous vehicle, even though the timeline for its deployment remains uncertain". Driverless services have great potential for transforming mobility, especially towards greater sustainability. Now, even if in Rouen or in the Phoenix suburb of Chandler, commercial self-driving cars services are available, these remain experiments and, as claimed by McKinsey[4], "the automotive industry is still only at the beginning of the AI disruption". Furthermore, many people are still reluctant to these innovations because of concerns regarding the nature of Artificial Intelligence in autonomous vehicles and "society will reject autonomous agents unless we have some credible means of making them safe" [31]. Safety issues are of utmost importance in the automotive industry, particularly after the fatal accidents of Tesla and Uber self-driving cars. In driverless vehicles, safety must necessarily include machine learning algorithms and deep learning, as these techniques are becoming more prevalent in automotive software [for a review see for instance 8, 9]), but concerns on their safety and trustworthiness have been raised [12].

The security and reliability of real-world safety-critical mobile systems is primarily addressed in the industry through a certification process and an explanation process. The certification process is carried out before the product is put into service to ensure its safety. The manufacturer has to demonstrate to the relevant certification authority that the system fulfills the legal safety constraints. The explanation process can be seen as a user manual that should explain to a user the set of expected behaviors of the system. Machine learning solutions, if they demonstrated their effectiveness [4, 22], do not bring today expected security guarantees. For instance regarding certification, an important low-level requirement for deep networks is their robustness to input perturbations. It has been shown that neural networks are not robust since they are vulnerable against adversarial attacks, at a pixel level where imperceptible input perturbations cause neural networks to misclassify or by using patches on the input [27].

RAIMo is mainly concerned with the advance of enabling techniques for the certification to machine and deep learning systems. This is a challenging issue, owing to the black-box nature of deep neural networks and the lack of rigorous foundations. We have made this the starting point of our research proposal about artificial intelligence in mobility: how to keep it safe? Will roads be safer if algorithms replace human drivers? How can we trust deep learning based algorithms?

To answer these questions, RAIMo will explore new methods and systems which can ensure Artificial Intelligence systems such as deep neural networks are more robust, safe and interpretable for mobility applications by ensuring that deep networks and other machine learning systems do what its mint for them to do. Our research program focuses on these safety issues related to deep learning on three complementary aspects: theoretical foundations, algorithmic considerations and implementation for experimental validation.

The access to experimental real data (an associated real problems) are guaranteed by the partnership of RAIMo with the Rouen Autonomous Lab and the TIGA initiative (see associated support letter). We recall that four autonomous vehicles with equipped environment are being experimented on the Madrillet campus. The monitoring of this data will be addressed by RAIMo in two scientific directions. One regards robust perception via multimodality sensor redundancy and fusion while the other one is the analysis of input data via novelty detection. To get robust networks we propose investigating the use of certification techniques formalizing the problem. Existing complete verifiers are based on Mixed Integer Programming (MIP) [10, 16]. But these can only handle specific networks with a small number of layers and neurons, RAIMo research program is structured around these three points, (i) the theoretical aspects of robustness and associated optimization issues, (ii) aspects related to the monitoring of data and decisions and (iii) the experimental component.

[4] https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-road-to-artificial-intelligence-in-mobility-smart-moves-required

2.1.1 Deep learning safe decision: theoretical foundation

Once the autonomous vehicle perceives its surroundings, it then needs to make decisions. All these processes include the use of deep learning architectures that have driven dramatic performance advances but whose theoretical foundations remain poorly understood. While some progress has been made recently towards a foundational understanding of deep learning, most theory work has been disjointed, and a coherent picture has yet to emerge. A way to ensure safety, is to prove the robustness of the deep networks used in autonomous systems by obtaining provable guarantees that they satisfy specifications relating their inputs and outputs through their level of resistance to adversarial attacks. Recently, this verification problem has been formulated as a mixed integer program (MIP) seeking to find the largest violation of the specification. But this approach is currently only possible for relatively small feedforward networks, and it is not clear how to use it to train robust networks, particularly in a sustainable way [17, 28, 32].

