**Requirements Analysis Document (RAD)**

**Access Control Subsystem (ACS)**

**for the**

**Predictive Wastewater Management System (PWMS)**

**Phase 1.0**

Prepared by

Fairleigh Dickinson Software Development - Analysis Team

**Security Notice**: The information contained within this document is Restricted. Unauthorized disclosure is prohibited. Failure to observe policy regarding proprietary information can result in disciplinary action, including dismissal, as well as result in a violation of proprietary rights and subject you and/or third parties to legal liability.

Purpose

This document is intended as a “package” agreement between development groups

Document Control

Document History

|  |  |  |
| --- | --- | --- |
| Date | Version | Comments |
| 02/18/2015 | 1.0 | Initial draft |
| 03/25/2015 | 2.0 | Amendments of compliance with SQAP |
| 04/04/2015 | 2.1 | Document placed under formal |
| 04/04/2015 | 2.2 | Internal control |

Authors

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Title | Organization | Phone |
| Santhosh Kumar Devarakonda Kankurthy | ACS Lead | Fairleigh Dickinson University, Teaneck, NJ | 201-464-3590 |
| William Phillips | FDU faculty | CS Department | 201-247-2573 |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Title | Organization | Phone |
| Mark LaPlante | Product Manager | Eastech | 918-664-1212 |
| William Phillips | FDU Faculty | CS Department | 201-247-2573 |
| Amitha Peddi | SQA Engineer | FDU SQA | 336-848-8346 |

Sign Off List

|  |  |  |
| --- | --- | --- |
| Name | Title | Phone |
| Mark LaPlante | Product Manager | 918-664-1212 |
| Alfredo Tan | CS Department Chair | 2324 |
| Amitha Peddi | SQA Engineer | 336-848-8346 |

Document Sign Off

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Table of Contents

1 Introduction 4

1.1 Purpose of the System 4

1.2 Scope of the System 5

1.2.1 Actors 5

1.2.2 Subsystems 5

1.2.3 Context Diagram 6

1.3 Objectives and Success Criteria of the Access Control Project 6

1.4 Definitions, Acronyms and Abbreviations 6

1.5 References 7

1.6 Overview 7

2 Current System 8

3 Proposed System 9

3.1 Functional Requirements 9

3.2 Nonfunctional Requirements 9

3.2.1 Interface 9

3.2.2 Session maintenance 9

3.3 Scenarios 10

3.3.1 User Enrollment 10

3.3.2 Authentication and Authorization 10

3.4 Use Cases 10

3.4.1 Administer ACS 10

3.4.2 User Requests a Watchman Role 11

3.4.3 Data Gathering Requests Authentication and Authorization 13

3.4.4 Use Case Diagram 14

3.5 Object Model 15

3.5.1 ACSDGSInterface (Boundary) 15

3.5.2 ACSDASInterface (Boundary) 15

3.5.3 AASACSInterface (Boundary) 15

3.5.4 UserRequestInterface (Boundary) 15

3.5.5 ACSSAInterface (Boundary) 15

3.5.6 MemberControl (Control) 15

3.5.7 ACSControl (Control) 16

3.5.8 SAConfigControl (Control) 16

3.5.9 ConfigurationData (Entity) 16

3.5.10 ACLStorage (Entity) 16

3.5.11 Conceptual Class Diagram 17

3.6 User Interface – Screen Mock-Ups 18

4 Dynamic model 20

4.1 Administer ACS 20

4.1.1 Sequence Diagram 20

4.1.2 Communication Diagram 21

4.2 User Requests a Watchman Role 22

4.2.1 Sequence Diagram 22

4.2.2 Communication Diagram 23

4.3 Data Gathering Requests Authentication and Authorization 24

4.3.1 Sequence Diagram 24

4.3.2 Communication Diagram 24

# Introduction

This document describes functional model and object model for the Access Control Subsystem of the Predictive Wastewater Management System.

## Purpose of the System

The PWMS subsystem that maintains access control lists (ACLs) for the system actors and enables users to assume roles for the PWMS.

