PANEL

IARIA Congress

Challenges of AI-based Technologies and Applications

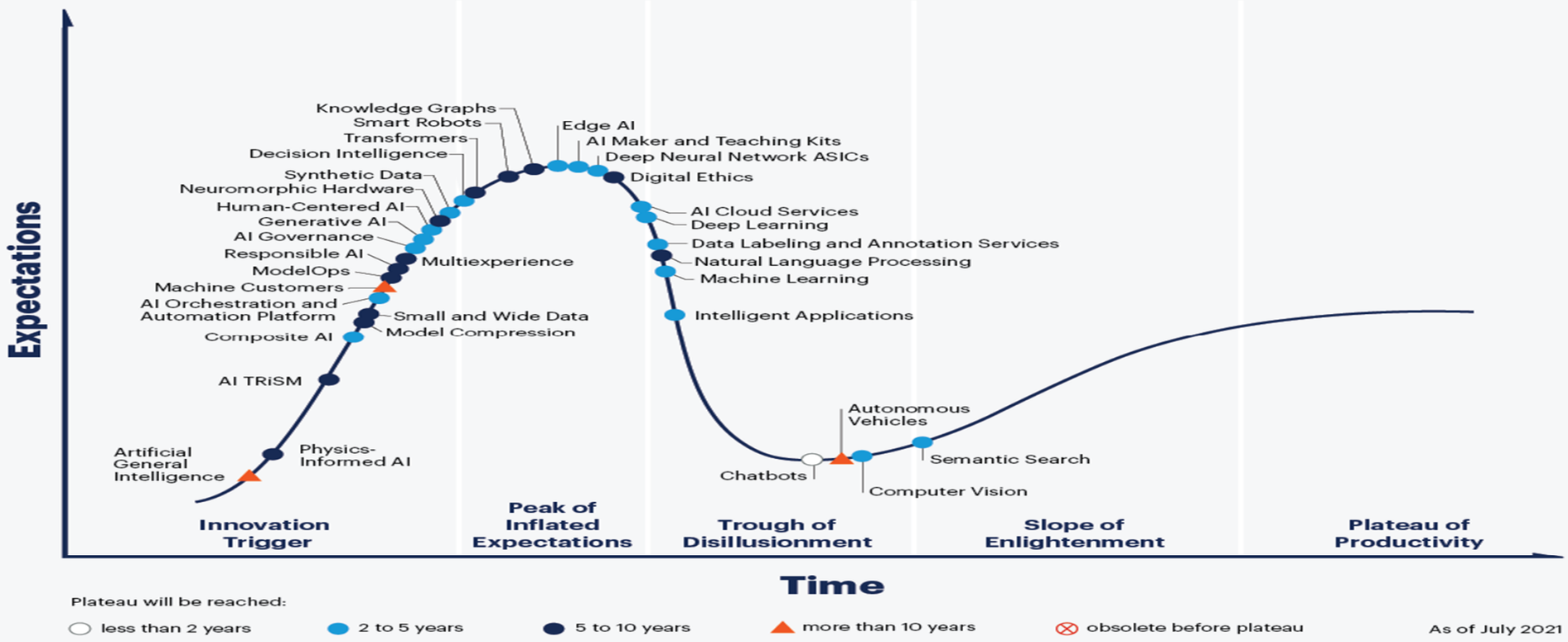
Preamble:

- **(i) The spam box/junk emails story** ***(trusted decision: -3rd party- and/or accepted decision -corporate-)***

- **(ii) Waste-management** ***(DeepLearning-based garbage collection and object recognition): next: on-move selection***

- **(iii) Touchless Touching in Virtual reality** ***(a new haptics with no hardware on a user's hand)***
  Haptic sensations are applied to the persons' (to the nerves) forehand (matching the movements of the fingers)

Hype Cycle for Artificial Intelligence, 2021

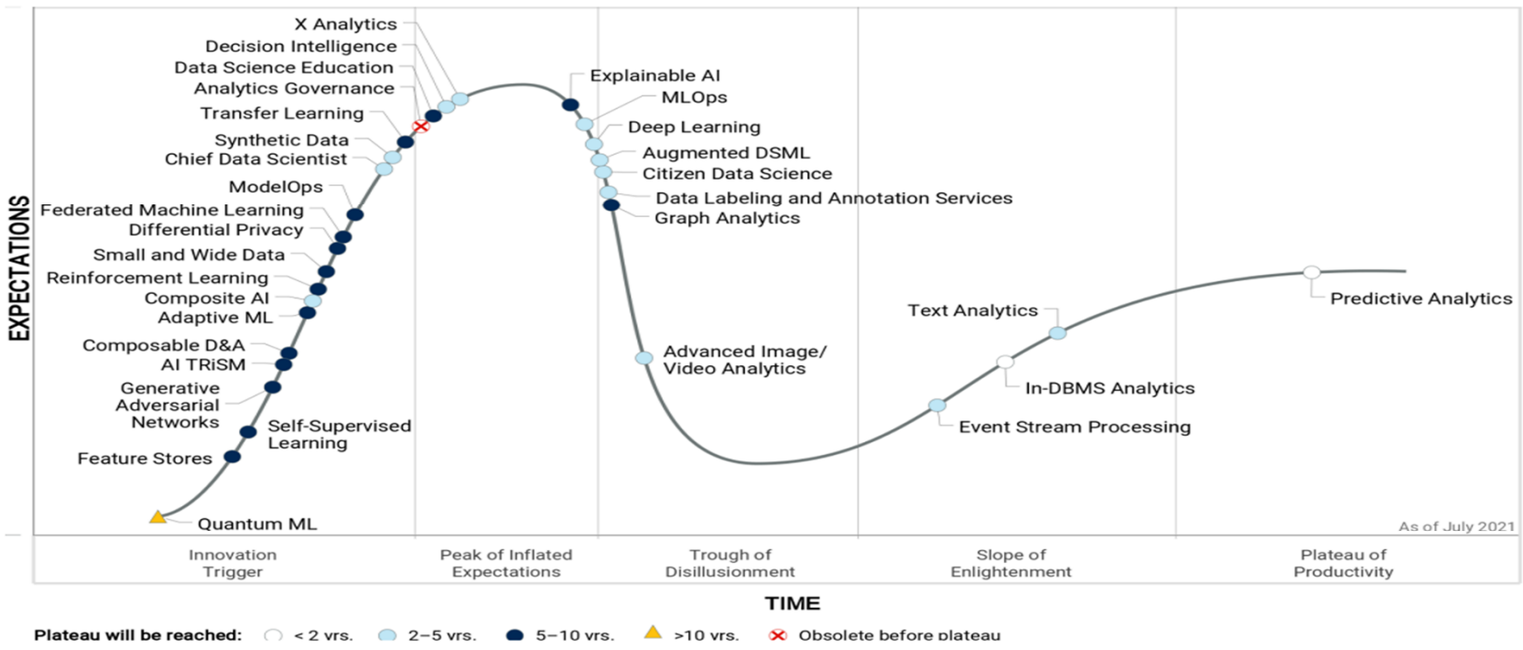


gartner.com

Source: Gartner

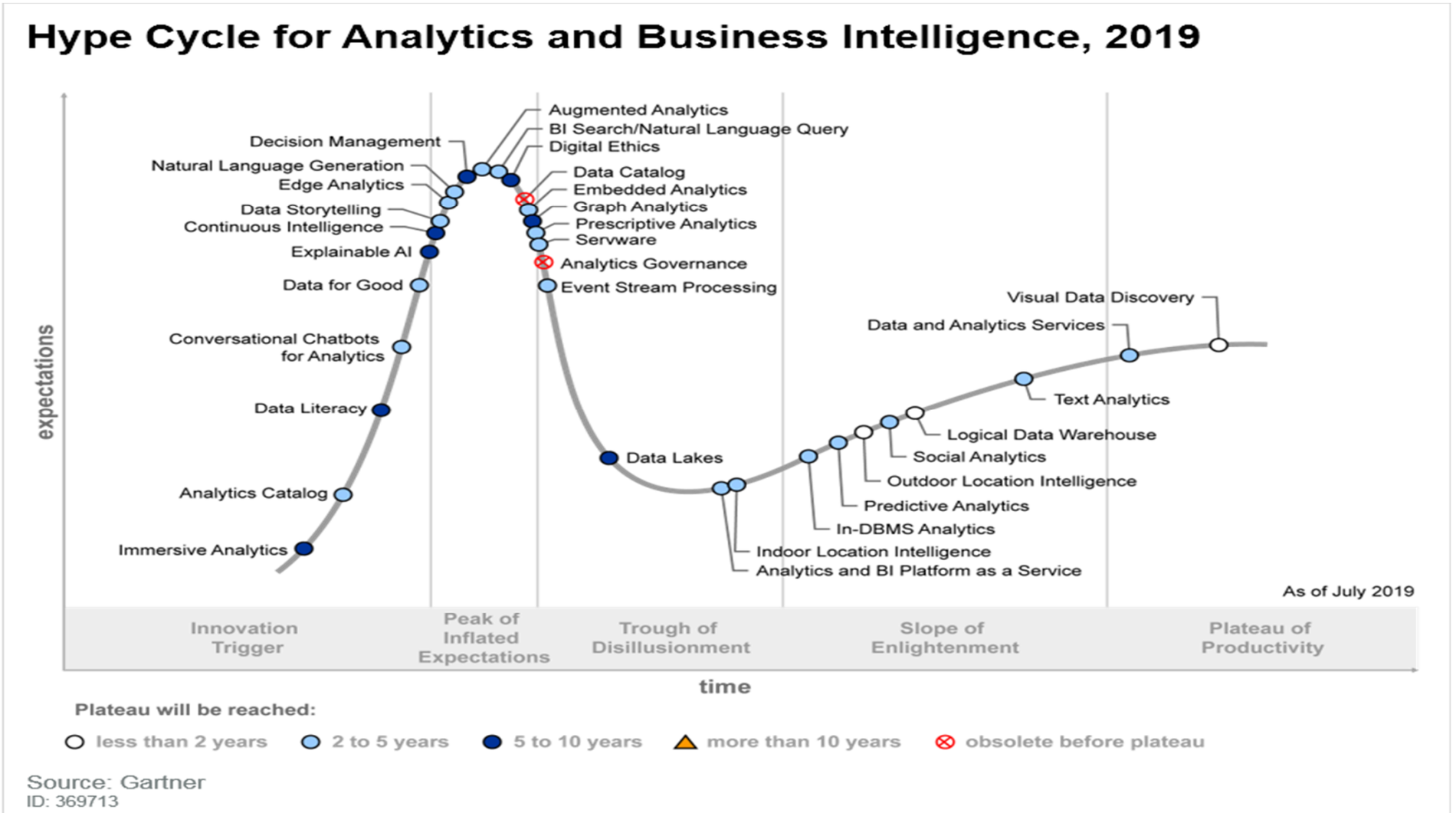
Gartner

Figure 1: Hype Cycle for Data Science and Machine Learning, 2021



Gartner

Source: Gartner (August 2021)


Hype Cycle for Analytics and Business Intelligence, 2019
expectations
Augmented Analytics
BI Search/Natural Language Query
Digital Ethics
Decision Management
Natural Language Generation
Edge Analytics
Data Storytelling
Continuous Intelligence
Explainable AI
Data for Good
Conversational Chatbots for Analytics
Data Literacy
Analytics Catalog
Immersive Analytics
Data Catalog
Embedded Analytics
Graph Analytics
Prescriptive Analytics
Servware
Analytics Governance
Event Stream Processing
Data Lakes
Visual Data Discovery
Data and Analytics Services
Text Analytics
Logical Data Warehouse
Social Analytics
Outdoor Location Intelligence
Predictive Analytics
In-DBMS Analytics
Indoor Location Intelligence
Analytics and BI Platform as a Service
As of July 2019
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time
Plateau will be reached:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau
Source: Gartner
ID: 369713

