# Hazard Analysis Software Engineering

Team 21, Alkalytics Sumanya Gulati Kate Min Jennifer Ye Jason Tran

Table 1: Revision History

Date	Developer(s)	Change
	Name(s) Name(s)	Description of changes Description of changes
	•••	

### Contents

1	Introduction	1			
2	Scope and Purpose of Hazard Analysis	1			
3	System Boundaries and Components	1			
4	Critical Assumptions Failure Mode and Effect Analysis				
5					
6	6.1 Access Requirements	4 5 5			
7	Roadmap	6			

#### 1 Introduction

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

### 2 Scope and Purpose of Hazard Analysis

The purpose of the hazard analysis is to identify potential hazards and its causes, assess the effects, and set mitigation strategies to eliminate or lessen the risk of the hazard. It is important to consider all possible hazards associated with the Alkalytics project and its components, as the following losses could be incurred from an insufficient hazard assessment:

- Data loss: The data gets unintentionally lost, deleted, or corrupted.
- Data integrity: The data is not complete, accurate, nor correct which can lead to computational errors.
- System availability: Users are unable to access the system due to factors such as unstable internet connection or server crashes.
- Security: If there are no proper measures for authentication, unauthorized access to the data or user information may occur.

### 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

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
Authentication	Unauthorized user access	Data breach, loss of data	Weak security protocols	Strengthen authentication mechanisms	SR-1, SR-2	H1-1
	User unable to log in	integrity Loss of productivity	System downtime, creden-	Ensure high system up-	FR-14,	H1-2
	Oser unable to log in	Loss of productivity	tial errors	time and credential recov-	SR-1,	111-2
			tial effors	ery	SR-4	
CSV Data Mi-	Data not uploaded to the	Loss of data availability	Incorrect file format or	Validate file format and	FR-3,	H2-1
gration	database	Loss of data availability	server issue	ensure server uptime	FR-4,	112-1
gration	database		server issue	ensure server uptime	SR-9	
	Data partially uploaded	Incomplete data leads to	Timeout during upload,	Implement error-checking	FR-3,	H2-2
	Data partially aploaded	incorrect analysis	corrupted file	during upload	FR-2	112-2
	Duplicate data entries	Conflicting results in data	No validation for dupli-	Add duplicate data detec-	SR-5,	H2-3
	D'apricate aata chirici	analysis	cates	tion and rejection logic	FR-4,	112 0
				l legic and rejection region	SR-7	
Data Visualiza-	Incorrect graph rendering	Misleading or inaccurate	Inaccurate parameter se-	Improve input validation,	FR-8,	H3-1
tion		data interpretation	lection	real-time graph updates	FR-9	
	Slow graph rendering	Poor user experience	Large dataset or ineffi-	Optimize graph rendering	PR-5,	H3-2
		1	cient plotting algorithm	speed	PR-2	
Query Function-	Data not returned or de-	User frustration, inability	Database connection or	Optimize query perfor-	FR-5,	H4-1
ality	layed	to retrieve data	query input error	mance and error handling	FR-6,	
					PR-2	
	Incorrect data returned	Incorrect conclusions from	Misconfigured query logic	Validate query structure	PR-6,	H4-2
		user		and results	FR-5	
	Query results outdated	Decisions based on stale	Data not refreshed in	Implement data refresh	PR-14,	H4-3
		data	database	strategy	FR-6	
Data Export	CSV export generates cor-	Data cannot be used in ex-	Incorrect formatting logic	Implement robust export	FR-15,	H5-1
	rupted files	ternal systems		validation	PR-6,	
					SR-3	
	Export missing data	Partial data exported, in-	Timeout during export or	Ensure export process	FR-15,	H5-2
		complete reports	data truncation	handles large data vol-	PR-8	
				umes		
	Session timeout too short	User repeatedly logged	Incorrect session configu-	Increase session timeout	FR-14,	H5-3
		out, inconvenience	ration	settings	SR-16,	
					SR-4	
Backend	Database connection lost	Data retrieval fails, analy-	Network issues, server	Improve database fault-	PR-9,	H6-1
Database		sis halted	downtime	tolerance and backups	PR-10	TIC 2
	Data corruption during	Loss of data integrity	Incorrect write operations	Implement database	SR-6,	H6-2
	storage	A 1: 4:	or hardware failure	checksums and backups	SR-7	II.C.O
	Insufficient storage space	Application crashes or	Lack of storage planning	Increase storage capacity	PR-12,	H6-3
		stops accepting data		and monitor usage	PR-13	

