Prevent, Mitigate, and Recover (PMR) Insight

Collective Knowledge System (PICK)

Software Design Document

Version 1.7

3/9/2020

Document Control

Approval

The Guidance Team and the customer shall approve this document.

Document Change Control

|  |  |
| --- | --- |
| Initial Release: | 0.1 |
| Current Release: | 1.0 |
| Indicator of Last Page in Document: | % |
| Date of Last Review: | 3/9/20 |
| Date of Next Review: | 3/10/20 |
| Target Date for Next Update: | 3/11/20 |

Distribution List

This following list of people shall receive a copy of this document every time a new version of this document becomes available:

Guidance Team Members:

Dr. Gates

Dr. Salamah

Dr. Roach

Steven Roach

Jake Lasley

Customer: Dr. Oscar Perez

Vincent Fonseca

Herandy Denisse Vazquez

Baltazar Santaella

Florencia Larsen

Erick De Nava

Software Team Members:

Abel Rodriguez

Elizabeth Barragan

Jose A. Leon Cordero

Yamel E. Hernandez

Manuel Delgado

Change Summary

The following table details changes made between versions of this document

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Modifier | Description |
| 1.0 |  |  | Creation of Document |
| 1.1 | 03-06-2020 | Manuel | Completed Document Control Details and Section 1.2 |
| 1.2 | 3/7/20 | Yamel | Sec 1.5 & Sec 3 Intro |
| 1.3 | 3/9/2020 | Antoine | Added 3.1 |
| 1.3 | 3/9/20 | Yamel | Filled in Sec 1.4, Sec 2 Ingestion Subsystem, & Sec 3 Ingestion Subsystem |
| 1.3 | 03-09-2020 | Manuel | Added section 3.4, intro to section 2, section 2.3 |
| 1.3 | 3/9/20 | Elizabeth | Added full Sec. 4, Sec 3.5 |

Table of Contents

[Document Control ii](#_Toc34675518)

[Approval ii](#_Toc34675519)

[Document Change Control ii](#_Toc34675520)

[Distribution List ii](#_Toc34675521)

[Change Summary ii](#_Toc34675522)

[1. Introduction 1](#_Toc34675523)

[1.1. Purpose and Intended Audience 1](#_Toc34675524)

[1.2. Scope of Product 1](#_Toc34675525)

[1.3. References 1](#_Toc34675526)

[1.4. Definitions, Acronyms, and Abbreviations 1](#_Toc34675527)

[1.4.1. Definitions 1](#_Toc34675528)

[1.4.2. Acronyms 2](#_Toc34675529)

[1.4.3. Abbreviations 2](#_Toc34675530)

[1.5. Overview 2](#_Toc34675531)

[2. Decomposition Description 3](#_Toc34675532)

[2.1. System Collaboration Diagram 3](#_Toc34675533)

[2.2. Subsystem and Component Descriptions 3](#_Toc34675534)

[2.3. Dependencies 3](#_Toc34675535)

[3. Detailed Description of Component <name> 4](#_Toc34675536)

[3.1. User Interface Subsystem 4](#_Toc34675537)

[3.1.1. Graphical User Interface Class 4](#_Toc34675538)

[3.2. Ingestion 5](#_Toc34675539)

[3.2.1. OCR 6](#_Toc34675540)

[3.2.2. Audio Transcriber 6](#_Toc34675541)

[3.2.3. Splunk 6](#_Toc34675542)

[3.3. Vector 6](#_Toc34675543)

[3.4. Splunk 7](#_Toc34675544)

[3.4.1. Sign In 7](#_Toc34675545)

[3.4.2. Send Log Files 8](#_Toc34675546)

[3.4.3. Check Delta 8](#_Toc34675547)

[3.4.4. Retrieve Log Entries 8](#_Toc34675548)

[3.4.5. Search 8](#_Toc34675549)

[3.4.6. Validate 9](#_Toc34675550)

[3.5. Storage Subsystem 9](#_Toc34675551)

[Database Class 9](#_Toc34675552)

[Version Control 9](#_Toc34675553)

[4. Database 11](#_Toc34675554)

[4.1. Database Schema 11](#_Toc34675555)

[4.1.1. ER Diagram 11](#_Toc34675556)

[4.1.2. ER Crow’s Notation 12](#_Toc34675557)

# Introduction

## Purpose and Intended Audience

<< document purpose: system design. Describe the intent behind this document >>

The purpose of creating the software design document is ...

