Elevator alarm system

51.702 – Security by Design Project

Group 5

- Zhang Zidong, 1008528
- Harish Navnit, 1008538
- Tang Fei, 1008558

Intro - Background

A system closely related to daily life and ubiquitous.

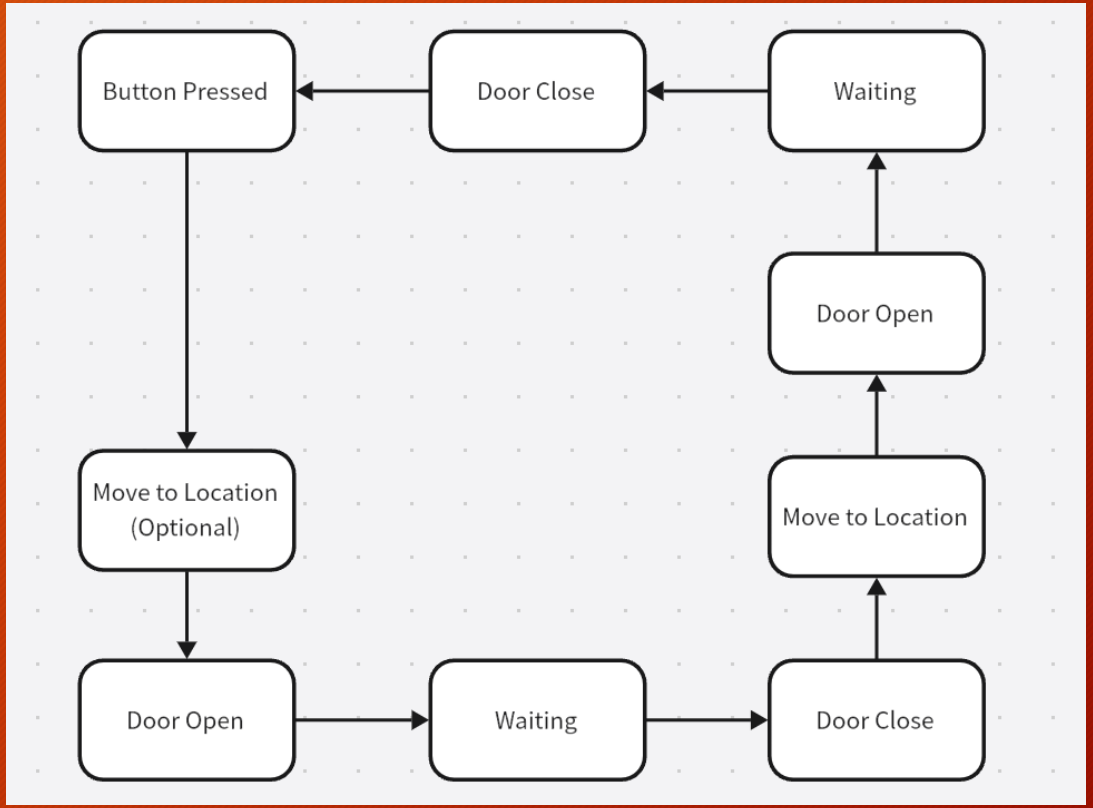
- High frequency usage
- High safety requirements
- Real-time
- Space constraints
- Emergency response mechanism
- Reliability

