Design Safety Report: **Single Tube Condenser**

# Introduction

This report covers the safety engineering concerning the Single Tube Condenser, Remote Labs Project.

# Experiment Outline

The single tube condenser experiment involves the heating of a fluid to boiling point, and measuring the temperature of feed water used to cool and condense the vapour produced.

## Modifications To Existing System

1. Removal of the steam heating infrastructure & replacement with electronic heaters
2. Replaced Lower heating tank with dual mode tank for heating water OR solvents using electronic heaters
3. Installed Flow Meter & Additional temperature sensors
4. Installed Electronic flow control valve to replace manual flow control valve for feed water.
5. Installed Electronic Automation & Control system for remote actuation of experiment. This utilises Advantech ADAM Industrial automation controllers for the majority of the IO processes, and an Arduino Mega MCU as a state machine sequencer & controller.
6. Installed Cameras with views of the following process areas:
   1. Condensation tube
   2. Analog Flow Meter
   3. Boiler

### Replacement Heating System

The original steam heater has been completely replaced with an electronic heating system.

In order to accommodate different working fluids with differing specific heat capacity and boiling points, two different heaters & heating methods are utilised.

### Water Heater

The water heater utilises a standard 3 × 3 kW, 3 phase heating element with a thermostat set to 100 °C. This heating element is fully submerged in the working fluid tank during operation.

#### Solvent Heater

The solvent heater utilises a 3 × 3 kW, 3 phase heating element with a thermostat set to 85 °C. The solvent heating element is submerged in a water bath below the working fluid tank. During operation the water bath is heated to 85 °C, and transfers heat through the tank walls into the working fluid tank. The heater in the working fluid tank MUST be disabled during this mode of operation.

# Existing Controls for Safe Operation

*Operation of equipment in person allows operator to intervene if any out of tolerance or unusual operation is observed.*

1. Final condensation coil & extraction fan to prevent release of evaporated solvent fumes.

# Risks Introduced by System Modification for Remote Access

1. Activation of Heating elements with incorrect working fluid levels.
2. Activation of Heating elements with incorrect working fluid.
   1. Working Fluid tank heater (water heater) active when working fluid is solvent.
      1. Could lead to overheating of solvent & damage to heating element.
3. Inability to power off heater due to local system error or firmware bug.
4. Extraction fan not placed correctly at opening to evaporator/condenser apparatus leading to release of solvent fumes.

# Mitigations to Introduced Risks

*In each instance of the risks identified, controls should be implemented to mitigate the risk of harm to people and damage to the equipment, with priority given to hardware controls and lock-outs that physically & passively prevent the identified situation from occurring.*

*If a suitable hardware control is not possible to implement, then a software control or soft-interlock should be implemented in the firmware to prevent or mitigate the likelihood of the identified situation from occurring.*

*Lastly, if no hardware or software control is possible then Operational controls & safe working procedures should be implemented to prevent the situation from occurring. Operational controls are considered last as they rely on human factors to prevent potentially dangerous situations. Hardware interlocks are prioritised as these will continue to function even in the case of firmware bugs, unintended operation, or loss of power to some or all of the system.*