The purpose of this document is to inform future maintainers on the description, collaborations, and protocols of each of our PICK system’s subsystems and components for future changes to the system. The document will go over the descriptions of each subsystem and component, along with the classes’ and collaborations’ descriptions associated with them. The collaborations will depict and explain which set of classes and contracts are grouped together, what data is sent to each class through the contracts, and the end result desired by the collaboration. Lastly, protocols will be an in-depth explanation of each collaboration’s method call in the system that will allow the maintainer to understand how to call a method, the inside workings of the that method, and the expected result outcome of the method.

## Scope of Product

The Lethality, Survivability, and HSI Directorate (LSH) recognizes the complexity and the time it takes to analyze the applicable logs, observation notes, and other artifacts gathered from an adversarial assessment from the red, blue, and white teams and generate a report that presents the events that took place during the adversarial assessment. They want a system that would aid their analysts in correlating red team’s activities to blue team’s responses and represent the events that took place during an adversarial assessment graphically.

The University of Texas at El Paso (UTEP) and LSH are collaborating to develop Prevent, Mitigate, and Recover (PMR) Insight Collective Knowledge System (PICK) that will provide the ability to correlate red team’s activities to blue team’s responses and graphically represent the events that took place during an adversarial assessment.

## References

[1] 08c\_SDD\_Outline.pdf

[2] 09Subsystems.pdf

[3]“Entity–relationshipmodel,”Wikipedia,09-Mar-2020.[Online].Available: <https://en.wikipedia.org/wiki/Entity–relationship_model>. [Accessed: 10-Mar-2020].

[4] SDD\_detailed\_component\_table\_template.docx

## Definitions, Acronyms, and Abbreviations

### Definitions

|  |  |
| --- | --- |
| **Data Cleansing** | Data cleansing is the removal of unwanted characters from uncleansed TMUX log file; removal of blank rows from uncleansed excel log file; and removal of blank lines from uncleansed log file. |
| **Data Validation** | Data validation is the process of inspecting data in the cleansed log files based on predefined data validation rules. |
| **Log Entry** | Splunk takes the validated log files and convert them into normalized data. The normalized data are called log entries. Users of the system can filter and edit log entries. |
| **Significant Log Entry** | A log entry selected by the user and associated with a vector. The attributes are the same as for a log entry. The system stores significant log entries. Splunk stores log entries in the normalized data files. |
| **Timestamp** | Denotes time in hours:minutes, date in month:date:year, and section in am/pm. |

### Acronyms

|  |  |
| --- | --- |
| **PICK** | Prevent, Mitigate, and Recover (PMR) Insight Collective Knowledge System |
| **UTEP** | University of Texas at El Paso |
| **LSH** | Lethality, Survivability, and HSI Directorate |
| **PMR** | Prevent, Mitigate, and Recover |
| **UI** | User Interface |
| **GUI** | Graphical User Interface |
| **OCR** | Optical Character Reader |

### Abbreviations

|  |  |
| --- | --- |
|  |  |
|  |  |

## Overview

The document will be composed of a detail description of our overall system. Section 2 will discuss how we decomposed our system into subsystems and components, that will go into details of their purpose and who they collaborate with. Section 3 will discuss the details of the components, their design, their contracts and their protocols. Lastly section 4 will discuss the database used and its schema on how it will contribute to the system.

# Decomposition Description

The overall descriptions for each component will describe how within the system, subsystems interact with each other. It will abstractly and concisely inform the reader what functions the specific component is in charge of displaying.