IARIA Congress Experts Panel
Challenges of AI-based Technologies and Applications

IARIA Congress 2022

Chair: Petre Dini, IARIA, EU/USA petre@iaria.org

Topics

- **AI**: Creativity, Emotion, Art, Music, Immersion
- **Computing**: Big Data, Deep Learning, Evolutionary, Cognitive
- **Trust**: Explainability, Legal, Hybrid-AI
- **HCI**: Brain Interfaces, Cognitive interfaces
- **Cohabitation**: Human-Robot society, Empathy, Sentiments
- **AI-based communication**: Adaptive Protocols, Digital Twins architectures, Reliability and Resilience, QoS/QoE parameters
- **Applications**: Industrial, Health, Financial, Agriculture, Transportation, Infrastructure, Energy, Social networks, Education

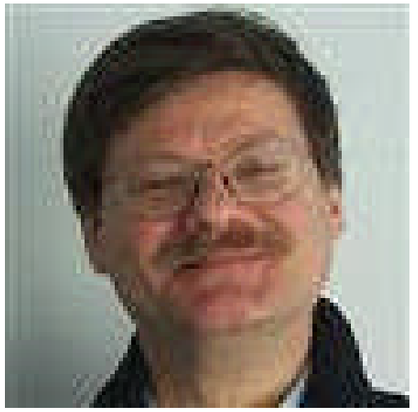
Panelists

- Luigi Lavazza, Universita degli Studi dell'Insubria, Italy
  Performance metrics and the actual *accuracy of AI models*
- Malcolm Crowe, University of the West of Scotland, United Kingdom
  Lifelong AI responds to *evolving situations*
- Arcady Zhukov, University Basque Country, Dept. Polymers Adv. Mater., Spain
  Right Data Set; *Low cost* and *high-performance* sensor technologies
- Dirceu Cavendish, Kyushu Institute of Technology, Japan/USA
  AI and *Security/Privacy*

position malcolm Panellist Position.pdf

Panellist Position

Performance metrics and the actual accuracy of AI models



Luigi Lavazza, Università degli Studi dell'Insubria luigi.lavazza@uninsubria.it

- Many performance metrics are available to evaluate the accuracy of classifiers, predictors, etc.
- The characteristics of performance metrics are largely ignored
- Researches use a given performance metrics just because before to evaluate similar work
- Several examples of incorrectly used performance metrics are available
- The evaluation of AI models is often unreliable because of the chosen performance metrics and how they are used

→ You must know performance metrics and their characteristics

→ You must know the risks connected with the incorrect usage of performance metrics

→ Are performance metrics needed at all?

Panellist Position

Lifelong AI responds to evolving situations

Malcolm Crowe, University of the West of Scotland, malcolm.crowe@uws.ac.uk

- Self driving cars allow for changes, obstacles
- Translation apps learn new phrases and improve
- Avoid rigid dependence on the training set
- Good AI can explain its reasons, offer advice
- Recognise and learn from feedback

→ Adaptation to evolving situations

→ Human-AI cohabitation

IARIA Congress Experts Panel
Challenges of AI-based Technologies and Applications

IARIA Congress 2022

Panellist Position

Artificial Intelligence-Based Technologies: role of smart sensor technologies

Arkady Zhukov, University of Basque Country arkadi.joukov@ehu.es

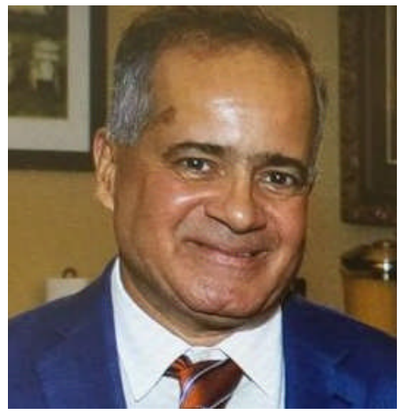
- Data Scarcity : information and communication technology (ICT)
- Data acquisition and storage
- Determining the Right Data Set
- Cost issues
- Integration into existing systems

→ Low cost and high-performance sensor technologies

Panellist Position

AI and Security/Privacy

Dirceu Cavendish, Kyushu Institute of Technology USA/Japan cavendish@ndrc.kyutech.ac.jp



- 6G networking
- IoT Systems Architecture
- Privacy Technologies
- Privacy Challenges
- AI/ML Security/Privacy

→ Pervasive deep personal data mining

→ Privacy regulations plays catch up with threats/attacks

→ AiModels' attacks will become commonplace

FULL PANELISTS' POSITIONS

= to be added into the booklet =

OPEN DISCUSSION

Gartner

2022 SARS-CoV2 case study

Smarter, faster, more responsible AI

- By the end of 2024, 75% of enterprises will shift from piloting to operationalizing AI, driving a 5X increase in streaming data and analytics infrastructures.

- Within the current pandemic context, AI techniques such as machine learning (ML), optimization and natural language processing (NLP) are providing vital insights and predictions about the spread of the virus and the effectiveness and impact of countermeasures. AI and machine learning are critical realigning supply and the supply chain to new demand patterns.

Challenges of AI-based Technologies and Applications

Performance metrics and the actual accuracy of AI models

IARIA Congress 2022 – Panel 2
Nice, France, July 24-28, 2022

Luigi Lavazza
Università degli Studi dell'Insubria, Varese, Italy

Luigi Lavazza

Professional experience

- Professor of Computer Science at the University of Insubria at Varese, Italy.
- Scientific consultant in digital innovation projects at CEFRIEL – Politecnico di Milano.

Scientific Activity

- Research: Empirical software engineering, software metrics and software quality evaluation; project management and effort estimation; Software process modeling, measurement and improvement; Open Source Software.
- Several international research projects
- Reviewer of EU funded projects.
- Co-author of over 170 scientific articles.
- PC member of several international Software Engineering conferences
- Editor in chief of the IARIA International Journal On Advances in Software (2013-2018).
- IARIA fellow since 2011

Università degli Studi dell'Insubria

Position statement

Context: performance metrics to evaluate the accuracy of AI models (classifiers, predictors, etc.)

- The right performance metrics are **NOT** used
- Performance metrics are **NOT** used right

} Unreliable evaluations

- A large amount of published research (AI models) is not adequately evaluated ➔ overoptimistic conclusions, incorrect comparisons, lack of data about the actual performance of models, …

Common problems

- Many performance metrics are available to evaluate the accuracy of classifiers, predictors, etc.
- The characteristics of performance metrics are largely ignored
- Researches use a given performance metrics just because before to evaluate similar work
- Several examples of incorrectly used performance metrics are available
- The evaluation of AI models is often unreliable because of the chosen performance metrics and how they are used

Let us consider the performance of binary classifiers

- Confusion matrix

	Actual negatives	Actual positives
Estimated negative	TN (true negatives)	FN (false negatives)
Estimated positive	FP (false positives)	TP (true positives)

- The confusion matrix represents completely the performance (accuracy) of a classifier
- Performance metrics try to “condense” the confusion matrix into a single number

How many performance metrics?

sensitivity, recall, hit rate, or true positive rate (TPR)

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{P}} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} = 1 - \mathrm{FNR}$$

specificity, selectivity or true negative rate (TNR)

$$\mathrm{TNR} = \frac{\mathrm{TN}}{\mathrm{N}} = \frac{\mathrm{TN}}{\mathrm{TN} + \mathrm{FP}} = 1 - \mathrm{FPR}$$

precision or positive predictive value (PPV)

$$\mathrm{PPV} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} = 1 - \mathrm{FDR}$$

negative predictive value (NPV)

$$\mathrm{NPV} = \frac{\mathrm{TN}}{\mathrm{TN} + \mathrm{FN}} = 1 - \mathrm{FOR}$$

miss rate or false negative rate (FNR)

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{P}} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TP}} = 1 - \mathrm{TPR}$$

fall-out or false positive rate (FPR)

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{N}} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} = 1 - \mathrm{TNR}$$

false discovery rate (FDR)

$$\mathrm{FDR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TP}} = 1 - \mathrm{PPV}$$

false omission rate (FOR)

$$\mathrm{FOR} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TN}} = 1 - \mathrm{NPV}$$

Positive likelihood ratio (LR+)

$$\mathrm{LR+} = \frac{\mathrm{TPR}}{\mathrm{FPR}}$$

Negative likelihood ratio (LR-)

$$\mathrm{LR-} = \frac{\mathrm{FNR}}{\mathrm{TNR}}$$

prevalence threshold (PT)

$$\mathrm{PT} = \frac{\sqrt{\mathrm{TPR}(-\mathrm{TNR}+1)} + \mathrm{TNR} - 1}{(\mathrm{TPR} + \mathrm{TNR} - 1)} = \frac{\sqrt{\mathrm{FPR}}}{\sqrt{\mathrm{TPR}} + \sqrt{\mathrm{FPR}}}$$

threat score (TS) or critical success index (CSI)

$$\mathrm{TS} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN} + \mathrm{FP}}$$

Prevalence

$$\frac{\mathrm{P}}{\mathrm{P} + \mathrm{N}}$$

accuracy (ACC)

$$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{P} + \mathrm{N}} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}$$

balanced accuracy (BA)

$$\mathrm{BA} = \frac{TPR + TNR}{2}$$

F1 score

is the harmonic mean of precision and sensitivity:

$$\mathrm{F_1} = 2 \times \frac{\mathrm{PPV} \times \mathrm{TPR}}{\mathrm{PPV} + \mathrm{TPR}} = \frac{2\mathrm{TP}}{2\mathrm{TP} + \mathrm{FP} + \mathrm{FN}}$$

phi coefficient (φ or r_φ) or Matthews correlation coefficient (MCC)

$$\mathrm{MCC} = \frac{\mathrm{TP} \times \mathrm{TN} - \mathrm{FP} \times \mathrm{FN}}{\sqrt{(\mathrm{TP} + \mathrm{FP})(\mathrm{TP} + \mathrm{FN})(\mathrm{TN} + \mathrm{FP})(\mathrm{TN} + \mathrm{FN})}}$$

Fowlkes–Mallows index (FM)

$$\mathrm{FM} = \sqrt{\frac{TP}{TP + FP} \times \frac{TP}{TP + FN}} = \sqrt{PPV \times TPR}$$

informedness or bookmaker informedness (BM)

$$\mathrm{BM} = \mathrm{TPR} + \mathrm{TNR} - 1$$

markedness (MK) or deltaP (Δp)

$$\mathrm{MK} = \mathrm{PPV} + \mathrm{NPV} - 1$$

Diagnostic odds ratio (DOR)

$$\mathrm{DOR} = \frac{\mathrm{LR+}}{\mathrm{LR-}}$$

This is jus a sample (thanks, Wikipedia!)

Università degli Studi dell'Insubria

Problems: F-measure $\left(\frac{2}{\frac{1}{Recall}+\frac{1}{Precision}}\right)$

- Originally proposed for information retrieval, where TN is usually very large and often unknown, i.e., when prevalence is very small
  - Prevalence = $\frac{AP}{AP+AN}$
- Used when TN is not large at all.
  - These confusion matrices have the same F-measure!

	Act. neg.	Act. pos.
Est. neg.	90	10
Est. pos.	10	90

	Act. neg.	Act. pos.
Est. neg.	5	10
Est. pos.	10	90

Problems: Accuracy $\left(\frac{TP+TN}{n}\right)$

- It does not distinguish between false positives and false negatives
- Very used to evaluate diagnostic models in the medical field
- Wait a moment: let us consider screening for a potentially fatal disease
  - A false positive gets a first diagnosis that is then corrected by the following more accurate analysis. Disadvantages: the patient gets scared for a few days; a not necessary accurate test is carried out
  - A false negative implies that the patient is not treated, until symptoms occur. Disadvantages: a stronger, linger and more expensive treatment is necessary, and it may not work.

