Hazard Analysis
Mission Control Terminal MC

Team 12, Autonomous Satellite Operations Scheduler
Diamond Ahuja
Rishi Vaya
Buu Ha
Umang Rajkarnikar
Dhruv Cheemakurti

October 20, 2023

Table 1: Revision History

Date	**Developer(s)**	**Change**
October 20, 2023	Q.H, R.V, D.A, D.C, U.R	Completed HA documentation

Contents

1 Introduction

The primary objective of our project MCT (Mission Control Terminal) is to provide satellite operators with a platform to automatically schedule and send commands to satellites as they pass overhead. In addition, the system will keep logs of all commands sent, responses, with concurrent access available. This is a hazard analysis document for the MCT capstone project.

2 Scope and Purpose of Hazard Analysis

Hazard Definition - Hazards can be defined as any situation within an application that can potentially lead to an unwanted or undesirable outcome which can include system failures, data loss, harm to users or any other consequences. These hazards can occur due to many factors such as design flaws, communication flaws, equipment failures and programming errors.

The purpose of this document is to find cases of hazards that may be encountered in the project and find potential methods to mitigate those hazards.

3 System Components

- Command Scheduling: Operators need to be able to schedule commands for engineering and NEUDOSE satellites. They should be able to work concurrently with other users
- Orbital Prediction: Operators need to be able to calculate and predict satellite overpasses and satellite illumination cycles.
- User Authentication and Authorization: Users must be able to log in, with a special admin user which controls access to satellite usage.
- Logging: Users must be able to retrieve a log of commands sent, and responses from the application.

4 System Boundaries

- Satellite Hardware and Control Systems: The application will not directly interface with the satellite's hardware, it will send commands to the ground station for transmission.
- Ground Station Infrastructure: The application will not manage or control the ground station equipment.

5 Critical Assumptions

- The linux server hosting the web application shall not be suspended or paused.
- The operator and system administrators using the application shall not misuse it or intentionally use it in an unintended way.
- Operators and system administrators are well-informed of security best practices, such that they are aware of attacks like phishing attacks.
- The authentication token provided by the OpenID Connect Protocol is cryptographically secure.
- The commands are verified by the operators before they are scheduled.

6 Failure Mode and Effect Analysis

Failure Mode and Effect Analysis System: Autonomous Satellite Operations Scheduler Subsystem: N/A Phase/Mode: System Requirements							
Design Function	Failure Modes	Effects of Failure	Causes of Failure	Detection	Recommended Actions	SR	Ref.
Predict Satellite Overpasses	Miscalculation	Inability to connect with Satellite	a. Extreme conditions b. TLE variation		a. Recalculate satellite overpasses b. Fetch TLE periodically	a. SR-1 b. SR-1	H1-1
Schedule Commands	Does not perform all Commands	Incomplete Data	a. Satellite becomes out of range b. Prior command alters state of satellite		a. Set minimum elevation food which connections will be made b. Satellite operators must determine the validity of the commands being sent	a. SR-2 b. SR-3	H2-1
	Invalid command inputs	Scheduling Error	a. Incorrect commands are inputted		a. Satellite operators to perform input validation	a. SR-3	H2-2
Logging	State of Database Altered	Incorrect Response Parsing	a. Various forms of responses returned		a. Database structure verification a. Data validation	a. SR-4 b. SR-4	H3-1
	Incomplete Database	Missing Data	a. Scheduling command failure b. Satellite failure c. Network failure		a. Assign relevant error messages in lieu of missing data b. Assign standardized error messages c. Assign standardized error messages	a. SR-5 b. SR-5 c. SR-5	H3-2
Web Interface	Browser compatibility issues	Visual Disparities	a. Missing browser specific features b. HTML/CSS validation		a. Testing the web interface on a variety of browsers and their different versions b. Assign a HTML/CSS validation service so the code is standardized	a. SR-6 b. SR-7	H4-1
	Poor responsiveness	Inefficiency in scheduling operations	a. Unoptimized algorithms b. Slower loading times		a. Optimize code by using efficient algorithms b. Use browser caching	a. SR-8 b. SR-8	H4-2
User Account Handling	Unauthorized access	Compromising Security	a. Weak user authentication measures		a. Implementing multi-factor authentication and limiting login attempts	b. SR-9, SR-10	H5-2

Figure 1: FMEA process

7 Safety and Security Requirements

SR-1:

The application shall periodically fetch TLE and calculate satellite overpasses to ensure the most recent data is being used to predict satellite overpasses.