Deep learning with safety guarantees Our starting point will be the definition of a robust learning system f at level ε as the following bi-level bi-objective optimization problem that can be seen as the following theoretical adversarial training problem

$$\min_f \mathbb{E}_{X,Y}(\text{loss}(f(X),Y)) \quad \text{and} \quad \max_f \mathbb{E}_X(\varepsilon(X)) \quad \text{with} \quad \varepsilon(x) = \min_z \|z-x\| \quad \text{s.t.} \quad \max_i f_i(z) > f_y(z).$$

The question is how to derive, from this principle, a generic, efficient and scalable learning algorithm with the expected robustness properties. Based on this principle, improved certification methods of neural networks against adversarial perturbations and providing an exact solution via MIP have been already proposed [2, 26, 29, 30], but yet addressing specific small size and specific neural architecture. Beyond this question of deep networks robustness, this research on MIP will encompass other optimization problems regarding deep and machine learning and related with combinatorial issues such as clustering or the ones related to the use of the ℓ_0 pseudo norm [15].

Available MIP solvers have the advantage of providing the unique global solution to the problem. However, at the scale of today's deep learning, they are not computationally efficient. To get this global solution more efficiently we will investigate the use of additional constraints as well as a clever initialization [5]. To this end, an efficient and scalable first order relaxation algorithm should be introduced. The local solution of the relaxed problem will be also used to get a relevant initial point in to the MIP. When coupled with adapted screening mechanism, the learning phase can be accelerated. Screening and relaxation for MIP initialization will be another important research direction [21].

Efficient MIP solver for machine learning Research is also needed to develop an efficient MIP solver specifically designed for deep and machine learning. This solver will embed dedicated exact or heuristic algorithms that exploit techniques from optimization field. Notably, branching algorithms [18] and mathematical programming [19] will be considered as they have been shown, along the years, highly effective in solving optimally a large panel of optimization problems. Besides, emerging techniques, like *memorization* [25] or *constraint generation approaches* [7], will be explored to speed up branching algorithms. The advantage of such algorithms is that they can be also easily transformed into heuristic algorithms: the optimal solution is no longer computed but at the gain of fast algorithms providing near-optimal solutions. Examples of heuristic branching algorithms are *beam search algorithms* and *Limited Discrepancy Search algorithms* [19]. The design of such exact or heuristic algorithms will be done by exploiting properties from the optimization problems emerging from machine learning.

Robust transfer learning Deep networks are trained based on data acquired at certain places and in certain environmental condition and even sometimes through simulation. Associated decision systems are supposed to be able to operate in the real world, often in uncontrolled and unpredictable environments. Our objective is to train a deep network from finitely many training samples that will perform well on unseen test samples [11]. We plan to tackle this problem through domain adaptation by learning matched representations and by integrating constraints in the spirit of distributionally

robust optimization when considering that our distributional uncertainty region is based on optimal transport and Wasserstein distance [14].

2.1.2 Safe perception for autonomous driving

Recent advancements in autonomous driving are mostly driven by vision-based deep learning. In order to achieve robust and accurate scene understanding, autonomous vehicles are usually equipped with different sensors (e.g. cameras, LiDARs, Radars), and those multiple sensing modalities can be fused to exploit their complementary properties. Despite significant improvements during the last decade on both sensors and scene understanding algorithms, embedded novelty/anomaly detection based on those multimodal perception is still lacking and we also envision that safe perception can also benefit from non-vision based perception.

Multimodal perception Multimodal perception in autonomous driving is mostly focused on different vision sensors. In this project, our objective is to exploit an under-tapped perception modality for assistive driving: audio. While sound events occuring on a road may have few impacts on driving in normal situations, abnormal situations or rare driving events may be characterised by sounds (breaks, going off tracks, screams...) While several works have addressed the problems of audio event classifications [13, 23], in RAIMo, we will tackle the question of detecting rare audio events [3] as a proxy for abnormal driving situation detection. For achieving this goal, we will investigate embedding-based unsupervised/weakly-supervised representation learning with regularizers encouraging compactness of known audio sound events and known normal audio background. We envision that such regularizers can be encoded through an appropriate design of several triplet losses and that end-to-end anomaly detection can be achieved by considering a loss function evaluating volume of empirical distributions of the embeddings.

