Project Management Part 2

Mind Map

(FIT3161 Final Year Project: Assignment)

Prepared by : MCS11

Alvin Andrean 33279071

Sheng Xin Chua 32837933

Steven Tirtadjaja 33068410

Marcholas Tjangnaka 33453128

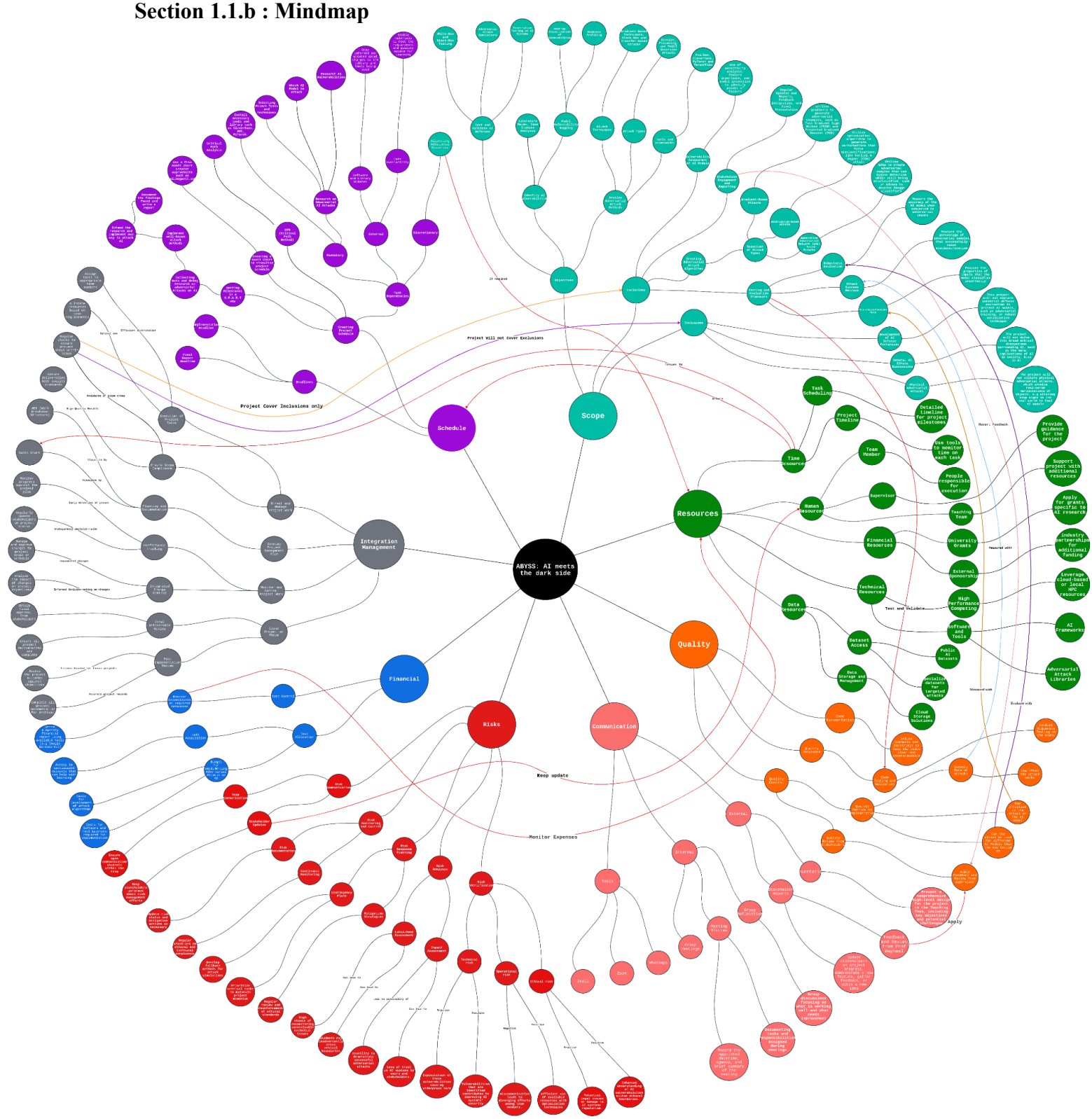
Monash University Malaysia
30-08-2024

Section 1.1.a: Introduction

The rapid advancement of Generative AI or Gen AI dazzled the world with its diverse applications in education (ChatGPT), entertainment (DALL-E), biology (AlphaFold) and chemistry (GNoME). Our project titled "Abyss: AI Meets the Dark Side", intends to explore the vulnerabilities and threats that are faced by AI systems. This project experiments on adversarial attacks on AI models to achieve this goal. This benefits the community of AI users as it uncovers and informs them about the vulnerabilities and potential errors of the AI models. Moreover, in the process of trying to undermine AI models, it is possible to trace back the reasoning and find potential ways to prevent it.

The objectives set for the project are to remain within the scope, schedule and budget constraints, which can only be accomplished with the help of effective project management practices. Needless to say, these practices not only play a key role in risk management but most importantly they affect the outcome of the project. To visualise and connect the various aspects of project management, a mind map is created. The visual representation in the form of the mind map provides a comprehensive overview of our plan and showcases how we intend to structure and achieve our objectives by relating to the critical elements of the project.

Section 1.1.b : Mindmap



Links:

https://lucid.app/lucidchart/0e705dee-7036-41c9-b1af-6e36a5b5bfd8/edit?viewport_loc=-10871%2C-6029%2C22144%2C12353%2C0_0&invitationId=inv_b765fdfc-1da9-4a2c-98a9-486c4b73ab2d

https://drive.google.com/file/d/1YgefgPycqI5-tKk5VzLL8TutmG471Onj/view?usp=sharing **(DOWNLOAD)**

Section 1.2: Mind Map Explanation

The mind map for this project centres around the title **"Abyss: AI Meets the Dark Side"** and extends to eight critical knowledge areas with each representing a key aspect of project management. The second and third levels of the map explore the tools and techniques that manage these areas within the context of our AI-focused project. The fourth level demonstrates how these tools are applied, ensuring a seamless transition from planning to execution. Each level has its own colour and interconnections between related areas are connected with arrows for visibility. The following sections are detailed breakdowns of each knowledge area represented in the mind map.

