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

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
Are driverless cars Safer?

- Tired/distracted driving
- Slower responses
- Indecision
- Poor judgement
- Human error

360 degree view
To 200 yards, 24/7
Zero distractions

- Quicker and more accurate responses
- Vehicle to vehicle communication keeps other cars safe too

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.aptit.com/media/article/2018/01/07/the-autonomous-driving-platform-how-will-carsactually-drive-themselves
Critical factors

Human factors
Adoption of intelligent evolving systems

Safety & Security
Ethics

Conceptual & technological
From business needs/value to system capabilities
Software & Systems Engineering

Perspective

AI/ML lifecycle
Software Engineering

Software production automation
Model-Driven Engineering/Architecture
Software Product Lines etc.

Initial Focus
Methods and methodology to tackle the problem of software reliability

Agile methods & DevOps
Scrum, Kanban, BDD, TDD, etc.

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])*

• “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)

Technical Management Processes
- Project Planning Process (Clause 6.3.1)
- Project Assessment and Control Process (Clause 6.3.2)
- Decision 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
- Business 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)
- Implementation Process (Clause 6.4.7)

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)

Engineering (and corporate) environment

Source: http://www.ices.kth.se/upload/events/13/6440410965d41e6a7d1cafd0db4eeb0.pdf

Disconnected Silos

Artificial Intelligence

AI/ML SPRING & Fear
Any $x / x \in \{\text{domain, problem, place, one, sector, etc.}\}$

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

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

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

“My” Data Science Lifecycle

- Data Management Lifecycle
- Preliminary Analysis (stats / visual)
- Evolution
- Exploitation
- Analysis
- Applications (value)
- Business Needs

- Data Selection
- Technique
- Training
- Validation
- Optimization
- Persistence
- Structure
- Access
- Acquisition
- Cleaning
- Enriching
- DML

- Data Management Lifecycle (DML)
- AI/ML function

- Technique
- Persistence
- Validation
- Optimization
- Access
- Acquisition
- Cleaning
- Enriching
- DML
Frameworks/Platforms/… → AI/ML as a Service

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


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

Source: https://algorithmia.com/

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 \(\mapsto\) \(\Longleftrightarrow\) 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

<table>
<thead>
<tr>
<th>Status</th>
<th>Concept</th>
<th>Opportunity</th>
<th>Debate</th>
</tr>
</thead>
</table>
| • AI/ML model lifecycle→several inter-related activities | • 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. |
| • Data management lifecycle (DML) not completely clear | | | |
| • Tangled environment of technology and tools | | | |
| • Lack of standardization | | | |
“My” Data Science Lifecycle

Data Management Lifecycle

- Business Needs
- Applications
- Exploitation
- Analysis
- Preliminary Analysis (stats / visual)

Evolution

- Data Selection
- Technique
- Optimization
- Persistence
- Validation
- Training
- AI/ML function

DML

- Cleaning
- Access
- Structure
- Persistence
- Enriching
Challenge #2: to integrate the AI/ML model lifecycle within the specification process of a system

<table>
<thead>
<tr>
<th>Status</th>
<th>Concept</th>
<th>Opportunity</th>
<th>Debate</th>
</tr>
</thead>
</table>
| • 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. | • Specification of requirements/models for AI/ML functions. | • 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. | • It mainly requires the extension of existing methods. |
**DSL for requirements (patterns, metrics, etc.)**

**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.”

**Quality metrics**
- Consistency over time
- Consistency between techniques and metrics.
- Consistency between requirements and techniques.

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

DIGITAL TWIN
- Virtual system model
- Virtual model instance
- Analysis results
- History

data
(performance, maintenance, health)

events, actions

adjustments/recommendations
(e.g., controller parameters, ...)

preventive maintenance schedule

PHYSICAL TWIN
- Physical system
- Performance data
- Health data
- Maintenance data

MBSE Tools
Other SE Tools

MBSE KB
- Sole source of truth

Data Acquisition Tools

SYSTEM LIFE CYCLE
- V&V
- Testing
- Maintenance
- Upgrade

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

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many technology providers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include a new technology stack:</td>
</tr>
<tr>
<td>Hardware</td>
</tr>
<tr>
<td>Software</td>
</tr>
<tr>
<td>Communication system</td>
</tr>
<tr>
<td>Computation system</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatic generation of execution environments (DevOps approach).</strong></td>
</tr>
<tr>
<td>Artificial “Intelligence as a Service” (AlaaS)</td>
</tr>
<tr>
<td>“Machine Learning as a Service” (MLaaS) [5]</td>
</tr>
<tr>
<td>Share models? (competitive advantage)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Debate</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the car industry, there are already strategic alliances between:</td>
</tr>
<tr>
<td>Car manufacturers (OEM)</td>
</tr>
<tr>
<td>Hardware providers</td>
</tr>
<tr>
<td>AI/ML providers</td>
</tr>
<tr>
<td>(Software) infrastructure providers</td>
</tr>
<tr>
<td>Research centers</td>
</tr>
</tbody>
</table>
Challenge #5: to integrate the AI/ML model lifecycle within the configuration and change management processes

<table>
<thead>
<tr>
<th>Status</th>
<th>Concept</th>
<th>Opportunity</th>
<th>Debate</th>
</tr>
</thead>
</table>
| • Many tools | • Configuration more relevant than ever ➔ more software and more data dependencies | • Proper management of baselines and versions  
• Round trip of data.  
• Change impact analysis acquires a new dimension.  
• Artefact synch (consistency + traceability).  
• See Challenge #3  
• ... | • 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

<table>
<thead>
<tr>
<th>Status</th>
<th>Concept</th>
<th>Opportunity</th>
<th>Debate</th>
</tr>
</thead>
</table>
| • Services | • Reuse of existing AI/ML models can save time and costs.  
• Increase reliability. | • 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. | • 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**

<table>
<thead>
<tr>
<th>Status</th>
<th>Concept</th>
<th>Opportunity</th>
<th>Debate</th>
</tr>
</thead>
</table>
| • 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

<table>
<thead>
<tr>
<th>Status</th>
<th>Concept</th>
<th>Opportunity</th>
<th>Debate</th>
</tr>
</thead>
</table>
| • 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.

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

### Challenge #9: to fulfill environmental requirements

<table>
<thead>
<tr>
<th>Status</th>
<th>Concept</th>
<th>Opportunity</th>
<th>Debate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A new knowledge area comes to the Systems Engineering discipline.</td>
<td>• Ensure the environment efficiency of the new systems (more than ever).</td>
<td>• Study strategies for optimization of AI/ML functions at all levels (hardware, software, communications, storage).</td>
<td>• It is something that is already in the roadmap of any engineering product.</td>
</tr>
</tbody>
</table>
Challenge #10: to ensure the construction of ethical machines

<table>
<thead>
<tr>
<th>Status</th>
<th>Concept</th>
<th>Opportunity</th>
<th>Debate</th>
</tr>
</thead>
</table>
| • MIT Moral Machine  
  • Ethical guidelines of AI Systems from the EC. | • Ethics, a necessary non-functional requirement. | • Certification of ethicality. | • How to check ethics? |
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.
Thank you for your attention!

Take a seat and comment with us!

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


