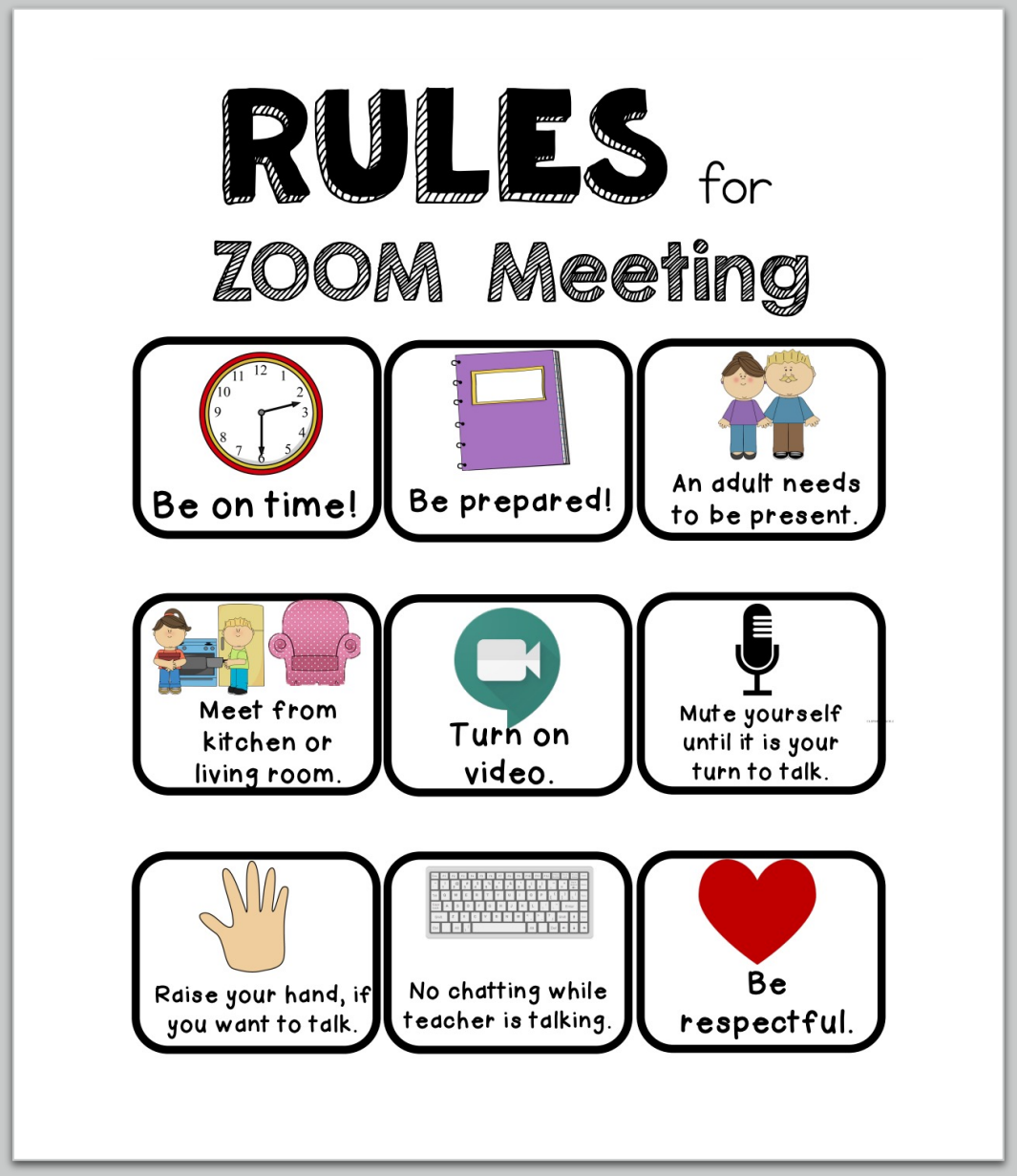
Course Overview and Introduction

SOEN 691: Engineering Ai-based Software Systems

Emad Shihab, Diego Elias Costa
Concordia University

First thing first…



https://www.teacherspayteachers.com/Product/Google-Hangout-and-Zoom-Meeting-Rules-for-Elementary-Students-5431502

Introductions

Engineering AI-based Software Systems

What is AI?

Britanica: "… the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings…"

Wikipedia: "… is intelligence demonstrated by machines, as opposed to natural intelligence displayed by animals including humans…"

IBM: "… is a field, which combines computer science and robust datasets, to enable problem-solving…"

Weak/narrow vs strong/general AI

What is AI?