Intro - Component 1

FLOOR 1

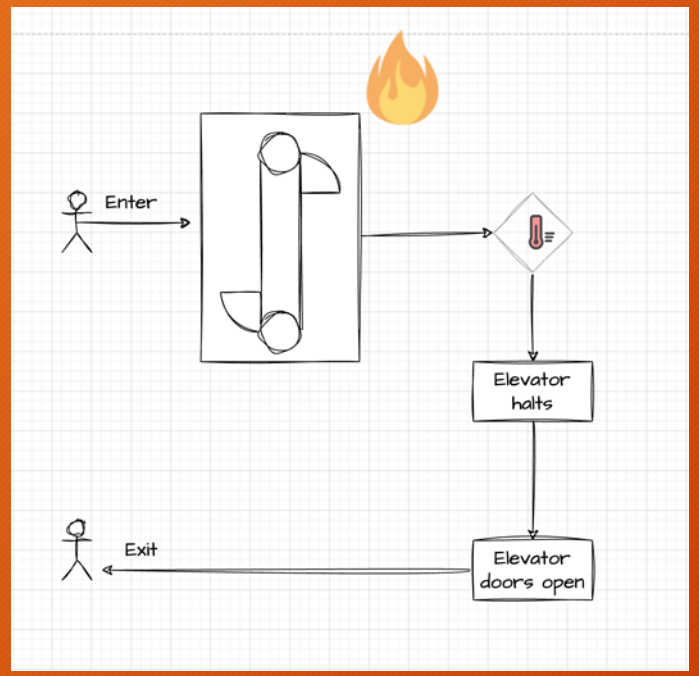
ELE

FLOOR 2



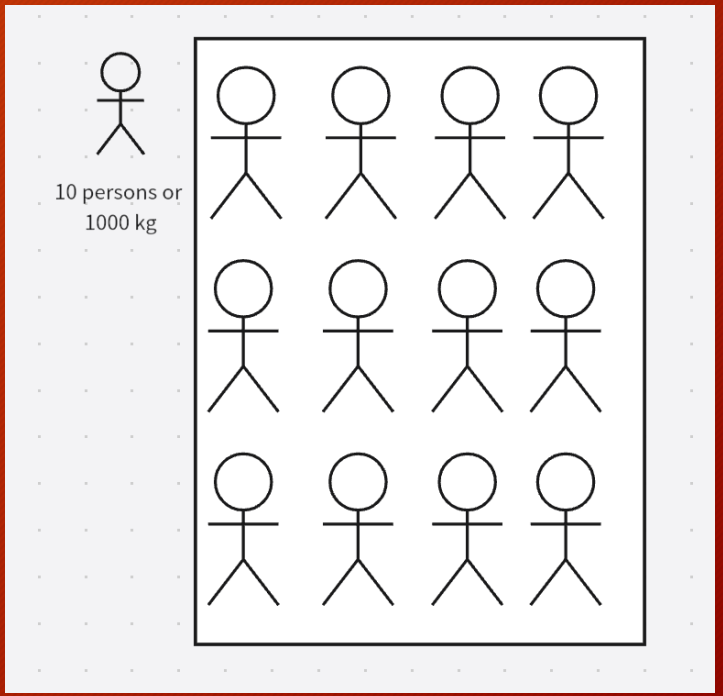
Intro – Component 2

Temperature Sensor

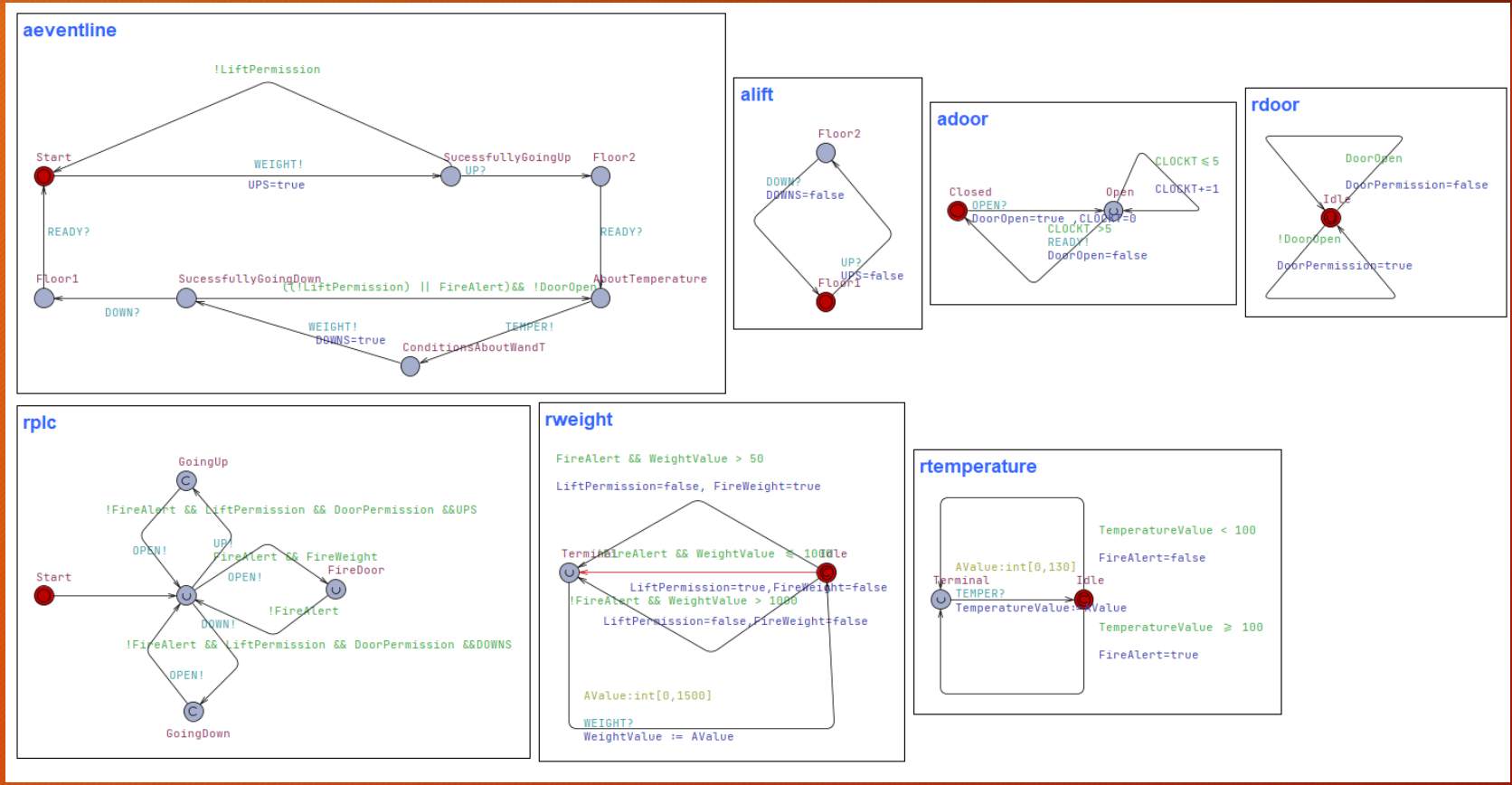


- Abnormal behavior detected
- Keep the door opening
- Elevator turns inactive
- Wait until back to normal