1. **Scope**

The scope section in the mind map describes the boundaries of the project, outlining what is included and excluded from the project and ensuring a clear understanding on what the project aims to achieve. The mind map's structure in the turquoise-highlighted section illustrates the scope that covers objectives, inclusions, and exclusions to manage expectations for the project.

At the first level of the scope, the diagram branches out into three key elements, namely objectives, inclusions, and exclusions. The inclusions specify what the project aims to cover, such as the development of adversarial attacks and identification of AI vulnerabilities. Exclusions define what is intentionally left out, like ethical discussions and physical attacks to prevent scope creep.

The mind map then delves deeper into specific focus areas, including detailed reports for stakeholders, exploration of several attack algorithms, and performing testing and evaluation to measure the success of these attacks on the AI. This structured approach allows for clear communication of project boundaries, objectives, and key focus areas to stakeholders, ensuring alignment throughout the project lifecycle. In addition, such clear division of what is inside and outside the scope of work keeps the team on track, saves time and effort not to be spent on irrelevant tasks, and effectively allocates resources to the most impactful areas of research and development.

2. **Schedule**

The management of time in a project is important because it helps in the organisation of all the activities that are involved in the project and their completion within the designated timeframe. In the second level of the schedule node, it emphasises the planning process, for instance, developing a project schedule. This process will inevitably result in defining task interdependencies, defining and setting up project milestones, and using the Critical Path Method or CPM, as well as visualising the project schedule with the help of the Gantt Chart. The mind map then expands to the illustration on how some of the tasks are more significant than the others, how the external factors such as software updates can affect the timeline, and how flexibility can be achieved by shifting resources from one task to the other.

3. **Resources**

The mind map's resources section outlines the pivotal resources, such as human, financial, technical, and data for driving project success. Effective collaboration among team members, supervisors, and teaching staff provides the expertise and guidance needed for complex AI vulnerability testing.