## System Collaboration Diagram

## Subsystem and Component Descriptions

<< Provide a description of subsystems and components in the diagrams in section 2.1. For each component or subsystem to be described in this document, give the name, describe the purpose, and list the contracts supported by this component (e.g., the subsystem contracts). Indicate where in the following detailed sections of this document each component is discussed. >>

## Dependencies

Components for optical character reader and audio transcriber have not yet been looked at individually therefore it impacts the time it will take to complete a detailed collaboration diagram. To take advantage of all the capabilities Splunk has to offer, there needs to be a considerable amount of time spent on understanding the parsing methods and the configuration files Splunk uses internally. We depend on understanding these components in order to deliver an optimize system.

# Detailed Description of Components

The following section will describe the system’s components with their functionalities and contracts with other components.

## User Interface Subsystem

This section describes the UI subsystem of the PICK system. The purpose of the UI subsystem is to present the PICK system to the user and provide a way for the user to interact with the system.

The following is the Collaboration Diagram of the UI subsystem:

A close up of text on a white background

Description automatically generated

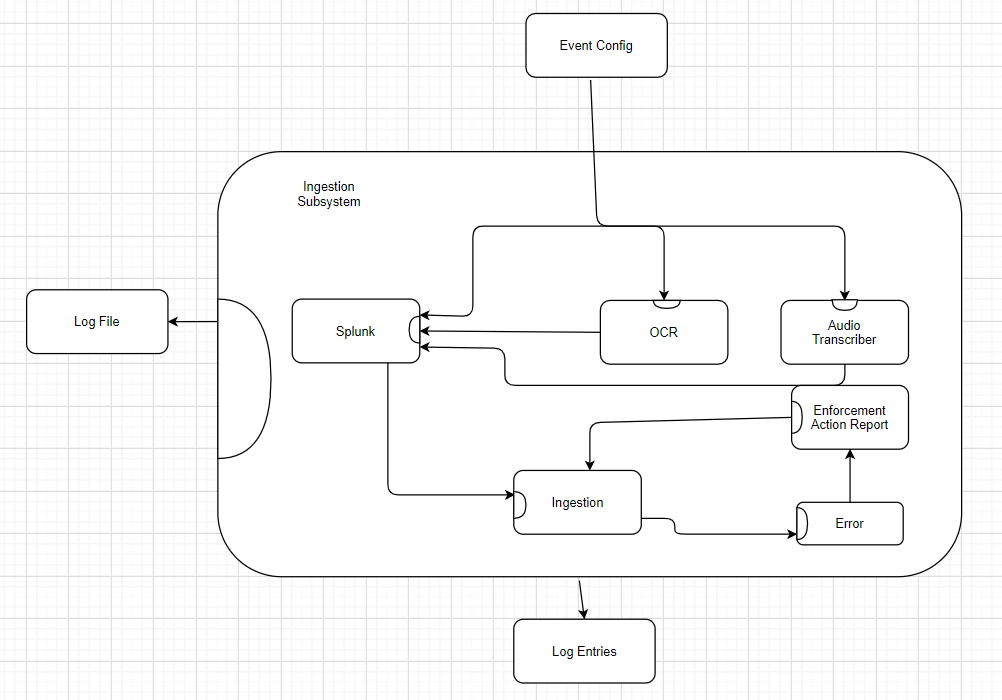
### Graphical User Interface Class

The GUI class leverages the PyQt5 Python framework to present the PICK system graphically. The GUI class is not a sub-class or superclass – it is broken down into several helper classes. Each helper class makes up one window or one PyQt5 frame. This is done to avoid coupling while maintaining cohesion of the GUI subsystem.

|  |  |
| --- | --- |
| **Class Name**: User Interface Class | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * Know current window format * Know which object * Display current window * Display object(s) info needed for current window * Can update object info on current window | |
| **Contract:** 1. Can receive user input | |
| **Responsibilities** | **Collaborations** |
| 1. Manipulate object’s info |  |

## Ingestion

The following section will depict and describe how the Ingestion subsystem The purpose of the ingestion subsystem is to provide a method for the user to ingest files into the system.



