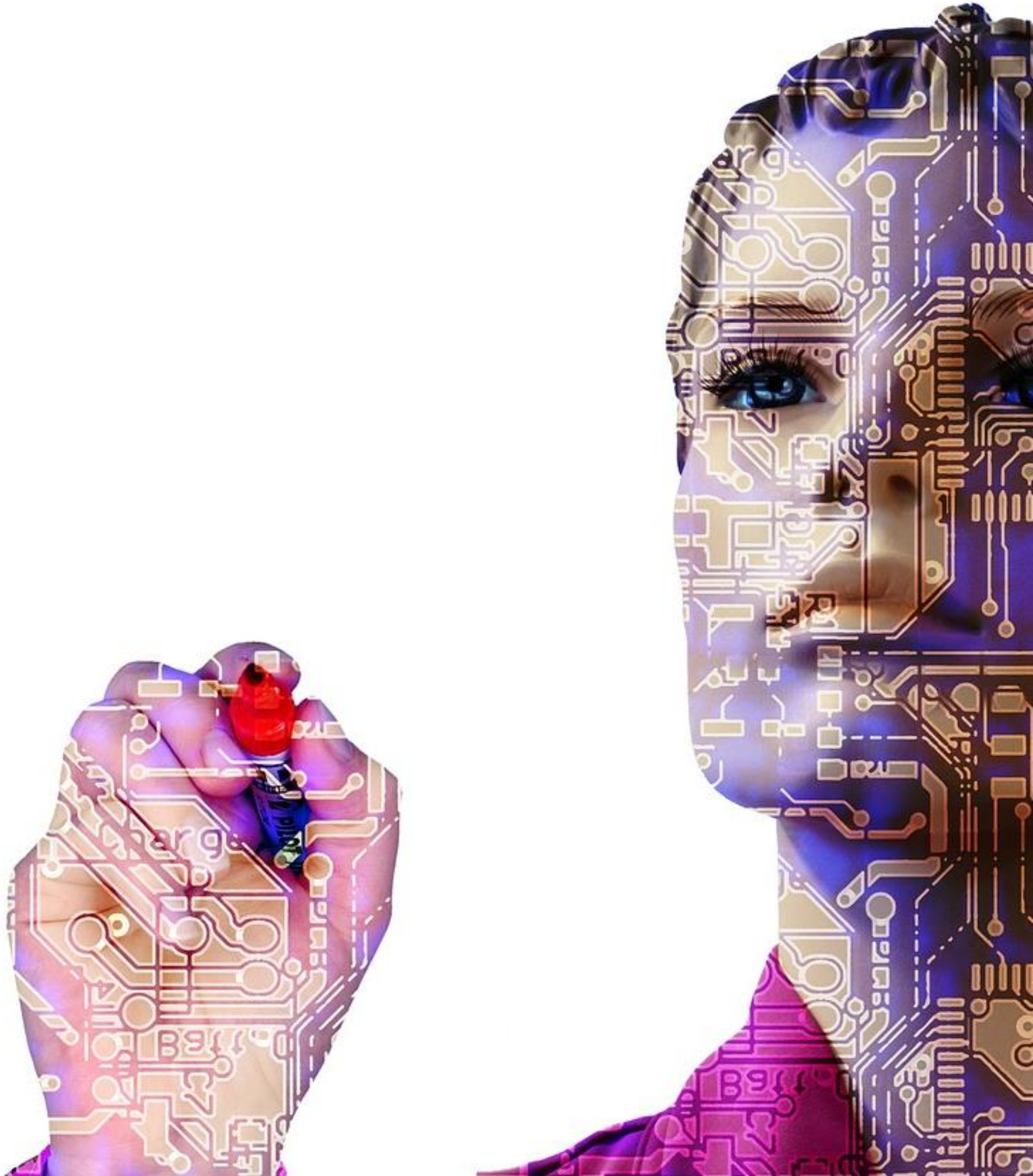
Challenges and opportunities in the integration of the Systems Engineering process and the AI/ML Lifecycle

Jose María Alvarez Rodríguez | Associate Professor | josemaria.alvarez@uc3m.es

Let’s ***speak*** some AI…



Digitalization

European companies

9/10

Digital technologies are an "opportunity".

Technology adoption

35%

Adopted 2 of 9 the key digital technologies

Big Data Analytics & AI

46%

Increase in their annual turnover being 24% BD and 5% AI

E. Union, "Digital Transformation Scoreboard 2018 EU businesses go digital: Opportunities, outcomes and uptake," COSME programme of the European Union, Luxembourg, 978-92-9202-353–9, 2018.

Context

Evolving and competitive market for Cyber-physical systems (CPS)

Legislation

Business needs and models

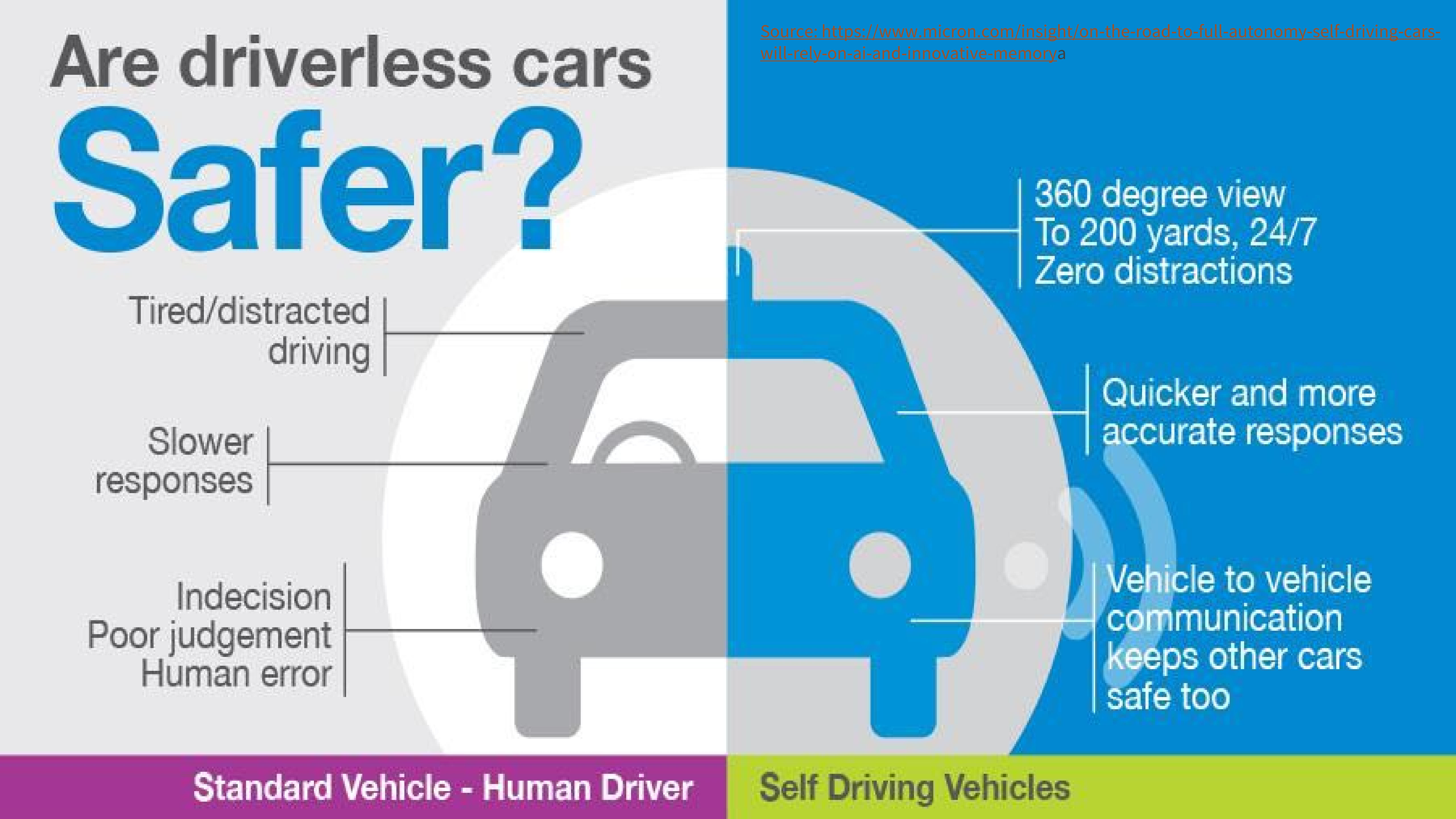
Quality

- Safety
- Reliability
- Cyber-security
- Certification
- Environment
- Standardization
- Ethics
- …

