Hazard Analysis
SFWRENG 4G06 Capstone Design Project

Team #18, InfiniView-AI
Anhao Jiao
Kehao Huang
Qianlin Chen
Qi Shu
Xunzhou Ye

20 October 2023

Table 1: Revision History

Date	**Developer(s)**	**Change**
13 October 2023	AJ, KH, QC, QS, XY	Initial draft
15 October 2023	AJ, KH, QS, XY	System Boundaries and Components, Critical Assumptions, Failure Mode and Effect Analysis, Safety and Security Requirements
	QC	Introduction, Scope and Purpose of Hazard Analysis
19 October 2023	AJ, KH, QS, XY	Failure Mode and Effect Analysis, Safety and Security Requirements, Roadmap
	QC	Introduction, Scope and Purpose of Hazard Analysis
25 March 2024	AJ, KH, QC, QS, XY	Rev1

Contents

1 Introduction **1**
- 1.1 Glossary . . . 1
- 1.2 Symbolic Constants . . . 1

2 Scope and Purpose of Hazard Analysis **2**

3 System Boundaries and Components **2**
- 3.1 System Components . . . 2
- 3.2 Environment Components . . . 2

4 Critical Assumptions **3**
- 4.1 Potential Mitigation Strategies . . . 3

5 Failure Mode and Effect Analysis **4**

6 Safety and Security Requirements **9**
- 6.1 Performance Requirements . . . 9
  - 6.1.1 Speed Requirements . . . 9
  - 6.1.2 Reliability and Availability Requirements . . . 9
  - 6.1.3 Scalability of Extensibility Requirements . . . 11
  - 6.1.4 Health and Safety Requirements . . . 11
- 6.2 Security Requirements . . . 12

7 Roadmap **12**

8 References **13**

List of Tables

1 Revision History . . . i
3 Symbolic constants in Hazard Analysis . . . 1
5 FMEA table . . . 5

1 Introduction

In alignment with the foundational principles laid out by Leveson [1], ~~a "hazard" within the context of our Tai Chi instruction platform can be identified as any inherent property or external condition. It could potentially cause the system to deviate from its intended functionality, particularly when interacting with various environmental factors.~~ a 'hazard' within the context of our Tai Chi instruction platform refers to any condition, event, or circumstance that could adversely affect the system's operation, integrity, or safety. This includes software malfunctions, hardware failures, user errors, or external disruptions. A hazard becomes a concern when it has the potential to interfere with the platform's ability to deliver instructional content effectively or to maintain a safe, secure, and engaging learning environment for the users

This document is dedicated to a comprehensive hazard analysis of our innovative Tai Chi video conferencing application, identifying the hazards and emphasizing the appropriate actions for the hazards.

1.1 Glossary

Tai Chi A classical Chinese martial art system practiced for health promotion and rehabilitation.

Instructor A person who teaches a Tai Chi class through an online conference system.

Practitioner A person who learns Tai Chi through an online conference system.

Machine Learning Model A mathematical model designed to find patterns and make predictions or decisions based on data

Annotation Pipeline A sequence of processing elements connected in series, which are responsible for generating annotations

SFU Selective Forwarding Unit, a component in real-time communication systems like WebRTC that routes and selectively forwards audio and video streams from one participant to others

STUN/TURN servers A component in real-time communication systems that is responsible for establishing and maintaining connections.

1.2 Symbolic Constants

Table 3: Symbolic constants in Hazard Analysis

Symbol	Value
MAX_DELAY	500 ms
MIN_RES	720p

2 Scope and Purpose of Hazard Analysis

This document describes the scope and purpose of hazard analysis for our WebRTC-based Tai Chi instruction application, focusing on identifying potential hazards within specific system boundaries and components, and prescribing comprehensive mitigation strategies. While acknowledging that users' diverse hardware configurations are beyond our control, the system is designed for broad compatibility, assuming standard web browser functionality on the user's device. Our analysis operates under the critical assumption that all application functionalities, particularly those related to real-time instructional mechanics, are performing as intended, thereby circumventing the need to predict various user inputs. Emphasis is placed on fortifying key components—backend server and UI—against potential failures. Through this analysis, we commit to ensuring an uninterrupted, secure, and user-centric experience, essential for the virtual dissemination and mastery of Tai Chi practices.

3 System Boundaries and Components

The system's boundaries are carefully defined to provide a clear understanding of the components that interact with and are integral to our Tai Chi video-conferencing application. These boundaries primarily encompass two categories of components: System Components and Environment Components.

By outlining system boundaries and components, we aim to establish a framework for hazard analysis that emphasizes the interplay between these key components and the broader environmental factors. This holistic approach allows us to identify and address potential hazards effectively while working to maintain the application's integrity and user satisfaction.