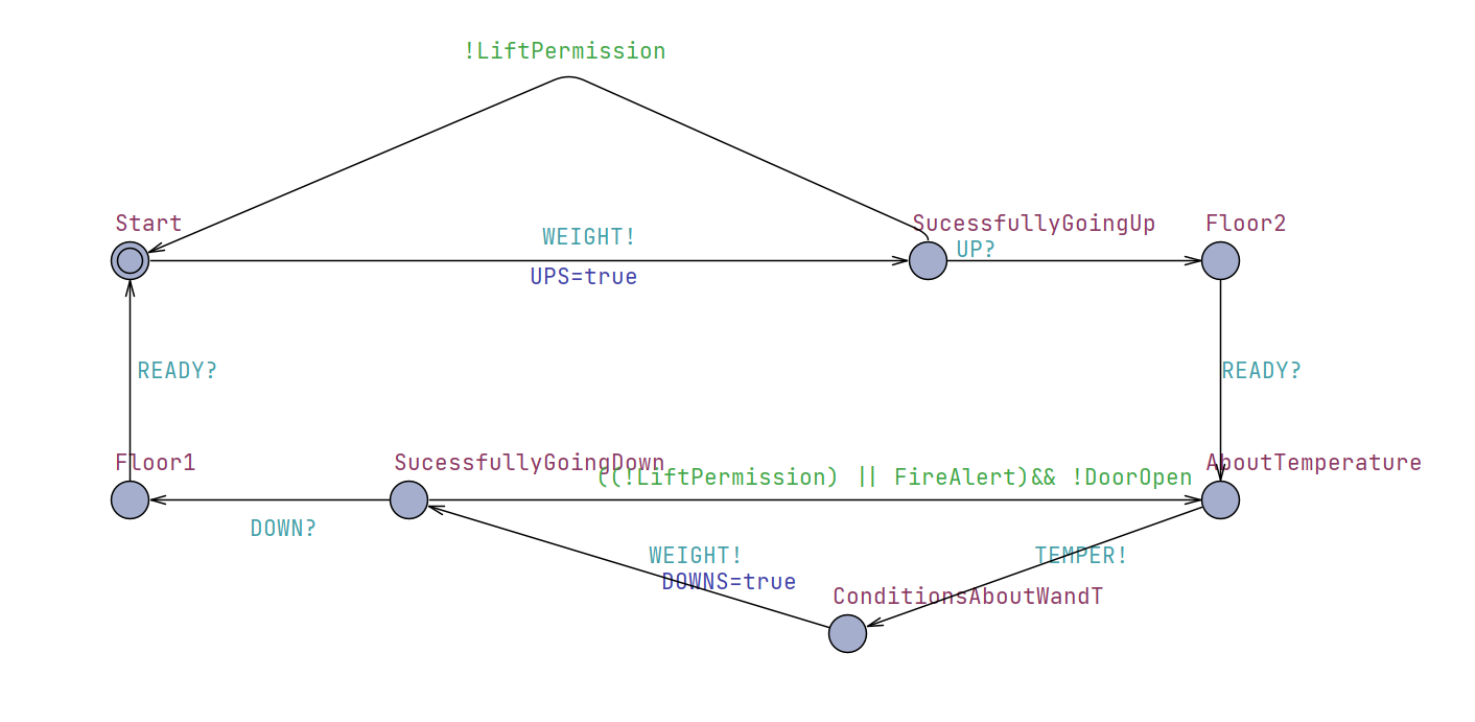
Weight Sensor

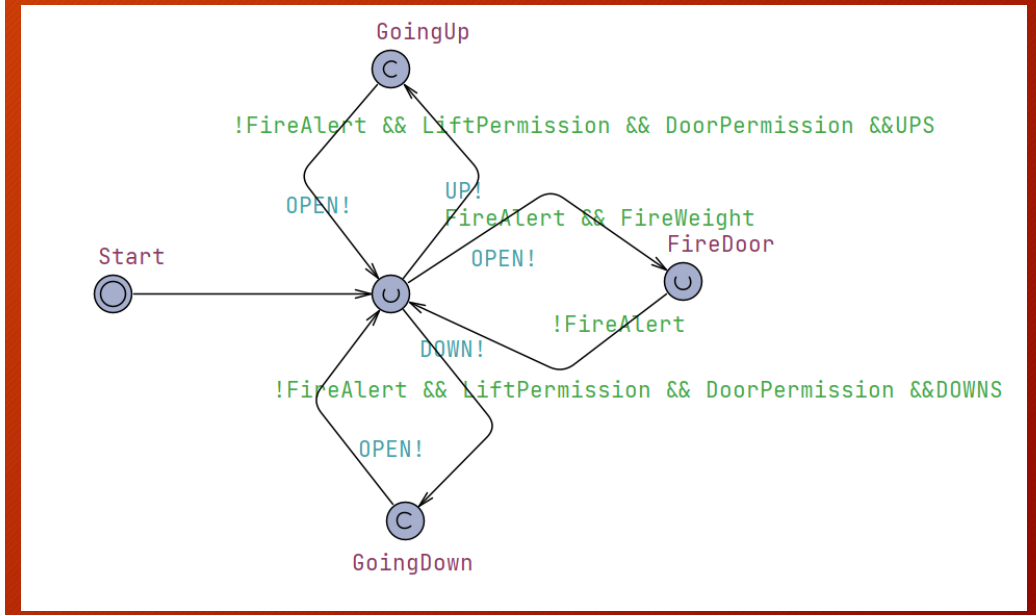


UPPAAL

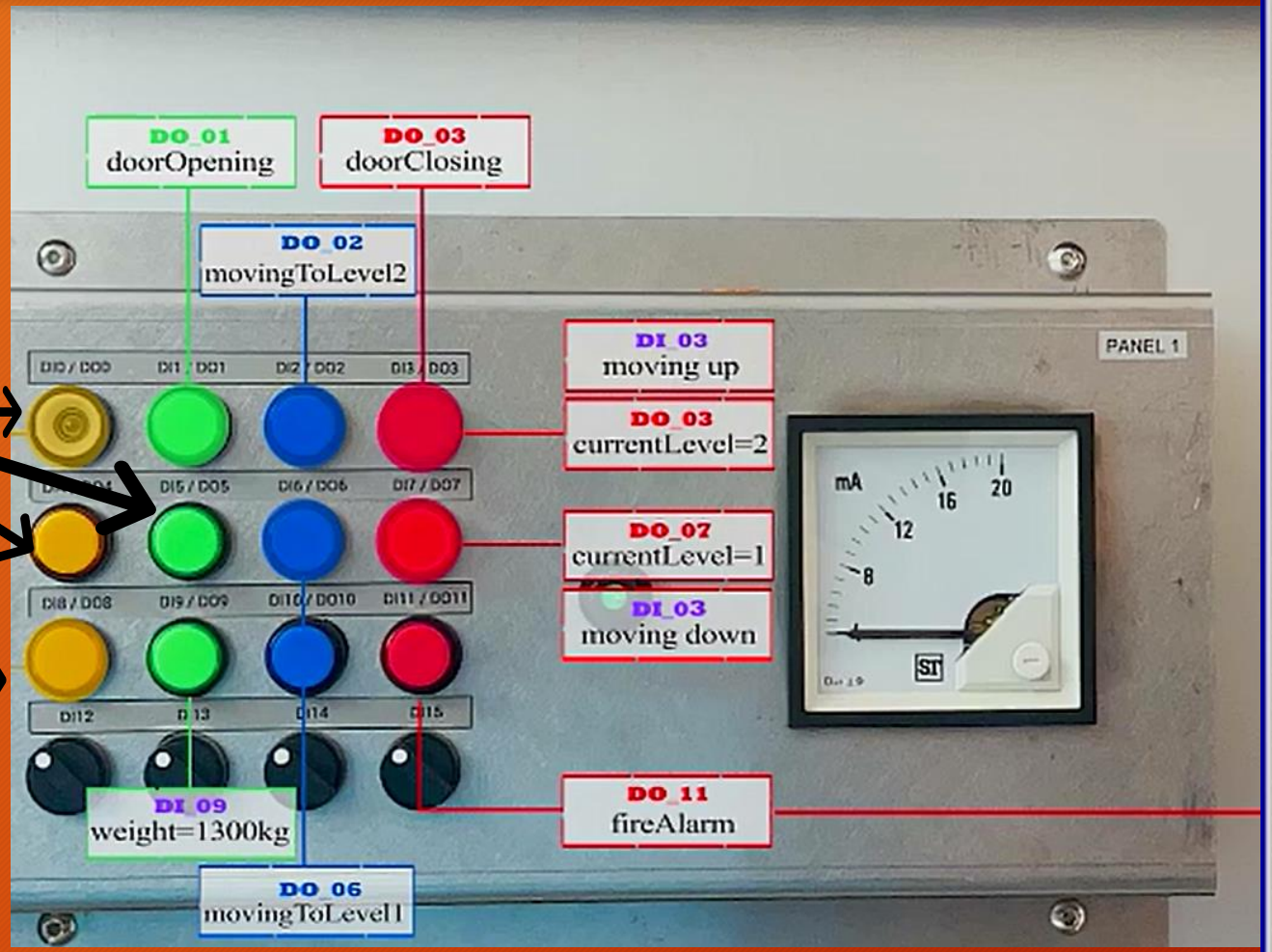

aeventline
!LiftPermission
Start
WEIGHT!
UPS=true
SucessfullyGoingUp
UP?
Floor2
READY?
READY?
Floor1
SucessfullyGoingDown
((!LiftPermission) || FireAlert)&& !DoorOpen
AboutTemperature
DOWN?
WEIGHT!
DOWNS=true
TEMPER!
ConditionsAboutWandT
alift
Floor2
DOWN?
DOWNS=false
UP?
UPS=false
Floor1
adoor
Closed
OPEN?
DoorOpen=true
Open
CLOCKT≤5
CLOCKT+=1
CLOCKT ==5
READY!
DoorOpen=false
rdoor
DoorOpen
DoorPermission=false
Idle
!DoorOpen
DoorPermission=true
rplc
GoingUp
!FireAlert && LiftPermission && DoorPermission &&UPS
OPEN!
UP!
FireAlert && FireWeight
FireDoor
Start
OPEN!
!FireAlert
DOWN!
!FireAlert && LiftPermission && DoorPermission &&DOWNS
OPEN!
GoingDown
rweight
FireAlert && WeightValue > 50
LiftPermission=false, FireWeight=true
Terminal
FireAlert && WeightValue ≤ 1000
Idle
LiftPermission=true,FireWeight=false
!FireAlert && WeightValue > 1000
LiftPermission=false,FireWeight=false
AValue:int[0,1500]
WEIGHT?
WeightValue := AValue
rtemperature
AValue:int[0,130]
Terminal
Idle
TEMPER?
TemperatureValue:=AValue
TemperatureValue < 100
FireAlert=false
TemperatureValue ≥ 100
FireAlert=true

UPPAAL – Event & Decision Logic





PLC



Watch

Current Routine

Name	Scope	Value
ButtonLevel1	MainProgram	0
ButtonLevel2	MainProgram	0
currentLevel	MainProgram	1
DI_03	Controller	0
DI_07	Controller	0
DI_08	Controller	0
DI_09	Controller	0
DO_00	Controller	0
DO_01	Controller	0
DO_02	Controller	0
DO_03	Controller	0
DO_04	Controller	0
DO_05	Controller	0
DO_06	Controller	0
DO_07	Controller	1
DO_08	Controller	0
DO_11	Controller	0
doorClosing	MainProgram	0
doorOpen	MainProgram	0
doorOpening	MainProgram	0
fireAlarm	MainProgram	0
MAX_TEMP	MainProgram	28.0
MAX_WEIGHT	MainProgram	1200.0
moving	MainProgram	0
movingToLevel1	MainProgram	0
movingToLevel2	MainProgram	0
Temp1	Controller	25.607834
ThresTemp	Controller	30.0
TON	Controller	{...}
TON.DN	Controller	1
TON.PRE	Controller	3000
TON.Reset	Controller	0
TON.TimerEnable	Controller	1

Simulation - Data

- Fire_Alert
- OverWeight
- Moving
- Moving to L1
- Moving to L2
- DoorOpen
- Temp
- MAX_TEMP
- Weight
- MAX_WEIGHT
- CurrentLevel
- ButtonLevel1
- ButtonLevel2
- Attack-Type

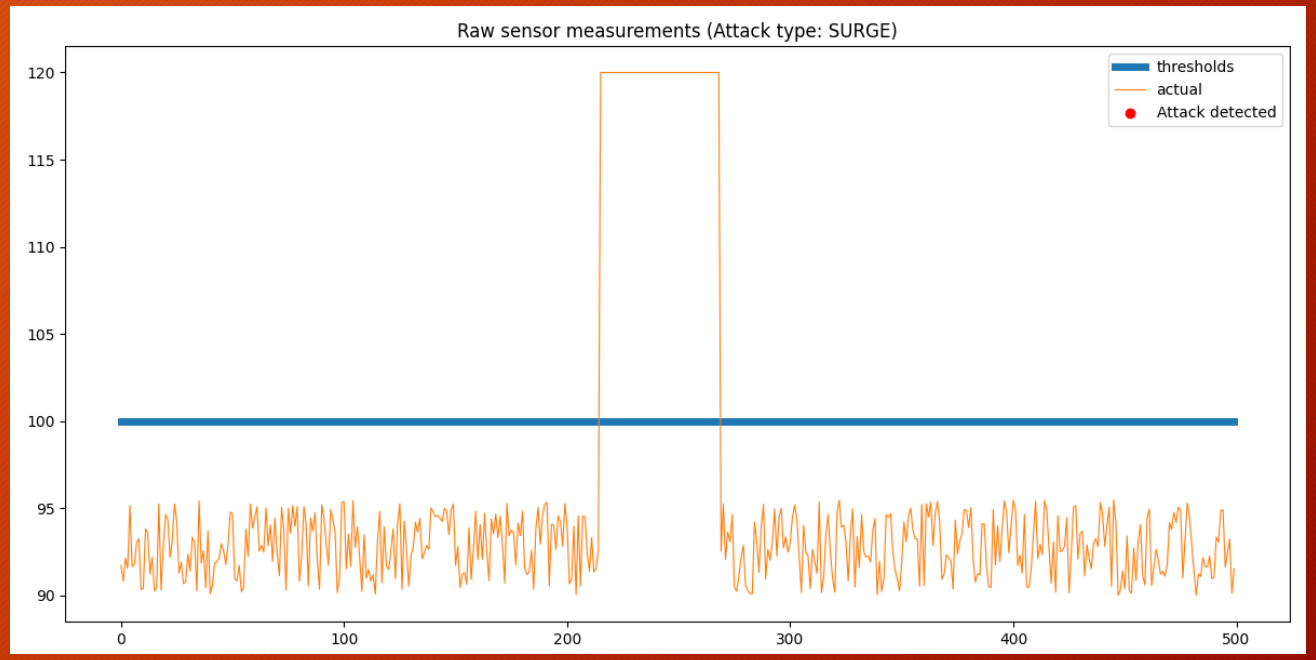
```
******  Simulation Run #6 *****
Attack type: ATTACK_MAX_WEIGHT
Attack started at t: 178
Attack ended at t: 224

******  Simulation Run #7 *****
Attack type: ATTACK_MAX_TEMP
Attack started at t: 192
Attack ended at t: 203

******  Simulation Run #8 *****
Attack type: BUTTON_ATTACK
Attack started at t: 100
Attack ended at t: 179

******  Simulation Run #9 *****
Attack type: BUTTON_ATTACK
Attack started at t: 32
Attack ended at t: 122

******  Simulation Run #10 *****
Attack type: RANDOM
Attack started at t: 290
Attack ended at t: 374

Number of simulations with attacks: 10
Time elapsed: 2.86004580000008 seconds
```

Simulation - Attack

- ATTACK_TYPE_ATTACK_MAX_TEMP
- ATTACK_TYPE_ATTACK_MAX_WEIGHT
- ATTACK_TYPE_BIAS
- ATTACK_TYPE_BUTTON_ATTACK
- ATTACK_TYPE_NONE
- ATTACK_TYPE_RANDOM
- ATTACK_TYPE_SURGE