Engineering process , methods, technology & tooling

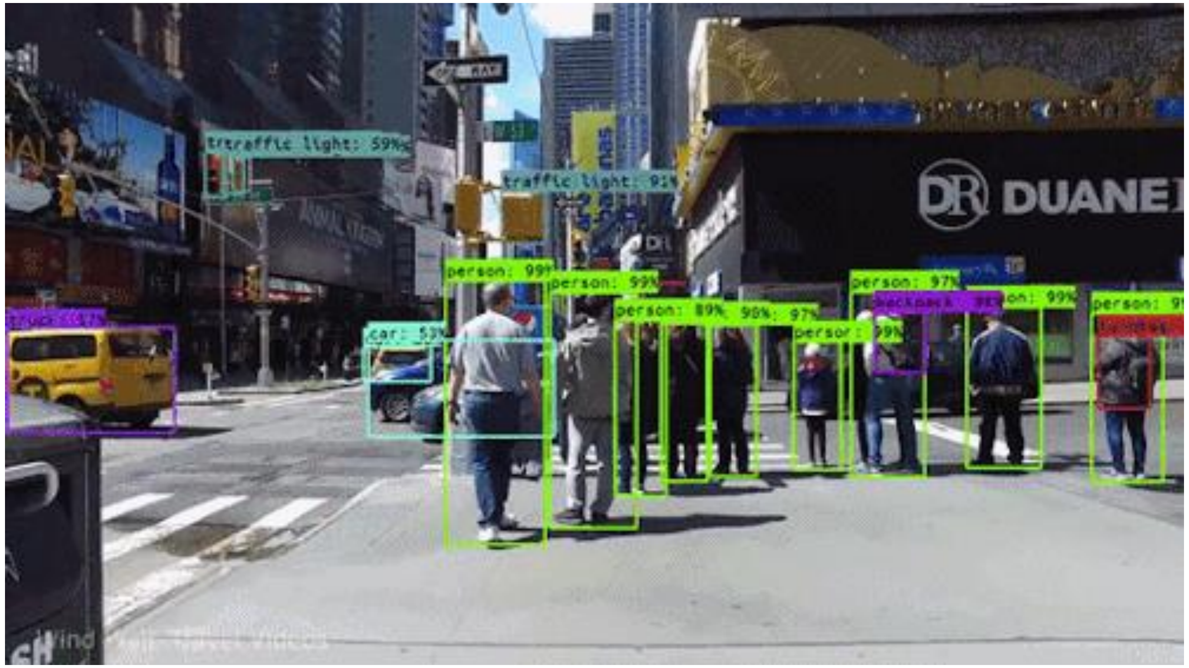
AI/ML & Deep Learning

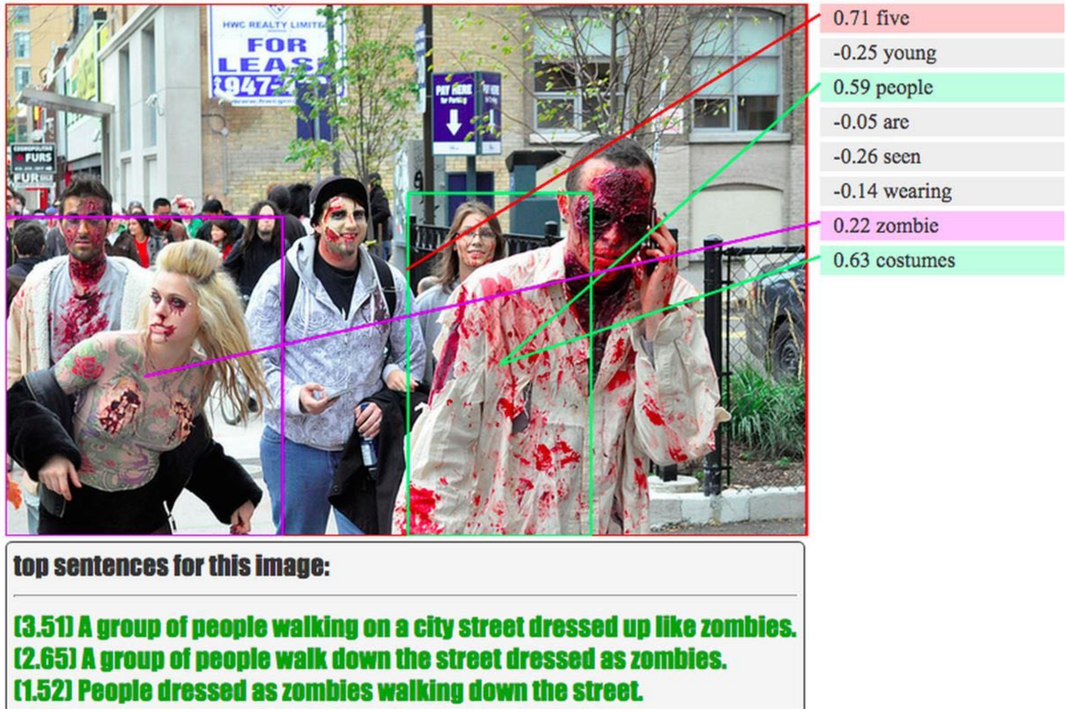
Source: https://www.micron.com/insight/on-the-road-to-full-autonomy-self-driving-cars-will-rely-on-ai-and-innovative-memorya



What can you see?

Self-Driving Cars (object recognition)

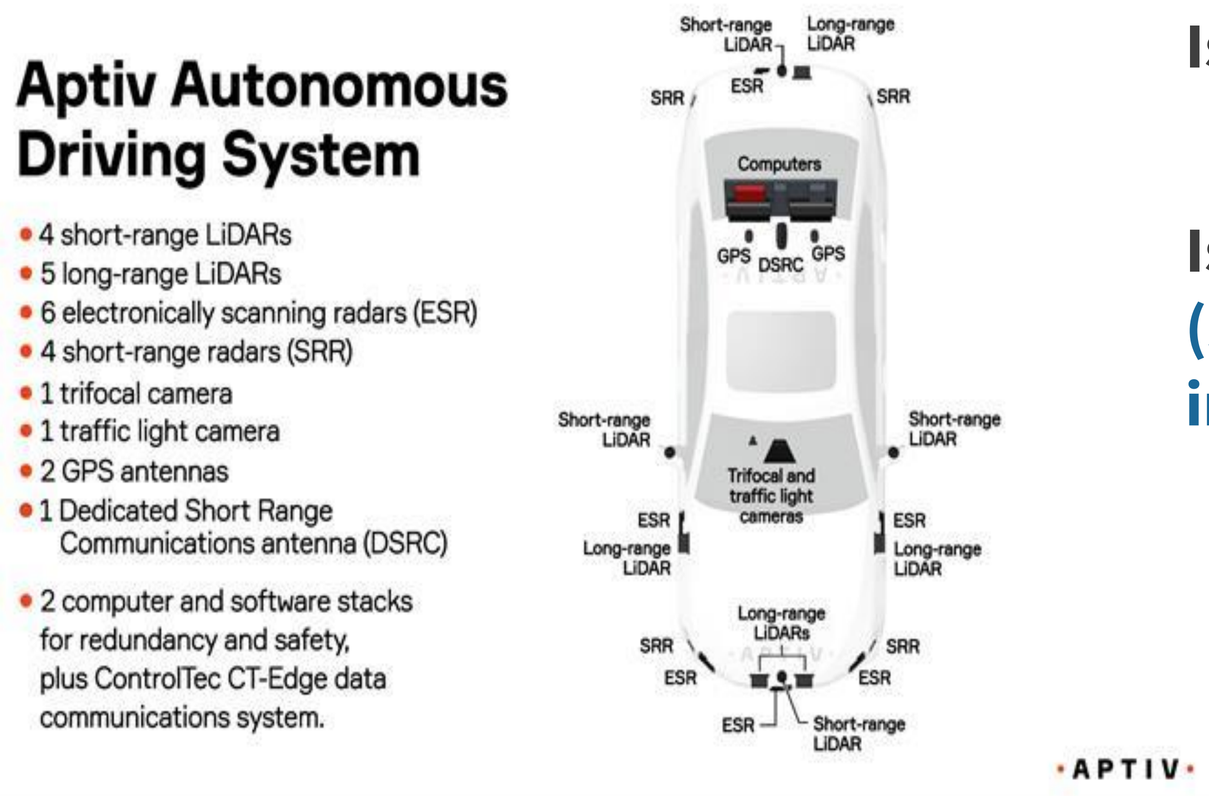




Source .https://towardsdatascience.com/how-do-self-driving-cars-see-13054aee2503

Source: https://www.theverge.com/2015/7/17/8985699/stanford-neural-networks-image-recognition-google-study

An example of architecture



Is it a Car?

Is it a kind of a computer (software and hardware intensive)?

Sensors/Actuators
GPUs
AI/ML models
5G
Edge Computing
...

Source: https://www.aptiv.com/media/article/2018/01/07/the-autonomous-driving-platform-how-will-cars-actually-drive-themselves

Critical factors

Human factors

Adoption of intelligent evolving systems

Safety & Security

Ethics

Conceptual & technological

From business needs/value to system capabilities

Perspective

Software & Systems Engineering

AI/ML lifecycle

Software Engineering

Software production automation

Model-Driven Engineering/Architecture
Software Product Lines
etc.

Agile methods & DevOps

Scrum, Kanban, BDD, TDD, etc.

Initial Focus

Methods and methodology to tackle the problem of software reliability

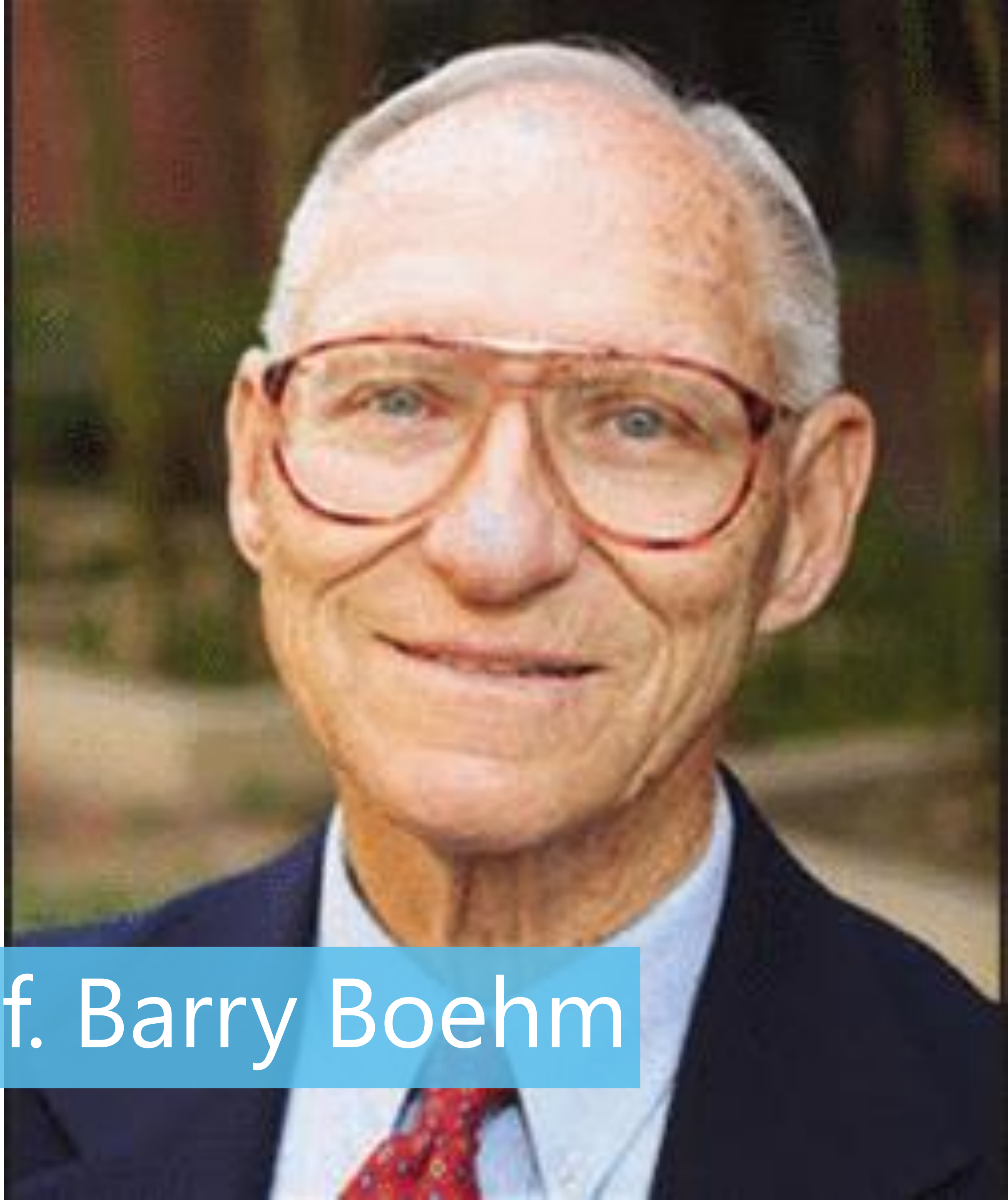
Standard notations

Languages, tools, quality management, maturity models, design patterns, components, etc.

