REAL-TIME SAFETY AND FAULT INJECTION

Prepared by A. Bakke, B. Thapa, H. Hassan and revised by Stefano Di Carlo, Alessandro Savino, Alessio Carpegna and Cristiano Chenet

Co-funded by the European Union
Erasmus+

MOTIVATION

REAL-TIME SAFETY CRITICAL APPLICATION

DEADLINE MISS -> CATASTROPHIC CONSEQUENCES

POSSIBLE SOURCE -> SINGLE EVENT UPSET (SEU)

SINGLE EVENT UPSET (SEU) AND SOFT ERROR

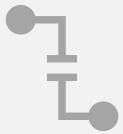
- SEU: ONE SINGLE IONIZING PARTICLE (IONS, ELECTRONS, PHOTONS...) STRIKING A SENSITIVE NODE(e.g., MEMORY CELL: “BIT”) IN A LIVE MICRO-ELECTRONIC DEVICE CAUSING CHANGE OF STATE (e.g., “BITFLIP”)
  - In 2003 in Schaerbeek, Belgium, an SEU was responsible for giving a candidate in an election an extra 4,096 votes.
  - In 2013, during the speed run of Super Mario 64 on Nintendo 64 console, a bit flip on the least significant bit of the most significant byte of Mario height value caused Mario to warp to the upper floor.
- RESULTING ERROR DUE TO SEU ALSO CALLED -> “SOFT ERROR”

Ian Johnston (17 February 2017). "Cosmic particles can change elections and cause planes to fall through the sky, scientists warn"

How An Ionizing Particle From Outer Space Helped A Mario Speedrunner Save Time

GOAL

Implementation of a monitoring technique for Soft Error.



Implementation of recovery technique from the soft error.

Soft error fault injection mechanism to test.

INSPIRATION FOR POSSIBLE SOLUTION

- A Novel Method for Online Detection of Faults Affecting Execution-Time in Multicore-Based Systems
  - ACM Transactions on Embedded Computing SystemsVolume 16Issue 4Article No.: 94pp 1–19https://doi.org/10.1145/3063313
  - Authors: Stefano Esposito, Massimo Violante, Marco Sozzi, Marco Terrone, Massimo Traversone

INTERFERENCE DETECTION BASED ON PERFORMANCE MONITORS

BOUNDED INTERFERENCE APPROACH

TWO PHASES: OFFLINE AND ONLINE

OFFLINE:

- DATA PROFILING AND WCET ESTIMATION
- THRESHOLD COMPUTATION -> BOUNDING A TASK WITHIN THRESHOLDS

ONLINE:

- SAFETY-NET USING PERFORMANCE COUNTER
- EVALUATE: COMPARE MEASUREMENT TO THRESHOLDS
- DETECT AND RECOVER AS NECESSARY

STEPS (OFFLINE)

METRIC SELECTION

ANY QUANTITY THAT CAN BE MEASURED AT RUN-TIME AND LIKELY TO BE AFFECTED WHEN INTERFERENCE OCCURS

E.G. CLOCK CYCLE COUNTERS

METRIC CHARACTERIZATION

METRIC OFTEN NON-DETERMINISTIC

MEASURE METRIC AND PROFILE

GATHER SAMPLES AND FIT TO A KNOWN PROBABILITY DENSITY FUNCTION(PDF)

THRESHOLDS DETERMINATION

DETECTION THRESHOLD: INTERFERENCE HAS OCCURRED

WARNING THRESHOLD: INTERFERENCE MIGHT HAVE OCCURRED

- NEED FURTHER OBSERVATION
- IF OBSERVED CONSECUTIVELY FOR SOME NUMBER OF TIMES, INTERFERENCE HAS OCCURRED

STEPS (ONLINE)

ON-LINE DETECTION

- READ PERFORMANCE COUNTER (METRIC)
- COMPARE TO THRESHOLDS
- IF METRIC ABOVE DETECTION THRESHOLD, RAISE ALARM (CRITICAL)
- IF METRIC BETWEEN WARNING THRESHOLD AND DETECTION THRESHOLD FOR $\propto$ MEASUREMENTS, RAISE WARNING (NON-CRITICAL)

RECOVERY

- GRACEFUL DEGRADATION: ALTERNATE SCHEDULING TO ALLOW TASKS TO COMPLETE WITHIN DEADLINE
- HARD RECOVERY: SWITCH TO AN AVAILABLE HOT STANDBY SPARE GUARANTEED TO RESTORE FUNCTIONALITY OR AT LEAST AVOID CATASTROPHIC CONSEQUENCE

DEMONSTRATION BY REAL-WORLD SIMULATION

- REAL-WORLD SYSTEM FOR EASIER UNDERSTANDING
- FULL USE OF A POWERFUL BOARD
- SYSTEM CHOICE: WATER TOWER SYSTEM

WATER TOWER SYSTEM

Roihuvuori water tower - Helsinki Finland
by Otto-Ville Mikkelä under CC-BY-SA 3.0
Source: Wikipedia
https://en.wikipedia.org/wiki/Water_tower#/media/File:Roihuvuori_water_tower_-_Helsinki_Finland.jpg

A LARGE ELEVATED TANK TO PROVIDE STEADY AND PRESSURIZED WATER TO BUILDINGS

MOST VISIBLE AND MOST COMMON PART OF WATER SUPPLY SYSTEM

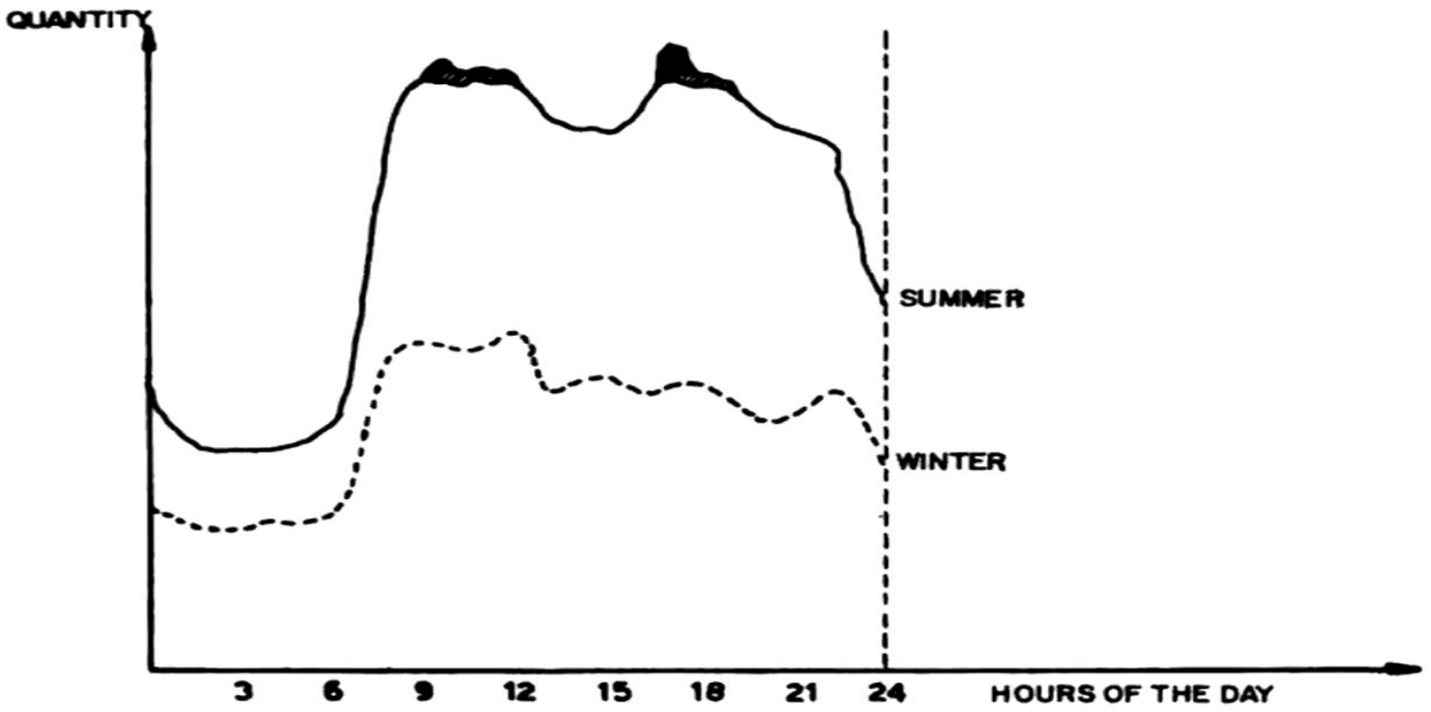
WHY?

