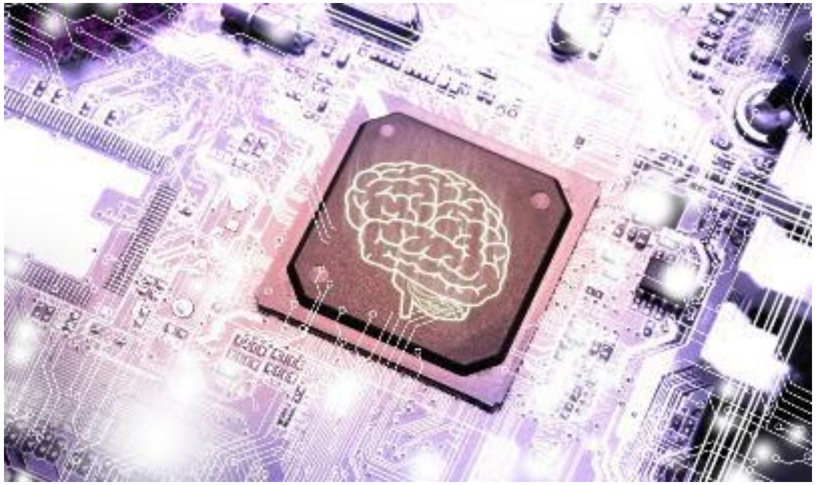


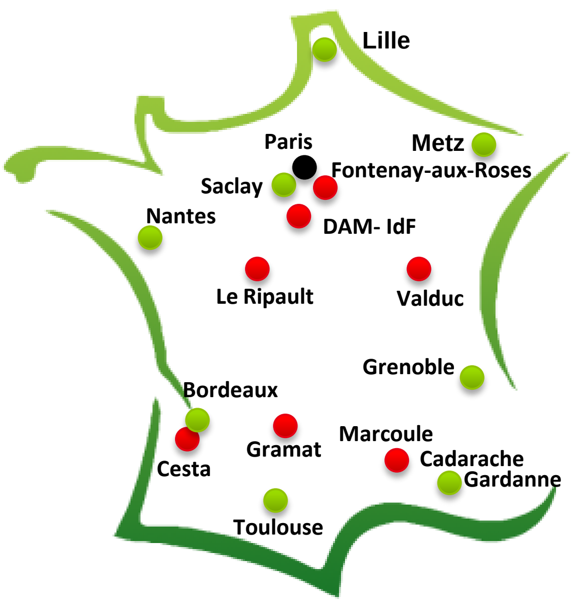
NEURO COMPUTING @ CEA TECH

Sandrine Varenne (Responsable partenariats industriels)
Etienne Hamelin (Chef du laboratoire cybersécurité)
Christian Gamrat (Responsable scientifique)
DACLE, Département Architecture Conception Logiciels Embarqués

- A short presentation of CEA Tech
- Neuromorphic Engineering
- Current Research
- Neuromorphic perspectives
- Cybersecurity
- Perspectives in Cybersecurity

CEA: FROM RESEARCH TO INDUSTRY

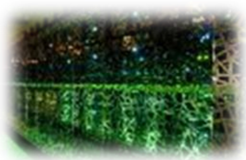
- » 16 000 employees
- » 10 research centers
- » 4 regional extensions
- » Budget of 4.3 billion €
- » 650 patents/year
- » 4700 publications/year
- » 50 Joint Research Laboratory
- » 170 startup creations in 40 years



Direction

Defense Security

Military Applications Division

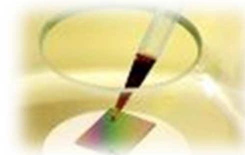


Nuclear Energy

Nuclear Energy Division

Key Enabling Technologies

cea tech



Technology

Fundamental research

Materials Sciences Division

Life Sciences Division

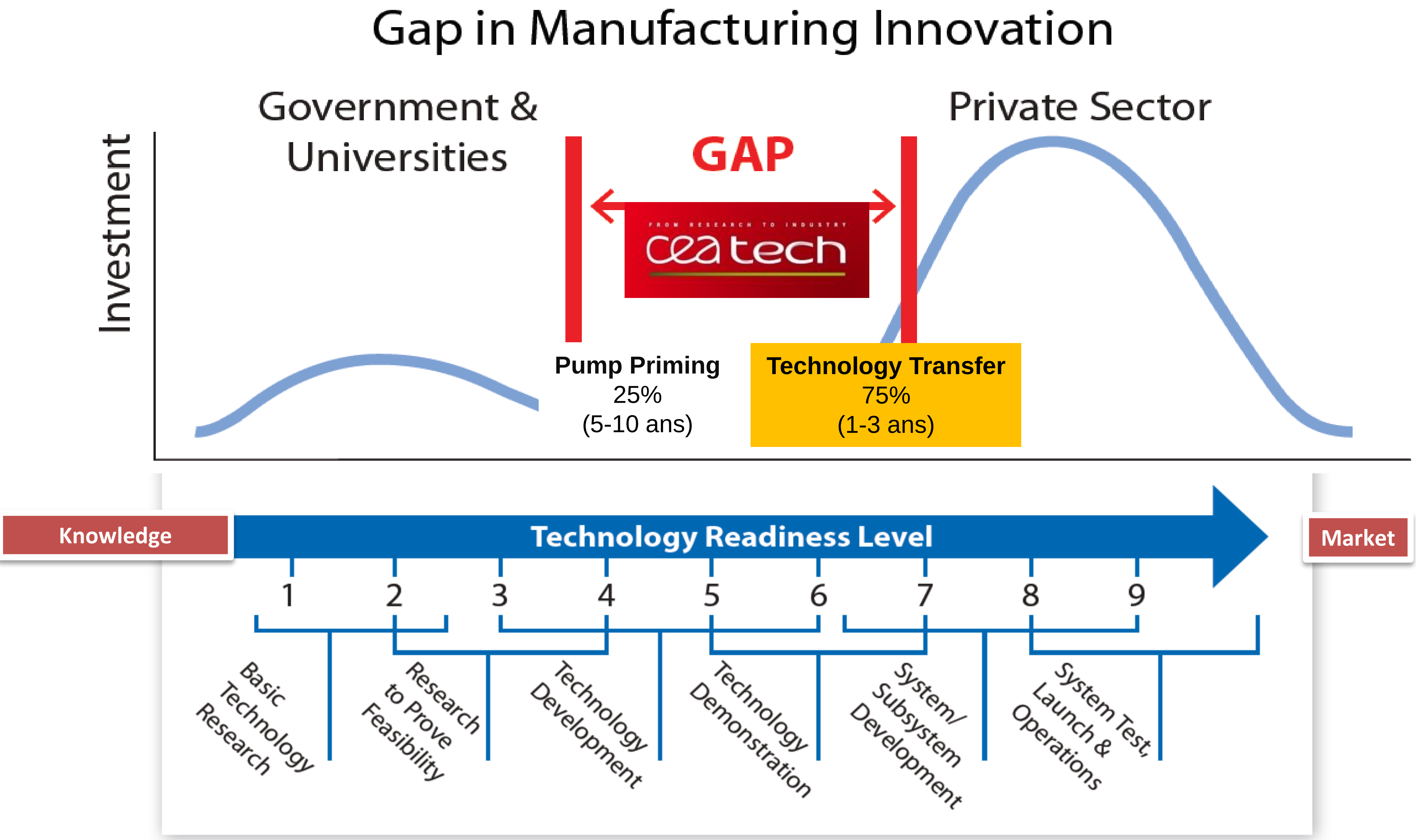
Science

MISSION : TO DEVELOP AND DISSEMINATE NEW TECHNOLOGY FOR INDUSTRY

- Annual operating budget of more than **€500 M**
- More than **50 HIGH-TECH START-UP** over the past 10 years
- **4,500 EMPLOYEES**
- **550 PRIORITY PATENT** applications per year par an

- **Our CUSTOMERS** :
  - ✓ **80 %** listed on the **CAC 40**
  - ✓ More than **500 SMBS**
  - ✓ **145 INTERNATIONAL CUSTOMERS**

CEA TECH: BRINGING COMPETITIVENESS TO OUR CUSTOMERS



Source: AMP Steering Committee

List Institute : YOUR INNOVATION PARTNER FOR THE DIGITAL TRANSITION

DISTINCTIVE STRENGTHS

1 Our Scientific Excellence

Maintaining our commitment to a high level of R&D activity,
in partnership with leading academic institutions

2 Industrial Culture

Responding to industries' needs
via long-term collaborative relationships

3 The Strength of our Ecosystem

« Technology Suppliers – Systems Integrators – End-Users »

4 Our Openness to the World

Addressing major societal & economic challenges

Reuters release – March 8th, 2016

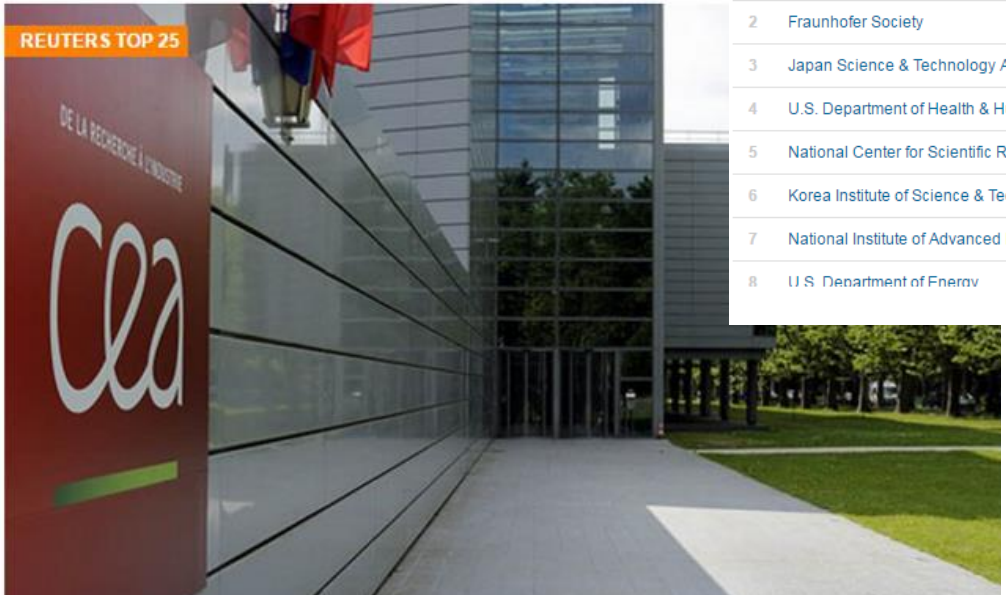
REUTERS EDITION: U.S. SIGN IN | REGISTER Search Reuters