Access Control Subsystem (ACS):

* Accepts user requests
* Assigns roles to the new users
* Notifies events in the system
* Reports alerts

This Requirements Analysis Document (RAD) specifies the functional and first cut object model for this sub-system.

## Scope of the System

The context diagram for the Access Control Subsystem (ACS) of PWMS is shown in section .1.2.2 Figures 1. The Access Control Subsystem (ACS) shall support the actors shown in section 1.2.1.

### Actors

Access Control Subsystem (ACS) subsystem shall support the following actors.

|  |  |
| --- | --- |
| **Actor Catalog** | |
| **Actor Name** | **Description** |
| System Administrator | The System Administrator is an actor who adds and deletes users to and from the PWMS, assigns roles, and performs other system administration duties |
| Auditor | An actor that traces events and verifies the integrity of the stored data for the PWMS |
| Data Gatherer | An actor that provides (gathers) data to be analyzed by the PWMS from the FlowCells |
| User | An actor that requests permission to become a watchman or auditor for the PWMS |
| Watchman | The Watchman actor responds to alertable events created by the PWMS |
| Data Analyst | An actor that performs data analysis by creating and using adaptive optimization algorithms on the data managed by the PWMS |

### Subsystems

|  |  |
| --- | --- |
| **Subsystems** | |
| **Subsystem Name** | **Description** |
| DataGathering(DGS) | The PWMS subsystem that collects the data from the FlowCell participatory sensors. |
| DataAnalysis(DAS) | The PWMS subsystem that performs data reduction, analysis and provides reports for the Data Analyst |
| AuditAndAlert(AAS) | The PWMS subsystem that periodically surveys the PWMS data and alerts the Watchman of a potential emergency situation. Maintains a store of audit records for the PWMS for an audit report. |
| DataStorage(DSS) | The PWMS subsystem that stores and organizes the PWMS data for use by the DataGathering, DataAnalysis, and AuditAndAlert subsystems. |

### Context Diagram



1. Access Control Subsystem (ACS) context diagram

## Objectives and Success Criteria of the Access Control Project

A review checklist shall be created for this RAD document. Success of this project or shall be contingent upon the checklist criteria being met to the satisfaction of Eastech and Fairleigh Dickinson

## Definitions, Acronyms and Abbreviations

PWMS – Predictive Wastewater Management System

RAD – Requirements Analysis Document

ACS – Access Control Subsystem

AAS – Audit and Alert Subsystem

DAS – Data Analysis Subsystem

DGS – Data Gathering Subsystem

DSS – Data Storage Subsystem

SA – System Administrator

UML- Unified Modeling Language

## References

System Level Requirements Analysis Document for the Predictive Wastewater Management System (PWMS)

Bernd Bruegge and Allen H. Dutoit, *Object-Oriented Software Engineering: Using UML, Patterns and Java*, 3rd

Edition, Prentice Hall, 2010 (ISBN 0-13-606125-7)

Jacobson, Ivar *Object-Oriented Software Engineering-A Use Case Driven Approach.* Addison Wesley 1992.

Martin Fowler, *UML Distilled: A Brief Guide to the Standard Object Modeling Language,* 3rd ed., Addison

Wesley, 2003.

Roger S. Pressman, *Software Engineering: A Practitioner’s Approach*, 7th Edition, McGraw Hill, 2009 (ISBN

9780071267823)

Black and Veatch, Smart Integrated Infrastructure White Paper, September 23, 2014.

## Overview

The PWMS subsystem that maintains access control lists (ACLs) for the system actors and enables users to assume roles for the PWMS. This RAD will explain the requirements how Access Control subsystem interacts with other subsystems in the PWMS system and interaction with various users in the system. The roles (actors) of the PWMS shall be implemented by Access Control Subsystem (ACS) security system that handles authentication and authorization for PWMS.

Since we are using a scenario/use case based approach, modeling of the system shall begin with the creation of scenarios and these shall evolve into the use cases for the Access Control Subsystem (ACS).