## Hardware Controls

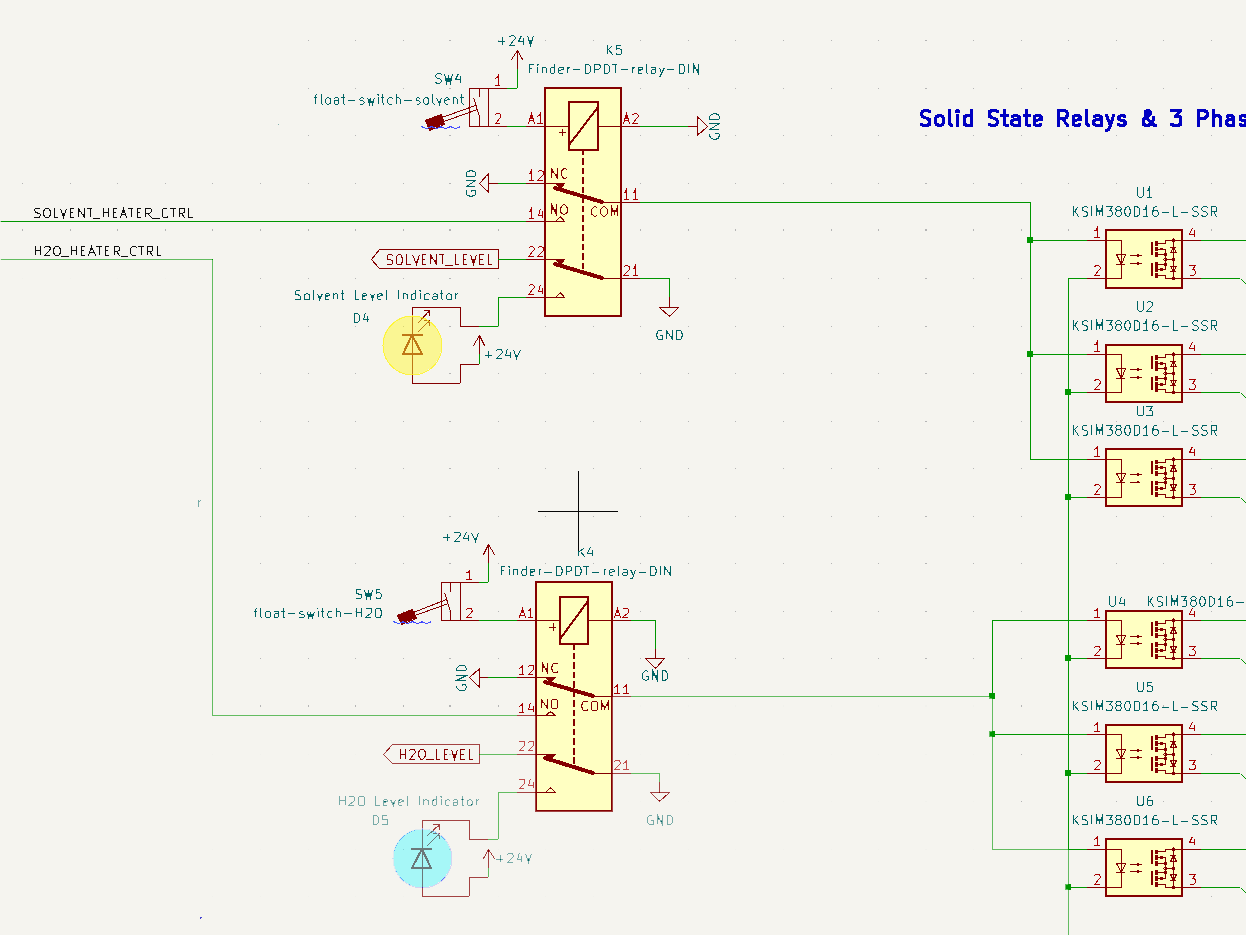
*Hardware controls are physical interlocks, hardware default conditions and other passive safety systems that will continue to work regardless of the status of the MCU controller or programming of the firmware.*

### Activation of Heating elements with incorrect working fluid levels

Mitigated through use of Float sensors in working fluid tank (Water Heater Tank) & water bath tank (Solvent Heater Tank).

The Two float sensors are wired into physical relays that control the activation signal for each heater, totally preventing their actuation if the float is LOW.

Relays default (off position) ground the control voltage to solid state heater control relays.