- WATER DEMAND VARIES THROUGHOUT THE DAY
- STEADY WATER SUPPLY AND ADEQUATE PRESSURE AND FLOW NECESSARY FOR WATER SUPPLY SYSTEM TO FUNCTION PROPERLY AND CORRECTLY

WATER TOWER ADVANTAGE:

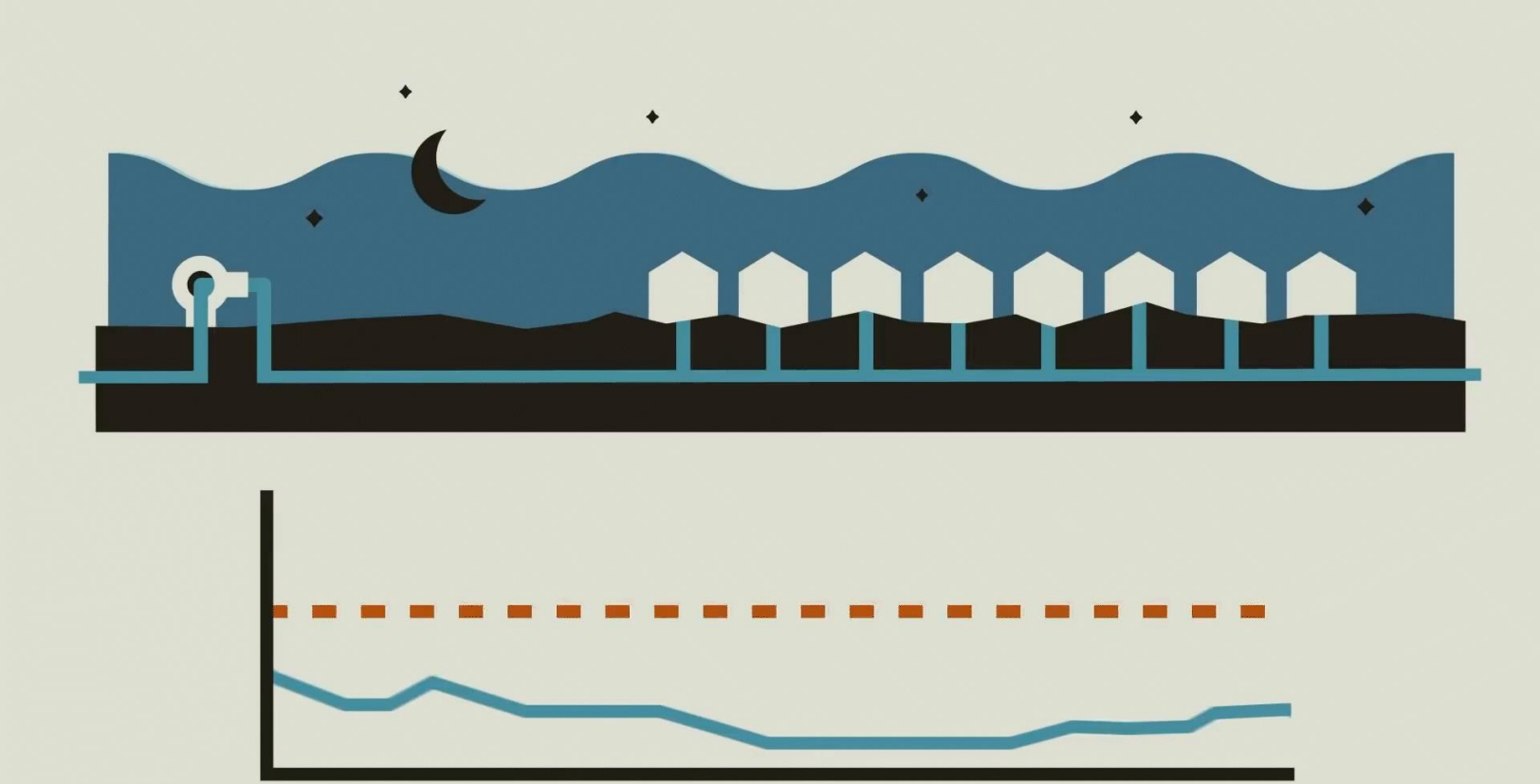
- FULFILL PEAK WATER DEMANDS FROM AVERAGE SIZED PUMP(LESS EXPENSIVE)
- FULFILL DEMAND DURING POWER OUTAGE
- MAINTAIN WATER PRESSURE

TYPICAL HOURLY WATER DEMAND



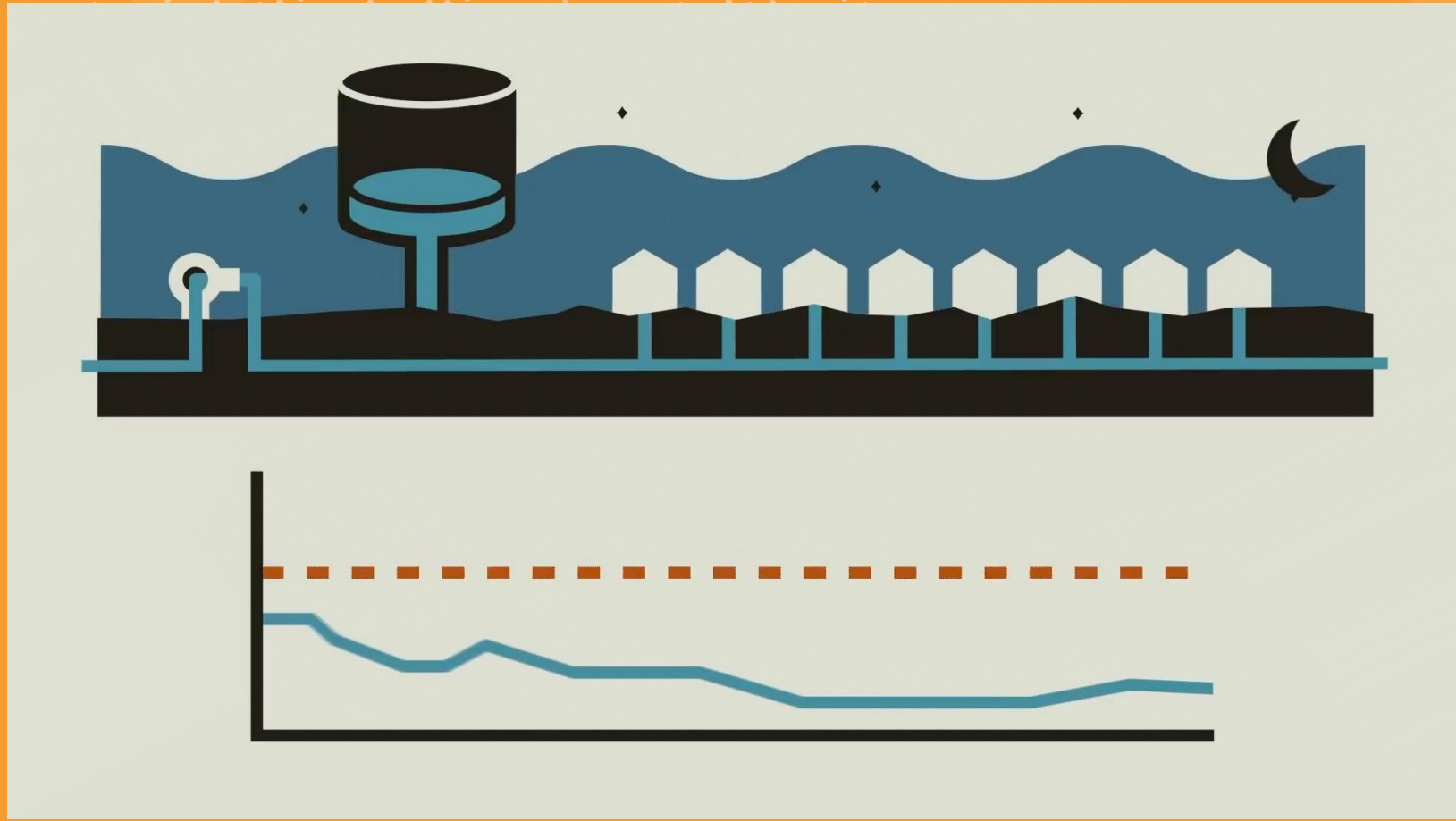
“How Water Towers Work" by Practical Engineering https://www.youtube.com/watch?v=yZwfcMSDBHs.

