Poster Presentation
Face Detection System

Product Backlog:

1. User Authentication and Access Control (U1)
2. Image Acquisition and Preprocessing (U2)
3. Face Detection Algorithm Development (U3)
4. Face Recognition Integration (U4)
5. Integration with External Systems (U5)
6. Continuous Integration and Deployment(U6)

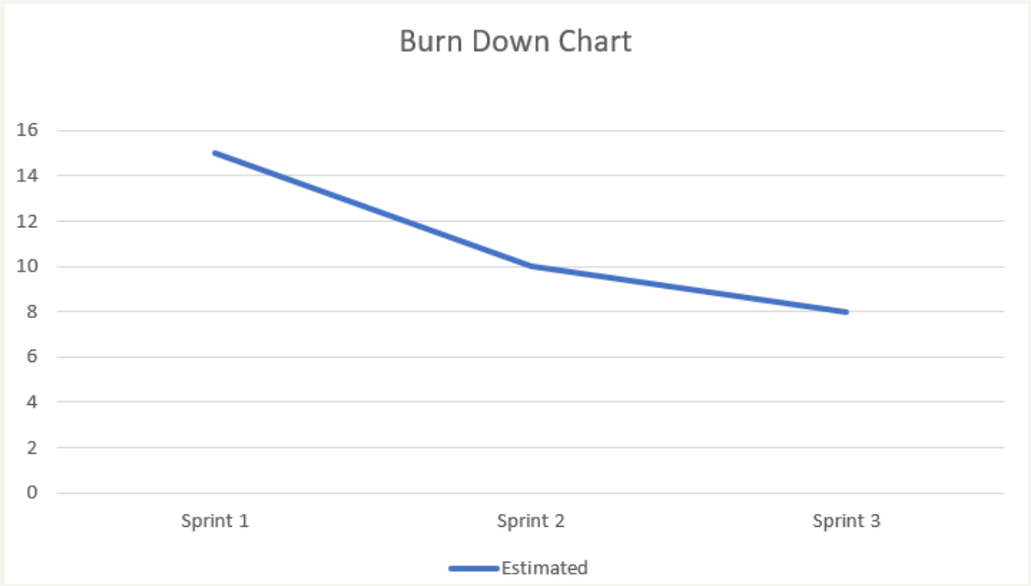
Sprint Backlog

Sprint 1:
1. U1, U2, U3

Sprint 2:
1. U4, U5

Sprint 3:
1. U6

Burn Down Chart



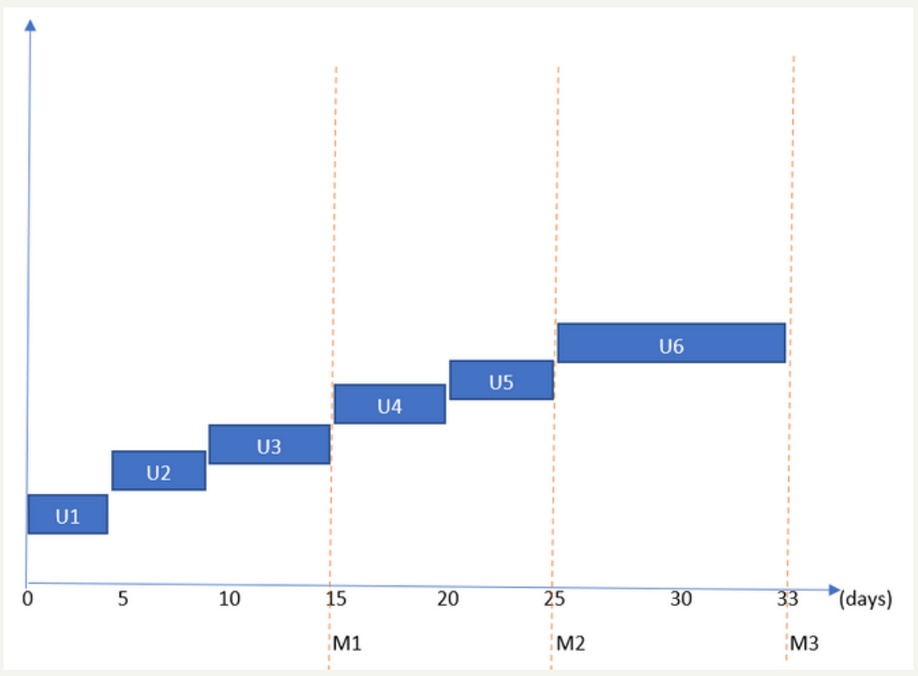
LOC method

Estimated Lines of Code = 25000
Average Productivity = 620 loc /pm
Laboured rate=8000 $ /m
Cost per line = 13 $
Total estimated project cost=325000 $
estimated efforts= 40 persons/month