# Current System

There is no current system in place for the PWMS. However, there are a number of applications involving participatory sensing systems and how those systems operate and can be made secure. The literature shall be thoroughly researched to leverage the state-of-the-art in implementing and securing the PWMS from unauthorized users.

# Proposed System

Our vision closely resembles the system described in the Black and Veatch Whitepaper. By employing the scenario/ use case driven approach we intend to define how end users will employ the system toward the measurement, monitoring, analysis and storage and role-enforcement functions of the PWMS.

## Functional Requirements

1. The ACS shall allow the System Administrator to add and delete users to and from the PWMS.
2. The ACS shall allow the System Administrator to add and delete roles to and from User.
3. Valid roles for users of the ACS are Auditor, Data Analyst, Data Gatherer, and Watchman, which shall identify these users as filling the role of Auditor, Data Analyst, Data Gatherer and Watchman or any combination.
4. The ACS will authenticate and authorize users for Data Gathering, Data Analysis, Audit and Alert sub-systems.
5. The ACS will authorize the algorithm created by Data Analyst
6. The ACS shall report Auditable Events to the Audit and Alert Subsystem (AAS).
7. The ACS shall report Alertable Events to the Audit and Alert Subsystem (AAS).
8. The System Administrator shall configure ACS.
9. Auditable events are,
   1. User created
   2. Role Assigned
   3. User Deleted
   4. Role Removed
   5. User Removed
   6. User authorized
   7. User login metrics
   8. User rejected
   9. Configuration file changed
10. Alertable events are
    1. Invalid user authentications
    2. Internal failures
    3. Failure to access other subsystems.

## Nonfunctional Requirements

### Interface

* The human interface devices shall be either hand-held, Android-based devices or flat-panel touch screen devices, easily read from a distance of six feet.
* Communication between the subsystems should be secured.

### Session maintenance

* Idle authentication session should expire in 3 minutes.
* Maximum failure login attempts should be 3 times.

## Scenarios

Scenarios depict the general flow of events occurring in the system when a particular actor or subsystem is acting on the system.

### User Enrollment

1. Mr. Bob requests Access Control Subsystem to create a Data Gatherer role for him.
2. System Administrator verifies user and assigns the user with Data Gatherer role using Access Control Subsystem
3. Access Control Subsystem notifies Audit and Alert Subsystem as User role created and assigned.
4. Access Control Subsystem notifies Bob as he has been given Data Gatherer role

### Authentication and Authorization

1. Data Gatherer logs into the system with appropriate authentication details through Data Gathering Subsystem interface.
2. Access Control Subsystem verifies the credentials provided and gives access to the Data Gathering Subsystem.
3. User lands on Data gathering subsystem internal UI.

## Use Cases

Use cases are provided as the functional model of PWMS. The use cases are realized by tracing the event flows through the analysis model as part of the dynamic modeling process

### Administer ACS

|  |  |  |  |
| --- | --- | --- | --- |
| **PWMS Use Case** | | | |
| ***Project*** | Administer Access Control Subsystem | | |
| ***ID Number*** | DAS001 | ***Status*** | For Customer Review |
| ***Creation Date*** | 02/28/15 | ***Last Revision Date 0***2/28/15 | |
| ***Author(s)*** | Santhosh Kumar Devarakonda Kankurthy | | |
| ***Requirements Map*** | 8,9 | | |

**Description/Intent**

**T**his Use Case describes the System Administrator administering the Access Control Subsystem.

**Actors**

System Administrator, Audit and Alert Subsystem

**Extends**

None

**Uses**

None

**Pre-Conditions**

The Access Control Subsystem is operating normally.

**Post-Conditions**

The Access Control Subsystem is operating normally. The Access Control Subsystem configuration is updated.

**Ideal Course of Action**

1. System Administrator logs into the Access Control Subsystem.
2. System Administrator selects the “Configure Access Control Subsystem” on the System Admin dashboard.
3. A menu of configurable data is displayed.
4. Changes are made to the configurable data.
5. System Administrator selects “configure”
6. An auditable event is sent to the Audit and Alert subsystem
7. The use case ends.