WITHOUT WATER TOWER



"How Water Towers Work" by Practical Engineering https://www.youtube.com/watch?v=yZwfcMSDBHs.

WATER TOWER SYSTEM



"How Water Towers Work" by Practical Engineering https://www.youtube.com/watch?v=yZwfcMSDBHs.

WATER TOWER SYSTEM SIMULATION

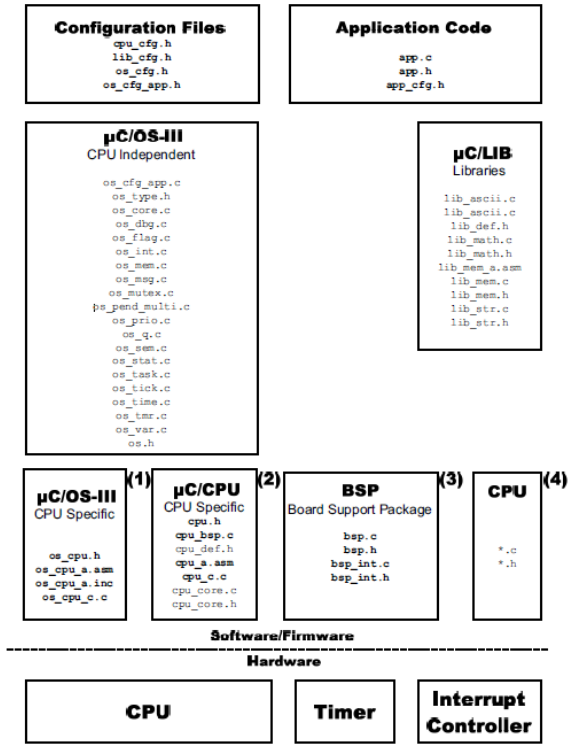
Tank fill and drain simulation

hourly update

Pump running at average demand rate when active

Demand varies depending on hour of the day

Rates are in tank-water-level/hour where a level is arbitrary amount of water.