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS MONEY LIFE PICTURES VIDEO

Technology | Tue Mar 8, 2016 12:36pm EST Related: SCIENCE, TECH

The World's Most Innovative Research Institutions

BY DAVID EWALT



TOP 25 INSTITUTIONS | 2015 RANKINGS

1	Alternative Energies and Atomic Energy Commission	FRANCE	Score: 206
2	Fraunhofer Society	GERMANY	Score: 202
3	Japan Science & Technology Agency	JAPAN	Score: 201
4	U.S. Department of Health & Human Services	USA	Score: 193
5	National Center for Scientific Research	FRANCE	Score: 189
6	Korea Institute of Science & Technology	SOUTH KOREA	Score: 183
7	National Institute of Advanced Industrial Science & Technology	JAPAN	Score: 182
8	U.S. Department of Energy	USA	Score: 179

cea tech

Principaux déposants de France à l'OEB – 2015
(par nombre de demandes)

1	TECHNICOLOR	769
2	COMMISSARIAT A L'ENERGIE ATOMIQUE	592
3	VALEO	521
4	ALCATEL LUCENT	474
5	SANOFI	454
6	SAFRAN	422
7	SAINT-GOBAIN	317
8	INSTITUT NATIONAL DE LA SANTE ET DE LA RECHERCHE MEDICALE	263
9	PSA PEUGEOT	246
10	RENAULT	235
11	SCHNEIDER ELECTRIC	234
12	THALES	214
13	L'OREAL	201
14	MICHELIN	189
15	CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE	165
16	ORANGE	163
17	ESSILOR	154
18	L'AIR LIQUIDE	149
19	ARKEMA	137
20	TOTAL	112
21	SEB	96
22	IFP ENERGIES NOUVELLES	82
23	ALSTOM	55
24	NEXANS	49
25	AREVA	48
25	ROQUETTE FRERES	48
27	SAGEMCOM	45
28	INSTITUT NATIONAL DE LA RECHERCHE AGRONOMIQUE	36
29	ELECTRICITÉ DE FRANCE	35
29	INGENICO GROUP	35

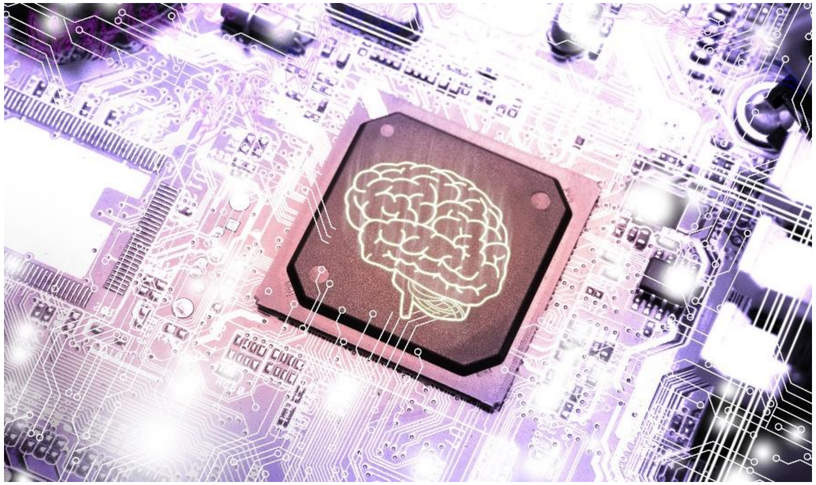
Source: Office européen des brevets.

*"Silicon Valley's hoodie-wearing tech entrepreneurs are the poster kids of innovation. But the innovators who are really changing the world are more likely to wear labcoats and hold government-related jobs in **Grenoble**, Munich or **Tokyo**."*

INSTITUT CARNOT CEA LIST

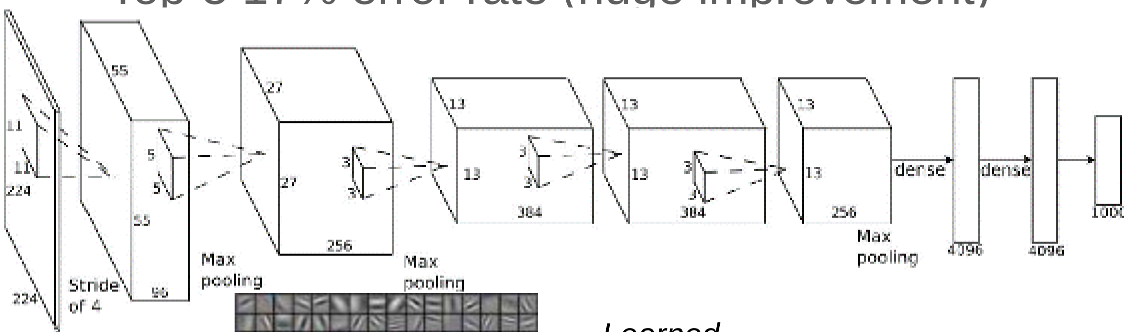
université PARIS-SACLAY

- A short presentation of CEA Tech
- **Neuromorphic Engineering**
- Current Research
- Perspectives



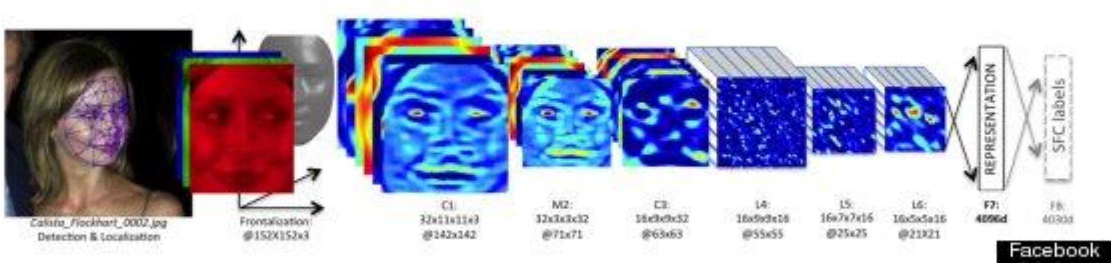
NEURAL NETWORKS: HOW SMART CAN WE GET?

- **ImageNet classification (Hinton's team, hired by Google)**
  - 1.2 million high res images, 1,000 different classes
  - Top-5 17% error rate (huge improvement)

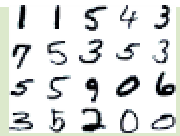


Learned features on first layer

- **Facebook's 'DeepFace' Program (labs head: Y. LeCun)**
  - 4 million images, 4,000 identities
  - 97.25% accuracy, vs. 97.53% human performance



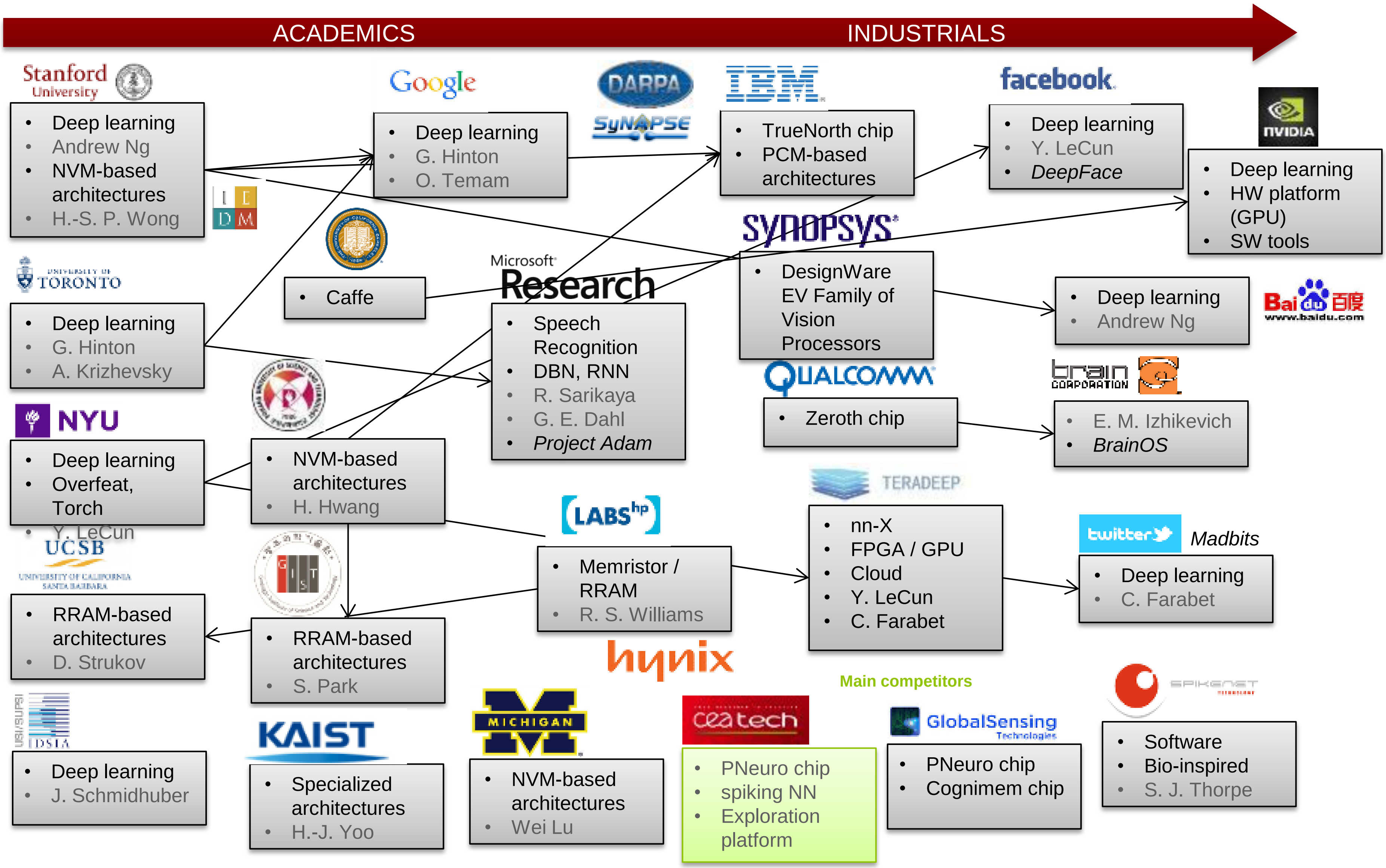
STATE-OF-THE-ART IN IMAGE RECOGNITION

Database		# Images	# Classes	Best score
MNSIT Handwritten digits		60,000 + 10,000	10	99.79% [3]
GTSRB Traffic sign		~ 50,000	43	99.46% [4]
CIFAR-10 airplane, automobile, bird, cat, deer, dog, frog, horse, ship, truck		50,000 + 10,000	10	91.2% [5]
Caltech-101		~ 50,000	101	86.5% [6]
ImageNet		~ 1,000,000	1,000	Top-5 83% [1]
DeepFace		~ 4,000,000	4,000	97.25% [2]