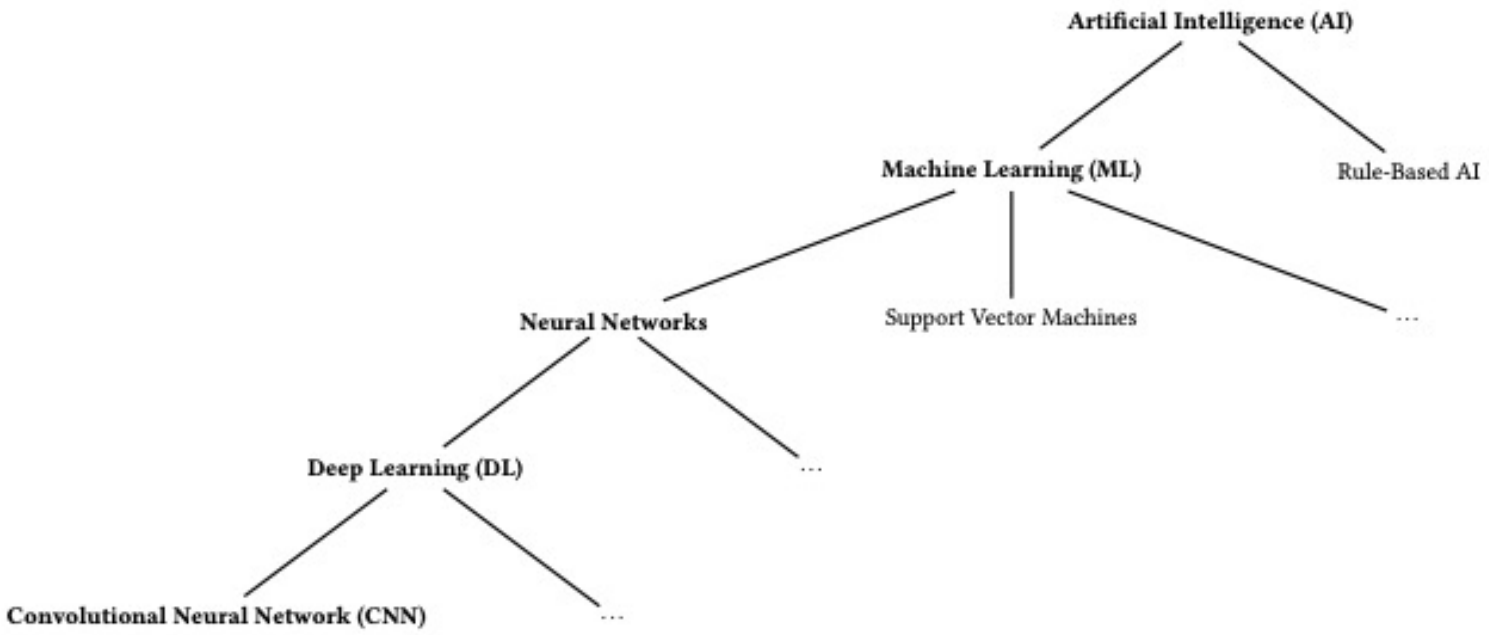


Fig. 17. Example taxonomic classification for paper [32].

What is an AI-based Software System?

- ….systems that learn by **analyzing their environment** and **taking actions** that aims to have **intelligent behavior**

- Systems that integrate AI capabilities
  - Statistical Learning
  - Machine Learning
  - Deep Learning

What is an AI-based Software System?

- AI-based Software Systems are systems that **include one or more AI component** (and other components)

- AI component: a part of the system that uses AI. Examples:
  - Embedded AI code
  - Using an AI library to implement an AI algo

- **Terms used**: AI technologies, AI-based systems, AI-infused systems, AI-enabled systems, AI/ML/DL software/system

The AI System "waves"

- According to DARPA, AI is in its third wave.

- First wave: (mostly) **rule-based** systems
- Second wave: **statistical learning** systems
- Third wave: **neural networks**, mostly DL

….at least AI and COVID have something in common…they both come in waves ☺

(Refresher)
Software Engineering Basics

Software Engineering

Software engineering is concerned with:

- **all aspects of software production** from the **early stages** of system **specification through maintenance** the system after it has gone into use.

Concerns all aspects of software production

- **Not just technical** process of development. Also project management and the development of tools, methods etc. to support software production.

SE Core Activities

- Requirement (elicitation, analysis, specification, etc.)
- Software design
- Software architecture
- Implementation & Integration
- Testing
- Maintenance
- ….

Fundamental SE Activities

Specification

Development

Validation

Evolution

Software Process Activities

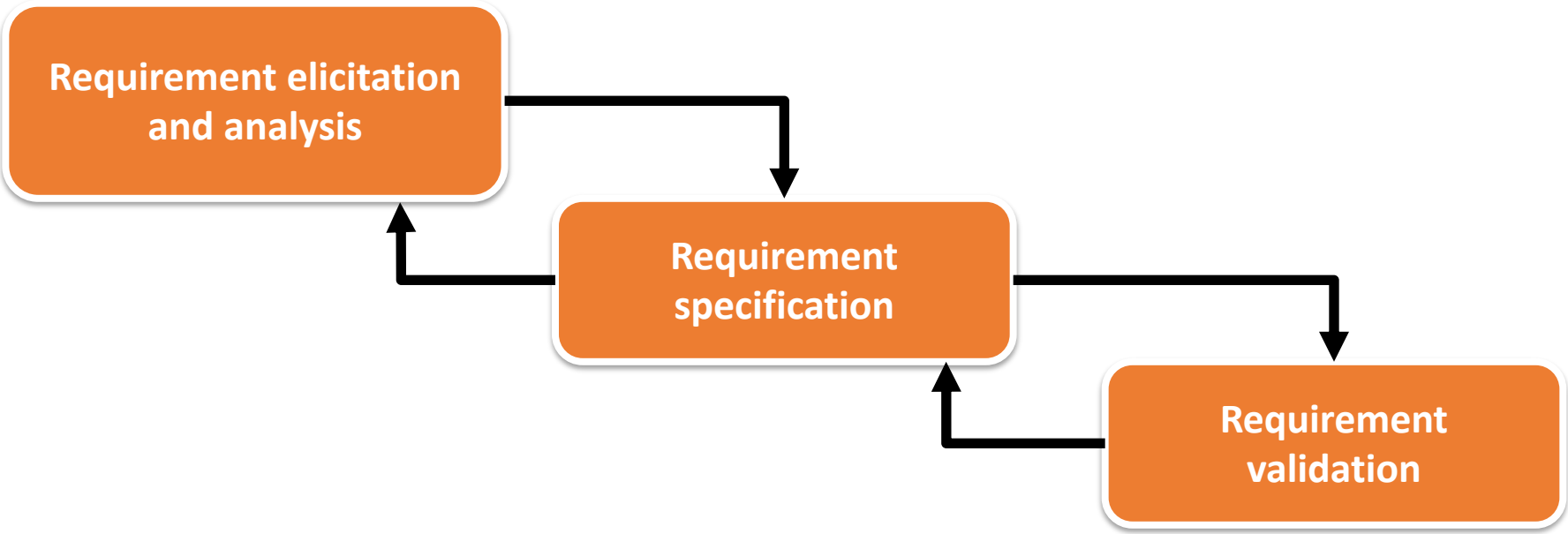
- **Software specification:** customers & engineers **define the software** that is to be produced and the **constraints on its operation**
- **Software development:** the software is **designed** and **programmed**
- **Software validation:** the software is **checked to ensure** that it is what the **customer requires**
- **Software evolution:** modifications done to meet **changing customer and market needs**