Rationale: An issue with calculating satellite overpasses is the variation in TLE and other conditions. Periodically retrieving and recalculating this piece of information will ensure a more accurate prediction of overpasses.

Associated Hazards: H-1a, H-1b

SR-2:

The application shall use a minimum elevation as a point of reference to evaluate whether a connection to the satellite can be made.

Rationale: In the case that a satellite is below the minimum elevation required to make a connection, the scheduled commands may not work and as a result, produce incomplete data. By having a minimum point of reference, the system can assess if a satellite is out of range.

Associated Hazards: H-2a

SR-3:

Operators shall be informed of errors that occur during the scheduling of commands, however, it is the operator's responsibility to ensure the validity of the commands.

Rationale: Since the application allows operators to send and schedule commands to the satellite, it is possible that an incorrect command is sent. In this case, it would be helpful to highlight the errors found in the operator's input data.

Associated Hazards: H-2b, H-3a

SR-4:

The system shall have a backup and recovery mechanism which is capable of restoring the database to its most recent correct state in the event of unexpected data failures.

Rationale: A situation may occur where the database enters into an unknown or corrupt state. The presence of a backup and recovery mechanism ensures

that the information in the database is still accessible by rolling back to the most recent correct state.

Associated Hazards: H3-1a, H3-1b

SR-5

In the event of a system, network, or satellite failure, all missing data fields shall be labelled with an appropriate error message as part of the data validation process. These error messages shall adhere to a standardized format.

Rationale There may be cases where a scheduled command produces responses with missing data attributes. By identifying the incomplete data using standardized error messages, it provides a consistent data state across all validation processes.

Associated Hazards: H3-2a, H3-2b, H3-2c

SR-6

Cross-browser testing across a range of browsers shall be performed to ensure the application functions consistently.

Rationale Due to slight variations in browsers such as Safari, Chrome, and Firefox, it is important to assess the performance of the application across all user-intended environments.

Associated Hazards: H4-1a

SR-7

The code base shall have HTML and CSS checks to ensure compatibility across different devices and browsers.

Rationale Incorporating the above checks can identify errors in the code base as well as possibly improve the application's user interface.

Associated Hazards: H4-1b

SR-8

All components which are required for scheduling operations shall be evaluated on their efficiency, where each component must complete within a minimum time frame.

Rationale By having a pipeline to test parts of the duration of a code, it can

prevent situations where there may exist an inefficiency in scheduling operations.

Associated Hazards: H4-2a

SR-9

The application shall not authenticate a user who has attempted to login with the same credentials ten times, consecutively. The application shall have a time-out period of five minutes before the user can authenticate themselves.

Rationale By having a timeout period for a set number of unsuccessful authentication attempts, it protects user accounts from unauthorized access and improves security.

Associated Hazards: H5-1a

SR-10

The application shall support multi-factor authentication such that a user must verify their identity through their registered email account.

Rationale Having multi-factor authentication provides an additional layer of security to the application, ensuring that unauthorized users are prohibited from accessing sensitive user and system data.

Associated Hazards: H5-1a

8 Roadmap

The hazard analysis introduced a number of new safety and security requirements for the project. The team will ensure that most of the requirements are implemented by the time of the first demonstration in February, 2024. The primary focus will be on implementing all requirements except SR-4. The team believes that a secure database will already be used in the project and hence there is no immediate need for a backup. However, it was decided that this could be implemented in the future of the application.