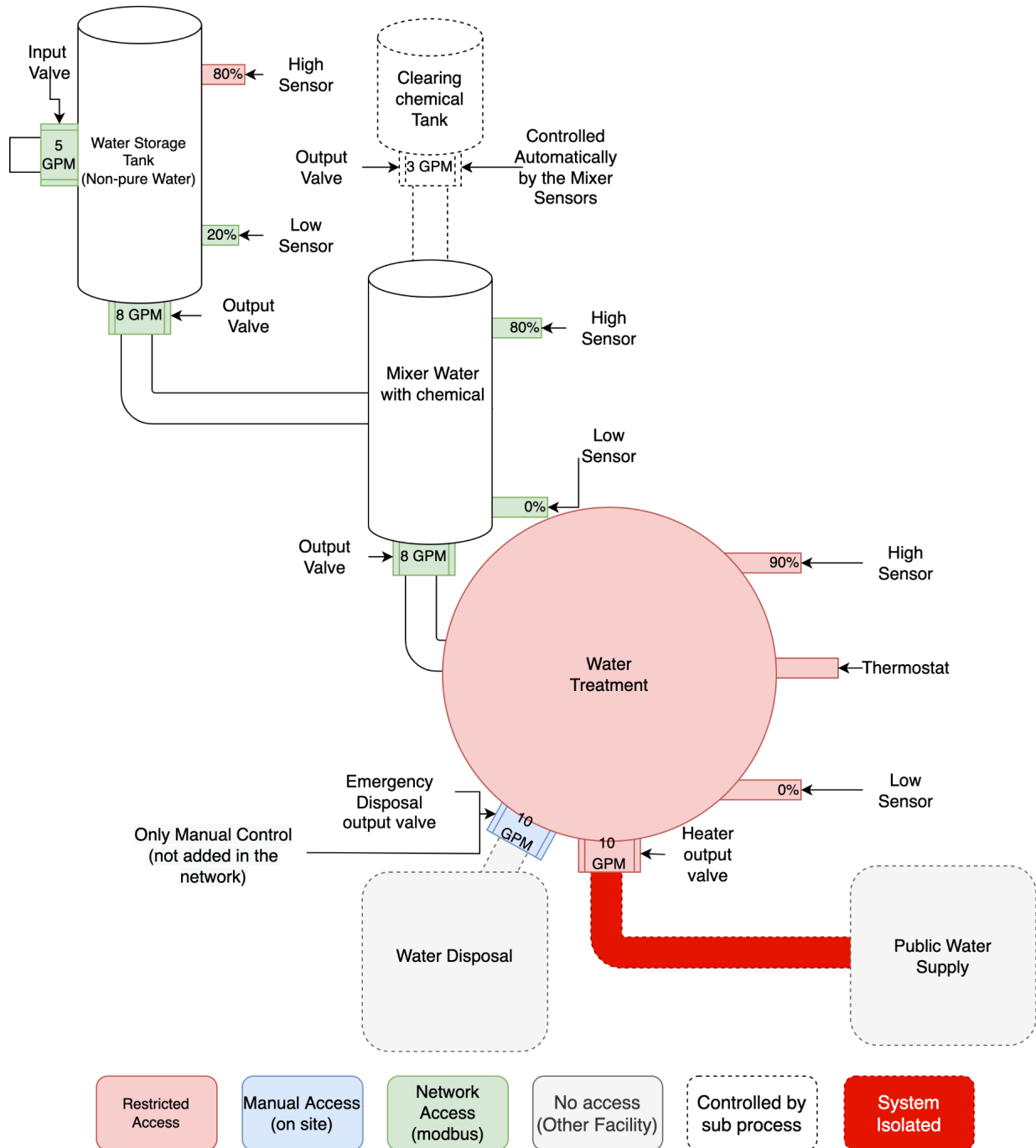# Water Treatment Facility

The diagram below describes the water treatment facility layout. Moreover, we have added information regarding its current state based on what our incident response team managed to understand about the system.