INCREASING COMPLEXITY

- **State-of-the-art are Deep Neural Networks *every time***

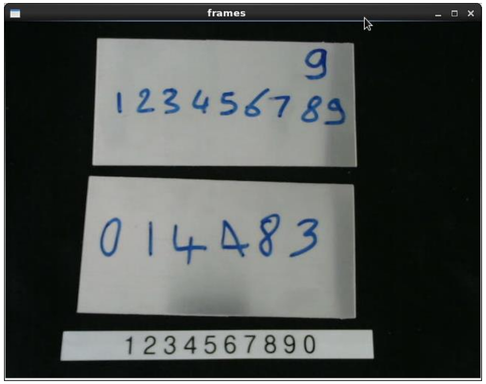
MAIN ACTORS AT INTERNATIONAL LEVEL



REAL-TIME EMBEDDED DIGITS RECOGNITION

Real-time digits recognition

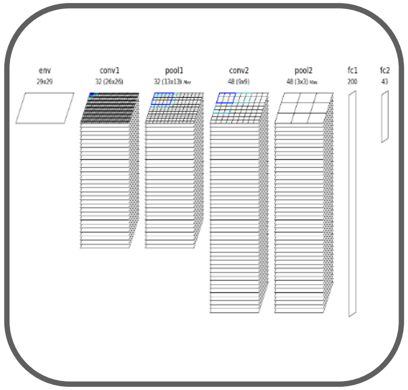
- Problem: recognize handwritten digits on numbered metal plates
  (in real time on a conveyor belt)
- Using standard webcam (640x480)
- MNIST database used for learning



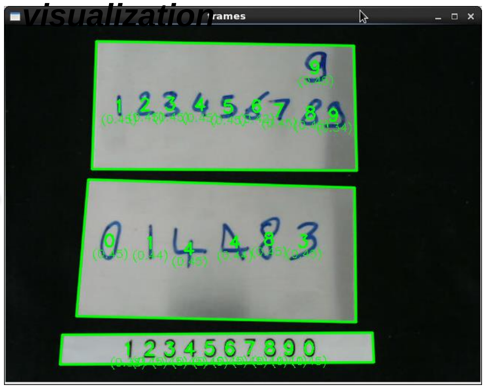
1) Plates extraction, perspective correction and segmentation

2) Digits extraction and normalization

3) Digits recognition with embedded CNN



4) Numbered plates with identification results visualization



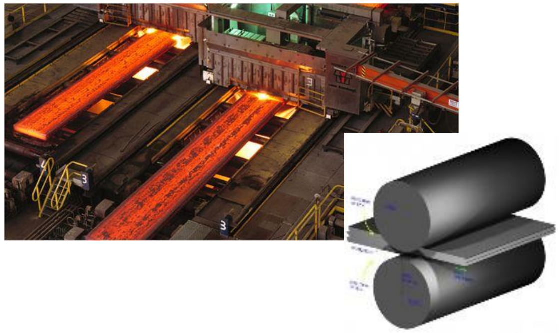
Performances: (digits recognition)

Platform	Performances (digits/s)
FPGA (HLS)	**1,000,000**
NVIDIA Tegra K1	364
NVIDIA Geforce GTX Titan X	12,500
Intel Xeon E5-2643 @ 3.4 GHz	67,000
NVIDIA Tegra K1 (**batch**)	50,000
NVIDIA Titan X (**batch**)	1,333,333

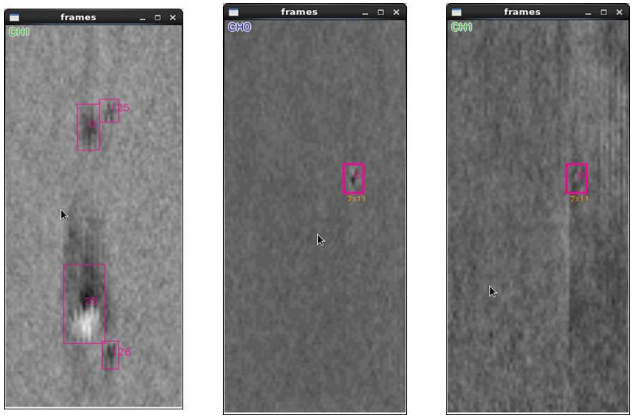
PART INSPECTION (CONFORMITY, DEFECTS…)

Defects identification on metal after rolling

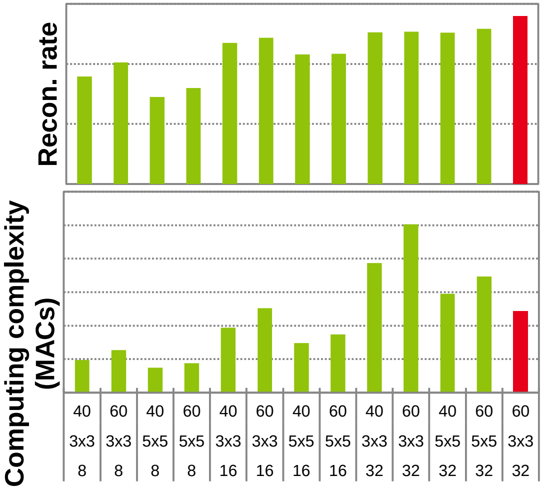
- Constraints:
  - Real-time with extremely high throughput
  - Tiny and low contrasted defects
- Solutions:
  - Database labeling and pre-processing
  - Fast NN topology exploration
  - Performances vs complexity analysis



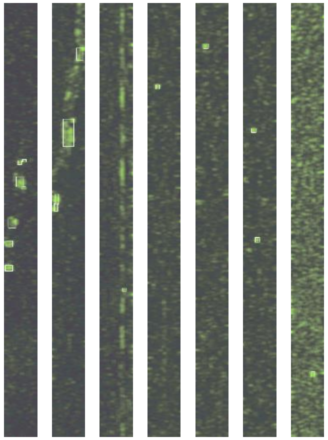
1) Defects labeling and visualization



2) NN Exploration and benchmarking



3) Defects identifications after NN learning



➔ From scratch exploration (database and NN construction) to industrial application

➔ 50,000 MACs NN synthetized in 100 cycles on FPGA @ 100 MHz (500 MACs/cycle)

AUTOMATIC IMAGE INDEXATION

Deep learning for automatic image indexation

- Large databases (> 10 TB)
- Multi-GPU for training

Semantic description

Deep Learning
50000 concepts
90% precision

Semantic image annotation:

- Short description allowing quick search

Participation to the ImageClef2015 contest

- Task: labelling and localizing, among 500 000 pictures (200 classes)

➔ Performances amongst the best (4th position over 14 teams)

PNEURO: MULTI-PURPOSE ENERGY-OPTIMIZED ACCELERATOR FOR NEURAL NETWORKS

Hardware architectures

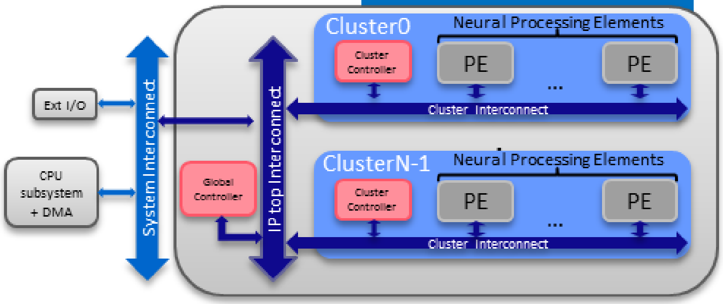
GlobalSensing Technologies

Energy efficient HW accelerator

Energy efficient HW accelerator
- Designed for DNN & image processing chains

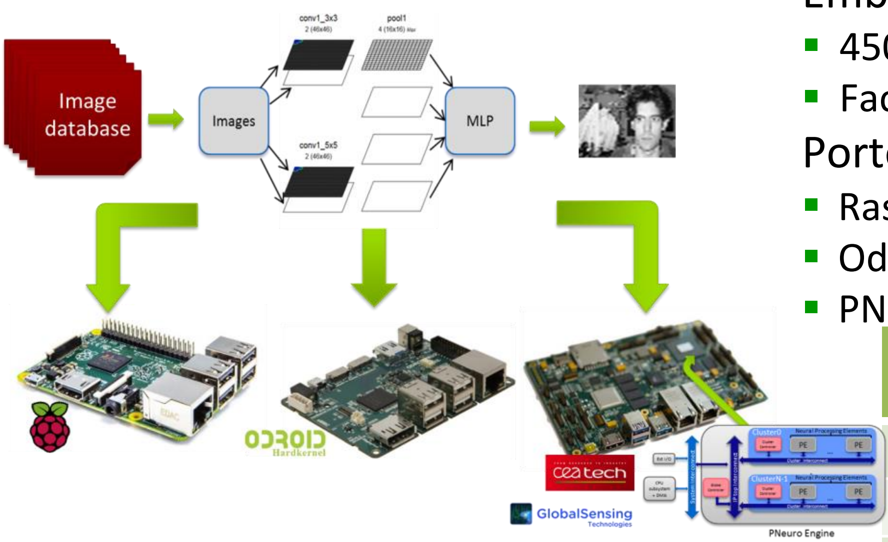
Clustered SIMD architecture

Optimized memory hierarchy



PNeuro Engine

Face Detection on a FPGA-based PNeuro



Embedded CNN application
- 450 KOPs, 60 neurons on hidden layer
- Face detection within 18000 images, 96% recognition rate

Ported on 3 architectures
- Raspberry PI 2B Quad ARM-A7
- Odroid XU3 Quad ARM-A15
- PNeuro FPGA-based prototype

Target	Frequency	Performance	Energy efficiency
Raspberry PI 2 B	900 MHz	480 images/s	380 images/W
Odroid Xu3	2000 MHz	870 images/s	350 images/W
PNeuro (FPGA)	100 MHz	5000 images/s	2000 images/W