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
Frontend Inter-	UI unresponsive	Poor user experience,	JavaScript errors, re-	Debug UI code, efficient	FR-7,	H7-1
face		tasks uncompleted	source overload, slow	resource management	PR-3	
			internet			
	Elements not displayed	Confusion, incorrect ac-	Browser compatibility is-	Test for compatibility	LFR-1,	H7-2
	correctly	tions performed	sues	across browsers	OER-3	
	Data input fields allow in-	Corrupted data entered	No input validation	Enforce input validation	FR-1,	H7-3
	valid entries	into system		on frontend	FR-4,	
					SR-7	
Performance	Slow page load times	User frustration, reduced	Unoptimized fron-	Optimize code and	PR-3,	H8-1
		productivity	tend/backend code	database queries	PR-5	
	High CPU/memory usage	System instability, crashes	Inefficient data processing	Implement memory man-	PR-4,	H8-2
			or memory leaks	agement and resource	PR-2	
				monitoring		
Error Tracking	Errors not logged	Difficulty identifying and	Lack of error handling in	Implement detailed error	FR-12,	H9-1
		resolving issues	code	logging	FR-13	
	Logged errors not dis-	Users unaware of issues	Incomplete error-handling	Display errors to user,	MSR-5,	H9-2
	played to user		UI	troubleshooting tips	PR-9	
	Errors logged but not cat-	Troubleshooting becomes	Poor error categorization	Create detailed error cat-	MSR-5,	H9-3
	egorized	complex		egories and log structure	FR-12	
Machine Learn-	Incorrect data prediction	Misleading trends, faulty	Inaccurate algorithm con-	Improve machine learning	FR-11	H10-1
ing Analysis		decisions	figuration	validation steps		
	Model training incomplete	Model unable to provide	Insufficient data or faulty	Ensure ample, clean train-	FR-11,	H10-2
		accurate predictions	training process	ing data	PR-8	
	Training data overfitting	Model provides unreliable	Model too tightly fitted to	Implement regularization	FR-11	H10-3
		results	training data	techniques		

### 6 Safety and Security Requirements

New safety and security requirements have been discovered and will be integrated within the SRS document. Note that the entire requirement codes have been changed with the new additions having expanded information, and the previous requirements displaying new codes.

#### 6.1 Access Requirements

- **SR-1.** Access to the application must be restricted to authorized personnel, with an authentication mechanism.
- **SR-2.** Only authenticated users should have the ability to query or modify the data, and each user's access must be limited to their capabilities within the application.
- **SR-3.** The application must restrict sensitive operations (e.g., data export) to authorized personnel only.
  - Rationale: Prevents unauthorized users from exporting or sharing sensitive data, protecting data integrity.
  - Fit Criterion: Only authorized users must be able to perform sensitive operations like data export.
  - Traceability: FR-15, SR-2.
- **SR-4.** The application must enforce session timeout and automatic logouts after a period of inactivity.
  - Rationale: Protects the application from unauthorized access if users leave their session unattended.
  - Fit Criterion: Sessions must time out and log users off automatically after a specified inactivity period.
  - Traceability: FR-14, SR-1, SR-4.

#### 6.2 Integrity Requirements

- **SR-5.** The application must validate data inputs to ensure they conform to expected formats and values before they are processed.
- SR-6. The application must not modify the data unnecessarily through its transfer process.
- **SR-7.** The application must ensure that any data processed or transferred is free from duplication or inconsistencies.
- **SR-8.** The application must have safeguards in place to maintain the accuracy of the transferred data.