Note that discussions have been carried about with Gael Richard from Telecom Paristech and Valéo AI to articulate our proposal regarding audio processing with the AI Chair proposal MALIS.

Novelty detection To be safe, a decision device learned from data requires a mechanism that adapts the decision according to whether or not there is a discrepancy between the distribution $p_{\text{train}}(X, Y)$ of the training samples and the ones of test samples $p_{\text{infer}}(X', Y')$. In case of distribution shift, deep-based-approaches may be overconfident and tend to treat the given inputs as one of the previously seen situations leading to mislabelling [1]. This brings to the scientific challenges of detecting out-of-distribution samples (the test point x' is marginally sampled from $p_{\text{infer}}(X') \neq p_{\text{train}}(X)$) or of recognizing that point x' belongs to an unseen class (new type of object occurs in the scenes) [24]. Moreover due to the multimodal nature of the inputs and sensors availability, the samples may not be embedded into the same space, and hence compromising the success of the detection task. We envision to leverage on optimal transport theory [20] to implement algorithms dealing with out-of-distribution detection in road scene data. Also we will investigate how to learn an appropriate metric and to design robust two-sample tests over metric-measure spaces [6] to cope with difference in embeddings and to ensure the minimal worst-case risk in novel samples detection.

2.1.3 Experimental safety in autonomous vehicles

To assess the reliability of an autonomous vehicle, the use of real data representing the many scenarios that it may face is needed. To this end, our project is articulated with the TIGA Rouen Normandy program *Mobilité intelligente pour tous* in general and especially with its action 1 "Deploy the autonomous vehicle in the metropolitan public transportation network". Among possible risks identified within TIGA, three of them are related with safety issues addressed by our core research program: accident risk, legal issues related with the need of a safety driver and social acceptance.

TIGA's autonomous vehicles will be used as a test platform to challenge the proposed solutions for guaranteed safe decisions while using software-based autonomous driving systems. TIGA will provide

us with hours of autonomous driving records and will validate proposed solutions in real driving conditions.

Note that we are aware of ethical aspects of AI in autonomous vehicles and we do believe these are very important but away from the scope of the project.

2.2 Feasibility of the chair project

The scientific background of the team: scientific expertise of the permanent staff of the Chair include machine learning, deep learning, optimization issues in machine learning and MIP and optimal transport. The expertise is evidenced by publication records in JMLR, IEEE transactions journals, NeurIPS, ICML and ECML.

The AI component of the Madrillet mobility campus: RAIMo is hosted in the Madrillet campus located at the south of Rouen. With 8000 engineer students expected in 2020, this campus is ready to compete at the highest international level. The goal is to develop the attractiveness of the campus as well as cultural life and scientific excellency. It benefits from existing infrastructures such as the CRIANN which offers HPC facilities and technical support to research teams for porting and optimization HPC-based calculation codes. It also hosts the Rouen Normandy Autonomous Lab (RAL), a joint private-public partnership associating Transdev, Renault and Matmut to name a few corporations. This lab experiments **the first on-demand mobility service** in Europe, delivered with electric autonomous cars driving on open roads, and accessible to the public. It will also host the PIA3's program TIGA « Mobilité Intelligente pour Tous ». This project carries an ambition of in-depth transformation of the urban mobility: ensuring total continuity of travel and significantly reducing the use of the car by developing new operational tools for intermodality and multimodal mobility. For this sake, TIGA pursues an ambitious research program including research in AI. RAIMo will strongly interact with TIGA and the RAL (see the letter in the associated materials). Thanks to these collaborations, RAIMo will have access to real mobility data and experimental autonomous cars in real conditions on which real-life experiments can be conducted. Furthermore, RAIMo will benefit from companion research in data science and mathematics carried out on the Madrillet campus in the LITIS, LMI and LMRS CNRS lab in mathematics.

Note that the Madrillet campus is well known in the french machine learning community since it hosted CAp, the french machine learning conference in 2018 and RFIA in 2015.