Input Valve

5 GPM

Water Storage Tank (Non-pure Water)

80% — High Sensor

20% — Low Sensor

8 GPM — Output Valve

Clearing chemical Tank

Output Valve — 3 GPM — Controlled Automatically by the Mixer Sensors

Mixer Water with chemical

80% — High Sensor

0% — Low Sensor

Output Valve — 8 GPM

Water Treatment

90% — High Sensor

— Thermostat

0% — Low Sensor

Emergency Disposal output valve

Only Manual Control (not added in the network)

10 GPM

10 GPM — Heater output valve

Water Disposal

Public Water Supply

Restricted Access

Manual Access (on site)

Network Access (modbus)

No access (Other Facility)

Controlled by sub process
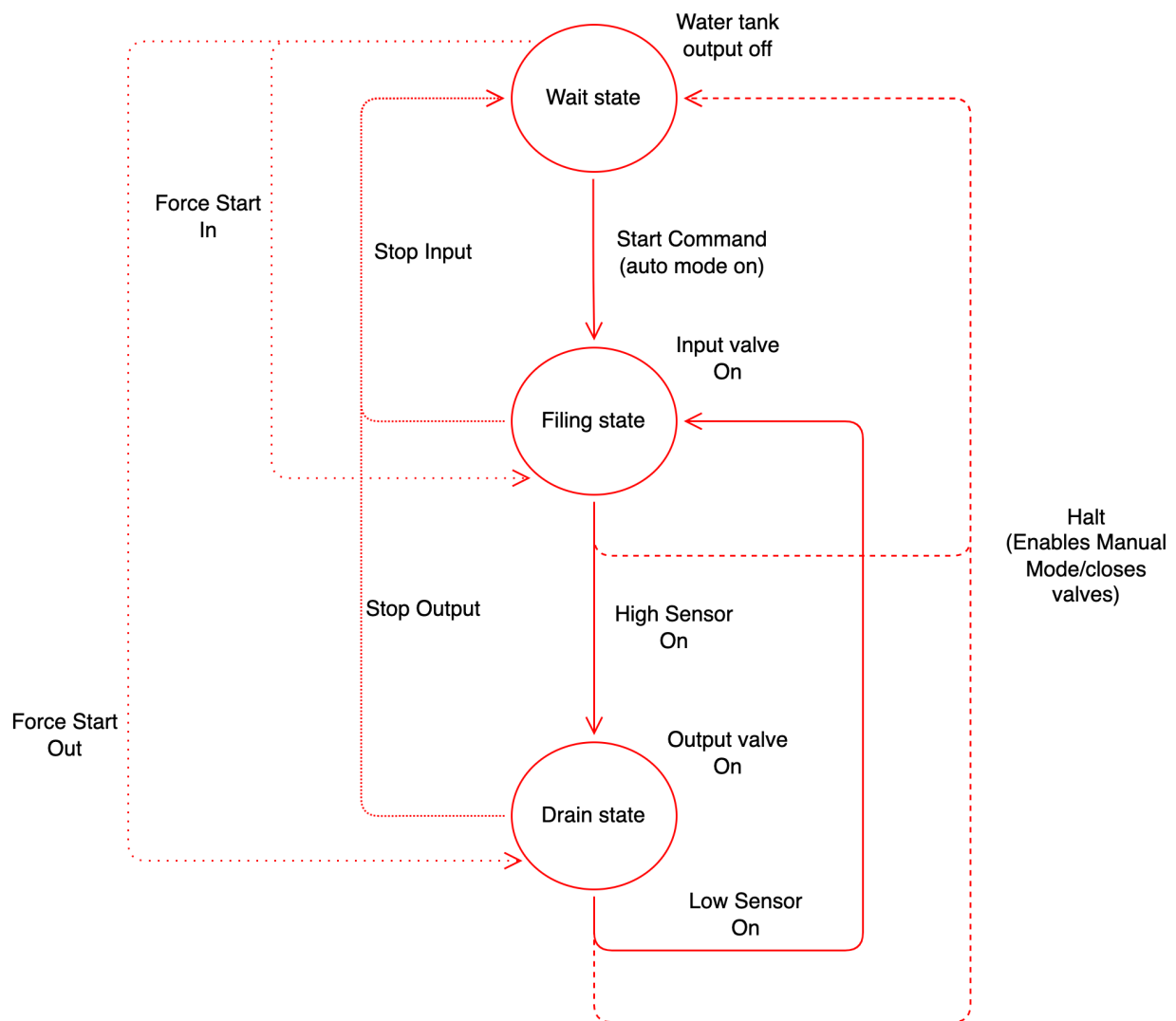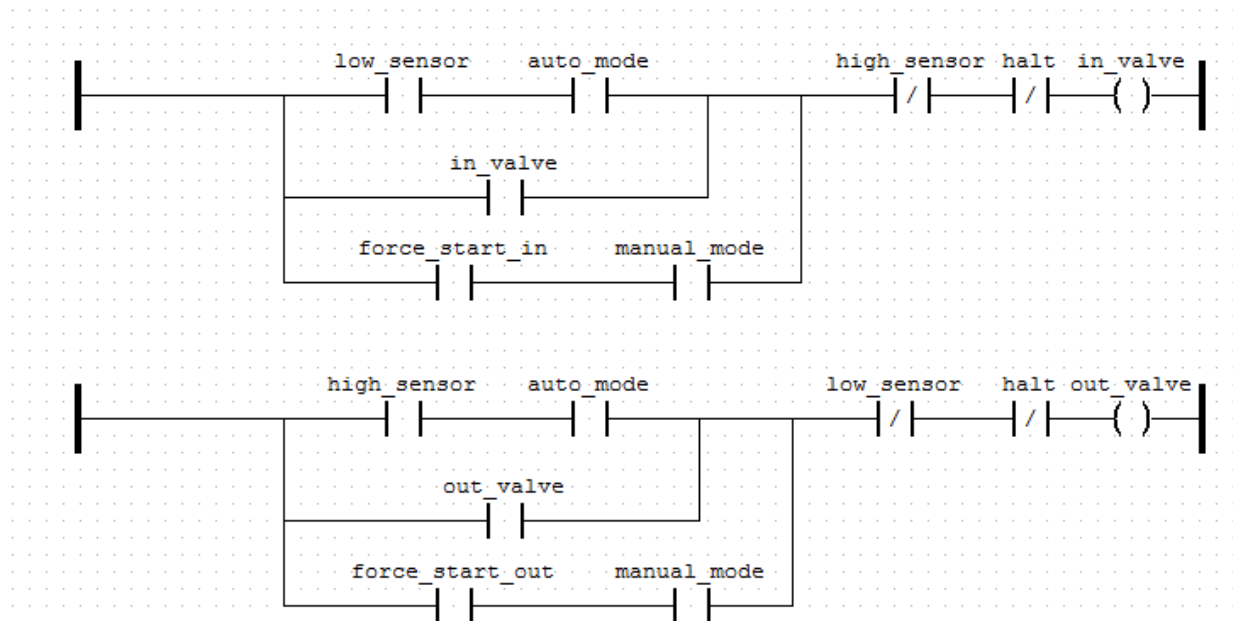
System Isolated

