mtc
Manufacturing
Technology Centre

Together we impact society.
The **RIGHT** Way

Utilising Externally Hosted AI / Generative AI Services in Manufacturing the Role of AI Governance

Dr. Mostafizur Rahman, Chief Technologist- Artificial Intelligence
The Manufacturing Technology Centre
Coventry, UK
www.the-mtc.org

09-11-2023

Applications of LLMs & Risks

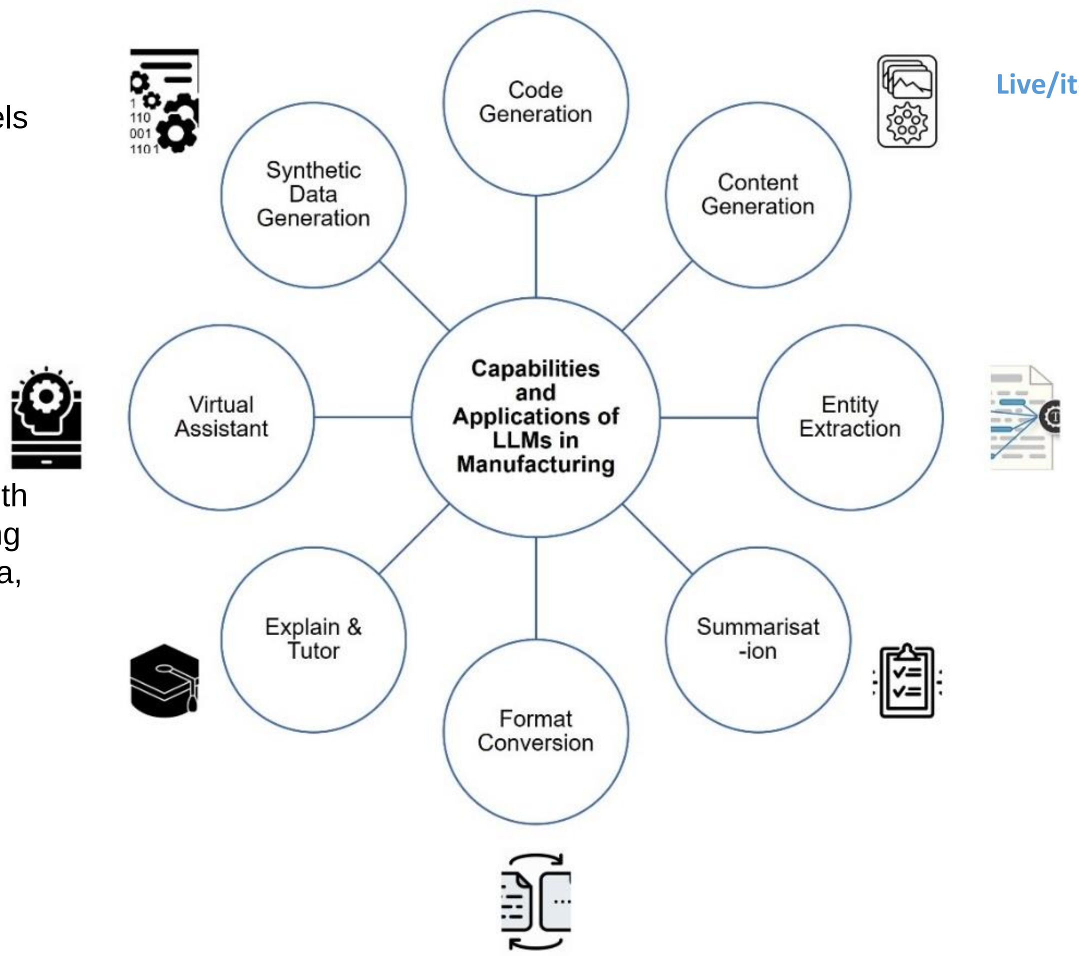
Together we impact society.
The **RIGHT** Way