AI in Normandy: RAIMo will also benefit from the regional dynamics about AI. First it has to be seen as a part of a regional network including 2 AI Chair proposals. Behind this initiative there are the IT research labs GREYC and LITIS, the research federation NormaSTIC and Norman mathematical research labs LMNO, LMRS and LMI. All these researchers are associated at the regional level in a *Réseau d'Intérêt Normand* (RIN) funded by the region through Normandy University. These structures support RAIMo (see associated support letters) with the vision of creating **a regional network on AI**. These supports have already been concretized by 2 research grants on AI and deep learning involving permanents of the Chair. They are : (i) the two years joint research grant **Norman'deep** which PI are F. Jurie for GREYC and S. Canu for LITIS, and (ii) **the labcom IGIL** associating the SME Itekube with the GREYC and the LITIS with topic related to the design of intelligent user interfaces using machine learning. Another regional project has strong synergies with RAIMo: the Norman **Datalab**, an innovative initiative to build a data ecosystem in Normandy. Like the RAL and TIGA, it is based on a public-private partnership involving both communities, companies and research laboratories in Normandy. Stéphane Canu is a founding member of the Datalab, so the Chair will benefit from its industrial network, including the Norman nugget Saagie which of he is scientific advisor.

Another important regional initiative to be coordinated with the AI Norman Chairs is **the EUR MINMACS Grad'School** about MAthematiCs and Information Science in Normandy. The MINMACS ambitions to become an international reference center for research and education in digital

science. To achieve such a goal, the scientific scope has been focused exclusively on Norman areas of excellence and on the fact that Mathematics and Information Science complement each other naturally. The AI curriculum proposed within the Chair proposal will benefit from the dynamic created by this Norman Graduate School.

Partnership away from Normandy: More than a Chair, RAIMo is a node of a network involving many partners. This network will capitalize and strengthen on the partnerships elaborated within collaborative research projects such as in 2016 the ANR project "Deep in France" coordinated by Stéphane Canu. Two partners of the former project are in 3IA institutes: Jakob Verbeek in "MIAI@Grenoble-Alpes" and Frédéric Précioso in "3IA Côte d'Azur". A. Rakotomamonjy and G. Gasso are active members of the French ANR OATMIL (Bringing Optimal Transport and Machine Learning Together) including connections with Rémi Flamary also involved in "3IA Côte d'Azur". Also, in 2017 the LITIS was granted the ANR Icub on non-conventional imaging for secure mobility in urban areas and involving Stereolabs and PSA as industrial partners. S. Canu has been appointed expert on deep learning with Renault. A. Rakotomamonjy is PI of the ANR Leauds on learning audio scene. Note regarding the HPC needs of RAIMo, S. Canu is a member of advisory board of Jean Zay, the french national HPC resources center.

RAIMo also includes explicit partnerships with Vincent T'Kindt (University of Tour), Laetitia Chapel (Université de Bretagne Sud) and Thierry Chateau from Institut Pascal (Clermont Auvergne University) evidenced by the co advising of Ph.D thesis. Ultimately, RAIMo will take advantage of international relationships of the team members attested by joint paper with Léon Bottou and Alex Smola for AI and Alberto Broggi in the intelligent transportation domain. S. Canu has also connections with Yann LeCun and Yoshua Bengio for quite a long time.

3 Impact of the Chair

3.1 For INSA Rouen Normandy, Madrillet campus and Normandy University

RAIMo is aligned with the INSA strategic objective of making the Madrillet a reference campus in the field of mobility ad engineering. Hence, beyond INSA Rouen, it's on the whole Madrillet campus that RAIMo will impact by making it a reference at the best international level in the field of secure AI for mobility. RAIMo aims at pooling and leveraging skills and resources in safe deep learning and specific high performance computing (HPC) for machine learning. It will bridge the gap between fundamental research in AI and application within self driving cars of the Rouen Autonomous Lab and mobility issues related with the TIGA initiative.

3.2 With regard to the national AI program

RAIMo is essentially focused on safe deep learning and involving very-large scale complex optimization problems. Regarding topics, transportation/mobility targeted by RAIMo is one of the four strategic sectors AI in France should focus in. Also, *developing the reliability, safety and security of AI technology* is identified as a key point to develop *an economic policy based on data.*

As stated above RAIMo aims at setting the foundation stone of Normandy research network within the data science RIN and has strong interaction with the Norman Datalab, a model of public-private partnerships of which Stéphane Canu is the scientific advisor. RAIMo will interact with the 3IA institutes and their future network based on well established collaborations such as the ones with Massih Amini and Jakob Verbeek from "MIAI@Grenoble-Alpes", Rémi Flamary and Frédéric Précioso from "3IA Côte d'Azur".