Commonly overlooked issues

- Consider random classification. You estimate a subject positive with probability ρ, where ρ is the prevalence observed in previous cases.
- Random classification has (on average)
  - F-measure=ρ
  - Accuracy=$\rho^2 +(1- \rho)^2$
- In many cases a model having F-measure=0.9 and Accuracy=0.82 would be considered really good.
- If ρ=0.9, both models are equivalent to random estimation
  - You could as well throw dice …

Common mistakes

- A given method is applied to many datasets.
- The performance with each dataset is evaluated via F-measure
- The mean of the obtained F-measures is computed and proposed as an “overall” evaluation of the method.
- This does not make sense, when the used dataset have different prevalence (that is, always, in practice).

- This problems has been observed in papers published major software engineering journals

Common mistakes

- The results obtained by a new technique are evaluated via performance metric $\mathscr{M}$.
- The results are compared with previously published results, also evaluated via $\mathscr{M}$.
- For many $\mathscr{M}$, this does not make sense, if the involved papers used datasets with different prevalence, which is very often the case.

- This problem occurs with exceeding frequency.

Conclusion (for the time being)

- There is a great ignorance about performance metrics. People do not know what performance metrics actually represent, what are their applicability conditions, etc.
  - The right performance metrics are **NOT** used
  - Performance metrics are **NOT** used right
- Consequence: a large amount of research is not correctly evaluated.

How to improve

- Providing the confusion matrix would be enough, in most cases.
  - It gives the size of the dataset
  - It tells the prevalence of the dataset
  - It supports the computation of any metric
  - It lets you weight elements (e.g., false positives and false negatives) differently
  - …

Thank you!

Challenges of AI-based technologies and applications

MALCOLM CROWE

Malcolm Crowe

University of the West of Scotland
Email: malcolm.crowe@uws.ac.uk

- Malcolm Crowe is an Emeritus Professor at the University of the West of Scotland, where he worked from 1972 (when it was Paisley College of Technology) until 2018. He was a head of department of Computing from 1985 to 1999.
- He gained a D.Phil. in Mathematics at the University of Oxford in 1979.
- His funded research projects before 2001 were on Programming Languages and Cooperative Work. Since 2001 he has worked on Reinforcement Learning and his main work is now on Database Technology.
- Books include “Constructing Systems and Information” (with R Beeby and J Gammack) and “Interdisciplinary Research” (ed. with J Atkinson).
- Prof. Crowe has recently been appointed an IARIA Fellow.

Like a machine?

- Created by a tool builder
- Fulfils a specified purpose reliably
  - May be adjustable if requirements change
- Better (in some sense) than a human actor
  - Cheaper, faster, reliable, more accurate
- Limited by its purpose (obsolescence)
- Requires maintenance

- Like a human?

Like a human?

- Abilities:
  - to perceive (recognition, opportunity)
  - to learn (induction, generalisation)
  - to reason (deduction, application)
  - to create (abstraction, tools)
  - to communicate (share, understand)
- Initiative (motivation, thirst)
- Takes 20 years of education to do anything
  - Laziness, tiredness, boredom, mistakes
- What we see is a product of what we think

Artificial Intelligence achievements

- Search (deduction)
- Classification (perception)
- Neural networks (induction)
- Reinforcement learning (exploration)
- Robot assistants (Alexa, Siri, …)

- What we need to do next

What we need to do next

- Communication/explanation
  - I saw many examples in which …
- Introspection/criticism
  - Identification of new patterns
- Transferable skills
  - Try to apply explanations in similar situations
- Abstraction/discovery
  - What would happen if ..

Panellist Position

Artificial Intelligence-Based Technologies: role of smart sensor technologies

Arkady Zhukov, , University of Basque Country arkadi.joukov@ehu.es

Data Scarcity : information and communication technology (ICT)

Data acquisition and storage

Determining the Right Data Set

Cost issues

Integration into existing systems

→ Low cost and high performance sensor technologies

Problems of Artificial Intelligence

Challenges of Implementing AI

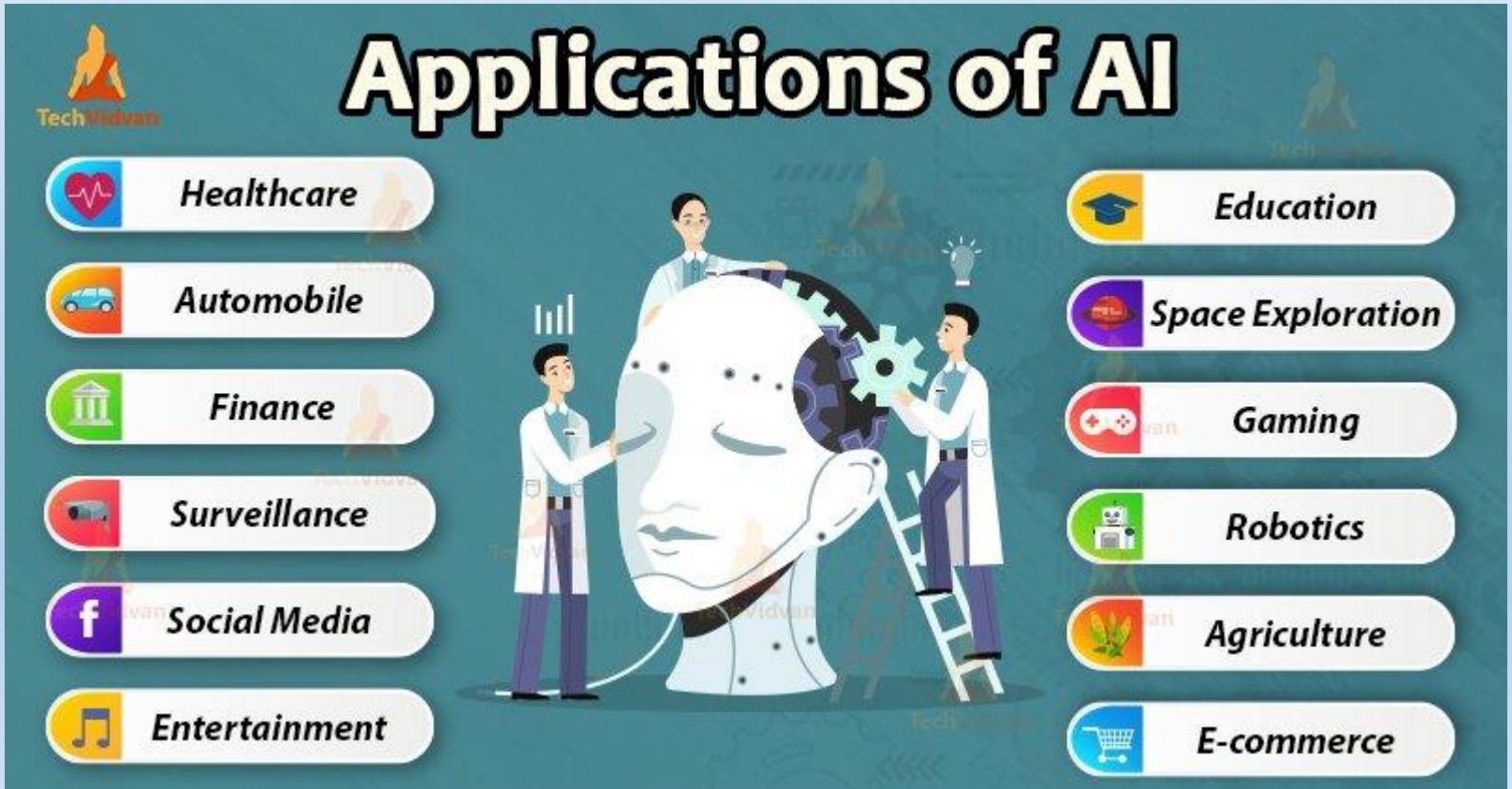
1.Determining the Right Data Set. As most of you are probably aware AI systems are driven and developed by leveraging quality data. ...

2.Data Security and Storage. ...

3.Infrastructure. ...

4.AI Integration into Existing Systems. ...

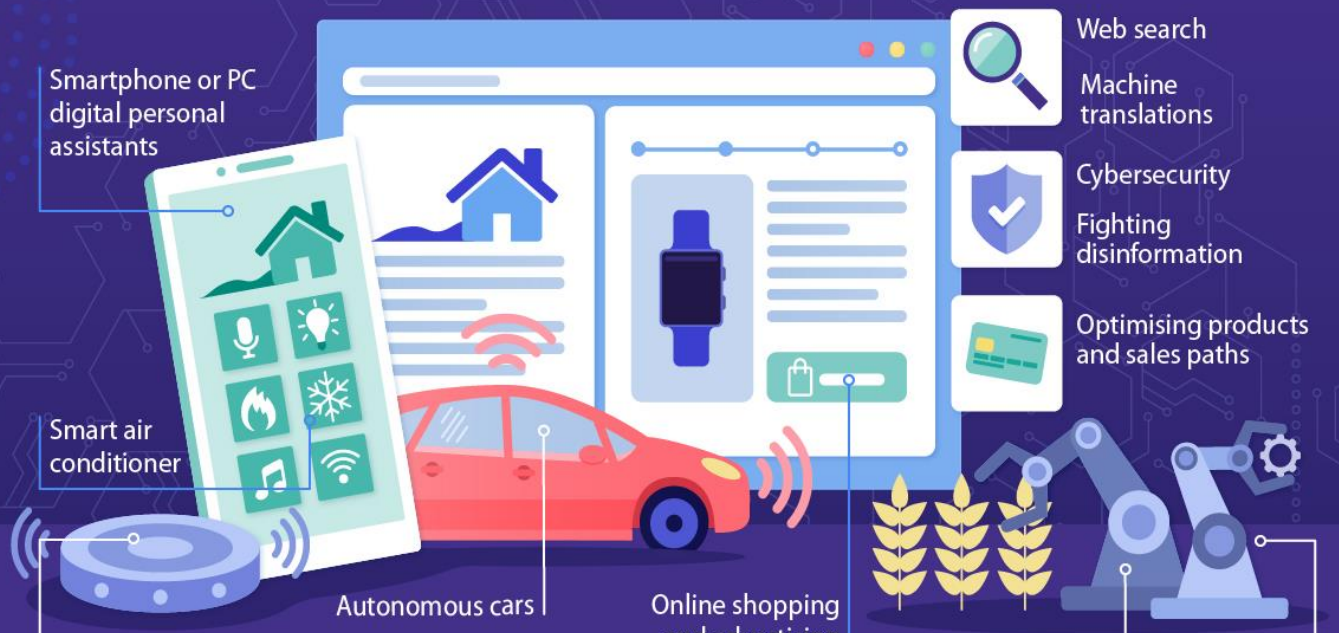
5.Complex Algorithms and Training of AI Models.