3.1 System Components

- Client application
- Signaling and media stream routing unit
- Machine learning annotation pipeline

System Components comprise the essential elements that constitute our application. These components are at the core of the system's functionality, facilitating user interactions, data routing, and real-time machine learning-based annotations.

3.2 Environment Components

- Personal computing devices
- Media capturing device

Environment Components encompass the external factors that influence the system's operation. These components are external to the system but play a critical role in ensuring a seamless and productive user experience.

4 Critical Assumptions

To ensure that the hazard assessment and analysis process remains transparent, accountable, and adaptable to changing circumstances, the following assumptions are made:

1. While the system is designed to mitigate and handle unintentional user errors and common misuse scenarios, it may not be fully resilient against sophisticated, intentionally malicious activities designed to exploit system vulnerabilities or deceive advanced machine learning algorithms.

2. It is anticipated that users will share only legal content on the conferencing platform. Nevertheless, it is understood that there may be attempts to share abusive, criminal, or pornographic content, and measures should be considered to detect and prevent the dissemination of such materials.

3. It is assumed that users have the physical capability to interact with and operate the system. This does not preclude the exploration of accessibility options to ensure that the system is inclusive and accommodating of users with physical disabilities.

4. Hazard analysis for the media capturing device component is scoped to consider typical use cases, excluding extreme conditions outside the intended use of the platform.

5. ~~The user does not intentionally attempt to break the system, such as providing deceptive inputs that aim to trick machine learning models (adversarial attacks).~~

6. ~~Only legal content is shared on the conferencing platform. The user does not deliberately exploit the system to spread abusive, criminal, pornographic content.~~

7. ~~The user has no physical disability, meaning that users are presumed to have the physical capability to interact with and operate the system without encountering any limitations related to physical disabilities.~~

8. ~~Hazard analysis for the media capturing device component only applies to instructors.~~

4.1 Potential Mitigation Strategies

The landscape of cybersecurity and system integrity presents a multitude of challenges that require diligent anticipation and proactive management. Recognizing that no system can be entirely immune to adversarial actions, the following potential mitigation strategies have been identified. These strategies are designed to enhance the resilience of the platform, reduce the likelihood of malicious exploitation, and ensure the integrity and continuity of the service provided. While some may extend beyond the current scope of the capstone project, they are integral to a comprehensive approach to system security and user safety. The subsequent list delineates methods and practices that could be implemented to safeguard the platform against a range of adversarial threats.

1. Implement Robust Input Validation: Use strong input validation checks to ensure that only expected types of data are processed by the system. This can help prevent a variety of injection attacks.

2. Employ Anomaly Detection: Utilize machine learning models for anomaly detection to identify unusual patterns that may indicate adversarial behavior.
3. Rate Limiting and CAPTCHA: Implement rate limiting to prevent automated attacks and CAPTCHA challenges to distinguish between human and automated access.
4. User Behavior Analytics: Analyze user behavior to identify potentially malicious actions and have measures in place for a quick response.

5 Failure Mode and Effect Analysis

In the Failure Mode and Effect Analysis (FMEA) section, we employ a structured methodology to systematically identify potential failure modes, assess their effects, and prioritize recommended actions to mitigate hazards and enhance the safety and performance of our Tai Chi video conferencing application. Table 5 summaries the FMEA for our project.

Table 5: FMEA table

Component	Failure Mode	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
Client Application	Unauthorized access to media capturing devices	Invasion of user privacy	Lack of considerations for user privacy in the design process	• Ask for permission to access media capturing devices • Have an indicator when a media capturing device is in use • Revoke access as soon as the capturing device is no longer needed	**SR4**, **SR5**	H1-1
	Unresponsive UI	The user interface is unresponsive to the user interaction	• Delayed response from the server • Insufficient client-side resource	• Design the system with redundant processing capacity in mind • Test with workload larger than that in the expected usage scenario	PR1	H1-2
Signaling and Stream Routing Unit	Signaling server down	New WebRTC connections cannot be established	Server hardware failures	Configure the system to automatically switch to a backup signaling server when the primary server experiences downtime.	**PR9**	H2-1
	SFU overload	• Decreased video and audio quality • Session crashes	• Unexpected spikes in number of participants • Insufficient resource	• Conduct stress tests to determine the system's maximum capacity. • Once reaches the maximum capacity, the system will put new requests for creating or joining sessions on hold.	PR2, PR6	H2-2

continue on next page ...