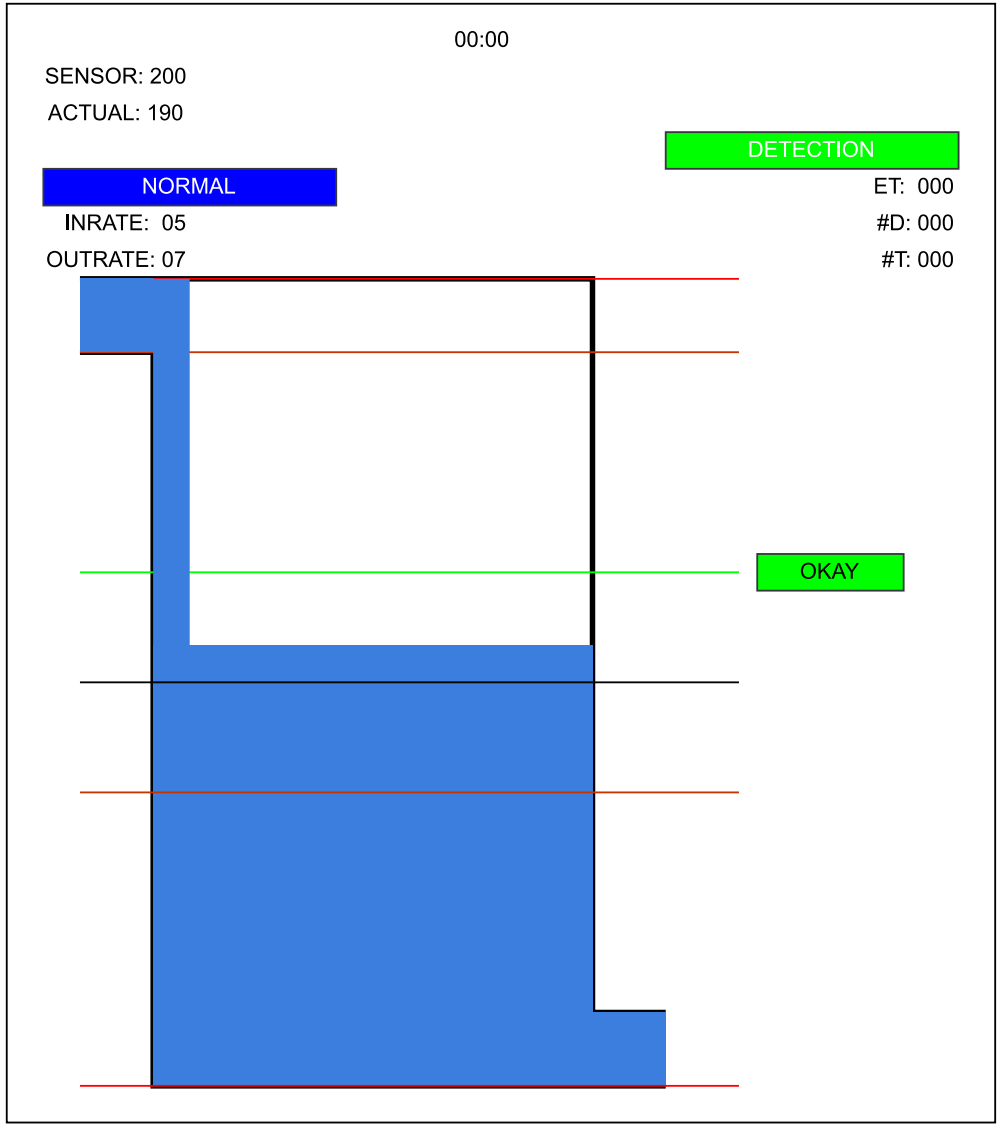
KEIL™
Tools by ARM

LAB SETUP

- BOARD: LANDTIGER V2.0
- OS: μC/OS-III
- µVision IDE - Keil

WATER TOWER SYSTEM: GUI

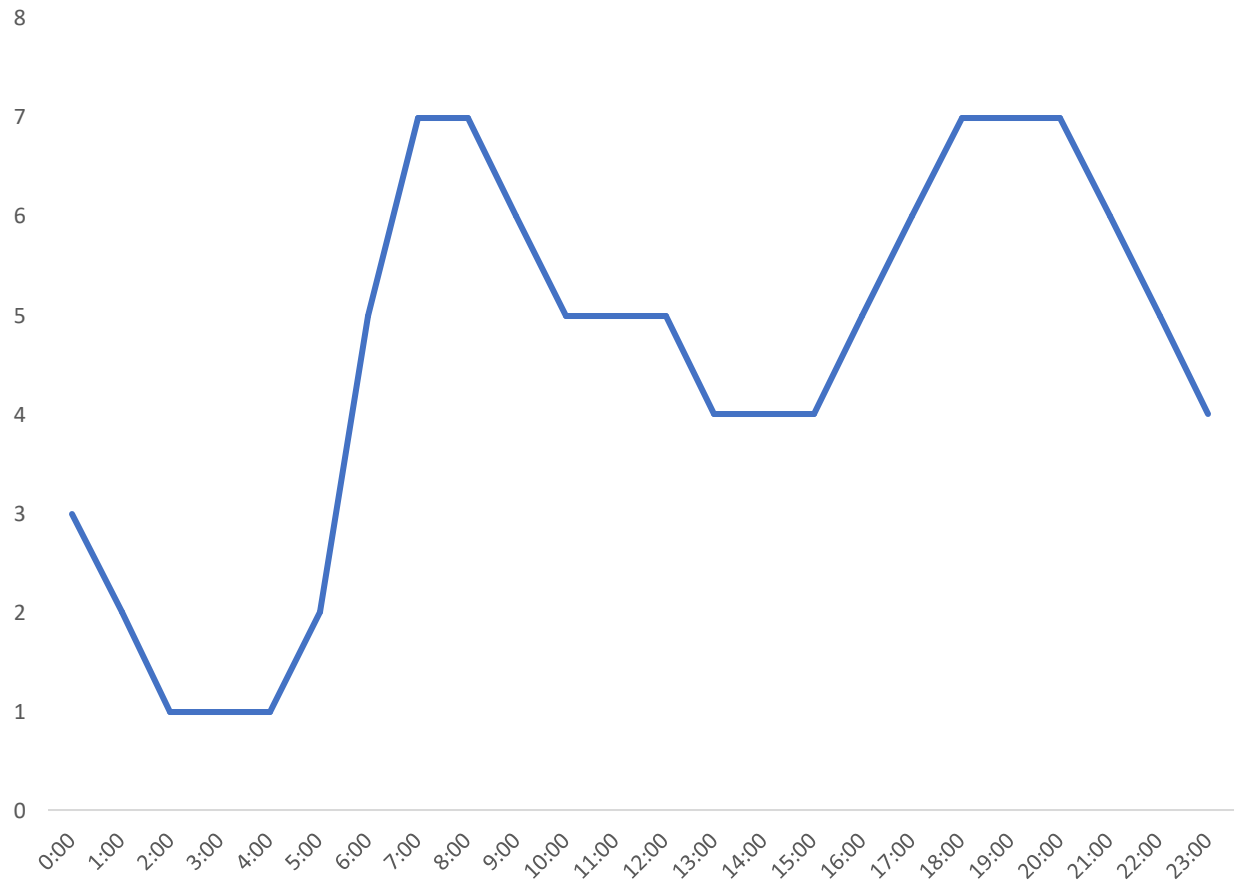
- SENSOR READING
- ACTUAL WATER LEVEL
- INFLOW RATE FROM PUMPS
- OUTFLOW RATE DUE TO DEMAND
- CONTROLLER MODE:
  - NORMAL
  - GRACEFUL DEGRAGATION
  - HARD RECOVERY
- DETECTION : ON/OFF
- EXECUTION TIME
- NUMBER OF DETECTION
- NUMBER OF FAULTS TOLERATED
- WATER LEVEL STATUS



WATER TOWER PARAMETERS

- AVERAGE OUTFLOW RATE DUE TO DEMAND : 5
- DEFAULT INFLOW RATE FROM PUMPS : 5
- TANK BOTTOM LEVEL : 310
- TANK TOP LEVEL : 120
- DESIRED LEVEL : 180
- THRESHOLD HIGH TO STOP PUMPS: 180-40=140
- THRESHOLD LOW TO START PUMPS: 180+40=220

WATER DEMAND SIMULATION



WATER TOWER SYSTEM:IMPLEMENTATION

EXPLOITING THE FUNCTIONALITY OF REAL TIME OS : UC/OS-III

APP TASK:

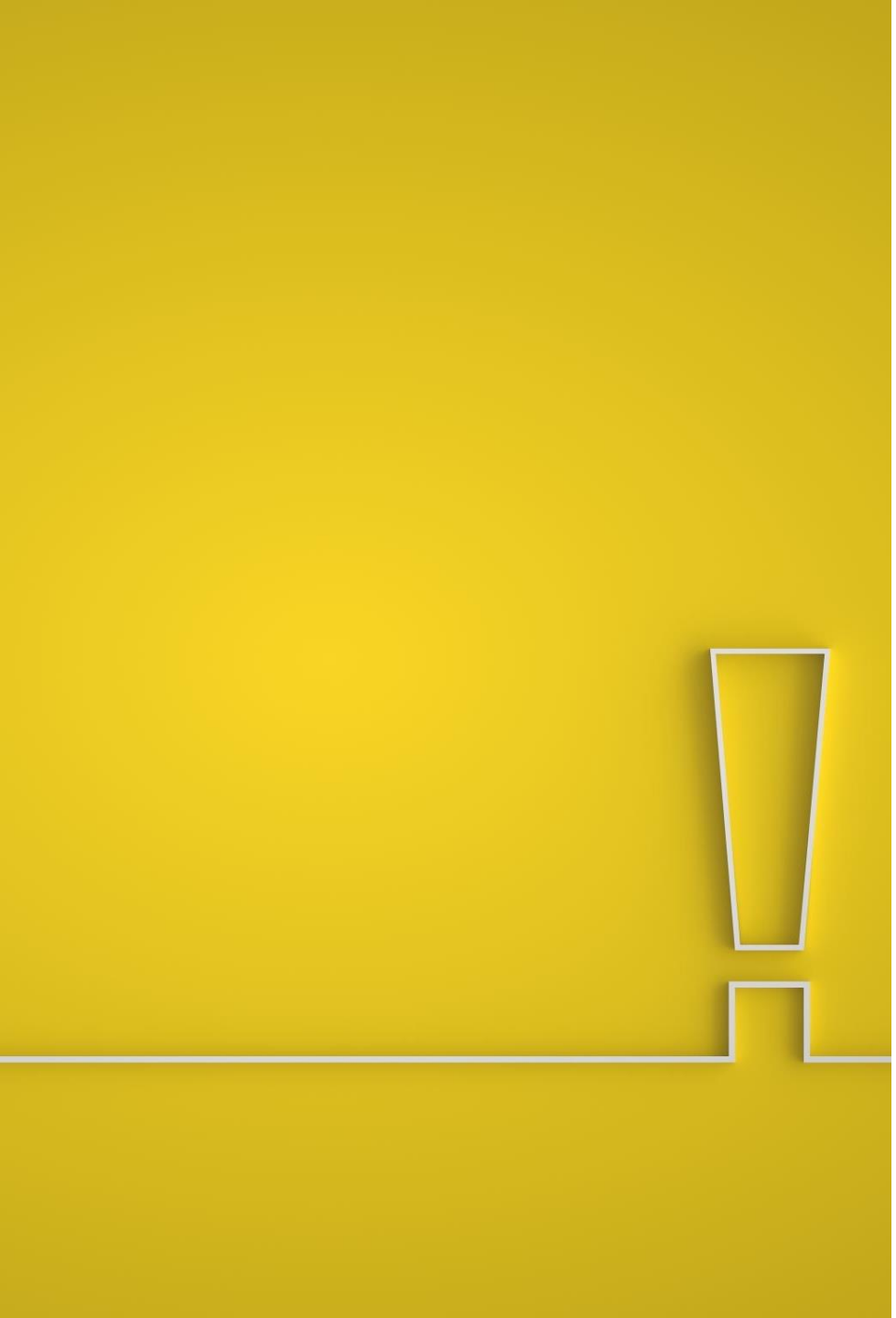
- LOWEST PRIORITY
- MOST FREQUENT USING WHILE(DEF_TRUE) AND NO WAIT
- MONITOR BUTTONS -> LOCKS SCHEDULER -> UPDATE GUI -> UNLOCK SCHEDULER -> REPEAT