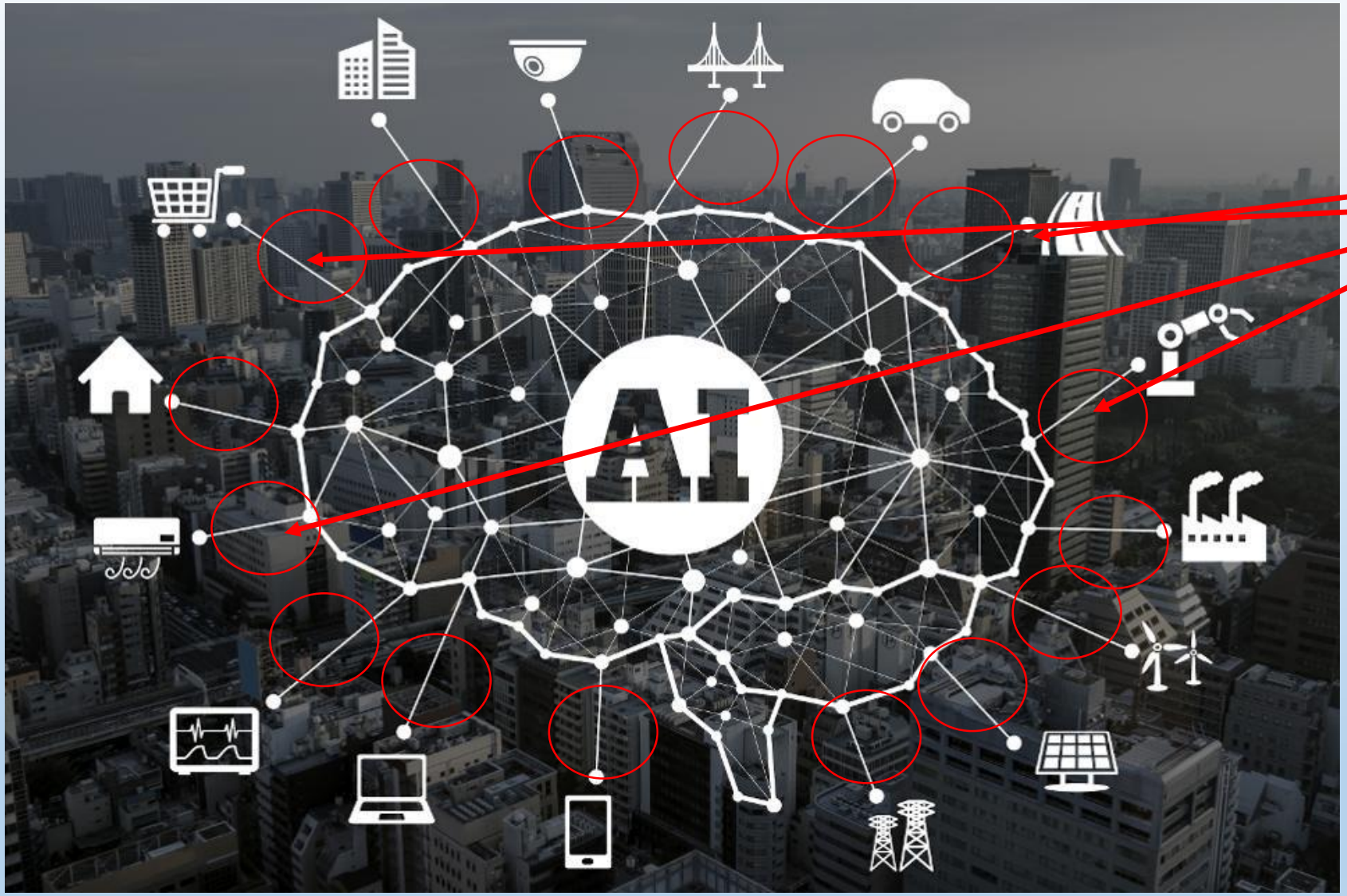
ARTIFICIAL INTELLIGENCE

Everyday and potential use

A few examples of how we already use AI and the possibilities it offers

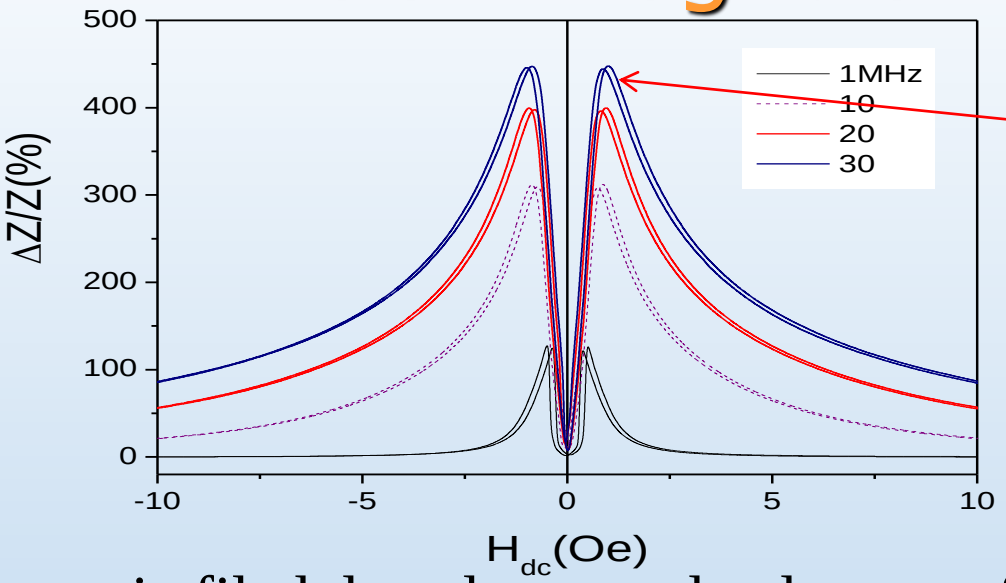


europarl.eu

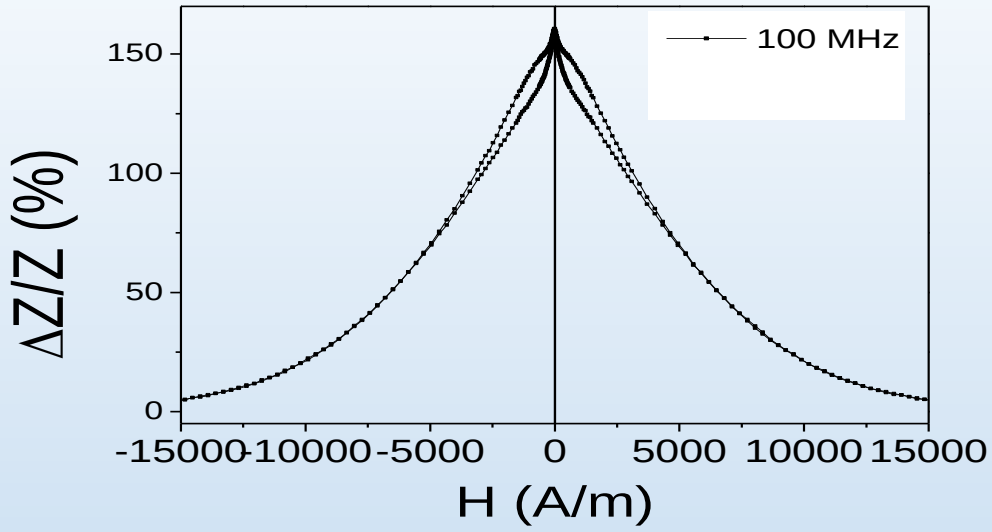


Sensors

Giant Magneto-impedance effect



500% change per 1 Oe

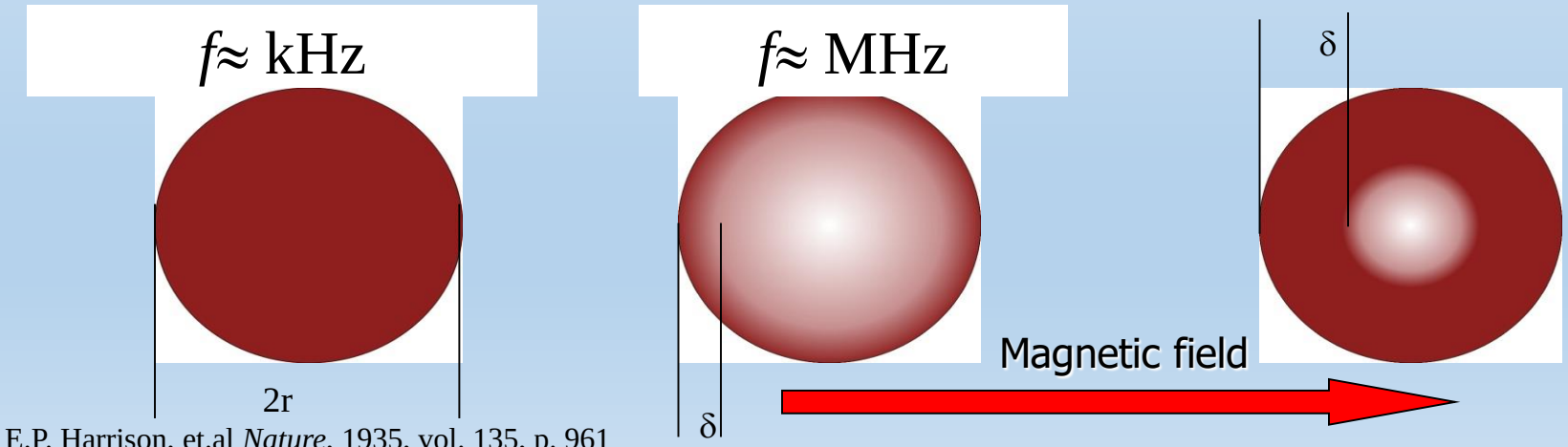


Magnetic filed depedence and value are affected by magnetic anisotropy

- Skin Effect of the Magnetic Conductor

AC current frequency

$\mu_\phi \Downarrow \rightarrow \delta \Uparrow$



E.P. Harrison, et.al *Nature*, 1935, vol. 135, p. 961

$$\delta = (\pi \sigma \mu\phi f)^{-1/2}$$

1. $\mu\phi(H,f)$ *(Soft magnets)*
2. $\delta < r$ (at high enough f)

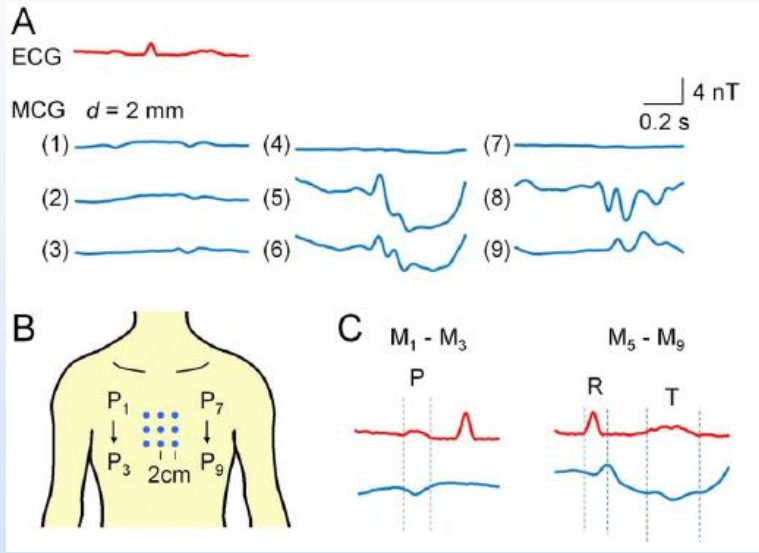
(Low dimensions)

Z(H)

$$\Delta Z / Z = \{|Z(H_{ex})| - |Z(H_{max})|\} / |Z(H$$

Essentialy to have magnetically soft conductor – cyllindrical geometry best

Magnetic Field and Magnetic Sensors



Bio magnetic field

Nature magnetic field

Industrial magnetic field

Space magnetic field

Geo-magnetisms

Storage and magnet

SC-magnet

pT nT μT mT T kT

Tesla (T)

Source: Prof. K. Mohri

10^{-10} 10^{-8} 10^{-6} 10^{-4} 10^{-2} 1 10^{2} 10^{4} 10^{6}

nG μG mG G kG MG

Gauss (G)

Intrinsic noise level at room temperature.