RAIMo will also address the shortage of engineers and Ph.D. students trained in artificial intelligence.

Based on its existing collaborations with Sherpa Engineering, Renault, Transdev (via RAN & TIGA) and contacts with Valéo AI and PSA, our Chair proposal will also improve knowledge transfer to startups, SMEs and larger corporations.

3.3 Impact on training AI program

The Chair will intervene, together with the INSA Rouen Normandy as part of Normandy University, in all levels of engineering training and in training through research programs. Thus, RAIMo will actively participate in the specialization and outreach of the Madrillet campus in the field of AI and mobility. It will be also deeply involved in the EUR MINMACS Grad'School project of Normandy University, specifically in the field of safe AI for mobility by proposing a minor.

AI engineering training: programs in AI engineering aim at preparing engineers to become experts at identifying, modeling and implementing AI applications in a mobility related business in order to create value from data and to improve their competitiveness. Staff involved with RAIMo will start by promoting the culture of data and artificial intelligence to all engineer-students. To this end we will introduce to learning outcomes of the domain by promoting, at undergraduate level (Bac + 2) a course of 42 hours entitled **Introduction to data science** open to all students. **A specialized training course of one year (210 h) in AI for mobility** oriented on safety issues for bac+4/5 students will be developed within the existing teaching departments of the INSA Rouen Normandy. It will include lectures such as deep learning, optimization for machine learning, computational and implementation issues in deep and machine learning, explainable AI, machine learning for mobility and Self-Driving Cars and unsupervised learning. These lectures will be shared within the Normandy University and proposed also at the master level (see below). A the bac+6 level, we will develop the alternate work-study program **Mastères spécialisés Expert en sciences des données** on AI to reinforce our industrial partnerships and to promote the AI culture within business industries.

AI in the MINMACS Grad'School: the MINMACS Grad'School intends to become an internationally renowned research and education center bringing together the Norman experts in Mathematics and Information Science, on a number of high-profile interdisciplinary challenges in digital science. It has been proposed for an EUR grant by the Comue Normandy University who also supports RAIMo (see attached support letters). Thanks to this coordination at regional level throughout Normandy, RAIMo will organize and energize the **minor "AI for mobility"** within the major "Data Science" of the joint Master's degree program. The students, selected according to the highest standards and assisted by academic mentors, will elaborate their own course of studies with majors and minors from the offered curriculum. This will lead to employment in industry, thanks to close contact with economic players and by an alumni association. Together with MINMACS, RAIMo will organize **summer schools** designed for Master's, Ph.D. students, a few selected undergraduate students, with participation of international scholars and industrials.

Other impacts of RAIMo on training AI program: a Small private online course (**Spooc**) on advance issues related with safety issues in deep learing will be set up. It will include practical session with python, blended learning and flipped classroom.

These coordinated training actions aim to **increase the flows of AI engineers** trained with competencies in data science for mobility.

3.4 Valorisation

A valorisation strategy including both dissemination and exploitation activities will be outlined at the very beginning of the project. We will pursue two main goals: (1) inform a large public about the know-how and technology being developed within RAIMo, and (2) help RAIMo to reach a very high profile and visibility, both nationally and internationally. This will be achieved by:

- Encouraging RAIMo researchers to publish in major international conferences and journal articles, where the ANR funding will always be duly acknowledged. We will seek publications with joint authorship between partners as much as possible.
- Website and newsletter: A project website that will provide information about project objectives, partners, main results, publications, internal/external events and news in a comprehensive way will be set up and properly maintained. Moreover, a newsletter will be published based on

partners' inputs and contributions and will provide updates on recent activities and developments as well as the current status of the project. The newsletter will be disseminated on various platforms including the project website and special email lists.