Phases and Models of Software Process

- There are many **different software process models**, but they all **share the same basic elements**

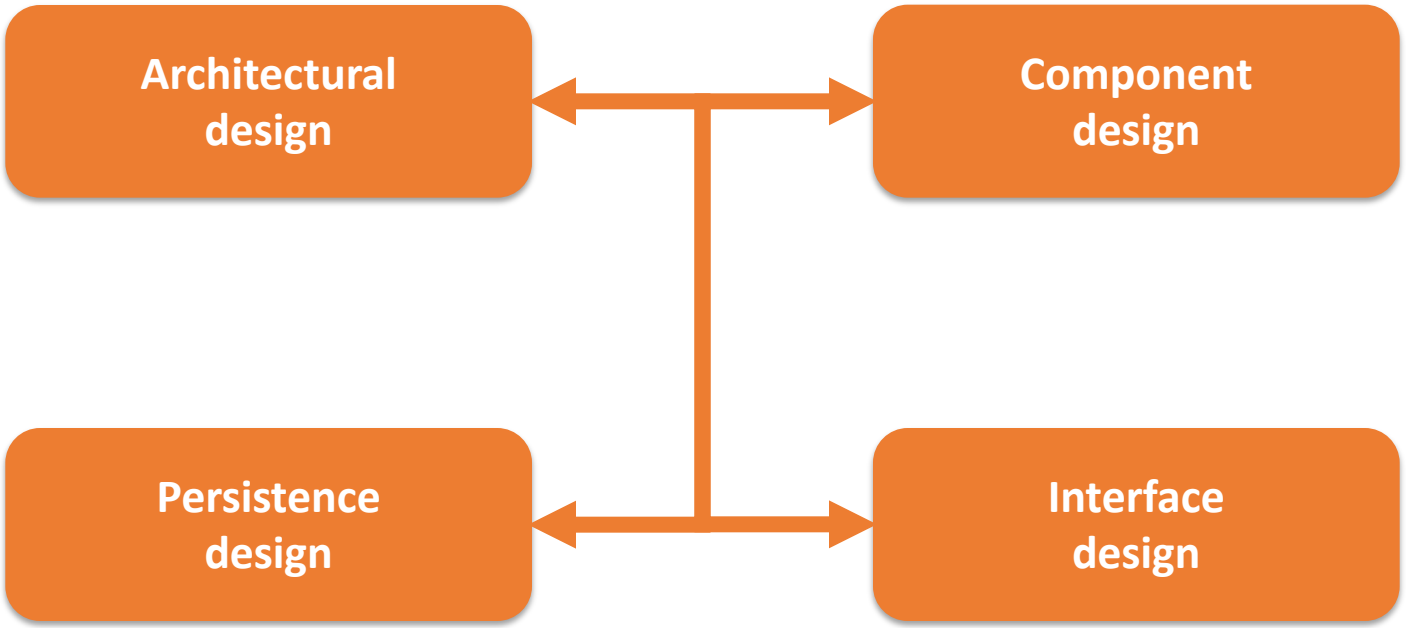
- The difference is in how these elements are organized.