Financial resources, including grants and sponsorships, enable access to advanced tools and computing power, ensuring that technical and data needs are met without constraints. Time management, facilitated through task scheduling and monitoring tools, keeps the project on schedule, ensuring deadlines are met efficiently.These interconnected resources ensure the project stays aligned and on track to meet its objectives.

4. **Risk**

Effective risk management is crucial for the successful implementation of any project, especially those with complexities such as AI integration. The mind map's structure in the red-highlighted section outlines our comprehensive risk management strategy. The second level focuses on essential processes like risk identification, monitoring, and control—steps designed to mitigate risks by identifying them, determining responses, and ensuring these are communicated effectively to all relevant stakeholders. At the third level, the mind map delves deeper into specific risks, such as ethical concerns, technical challenges, and operational risks, and outlines strategies for mitigating, analysing, and addressing them. Additionally, it emphasises the importance of maintaining ongoing communication with stakeholders to keep them well-informed about risk statuses and any necessary actions that the team must take.

5. **Communication**

The communication section of the mind map shows a clear and structured approach on how internal and external communication will be handled, which are both essential for the project's overall success. Organisation and internal communication concentrates on successful project management and maintaining project integrity by holding meetings among the members. These include meeting agendas and minutes where every meeting's goals, objectives, assigned tasks, responsibilities, and decisions made are recorded to ensure that all the attendees are well informed. Tools like Zoom, Whatsapp and Gmail facilitate these interactions and to make communication as clear and consistent as possible to keep all the participants involved in the project.

On the other hand, external communication is used to ensure that a number of stakeholders such as the teaching team and the professors are updated through presentations and stakeholder reports. Such reports are meant to cover regular updates on the progress of our project, highlight key developments, updates on newly implemented features, and gain constructive feedback from stakeholders.

6. **Quality**

Quality management is essential to ensure that the project meets the requirements standards. At the second and third level, it highlights the importance of both quality assurance and control. Quality assurance makes sure that the project's code is thoroughly tested and well-documented in order to prevent problems down the line. Quality control, on the other hand, ensures that the result meets the expected standards.

The fourth level delves deeper into both quality assurance and control. This involves writing inline comments and docstrings, conducting rigorous testing to ensure that the codes used for adversarial attacks on AI are effective, as well as applying feedback from stakeholders to ensure the implementation meets the metrics and expectations.

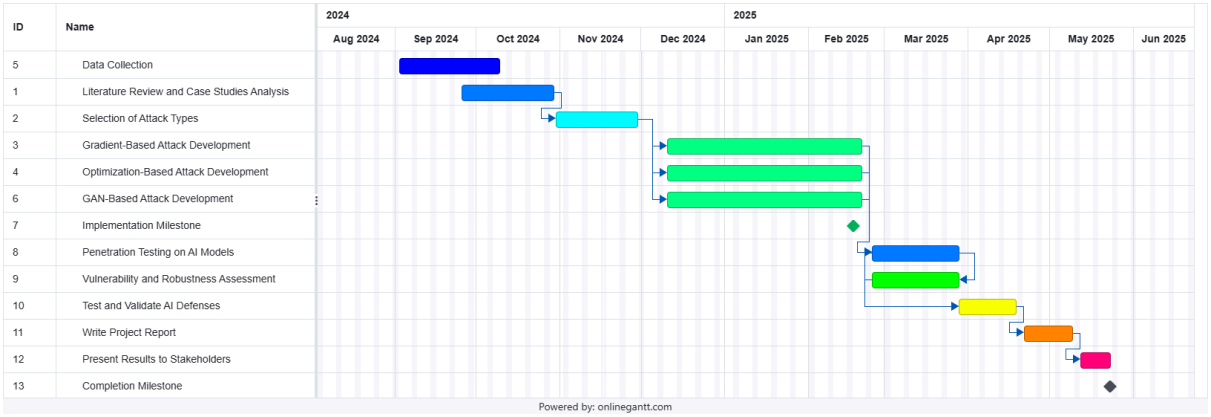
7. **Financial**

The mind map depicts a systematic approach to the management of funds with emphasis on costs and their distribution across a project. At the second level, it highlights the need to control costs that are associated with the acquisition of necessary resources. In terms of cost allocation, the third level emphasises data acquisition and budget allocation for adversarial AI attacks. This is further detailed at the fourth level, where the budget allocation is broken down into specific costs such as developing AI attack algorithms and acquiring necessary software and licences. In addition to these details, we'll write a monthly report that captures our financial management. The report will serve as a valuable tool for tracking expenses and ensure transparency within our project.