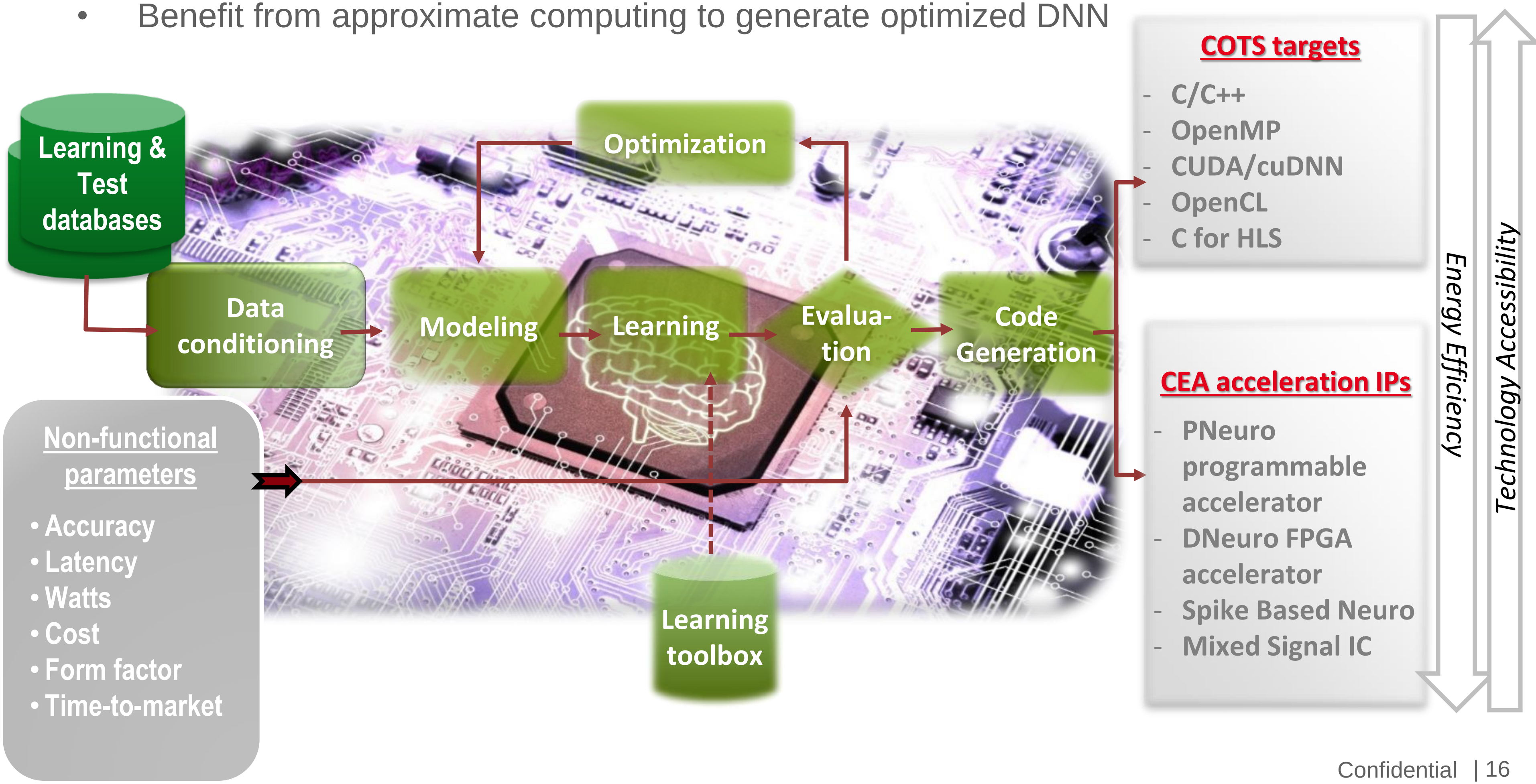
➔ +60% energy efficiency (450 GMACS/W on FDSOI28 @1GHz) vs Synopsys solution

➔ x3.8 MOPS/W energy efficiency vs Quad ARM A7

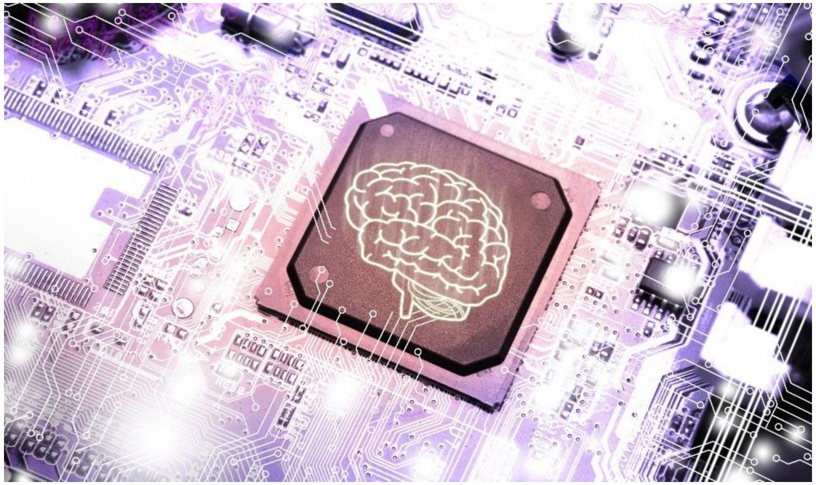
N2-D2 PLATFORM
At a glance

A single platform to

- Explore Deep Neural Network (DNN) topologies
- Experiment 'State Of The Art' Learning techniques with large databases
- Benefit from approximate computing to generate optimized DNN

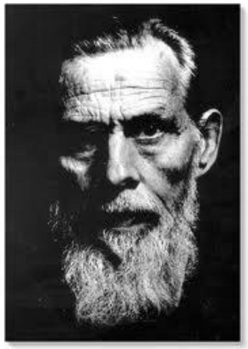


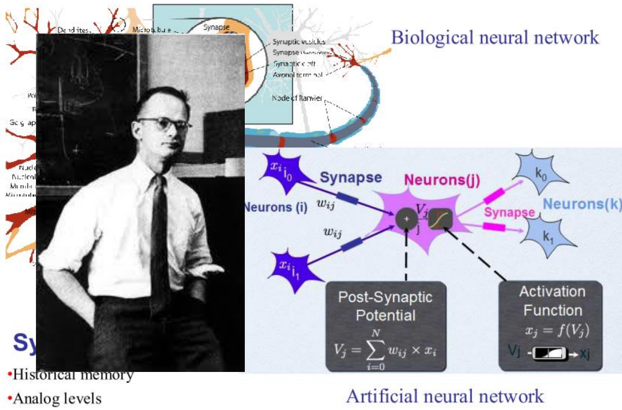
- A short presentation of CEA Tech
- Neuromorphic Engineering
- **Current Research**
- Perspectives



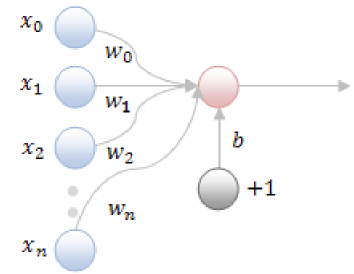
A BRIEF HISTORY OF NEURAL NETWORKS

1943 – Mc Culloch & Pitts
The formal neuron

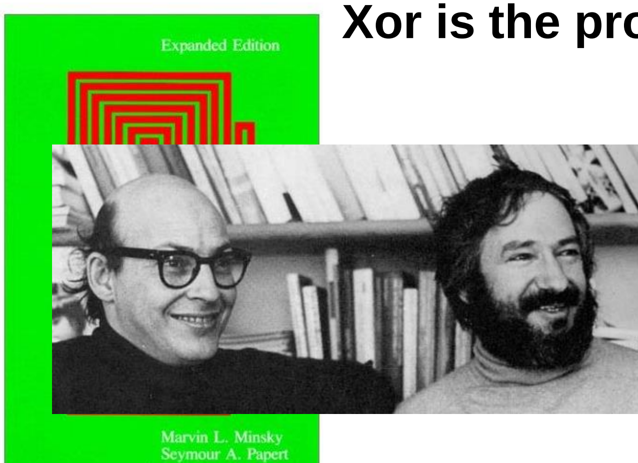


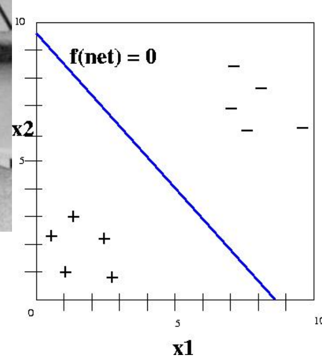


1958 – F. Rosenblatt
The perceptron

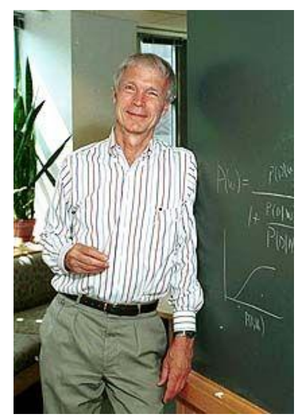


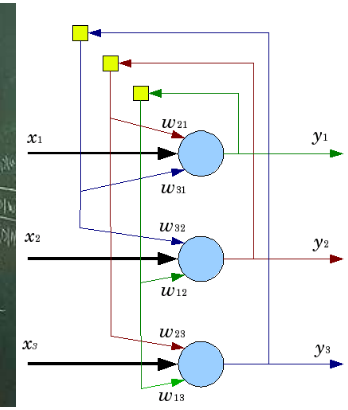
1970 – Minsky & Pappert
Xor is the problem!