- Organization of international workshops in conjunction with international conferences (such as ICML or NeurIPS) and summer school, coordinated with other initiatives such as the ones coming out from AI institutes. These workshops should involve talks from RAIMo researchers, live demonstrations and prestigious invited speakers such as R. Urtasun (Uber), P. Perez (Valéo AI), A. Broggi, Y. Bengio, L. Bottou and Y. LeCun. Thanks to our previous relationship with them, they may consider positively such invitations.
- Open source: platforms and software libraries developed within RAIMo will be open source and freely available. To facilitate technology transfer, we ensure all development will take place in one of the major platforms such as Pytorch, Keras, or TensorFlow. Interaction with scikitlearn will be also considered.

New research directions will be defined upon research breakthroughs coming out from the project. Long-term technology transfer will be encouraged, and INSA Rouen Normandy together with Normandy University have a longstanding experience in technology transfer.

4 Budget

The funding of the project includes staff and Operating costs. Regarding staff issues, an associate professor will be recruited by INSA to its research within RAIMo, a research engineer to work on the experiment platform and six Ph.D. students are also planned.

The permanent staff involved (S. Canu, G. Gasso and A. Rakotomamonjy and future associate professor) are the basis of the project. The research engineer to be hire will be its corner stone since he or she will be in charge of the practical implementation. Finally, the 6 Ph.D. student are its spearhead. Three Ph.D. will begin on the first year of the Chair while the remaining are planned to be launched one year after. The proposed theses will cover the following topics:

1. Safe decision in deep learning as a MIP advised by S. Canu.
2. MIP solver for machine learning in co-advised by S. Canu and Vincent T'Kindt (Univ. of Tours).
3. Audio scene analysis and rare audio event detection advised by A. Rakotomamonjy.
4. Optimal transport for out-of-distribution detection, advised by G. Gasso and A. Rakotomamonjy.
5. Robust two sample tests for novelty detection, co-advised by G. Gasso and Laetitia Chapel (Université de Bretagne Sud).
6. The CIFRE Ph.D. with Sherpa Engineering will be on the problem of *data based safety in transfer learning*. It will be co-advised by S. Canu in collaboration with Thierry Chateau from Institut Pascal (Clermont Auvergne University).

References

[1] Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., and Mané, D. (2016). Concrete problems in ai safety. *arXiv preprint arXiv:1606.06565*.

[2] Anderson, R., Huchette, J., Tjandraatmadja, C., and Vielma, J. P. (2019). Strong mixed-integer programming formulations for trained neural networks. In *ICIPCO*. Springer.

[3] Arora, V., Sun, M., and Wang, C. (2019). Deep embeddings for rare audio event detection with imbalanced data. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 3297–3301. IEEE.

[4] Bansal, M., Krizhevsky, A., and Ogale, A. (2018). Chauffeurnet: Learning to drive by imitating the best and synthesizing the worst. *arXiv preprint arXiv:1812.03079*.

[5] Bertsimas, D., King, A., Mazumder, R., et al. (2016). Best subset selection via a modern optimization lens. *The annals of statistics*, 44(2):813–852.

[6] Brécheteau, C. et al. (2019). A statistical test of isomorphism between metric-measure spaces using the distance-to-a-measure signature. *Electronic Journal of Statistics*, 13(1):795–849.

[7] Della Croce, F., Koulamas, C., and T'kindt, V. (2017). A constraint generation approach for two-machine shop problems with jobs selection. *European Journal of Operational Research*, 259(3):898–905.

[8] Falcini, F., Lami, G., and Costanza, A. M. (2017). Deep learning in automotive software. *IEEE Software*, 34(3).

[9] Feng, D. and et al. (2019). Deep multi-modal object detection and semantic segmentation for autonomous driving: Datasets, methods, and challenges. *arXiv preprint arXiv:1902.07830*.

[10] Fischetti, M. and Jo, J. (2018). Deep neural networks and mixed integer linear optimization. *Constraints*, 23(3):296–309.

[11] Gao, R., Xie, L., Xie, Y., and Xu, H. (2018). Robust hypothesis testing using wasserstein uncertainty sets. In *Advances in Neural Information Processing Systems*, pages 7902–7912.