The way through

There is a huge body of **knowledge** and **practice** that allow us to **acknowledge which ARE, and which ARE NOT, the software engineering practices** that **really** represent **timeless scientific and technological foundations** for a proper software development process.

***(My own summary based on [1]*)**



Prof. Barry Boehm

- ***"A Conversation with Barry Boehm: Recollections from 50 Years of Software Engineering". IEEE Software, vol. 35 (5). 2018***
- ***"A View of 20th and 21st Century Software Engineering "***

Software & Systems Engineering process

System Life Cycle Processes

Agreement Processes
- Acquisition Process (Clause 6.1.1)
- Supply Process (Clause 6.1.2)

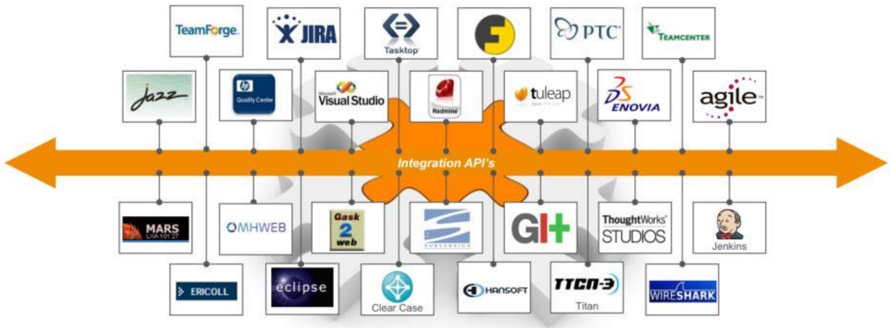
Organizational Project-Enabling Processes
- Life Cycle Model Management Process (Clause 6.2.1)
- Infrastructure Management Process (Clause 6.2.2)
- Portfolio Management Process (Clause 6.2.3)

Technical Management Processes
- Project Planning Process (Clause 6.3.1)
- Project Assessment and Control Process (Clause 6.3.2)
- Decisión Management Process (Clause 6.3.3)
- Risk Management Process (Clause 6.3.4)
- Configuration Management Process (Clause 6.3.5)
- Information Management Process (Clause 6.3.6)
- Measurement Process (Clause 6.3.7)

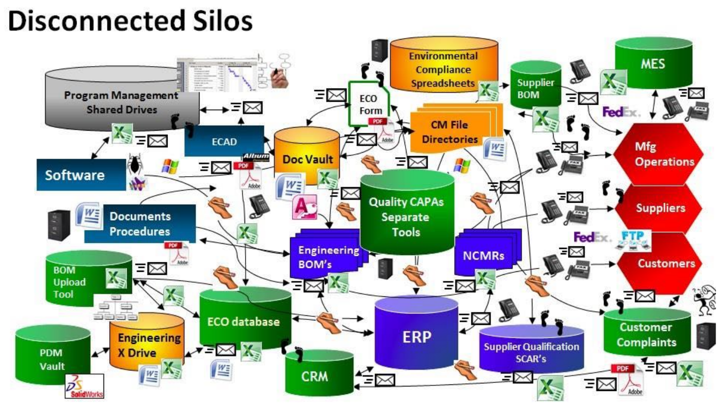
Technical Processes
- Bussiness or Mission Analysis Process (Clause 6.4.1)
- Stakeholder Needs & Requirements Definition Process (Clause 6.4.2)
- System Requirements Definition Process (Clause 6.4.3)
- Architecture Definition Process (Clause 6.4.4)
- Design Definition Process (Clause 6.4.5)
- System Analysis Process (Clause 6.4.6)
- Implentation Process (Clause 6.4.7)

ISO 12207:2017 **ISO 15288:2015**

Engineering (and corporate) environment



Mats Berglund (Ericsson)
http://www.ices.kth.se/upload/events/13/84404189f85d41a6a7d1cafd0db4ee80.pdf



Source: http://beyondplm.com/2014/07/22/plm-implementations-nuts-and-bolts-of-data-silos/

Artificial Intelligence

AI/ML SPRING & Fear
Any x / x ε {domain, problem, place, one, sector, etc.}

04

AI/ML Boost
Theoretical foundations
Algorithms & Techniques
From Deep Blue to Alexa
Lack of data, computational power, etc. (not anymore*)

03

AI/ML WINTER
AI/ML is not cool!
“We can not solve anything”

02

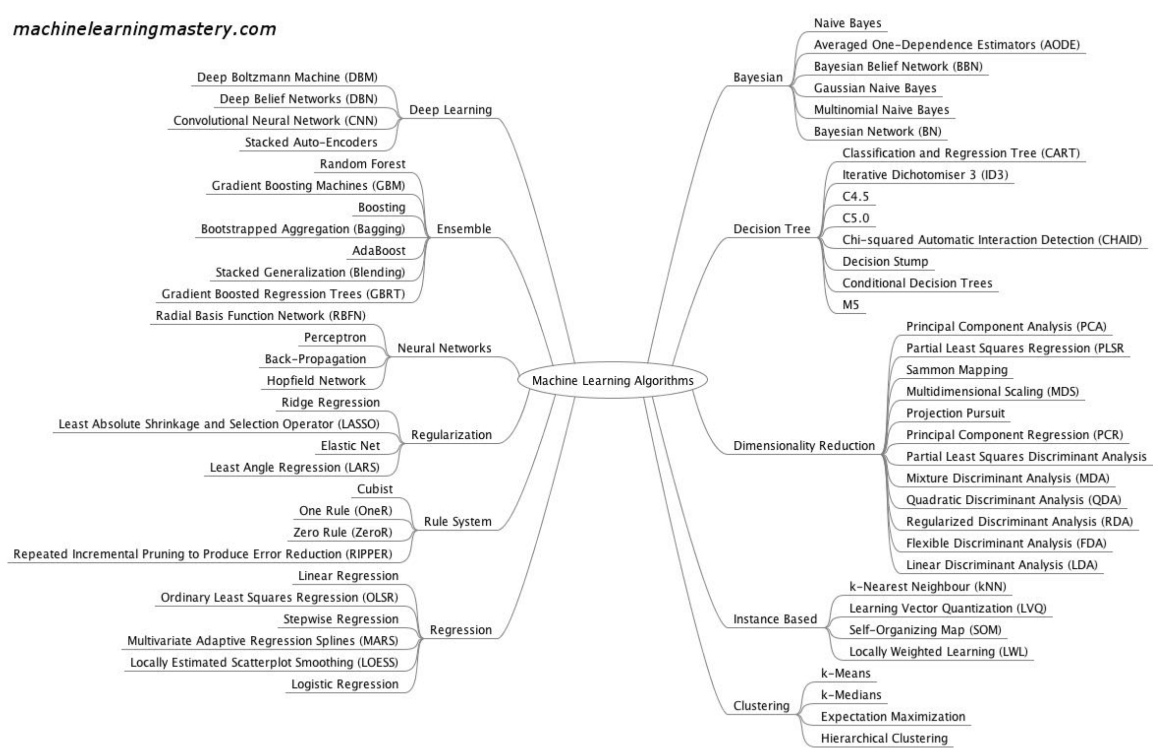
Turing Test, Conversational Systems & Expert Systems
ELIZA
Medical Support Systems
“We can solve everything”

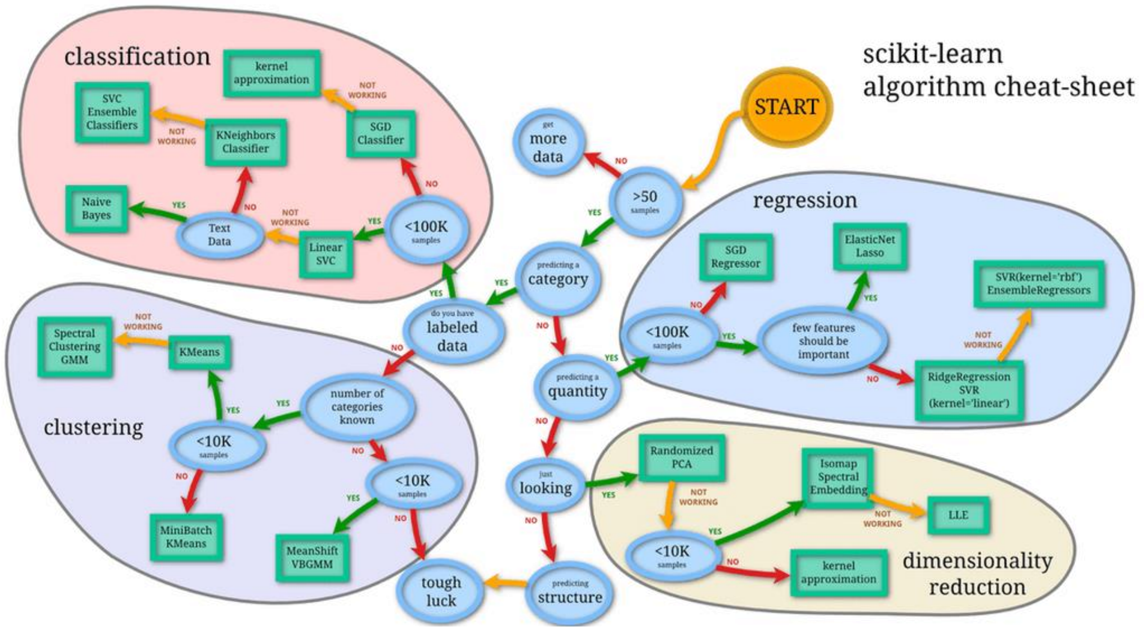
01

The way through

"The **new spring in AI is the most significant development in computing in my lifetime**. Every month, there are **stunning new applications and transformative new techniques**. But such powerful tools also bring with them **new questions and responsibilities**"