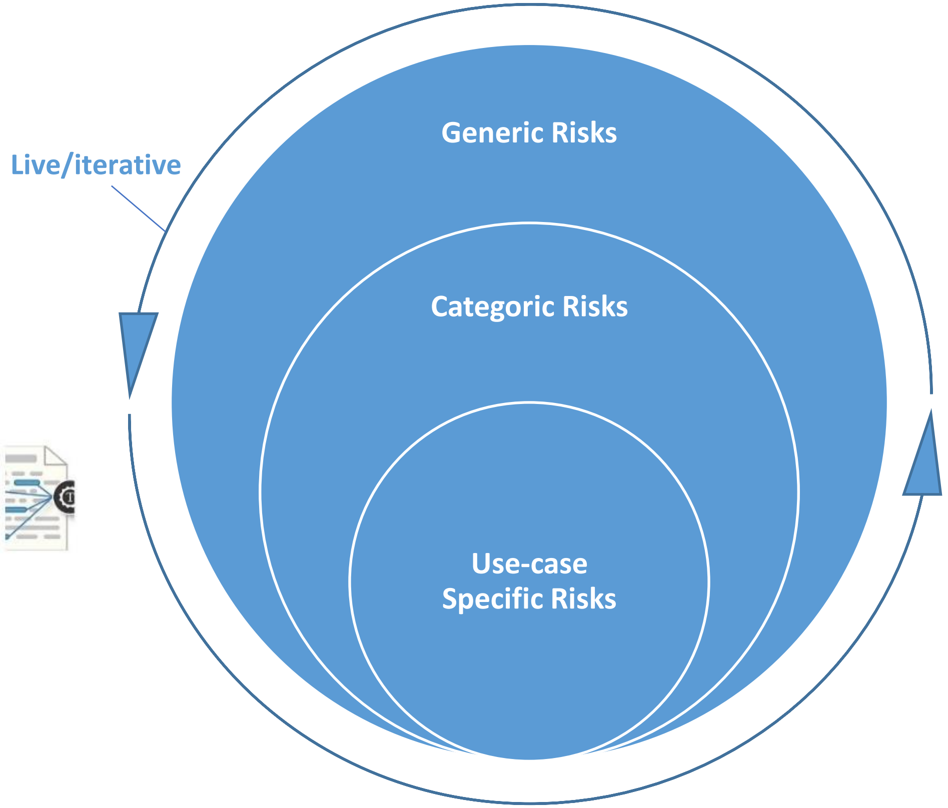
Externally hosted AI services including Large Language Models (LLMs), such as ChatGPT, can offer **great benefits** to organisations in manufacturing when customised to their use-cases or integrated into their systems improving their efficiencies.

However, these benefits come with several **important risks** emerging from emerge from third-party data, software, hardware, or policies. Examples of such risks are:

- Sharing sensitive data
- Lack of transparency
- Legal implications (e.g., Intellectual Property (IP) infringement and use of customers data)