- MAX_TEMP
- MAX_WEIGHT
- Temp or Weight
- States of ELE

Example - Surge



Detection

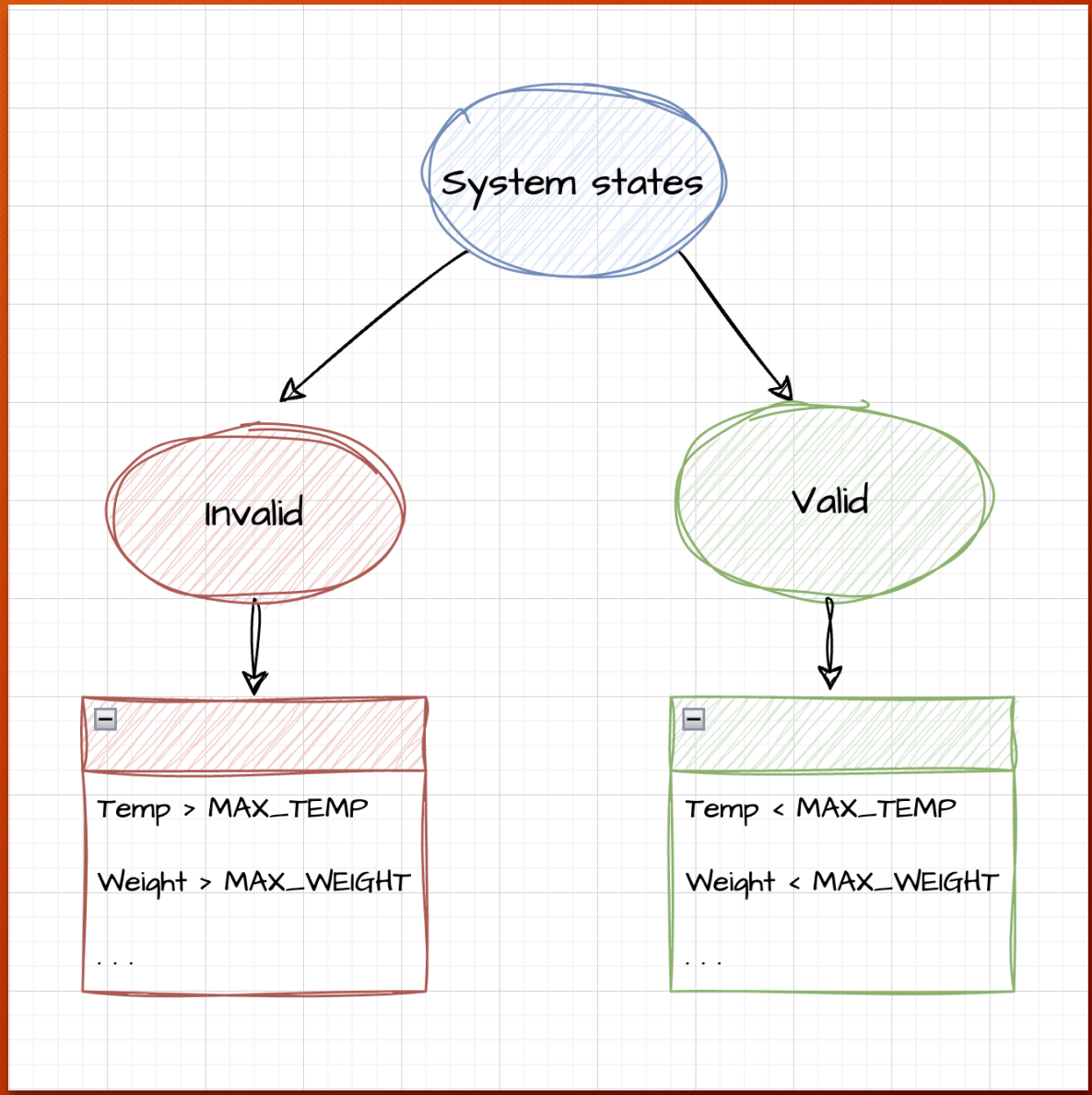
A System can enter any state

- Allowed (valid)
- Restricted (valid)

A system consists of

- Sensors (analog)
- Components (binary)

Anomaly Detection = Monitoring a system's state + values of sensors & components



Detection

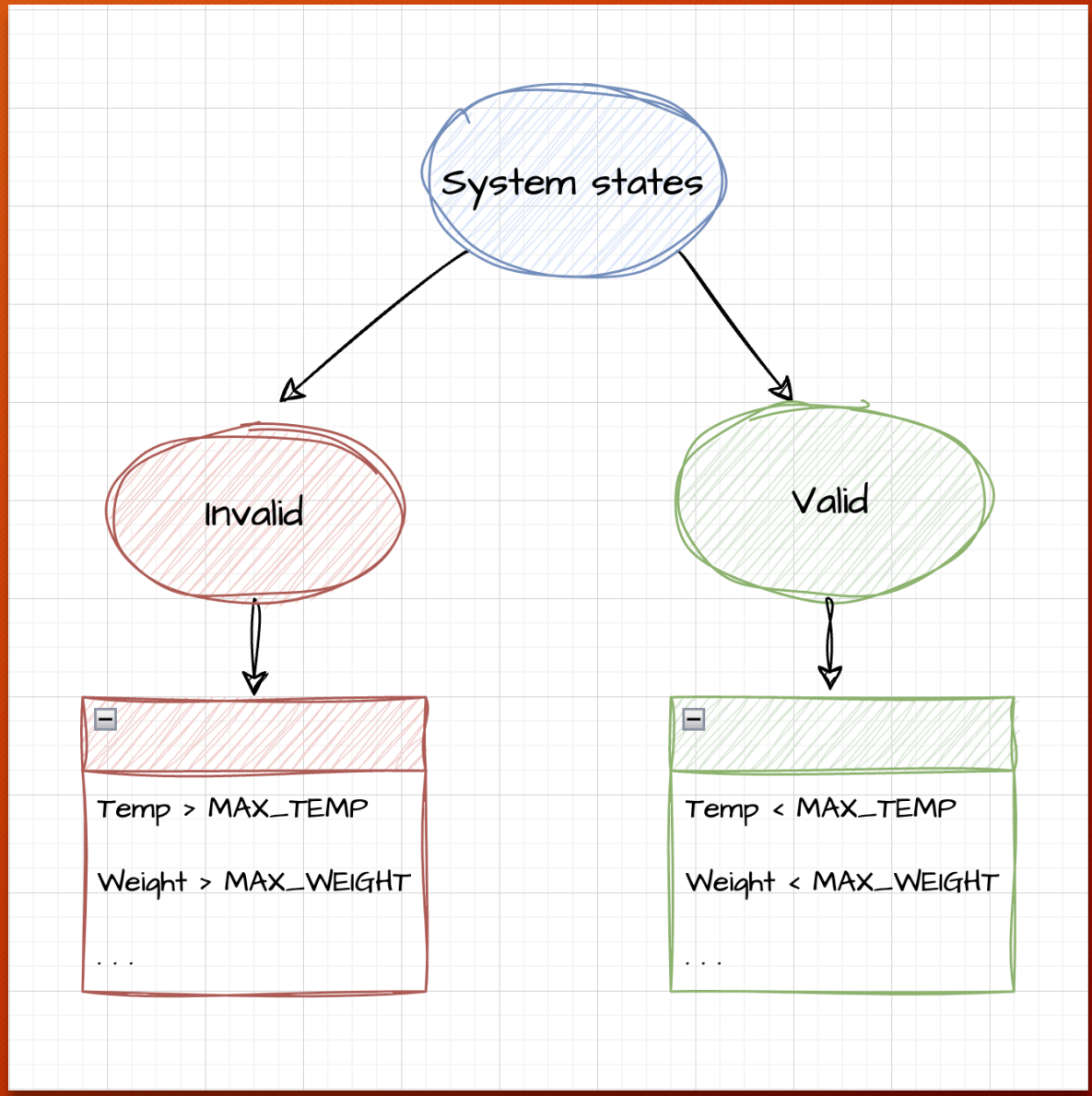
A System can enter any state

- Allowed (valid)
- Restricted (valid)

✅ Verify the combination of current state parameters.

✅ Check if the combination of state parameters falls into an allowed or restricted state.