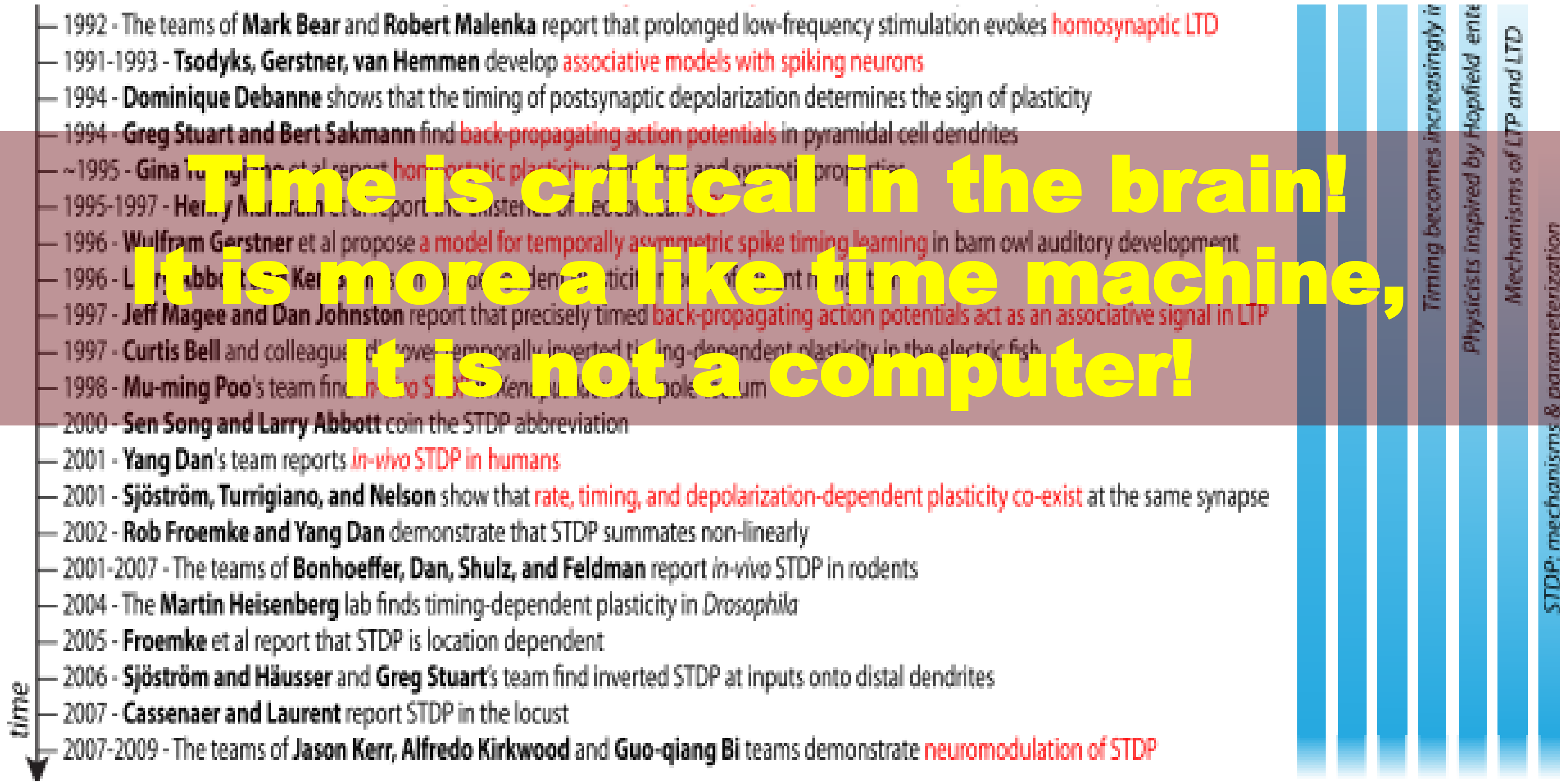
1981 – J.J. Hopfield
Physics to the rescue





LES PROGRÈS EN NEUROSCIENCES DES ANNÉES 90

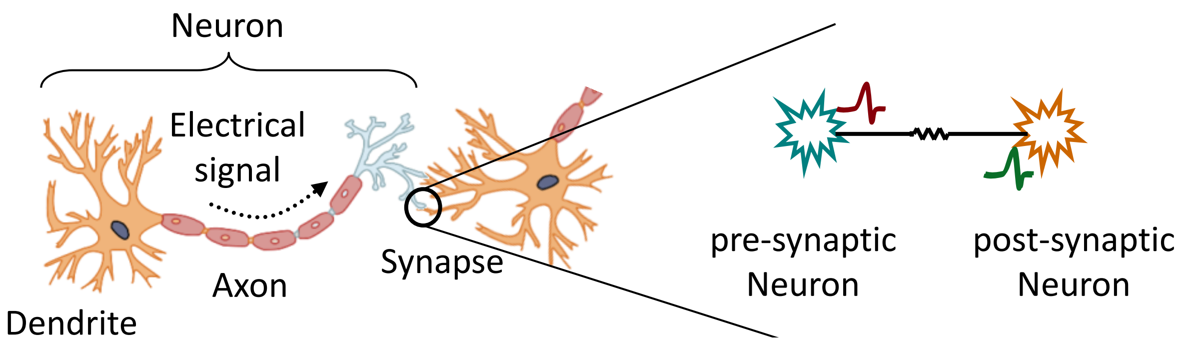
- **Montrent les limitations de l'approche du perceptron et introduisent LTP/LTD and STDP**



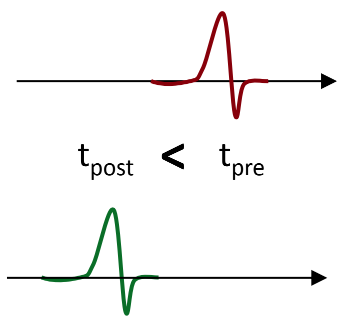
Time is critical in the brain!
It is more a like time machine,
It is not a computer!

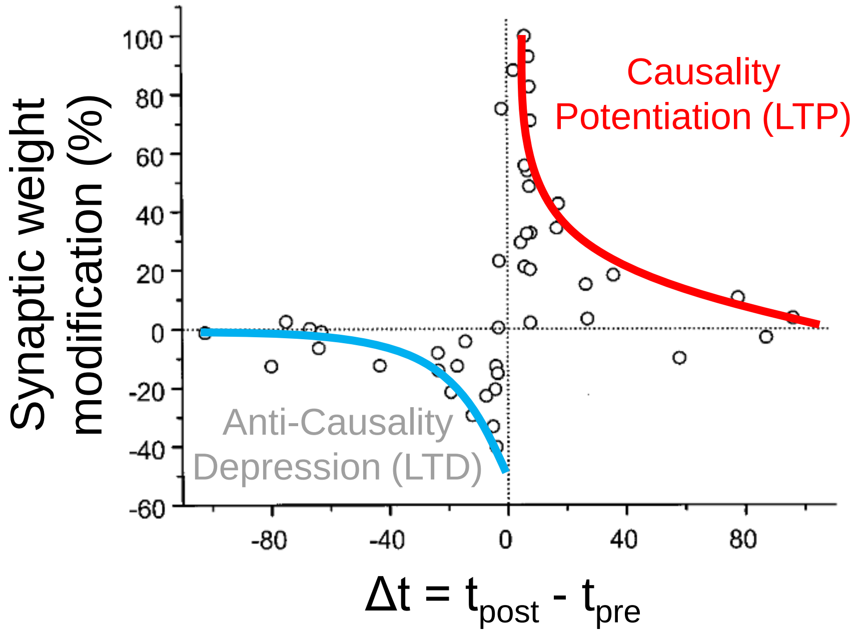
from Markram et al. "A history of spike-timing-dependent plasticity," in *Frontiers in Synaptic neuroscience*, Vol 3, August 2011

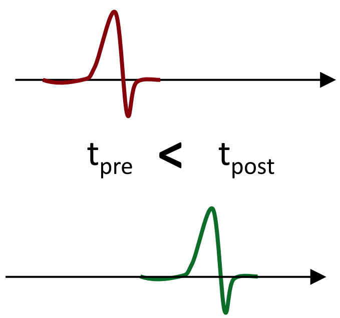
LEARNING FROM NEUROSCIENCE: A STDP PRIMER



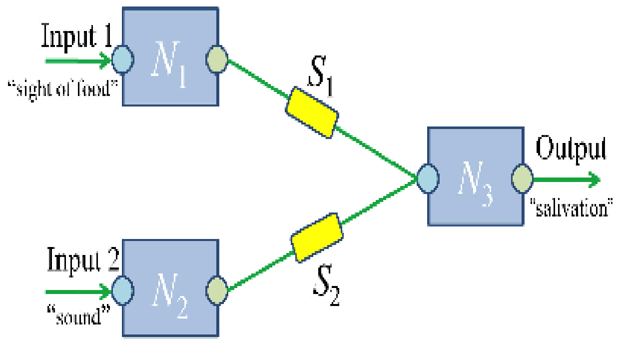
STDP = correlation detector
➔ Possible learning model of the mind

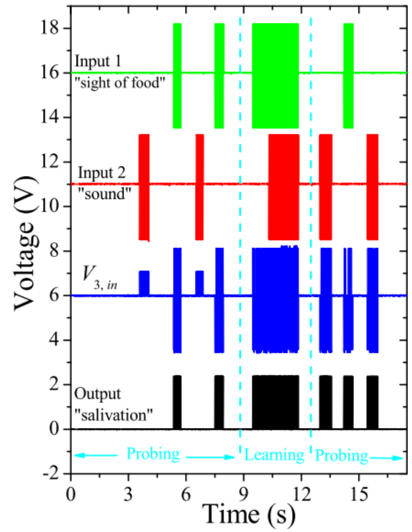


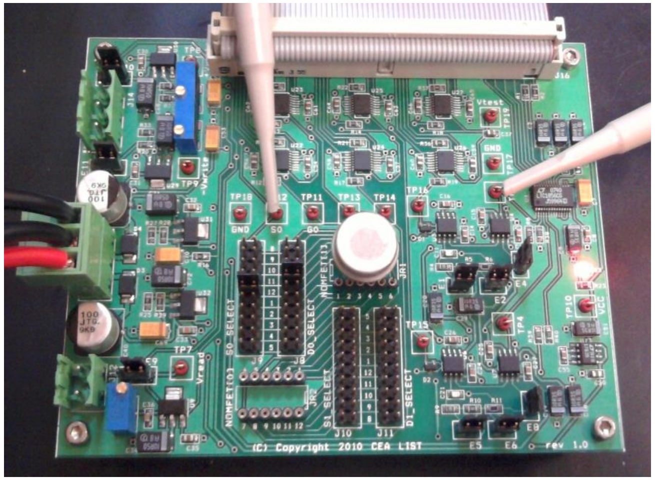




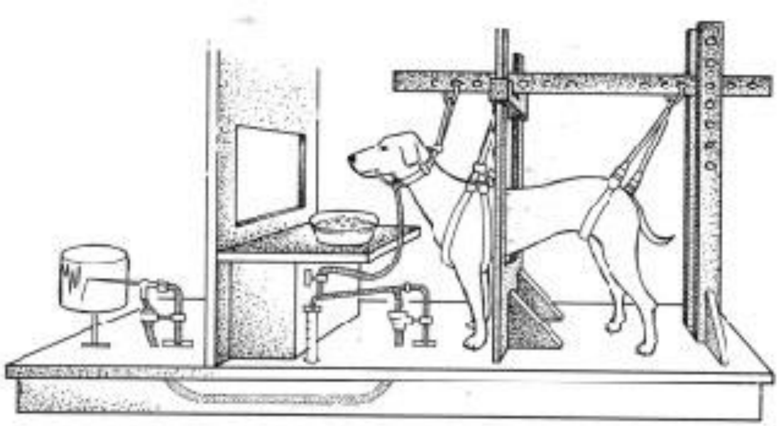
CAN IT LEARN ON ITS OWN? A DOG WITH 2 SYNAPSES!