**Figure 3.2:** Ingestion Collaboration Diagram

|  |  |
| --- | --- |
| **Class Name**: Ingestion | |
| **Superclass**: None | |
| **Subclasses**: None | |
| **Private Responsibilities**   * Cleanse log files * Validate log files * Ingest log files | |
| **Contract:** Scan for Changes | |
| **Responsibilities** | **Collaborations** |
| 1. Scan for changes to log files | Event Configuration (2) |
| **Contract**: 2. Provide Some Attributes | |
| **Responsibilities** | **Collaborations** |
| 1. Know validation parameters 2. Know log file directories | Event Configuration (1)  Event Configuration (2) |

### OCR

|  |  |
| --- | --- |
| **Class Name**: OCR | |
| **Superclass**: None | |
| **Subclasses**: None | |
| **Private Responsibilities**   * Know how to parse files that are in an OCR format | |
| **Contract:** | |
| **Responsibilities** | **Collaborations** |
|  |  |
| **Contract**: | |
| **Responsibilities** | **Collaborations** |
|  |  |

### Audio Transcriber

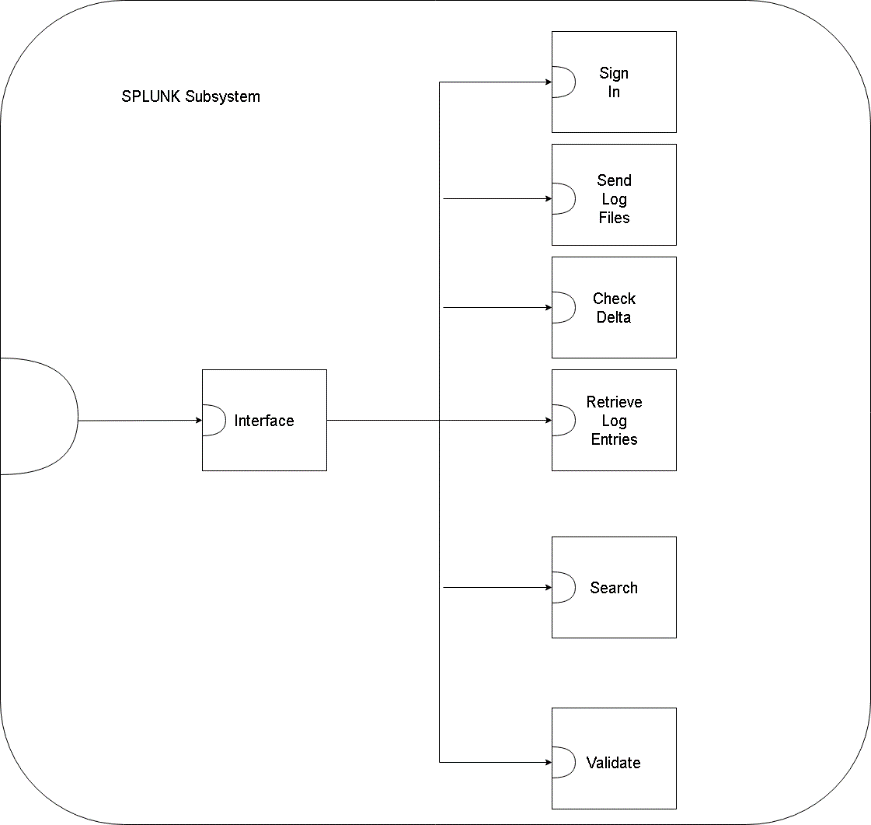
|  |  |
| --- | --- |
| **Class Name**: Audio Transcriber | |
| **Superclass**: None | |
| **Subclasses**: None | |
| **Private Responsibilities**   * Know how to parse files that are audio files | |
| **Contract:** | |
| **Responsibilities** | **Collaborations** |
|  |  |
| **Contract**: | |
| **Responsibilities** | **Collaborations** |
|  |  |

### Splunk

|  |  |
| --- | --- |
| **Class Name**: Splunk | |
| **Superclass**: None | |
| **Subclasses**: None | |
| **Private Responsibilities**   * Parse files | |
| **Contract:** | |
| **Responsibilities** | **Collaborations** |
|  |  |
| **Contract**: | |
| **Responsibilities** | **Collaborations** |
|  |  |

## Splunk

The following section will display a semi complete collaboration graph for a subsystem identified as Splunk.