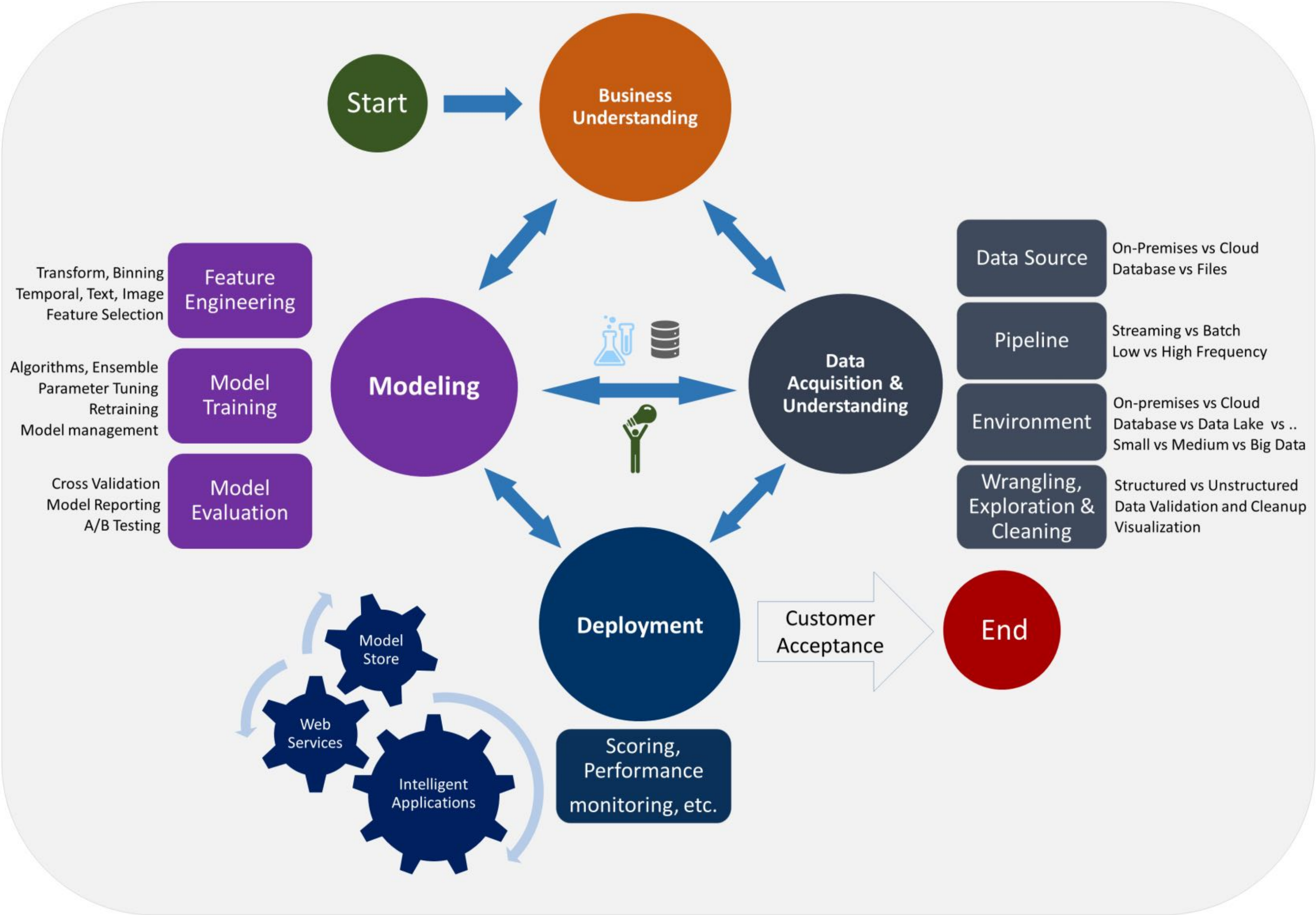
Sergey Brin





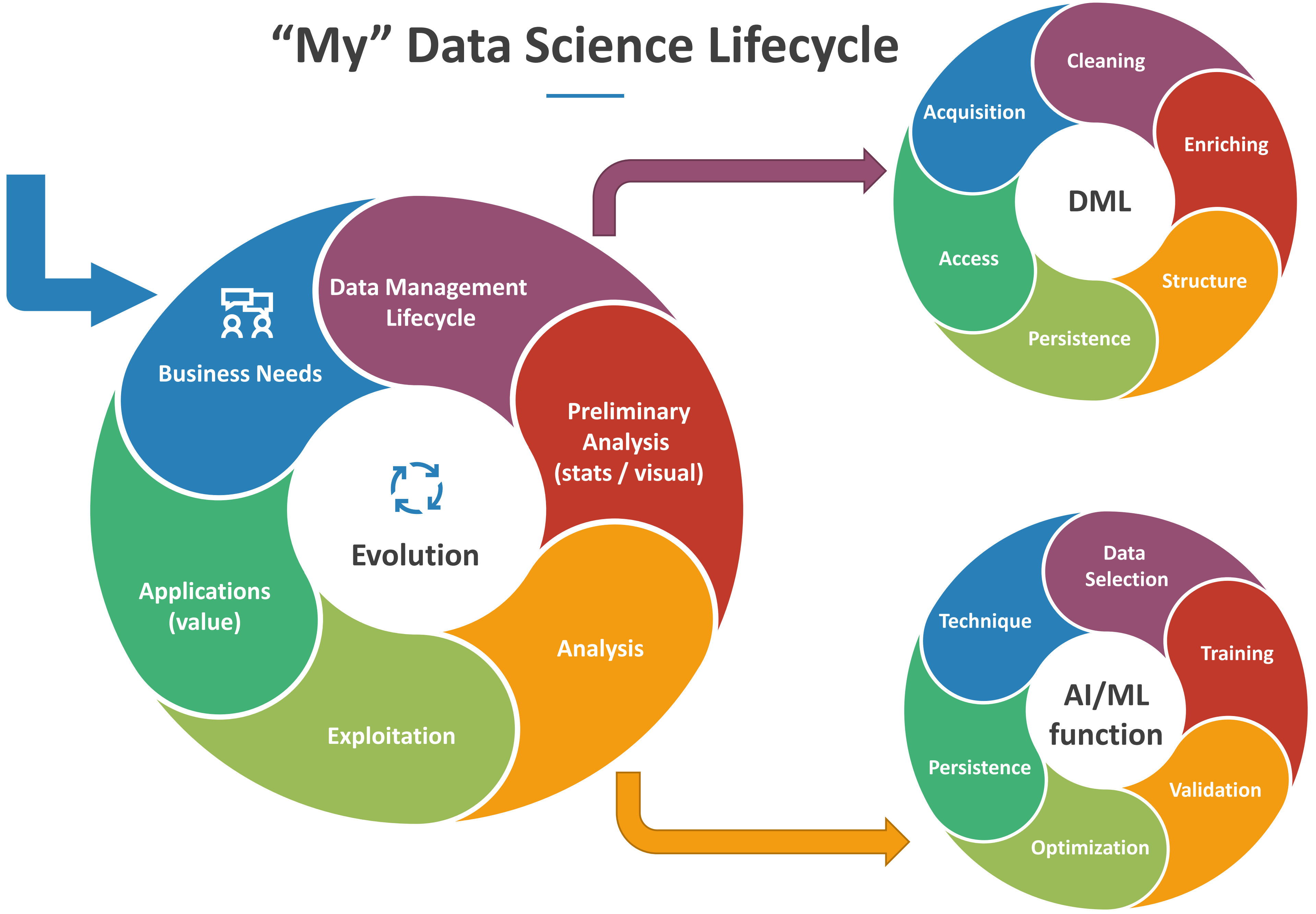
AI/ML Techniques

Data Science Lifecycle

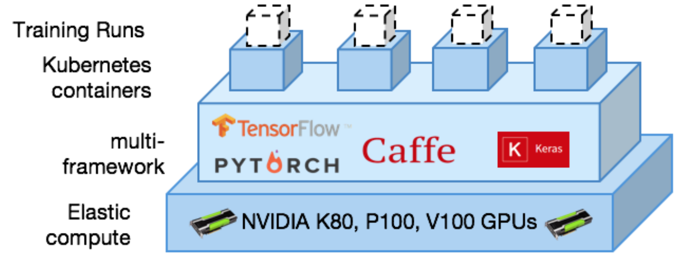


Source: https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/overview

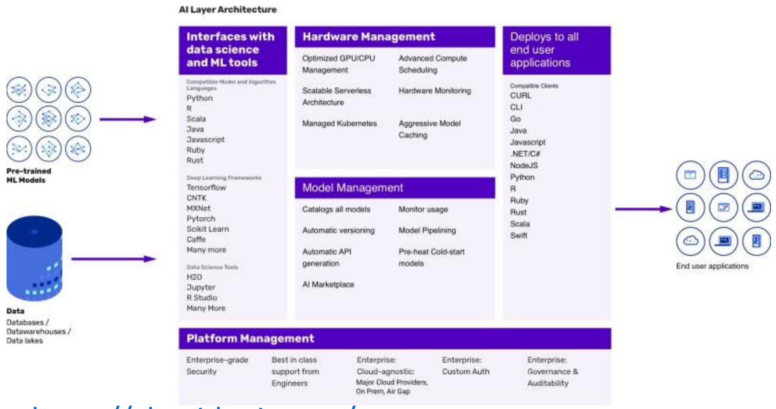
“My” Data Science Lifecycle



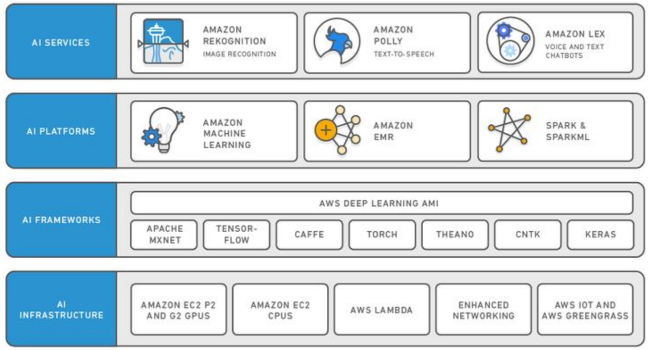
Frameworks/Platforms/...→AI/ML as a Service



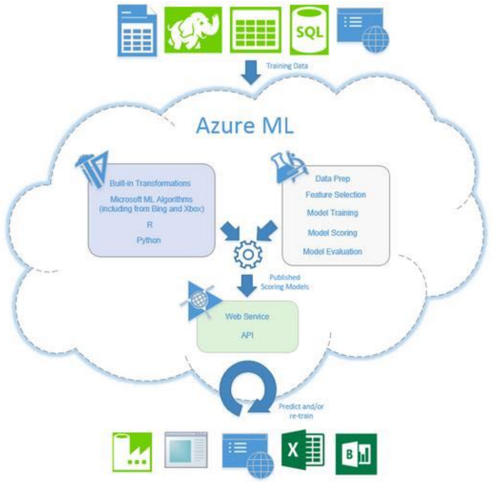
Source: https://www.ibm.com/blogs/research/2018/03/deep-learning-advances/