Requirements/Specification

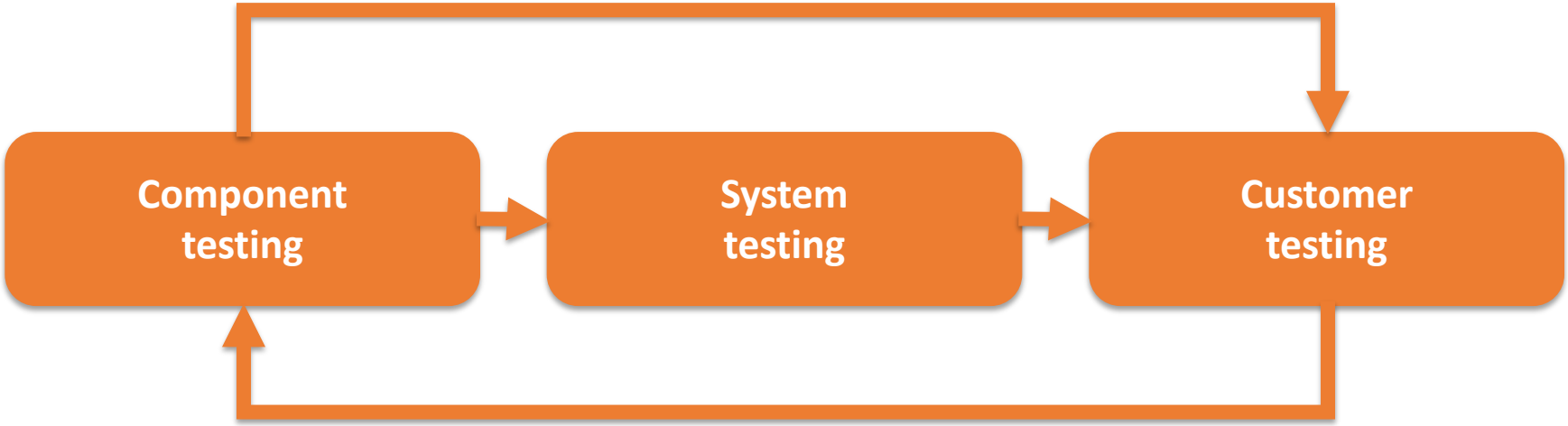


- User vs. System
- Functional vs Non-functional

Design


Architectural design
Component design
Persistence design
Interface design

Validation/Testing



Done by the person who writes the code

Often considered as part of testing

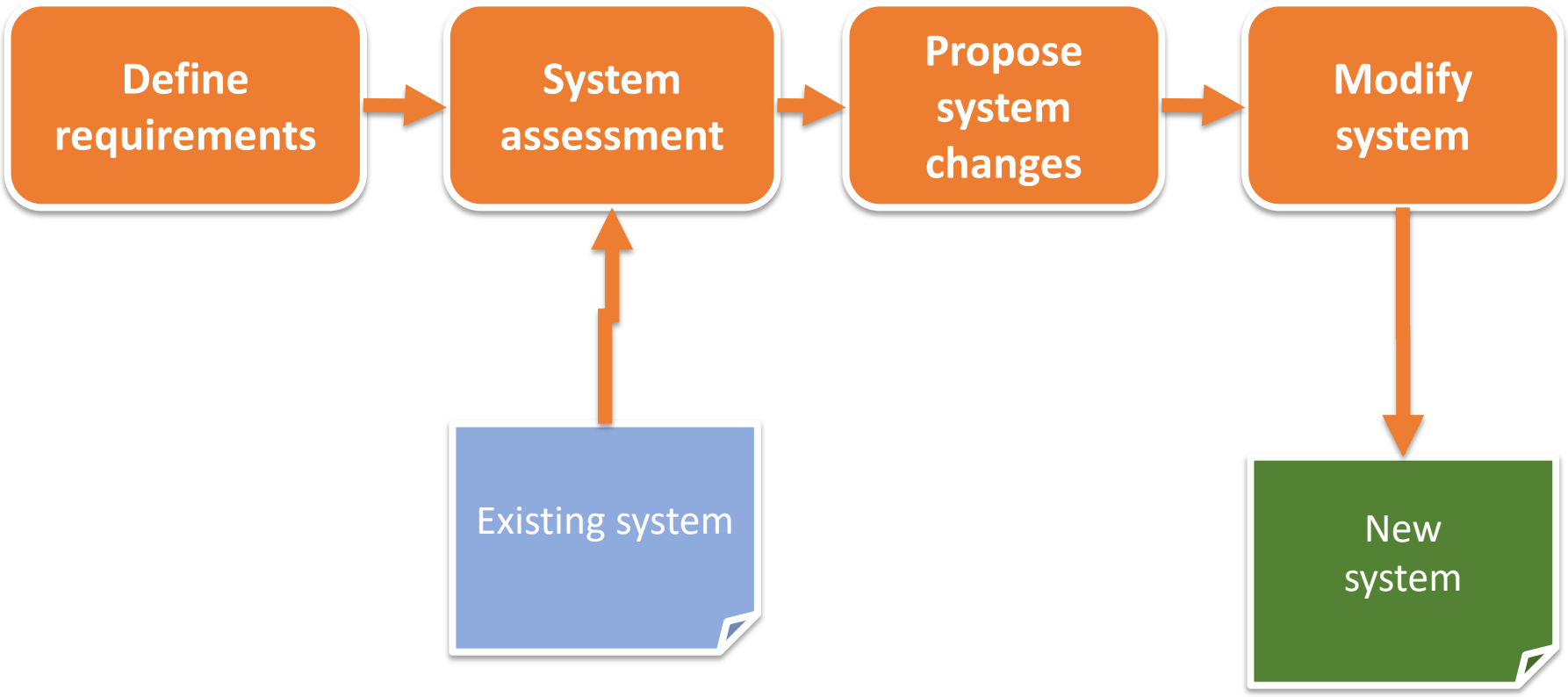
Feature and performance testing

Regression testing

Acceptance testing

Field testing

Evolution


Define requirements
System assessment
Propose system changes
Modify system
Existing system
New system


How the customer explained it

Software Engineering
+
AI-based Software Systems

So… What's the Big Deal?

- In AI-based systems, **rules and system behavior** are inferred from training data (amongst others), rather than program logic and code only

- Moving parts include:
  - Large datasets that play a critical role in system behavior
  - Algorithmic performance
  - Infrastructure
  - Ethics and equity
  - ….

- Because of this, we need SE4AI!