Applications of LLMs

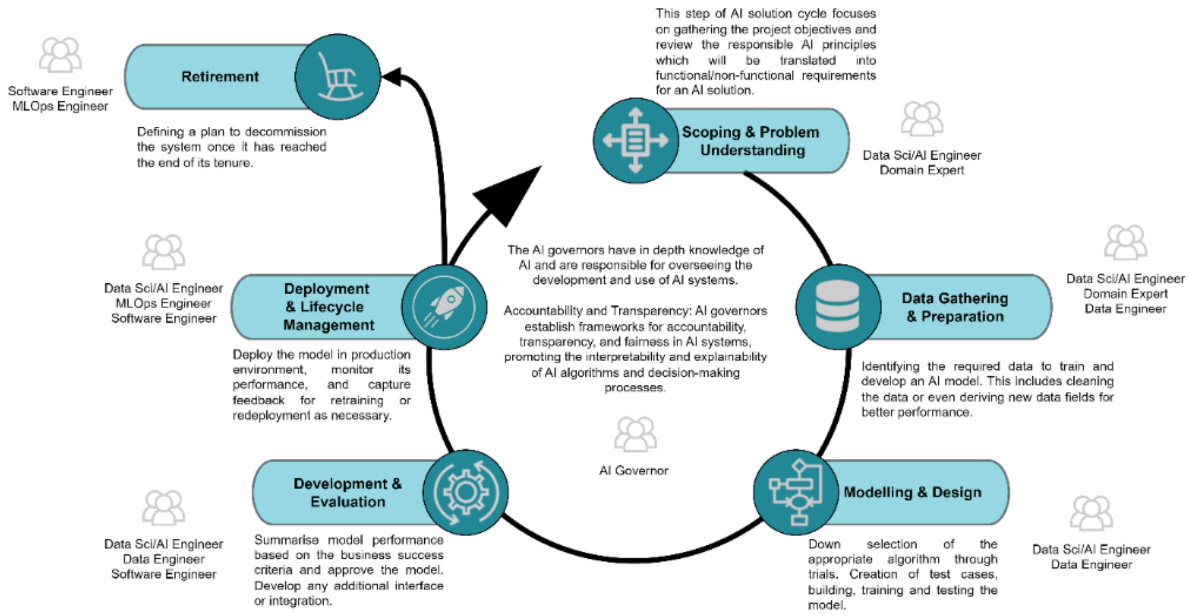




Risks

Developing the Process of Using Externally Hosted AI Services and the Role of AI Governance

Together we impact society.
The **RIGHT** Way



This step of AI solution cycle focuses on gathering the project objectives and review the responsible AI principles which will be translated into functional/non-functional requirements for an AI solution.

Scoping & Problem Understanding

Data Sci/AI Engineer
Domain Expert

Data Gathering & Preparation

Data Sci/AI Engineer
Domain Expert
Data Engineer

Identifying the required data to train and develop an AI model. This includes cleaning the data or even deriving new data fields for better performance.

Modelling & Design

Data Sci/AI Engineer
Data Engineer

Down selection of the appropriate algorithm through trials. Creation of test cases, building, training and testing the model.

Development & Evaluation

Data Sci/AI Engineer
Data Engineer
Software Engineer

Summarise model performance based on the business success criteria and approve the model. Develop any additional interface or integration.

Deployment & Lifecycle Management

Data Sci/AI Engineer
MLOps Engineer
Software Engineer

Deploy the model in production environment, monitor its performance, and capture feedback for retraining or redeployment as necessary.

Retirement

Software Engineer
MLOps Engineer

Defining a plan to decommission the system once it has reached the end of its tenure.

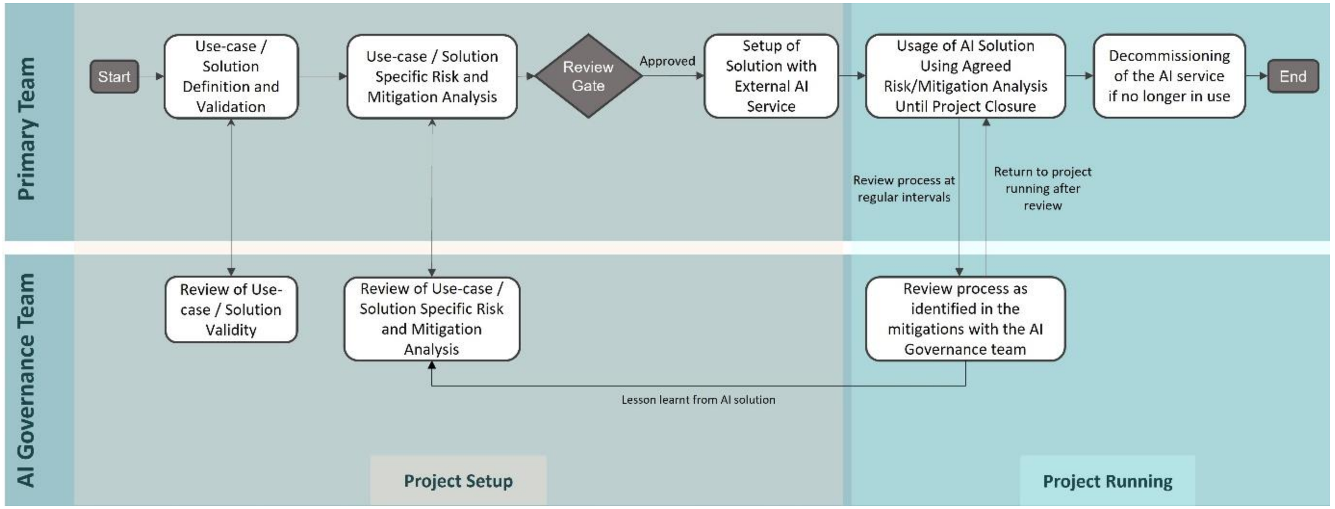
The AI governors have in depth knowledge of AI and are responsible for overseeing the development and use of AI systems.