Hall sensor (0 ~ 1 MHz)

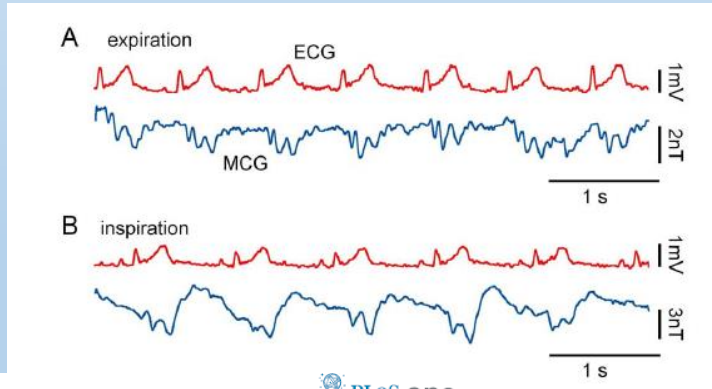
MR, GMR sensor (0 ~ 10 MHz)

Fluxgate sensor (0 ~ 10 kHz)

Amorphous wire MI sensor (0 ~ 10 MHz)

SQUID

Proton magnetometer (0 ~ 0.01Hz)



OPEN ACCESS Freely available online
PLoS one

Pulse-Driven Magnetoimpedance Sensor Detection of Cardiac Magnetic Activity

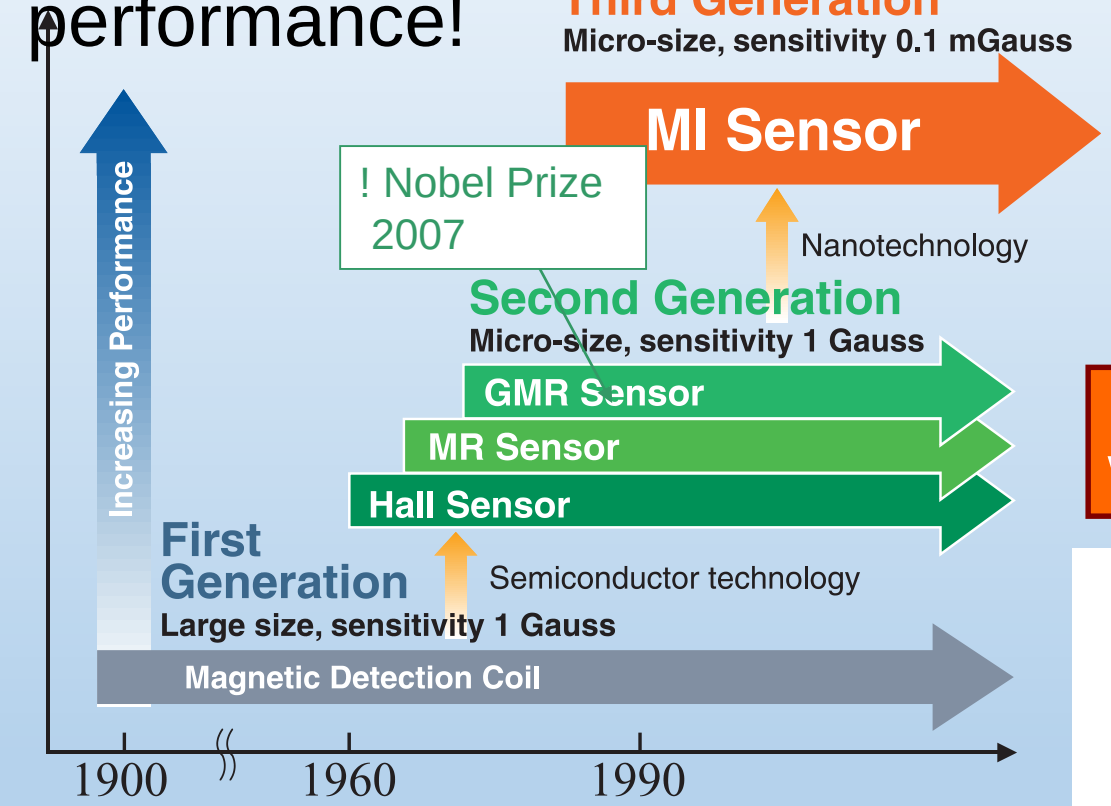
Shinsuke Nakayama[1], Kenta Sawamura[1], Kaneo Mohri[2], Tsuyoshi Uchiyama[2]*

1 Department of Cell Physiology, Nagoya University Graduate School of Medicine, Nagoya, Japan, 2 Department of Electronics, Nagoya University of Graduate School of Engineering, Nagoya, Japan

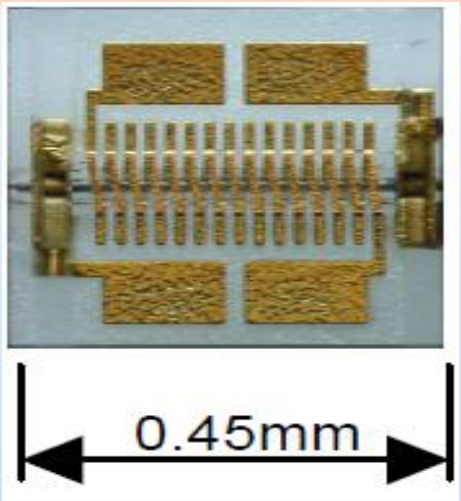
Magnetic sensors and smart composites (GMI effect involved)

Third Generation of Magnetic Sensors Smart composites

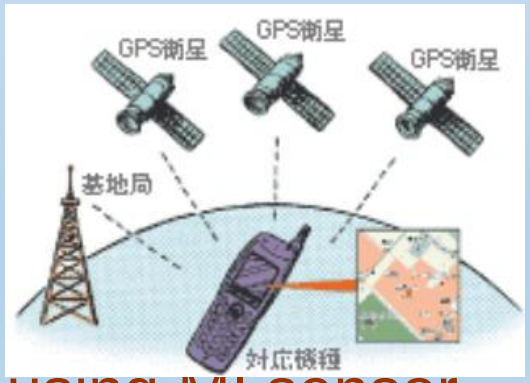
MI Sensors with excellent performance!

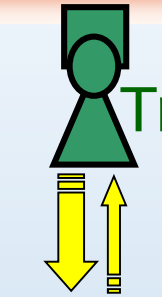


Magnetic Sensor History

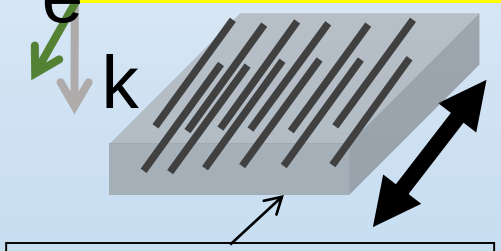


Based on Amorphous Wwire since 2010





Microwave radiation



External stimuli: strain, compression, magnetic field or heating

CASIO 2013.June 68250yen

Amorphous wire:
(glass-coated wire)
Metal dia. : 11.3 μm
Total wire : 14.5 μm
Wire length: 520 μm

Amorphous Wire 3-axis Electronic Compass chip: *A MI 306*

Resolution	0.16 μT (160 nT)
Dynamic range	± 1.2 mT (±12 Oe)
Power voltage V_{dd}	1.7 V
Power current I_{dd}	150 μA
Power consumption	255 μW
Operating temperature	−45 ~ 80 ℃
Chip dimension	2.04 × 2.04 × 1.0 mm
Reversibility for big disturbance magnetic field shock	∞

Advantageous of MI sensor :

1) Micro size and small power consumption (sub-mW)
2) High sensitivity with resolution of 0.01 % for dynamic range (Pico-Tesla resolution)
3) Quick response with GHz
4) High reversibility for big magnetic field disturbance shock
5) High temperature stability

Advanced 3-axis MI sensor chip installed in watch

Industrial application in Smart phone using MI sensor

Last tendencies: Size reduction, frequency increasing

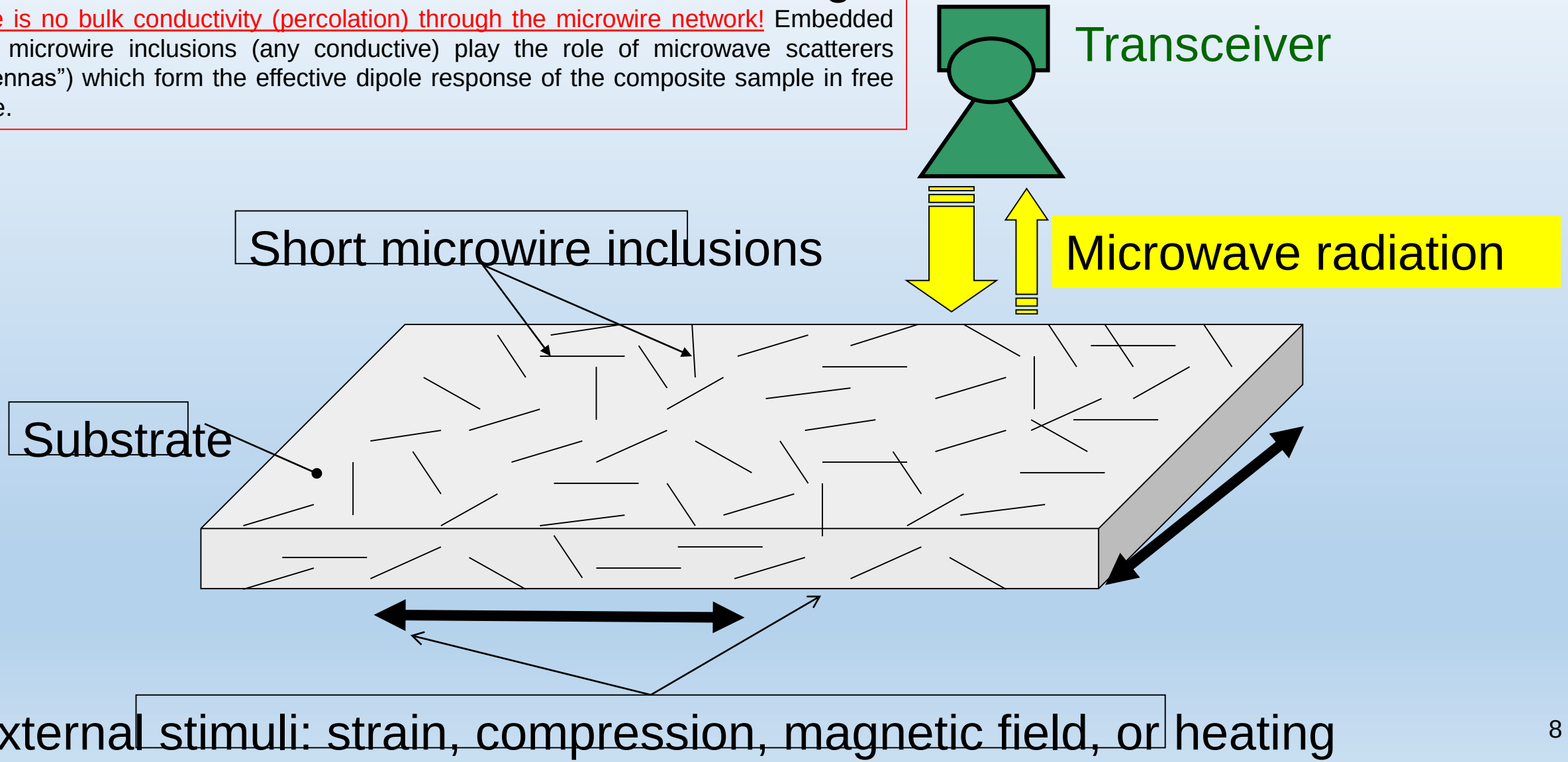
Soft magnets are needed

Source: Aichi Micro Intelligent Corporation

Smart composites with magnetic wire inclusions

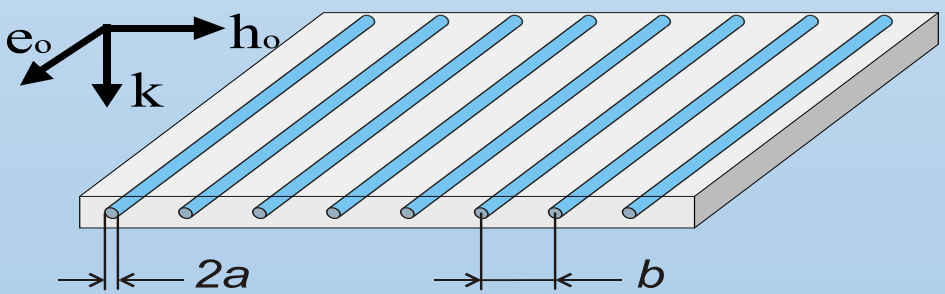
Free-space microwave sensing technique: embedded short ferromagnetic microwires