[12] Huang, X., Kroening, D., Kwiatkowska, M., Ruan, W., Sun, Y., Thamo, E., Wu, M., and Yi, X. (2018). Safety and trustworthiness of deep neural networks: A survey. *arXiv preprint arXiv:1812.08342*.

[13] Jansen, A., Plakal, M., Pandya, R., Ellis, D. P., Hershey, S., Liu, J., Moore, R. C., and Saurous, R. A. (2018). Unsupervised learning of semantic audio representations. In *ICASSP*, pages 126–130. IEEE.

[14] Kuhn, D., Mohajerin Esfahani, P., Nguyen, V. A., and Shafieezadeh Abadeh, S. (2019). Wasserstein distributionally robust optimization: Theory and applications in machine learning. Technical report.

[15] Liu, Y., Canu, S., Honeine, P., and Ruan, S. (2019). Mixed integer programming for sparse coding: Application to image denoising. *IEEE Transactions on Computational Imaging*.

[16] Lomuscio, A. and Maganti, L. (2017). An approach to reachability analysis for feed-forward relu neural networks. *arXiv preprint arXiv:1706.07351*.

[17] Mirman, M., Gehr, T., and Vechev, M. (2018). Differentiable abstract interpretation for provably robust neural networks. In *International Conference on Machine Learning*, pages 3575–3583.

[18] Morisson, D., Jacobson, S., Sauppe, J., and Sewell, E. (2016). Branch-and-bound algorithms: A survey of recent advances in searching, branching, and pruning. *Discrete Optimization*, 19:79–102.

[19] Nemhauser, G. and Wolsey, L. (1999). *Integer and Combinatorial optimization*. Wiley.

[20] Peyré, G., Cuturi, M., et al. (2019). Computational optimal transport. *Foundations and Trends® in Machine Learning*, 11(5-6):355–607.

[21] Rakotomamonjy, A., Gasso, G., and Salmon, J. (2019). Screening rules for lasso with non-convex sparse regularizers. *arXiv preprint arXiv:1902.06125*.

[22] Schwarting, W., Alonso-Mora, J., and Rus, D. (2018). Planning and decision-making for autonomous vehicles. *Annual Review of Control, Robotics, and Autonomous Systems*, 1:187–210.

[23] Serizel, R., Turpault, N., Eghbal-Zadeh, H., and Shah, A. P. (2018). Large-scale weakly labeled semi-supervised sound event detection in domestic environments. *arXiv preprint arXiv:1807.10501*.

[24] Shafaei, A., Schmidt, M., and Little, J. (2018). Does your model know the digit 6 is not a cat. *A less biased evaluation of" outlier" detectors. CoRR, abs/1809.04729*.

[25] Shang, L., T'kindt, V., and Della Croce, F. (2018). The memorization paradigm: Branch & memorize algorithms for the efficient solution of sequencing problems. *HAL preprint https://hal.archives-ouvertes.fr/hal-01599835v2*.

[26] Singh, G., Gehr, T., Püschel, M., and Vechev, M. (2019). Boosting robustness certification of neural networks. In *ICLR*.

[27] Thys, S., Van Ranst, W., and Goedemé, T. (2019). Fooling automated surveillance cameras: adversarial patches to attack person detection. In *CVPR Workshops*.

[28] Tian, Y., Pei, K., Jana, S., and Ray, B. (2018). Deeptest: Automated testing of deep-neural-network-driven autonomous cars. In *Proceedings of the 40th international conference on software engineering*, pages 303–314. ACM.

[29] Tjeng, V., Xiao, K. Y., and Tedrake, R. (2019). Evaluating robustness of neural networks with mixed integer programming. In *ICLR*.

[30] Wang, S., Pei, K., Whitehouse, J., Yang, J., and Jana, S. (2018). Efficient formal safety analysis of neural networks. In *Advances in Neural Information Processing Systems*, pages 6367–6377.

[31] Weld, D. and Etzioni, O. (1994). The first law of robotics (a call to arms). In *Proceedings of the Twelfth AAAI National Conference on Artificial Intelligence*, pages 1042–1047. AAAI Press.

[32] Wong, E. and Kolter, Z. (2018). Provable defenses against adversarial examples via the convex outer adversarial polytope. In *International Conference on Machine Learning*, pages 5283–5292.