Hazard Analysis
Software Engineering

Team #10, Five of a Kind
Omar Abdelhamid
Daniel Maurer
Andrew Bovbel
Olivia Reich
Khalid Farag

Table 1: Revision History

Date	**Developer(s)**	**Change**
Date1	Name(s)	Description of changes
Date2	Name(s)	Description of changes
...	...	...

Contents

1 Introduction 1

2 Scope and Purpose of Hazard Analysis 1

3 System Boundaries and Components 1

4 Critical Assumptions 1

5 Failure Mode and Effect Analysis 2

6 Safety and Security Requirements 4

7 Roadmap 6

[You are free to modify this template. —SS]

1 Introduction

[You can include your definition of what a hazard is here. —SS]

2 Scope and Purpose of Hazard Analysis

[You should say what **loss** could be incurred because of the hazards. —SS]

3 System Boundaries and Components

[Dividing the system into components will help you brainstorm the hazards. You shouldn't do a full design of the components, just get a feel for the major ones. For projects that involve hardware, the components will typically include each individual piece of hardware. If your software will have a database, or an important library, these are also potential components. —SS]

4 Critical Assumptions

[These assumptions that are made about the software or system. You should minimize the number of assumptions that remove potential hazards. For instance, you could assume a part will never fail, but it is generally better to include this potential failure mode. —SS]

5 Failure Mode and Effect Analysis

In this section, we will be analyzing the failure modes and effects of the system. The following table will break down the potential failure modes, their causes, effects, recommended actions, and the safety requirements that are associated with them.

Table 2: Failure Mode and Effect Analysis (FMEA) - Part 1

Component	**Failure Mode**	**Causes of Failure(s)**	**Effects of Failure(s)**	**Recommended Action(s)**	**SR**	**Ref.**
Import Manager	The system does not process the CAD file correctly as the user is expecting.	• The inputed STL file is corrupted therefore it can't be read by the system. • The input file is not in the correct format so the system can't process it.	• The system can't process the file therefore it can't be sliced. • Due to the confusion in system not reading the file, this will result in user frustration. • It will lead to user spending more time to get the system to process the file.	When the file is first inputted into the system, the system will validate that the file is first in the correct format, and that it does not contain any corrupt information. This will then lead to the system prompting the user to re-enter the file or input a new one in.	F212, NF211, SCR1, SCR9	H1
Visualization Manager	The system fails to render the 3D image of the model	• The device that is being used to run the system does not have enough memory to render the image. • The device's GPU driver is not working correctly or is not up to date as required for the system to render the image.	• Model is not displayed leading to poor user experience. • Designers can't proceed with the design review, and fall back to using their old design software to add magnetization and material properties to the design.	The system should check if the device has enough memory to render the image, and if the GPU driver is working correctly. If not, the system should prompt the user to use a different device or update the GPU driver.	F221, NF221, SCR2, SCR9	H2
Visualization Manager	The voxels displayed as selected/currently editing do not match the voxels actually being edited.	• Logical error in the system's selection/editing mechanism. • UI rendering bug not accurately reflecting the backend state. • Inconsistent data synchronization between front-end display and back-end data model.	• Poor user experience (UX) as the user thinks they're doing one thing, but the system is actually editing something completely different. • Incorrect modifications to the model. • Loss of user trust in the system's accuracy. • Time wasted correcting errors.	The system shall ensure real-time synchronization between the UI display of selected/edited voxels and the backend data model.	F226, FF228, NF221, SCR3, SCR8	H3

Table 3: Failure Mode and Effect Analysis (FMEA) - Part 2

Component	**Failure Mode**	**Causes of Failure(s)**	**Effects of Failure(s)**	**Recommended Action(s)**	**SR**	**Ref.**
Export Manager and Property Manager	Exported file is missing magnetization and material properties	• The system does not export the magnetization and material properties to the CSV file correctly. • The system fails to save the magnetization and material properties for certain voxels	• The Java program that reads the CSV file receives incomplete data causing print failure or defects. • The Java program reads the file correctly, however the printer crashes due to missing magnetization and material properties. • Material will be wasted if printer crashes after printing a few layers.	The system should validate that the magnetization and material properties are saved for all voxels. If not, the system should prompt the user to re-export the file.	F231, F233, NF232, SCR4	H4
Export Manager	File format is exported in the incorrect format	• The system does not export the CSV file in the correct structure and format.	The Java program can't read the file correctly because of the wrong format therefore causing the program to crash.	The system should check that the structure of the CSV file is correct and matches the required format.	F241, F242, NF241, SCR5	H5
Full System	User progress is lost	• Unexpected software bug that causes the system to crash, which causes the system to lose its state. • The user experiences a hardware malfunction (e.g., power loss, memory failure), which causes the system to lose its state.	• User loses signifcant work and would need to re-do the work. • User will start getting frustrated and lose trust in the system. • User will lose signicant time in the total workflow of their design due to the need to redo the work.	The system shall implement a auto-saving mechanism to periodically save the state of the user's process to allow for recovery in case of a system shutdown or failure.	F234, SCR6, SCR7	H6

6 Safety and Security Requirements

In this section, we will be analyzing the safety requirements of the system. The following table will break down the potential safety requirements, their associated hazards, and their priority.