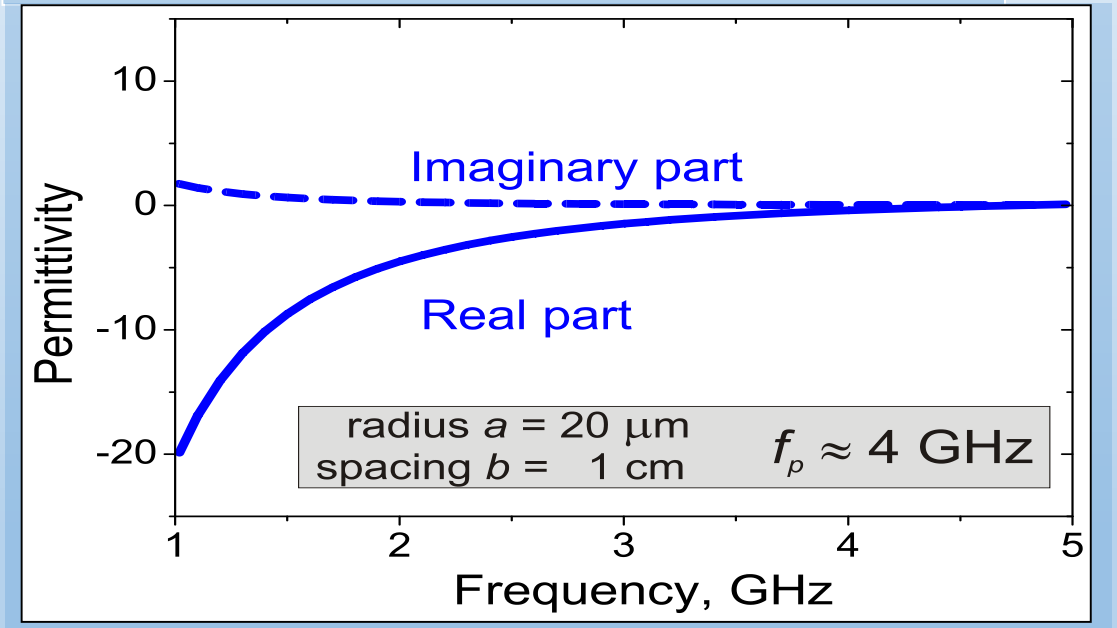
There is no bulk conductivity (percolation) through the microwire network! Embedded short microwire inclusions (any conductive) play the role of microwave scatterers (“antennas”) which form the effective dipole response of the composite sample in free space.



Composites with unusual dispersion of permittivity

1. Ordered long wire inclusions



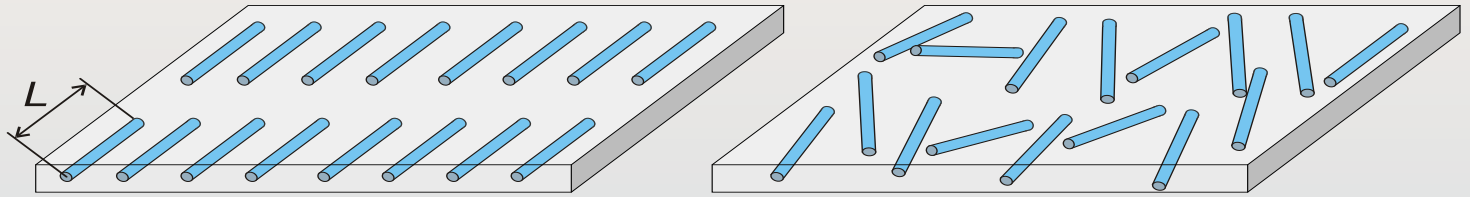


Ordered thin long wire structures behave like a plasma in the microwave region with a plasma frequency:

$$\omega_p^2 = \frac{2\pi c^2}{b^2 \ln(b/a)}$$

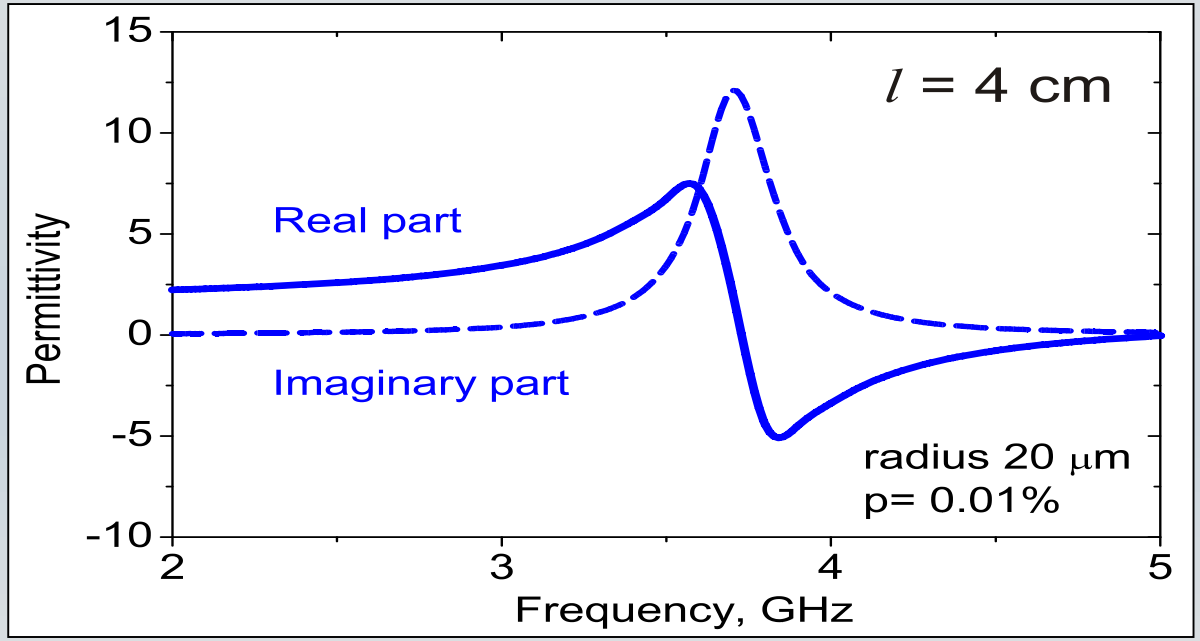
2. Ordered short wire inclusions (0.5-5 cm)

3. Arbitrary directed short wire inclusions (0.5-5 cm)



The short wire composites are characterized by resonance type of the ε_{ef} as the wires behave as dipole antennas with the resonance at half wave length:

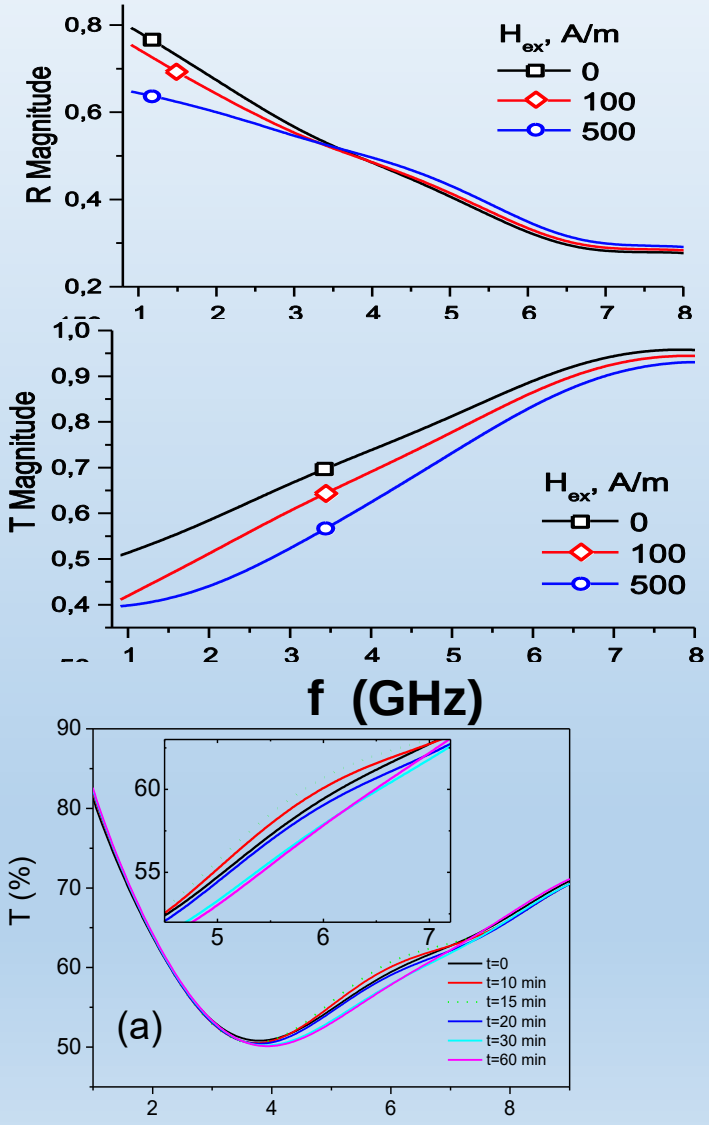
$$\omega_{res} = \frac{\pi c}{l\sqrt{\varepsilon_d}}$$



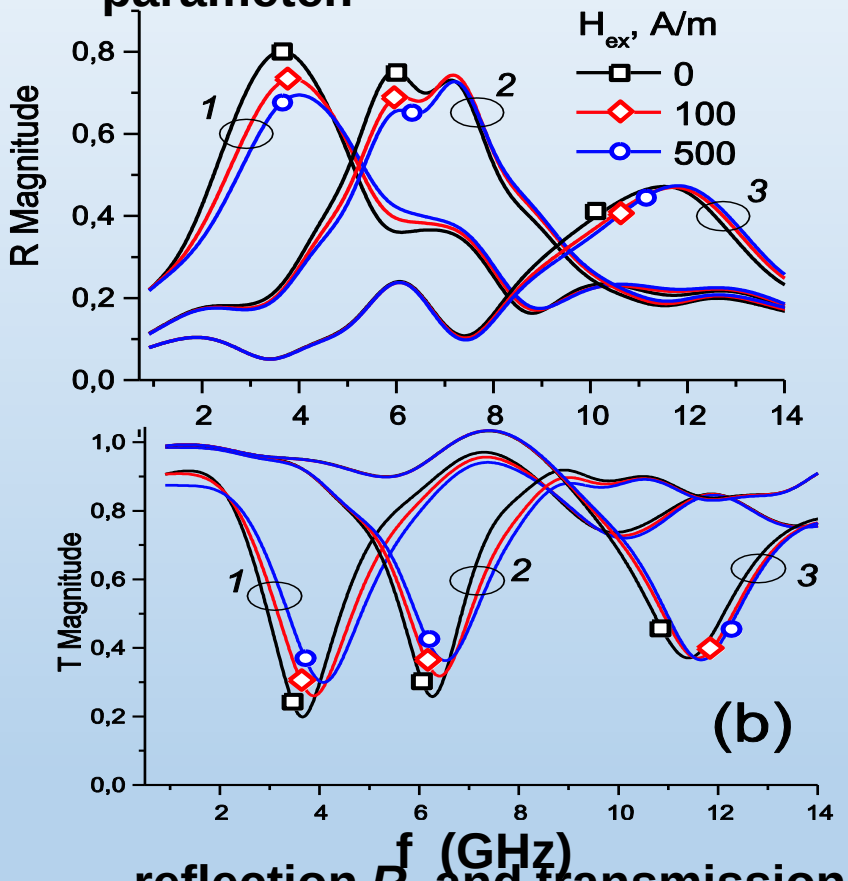
Smart composites with magnetic wire includions

experiment

Spectra of *R*, *T* for composites with long wires with *Hex* as a parameter (*Hex*=0,100, 500A/m).