GUI TASK:

- UPDATES HOUR THEREFORE THE WATER DEMAND AND ACTUAL WATER LEVEL
- PERIODIC, RUNS AT EACH TICK
- EACH TICK = 1 HOUR INCREMENT

WATER TOWER SYSTEM:IMPLEMENTATION

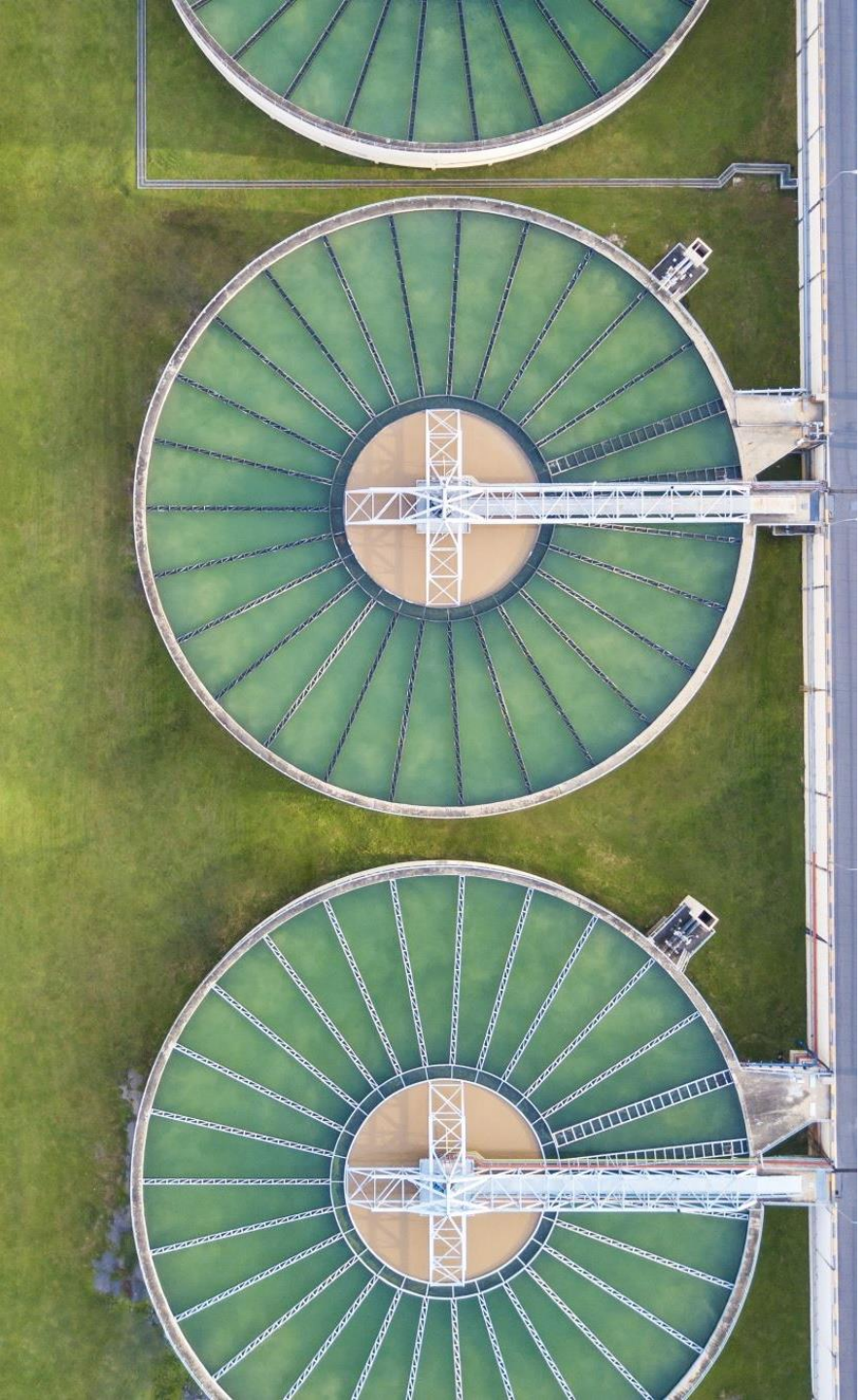
- DETECTOR TASK:
  - CAN BE ACTIVATED USING BUTTON
  - PERIODIC, ALSO RUNS AT EACH TICK
  - IMPLEMENTS THE INTERFERENCE DETECTION AND RAISES ALARM/WARNING TO THE CONTROLLER
- CONTROLLER TASK:
  - RESPONSIBLE OF OPENING/CLOSING VALVES THAT FILL AND DRAIN THE TANK.
  - ALSO RESPOND TO THE RASED ALARM/WARNING FROM THE DETECTOR BY STARTING RECOVERY ACTION.
  - PERIODIC, RUNS AT EVERY TWO TICKS.
  - CAN BE TAKEN AS USING 1 TICK FOR TANK CONTROL WHILE USING OTHER TICK TO DO OTHER SYSTEM OPERATIONS THAT TAKE 1 TICK TO FINISH.
  - BEHAVIOUR: IT STARTS SENSOR, WHILE SENSOR PREPARES READING PERFORMS OTHER OPERATIONS AND ONLY AFTER THEIR COMPLETION, READS VALUE FROM SENSOR AND CONTROLS VALVES ACCORDINGLY.



SOFT ERROR INJECTION

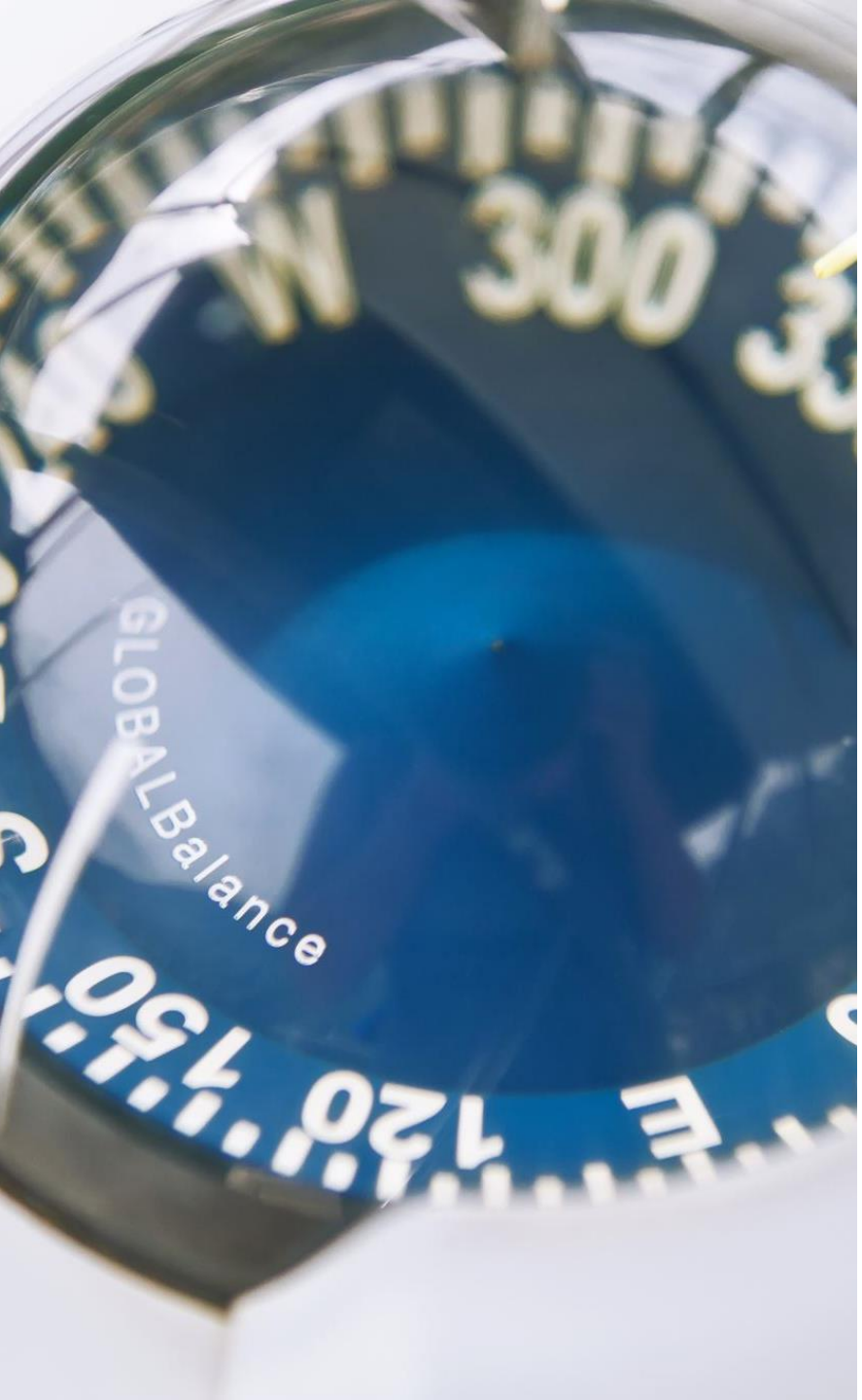
- RANDOM BIT FLIP ON THE SENSOR READING
- WILL IT INTRODUCE ERROR?
  - YES, CONTROLLER TASK STARTS SENSOR AND ONLY READS THE VALUE AFTER FINISHING OTHER OPERATIONS. IN THIS TIME, FAULT INJECTION CAN CHANGE THE READING AND THEREFORE CONTROLLER BEHAVIOUR.