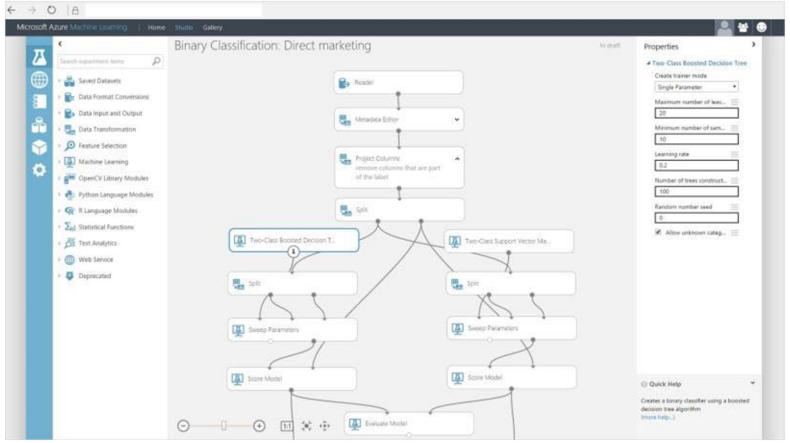


Source: https://algorithmia.com/

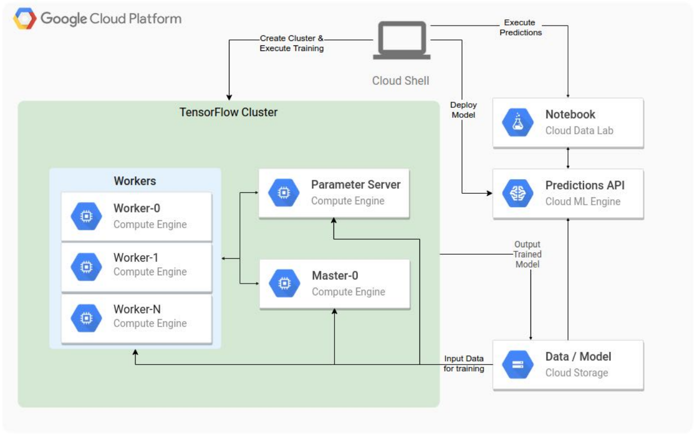


Source: https://www.morpheusdata.com/blog/2017-09-14-cloud-and-ai-a-work-in-progress-with-unlimited-upside





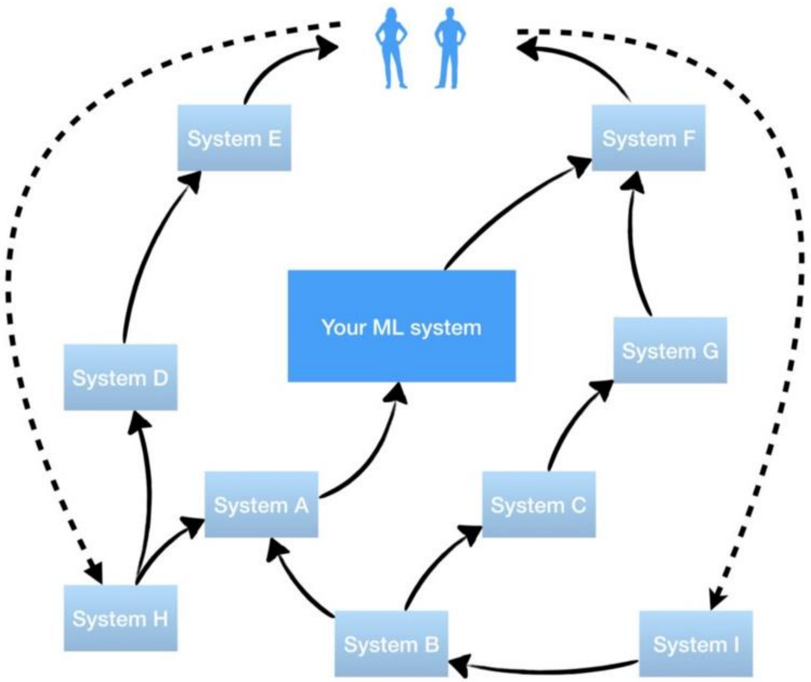
Source: https://azure.microsoft.com/es-es/services/machine-learning-studio

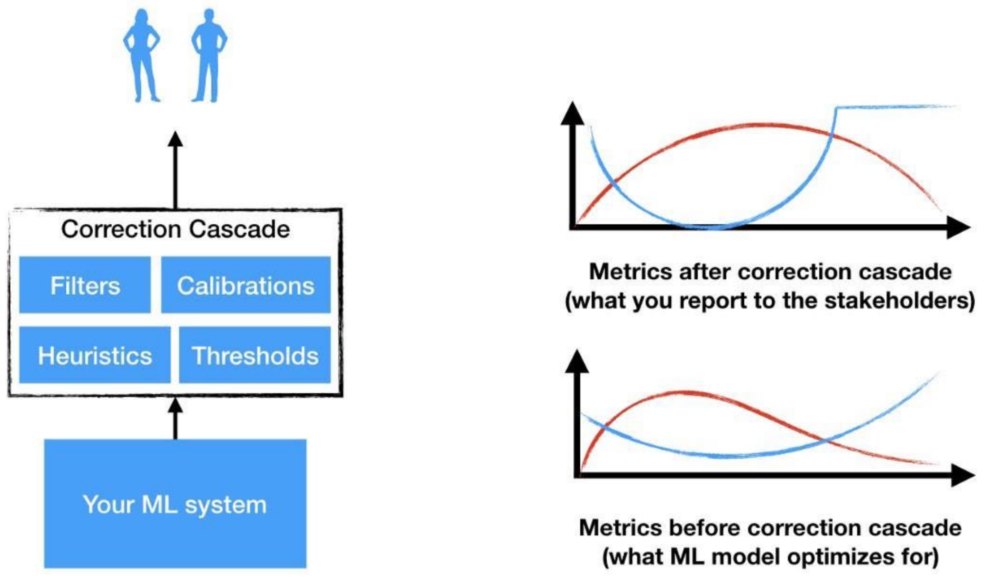


Source: https://cloud.google.com/automl/?hl=es-419

Technical debt in AI/ML functions [2, 4]

Garbage features





Feedback loops

Correction cascades

Source: https://towardsdatascience.com/technical-debt-in-machine-learning-8b0fae938657

Harmonization

Software & Systems Engineering

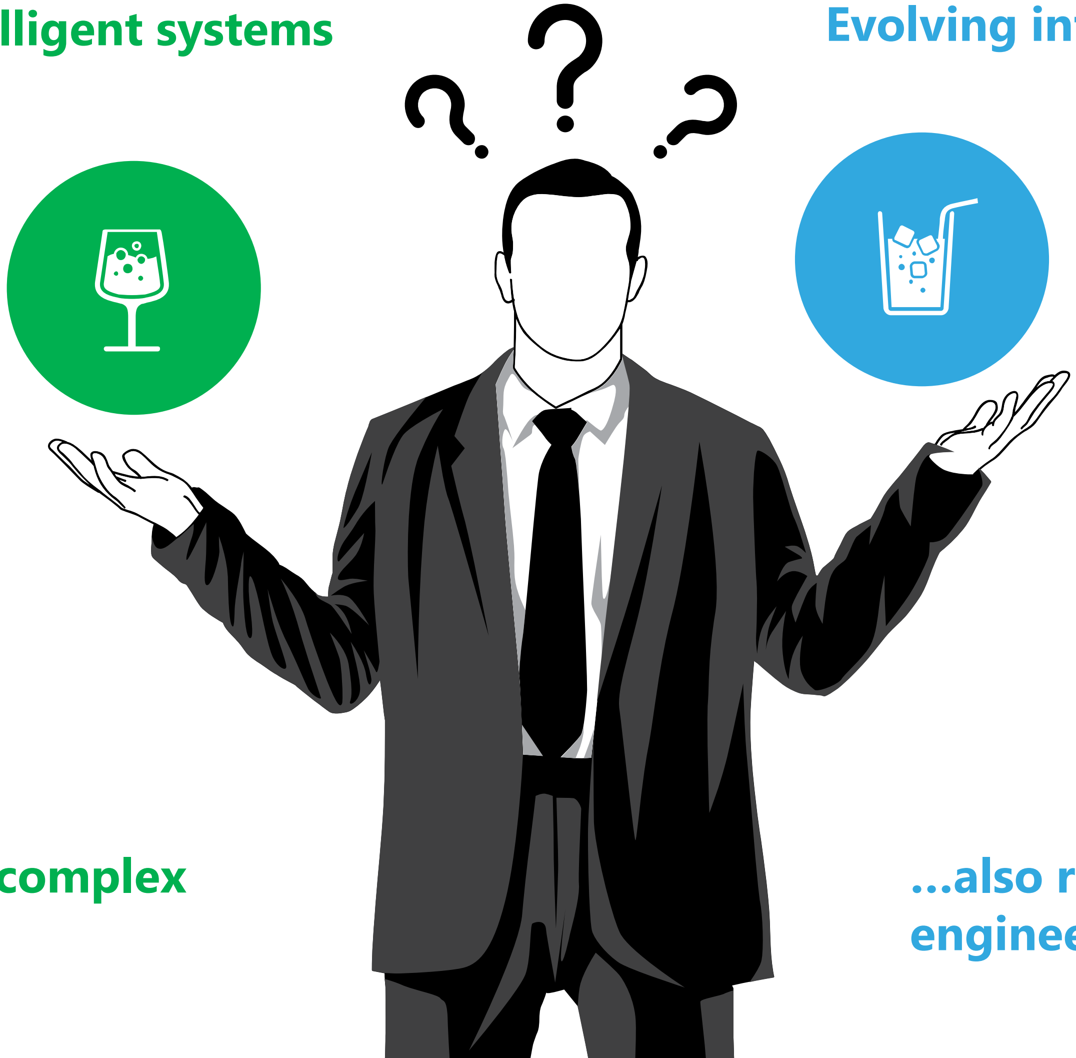
AI/ML lifecycle

Engineering (of→ ←for) AI/ML

Engineering of evolving intelligent systems

How to integrate the engineering process with the AI/ML lifecycle?

- ➕ Current trend
- ➕ Challenges ahead
- ➕ Opportunities ahead
- ➖ No clear view
- ➖ Lack of expertise: from deterministic to evolving systems



Evolving intelligent systems for engineering

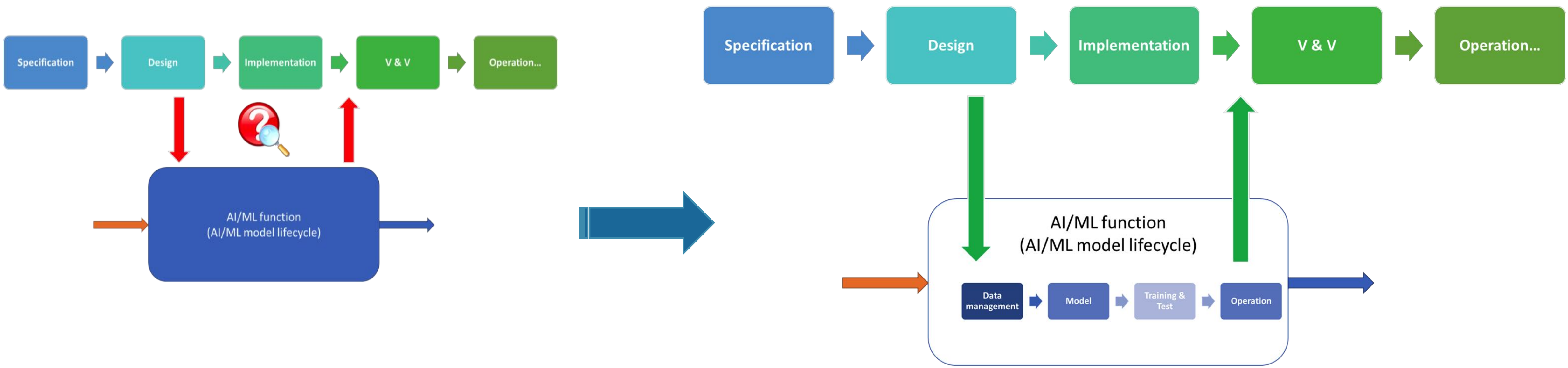
How to use intelligence to help engineering processes?