Current State of SE4AI

Software Engineering for AI-Based Systems: A Survey

SILVERIO MARTÍNEZ-FERNÁNDEZ, Universitat Politècnica de Catalunya - BarcelonaTech, Spain
JUSTUS BOGNER, University of Stuttgart, Institute of Software Engineering, Germany
XAVIER FRANCH, Universitat Politècnica de Catalunya - BarcelonaTech, Spain
MARC ORIOL, Universitat Politècnica de Catalunya - BarcelonaTech, Spain
JULIEN SIEBERT, Fraunhofer Institute for Experimental Software Engineering IESE, Germany
ADAM TRENDOWICZ, Fraunhofer Institute for Experimental Software Engineering IESE, Germany
ANNA MARIA VOLLMER, Fraunhofer Institute for Experimental Software Engineering IESE, Germany
STEFAN WAGNER, University of Stuttgart, Institute of Software Engineering, Germany

AI-based systems are software systems with functionalities enabled by at least one AI component (e.g., for image-, speech-recognition, and autonomous driving). AI-based systems are becoming pervasive in society due to advances in AI. However, there is limited synthesized knowledge on Software Engineering (SE) approaches for building, operating, and maintaining AI-based systems. To collect and analyze state-of-the-art knowledge about SE for AI-based systems, we conducted a systematic mapping study. We considered 248 studies published between January 2010 and March 2020. SE for AI-based systems is an emerging research area, where more than 2/3 of the studies have been published since 2018. The most studied properties of AI-based systems are dependability and safety. We identified multiple SE approaches for AI-based systems, which we classified according to the SWEBOK areas. Studies related to software testing and software quality are very prevalent, while areas like software maintenance seem neglected. Data-related issues are the most recurrent challenges. Our results are valuable for: researchers, to quickly understand the state-of-the-art and learn which topics need more research; practitioners, to learn about the approaches and challenges that SE entails for AI-based systems; and, educators, to bridge the gap among SE and AI in their curricula.

CCS Concepts: • **Software and its engineering → Software creation and management**; • **Computing methodologies → Machine learning**;

Additional Key Words and Phrases: software engineering, artificial intelligence, AI-based systems, systematic mapping study