IMPLEMENTING INTERFERENCE DETECTION BASED ON PERFORMANCE MONITORS



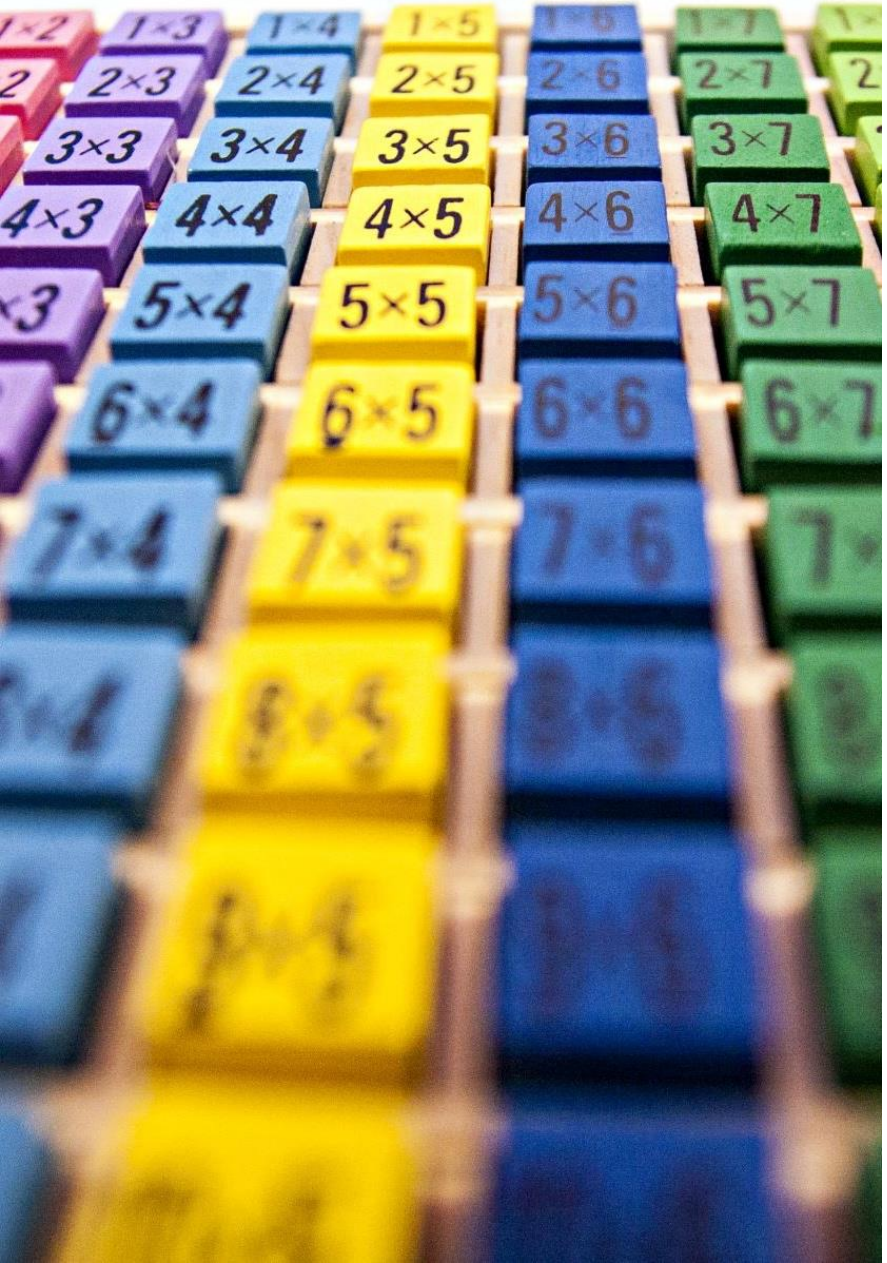
METRIC SELECTION

- ANY QUANTITY THAT CAN BE MEASURED AT RUN-TIME AND LIKELY TO BE AFFECTED WHEN INTERFERENCE OCCURS
  - WHEN TANK GETS FULL, THE WATER WILL OVERFLOW WHICH CAN BE SAFELY REDIRECTED
  - WHEN TANK GETS EMPTY THOUGH, THE WATER PRESSURE IN THE DISTRIBUTION NETWORK DECREASES AND MAY EVENTUALLY STOP WATER SUPPLY TO HOMES AND BUSINESSES.
  - IN EMERGENGY SUCH AS HOUSE FIRE THERE WILL NOT BE ENOUGH WATER AVAILABLE
  - OVERALL -> CATASTROPHICAL CONSEQUENCES!
  - EMPTY TANK SITUATION MUST BE AVOIDED



METRIC SELECTION

- IN WATER TOWER SYSTEM, THE QUANTITY THAT WILL MOST LIKELY BE AFFECTED DUE TO FAULTY SENSOR READING IS THE WATER LEVEL.
- DUE TO VARYING WATER DEMAND AND CONTROLLER ACTIONS, THE WATER LEVEL FLUCTUATES THROUGHOUT THE DAY.
- WHEN WATER LEVEL GETS LOW, CONTROLLER STARTS FILLING THE TANK.
- IN ORDER TO IMPLEMENT SAFETY-NET USING PERFORMANCE COUNTER, WE CAN THEN MEASURE THE TIME WATER LEVEL STAYS BELOW A CERTAIN LEVEL BEFORE RISING BACK AGAIN.
- IF INTERFERENCE OCCURS PREVENTING CONTROLLER FROM DETECTING LOW WATER LEVEL, THIS SHOULD RESULT IN LONGER TIME FOR THE WATER LEVEL TO RISE BACK.