**Exceptional Course of Action**

None

**Comments**

None

### User Requests a Watchman Role

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PWMS Use Case** | | | | |
| ***Project*** | Access Control System | | | |
| ***ID Number*** | ACS001 | ***Status*** | For Customer Review | |
| ***Creation Date*** | 02/18/2015 | ***Last Revision Date*** | | 02/18/2015 |
| ***Author(s)*** | Santhosh Kumar Devarakonda Kankurthy | | | |
| ***Requirements Map*** | 1, 2, 3, 7 | | | |

**Description/Intent**

A user requests a Role as Watchman in PWMS system through an interface of Access Control System (ACS). User provides the enrollment information on screen along with desired role and submits the form.

**Actors**

* **User**
* **System Administrator**
* **Watchman**
* **AuditandAlert Subsystem**

**Extends**

None

**Uses**

The use case is used for a user enrollment.

**Pre-Conditions**

PWMS system should be working normally.

**Post-Conditions**

A user with Watchman role should be created and user details should be persisted into the storage. Audit events 'User Created', 'Role Assigned' should be reported.

**Ideal Course of Action**

1. A User tries to enroll through Access Control Subsystem (ACS) as a Watchman
2. User enters required information on the form along with desired role selected
3. Access Control Subsystem (ACS) system accepts user details and validates.
4. System Administrator will approve the user as Watchman.
5. User will be informed about approval by common communication means.
6. Access Control will report an Auditable events as 'User Created', 'Role Assigned' to Audit and Alert Subsystem

**Exceptional Course of Actions**

1. System Administrator will rejects the enrollment using Administration interface
2. User will be informed about rejection by common communication means.
3. Access Control will report an Auditable event as 'User Rejected' to Audit and Alert Subsystem

**Comments**

None

### Data Gathering Requests Authentication and Authorization

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PWMS Use Case** | | | | |
| ***Project*** | Access Control System | | | |
| ***ID Number*** | AAS002 | ***Status*** | For Customer Review | |
| ***Creation Date*** | 02/18/2015 | ***Last Revision Date*** | | 02/18/2015 |
| ***Author(s)*** | Santhosh Kumar Devarakonda Kankuthy | | | |
| ***Requirements Map*** | 4 | | | |

**Description/Intent**

A Data Gatherer login into the Data Gathering Subsystem by Data Gathering interface. Access Control Subsystem (ACS) will authenticate the user details and authorizes if the details are authentic.

**Actors**

* **Data Gathering Subsystem**
* **AuditandAlert Subsystem**

**Extends**

None

**Uses**

This use case is used when a user is trying to access a subsystem in PWMS with valid credentials for that subsystem.

**Pre-Conditions**

* PWMS system and subsystems must be up and running.
* Data storage must be up and responding.

**Post-Conditions**

* Data Gatherer should be logged into the Data Gathering Subsystem successfully

**Ideal Course of Action**

1. Data Gathering Subsystem will send user credentials to the Access Control Subsystem (ACS)
2. Access Control Subsystem (ACS) will verify the credentials and authenticates the user to access Data Gathering Subsystem.
3. Access Control will report an Auditable events as 'Data Gatherer authenticated'

**Exceptional Course of Actions**

1. Access Control Subsystem (ACS) will verify the credentials and rejects the user to access Data Gathering Subsystem if the credentials are invalid.

**Comments**

None

### Use Case Diagram



1. Access Control Subsystem (ACS) Use case diagram

## Object Model

The Conceptual Class Diagram shown on Fig 3.0 represents the Object Model. The boundary, entity and control objects are described as follows.

### ACSDGSInterface (Boundary)

ACSDGSInterface is used by Data Gathering subsystem to interact with ACS for authenticating and authorizing Data Gatherers.

### ACSDASInterface (Boundary)

ACSDASInterface is used by Data Analysis subsystem to interact with ACS for authenticating and authorizing Data Analysts.

### AASACSInterface (Boundary)

AASACSInterface is used by Audit and Alert Subsystem to interact with ACS for authenticating and authorizing Auditors and Watchmen.