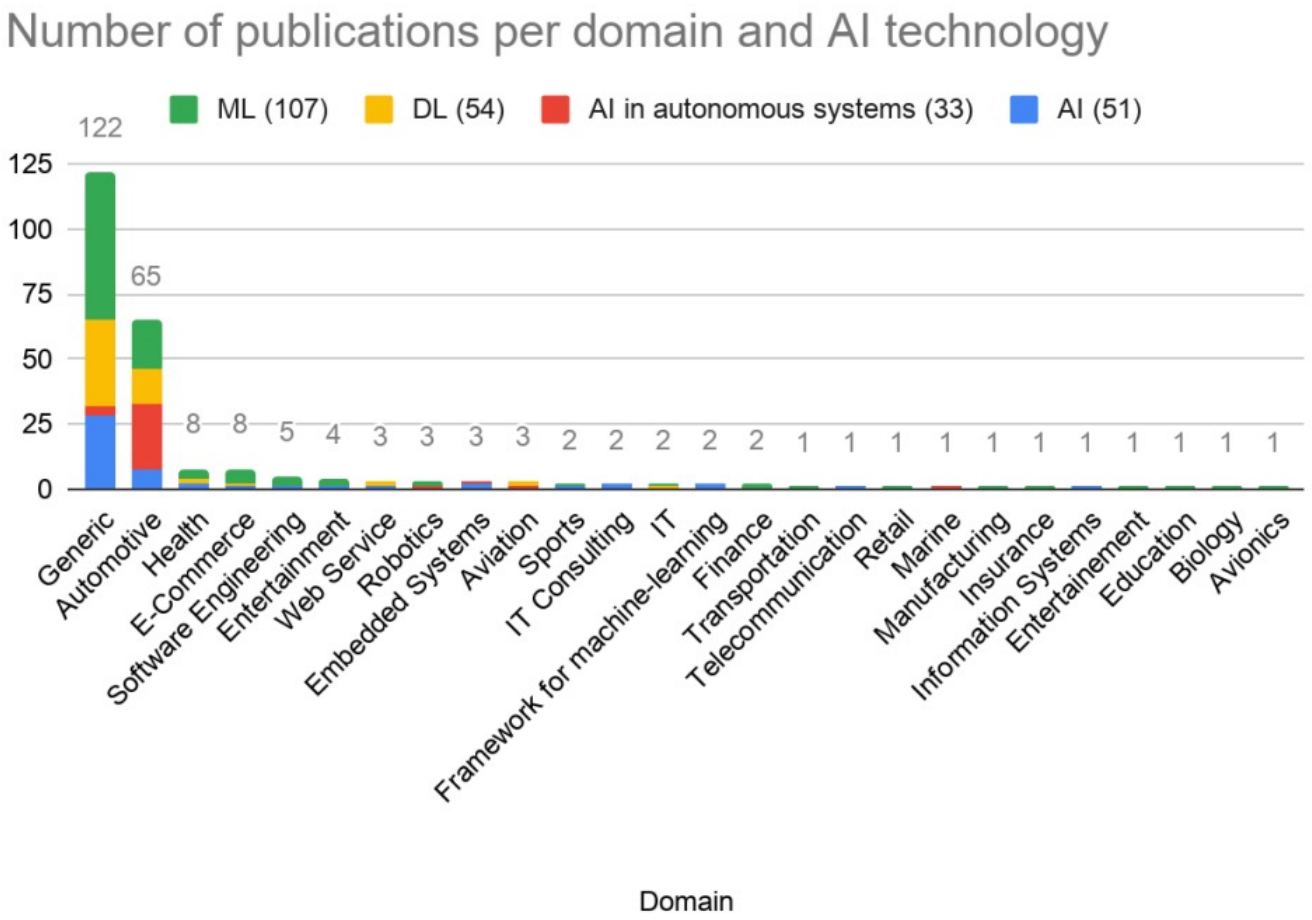
1 INTRODUCTION

In the last decade, increased computer processing power, larger datasets, and better algorithms have enabled advances in Artificial Intelligence (AI) [11]. Indeed, AI has evolved towards a new wave, which Deng calls "the rising wave of Deep Learning" (DL) [46][1]. DL has become feasible, leading to Machine Learning (ML) becoming integral to many widely used software services and applications [46]. For instance, AI has brought a number of important applications, such as image- and speech-recognition and autonomous, vehicle navigation, to near-human levels of performance [11].

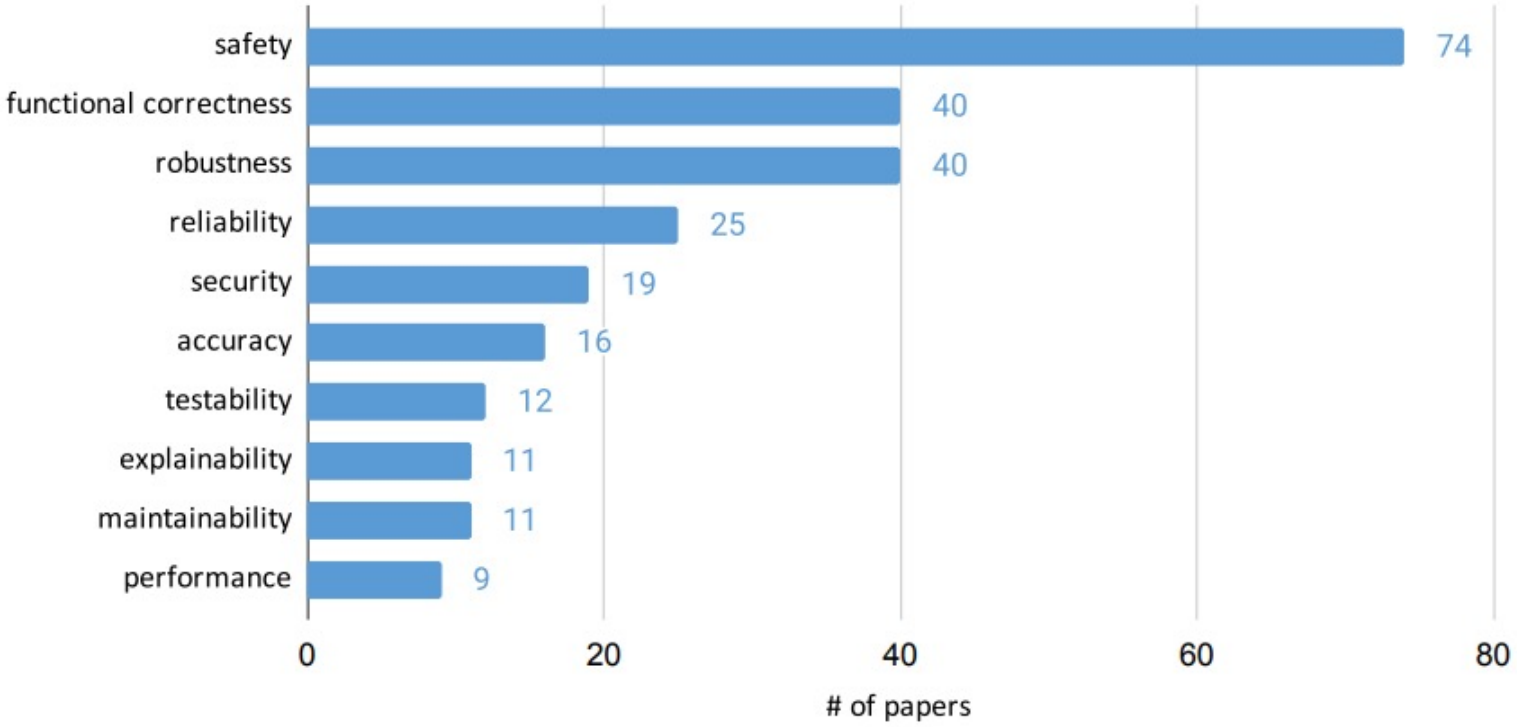
The new wave of AI has hit the software industry with the proliferation of AI-based systems integrating AI capabilities based on advances in ML and DL [6, 24]. AI-based systems are software systems which include AI components. These systems learn by analyzing their environment and taking actions, aiming at having an intelligent behaviour. As defined by the expert group on AI of the European Commission, "AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems)

[1] https://en.wikipedia.org/wiki/History_of_artificial_intelligence#Deep_learning,_big_data_and_artificial_general_intelligence:_2011-present

Domains of AI-based Software Systems



Quality goals of AI-based Software Systems



Less studied concepts: **usability, trustworthiness, understandability, explainability and transparency**