- ➕ Technology available
- ➖ Methods not ready
- ➖ Change resistance
- ➕ Room for improvement
- ➕ Cultural change and new mindset

Engineering more intelligent complex products/services...

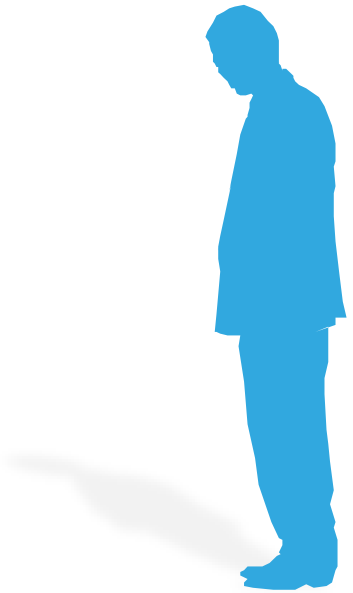
...also requires more intelligent engineering methods and tools.

Harmonization of the SE process and the AI/ML function



Paying the “hidden” technical debt

10 major challenges & coffee evaluation

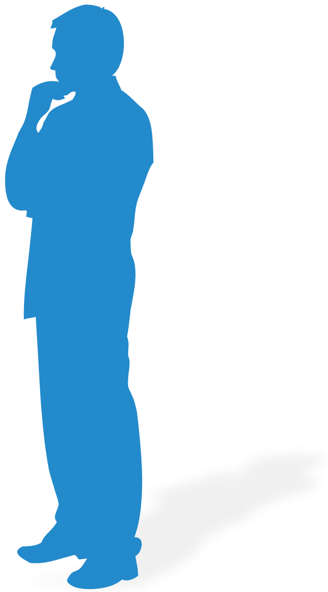


Status

How we do things now?

Concept

Can we define a challenge?



Opportunity

What to do to tackle the challenge?

Debate

Is it really a challenge?

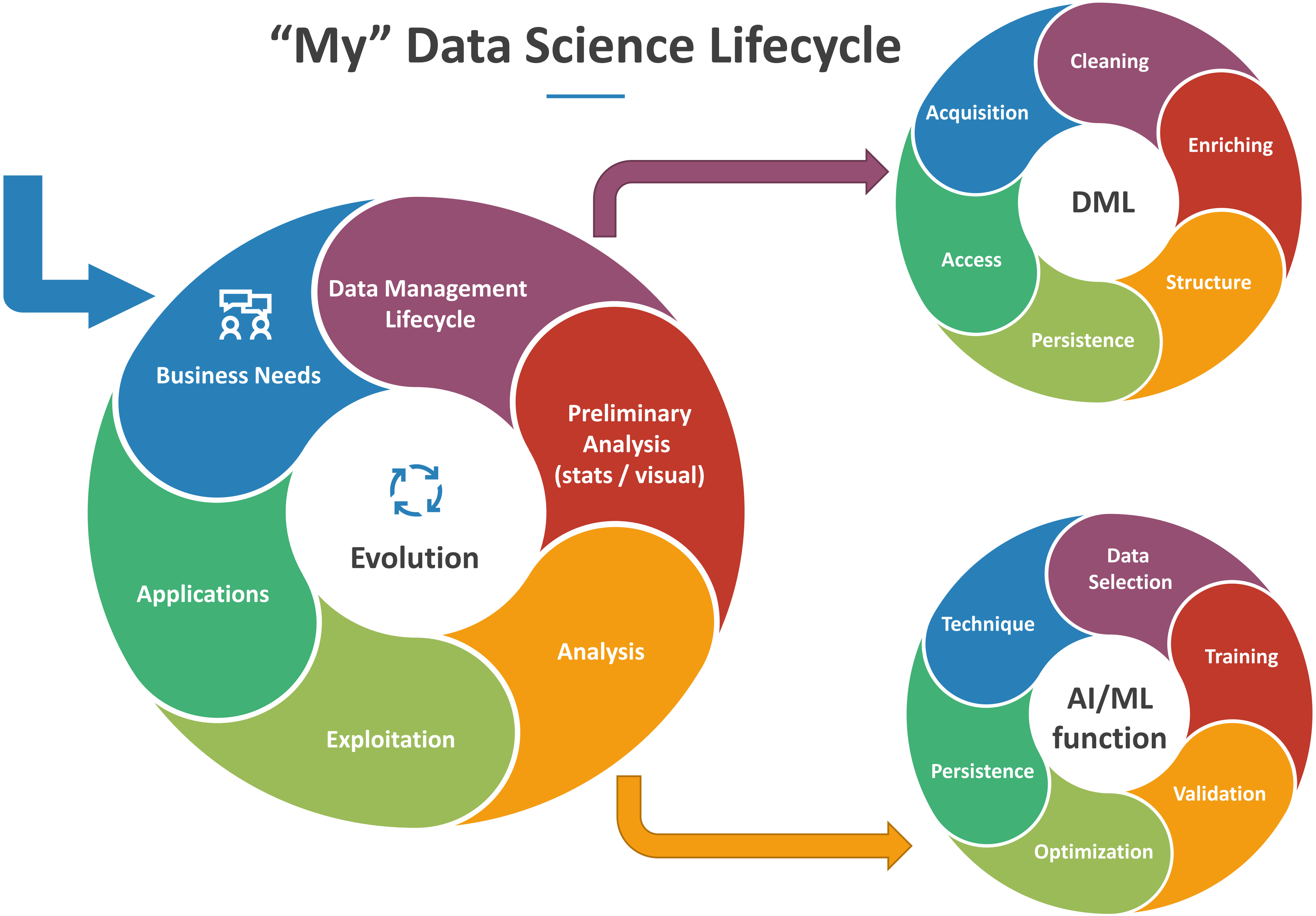
Is there an opportunity?

...and the necessary tea/coffee cups per hour

Challenge #1: to describe the needs and capabilities of the resources which are part of the AI/ML model lifecycle

Status	Concept	Opportunity	Debate
• AI/ML model lifecycle→several inter-related activities • Data management lifecycle (DML) not completely clear • Tangled environment of technology and tools • Lack of standardization	• Description of needs and capabilities of the AI/ML model lifecycle	• Catalogue of technology and tools. • Specify the DML stages. • Describe a DML using standards. • Orchestration of DML activities. • Access to functionalities as a service.	• DML has been already managed in the context of Big Data applications and Data Science.

"My" Data Science Lifecycle



Challenge #2: to integrate the AI/ML model lifecycle within the specification process of a system

Status

- Stages of the AI/ML model lifecycle: data, training, test, optimization and operation.
- Many models with different characteristics and applications.
- Performance metrics: precision, recall, accuracy, etc. depending on the type of model.

Concept

- Specification of requirements/models for AI/ML functions.

Opportunity

- New set of subsystems: AI/ML based.
- New set of metrics.
- New set of patterns to specify requirements/models about AI/ML functions.
- **Adaptation of the CCC in the context AI/ML functions.**
- Blocks for non-deterministic functions.
- **Consistency over time (evolvability).**
- Human factors.

Debate

- It mainly requires the extension of existing methods.

DSL for requirements (patterns, metrics, etc.)

Vocabulary

Techniques, metrics, types of problems to solve, etc.

Quality metrics

Consistency over time

Consistency between techniques and metrics.

Consistency between requirements and techniques.

Patterns

P1: The <AI_system> shall <action> <entity> with a <metric> of <value> <unit> under <weather_condition_type>.

Requirements

R1: "The entity recognition subsystem shall provide an explanation of at least 10 words about the recognized objects.

R2: "The entity recognition subsystem shall recognize a person with an accuracy of 90% under light snow."

Challenge #3: to integrate the AI/ML model lifecycle within the verification and validation (V&V) process of a system.

Status

- AI/ML already used for testing (data, test case generation, execution).
- Languages to specify (safety) test cases, e.g. Open Scenario (AVL).
- Digital twin environment.

Concept

- V&V of evolving systems.
  - **How to make deterministic a non-deterministic system?**
- Feedback loop:
  - In-lab V&V vs physical V&V