**Figure 3.4:** Splunk Subsystem

### Sign In

|  |  |
| --- | --- |
| **Class Name**: Sign In | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * Know user information to connect to Splunk | |
| **Contract:** 1. Log In | |
| **Responsibilities** | **Collaborations** |
| 1. Create a log in instance to access Splunk. |  |

### Send Log Files

|  |  |
| --- | --- |
| **Class Name**: Send Log Files | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * Send log files to Splunk | |
| **Contract:** Send Log Files | |
| **Responsibilities** | **Collaborations** |
| 1. Log in 2. Know directory 3. Know which files to send | Sign In (1)  Something ()  Something else () |

### Check Delta

|  |  |
| --- | --- |
| **Class Name**: Check Delta | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * Check for new files in defined directories, update log entries. | |
| **Contract:** 1. Delta Check | |
| **Responsibilities** | **Collaborations** |
| 1. Know previous state of directories |  |

### Retrieve Log Entries

|  |  |
| --- | --- |
| **Class Name**: Retrieve Log Entries | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * Return log entries | |
| **Contract:** | |
| **Responsibilities** | **Collaborations** |
| 1. Log in 2. Send log entries | Sign in (1) |

### Search

|  |  |
| --- | --- |
| **Class Name**: Search | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * Get the results desired and return them to the user | |
| **Contract:** Search | |
| **Responsibilities** | **Collaborations** |
| 1. Log in 2. Search | Sign In (1)  User Interface |

### Validate

|  |  |
| --- | --- |
| **Class Name**: Validate | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * Accept log files that fall within parameters | |
| **Contract:** Validate | |
| **Responsibilities** | **Collaborations** |
| 1. Log in 2. Know validation parameters | Sign In (1)  Event Configuration () |

## Vector

|  |  |
| --- | --- |
| **Class Name**: A | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * Know some attribute | |
| **Contract:** 1. Print Information | |
| **Responsibilities** | **Collaborations** |
| 1. Do something | B (3) |
| **Contract**: 2. Provide Some Attributes | |
| **Responsibilities** | **Collaborations** |
| 1. Know Something 2. Know another thing | X (7) |

|  |  |
| --- | --- |
| **Class Name**: B | |
| **Superclass**: | |
| **Subclasses**: | |
| **Contract 3:** Calculation | |
| **Responsibilities** | **Collaborations** |
| 1. Do some calculation |  |

## Storage Subsystem

A screenshot of a cell phone

Description automatically generated

### Database Class

|  |  |
| --- | --- |
| **Class Name**: Database | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * Creates tables * Updates changes in log files, log entries in tables | |
| **Contract:** Database | |
| **Responsibilities** | **Collaborations** |
| 1. Reads log files, log entries from tables 2. Insert log files, log entries into tables 3. Deletes log files, log entries from tables | Version Control (3,4)  Version Control (3,4)  Version Control (3,4) |

### Version Control

|  |  |
| --- | --- |
| **Class Name**: Version Control | |
| **Superclass**: | |
| **Subclasses**: | |
| **Private Responsibilities**   * None | |
| **Contract:** Version Control | |
| **Responsibilities** | **Collaborations** |
| 1. Merge network changes to project database 2. Merge local changes to project database 3. Track changes to database | Networking (1)  Networking (1)  Signal Controller (1,2) |

# Database

## Database Schema

This section describes and demonstrates the use of a database in our system. In our system the handling of log files will be crucial, in order to keep track of the original log files, log entries produced from the log files, its node structure and the vectors in which they belong to, a database will be used as a storing mechanism. The database will be also utilized to retrieve the stored contents for a user to manipulate and create visualizations through our system’s interface. This section displays the Entity Relationship (ER) diagram along with the crow’s notation.

### ER Diagram

A picture containing text

Description automatically generated**Figure n:** ER Diagram of the project database

### ER Crow’s Notation

A screenshot of a map

Description automatically generated

**Figure n:** ER Diagram Crow’s Notation

%