Software Engineering + AI

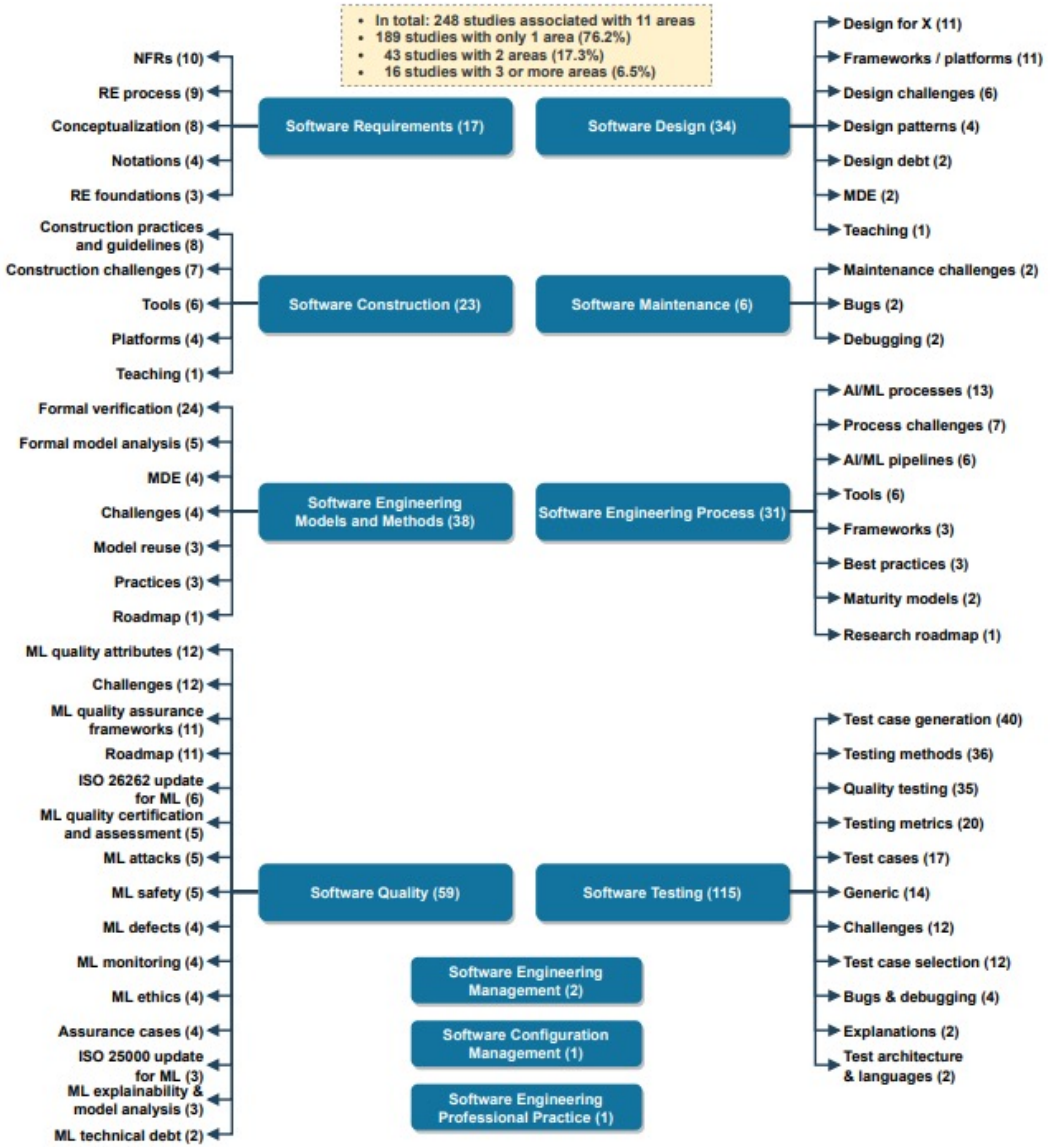


Fig. 18. The 248 primary studies classified into 11 SWEBOK Knowledge Areas based on their SE contributions for AI-based systems.

Requirements in AI-based Software Systems

- Considerations that need to be addressed include:
  - Detection of data anomalies
  - Algorithmic discrimination
  - Requirements for explainable and safe AI
  - Specification of requirements in AI-based systems

Design in AI-based Software Systems

- Considerations that need to be addressed include:
  - Specific design strategies/patterns for AI systems in safety critical domains (e.g., autonomous vehicles)
  - Reliability, user experience, fairness, etc.
  - Frameworks and platforms for ML applications (e.g., to address recurrent business analytics problems with ML)

Testing in AI-based Software Systems

- Considerations that need to be addressed include:
  - Testing for explainability
  - Testing for safety, robustness, security, fairness
  - Automated test generation to improve coverage for different inputs/data
  - **Test quality metrics**: coverage (majority), diversity, importance, suspiciousness, probability, disagreement

Process and Maintenance in AI-based Software Systems

- Considerations that need to be addressed include:
  - Data (cleaning, pre-processing, versioning)
  - Modeling: choosing the best vs. combining, etc.
  - Deployment: computation performance, dealing with real-life inputs, integration within a larger system
- Evolution:
  - Auto labelling data
  - Managing multiple models (e.g., to incorporate new tech)
  - A/B testing
  - Monitoring & logging: to deal with inaccuracies and auditing

Open Challenges

Requirements in AI-based Software Systems

- **Better understanding of NFR**
- Elicitation of **user centered features** such as explainability are needed. Creating fair and equitable systems may need information about users such as gender and ethnicity
- Dealing with undeclared users (and the relation to ethics)
- Dealing with not 100% accurate systems
- Specifying **concepts used by ML techniques** (may require domain knowledge)
- **Validation** can be difficult due to the uncertainty in the results produced