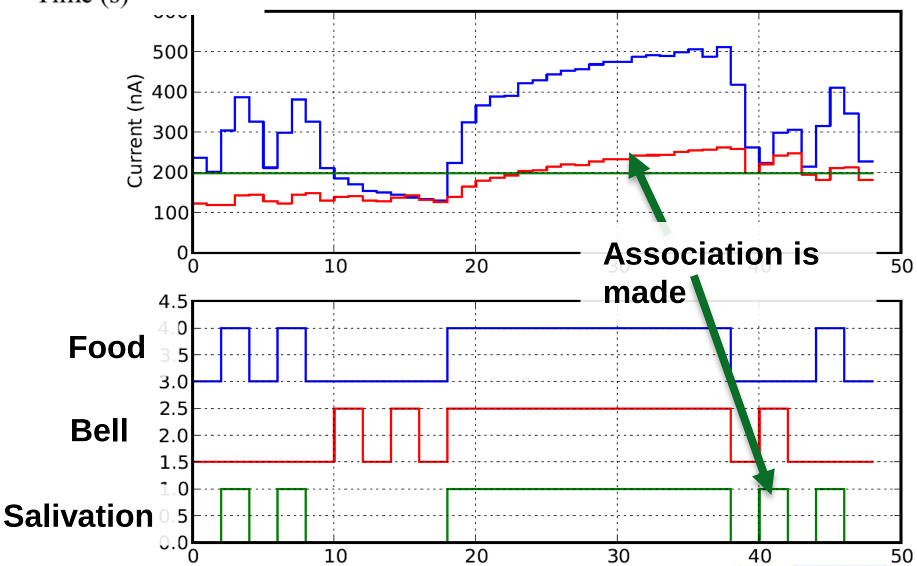






Experimental setup for a Pavlovian associative memory based on memristive devices as proposed by Di Ventra et col.[2]

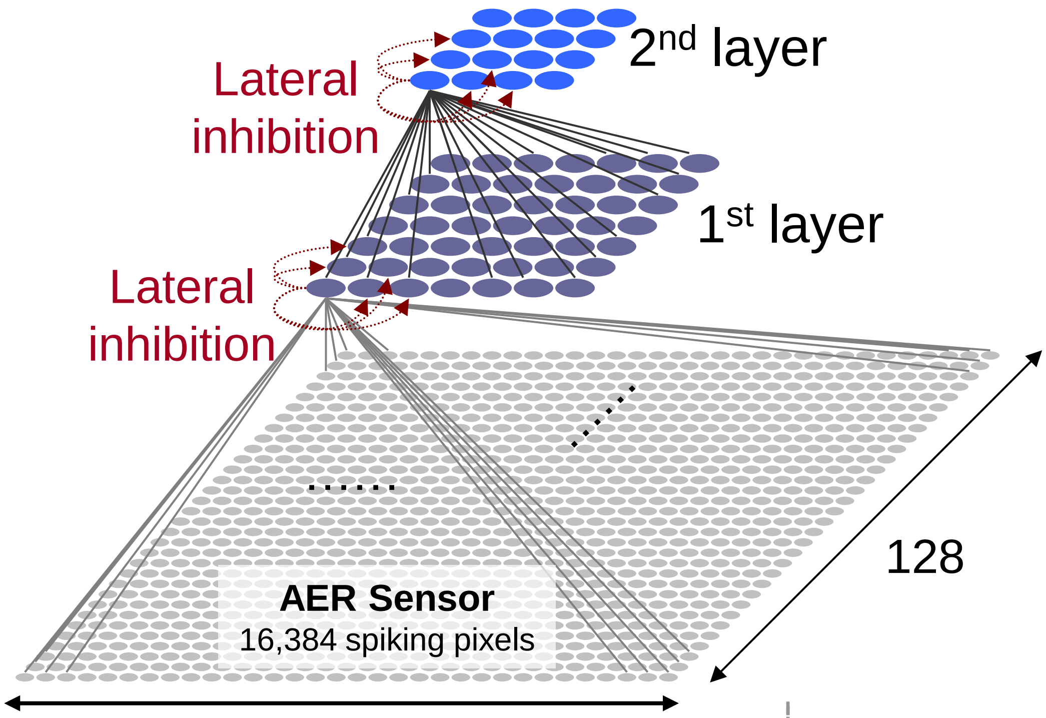


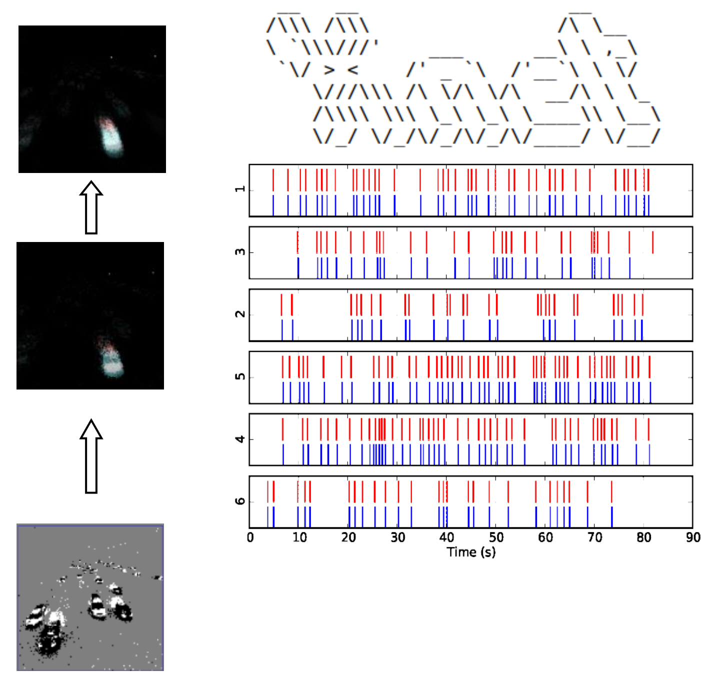


[1] O. Bichler, W. Zhao, F. Alibart, S. Pleutin, S. Lenfant, D. Vuillaume, C. Gamrat, "Pavlov's Dog Associative Learning Demonstrated on Synaptic-like Organic Transistors", Neural Computation, 2012

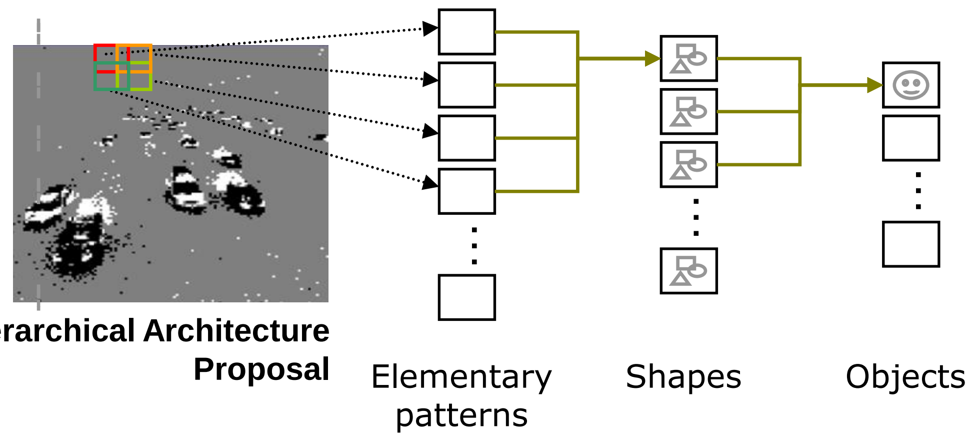
[2] Pershin, Y.V. & Di Ventra, M. "Experimental demonstration of associative memory with memristive neural networks." Arxiv *0905.2935* (2009).

A PRETTY REALISTIC APPLICATION EXAMPLE





Two-layers system
~ 2 million devices with STDP

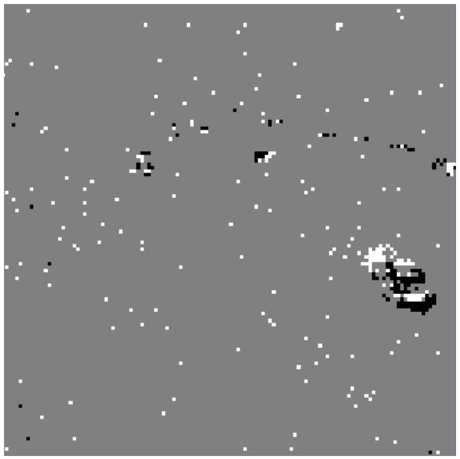


Hierarchical Architecture Proposal

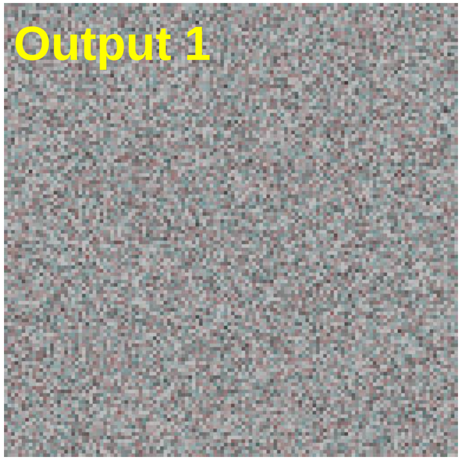
O. Bichler, D. Querlioz, S. J. Thorpe, J.-P. Bourgoin and C. Gamrat, *"Unsupervised Features Extraction from Asynchronous Silicon Retina through Spike-Timing-Dependent Plasticity"*, International Joint Conference on Neural Networks IJCNN August 2011