8. **Integration**

Effective integration management is essential for the seamless execution of complex projects, especially those involving diverse components like AI systems. The second level focuses on the foundational processes, including developing and monitoring the project to ensure that all activities stay within scope and adhere to the project requirements. This level involves setting up the framework for planning, documentation, and performance tracking, which are crucial for maintaining alignment with project goals. The third level then focuses on key processes such as planning, execution, and monitoring—critical steps to ensure that various project elements work together cohesively. Moving to the fourth level, the mind map explores specific integration tasks, such as coordinating cross-functional teams, managing data flow, and ensuring system interoperability. It also addresses potential challenges and provides strategies for overcoming them, such as the use of gantt charts or WBS(work breakdown structure).

Section 2: Short Essay



Effective timing management is recognized as being essential for the success of our research on adversarial attacks on AI models within the "Abyss: This is the case of the “AI Meets the Dark Side” project. This essay will discuss the importance of project timeline, the steps involved in managing the schedule and our strategies for the project.

Summary of Project Timetable

The project is divided into several phases where the tasks and milestones vary to achieve the overall objective of assessing and authenticating AI models against adversarial attacks. A special emphasis will be given to the process of selecting the most suitable attack type and technique. The project is initiated with installing the necessary libraries and tools followed by the development and implementation of adversarial attack algorithms. Following this, the algorithms will be run on various AI models in the testing phase and the results will be assessed to measure the effectiveness. The last phase of the project is the documentation and presentation of results.

This project will be completed according to a planned timeline in the form of Gantt Charts and Critical Path Method (CPM). These include milestones such as the completion of the research stage, the development of the algorithms, the completion of testing and the presentation of the final report. Each of the milestones will be accompanied by markers that ensure that the project is properly structured and progresses as planned.

Importance of Managing a Timetable

Time management is important for several reasons. It provides a clear vision of the project’s plan and ensures that all the members of the team recognize the time frame and their responsibilities. Schedule management especially assists in maintaining focus and ensuring that the project stays on track by breaking it down into work packages with set timelines.

Subsequently, proper time allocation allows the team to identify potential risks at an early stage. Schedule management methods provide the team with the ability to adjust the timeline, reallocate resources or invoke contingency plans in case of a specific task taking more time than anticipated. Proactive approach to scheduling is important for our project because the complexity of the task and the possible obstacles in creating and testing adversarial attacks may lead to delays.

Moreover, managing schedules assists the team members in conveying and synchronising their activities. A detailed and accurate time table helps the team members to track the progress of the project, share information and collaborate effectively. This is especially important in our project since the tasks are interdependent and the completion of one phase often depends on the completion of the previous phase.

Process of managing schedule

The schedule management process of the project comprises the following basic steps. First of all, the detailed project schedule based on Gantt Charts is to be created to identify the activities, their duration and dependencies. This timetable will also be frequently reviewed in order to ensure that it is accurate and as up to date as possible.

Following that, we will establish a monitoring and control system to track the project's progress in comparison to the project schedule. Regular team meetings will be held to assess task status, address any problems or delays and modify the schedule as needed. Critical Path Method (CPM) will be utilised to pinpoint the crucial tasks for the success of the project and to guarantee that these tasks receive top priority in terms of resources and attention.

We will establish a reporting system to share the project's development with supervisors and team members. This will make sure that all individuals are informed about the present situation of the project, any modifications to the timetable and the justifications for those modifications.

In summary, an organised project timeline and efficient schedule management process is conducive to success. Schedule management ensures that the project is finished on schedule and within scope and budget by establishing clear guidelines, recognizing possible challenges and fostering communications between participants of the project.