- **SR-9.** The application must validate CSV data thoroughly before upload to prevent corrupted or incomplete data entries.
  - Rationale: Ensures that only valid, complete, and accurate data enters the application to prevent faulty analysis.
  - Fit Criterion: The application shall reject any data that does not meet the validation criteria.
  - Traceability: FR-3, FR-4.

#### 6.3 Privacy Requirements

- **SR-10.** All personal information related to experimental participants or stakeholders, if applicable, must be anonymized and handled in accordance with relevant privacy laws and regulations.
- **SR-11.** The application must restrict data sharing with external parties unless expressly authorized by stakeholders, and users must be fully informed about the privacy policies.
- **SR-12.** The application must monitor database storage capacity and alert administrators when thresholds are reached to prevent application crashes.
  - Rationale: Ensures the application continues operating smoothly by addressing storage limits proactively.
  - Fit Criterion: The application shall send alerts when storage capacity exceeds 80% usage.
  - Traceability: PR-12, PR-13.

#### 6.4 Audit Requirements

- **SR-13.** The application must maintain a comprehensive audit trail, logging all access and modification events, including timestamps and identities of users performing actions.
- SR-14. Audit logs must be securely stored and accessible only by authorized personnel.
- **SR-15.** The application must display real-time error logs to users to enhance troubleshooting when applicable.
  - Rationale: Ensures users are informed about application issues and can take corrective action promptly.
  - Fit Criterion: All errors must be logged and displayed clearly to users in real-time.
  - Traceability: FR-12, MSR-5.

#### 6.5 Immunity Requirements

**SR-16.** The application must have proactive measures to detect and mitigate suspicious activities, such as repeated unauthorized access attempts, ensuring the application remains secure at all times.

**SR-17.** Real-time monitoring and optimization of application resources must be implemented to avoid crashes due to resource overload.

- Rationale: Prevents application downtime by ensuring efficient use of CPU and memory.
- Fit Criterion: The application must manage memory and CPU usage dynamically to avoid overloads.
- Traceability: PR-4, PR-9.

### 7 Roadmap

The following table outlines a proposed roadmap of when each safety requirement will be implemented within the capstone timeline and justifications.

Stage	Req. Category	Req. ID(s)	Rationale
PoC Demo (Nov 11)	Access	N/A	The PoC plan will not consider user access features at this time.
	Integrity	SR-5, SR-6, SR-7, SR-8, SR-9	The database must adhere to these requirements for a successful PoC.
	Privacy	N/A	Since the PoC plan will
	Audit	N/A	only have the database
	Immunity	N/A	these requirements are not applicable.
Rev0 Demo (Feb 3)	Access	SR-1	User authentication should be implemented during front-end development.
	Integrity	N/A	The crucial integrity requirements will have already been implemented by the PoC demo.
	Privacy	SR-10, SR- 11	At this point there will be user access, thus these requirements must be implemented.
	Audit	N/A	These requirements
	Immunity	N/A	are not high-priority.

Stage	Req. Category	Req. ID(s)	Rationale
Rev1 Final Demo (Mar 24)	Access	SR-2, SR-3	User access must be extended to permissions and capabilities prior to release.
	Integrity	N/A	The crucial integrity requirements will have already been implemented by the PoC demo.
	Privacy	SR-12	This requirement is necessary for system availability and robustness to extend past capstone.
	Audit	SR-15	Client and users must be informed about sys- tem issues and be able to troubleshoot even with- out the original develop- ment team.
	Immunity	SR-17	This requirement is necessary for system availability and robustness to extend past capstone.
Future considerations	Access	SR-4	This requirement is out of scope for the project timeline.
	Integrity	Integrity SR-11 This requirement of scope for the timeline.	
	Privacy	N/A	All privacy requirements have been covered.
	Audit	SR-13, SR- 14	These requirements would be nice-to-haves but are not essential for the project.
	Immunity	SR-16	This requirement is out of scope for the project timeline.

Table 3: Roadmap of the implementation of the safety and security requirements.

## Appendix — Reflection

#### [Not required for CAS 741—SS]

- 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?