### UserRequestInterface (Boundary)

UserRequestInterface is used by new users of the PWMS system to enroll into the system.

### ACSSAInterface (Boundary)

ACSSAInterface is a interface used by the System Administrator to configure/manage members in ACS.

### MemberControl (Control)

MemberControl is used to control the member enrollment and Member Approval/Reject operations by System Administrator. MemberControl uses ACLStorage to access member details.

### ACSControl (Control)

ACSControl is used to control the various subsystems and authenticate and authorize their users in PWMS.

### SAConfigControl (Control)

SAConfigControl is used to control the configuration of ACS subsystem in PWMS.

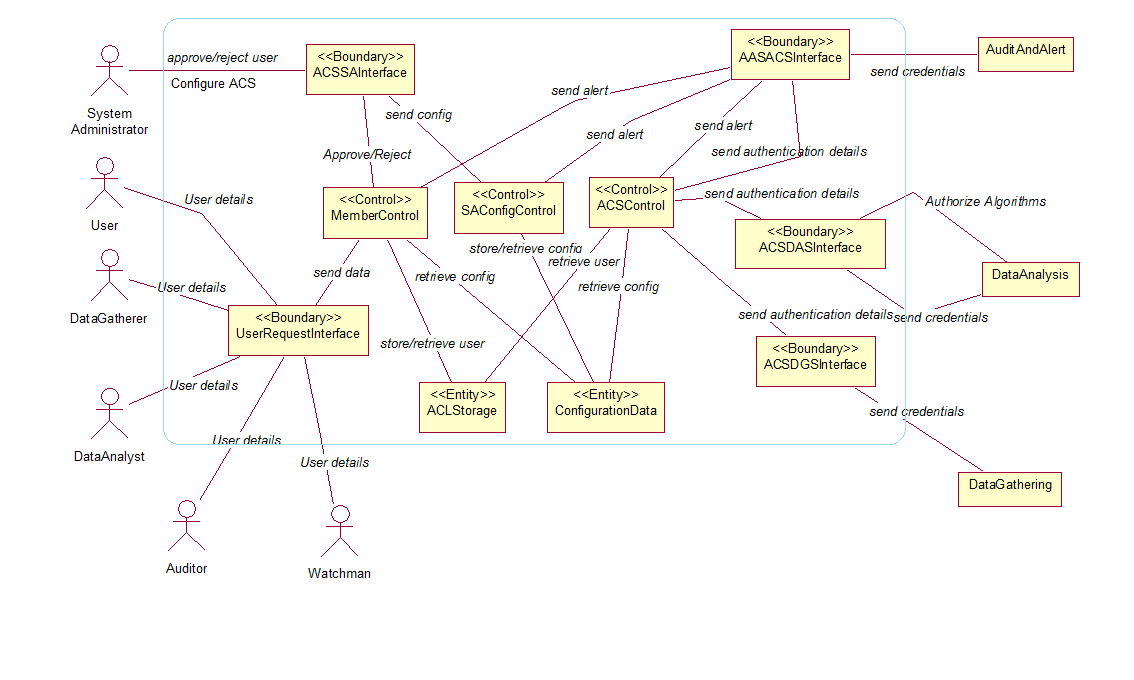
### ConfigurationData (Entity)

ConfigurationData entity is the model of the persistent configuration file in PWMS for ACS.

### ACLStorage (Entity)

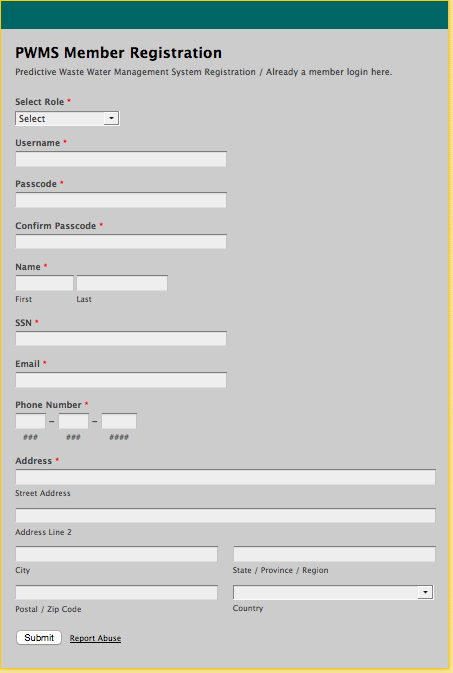
ACLStorage entity is the model of persistent members in PWMS.

### Conceptual Class Diagram

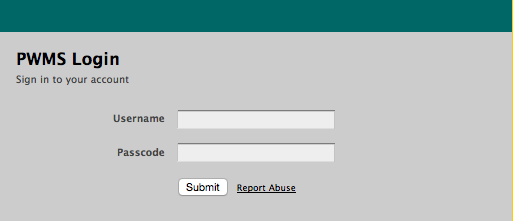


1. Access Control Subsystem (ACS) conceptual class diagram

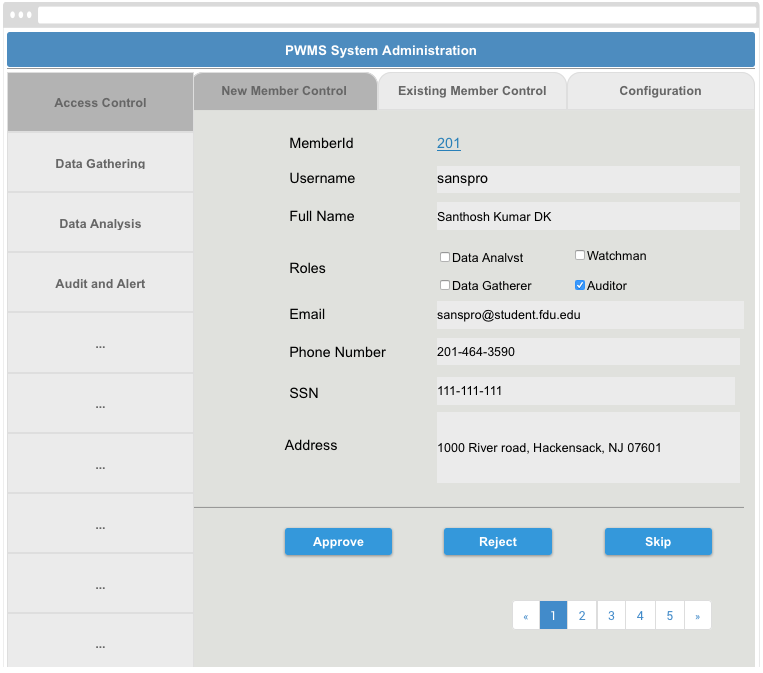
## User Interface – Screen Mock-Ups



1. PWMS Member registration form



1. PWMS Member login



1. PWMS System Administrator UI for Access Control Subsystem

# Dynamic model

The dynamic model depicting interaction among the ACS subsystem objects are described in this section. Dynamic modeling at this level shows interactions amongst the ACS subsystem objects with other subsystems decomposed into entity, boundary and control objects for each subsystem in the individual RADs for each of the subsystems. Sequence, communication, state and activity diagrams are the Unified Modeling Language (UML) components that are used to show the dynamic model.

The sequence and communication diagrams correspond one-to-one with the use cases of this document.

## Administer ACS

### Sequence Diagram



1. Administer ACS - Sequence Diagram

### Communication Diagram



1. Administer ACS - Communication Diagram

## User Requests a Watchman Role

### Sequence Diagram



1. User Requests a Watchman Role - Sequence Diagram

### Communication Diagram



1. User Requests a Watchman Role - Communication Diagram

## Data Gathering Requests Authentication and Authorization

### Sequence Diagram



1. Data Gathering Requests Authentication and Authorization - Sequence Diagram

### Communication Diagram



1. Data Gathering Requests Authentication and Authorization - Communication Diagram