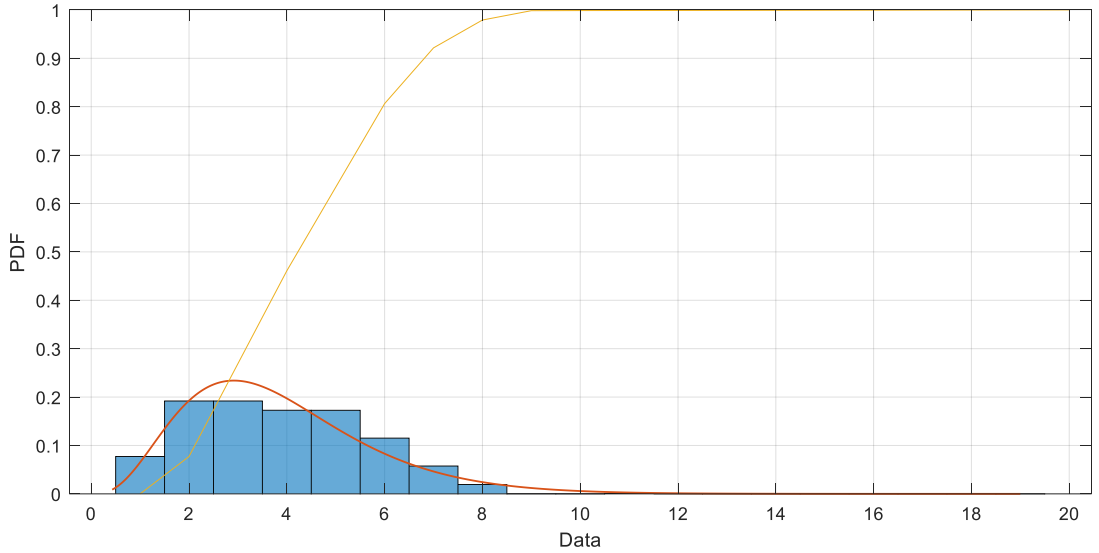


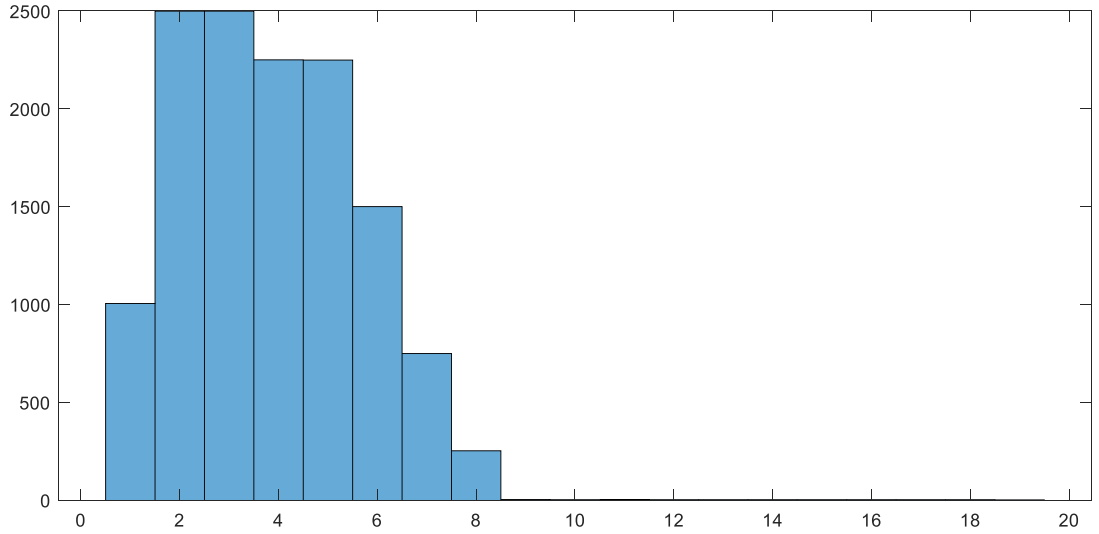
METRIC CHARACTERIZATION

- SINCE THE TASK ACTIVATIONS HAVE BEEN SYNCHRONIZED USING TIMERS, ALMOST EXACT WORKING CAN BE SIMULATED IN MATLAB.

METRIC CHARACTERIZATION

- 10000 DAYS SIMULATION
- RIGHT:
  - X: Time taken to rise back above threshold
  - Y: Number of occurrences
- LEFT: fitted to gamma pdf





THRESHOLD DETERMINATION

- WARNING THRESHOLD : 15 TICKS
- $\propto$, NUMBER OF CONSECUTIVE WARNINGS FOR DETECTION: 3
- DETECTION THRESHOLD: 25 TICKS

ONLINE DETECTION

- IN THE DETECTOR TASK
- START TIMING TICKS EVERYTIME THE WATER-LEVEL FALLS BELOW LOW WATER LEVEL THRESHOLD.
  - WE CAN SAY, IT IS MONITORING A FLOAT SWITCH THAT CHANGES STATE WHEN FLOATING VS WHEN NO WATER TO FLOAT
  - NO FAULTY SENSOR READING INTERFERANCE ON THE DETECTOR

ONLINE DETECTION

- IF THE TIMER CROSSES DETECTION THRESHOLD, IMMEDIATELY RAISE ALARM SIGNAL AND WAKE UP CONTROLLER
- IF THE WATER LEVEL RISES BACK BEFORE DETECTION THRESHOLD,BUT AFTER WARNING THRESHOLD, INCREASE A COUNTER.
  - REPEAT IF THIS OCCURS THE NEXT TIME WATER LEVEL FALLS BELOW LOW THRESHOLD UNTIL COUNTER CROSSES $\propto$ IN WHICH CASE RAISE WARNING SIGNAL AND WAKE CONTROLLER.
  - OTHERWISE, IF NEXT TIME WATER LEVEL RISES BEFORE WARNING THRESHOLD, THEN RESET COUNTER.

RECOVERY

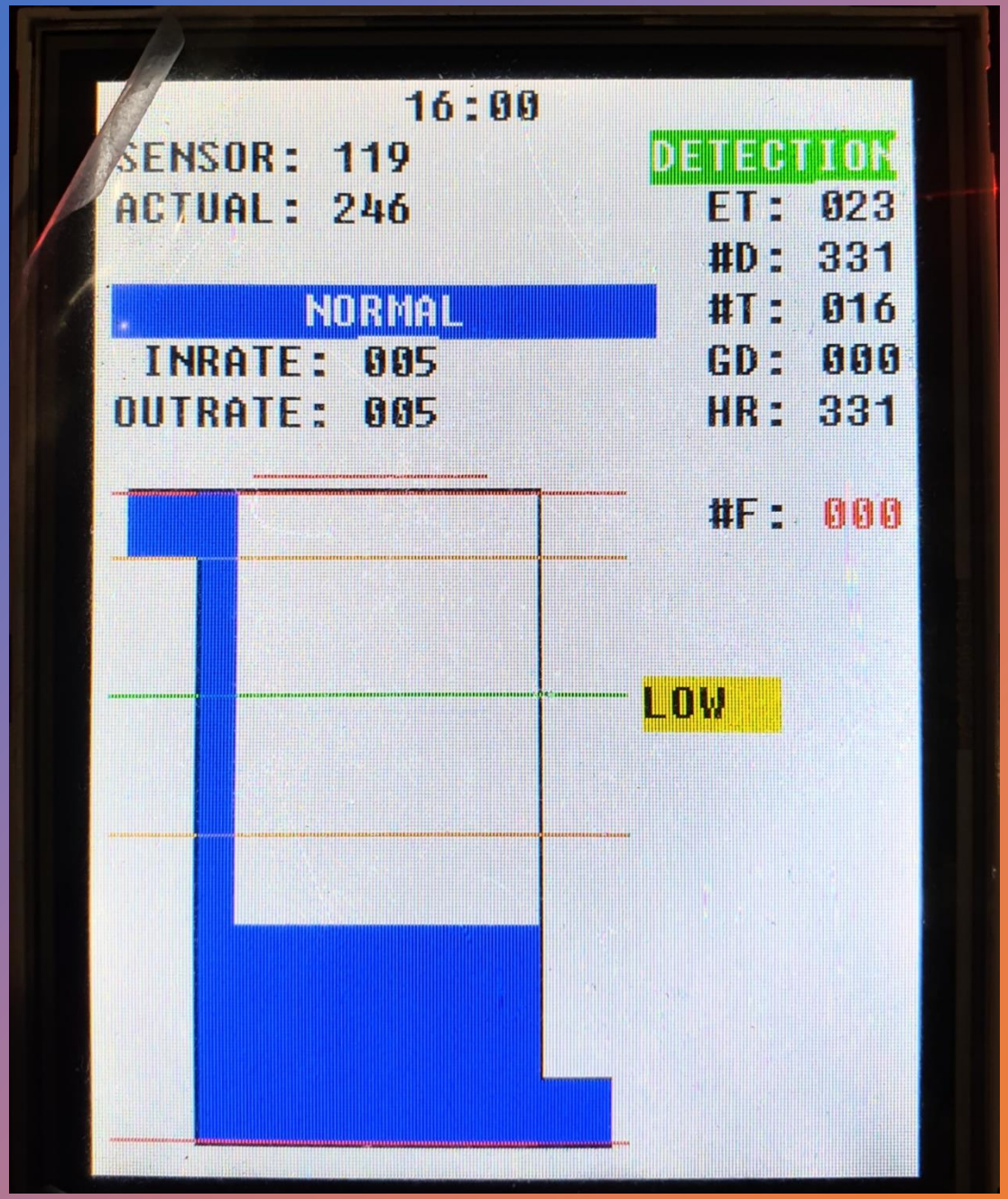
- IN CONTROLLER TASK
- NORMAL MODE:
  - WHEN NO SIGNAL IS RAISED BY DETECTOR
  - OPEN IN-VALVE WHEN SENSOR READING IS LOWER THAN LOW WATER THRESHOLD
  - CLOSE IN-VALVE WHEN SENSOR READING IS HIGHER THAN HIGH WATER THRESHOLD