If Working Fluid == SOLVENT:

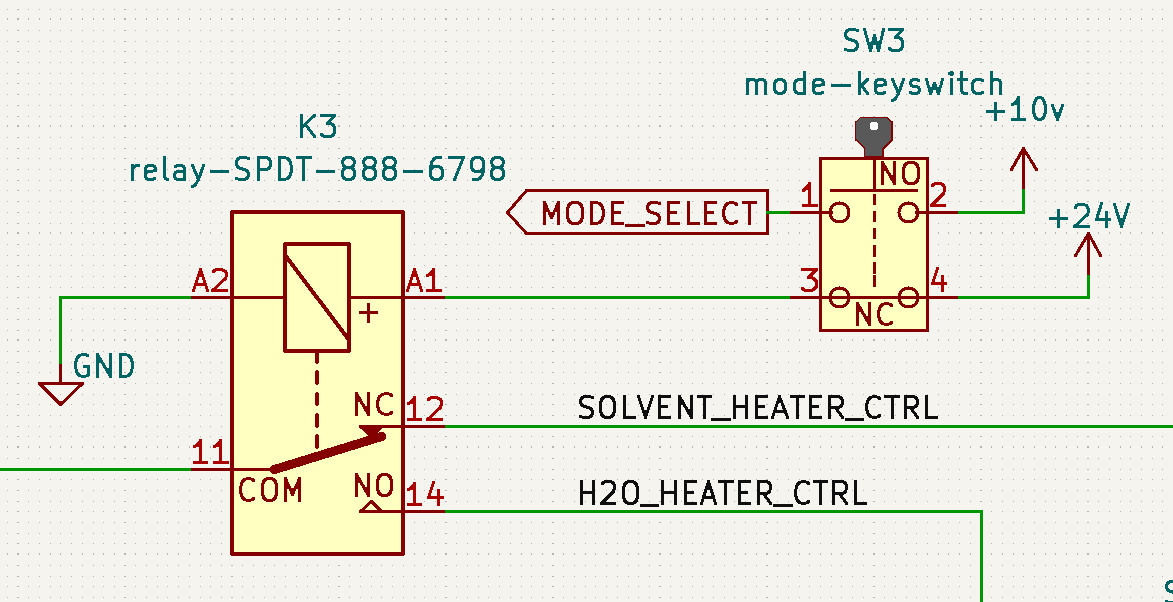
1. If Solvent level in working fluid tank is too low, heater is still submerged in water bath and no dangerous situation can result.
2. If Solvent Level in working fluid tank is too high, no hardware mitigation -> see Software & Operational controls.
3. If Water Bath level is too low, float will be LOW and heater will be prevented from activating.

If Working Fluid == WATER:

1. If Water level in working fluid tank is too low, heater will be exposed but float will be LOW and heater will be prevented from activating.
2. If Water level in water bath tank is too low no dangerous situation can result.

### Activation of Heating elements with incorrect working fluid

Mode selection via a relay that routes control voltage to the correct solid-state relays used for the actuation of each heater. Relay default (OFF) position routes control voltage to SOLVENT heater, as there is no additional risk for actuation of solvent heater if the working fluid is water.



Working Fluid mode is set via a manual switch on the operators control panel containing the automation system. This switch default position is SOLVENT. The current working fluid mode is indicated by a clearly labelled panel mount light. No Hardware control possible to prevent operator error when selecting working fluid mode -> see Operational Controls.

### Inability to power off heater due to local system error

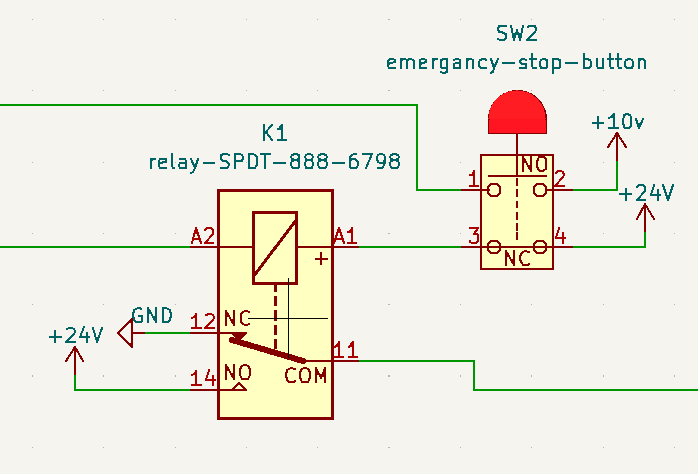
Control voltage is supplied to the heaters via an additional relay, itself controlled via the ADAM industrial process controller. Default (off) position of the relay grounds control voltage input to solid state heater relays, ensuring they cannot be powered on.