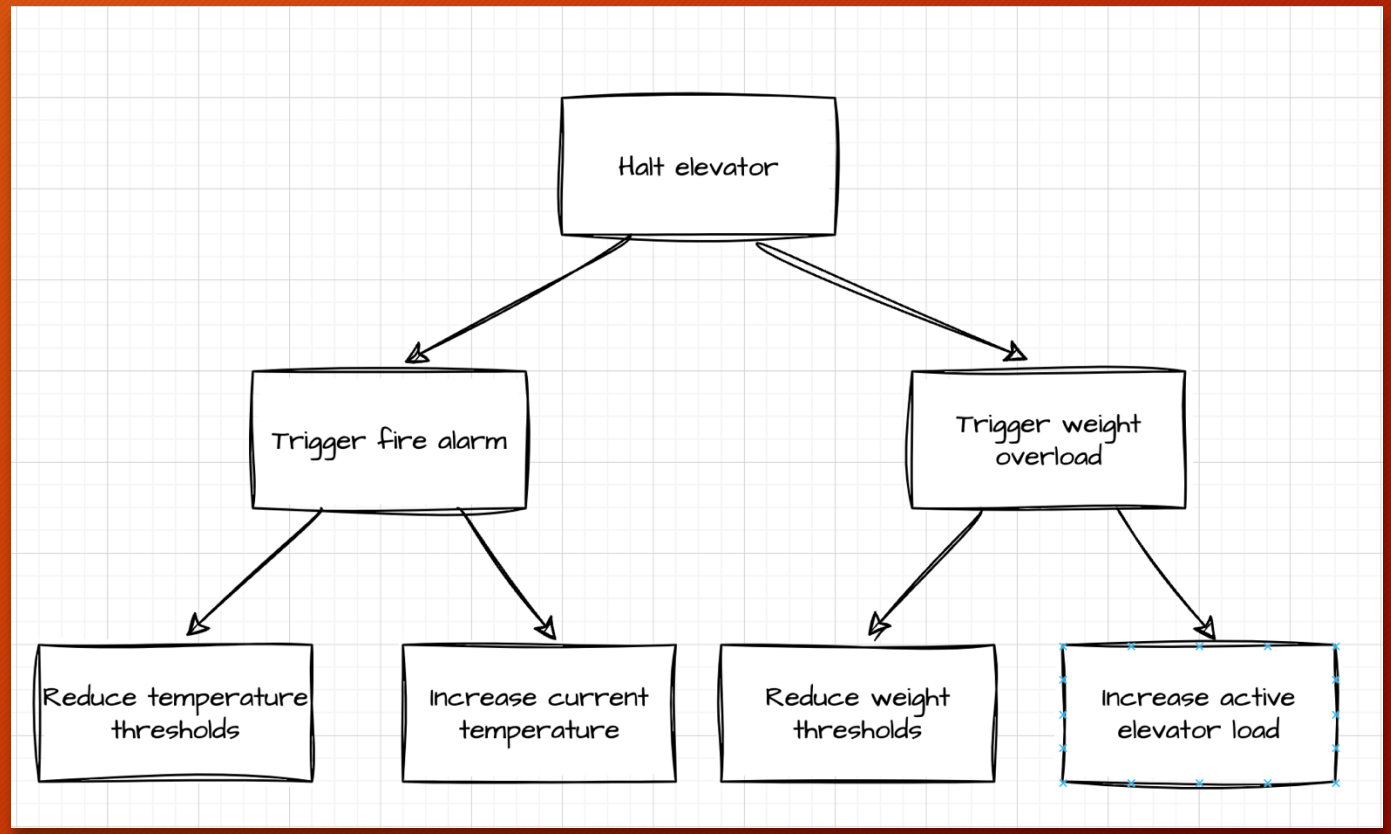
✅ State monitoring allows us to **completely eliminate** false-positives.



Detection

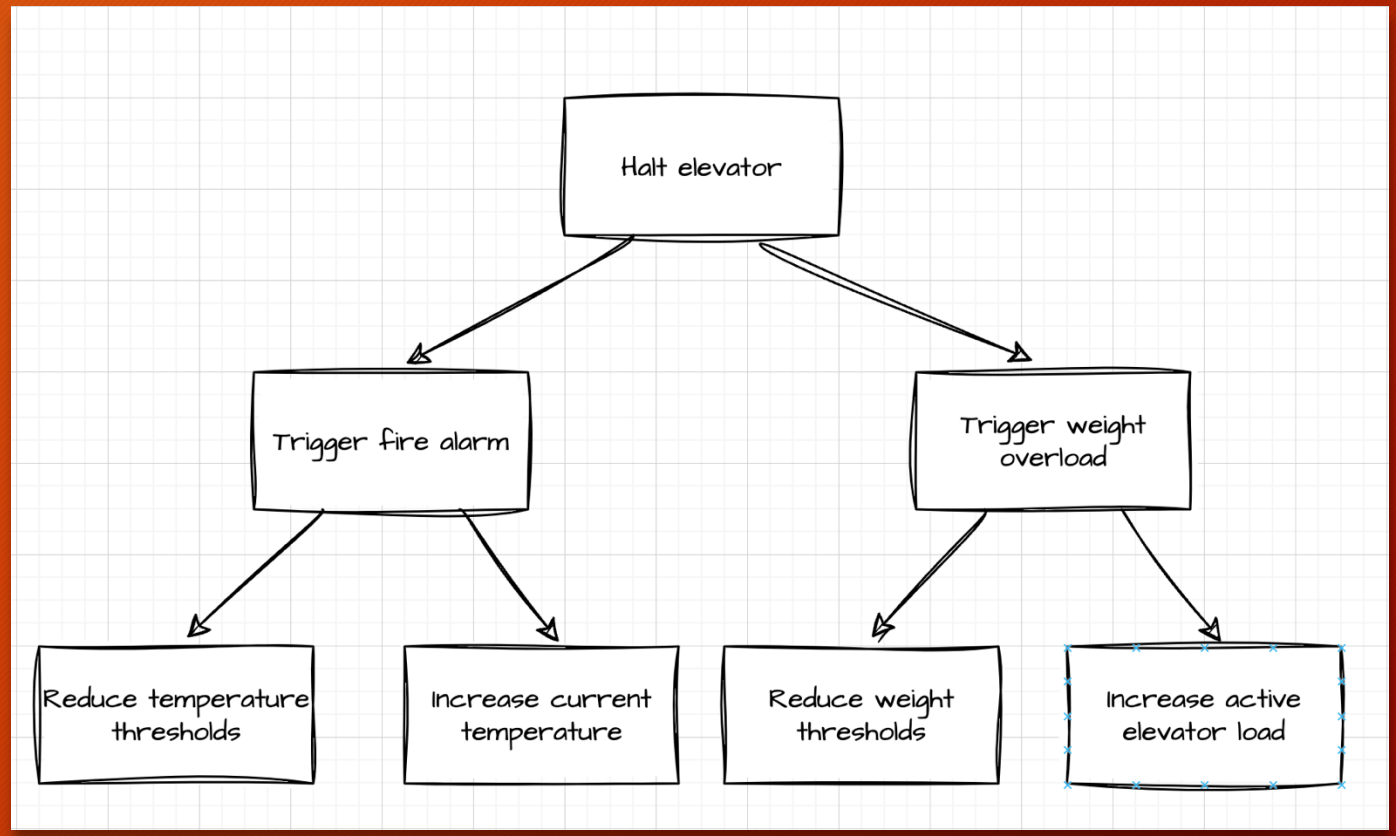
- A system consists of
- Sensors (analog)
- Components (binary)

- Prepare a Threat model
- Understand attack types
  - BIAS
  - SURGE
  - RANDOM
  - BUTTON ATTACKS
  - ATTACK MAX WEIGHT
  - ATTACK MAX TEMPERATURE