RECOVERY

- GRACEFUL DEGRADATION:
  - WHEN WARNING SIGNAL RAISED BY DETECTOR
  - SCHEDULE CHANGE
  - CONTROLLER RESTARTS SENSOR, WAITS AND IMMEDIATELY READS THE SENSOR VALUE AND THEN AFTER CONTROLLING THE VALVES SAME WAY AS IN NORMAL MODE, PERFORMS OTHER TASKS.
  - RETURN TO NORMAL MODE, WHEN THE DETECTOR SIGNALS THAT WATER LEVEL HAS RISEN ABOVE LOW THRESHOLD

RECOVERY

- HARD RECOVERY:
  - WHEN ALARM SIGNAL IS RAISED BY DETECTOR
  - RESTART SENSOR AND READ IMMEDIATELY LIKE IN GRACEFUL DEGRADATION
  - INCREASE IN-FLOW PUMP RATE BY 20% AND LIMIT PEAK OUT-FLOW TO THE NEW-INFLOW RATE
    - WATER LEVEL EITHER CONSTANT OR INCREASES
  - RETURN TO NORMAL MODE, WHEN THE DETECTOR SIGNALS THAT WATER LEVEL HAS RISEN ABOVE LOW THRESHOLD

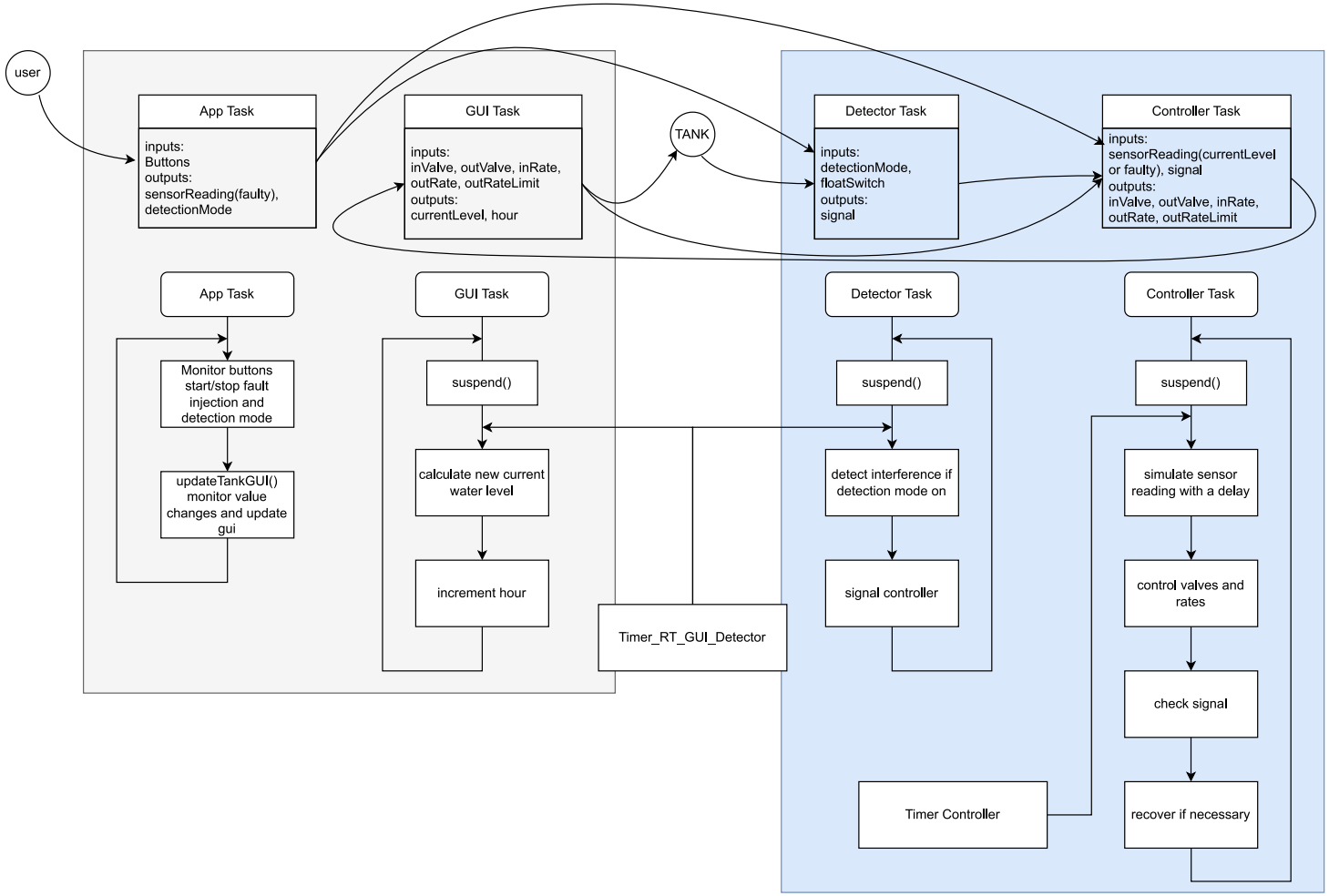


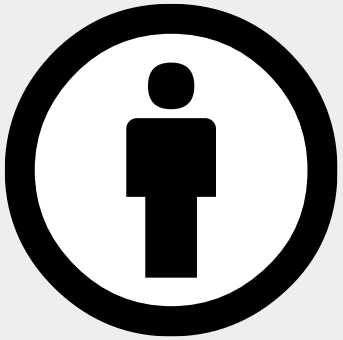
RESULT AFTER ~30 MIN RUN WITH FAULT INJECTION

- #INTERFERENCE DETECTED: 331
- #POTENTIAL INTERFERENCE TOLERATED: 016
- #GRACEFUL DEGREDATION: 0
- #HARD RECOVERY: 331
- #TANK EMPTIED: 0

DIY

- Tank is independent and provides interface (variables) for the microcontroller
- Can implement your own controller and detector using the input and output variables available for the tasks.
- Template and configuration files are provided





PROJECT 6 REAL-TIME SAFETY AND FAULT INJECTION: LAB DEMONSTRATION

BY: ANDREAS SANDSMARK BAKKE, BIPIN THAPA, HEBA MAHMOUD MOHAMED EMAD HASSAN

"This material was originally developed as part of an assignment of the Operating systems for embedded systems course delivered at Politecnico di Torino by Prof. Stefano Di Carlo".


Thank you