Logic

This section contains the logic of the PLCs in the facility. The original files are missing and we are unable to recover the logic from them so we have to draft some state diagrams.

Water Storage Tank

State diagram

Ladder Logic of Valves

```
        low_sensor      auto_mode              high_sensor  halt   in_valve
    |------+---] [-------] [------+---------------]/[-------]/[-----( )------|
           |                      |
           |       in_valve       |
           +-------] [------------+
           |                      |
           |   force_start_in    manual_mode
           +-------] [-------------] [----------+


        high_sensor     auto_mode              low_sensor  halt  out_valve
    |------+---] [-------] [------+---------------]/[-------]/[-----( )------|
           |                      |
           |       out_valve      |
           +-------] [------------+
           |                      |
           |   force_start_out   manual_mode
           +-------] [-------------] [----------+
```

Mixer Tank

Tank
output off

Wait state

Water Valve On

Input valve
On

Filing & Mix
state

High
Sensor On

Low
Sensor On
&
Water
valve On

Low
Sensor On
&
Water
valve Off

Output
valve On

Drain state
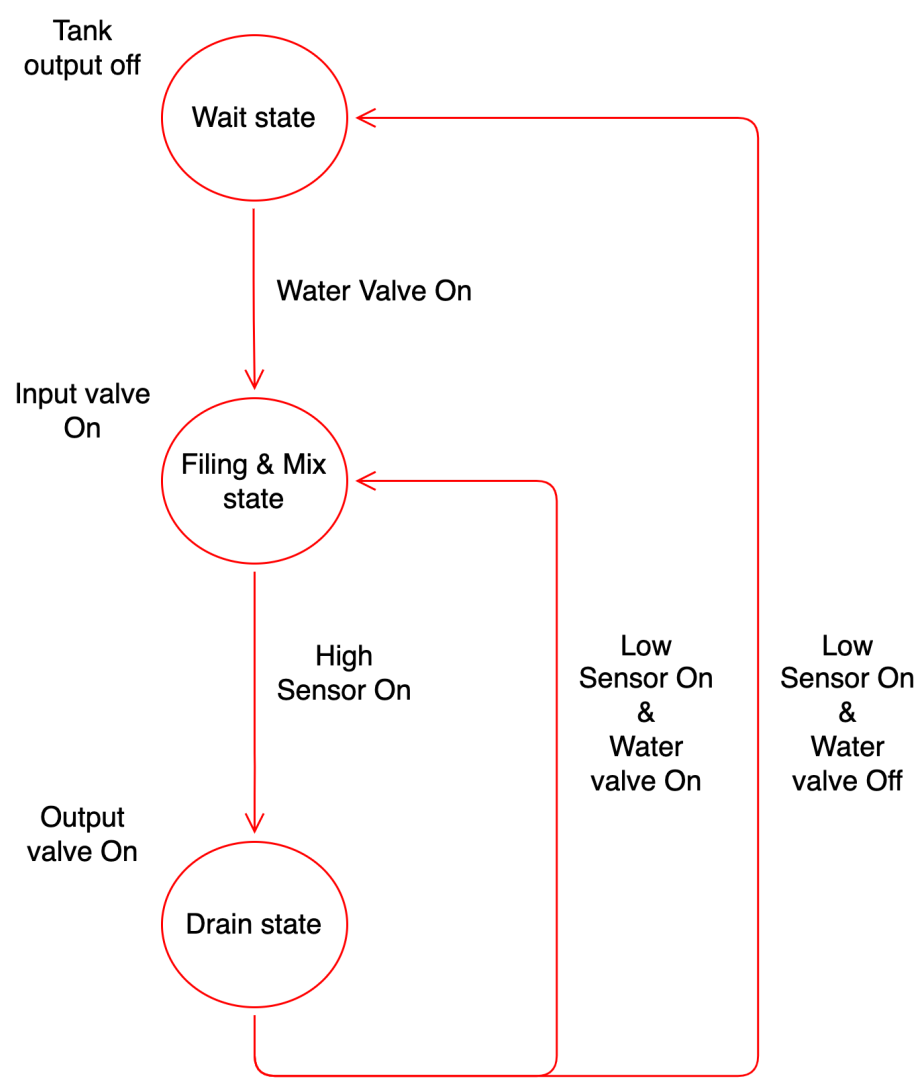
Remote Lab Layout

The HMI interface and remote network interface are unresponsive but you can remotely access via **netcat** the low-level command-line interface used in the serial network. The diagram below contains all the information you might need regarding the setup the field team has prepared. Be aware some functionality might be limited or unresponsive but you need to find a way to achieve the objective. Try to create as low traffic as possible to avoid putting additional stress on the system, don't write multiple values, and identify the correct PLCs first. Remember we need a clear path for the water with no bottlenecks.

Remote ICS Plant

(Target)

Serial modbus connection to transmit commands to the PLCs

(2)

SCADA (PLCs)
The PLC devices in the facility/network

Laptop-2
Converts received modbus packet into a valid packet (with CRC) and forwards into the real modbus RTU network

The "Remote Interface" enables communication with the serial modbus network

(1)

(Host)

Laptop-1
Sends modbus commands that Laptop-2 will forward into the main network to perform operations in the infrastructure

(1) Send modbus command to Laptop-2

(2) Calculate CRC and forward modbus RTU command on the real network

Address (decimal)	Coil
53	start
64	low_sensor
65	high_sensor
200	manual_mode_control
206	cutoff
1234	force_start_out
1336	force_start_in

Water Tank 1 Coil Addresses in the modbus network

Address (decimal)	Coil
45	start
67	low_sensor
68	high_sensor

Mixer Tank Coil Addresses in the modbus network