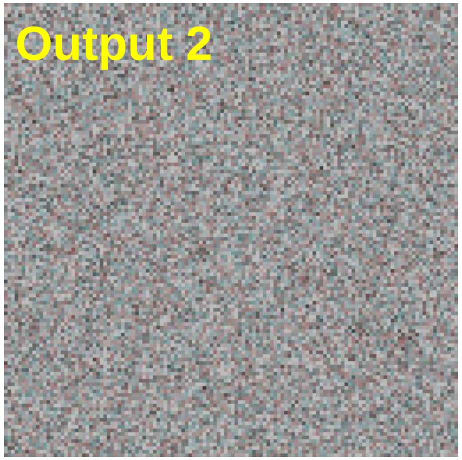
WEIGHTS EVOLUTION DURING LEARNING

Recorded stimuli



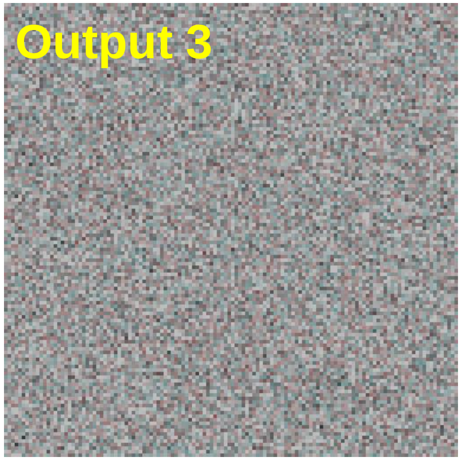
Synaptic maps for 4 neurons on the first layer

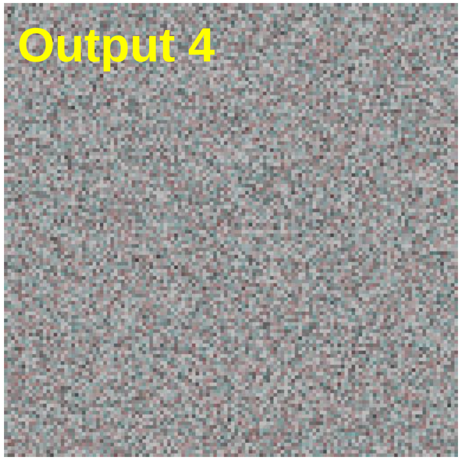




Lane 2

Lane 4



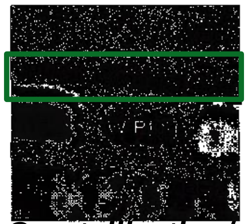


Lane 5 Lane 1

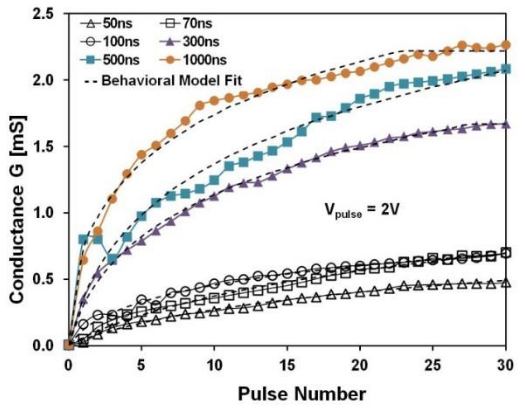
ARTIFICIAL SYNAPSES IMPLEMENTATIONS

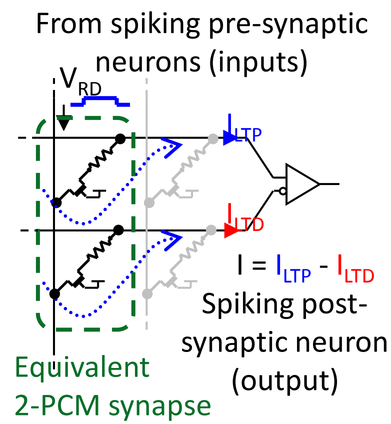
2-PCM synapses for unsupervised cars trajectories extraction

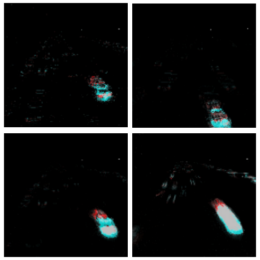
PCM



Crystallization/ Amorphization



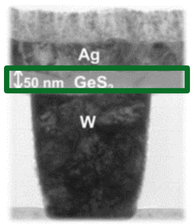




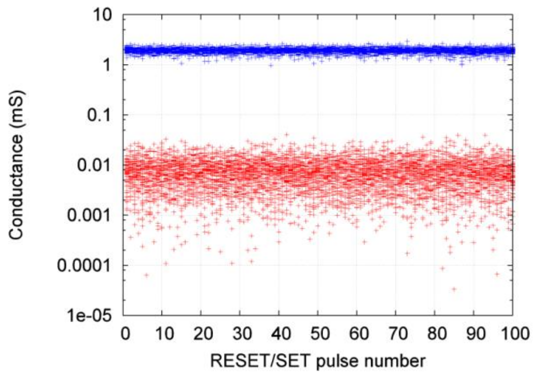
[O. Bichler et al., Electron Devices, IEEE Transactions on, 2012]

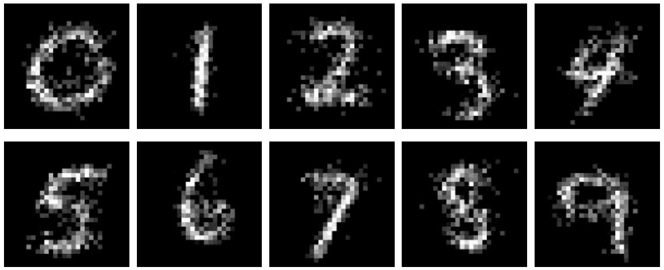
CBRAM binary synapses for unsupervised MNIST handwritten digits classification with stochastic learning

CBRAM



Forming/Dissolution of conductive filament





[M. Suri et al., IEDM, 2012]

- A short presentation of CEA Tech
- Neuromorphic Engineering
- Current Research
- **Perspectives in neuro engineering**

PERSPECTIVES

- **Existing technologies can be useful for supervised learning (Deep learning)**
  - But they are still computing intensive
- **New memory technologies shall allow the implementation of embedded deep learning systems**
- **Spike coding shall allow for better time/trends processing**
- **Progresses have been made toward the brain understanding...**
- **…But a Big LOT remains to be made!**
- **The brain is a very different data processing engine?**
- **It really looks more like a Time Machine than a computer**
  - Neural net technolgies might be used to « predict » or infer trends

CYBERSECURITY : CODE ANALYSIS & CRYPTOCOMPUTING

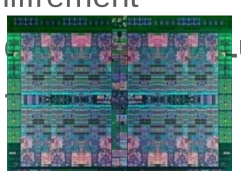
LE PROGRAMME DE R&D CYBERSÉCURITÉ DU CEA

Trois axes majeurs identifiés

- Répondre aux besoins internes du CEA en tant qu'opérateur de systèmes cyber (Systèmes Industriels, HPC,…)
- Apporter une mission d'expertise et de conseil auprès de certains services de l'Etat (ANSSI, Défense,…)
- S'insérer en tant qu'acteur de R&D dans la dynamique industrielle existante en mettant en place des partenariats industriels structurants

Trois objectifs techniques en lien avec les besoins Défense

- **Architectures sécurisées** destinées à assurer la cybersécurité des systèmes industriels
- **Technologies de cyberprotection** incluant notamment la cryptographie et les produits de chiffrement
- Technologies … **Lut** … **qu** … ervision, détection d'intrusions,…

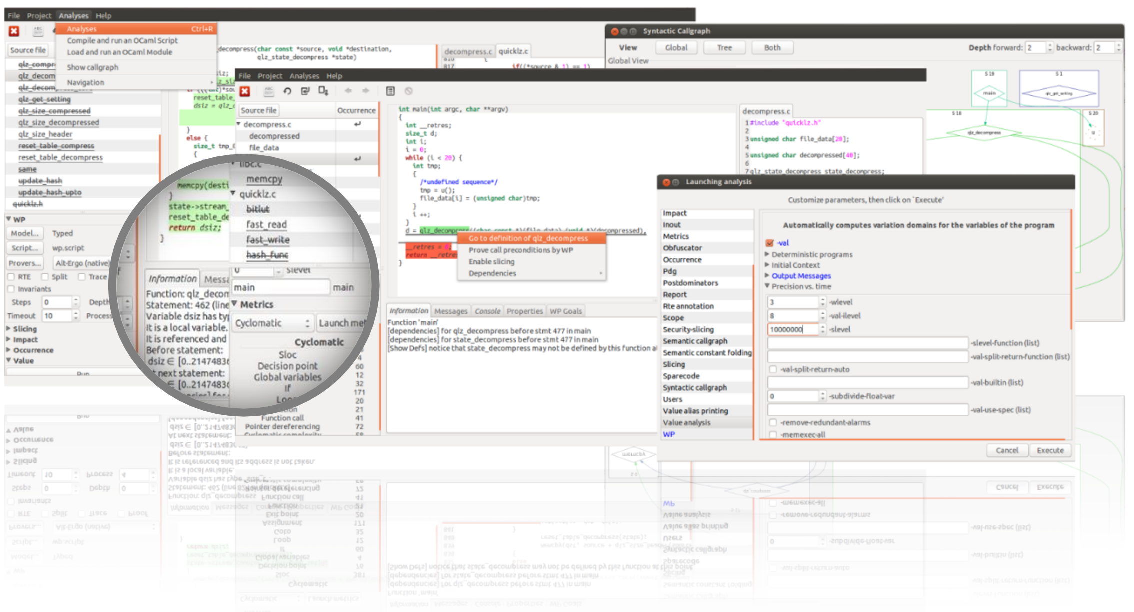


```
#ifndef OPENSSL_NO_HEARTBEATS
int
tls1_process_heartbeat(SSL *s)
	{
	unsigned char *p = &s->s3->rrec.data[0], *pl;
[…]
	/* Read type and payload length first */
	hbtype = *p++;
	n2s(p, payload);
	pl = p;
[…]
	if (hbtype == TLS1_HB_REQUEST)
		{
[…]
		/* Enter response type, length and copy payload */
		*bp++ = TLS1_HB_RESPONSE;
		s2n(payload, bp);
		memcpy(bp, pl, payload);
		bp += payload;
		/* Random padding */
		RAND_pseudo_bytes(bp, padding);

		r = ssl3_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload + padding);

		if (r >= 0 && s->msg_callback)
			s->msg_callback(1, s->version, TLS1_RT_HEARTBEAT,
				buffer, 3 + payload + padding,
				s, s->msg_callback_arg);

		OPENSSL_free(buffer);

		if (r < 0)
			return r;
		}
	else if (hbtype == TLS1_HB_RESPONSE)
```

BUILDING SOFTWARE SECURITY ANALYSIS TOOLS

Open innovation infrastructure

Software Analyzers



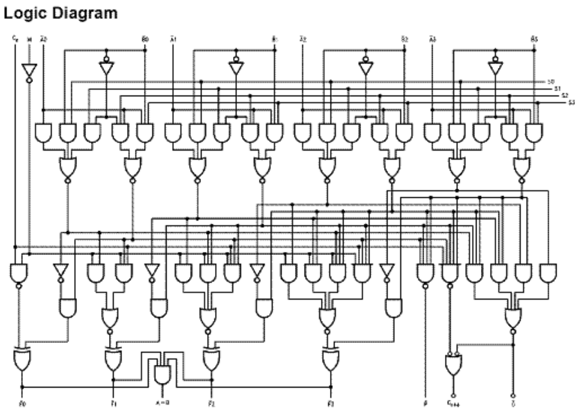
CHALLENGE – **Mix technology and expertise to help demonstrate the quality of security-critical software**

HOMOMORPHIC ENCRYPTION

- **Cryptography**
  - Classically protects confidential data at rest, or in transit.
  - How to protect data *while being processed*?