Component	Failure Mode	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
ML Annotation Pipeline	Inaccurate annotation produced	~~Negatively impact learning outcomes.~~Inaccurate annotation produced leads to misaligned or incorrect information being associated with the learning content. This can cause confusion, misunderstandings, and the potential propagation of misinformation among users, hindering their ability to accurately learn and apply new knowledge.	• Corrupted input data. • Low-fidelity input data.	• Set a confidence threshold. Refuse to process if below the threshold. Forward feedback to the front end. • Increase allowance/tolerance of "bad" data, increase the robustness of the annotation pipeline.	**PR12**	H3-1

continue on next page . . .

Component	Failure Mode	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
	Latency in Annotation	~~Negatively impact learning outcomes.~~Latency in annotation may result in delayed synchronization between the educational content and its corresponding annotations. This can disrupt the learning flow, reduce engagement, and prevent timely comprehension of the material presented. Users may experience frustration and a lack of continuity that can diminish the overall effectiveness of the learning session.	• Heavy system load, inefficient machine learning model • The high volume of render requests.	• Improve the efficiency of the machine learning model. • Allocate additional resources to accommodate higher loads.	**PR14**	H3-2
Personal Computing Device	The application is not running correctly	App crashed	• Insufficient running memory. • Outdated OS version.	Automatically save conference metadata, try to reconnect after the application restart.	HS1, **PR7**	H4-1
	Network Interruption	Client-Server connection lost	No internet connection on the user's side.	Retry connection after a predetermined delay.	**PR7**	H4-2
	Network stability fluctuation	Inefficient bit rate and low-resolution	Unstable internet connection on the user's side	• Monitor network quality in real-time. Warn users if instability is detected. • Put user on hold if network problem persists.	**PR8**	H4-3
Media Capturing Device	Device lost connection	Loss of source video stream	A malfunctioning physical device or loose device connection	Send warnings to users when video or audio devices are disconnected	**PR10**	H5-1

continue on next page . . .

Component	Failure Mode	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
	Vision obscured	Part of the instructor's body is invisible from the perspective of the video-capturing device	Misplaced capturing device; The user moves or rotates the video-capturing device by accident	Send warnings to the user when no full human body is detected in the capturing device	**PR15**	H5-2
	Insufficient resolution	Low-fidelity output data	Limited hardware capability	• Perform hardware capability examination, and warn the user if incapable hardware detected • Specify and notify the user of the minimum system requirements/environment for running the application	**PR11**	H5-3
	Multiple devices detected	The client application is unable to select the correct media-capturing device	Multiple media-capturing devices are connected to the machine running the application	Send warnings to the user when multiple media capturing devices are detected, and ask users to select the one they wants to use	**PR13**	H5-4

6 Safety and Security Requirements

New requirements identifiers are highlighted in bold.

6.1 Performance Requirements

6.1.1 Speed Requirements

PR1 The system shall respond to user interactions (e.g. button clicks, menu selections) within 1 second.

Rationale To provide a responsive and smooth user experience.

Fit Criteria User interactions result in near-instantaneous system responses under typical conditions.

Priority Medium

PR14 The system shall provide annotations with minimal delay, ensuring real-time alignment with the instructor's live stream.

Rationale To ensure the highest quality of instructional annotations that effectively enhance the user experience and learning process. The latency of annotation should not be noticeable.

Fit Criteria The generated annotation should have less than MAX_DELAY latency between the stream image and annotation.

Priority High

6.1.2 Reliability and Availability Requirements

PR2 The signaling server, SFU, and STUN/TURN servers shall operate with high reliability, minimizing service interruptions during live sessions.

Rationale To ensure a consistent and uninterrupted learning experience for users.

Fit Criteria Real-time communication services are always available.

Priority High

PR7 The system shall be able to resume the previous session when the session is accidentally terminated due to an application crash or internet interruption.

Rationale To enhance the overall user experience by minimizing disruptions caused by unforeseen events.

Fit Criteria The system shall automatically save snapshots of conference metadata, try reconnecting after the application successfully restarts or internet access resumes.

Priority Medium

PR8 The system shall monitor the user's network quality while the user is using the application.

Rationale To ensure the conference quality of other users.

Fit Criteria The system shall warn the user if network instability is detected, and put the user on hold if the issue persists.

Priority Medium

PR9 ~~The system shall be running when the primary signaling server is down.~~The core functionalities of the system(starting the session, joining the session, getting annotated video) shall remain operational in the event that the primary signaling server is down.

Rationale ~~To enhance system resilience and reliability and reduce system downtime.~~ This requirement is to enhance system resilience and reliability by ensuring that essential services can continue without interruption, thereby reducing system downtime.

Fit Criteria A redundant signaling server shall be maintained alongside the primary signaling server, and shall be deployed when the primary signaling server is down.

Priority Medium

PR10 The system shall send warnings to users when video/audio capturing devices are disconnected.