Symbol	Value
MAX_VOXEL_COUNT	103,680,000 voxels
MAX_VOXEL_SELECTION	1000 voxels
INPUT_FILE_VALIDATION_THRESH	100%
MIN_RENDER_MEMORY	16 GB
UI_SYNC_ACCURACY	100%
EXPORT_COMPLETENESS_THRESH	100%
CSV_FORMAT_VALIDATION	100%
AUTO_SAVE_INTERVAL	5 minutes
UNDO_HISTORY_SIZE	10 actions
FILE_IMPORT_EXPORT_TIMEOUT	2 minutes
FEEDBACK_UPDATE_TIME	30 seconds

Table 4: Symbolic Constants

SCR 1. *The system shall validated the importaed CAD files (STL/OBJ) for their format correctness before processing the model.*
Rationale: The corrupted files can cause the system to fail and prevent successful voxelization to the workflow disruption.
Fit Criterion: `INPUT_FILE_VALIDATION_THRESH` of the imported files must pass the validation checks, and the system should reject any files that fail to do so.
Associated Hazards: H1
Priority: High

SCR 2. *The system shall check if the device has enough memory and GPU capabilities before attempting to render 3D models and voxel grids.*
Rationale: The insufficient memory or outdated GPU drivers can cause rendering failures with the system, preventing users from visualizing their models and proceeding with property assignments.
Fit Criterion: The hardware where the system is running on must have at least `MIN_RENDER_MEMORY` of memory, and the GPU driver must be compatible with the system.
Associated Hazards: H2
Priority: Medium

SCR 3. *The system shall maintain real-time synchronization between the UI component of selected/edited voxels and the backend data model.*
Rationale: Any failures in this synchronization can lead to user editing unintended voxels, causing incorrect property assignment and loss of user trust in system accuracy.
Fit Criterion: `UI_SYNC_ACCURACY` of voxel selections and edits must be accurately reflected

in both UI display and backend data model.
Associated Hazards: H3
Priority: High

SCR 4. *The system shall validate all magnetization and material properties before exporting the file containing the metadata for all voxels.*
Rationale: Missing these important information can cause excessive time and material waste, and in some cases can cause printer failures.
Fit Criterion: `EXPORT_COMPLETENESS_THRESH` of exported files must contain complete magnetization and material property data for all voxels.
Associated Hazards: H4
Priority: High

SCR 5. *The system shall validate the CSV file format and structure before exporting the file, ensuring that it is compatible with the next system that will read the file.*
Rationale: Incorrect CSV format can cause the Java printer program to crash, preventing the user from continuing with the workflow, leading to user frustration.
Fit Criterion: `CSV_FORMAT_VALIDATION` of exported CSV files must match the required structure and format expected by the next system that will read the file.
Associated Hazards: H5
Priority: High

SCR 6. *The system shall implement auto-saving functionality to preserve user progress and enable recovery from any system crashes or hardware failures.*
Rationale: Any sysetm crashes or hardware failures can lead to signicant amount of work loss,which would require the user to restart the workflow from scratch, which would be very time consuming and frustrating.
Fit Criterion: The system must automatically save user progress every `AUTO_SAVE_INTERVAL`.
Associated Hazards: H6
Priority: High

SCR 7. *The system shall provide undo/redo functionality to allow users to correct their mistakes without losing signifcant work.*
Rationale: Human errors in design are common and users need the ability to easily correct these mistakes without restarting the process.
Fit Criterion: The system must maintain an undo history of at least `UNDO_HISTORY_SIZE` actions and provide clear undo/redo controls.
Associated Hazards: H6
Priority: Medium

SCR 8. *The system shall limit the number of voxels that can be selected simultaneously to prevent any performance issues.*
Rationale: Slecting too many voxels at a time can cause system slowdowns, UI freezing and an overall poor user experience.
Fit Criterion: The system must limit voxel selection to a maximum of `MAX_VOXEL_SELECTION` voxels at any time and provide clear feedback when limits are reached.
Associated Hazards: H3
Priority: Medium

SCR 9. *The system shall provide progress updates and timeout handling for long running operations such as importing/exporting the file, and voxelization.*
Rationale: Large CAD files can take significant time to process, and users need feedback on progress to avoid waiting indefinitely.
Fit Criterion: All import and export operations must timeout after `FILE_IMPORT_EXPORT_TIMEOUT`, and all operations exceeding `FEEDBACK_UPDATE_TIME` must provide progress updates.
Associated Hazards: H1, H2
Priority: Medium

7 Roadmap

In this section, we will state which safety requirements will be implemented as part of the capstone timeline, and which requirements will be implemented in the future.

Requirements that will be implemented as part of the capstone timeline:

- SCR 1
- SCR 2
- SCR 3
- SCR 4

Requirements that will be implemented in the future:

- SCR 5
- SCR 6
- SCR 7
- SCR 8

Appendix — Reflection

[Not required for CAS 741 —SS]

The purpose of reflection questions is to give you a chance to assess your own learning and that of your group as a whole, and to find ways to improve in the future. Reflection is an important part of the learning process. Reflection is also an essential component of a successful software development process.

Reflections are most interesting and useful when they're honest, even if the stories they tell are imperfect. You will be marked based on your depth of thought and analysis, and not based on the content of the reflections themselves. Thus, for full marks we encourage you to answer openly and honestly and to avoid simply writing "what you think the evaluator wants to hear."

Please answer the following questions. Some questions can be answered on the team level, but where appropriate, each team member should write their own response:

1. What went well while writing this deliverable?

2. What pain points did you experience during this deliverable, and how did you resolve them?

3. Which of your listed risks had your team thought of before this deliverable, and which did you think of while doing this deliverable? For the latter ones (ones you thought of while doing the Hazard Analysis), how did they come about?

4. Other than the risk of physical harm (some projects may not have any appreciable risks of this form), list at least 2 other types of risk in software products. Why are they important to consider?