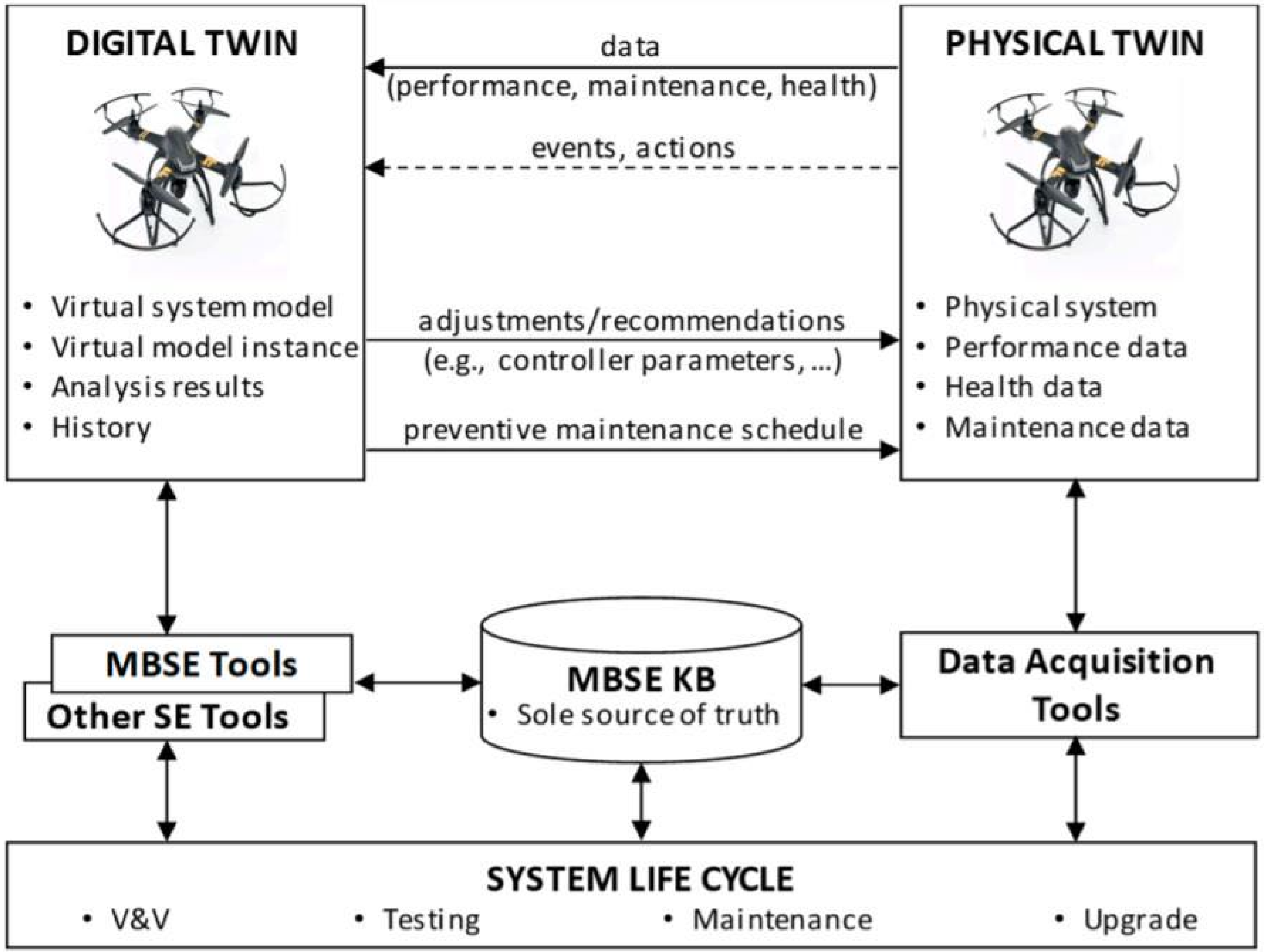
Opportunity

- Methods to connect a digital twin environment.
- Methods to deriving testing environments.
- Methods for re-verification, re-validation, re-certification, re-qualification.
  - **Virtual and Physical**
  - **Continuous RE-V&V**
- **Consistency over-time.**
  - **Simulation++++ (and its orchestration)**

Debate

- Connection between both sides of the Vee model.
  - W model.
- Legal framework.

Digital twin environment

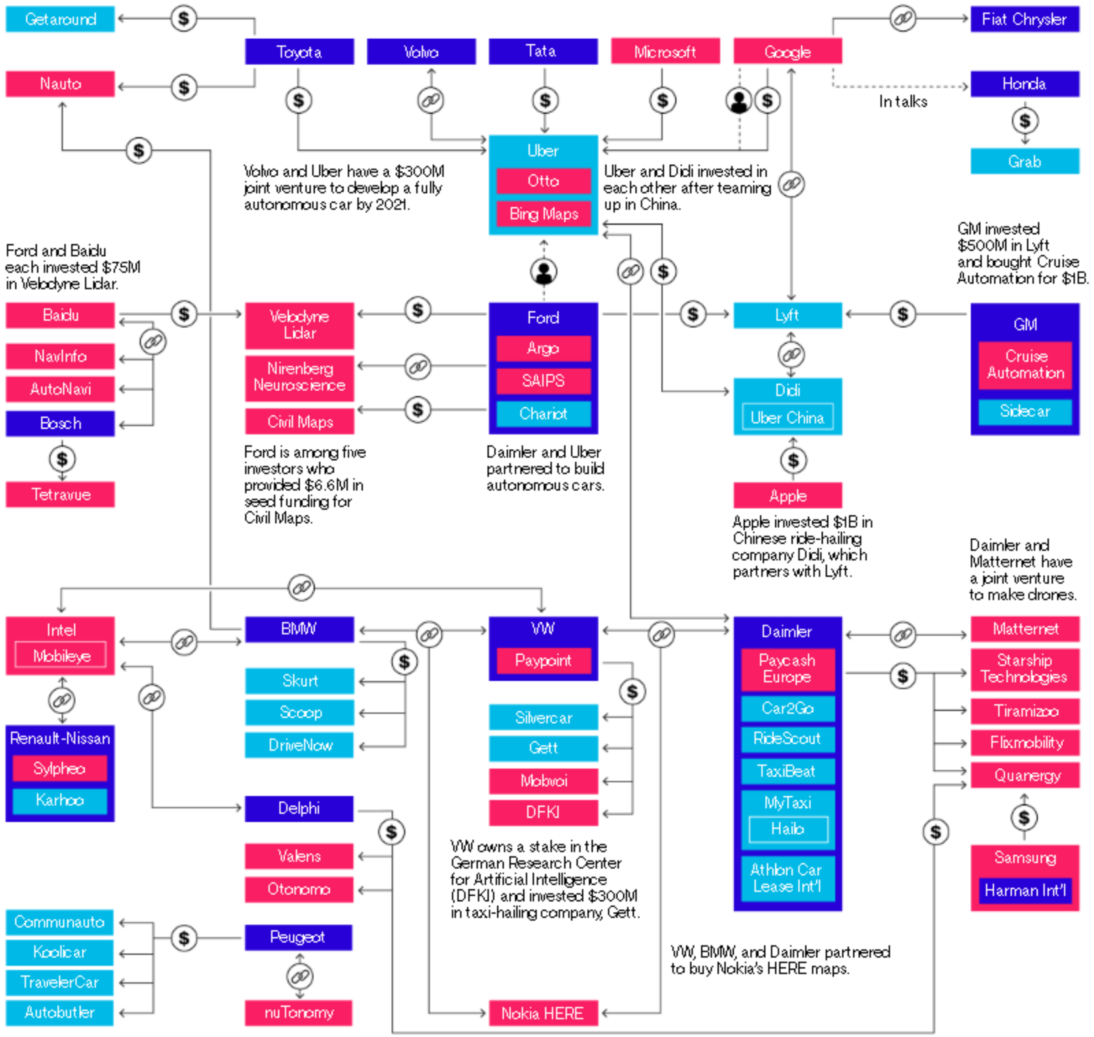


Source: https://www.mdpi.com/2079-8954/7/1/7/pdf

Challenge #4: to integrate the technology stack of the AI/ML model lifecycle within the system execution environment

Status	Concept	Opportunity	Debate
• Many technology providers	• Include a new technology stack: ◦ Hardware ◦ Software ◦ Communication system ◦ Computation system	• **Automatic generation of execution environments (DevOps approach).** • Artificial "Intelligence as a Service" (AIaaS) • "Machine Learning as a Service" (MLaaS) [5] • Share models? (competitive advantage)	• In the car industry, there are already strategic alliances between: ◦ Car manufacturers (OEM) ◦ Hardware providers ◦ AI/ML providers ◦ (Software) infrastructure providers ◦ Research centers

Technology and Car Companies



Source: Data compiled by Bloomberg
Additional work: John Lippert, Keith Naughton, Cedric Sam and Kevin Tynan

Source: https://www.bloomberg.com/graphics/2016-merging-tech-and-cars/

Challenge #5: to integrate the AI/ML model lifecycle within the configuration and change management processes

Status

- Many tools

Concept

- Configuration more relevant than ever→more software and more data dependencies

Opportunity

- Proper management of baselines and versions
- Round trip of data.
- Change impact analysis acquires a new dimension.
- **Artefact synch (consistency + traceability).**
- See Challenge #3
- …

Debate

- Existing techniques and tools are ready to manage changes and configuration in a digital twin environment.

Challenge #6: to ease the reuse of existing AI/ML models

Status

- Services

Concept

- Reuse of existing of AI/ML models can save time and costs.
- Increase reliability.

Opportunity

- Methods to check the reusability factor of an AI/ML model.
- Licensing and catalogue of datasets (market).
- Licensing and catalogue of AI/ML models (e.g. like Modelica libraries) (market).
- See Challenge #4. Services.

Debate

- The Big Data and Data Science communities have already passed over here.

Challenge #7: to standardize the integration of AI/ML model lifecycle within the engineering process

Status	Concept	Opportunity	Debate
• A new knowledge area comes to the Systems Engineering discipline.	• Avoid ad-hoc, non-controlled or vendor-lock-in integrations.	• Update of methods and standards. • Update of architectural frameworks. • Sustainability. • Bring new professionals to a SE team.	• It can be considered as another part of the software development process.