Accountability and Transparency: AI governors establish frameworks for accountability, transparency, and fairness in AI systems, promoting the interpretability and explainability of AI algorithms and decision-making processes.

AI Governor

AI Development life cycle

AI Governance



Primary Team

Start

Use-case / Solution Definition and Validation

Use-case / Solution Specific Risk and Mitigation Analysis

Review Gate

Approved

Setup of Solution with External AI Service

Usage of AI Solution Using Agreed Risk/Mitigation Analysis Until Project Closure

Decommissioning of the AI service if no longer in use

End

Review process at regular intervals

Return to project running after review

AI Governance Team

Review of Use-case / Solution Validity

Review of Use-case / Solution Specific Risk and Mitigation Analysis

Review process as identified in the mitigations with the AI Governance team

Lesson learnt from AI solution

Project Setup

Project Running

mtc

UTILISING EXTERNALLY HOSTED AI/ GENERATIVE AI SERVICES IN MANUFACTURING:

Capabilities, Limitations, Risks and Mitigations, and the Role of AI Governance

October 2023

White paper :

UTILISING EXTERNALLY HOSTED AI/ GENERATIVE AI SERVICES IN MANUFACTURING: Capabilities, Limitations, Risks and Mitigations, and the Role of AI Governance

Discussion: G7 Guiding Principles on generative Artificial Intelligence

Together we impact society.
The **RIGHT** Way

Principle 1**: Take appropriate measures** throughout the development of advanced AI systems, including prior to and throughout their deployment and placement on the market, to identify, evaluate, mitigate risks across the AI lifecycle.

Principle 2: **Identify and mitigate vulnerabilities**, and, where appropriate, incidents and patterns of misuse, after deployment including placement on the market.

Principle 3: Publicly report **advanced AI systems' capabilities, limitations** and domains of appropriate and inappropriate use, to support ensuring sufficient **transparency.**

Principle 4: Work towards **responsible information sharing** and reporting of incidents among organizations developing advanced AI systems including with industry, governments, civil society, and academia.

Principle 5: Develop, **implement and disclose AI governance and risk** management policies, grounded in a risk-based approach – including privacy policies, and mitigation measures, in particular for organizations developing advanced AI systems.

Principle 6: Invest in and implement **robust security controls**, including physical security, cybersecurity and insider threat safeguards across the AI lifecycle.

Principle 7: Develop and deploy **reliable content authentication** and provenance mechanisms such as watermarking or other techniques to enable users to identify AI-generated content.

Principle 8: Prioritize **research to** mitigate societal**, safety and security risks** and prioritize investment in effective mitigation measures.

Principle 9: Prioritize the **development of advanced AI systems** to address the world's greatest challenges, notably but not limited to the **climate crisis, global health and education.**

Principle 10: Advance the development of and, where appropriate, adoption of where appropriate, **international technical standards.**

Principle 11: Implement **appropriate** data input **controls and audits**.

mtc
Manufacturing
Technology Centre

Together we impact society.
The **RIGHT** Way

Thank You

Mostafizur.Rahman@the-mtc.org

DISCLAIMER:
The data contained in this document contains proprietary information. It may not be copied or communicated to a third party, or used for any purpose other than that for which it was supplied, without the MTC's prior written consent ©MTC

CATAPULT
High Value Manufacturing