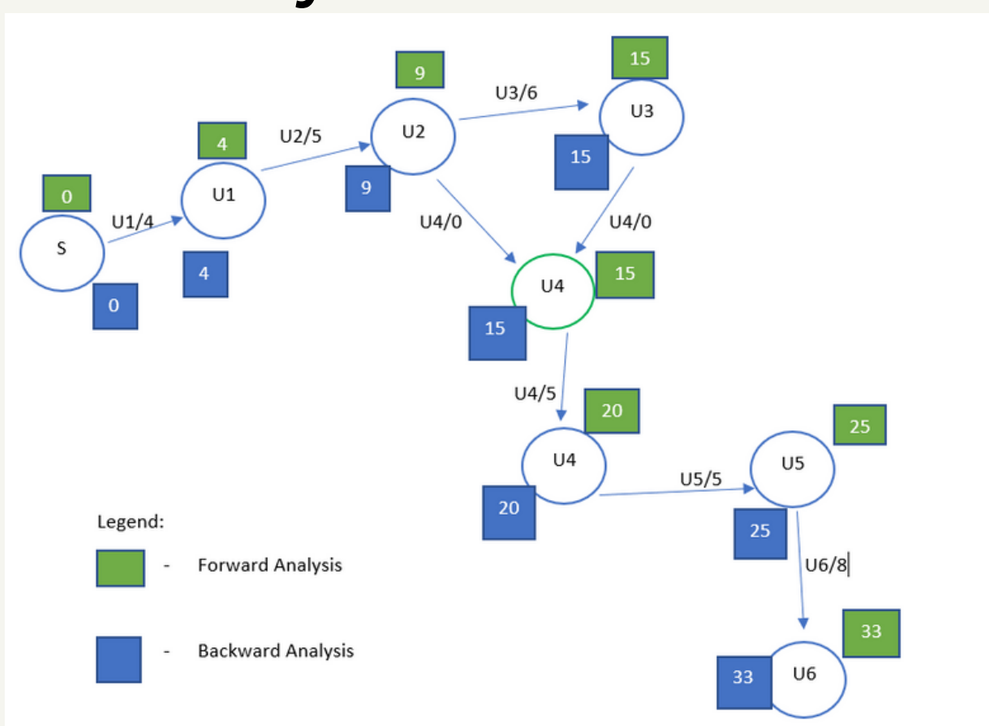
Task and Dependency

Task	Duration	Dependency
U1	4	-
U2	5	U1
U3	6	U2
U4	5	U2,U3
U5	5	U4
U6	8	U5

Gaant Chart



PERT Analysis



Risk Table

Risk	Probability	Impact
Data Quality and Availability	70	Catastrophic
Algorithm Selection	60	Marginal
Skill and Resource availability	40	Marginal
Hardware Constraints	30	Marginal
Integration Challenges	45	Catastrophic
System Calibration and Tuning	20	Negligible
Privacy and Security Concerns	50	Catastrophic

RMMM:

1) Data Quality and Availability:
Risk Mitigation:
The dataset chosen should be carefully analysed and pre-processed so that the overall quality of the code can be maintained thus leading to a better accuracy for our face detection algorithm
Risk Monitoring:
The dataset can be cross verified by another person checking for any discrepancies in the dataset .Moreover a dry run can be run on the dataset so that we can verify the performance of the model based on our dataset.
Risk Management:
If the dataset even after the pre-processing stage and monitoring stage leads to downgrade in performance of our model then either the dataset can be discarded or new features can be added to the dataset to improve the accuracy.
2) Privacy and Security Concerns:
Risk Mitigation:
Implement strong encryption and secure storage: Use robust encryption algorithms to protect sensitive data, such as facial templates or user credentials, both during transmission and storage. Implement secure storage mechanisms, such as encrypted databases or secure file systems, to prevent unauthorized access to the data.
Risk Monitoring:
Regular security audits and vulnerability assessments: Conduct periodic security audits and vulnerability assessments to identify potential security weaknesses or vulnerabilities in the face detection system. Stay updated with security best practices and address any identified issues promptly to mitigate security risks.
Risk Management:
Establish a comprehensive privacy and security policy: Develop and document a clear privacy and security policy that outlines how personal data will be handled, stored, and protected within the face detection system. Ensure compliance with relevant privacy laws and regulations. Regularly review and update the policy to reflect any changes in regulations or system requirements.

Git Link:

https://github.com/joanishmuthu/Software-Engineering-Management