Framework for Highly Automated Vehicle Safety Validation

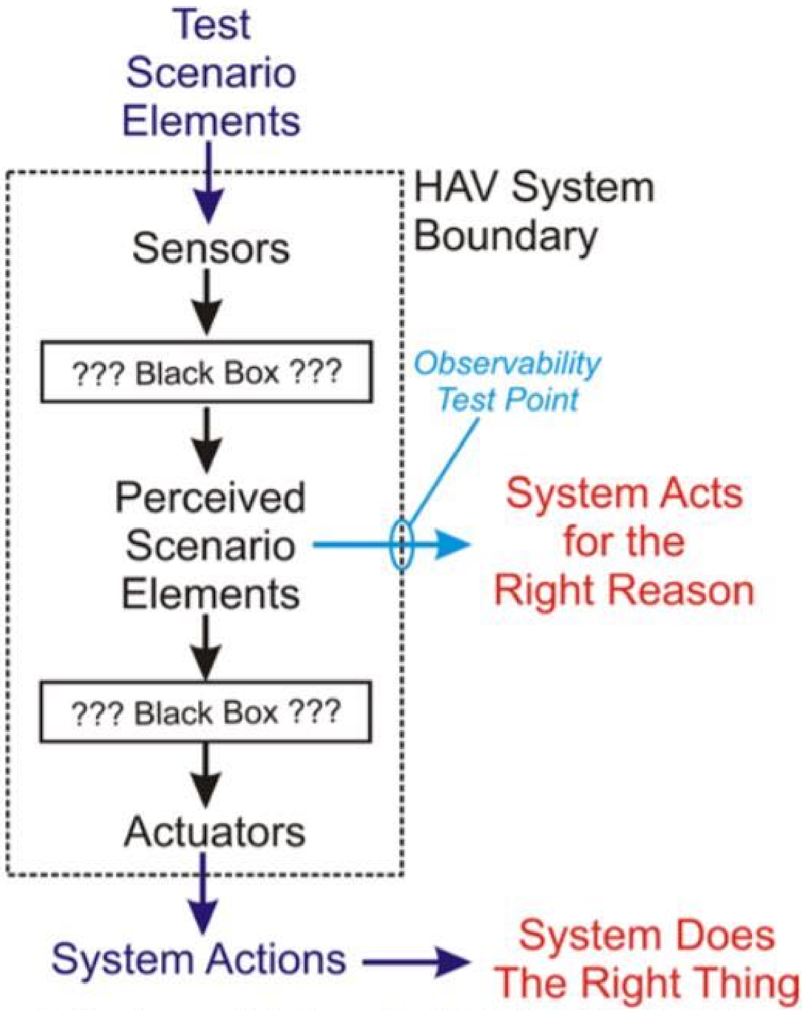
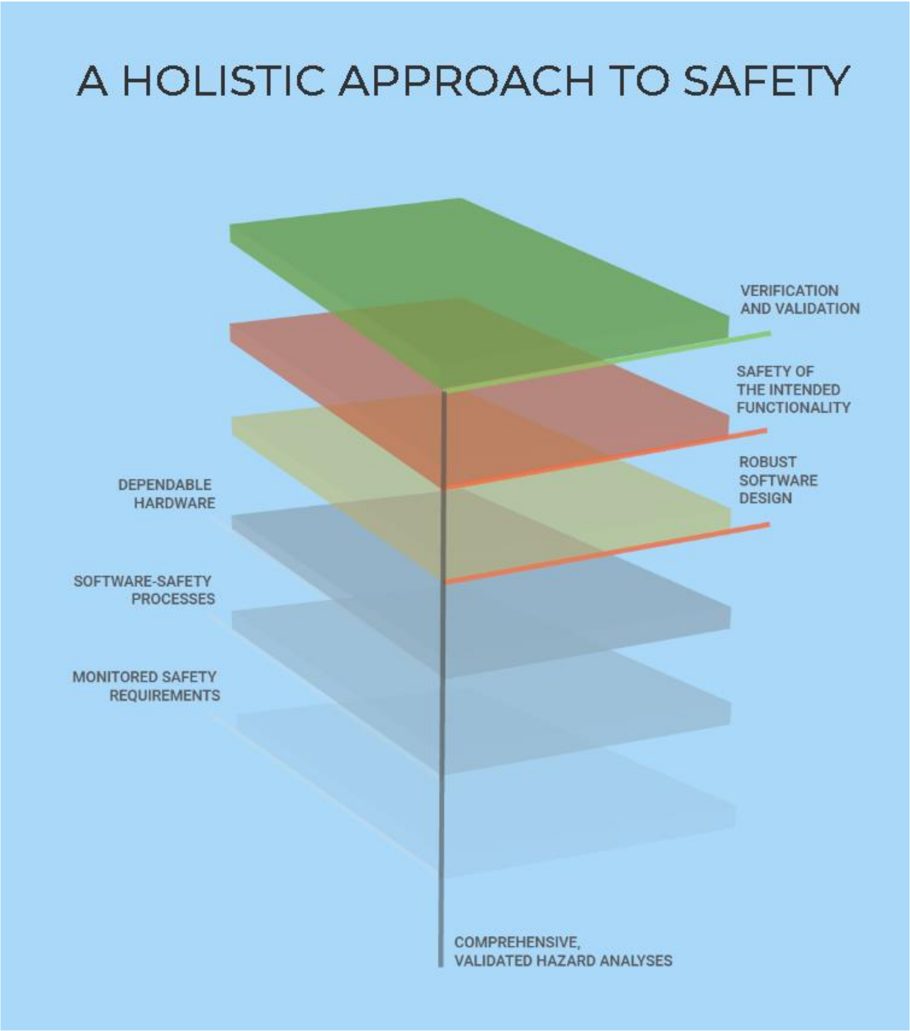


Figure 1. System validation should determine that the system does the right thing for the right reason.



Source: https://users.ece.cmu.edu/~koopman/pubs/koopman18_av_safety_validation.pdf

"First Comprehensive Autonomous Product Safety Standard (UL 4600)"
Source: https://edge-case-research.com/

Challenge #8: to educate a new wave of professionals to deal with AI/ML applying engineering methods

Status	Concept	Opportunity	Debate
• A new knowledge area comes to the Systems Engineering discipline.	• Equip people with the required skills to understand AI/ML functions.	• New courses and training methods. • New positions: AI/ML explainer, AI/ML engineer, etc.	• These are already covered as in any other discipline.

New roles and positions in AI

The Jobs That Artificial Intelligence Will Create (Continued from page 15)

REPRESENTATIVE ROLES CREATED BY AI

Accenture's global study of more than 1,000 large companies identified the emergence of three new categories of uniquely human jobs.

TRAINERS	**Customer-language tone and meaning trainer**	Teaches AI systems to look beyond the literal meaning of a communication by, for example, detecting sarcasm.
	Smart-machine interaction modeler	Models machine behavior after employee behavior so that, for example, an AI system can learn from an accountant's actions how to automatically match payments to invoices.
	Worldview trainer	Trains AI systems to develop a global perspective so that various cultural perspectives are considered when determining, for example, whether an algorithm is "fair."
EXPLAINERS	**Context designer**	Designs smart decisions based on business context, process task, and individual, professional, and cultural factors.
	Transparency analyst	Classifies the different types of opacity (and corresponding effects on the business) of the AI algorithms used and maintains an inventory of that information.
	AI usefulness strategist	Determines whether to deploy AI (versus traditional rules engines and scripts) for specific applications.
SUSTAINERS	**Automation ethicist**	Evaluates the noneconomic impact of smart machines, both the upside and downside.
	Automation economist	Evaluates the cost of poor machine performance.
	Machine relations manager	"Promotes" algorithms that perform well to greater scale in the business and "demotes" algorithms with poor performance.

Source: http://ilp.mit.edu/media/news_articles/smr/2017/58416.pdf

Challenge #9: to fulfill environmental requirements

Status	Concept	Opportunity	Debate
• A new knowledge area comes to the Systems Engineering discipline.	• Ensure the environment efficiency of the new systems (more than ever).	• Study strategies for optimization of AI/ML functions at all levels (hardware, software, communications, storage). • Reuse as a primitive.	• It is something that is already in the roadmap of any engineering product.

Challenge #10: to ensure the construction of ethical machines

Status	Concept	Opportunity	Debate
• MIT Moral Machine • Ethical guidelines of AI Systems from the EC.	• Ethics, a necessary non-functional requirement.	• Certification of ethicality.	• How to check ethics?

Summary

01 Data Management Lifecycle

02 Specification of AI/ML functions

03 Continuous V&V of evolving sys.

04 Technology stack integration

05 Configuration and change mgt.

06 Reuse of AI/ML models

07 Standards update

08 Skills, Training & Education

09 Environmental footprint

10 Ethics

11 ...

12 ...

Conclusions

Keypoints

Key points and next steps

1. Research on AI/ML and Systems Engineering is a key/active area.
2. Cyber-physical systems must be safer, cost-effective and environmentally friendly and…deliver on time (reacting to market needs).
3. Engineering processes must integrate a new discipline and adapt engineering methods to support the new technical capabilities.
4. Engineering of intelligent and evolving systems also requires "intelligent" tools.
5. Ethics is IMPORTANT, Safety a MUST.

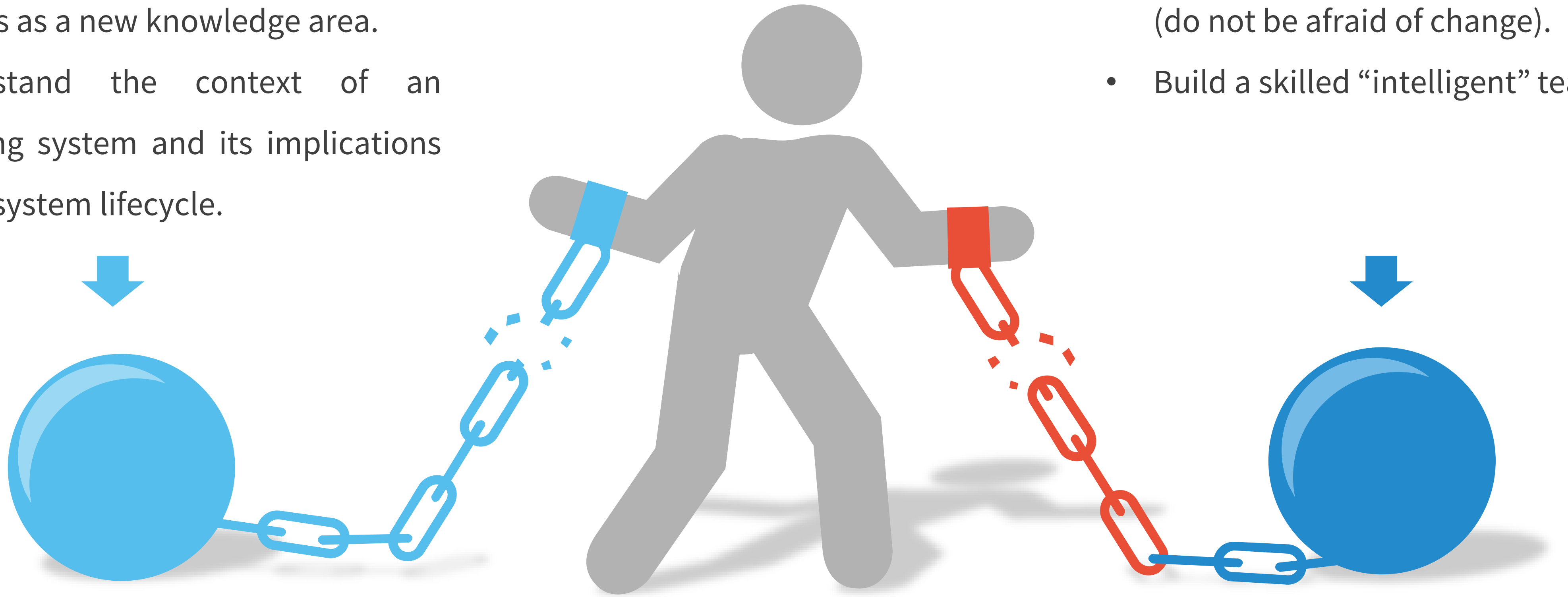
Do NOT be a "*technological*" slave

Build intelligent systems…

- Integrate the background of AI/ML experts as a new knowledge area.
- Understand the context of an evolving system and its implications in the system lifecycle.

…with intelligence

- Make use of existing and new tools (do not be afraid of change).
- Build a skilled "intelligent" team.



Take a seat and comment with us!

Thank you for your attention!

Jose María Álvarez-Rodríguez
Josemaria.alvarez@uc3m.es
@chema_ar

the REUSE company

uc3m Universidad Carlos III de Madrid

References

1. C. Ebert, “50 Years of Software Engineering: Progress and Perils,” IEEE Softw., vol. 35, no. 5, pp. 94–101, Sep. 2018.
2. F. Khomh, B. Adams, J. Cheng, M. Fokaefs, and G. Antoniol, “Software Engineering for Machine-Learning Applications: The Road Ahead,” IEEE Softw., vol. 35, no. 5, pp. 81–84, Sep. 2018.
3. D. Sculley et al., “Hidden Technical Debt in Machine Learning Systems,” in Proceedings of the 28th International Conference on Neural Information Processing Systems - Volume 2, Cambridge, MA, USA, 2015, pp. 2503–2511.
4. D. Sculley et al., “Machine Learning: The High Interest Credit Card of Technical Debt”. Google Research, 2014.
5. M. Ribeiro, K. Grolinger, and M. A. M. Capretz, “MLaaS: Machine Learning as a Service,” in 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 2015, pp. 896–902.