Design in AI-based Software Systems

- The difference between **critical and non-critical systems** needs to be taken into considerations
- Incorporating AI components in larger systems (or systems-of-systems)
- Exposure to **AI systems' metadata**
- **Dependency on external frameworks, APIs, implementations** (sometimes in different programming languages)

Testing in AI-based Software Systems

- Data and models cannot be deterministically specified
- **Scalability** of testing can be difficult based on the data or models used (to emulate realistic scenarios)
- **Traceability** is difficult in large pipelines
- Having representative **test quality metrics**
- Having a **ground truth** can be **difficult or impossible**

Process and Maintenance in AI-based Software Systems

- Need highly iterative processes since **models can evolve quickly**
- How to **incorporate and maintain the right ML technologies**
- Having **proper and accurate logging** mechanisms to monitor, correct and evelove AI-based software systems

Deployment of AI-based Software Systems

- Ensuring **continuous trust** in the deployed systems
- Dealing with **unpredictable behavior**
- **Runtime and updates** need to be done in an acceptable timeline
- **Configuration management** to ensure behavior in a **real context**

SOEN 691: Engineering AI-based Software Systems

The course

- **Familiarize** you with the **challenges and concepts** of engineering AI-based software systems
- Expose you to **common techniques used to engineer** AI-based software systems
- Get you to think **critically** about research in the area of AI-based software systems

Course Format

- Class:
  - Mondays 9:00 AM to 11:30 AM on Zoom (for now)
  - We will take a 5 minute break midway

- Classes are expected to be open in nature and include lively discussions of the materials being presented

Course Organization

- **Part 1**: Build necessary knowledge in the area of AI-based software systems

- **Part 2**: Study state-of-the-art in the engineering of AI-based software systems area
- Read and critique emerging research in the area

- **Contribute** to the state-of-the-art in AI-based software systems

Course Outcomes

- **Part 1**: Be able to understand and recognize the **terminology and basic building blocks** of AI-based software systems

- **Part 2**: Understand the main **components, challenges and techniques** pertaining to the engineering of AI-based software systems

- **Improve the state-of-the-art** and communicate these findings so others can benefit

Reference Materials

- We will mostly use a number of research papers that will be posted on the course website
- Course slides
- Reference text:
  - Building Intelligent Systems: A Guide to Machine Learning Engineering, 2018. Geoff Hulten

Tentative Outline

Week	Date	Topic
1	Jan. 10	Introduction & overview
2	Jan. 17	AI for Software Engineers
3	Jan. 24	Quality of AI-based systems
4	Jan.31	Software requirements for AI-based systems
5	Feb. 7	Software architectures of AI-based systems
6	Feb. 14	Data validation and management
7	Feb. 21	**Project updates (student presentations)**
8	Mar. 7	Model selection and experimentation
9	Mar. 14	Deployment and testing
10	Mar. 21	Continuous delivery
11	Mar. 28	Interpreting, explaining, monitoring models, and MLOps (special topics)
12	Apr. 4	**Quiz**
13	Apr. 11	**Project presentations (student presentations)**

Course Evaluation

Class participation	10%
Paper critiques & activities	20%
Project proposal	10%
Research project	40%
Quizzes and exams	20%

You must pass the quizzes and the course project to pass the course

Course Expectations

- Attend lectures and participate in discussions (Yes, we expect you to talk!)
- Do the assigned readings and assignments!
- Bring your ideas and concerns to class

Asking Questions and Communication

- Ask me or Diego by email
- Schedule a Zoom meeting if needed
  - We will stay for 15 minutes after class (most classes)
- Ask in class
- Discuss with your classmates

Paper Critiques

- Most weeks, you will need to submit:
  - A summary of 1 of the papers (< half-page)
  - A critique of the other paper (1 page). The critique should include a summary, at least 3 weak points and at least 3 strong points

- Critiques and summaries are due at **noon (12 PM)** on Fridays **the week before class**

Course Project

- A large portion of the course mark is based on the course project
- Course projects are to be carried out in groups (4-5)
- You are free to do your project on any course-related topic, with instructor's approval

Course Project

- You will hand in a project proposal in week 6 (3 pages, IEEE format)
- You will present a progress update in week 7
- You will present the project in week 13 and hand in the final report at the end of week 13 (10 pages, IEEE format)

Lateness Policy for All Course Deliverables

NO LATE DELIVERABLES!

NO LATE DELIVERABLES!

Academic Integrity and Cheating

- Cheating, plagiarism and other forms of academic fraud are taken very seriously by the University, the Faculty, and the teaching staff
- Examples:
  - Submitting the work of another person as your original work
  - Incorporating others work in your work and not referencing it
  - It is permitted and encouraged to discuss with your peers but **NOT** permitted to copy their solutions. Both parties will be penalized.

Homework

- Have a look at the topic list on the course's web page
  - 1. Submit a list of 3 topics areas that you would like to do your project on
    - For each topic, give a list of 3 relevant papers
  - 2. Submit a list of 4-6 names of people you want to do your project with. The names need to be from at least 2 other Universities.
  - Due Monday, Jan. 14 at 9 AM on the course webpage
  - **Make sure to put your name, student id and date are on all pages. Submit as a PDF file.**

References

- Textbook
  - Software Engineering by Ian Sommerville (10th edition)
  - Available at Concordia Library
  - https://www.darpa.mil/news-events/2018-07-20a
  - https://www.ibm.com/cloud/learn/what-is-artificial-intelligence
  - https://en.wikipedia.org/wiki/Artificial_intelligence
  - https://www.britannica.com/technology/artificial-intelligence