Rationale The source video stream from the instructor is essential for a demonstrational conference session. If these devices become disconnected without warning, users may not be aware of the issue, leading to confusion and frustration.

Fit Criteria The system should send clear and user-friendly warnings or notifications when it detects the disconnection of video or audio capturing devices.

Priority Critical

PR11 The system shall ensure that the quality of the video stream captured meets the minimum resolution requirement.

Rationale To ensure the quality of the input data to the ML pipeline.

Fit Criteria The system shall perform hardware capability examination in any detected and authorized video capturing device, and notify users of the required resolution rate of MIN_RES.

Priority Critical

PR12 The system shall generate accurate annotation on top of the user's live stream.

Rationale To ensure the highest quality of instructional annotations that effectively enhance the user experience and learning process. The generated annotation should be accurate enough.

Fit Criteria The system should generate annotation that meets 4 out of 5 team members' accuracy expectations. The accuracy expectations can be met by team members manually checking the annotation.

Priority High

PR13 The system shall use the media capturing devices the user specified when multiple types of capturing devices are detected.

Rationale To ensure the user experience, users should be able to specify the media capturing device they want to use.

Fit Criteria When the system detects the presence of multiple media capturing devices of the same type (e.g. cameras, microphones), it shall display a notification to inform the user of this condition. The system will then prompt the user to select which media capturing device to utilize through a device selection form. This form shall allow the user to choose between the available devices of each type that were detected. Upon submission of the form, the chosen media capturing devices will be activated for use within the application.

Priority Medium

PR15 The system shall make sure the view of the subject is within the field of view of the media capturing device.

Rationale Having a complete view of the subject's body ensures the quality of data feeding into the system for analyzing human body motions.

Fit Criteria The system shall present detailed instructions for the user to properly set up the media capturing device, making sure the body of the subject is fully visible from the perspective of the camera.

Priority Critical

6.1.3 Scalability of Extensibility Requirements

PR6 The Selective Forwarding Unit (SFU) shall be scalable to accommodate an increasing number of simultaneous video streams as the user base grows.

Rationale To support a growing user community without performance degradation.

Fit Criteria The SFU can handle AT least 10 simultaneous video streams during peak usage.

Priority Medium

6.1.4 Health and Safety Requirements

HS1 The system shall not cause the computers to overload.

Rationale The system should not overload the users' computers.

Fit Criteria The hardware running the system is under normal temperature.

Priority Medium

HS2 The system shall not affect users' physical and mental health.

Rationale The system must not harm users' health and safety.

Fit Criteria Users feel comfortable using the system in various situations.

Priority Critical

6.2 Security Requirements

SR4 The system shall access media capturing devices only when user permission is granted.

Rationale To protect user privacy

Fit Criteria A dialogue shall be displayed to ask for user permission to access media capturing devices.

Priority Critical

SR5 The system shall ensure the user is always aware of any active media capturing device.

Rationale To protect user privacy

Fit Criteria An indicator shall be presented for each active media capturing device.

Priority Critical

SR6 The system shall not retain access to any media capturing device when they are not needed for video conferencing sessions.

Rationale To protect user privacy

Fit Criteria The access to any media capturing device is terminated as soon as the session ends or the user exits the session.

Priority Critical

7 Roadmap

In the hazard analysis documentation for our Tai Chi video conferencing application, we have identified and prioritized a comprehensive set of safety and security requirements together with other non-functional requirements through the process of discovering potential hazards. These requirements are essential for mitigating potential hazards, ensuring the reliability and integrity of our system, and creating a secure and user-centric experience.

Requirements that address fundamental safety and security concerns, such as user privacy, system reliability, and user well-being, are given critical priority. These requirements include **PR10**, **PR11**, **PR15**, HS2, **SR4**, **SR5**, and **SR6**. Requirements related to the seamless operation of our system during both normal and unforeseen events, such as system crashes or network interruptions, are considered high priority. These requirements include **PR14**, PR2, and **PR12**. Requirements that focus on system performance, scalability, and the quality of user experience are rated as medium priority. PR1, PR6, **PR7**, **PR8**, **PR9**, **PR13**, and HS1 fall under this category.

Given the limited time and human resource within the capstone project timeline, all requirements of "critical" priority shall be implemented by the end of the capstone project. Other requirements with lower priorities could be met by future implementations. This roadmap will serve as a guide to ensure that our Tai Chi video conferencing application evolves in a way that aligns with our commitment to safety, security and user satisfaction.

8 References

[1] N. Leveson, Engineering a safer world: systems thinking applied to safety (Engineering systems). Cambridge, Mass: MIT Press, 2011, 534 pp., OCLC: ocn719429220, ISBN: 978-0-262-01662-9. [Online]. Available: https://direct.mit.edu/books/oa-monograph/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied.