Aaron Fifarek, Kerianne Gross, Jon Hoffman

Coupled Tanks Requirements Document

Contents

[Introduction 2](#_Toc410900937)

[System Description 3](#_Toc410900938)

[System Level Assumptions 6](#_Toc410900939)

[1. Inflow 6](#_Toc410900940)

[2. Outflow 6](#_Toc410900941)

[System Level Requirements 6](#_Toc410900942)

[High Level Requirements 6](#_Toc410900943)

[Primary Subsystems 7](#_Toc410900944)

[1. Environment 7](#_Toc410900945)

[1.1 System Time Increment Assumptions 7](#_Toc410900946)

[1.2 Tank 1 Size Assumptions 7](#_Toc410900947)

[1.3 Tank 2 Size Assumptions 7](#_Toc410900948)

[1.4 Previous Height Assumptions 8](#_Toc410900949)

[1.5 Control Input Assumptions 8](#_Toc410900950)

[1.6 Sensor Requirements 9](#_Toc410900951)

[1.7 Tank 1 Requirements 10](#_Toc410900952)

[1.8 Tank 2 Requirements 12](#_Toc410900953)

[2. Controller 13](#_Toc410900954)

[2.1 Tank 1 Controller 13](#_Toc410900955)

[2.2 Tank 2 Controller 14](#_Toc410900956)

[Simulation Requirements 15](#_Toc410900957)

[1. Updater 15](#_Toc410900958)

[Mode State Transitions 17](#_Toc410900959)

[Mode Diagrams 17](#_Toc410900960)

[1.1 Tank 1 Modes: 17](#_Toc410900961)

[1.2 Tank 2 Modes: 17](#_Toc410900962)

[Appendix A – Environmental Constants 18](#_Toc410900963)

# Introduction

The Verification and Validation of Autonomous Systems (VVAS) Team at the Air Force Research Laboratory’s Aerospace Systems Directorate seeks to expand the current design paradigm to incorporate more verification and validation techniques early in system design in order to generate evidence throughout the design process and supplement traditional modeling, simulation, test, and evaluation techniques. This approach to certification is called an Assurance Case[[1]](#footnote-2) and it is envisioned to be a compilation of analytical proofs, comprehensive test, and bounding of an advanced system at runtime presented to make the case for system certification.

The vision for incorporating verification and validation techniques early in design is to start by formally expressing requirements, architecture, and modeling development in a compositional structure and iterative process that employs formal methods to generate analytical proofs and reason about the design at the earliest stages when discovering errors is the least costly. Rather than creating monolithic designs, systems will be logically broken out by components with analysis completed at each level of the design.

This document is an example requirements document for this new paradigm. As the design process is envisioned to be iterative, this requirements document reflects a later, more mature iteration in which some elements of the design will be reflected in derived requirements in order to produce a more complete picture and foundation for analysis.

Requirements documented here are also written formally in a tool developed by Rockwell Collins and AFRL called Specification and Analysis of Requirements (SpeAR). The SpeAR framework allows requirements to be analyzed using model checking and theorem proving. These requirements are used to analyze the defined architecture and model of the system in the next two design phases.

In order to demonstrate the assurance case concept and evaluate available tools for the early system design, a publically releasable, academic control example simple enough to completely design and evaluate in software, but with enough richness to expand with complex equations, mode logic, advanced control algorithms, fault tolerance, etc. was desired. After evaluating a couple options, the coupled tank system was selected as a popular academic example used in control theory exercises with potential application to the F-35 program. This is the first iteration of this system design and seeks only to define very basic functionality with many simplifying assumptions included.

The document provides a description of the coupled tanks system used in this proof of concept assurance case as well as a list of requirements.

# System Description

The coupled tank system utilized draws liquid of some form from a limitless source, temporarily stores it in order for some process such as mixing or temperature control to occur, and then releases the liquid into a bottomless sink. As the name would suggest, the system contains two tanks that are each controlled by one of two independent controllers that operate four actuators between the two tanks and receive feedback from five sensor dispersed between the two tanks that provide a rudimentary understanding of the state of the liquid height in each tank. The system is implemented in the architecture phase with the physical definition presented in Figure 1. The interaction between the physical design and that of the system controller is presented in Figure 2.

|  |  |
| --- | --- |
| Figure 1: Coupled Tanks Physical Architecture | Figure 2: Coupled tanks physical sensor and actuator signal connections to the system controller. |

Liquid is drawn into Tank 1 by a simple on/off pump and expelled from Tank 1 by a simple on/off valve, which empties liquid directly into Tank 2. Tank 1 which is 7.0 meters high and 1.0 square meter in cross-sectional area. The objective of the Tank 1 controller is to keep the height of the liquid between the High Sensor (SH) and the Low Sensor (SL) in the “safe” region by controlling the state of the pump and valve.

Liquid enters Tank 2 by the valve from Tank 1 and exits via a production valve or a larger emergency valve when a larger flow out is required for the system to maintain safety. Tank 2 is 4.0 meters in height and 2.0 square meters in cross sectional area. The objective of the Tank 2 controller is to keep the height of the liquid in tank two in the “safe” region monitored by the position of a high (SH), medium (SM), and low (SL) sensor in Tank2 by controlling the state of the production and emergency valves. Control of the input valve rests only with the Tank 1 controller, so Tank 2 is a reactionary controller to the input from Tank 1.

It is assumed that the flow rate through the pump and three valves is either zero or a constant value, that no faults or leaks occur in the system, and there are not external disturbance inputs to the coupled tank system. All sensors used in this system are assumed to be Boolean sensors that report 1 if the liquid is at the sensor height and 0 if the liquid is not at the sensor’s height. Simple components such as the actuators and sensors in this example might be selected to reduce cost and opportunity for the system to malfunction.

The system is organization in a functional composition as depicted in Figure 3:

Figure 3: Functional Compositional Architecture of the Coupled Tanks System

The Coupled Tanks System is broken down from the highest level into a controller and environment. The controller is then broken down into a separate controller for each tank. The environment is broken down functionally into each type of component (Tanks, Valves, Pumps, and Sensors) and then broken down even further from there into the individual components. This structure allows analysis to be completed at the lowest levels of the design with results of the proof flowing up to higher levels of the design until the entire system is analyzed. This is in contrast to monolithic approaches that only analyze the system as a whole, which presents a large computational burden and makes it difficult to identify particular faults in the system design.

# System Level Assumptions

## Inflow

###### There is an unlimited supply of water to be pumped into the coupled tanks system

###### The water is not pressurized in the production line and cannot be gravity fed into the coupled tanks system, it must be pumped into the coupled tanks system

###### The system shall contain a pump to draw liquid into tank 1.

## Outflow

###### There is an unlimited receptacle to receive an unlimited quantity of liquid emptied from the production valve.

###### There is an unlimited receptacle can receive an unlimited amount of liquid emptied from the emergency valve.

###### The system shall contain a valve to transport liquid from tank 1 to tank 2.

###### The system shall contain a valve to transport liquid from tank 2 to the production line

###### The system shall contain a valve to transport liquid from tank 2 to an acceptable area outside the production system in case of emergency.

# System Level Requirements

## High Level Requirements

#### Tank 1 shall not overflow.

Rationale: An overflow of the tank is a safety hazard.

#### Tank 2 shall not overflow.

Rationale: An overflow of the tank is a safety hazard.

#### The initial liquid height Tank 1 shall be known to the control system.

Rationale: In order to properly track the liquid height in Tank 1, the initial liquid height must be known. This system will meet this requirement by starting from a completely empty state or some initial known height below the low sensor height.

#### The initial liquid height Tank 2 shall be known to the control system.

Rationale: In order to properly track the liquid height in Tank 2, the initial liquid height must be known. This system will meet this requirement by starting from a completely empty state or some initial known height below the low sensor height.

#### The height of the tank 1 liquid shall not be over the tank 1 high safety level for more than the specified time. This specified time is dependent on the flowrate per timestep.

Rationale: Prolonged periods of time where the liquid is higher than the safety level could cause an unsafe situation to occur. This is dependent on the specified time increment per timestep. A violation will be identified but will not change the pump and valve states until a following timestep. Therefore the number of allowable timesteps that the system can violate the safety boundary before returning to the safe region is dependent on the system architecture.

#### The height of the tank 1 liquid shall not be lower than the tank 1 low safety level (once it has already crossed it) for more than the specified time. This specified time is dependent on the flowrate per timestep.

Rationale: Prolonged periods of time where the liquid is lower than the safety level could cause an unsafe situation to occur. This excludes the initial startup period while the tank is filling for the first time. This is dependent on the specified time increment per timestep. A violation will be identified but will not change the pump and valve states until a following timestep. Therefore the number of allowable timesteps that the system can violate the safety boundary before returning to the safe region is dependent on the system architecture.

#### The height of the tank 2 liquid shall not be over the tank 2 high safety level for more than the specified time. This specified time is dependent on the flowrate per timestep.

Rationale: Prolonged periods of time where the liquid is higher than the safety level could cause an unsafe situation to occur. This is dependent on the specified time increment per timestep. A violation will be identified but will not change the pump and valve states until a following timestep. Therefore the number of allowable timesteps that the system can violate the safety boundary before returning to the safe region is dependent on the system architecture.

#### The height of the tank 2 liquid shall not be lower than the tank 2 low safety level (once it has already crossed it) for more than the specified time. This specified time is dependent on the flowrate per timestep.

Rationale: Prolonged periods of time where the liquid is lower than the safety level could cause an unsafe situation to occur. This excludes the initial startup period while the tank is filling for the first time. This is dependent on the specified time increment per timestep. A violation will be identified but will not change the pump and valve states until a following timestep. Therefore the number of allowable timesteps that the system can violate the safety boundary before returning to the safe region is dependent on the system architecture.

# Primary Subsystems

## Environment

The purpose of the environment subsystem is to represent the physical attributes of the system. Specifically this subsystem includes all the tanks, actuators, pumps, valves, and sensors that is necessary to allow the system to exist in a physical representation. This subsystem produces changes in component states only in response to the physical attributes of the tanks.

### System Time Increment Assumptions

###### The default time increment of the system, once defined, does not change.

Rationale: The time increment represents the global polling rate of the physical system and is not variable. The rate is defined globally and governs represents the rate that the system can check the dynamic state of the system.

### Tank 1 Size Assumptions

###### The tank 1 has a specified volume that is known globally and does not change.

Rationale: The tank 1 specified volume is known so that system can calculate the expected volume in the tank depending on inflow and outflow calculations.

###### The tank 1 has a specified cross-sectional area that is known to the controller and does not change.

Rationale: The tank 1 specified cross-sectional area is known so that system can calculate the expected volume in the tank depending on inflow and outflow calculations. Furthermore, this information provides the ability determine liquid height in tank 1by volume or to determine the tank volume by the liquid height.

###### The tank 1 has a specified height that is known to the controller and does not change.

Rationale: The tank 1 specified height is known so that the system can determine whether or not an overflow of tank 1 has occurred.

### Tank 2 Size Assumptions

###### The tank 2 has a specified volume that is known to the controller and does not change.

Rationale: The tank 2 specified volume is known so that system can calculate the expected volume in the tank depending on inflow and outflow calculations.

###### The tank 2 has a specified cross-sectional area that is known to the controller and does not change.

Rationale: The tank 2 specified cross-sectional area is known so that system can calculate the expected volume in the tank depending on inflow and outflow calculations. Furthermore, this information provides the ability determine liquid height in tank 2 by volume or to determine the tank volume by the liquid height.

###### The tank 2 has a specified height that is known to the controller and does not change.

Rationale: The tank 2 specified height is known so that system can determine whether or not an overflow of tank 2 has occurred.

### Previous Height Assumptions

###### The previous liquid height of tank 1 is the liquid height at the previous time step.

Rationale: The previous liquid height in tank 1 is defined as the liquid height at the previously polled timestep. The initial liquid height of the tank is below the low sensor and is known.

###### The previous liquid height of tank 2 is the liquid height at the previous time step.

Rationale: The previous liquid height in tank 2 is defined as the liquid height at the previously polled timestep. The initial liquid height of the tank is below the low sensor and is known.

### Control Input Assumptions

###### The pump is initially off when the system is started.

Rationale: The initial state of the pump is necessary to ensure that the system does not have any ability to fill or drain that is not under control.

###### The tank 1 outflow valve is initially closed.

Rationale: The tank 1 should not drain unless controlled to do so. This sets the understood initial state of the tank 1 outflow valve.

###### The tank 2 production valve is initially closed.

Rationale: The tank 2 should not drain liquid into the production line unless controlled to do so. This sets the understood initial state of the tank 2 production valve.

###### The tank 2 emergency valve is initially closed.

Rationale: The tank 2 should not drain liquid into through the emergency valve unless controlled to do so. This sets the understood initial state of the tank 2 emergency valve.

###### The system liquid sensors shall be placed properly in each tank to match the predefined sensor height locations.

Rationale: All tank liquid sensors will be placed in the tank at predefined heights and those heights will be globally known to the overall system. The physical placement of these sensors will match the system configured placement.

###### When the pump is ON, the pump shall maintain a maximum flowrate that is known to the system.

Rationale: The pump into the tank 1 will provide a maximum inflow to that is defined in the system. Other subsystems will use this value when requesting the maximum inflow into tank 1.

###### The valves in the system shall have a constant maximum flowrate that is known to the system.

Rationale: All the valves in the system will have globally known maximum flowrates that can be used by other subsystems in order to estimate the current liquid heights in the tanks.

### Sensor Requirements

#### The tank 1 HIGH sensor is physically placed at a greater height (above) the tank 1 LOW sensor.

Rationale: The HIGH sensor is assumed to be placed at a height level within tank 1 that would signal a greater height of liquid in tank 1 than that of the LOW sensor.

#### The tank 2 HIGH sensor is physically placed at a greater height (above) the tank 2 MID sensor.

Rationale: The HIGH sensor is assumed to be placed at a height level within tank 2 that would signal a greater height of liquid in the tank than that of the MID sensor.

#### The tank 2 MID sensor is physically placed at a greater height (above) the tank 2 LOW sensor.

Rationale: The MID sensor is assumed to be placed at a height level within tank 2 that would signal a greater height of liquid in tank 2 than that of the LOW sensor.

#### The sensor outputs shall initially be false.

Rationale: Tank 1 and tank 2 will initially have no liquid (empty) or be filled to a level below low sensor heights and therefore the liquid height sensors in the system will provide a false, or 0, initial output.

#### If the tank 1 liquid height is greater than or equal to the sensor height of the tank 1 HIGH liquid sensor then the sensor should return an active (TRUE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid reaches that defined height of the sensor then it returns a signal that informs the system.

#### If the tank 1 liquid height is below (less than) the placement height of the tank 1 HIGH liquid sensor then the sensor should return a (FALSE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid does not reach that defined height of the sensor then a lack of a signal informs the system water is not present at that level.

#### If the tank 1 liquid height is greater than or equal to the placement height of the tank 1 LOW liquid sensor then the sensor should return an active (TRUE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid reaches that defined height of the sensor then it returns a signal that informs the system.

#### If the tank 1 liquid height is below (less than) the placement height of the tank 1 LOW liquid sensor then the sensor should return a (FALSE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid does not reach that defined height of the sensor then a lack of a signal informs the system water is not present at that level.

#### If the tank 2 liquid height is greater than or equal to the placement height of the tank 2 HIGH liquid sensor then the sensor should return an active (TRUE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid reaches that defined height of the sensor then it returns a signal that informs the system.

#### If the tank 2 liquid height is below (less than) the placement height of the tank 2 HIGH liquid sensor then the sensor should return a (FALSE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid does not reach that defined height of the sensor then a lack of a signal informs the system water is not present at that level.

#### If the tank 2 liquid height is greater than or equal to the placement height of the tank 2 MID liquid sensor then the sensor should return an active (TRUE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid reaches that defined height of the sensor then it returns a signal that informs the system.

#### If the tank 2 liquid height is below (less than) the placement height of the tank 2 MID liquid sensor then the sensor should return a (FALSE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid does not reach that defined height of the sensor then a lack of a signal informs the system water is not present at that level.

#### If the tank 2 liquid height is greater than or equal to the placement height of the tank 2 LOW liquid sensor then the sensor should return an active (TRUE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid reaches that defined height of the sensor it will return a signal that informs the system.

#### If the tank 2 liquid height is below (less than) the placement height of the tank 2 LOW liquid sensor then the sensor should return a (FALSE) state to the system.

Rationale: The sensors are binary switches that trigger when the liquid has reached the sensor height. If the liquid does not reach that defined height of the sensor then a lack of a signal informs the system water is not present at that level.

### Tank 1 Requirements

#### The tank 1 is initially empty or below the low tank 1 liquid height sensor. If the tank is not empty the liquid height must be known to the system.

Rationale: The system is designed to have a specified start condition to sync the controller and that environment.

#### The tank 1 change in liquid volume for each timestep is limited by the maximum inflow and outflow for each timestep.

Rationale: Tank 1 can only fill or empty by the properties of the overall inflow and outflow from the tank which is limited by the state of the pump and valve. The tank liquid height must follow the physical properties of these components.

#### The tank 1 resulting liquid height for each timestep is dependent on the liquid height in the previous timestep plus the additional liquid height defined by the net flow rate from the state of the pump and the valve and the cross-sectional area of tank 1.

Rationale: Tank 1 can only fill or empty dependent on the pump and valve state. Each timestep would allow a delta height into the tank which will change the liquid height in the previous timestep.

#### When the tank 1 pump is ON and the valve is CLOSED the liquid height in the tank shall increase from the previous timestep.

Rationale: When the tank 1 pump is providing an inflow of liquid into the tank and the valve is closed, which prevents any outflow of liquid from this tank, the liquid height in the tank will increase (rise).

#### When the tank 1 pump is OFF and the valve is OPEN the liquid height in the tank shall decrease from the previous timestep.

Rationale: When the tank 1 pump has no inflow of liquid into the tank and the valve is open, which drains liquid from this tank, the liquid height in the tank will decrease (drop).

#### When the tank 1 pump is OFF that the valve is CLOSED the liquid height in the tank shall remain equivalent to the liquid height from the previous timestep.

Rationale: When the tank 1 pump has no inflow of liquid into the tank and the valve is closed, which prevents any outflow of liquid from this tank, the liquid height in the tank will be equal to the height at the previous timestep (remain steady).

#### When the pump is ON there should be inflow into the tank 1.

Rationale: When this pump is on then an inflow of liquid should be added to tank 1. The tank can still have a negative flowrate depending on the states of the outflow properties of the tank.

#### When the pump is OFF there should be NO inflow into tank 1.

Rationale: When this pump is off then can be no inflow of liquid added to tank 1.

#### When the tank 1 valve is OPEN the flow rate shall be equal to the physical maximum flow rate of the valve.

Rationale: When this valve is open then liquid can flow from tank 1 into tank 2. This will only hold as long as there is available liquid in tank 1 to transfer to tank 2. In the event that tank 1 is empty then there would be no flow to the tank 2.

#### When the tank 1 valve is CLOSED the flow rate of the valve shall be zero.

Rationale: When this valve is closed then liquid cannot flow from tank 1 into the tank 2.

### Tank 2 Requirements

#### Tank 2 is initially empty or below the tank 2 low liquid height sensor. If the tank is not empty the liquid height must be known to the system.

Rationale: The system is designed to have a specified start condition to sync the controller and that environment.

#### The tank 2 change in liquid volume for each timestep is limited by the maximum inflow and outflow for each timestep.

Rationale: Tank 2 can only fill or empty by the properties of the overall inflow and outflow from the tank which is limited by the state of the inflow valve and the production and emergency outflow valves. The tank liquid height must follow the physical properties of these components.

#### The resulting tank 2 liquid height for each timestep is a function of the liquid height in the previous timestep, the additional liquid height as defined by the net flow rate from the state of the inflow valve from tank 1 and tank 2 outflow valves (production and emergency), and the cross-sectional area.

Rationale: Tank 2 can only fill or empty dependent on the inflow valve state and the outflow by the production and emergency valve states. Each timestep would allow a delta height into the tank which will change the liquid height in the previous timestep.

#### When the tank 1 valve is OPEN and the tank 2 outflow valves (emergency and production) are CLOSED the liquid height in tank 2 shall increase from the previous timestep.

Rationale: When the tank 1 valve is providing an inflow of liquid into tank 2 and the tank 2 valves (production and emergency) are closed, which prevents any outflow of liquid from tank 2, the liquid height in the tank 2 will increase (rise).

#### When the tank 1 valve is OPEN, the tank 2 production valve is OPEN, and the tank 2 emergency valve is CLOSED the liquid height in tank 2 shall increase from the previous timestep.

Rationale: When the tank 1 valve is providing an inflow of liquid into tank 2, the tank 2 production valve is open (outflow), and the tank 2 emergency valve is closed, the tank 2 liquid height will increase (rise). This will not hold if the production valve flowrate is greater than or equal to the flowrate of the valve from the tank 1.

#### When the tank 1 valve is OPEN, the tank 2 production valve is CLOSED, and the tank 2 emergency valve is OPEN the liquid height in tank 2 shall decrease from the previous timestep.

Rationale: When the tank 1 valve is providing an inflow of liquid into tank 2, while the tank 2 production valve is closed, and while the tank 2 emergency valve is open (outflow), the tank 2 liquid height will decrease (fall). This will not hold if the emergency valve flowrate is less than or equal to the flowrate of the valve from tank 1.

#### When the tank 1 valve is CLOSED that the tank 2 valves (production and emergency) are CLOSED the liquid height in tank 2 shall remain the same from the previous timestep.

Rationale: When the tank 1 valve provides no inflow of liquid into tank 2and the tank 2 valves are closed, which prevents any outflow of liquid from this tank, the liquid height in tank 2 will be equal to the height at the previous timestep (remain steady).

#### When the tank 2 production valve is OPEN there should be an outflow equal to that of the max production flow.

Rationale: While the production valve in tank 2 is open the flow through that valve should be equal to the max flowrate through the valve as defined by the physical attributes of that valve.

#### When the tank 2 production valve is CLOSED there should be no flow from that valve.

Rationale: While the production valve in the tank 2 is closed there should be no flow through the valve since it is in engaged in a blocked state.

#### When the tank 2 emergency valve is OPEN there should be an outflow equal to that of the max emergency output flow.

Rationale: While the emergency valve in tank 2 is open the flow through that valve should be equal to the max flowrate through the valve as defined by the physical attributes of that valve.

#### When the tank 2 emergency valve is CLOSED there should be no flow from that valve.

Rationale: While the emergency valve in tank 2 is closed there should be no flow through the valve since it is in engaged in a blocked state.

## Controller

The purpose of the controller subsystem is to provide the control responses to the system to manage the liquid level of the tanks through the use of the pump, valves, and sensors. The controller is provided information from the physical system in the manner that the physical system can provide. This subcomponent provides the logic in response to the signals provided by the physical subsystem.

### Tank 1 Controller

###### When the tank 1 HIGH sensor provides a TRUE signal to the controller, it is understood that the tank 1 LOW sensor is also TRUE.

Rationale: If the liquid level has reached the high sensor in tank 1 and physically (as defined in the environment) the low sensor is at lesser height (lower) in the tank than if the water reaches the high sensor it must also exceed the height of the low sensor height and therefore should also be TRUE.

#### When the tank 1 LOW liquid sensor is FALSE, the tank 1 pump shall be ON and the tank 1 outflow valve shall be CLOSED.

Rationale: This requirement defines an operational behavior of tank 1. In the event that the safety low sensor level is not reached (water level too low) then the controller will not allow any liquid to drain from the tank until the water volume has filled to an appropriate level.

#### When the tank 1 HIGH liquid sensor is TRUE, the tank 1 pump shall be OFF and the tank 1 outflow valve shall be OPEN.

Rationale: This requirement defines an operational behavior of tank 1. In the event that the safety high sensor level is reached or exceeded (water level too high) then the controller will drain liquid from the tank until the water volume has filled to an appropriate level. This is accomplished by turning off the pump and opening the outflow valve, thus removing inflow and maximizing outflow.

#### When the tank 1 HIGH liquid sensor is FALSE and the tank 1 LOW liquid sensor is TRUE then the tank 1 pump and the tank 1 outflow valve shall maintain the states they were set to in the previous timestep.

Rationale: This requirement defines an operational behavior of tank 1. In the event that the safety high sensor level is reached or exceeded (water level too high) then the controller will drain liquid from the tank until the water volume has filled to an appropriate level. This is accomplished by turning off the pump and opening the outflow valve, thus removing inflow and maximizing outflow.

### Tank 2 Controller

###### When the tank 2 HIGH sensor provides a TRUE signal to the controller, it is understood that the tank 2 MID sensor is also TRUE.

Rationale: If the liquid level has reached the high sensor in tank 2, the mid sensor is at lesser height (lower) in the tank. Therefore if the water reaches the high sensor it must also exceed the height of the mid sensor height.

###### When the tank 2 MID sensor provides a TRUE signal to the controller, it is understood that the tank 2 LOW sensor is also TRUE.

Rationale: If the liquid level has reached the mid sensor in tank 2, the low sensor is at lesser height (lower) in the tank. Therefore if the water reaches the mid sensor it must also exceed the height of the low sensor height.

#### When the system is initially started the tank 2 production valve shall be CLOSED.

Rationale: In order to prevent the production line from receiving liquid from the system prior to the completion of startup, the production valve is closed at the initial startup of the system.

#### When the system is initially started the tank 2 production valve shall be CLOSED.

Rationale: In order to prevent the production line from receiving liquid from the system prior to the completion of startup, the production valve is closed at the initial startup of the system.

#### When the system is initially started the tank 2 emergency valve shall be CLOSED.

Rationale: The emergency valve is closed at the initial startup of the system in order to ensure that the system does not start in a state where liquid can leave the tanks without a command by the tank controllers.

#### When the tank 2 LOW sensor is FALSE, the emergency valve and the production valve (outflow valves) shall be commanded to be CLOSED.

Rationale: When the tank 2 low sensor is FALSE that signal informs the tank 2 controller that the liquid in tank 2 has not yet met the minimum height requirement to allow outflow from the tank. Therefore all outflow valves are closed.

#### When the tank 2 LOW sensor is TRUE and the tank 2 MID sensor is FALSE, then emergency valve shall be commanded to be CLOSED and the production valve shall be commanded to be OPEN.

Rationale: When the tank 2 low sensor is TRUE and the tank 2 mid sensor is FALSE, those signals inform the tank 2 controller that the liquid in tank 2 has not yet met the mid tank height sensor but has exceeded the low sensor tank height. This provides the controller knowledge at which height band in the tank is the liquid level.

#### When the tank 2 HIGH sensor is TRUE, the emergency valve and the production valve (outflow valves) shall be commanded to be OPEN.

Rationale: When the tank 2 high sensor is TRUE, that signal informs the tank 2 controller that the liquid in tank 2 has met or exceeded the maximum height requirement in tank 2. Therefore all outflow valves are open.

#### When the tank 2 MID sensor is TRUE, the tank 2 HIGH sensor is FALSE, and the emergency valve was previously open, then the emergency valve and the production valve (outflow valves) shall be commanded to be OPEN.

Rationale: When the tank 2 mid sensor is TRUE, the tank 2 high sensor is false, and that emergency valve was previously open means that tank 2 had been in a exceed high sensor state at a previous timestep. In this situation the tank should empty until the mid sensor is no longer active (TRUE) to eliminate the emergency fill height situation.

#### When the tank 2 MID sensor is TRUE, the tank 2 HIGH sensor is FALSE, and the emergency valve was not previously open, then the emergency valve shall remain commanded CLOSED and the production valve shall be commanded to be OPEN.

Rationale: When the tank 2 mid sensor is TRUE, the tank 2 high sensor is false, and that emergency valve was not previously open means that tank 2 liquid level is in the High-Mid liquid band. This does not represent an emergency drain state and therefore should just continue to outflow to the production line as expected.

# Simulation Requirements

In order to design a simulation of the described system it is necessary to add an additional primary subsystem to the design. This subsystem is responsible for updating the state variables that track the current and previous states of the system.

## Updater

This subsystem provides the system an ability to have a history of the previous state of the system as defined by the global time increment. This subsystem provides this data so that the controller subsystem can use the data to calculate expected physical data of the environment.

#### The Tank 1 Previous Height shall initially be the specified initial value.

Rationale: The Tank 1 Previous Height should be initialized correctly.

#### The Tank 2 Previous Height shall initially be the specified initial value.

Rationale: The Tank 2 Previous Height should be initialized correctly.

#### The Previous Pump State shall initially be the specified initial value.

Rationale: The Previous Pump State should be initialized correctly.

#### The Previous Valve State shall initially be the specified initial value.

Rationale: The Previous Valve State should be initialized correctly.

#### The Previous Production Valve State shall initially be the specified initial value.

Rationale: The Previous Production Valve State shall be initialized correctly.

#### The Previous Emergency Valve State shall initially be the specified initial value.

Rationale: The Previous Emergency Valve State shall be initialized correctly.

#### After the initial time step, the Tank 1 Previous Height shall be equal to the Tank 1 Height in the previous step.

Rationale: The Tank 1 Previous Height should be updated to take the value of the Tank 1 Height in the previous step.

#### After the initial time step, the Tank 2 Previous Height shall be equal to the Tank 2 Height in the previous step.

Rationale: The Tank 2 Previous Height should be updated to take the value of the Tank 2 Height in the previous step.

#### After the initial time step, the Previous Pump State shall be equal to the Pump State in the previous step.

Rationale: The Previous Pump State should be updated to take the value of the Pump State in the previous step.

#### After the initial time step, the Previous Valve State shall be equal to the Valve State in the previous step

Rationale: The Previous Valve State should be updated to take the value of the Valve State in the previous step.

#### After the initial time step, the Previous Production Valve State shall be equal to the Production Valve State in the previous step.

Rationale: The Previous Production Valve State shall be updated to take the value of the Production Valve State in the previous step.

#### After the initial time step, the Previous Emergency Valve State shall be equal to the Emergency Valve State in the previous step.

Rationale: The Previous Emergency Valve State shall be updated to take the value of the Emergency Valve State in the previous step.

# Mode State Transitions

This section defines the designed mode logic of the tank controllers in the system.

## Mode Diagrams

### Tank 1 Modes:

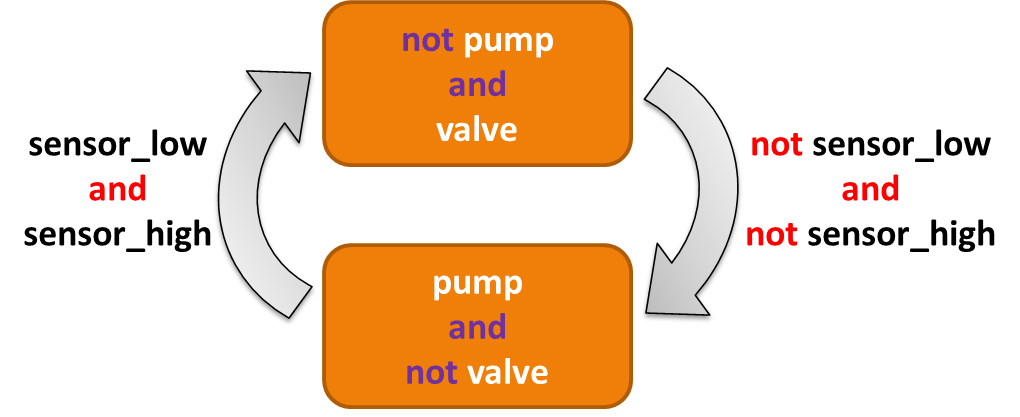


Figure 4: Tank 1 mode logic state machine

### Tank 2 Modes:

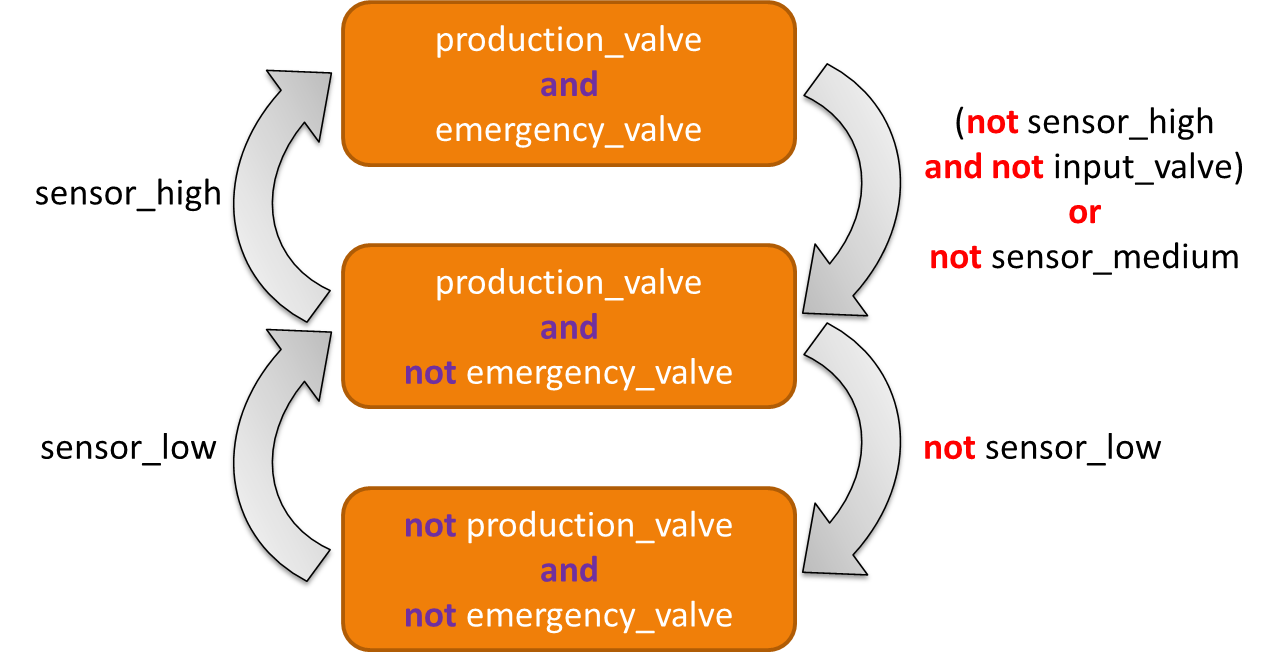


Figure 5: Tank 2 mode logic state machine

# Appendix A – Data Tables

Table 1: Environmental constants used in the System Simulation

|  |  |  |
| --- | --- | --- |
| Environment Constants | Value | Units |
| Time\_constant | 0.1 | s |
| Tank1\_Sensor\_High\_Height | 5.0 | m |
| Tank1\_Sensor\_Low\_Height | 2.0 | m |
| Tank1\_Pump\_Flow\_Rate | 0.2 | m3/s |
| Tank1\_Valve\_Flow\_Rate | 0.1 | m3/s |
| Tank1\_Cross\_Section\_Area | 1.0 | m2 |
| Tank1\_Max\_Volume | 7.0 | m3 |
| Tank2\_Sensor\_High\_Height | 3.0 | m |
| Tank2\_Sensor\_Mid\_Height | 2.0 | m |
| Tank2\_Sensor\_Low\_Height | 1.0 | m |
| Tank2\_Production\_Valve\_Flow\_Rate | 0.05 | m3/s |
| Tank2\_Emergency\_Valve\_Flow\_Rate | 0.2 | m3/s |
| Tank2\_Cross\_Section\_Area | 2.0 | m2 |
| Tank2\_Max\_Volume | 8.0 | m3 |

Table 2: Summary of the initial state of the system to be maintained in the physical and simulated design

|  |  |  |
| --- | --- | --- |
| Initial State of System Components | Value | Units |
| Pump State | Off | - |
| Tank1 Valve State | Closed | - |
| Tank1 Liquid Height (if empty) | 0.0 | m |
| Tank1 Liquid Height (if not empty) | 0.0 < x < Tank1\_Sensor\_Low\_Height | m |
| Tank1\_Sensor\_High | Inactive (Off) | - |
| Tank1\_Sensor\_Low | Inactive (Off) | - |
| Tank2 Liquid Height (if empty) | 0.0 | m |
| Tank2 Liquid Height (if not empty) | 0.0 < x < Tank2\_Sensor\_Low\_Height | m |
| Tank2\_Sensor\_High | Inactive (Off) | - |
| Tank2\_Sensor\_Mid | Inactive (Off) | - |
| Tank2\_Sensor\_Low | Inactive (Off) | - |
| Tank2 Production Valve | Closed | - |
| Tank2 Emergency Valve | Closed | - |

1. Assurance Cases. (2014). Retrieved January 12, 2015, from http://www.sei.cmu.edu/dependability/tools/assurancecase/ [↑](#footnote-ref-2)