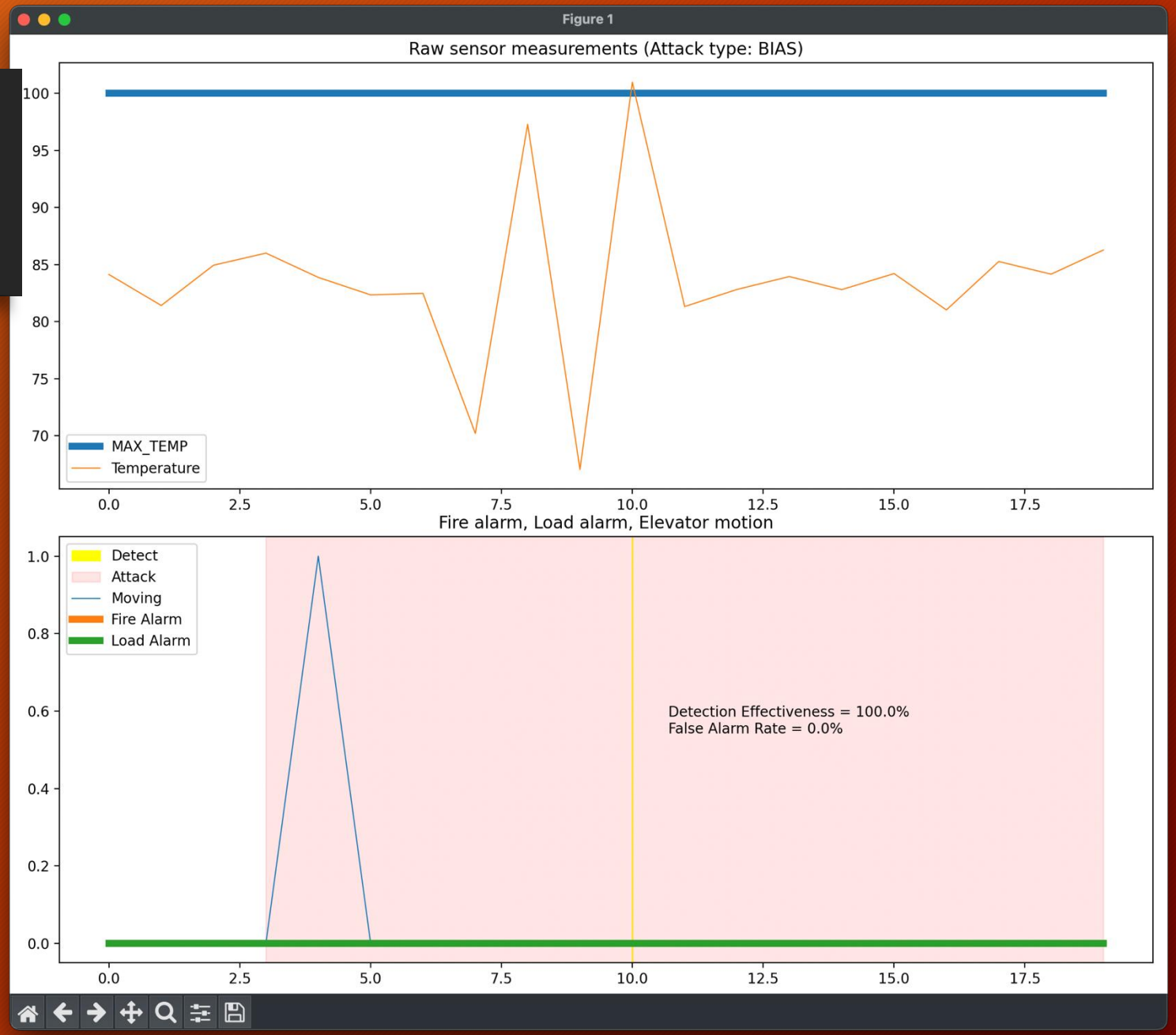
Detection

- Monitor sensors & components.
- Understand attack types
  - BIAS
  - SURGE
  - RANDOM
  - BUTTON ATTACKS
  - ATTACK MAX WEIGHT
  - ATTACK MAX TEMPERATURE
- Prepare a Threat model



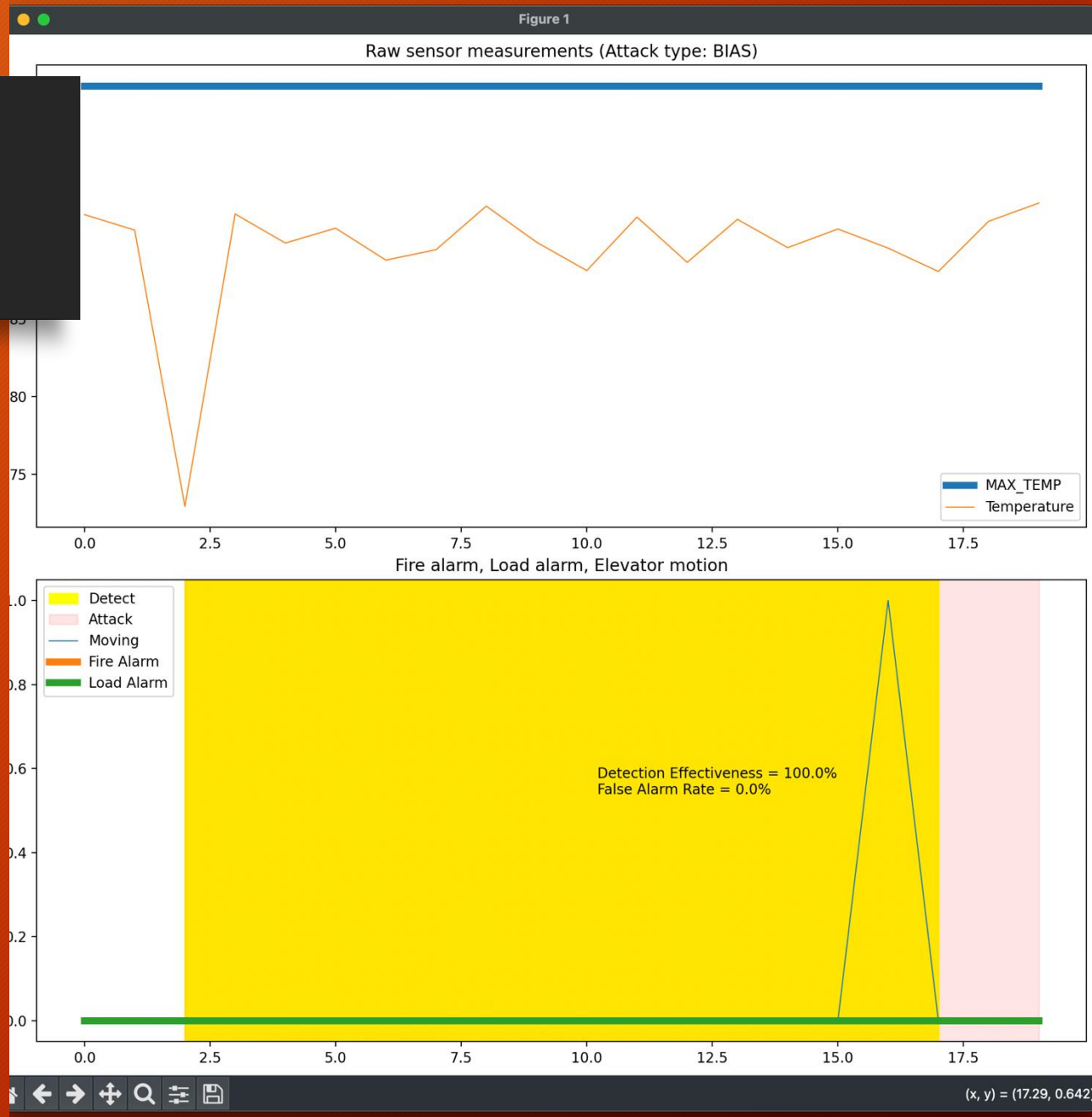
BIAS attacks

- Monitor sensors & components.
- Understand attack types
  - **BIAS**
  - SURGE
  - RANDOM
  - BUTTON ATTACKS
  - ATTACK MAX WEIGHT
  - ATTACK MAX TEMPERATURE
- Prepare a Threat model