Watchdog timer in ADAM controller will shut off active heater output if no keepalive signal is received within 3 seconds. Although this is a programmed control, it operates outside of the MCU Firmware and is passive in its operation. In the case of loss of power to the ADAM, this control will go low and ground the control voltage. If system loses power, then control voltage running through the relay will be lost and heaters will power down, even if heater power is still available on a different phase.

### Additional Hardware Controls

*Hardware controls implemented but not tied to any specific potential fault.*

1. Emergency Stop Button – Hardware interlock switch that actuates a relay when pulled, allowing control signal to be routed towards the heaters Solid State Relays. Pushing the Emergency stop cuts power to the relay (if powered) and grounds the heater control signal if manually actuated.



## Software Controls

*Software controls are defined as any control included in the firmware running on the process controller MCU, in this case the Arduino Mega Controller. They rely on the correct functioning of the controller and firmware to be effective.*

### Activation of Heating elements with incorrect working fluid levels

Heater Tank floats are also wired to ADAM6024 DI (Digital Input) to allow firmware to track state of each float. In the case of low fill level, software is able to detect this and prevent actuation of the heaters while alerting the user as to the error.

### Activation of Heating elements with incorrect working fluid

Heater Tank floats are also wired to ADAM6024 DI (Digital Input) to allow firmware to track state of each float.

During solvent operation, Working Fluid Tank (Water Heater Tank) Float MUST be LOW and Water Bath Tank (Solvent Heater Tank) Float must be HIGH.

Water Heater Tank Float reading HIGH during solvent operation would indicate either incorrect fill level for solvent in tank or incorrect fluid added to tank, and system would be prevented from operation.

There is no additional risk for actuation of solvent heater if the working fluid is water and the water bath tank is filled.

### Extraction fan not placed correctly at opening to evaporator/condenser apparatus

Pitot tube implemented at entrance to Extraction fan. Software interlock and FATAL error generated if the system does not detect low pressure.

### Additional Software Controls

*Software controls implemented but not tied to any specific potential fault.*

1. Emergency Stop Button – Software interlock will disable any attempt to actuate the heaters & will warn user if Emergency stop button has been pressed.

## Operational Controls

*Operational controls are any controls that involve human intervention or the application of safe standard working procedures. Operational controls must acknowledge human factors, and include multiple levels of mitigation to avoid small errors causing significant problems.*

### Activation of Heating elements with incorrect working fluid

When servicing the equipment and topping up working fluids & water bath, operator MUST check mode switch to ensure it is set for the correct working fluid. Two indication lights are provided & labelled to indicate correct setting of working fluid mode switch.

If the mode switch is not set correctly:

If Working Fluid == SOLVENT, AND Working fluid tank is filled with WATER:

* No dangerous situation can result

If Working Fluid == WATER, AND Working fluid tank is filled with SOLVENT:

* If correct level of solvent is added, Float switch will be LOW and heater will be prevented from actuation
* If incorrect level of solvent is added (filled to the same level as water):
  + Float switch will be HIGH, and heater will be able to actuate.
    - This situation is mitigated as the amount of solvent required to fill tank to this level would raise alarm with stock controllers. No lab has this amount of solvent ready to use.

To prevent any errors involving powering on the water bath (solvent) heater, the water bath will always remain filled during every mode of operation.

## Future Controls & Improvements

*This section details additional controls & improvements that could be made to any subsystem, which are possible but may incur development timeline overheads that are not in line with the defined risk they are designed to mitigate, or require additional testing on the working apparatus to validate.*

### Tracking dT/dt for working fluids

Tracking dT/dt for working fluids may give additional indication that working fluids have been set incorrectly.

### Time & Temperature interlock implemented for Water Bath and Working Fluid Tank

Tracking temperature of working fluid tank in WATER working fluid mode, and water bath in SOLVENT heating mode, if temperature has not risen above a predefined temperature by time T after actuation, system assumes fault, shuts off heaters and generates FATAL error report.