Spectra of *R*, *T* of composites with cut wires of length 40 (1), 20 (2) and 10 (3) mm with the field as a parameter.

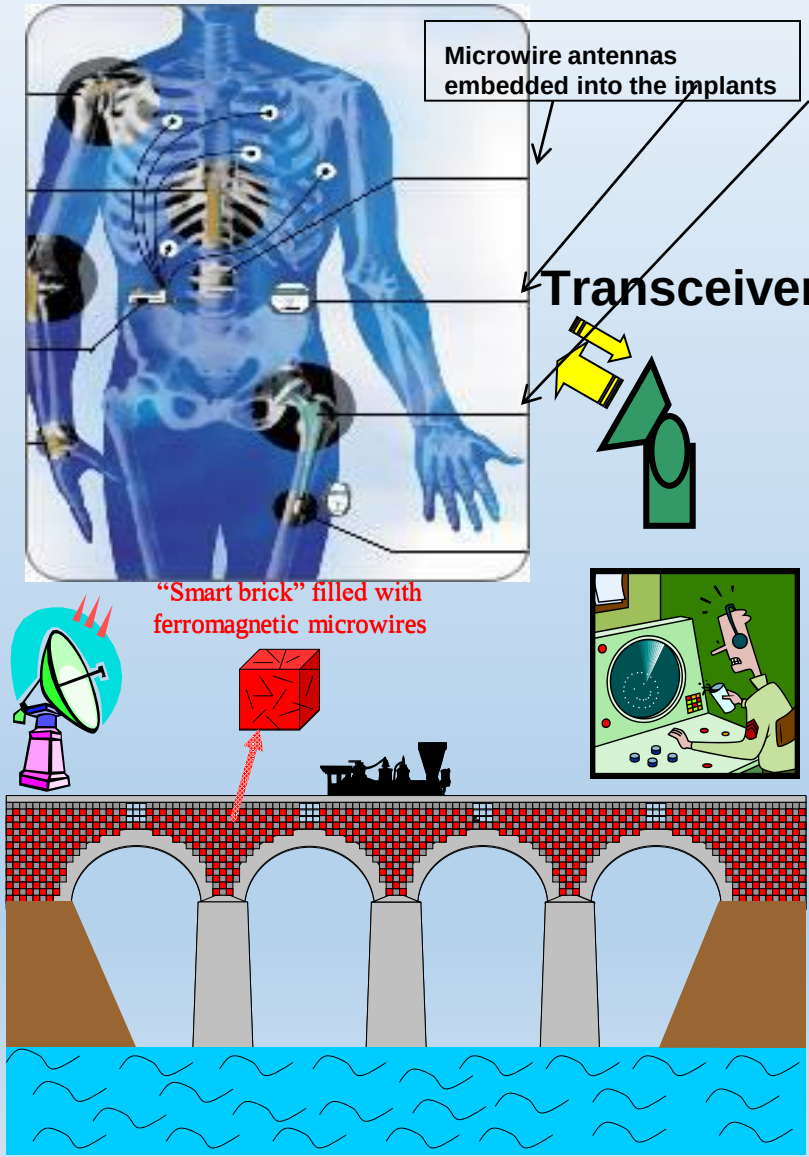


reflection *R* and transmission *T* spectra

L.V. Panina, M. Ipatov, V. Zhukova, A. Zhukov and J.Gonzalez, Applied Physics A: Materials Science and Processing (2011), DOI: 10.1007/s00339-010-6198-7

A. Allue, et.al "Composites Part A: Applied Science and Manufacturing, 120 (2019) 12-20

Applicaions:



https://www.japanautomotivedaily.com/2018/02/20/magnetic-sensors-used-in-autonomous-bus-demo-tests-by-mlit/

Magnetic Sensors Used in Autonomous Bus Demo Tests by MLIT

Feb. 20, 2018

The Ministry of Land, Infrastructure, Transport and Tourism (MLIT) began a series of autonomous bus demonstration tests on public roads …

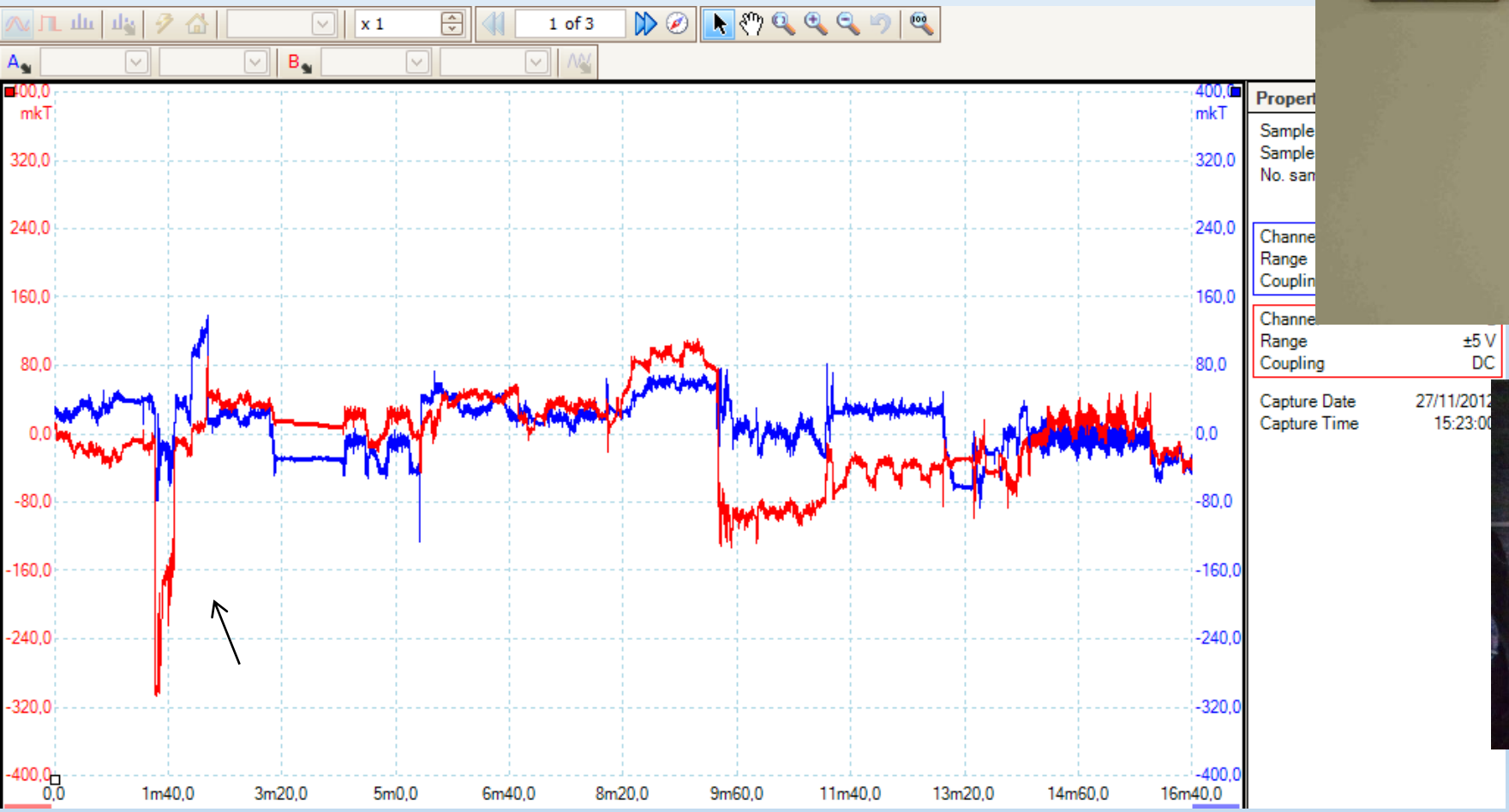
(1) 2017. 11.11-17 ; Shiga pref., Higashi-ohmi, Okueigenji, Michinoeki area
(2) 2017. 12.03-10 ; Hokkaido, Hiroo-gun, Michinoeki area
(3) 2018. 02.10-17 ; Nagano pref. Ina city, Hase, Michinoeki area
The test bus has been developed by Advanced Mobility Co. Ltd.

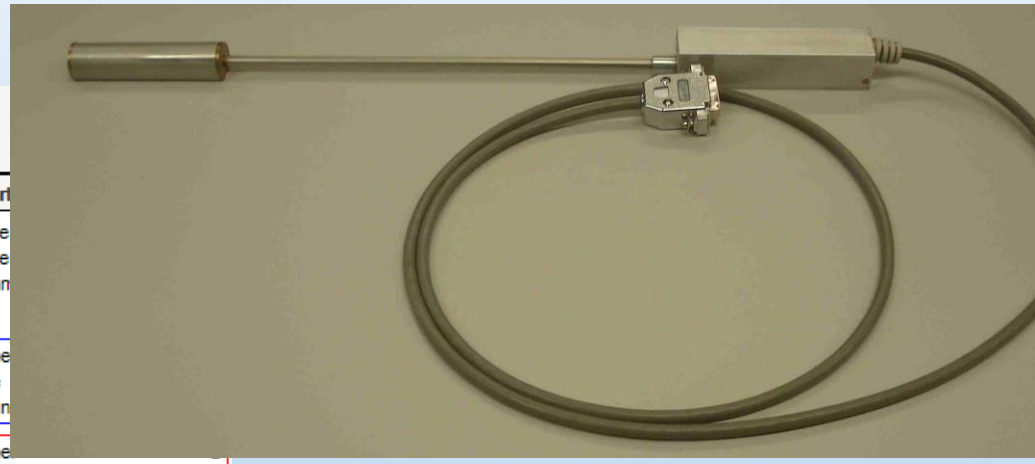
The magnetic guide system (**MPS**) has been developed by Aichi Steel Corp. using Amorphous Wire Magneto-Impedance sensors (MI sensor) module which detects only a weak magnetic field generated from the ferrite magnet marker set on the road surface cancelling various road ambient large disturbance magnetic fields.

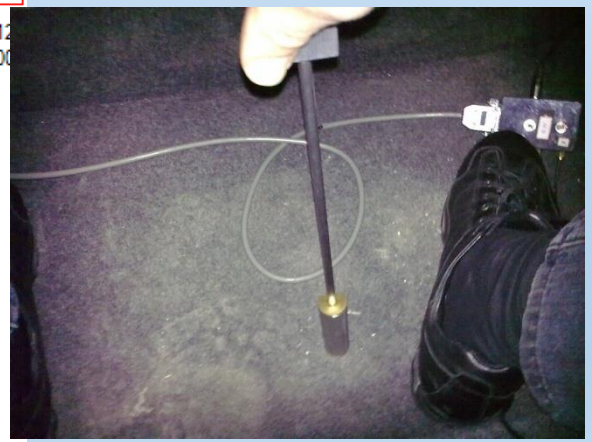
(Memo K.Mohri 2018.3.8)

EU project: development of magnetic sensor based on GMI effect for control of EM- safety of electric car (FIAT, MIRA….)