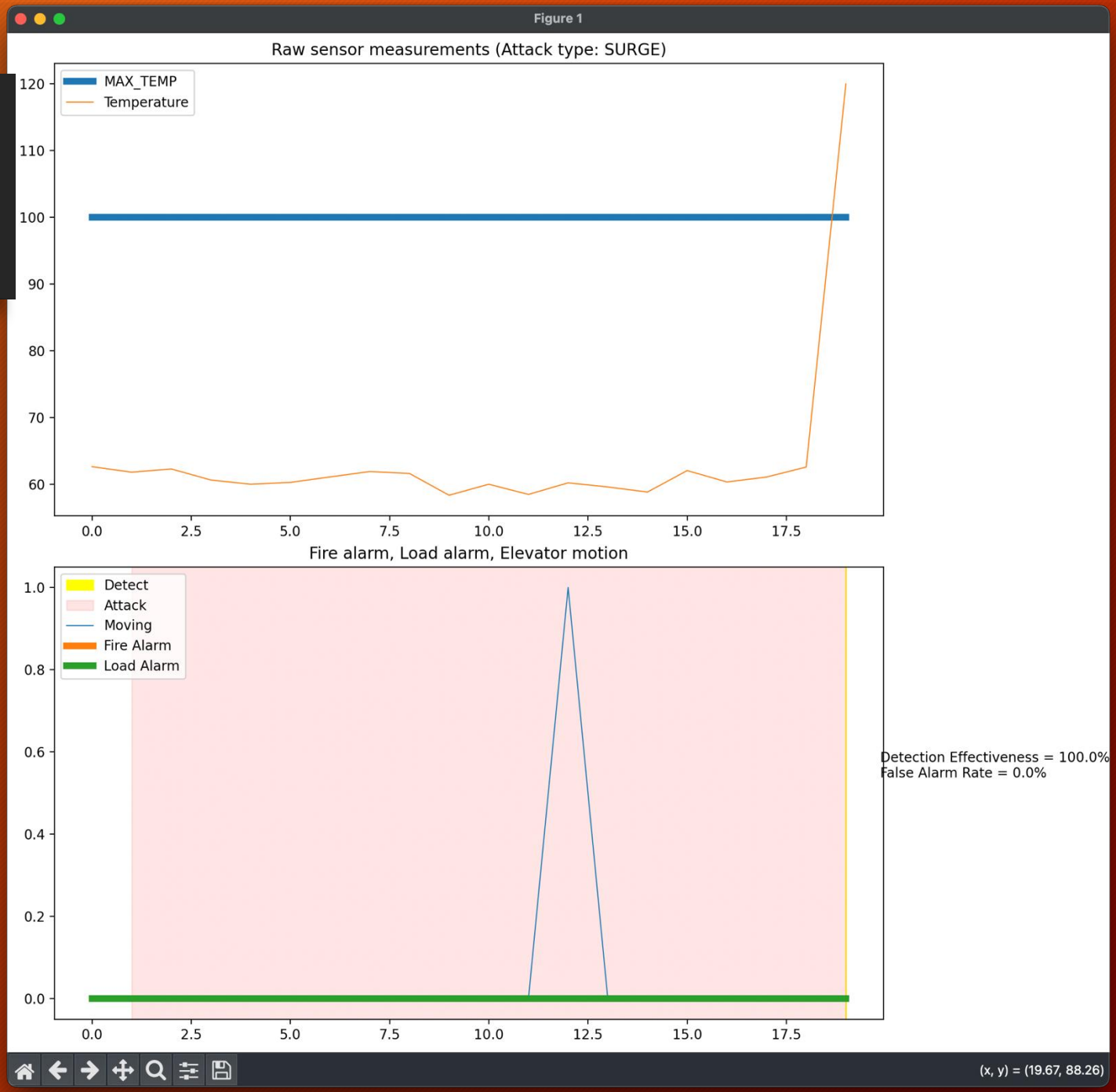
BIAS attacks

- State monitoring allows us to completely eliminate false positives.
- But it also results in false negatives.
- **Assumption**: It is safe to overlook false negatives that don't result in the system entering a restricted state.
- Can you think of any false-negative BIAS attacks that can cause harm?



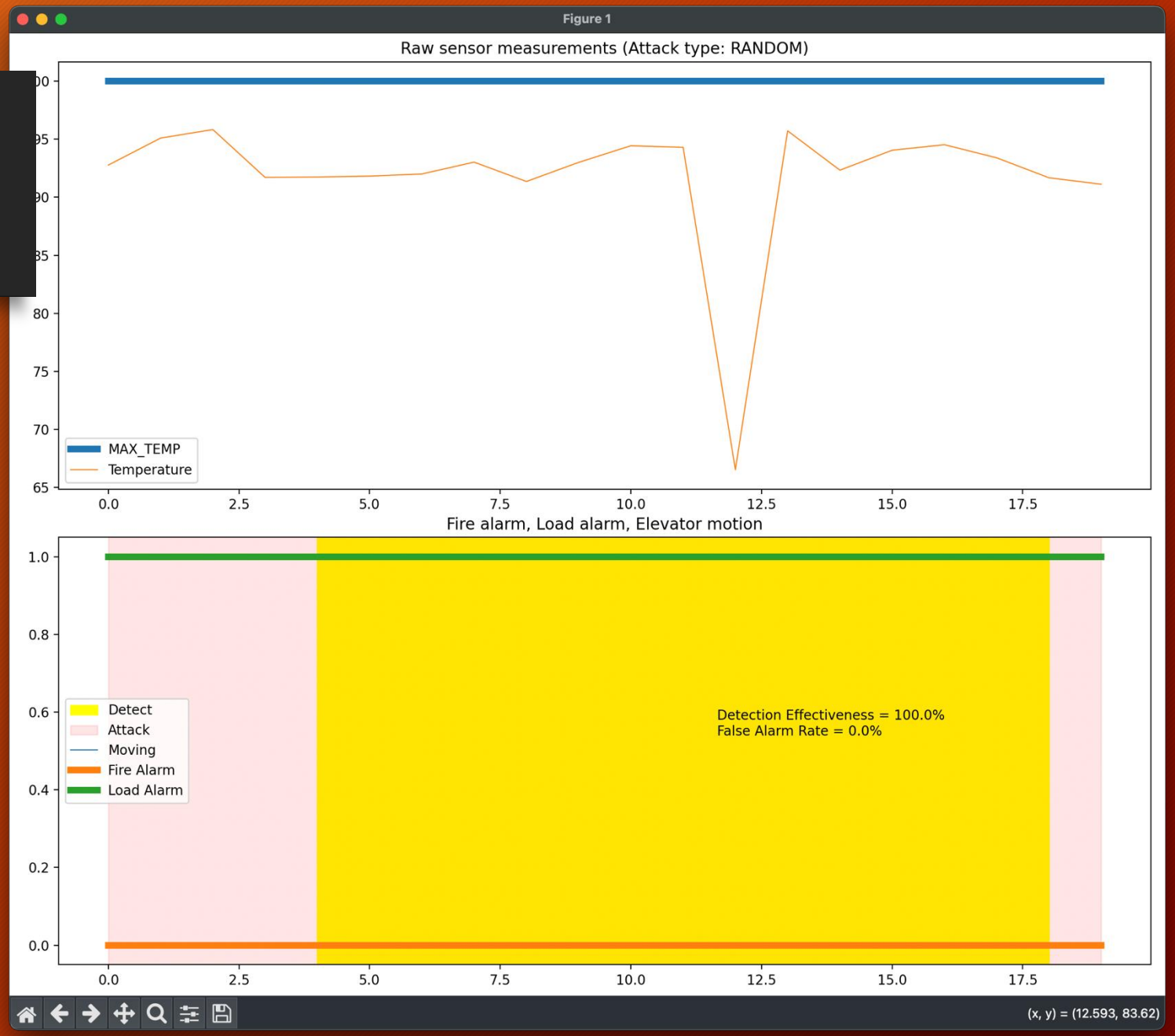
SURGE attacks

- Monitor sensors & components.
- Understand attack types
  - BIAS
  - **SURGE**
  - RANDOM
  - BUTTON ATTACKS
  - ATTACK MAX WEIGHT
  - ATTACK MAX TEMPERATURE
- Prepare a Threat model



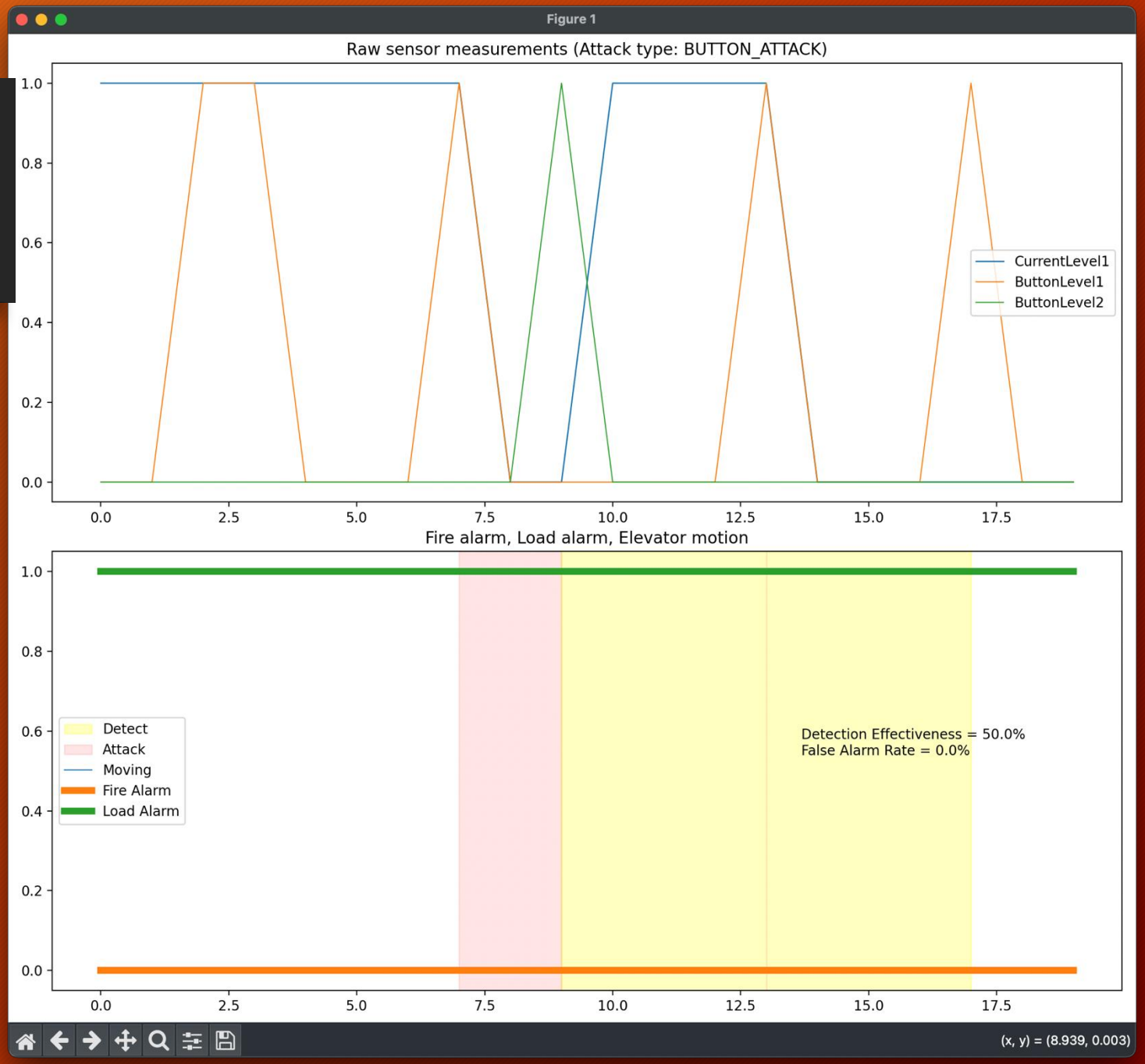
RANDOM attacks

- Monitor sensors & components.
- Understand attack types
  - BIAS
  - SURGE
  - **RANDOM**
  - BUTTON ATTACKS
  - ATTACK MAX WEIGHT
  - ATTACK MAX TEMPERATURE
- Prepare a Threat model