- **Cryptosystem**
  - $c = Enc_{pk}(m)$
  - $m = Dec_{sk}(c)$

- **Homomorphism property**
  - $c_1 = Enc_{pk}(m_1), c_2 = Enc_{pk}(m_2)$
  - $Dec_{sk}\left(\boldsymbol{Or}_{pk}(c_1, c_2)\right) = m_1 \oplus m_2$
  - $Dec_{sk}\left(\boldsymbol{Xor}_{pk}(c_1, c_2)\right) = m_1 \otimes m_2$



- Applications

Turing-complete cryptocomputing machine!

Postulated since ~1970s

Proof of concept : Craig Gentry 2009. ~30min computing per logic gate…

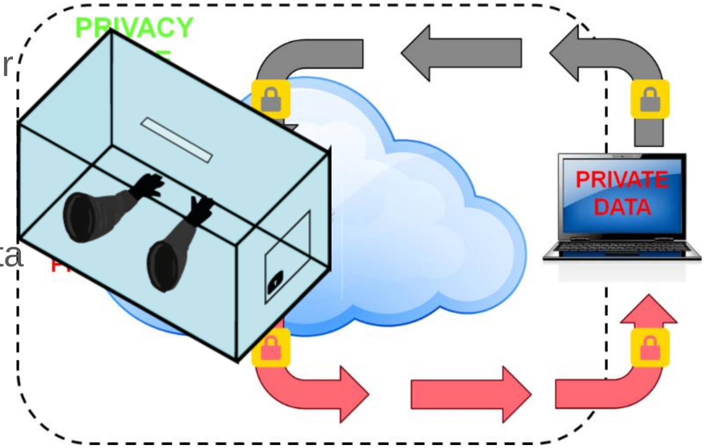
Usable protoypes: 10s gates/s since ~2014

HOMOMORPHIC ENCRYPTION

A homomorphic encryption system is a cryptosystem that allows
Data encryption and decryption and
Calculation performance **in the encrypted domain**.

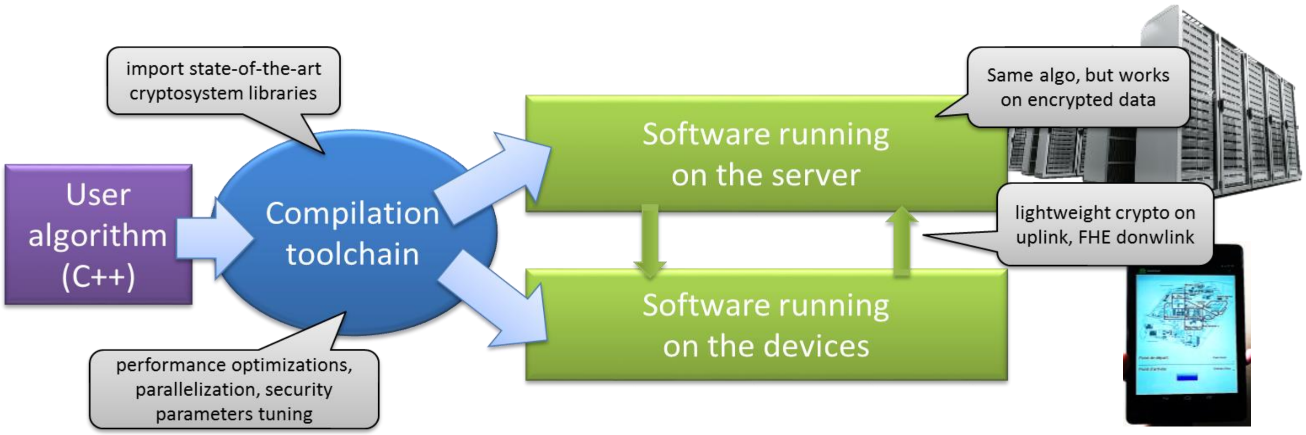
- **In the most basic settings, two parties are involved**
  - The user: owner of some private data.
  - The server: owner of an algorithm, and possibly some data to inject.

- **The process**
  - User encrypts its private data
  - Sends encrypted data to the server
  - Server injects other data when necessary
  - Server processes algorithm homomorphically on encrypted data
  - Server sends encrypted output
  - User only can decrypt output.



THE CINGULATA COMPILER & RTE

- **Prototype of a compiler infrastructure for high-level cryptocomputing-ready programming, taking C++ code as input.**
- **Parallel code generation and « cryptoexecution » runtime environment.**
- **Optimized prototypes of the most efficient HE systems known so far.**



RECENT USE-CASES

- **Privacy-preserving healthcare data handling**

  Diagnosis latency < 20 sec

- **Tweets judiciary analysis**

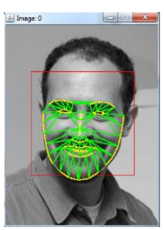
  Rate > 15 tweets/sec (16core)

- **Intrusion detection with masked rules**

  Alert latency < 5 sec

- **Personal energy usage profiling**

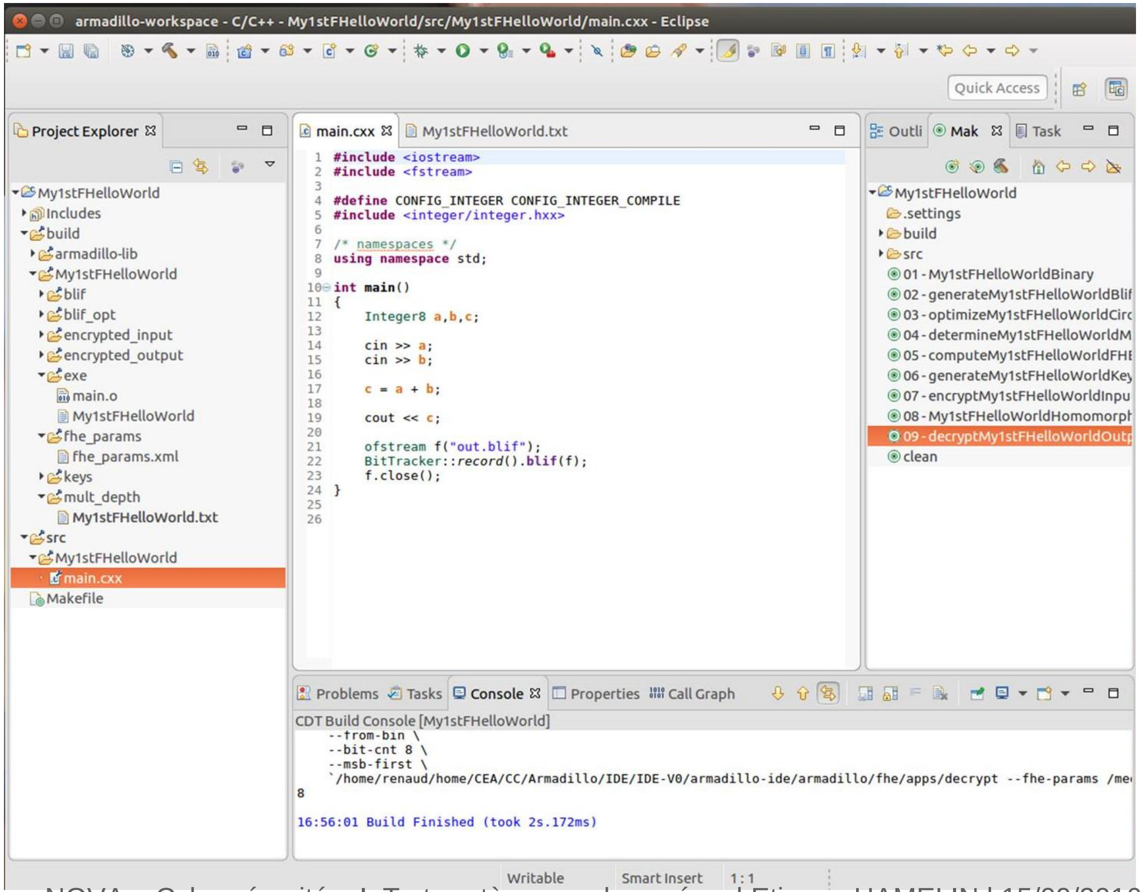
  Profiling < 1 sec



- **Biometric authentication**

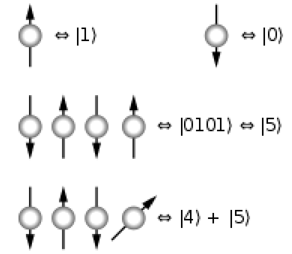
  Enlistment ~30sec, authentication <1sec (4core)

ENVIRONNEMENT DE PROGRAMMATION POUR LE CRYPTOCALCUL



QUELQUES SUJETS À LA MODE

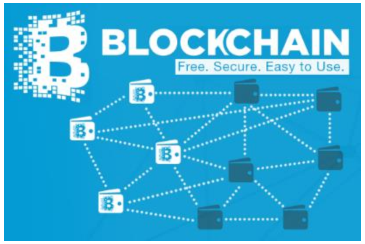
- **Crypto spécifiquement pour l'IoT**
  - Obfuscation
  - lwC : compromis sécurité, power, perf.
  - PUF : hardware-entangled crypto



qubits can be in a superposition of all the clasically allowed states

- **Crypto long-terme / post-quantique**

  Nouveaux cryptosystèmes: réseaux euclidiens, cartes multilinéaires, ... Défi : délai de déploiement !
  NSA *: « don't invest on ECC, wait for PQC »*



- **Nouvelles formes de confiance: Blockchain**

  Crypto classique + généraux byzantins + proof-of-work +
  théorie des jeux ➔ système multi-acteurs régulé
  - Applications foisonnantes: Bitcoin

université PARIS-SACLAY

INSTITUT CARNOT CEA LETI

INSTITUT CARNOT CEA LIST

MINATEC

digiteo

leti
Centre de Grenoble
17 rue des Martyrs
38054 Grenoble Cedex

list
Centre de Saclay
Nano-Innov PC 172
91191 Gif sur Yvette Cedex