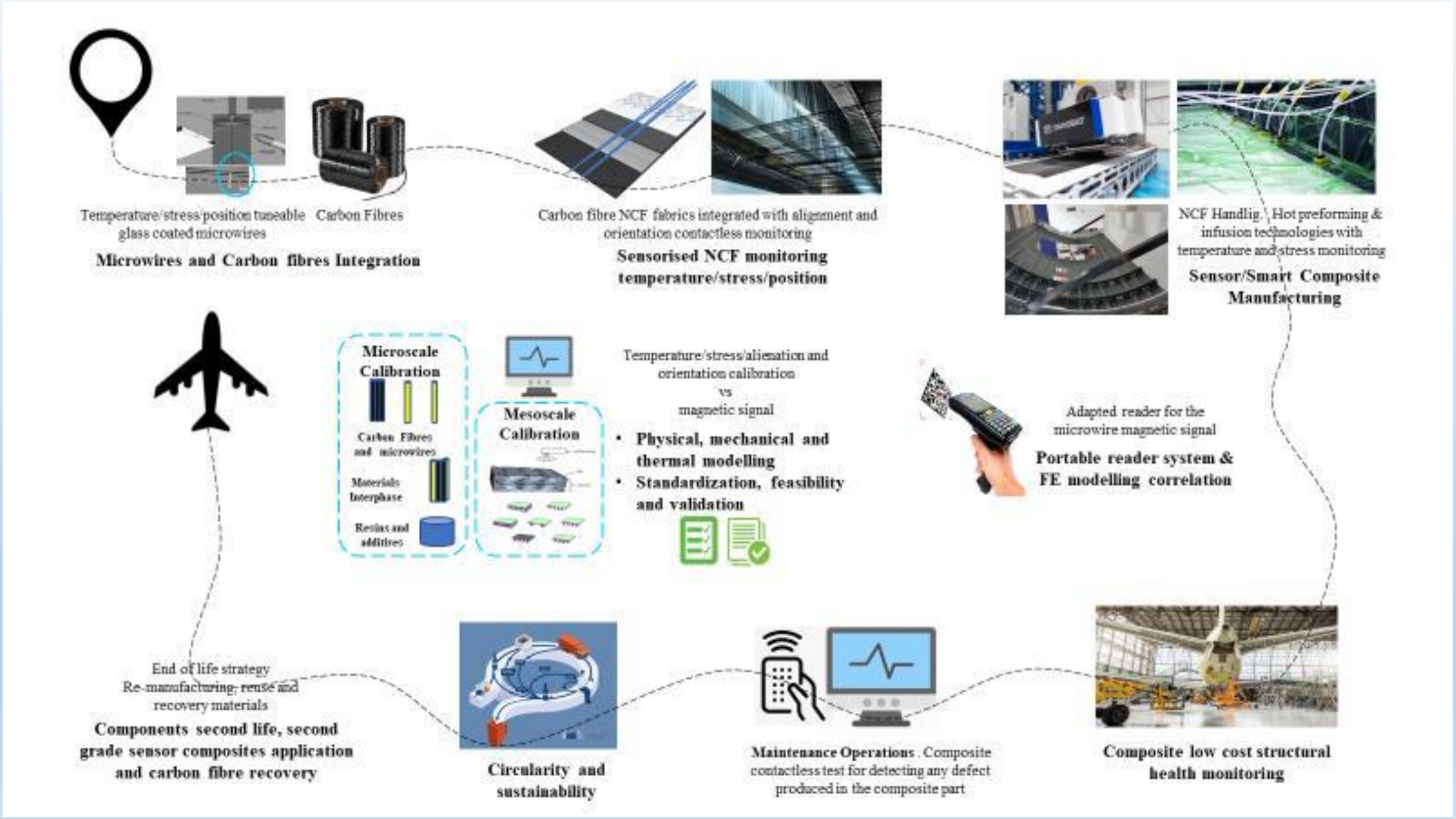
MAGNETIC FIELD MEASUREMENTS WITH GMI MAGNETOMETER inside the electric car (FIAT Turin Nov. 2012) (FP7 project)







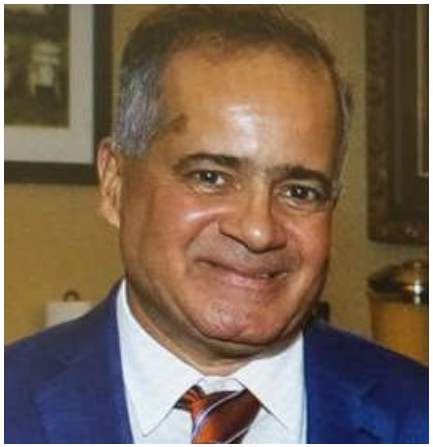
INFINITE: Aerospace Composites digitally sensorised from manufacturing to end-of-life (Horison EU project – our group involved)



Panel:
Challenges on AI-based Technologies
(AI and Security/Privacy)

InfoWare 2022

Panellist Position



AI and Security/Privacy

Dirceu Cavendish, Kyushu Institute of Technology USA/Japan cavendish@ndrc.kyutech.ac.jp

- 6G networking
- IoT Systems Architecture
- Privacy Technologies
- Privacy Challenges
- AI/ML Security/Privacy

→ Pervasive deep personal data mining

→ Privacy regulations plays catch up with threats/attacks

→ AiModels' attacks will become commonplace

IARIA 2022 Panel

Challenges on AI-based Technologies

AI and Privacy/Security

Dirceu Cavendish, Kyushu Institute of Technology, Japan

6G Networking

6G Salient Characteristics

- Full spectrum efficiency (sub-6Ghz, mmWave, THz, visible light)
- Technical objectives
  - 1Tb/s peak data rates
  - 10/100usec latency
  - 1000 km/h mobility
  - 1Gb/sec user peak data rates
  - 10^7 devices/km^2 density
  - 1Gb/sec/m^2 traffic
  - 5x to 10x 5G spectrum efficiency

IoT systems architectures

- Small edge devices
- Cloud intelligent services
- Smartphone command and control

- AI driven channel statistics prediction (6G controls)
- Efficient data transport: control/emergency/low latency

- ML supported verticals
  - Automotive: autonomous driving
  - Full sensory virtual reality (VR)/augmented reality (AR)
  - Smart Healthcare: smart medical devices, disease control

IoTRC Kyushu Institute of Technology

6G IoT Systems

Architecture

- Small edge devices: sensor, actuator, data edge processor
- Cloud infrastructure
  - Data gathering and analysis
  - System security
- Command and control device: smartphone

Services Verticals

- Home management
- Transportation: Autonomous vehicle driving, traffic control
- Healthcare: data analysis, therapy delivery, disease propagation/control
- Manufacturing industry (AR/VR)

IoTRC Kyushu Institute of Technology

Privacy challenges

Unreadable/unenforceable EULAs

- Cumbersome End-User License Agreements
- Click through services

Data sharing

- Health personal data controlled sharing (medical personnel)
- Vehicle data gathering for autonomous driving vs insurance companies
- Massive data gathering (medical, transportation, VR/AR)

Third party data gathering

- Social networks gathering (users and non-users)
- Surveillance systems: photos, geolocation
- Financial institutions: credit card activities, trading data.
- Wide scale shopping behavior: grocery stores (reward programs), wholesale stores, gas stations.

Technology failures and privacy

- IoT device hacking: cheap HW, small SW footprint
- Cloud systems miss-management
- Cryptographic material leaks
- Biased training data sets

IoTRC Kyushu Institute of Technology

Current privacy technologies

Data encryption at rest and in transit

- Strong requirements for Healthcare (HIPAA)
- Non-existent regulations for other vertical IoT markets

Authentication and Authorization

- Multifactor authentication
- Oauth2.0: explicit resource authorizations via security tokens
- Hardware Security Module (HSM): management of security credentials

IoTRC Kyushu Institute of Technology

AI/ML Systems and Privacy/Security

Machine learning: massive data gathering/processing

- Supervised learning
- Unsupervised learning
- Reinforcement learning

Data privacy regulations

- EU General Data Protection Regulation (GDPR)
- IEEE P3652.1 Federated Learning and Reference Architecture
- Federated AI Technology Enabler (FATE)

Data Sets and ML Model processing challenges

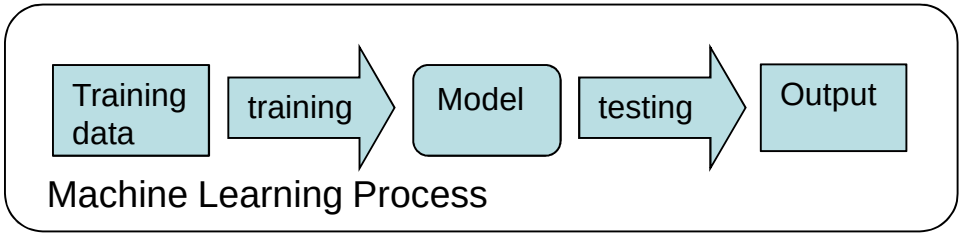
- Data anonymization
- Data set access to a particular ML Model only

IoTRC Kyushu Institute of Technology

ML Threats and Mitigations

Machine Learning Vulnerabilities/attacks and impacts

- Training data manipulation/poisoning: misprediction
- Training data leakage: model extraction, model biasing
- Manipulation of testing sets: misprediction
- Parameters manipulation: misprediction



Machine Learning Defensive Measures

- Model access control (parameters)
- Data sets Integrity/Privacy protection (encryption)
- Data quality controls

Machine Learning Threats

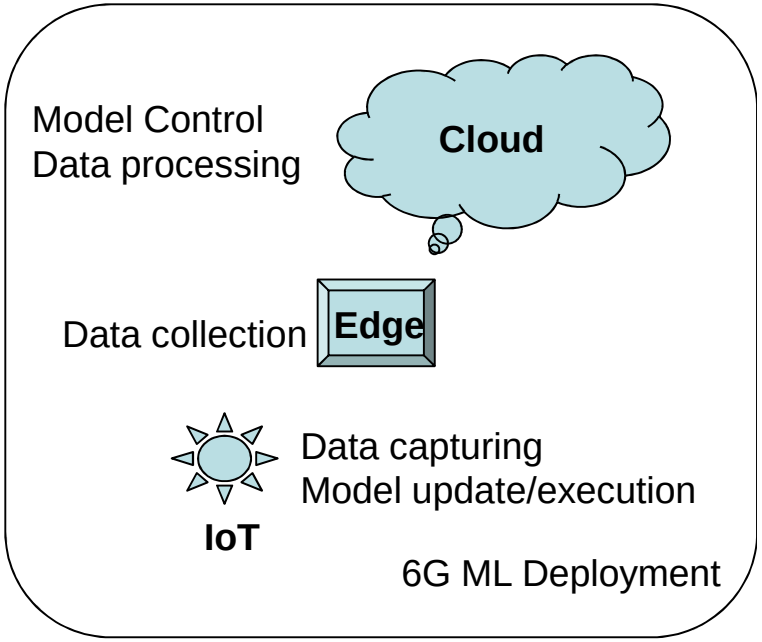
- Edge devices ML model updates: opportunity for attacks
- Cloud systems data collection/model adjustment attacks

Machine Learning as Attack Tool

- User traffic eavesdropping/user behavior inference
- De-anonymization of user data
- IoT type/location inference

Machine Learning as Defense Tool

- Malware detection
- Data sanitization/tampering detection



IoTRC Kyushu Institute of Technology

AI/ML in 5G wireless: security/privacy

Sensing AI: Channel State Information and image data collection

- People counting – privacy: CSI data anonymization
- Object detection – privacy: feature maps extraction
- IoT node/user device localization – privacy: CSI data anonymization
- Motion (e.g. gait abnormality) and activity recognition – privacy:CSI data anonymization

Network Node AI

- Content caching (backhaul load reduction) – user preference privacy
- Edge computing management (resource allocation) – security (power control)
- Network orchestration: edge computing, caching, networking resources – security (blockchain)

Network Transmission AI

- PHY: CSI acquisition (massive MIMO), coding/decoding (channel model) - security
- MAC: Channel allocation, power control, interference management – security
- Network: Spectrum allocation, data offloading, network resource management - security

Device AI

- Malware detection - security
- Motion detection – privacy
- Biometric detection - security

IoTRC Kyushu Institute of Technology

OPEN DISCUSSION