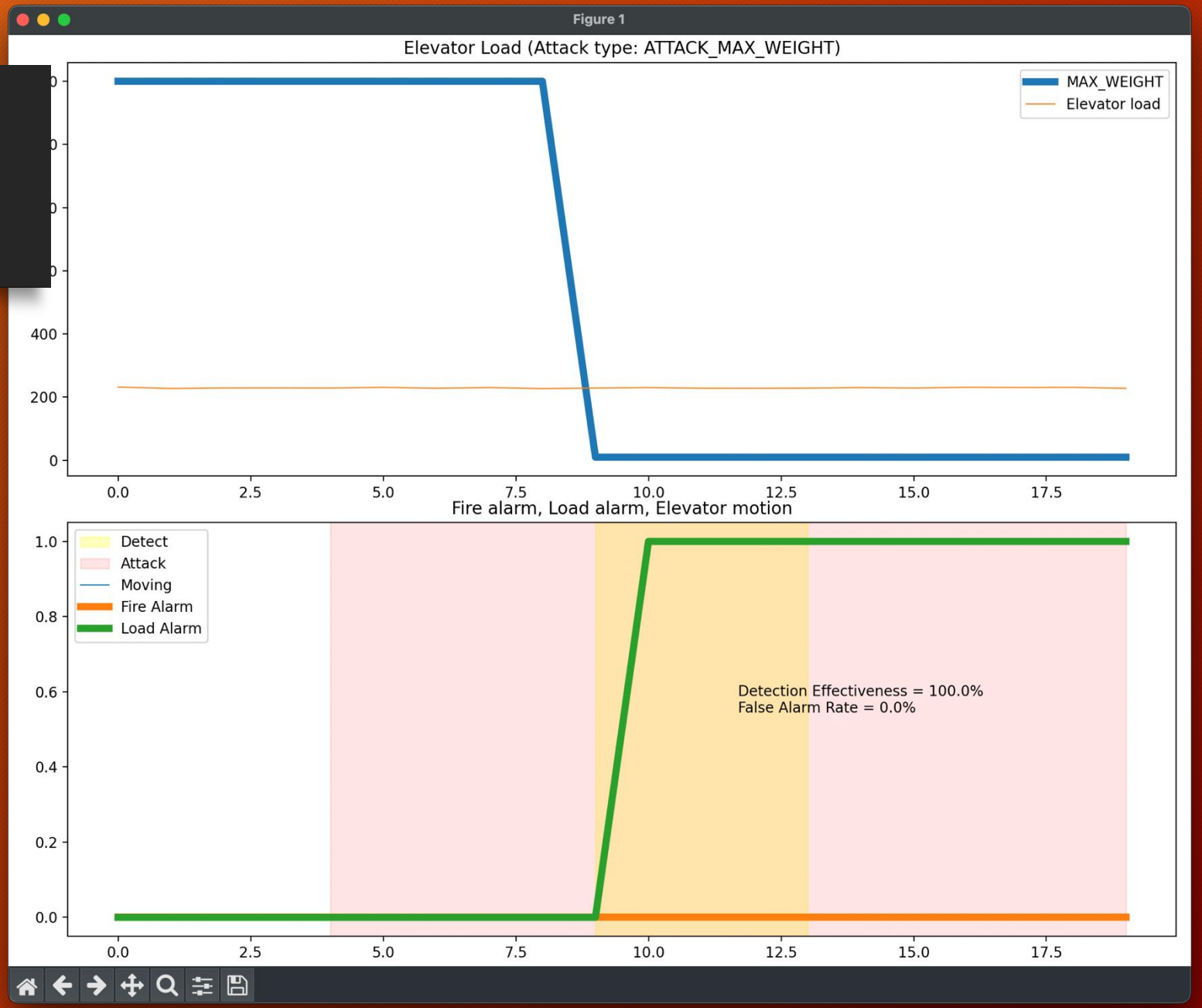
BUTTON attacks

- Monitor sensors & components.
- Understand attack types
  - BIAS
  - SURGE
  - RANDOM
  - **BUTTON ATTACKS**
  - ATTACK MAX WEIGHT
  - ATTACK MAX TEMPERATURE
- Prepare a Threat model



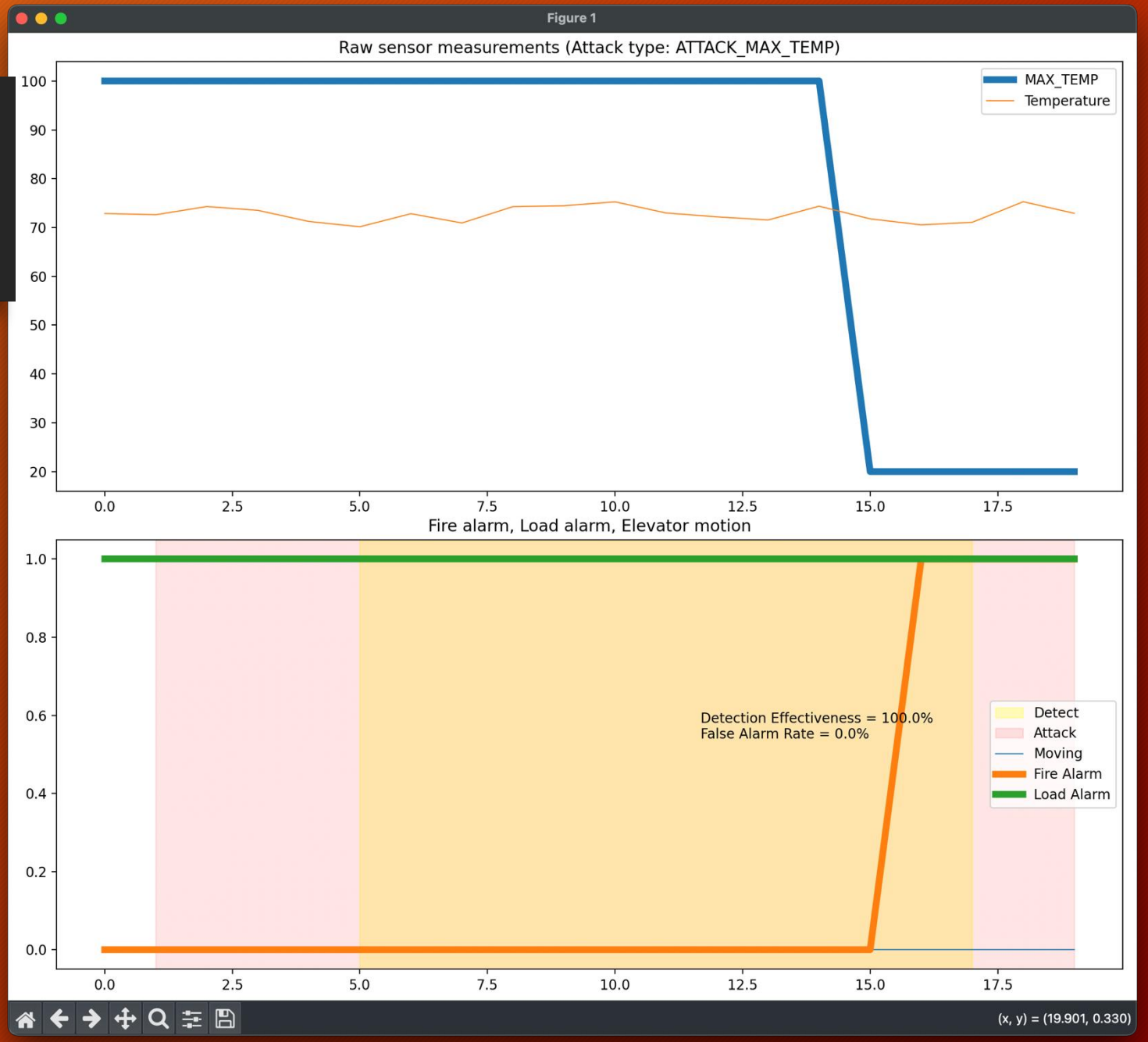
Weight threshold attacks

- Monitor sensors & components.
- Understand attack types
  - BIAS
  - SURGE
  - RANDOM
  - BUTTON ATTACKS
  - **ATTACK MAX WEIGHT**
  - ATTACK MAX TEMPERATURE
- Prepare a Threat model



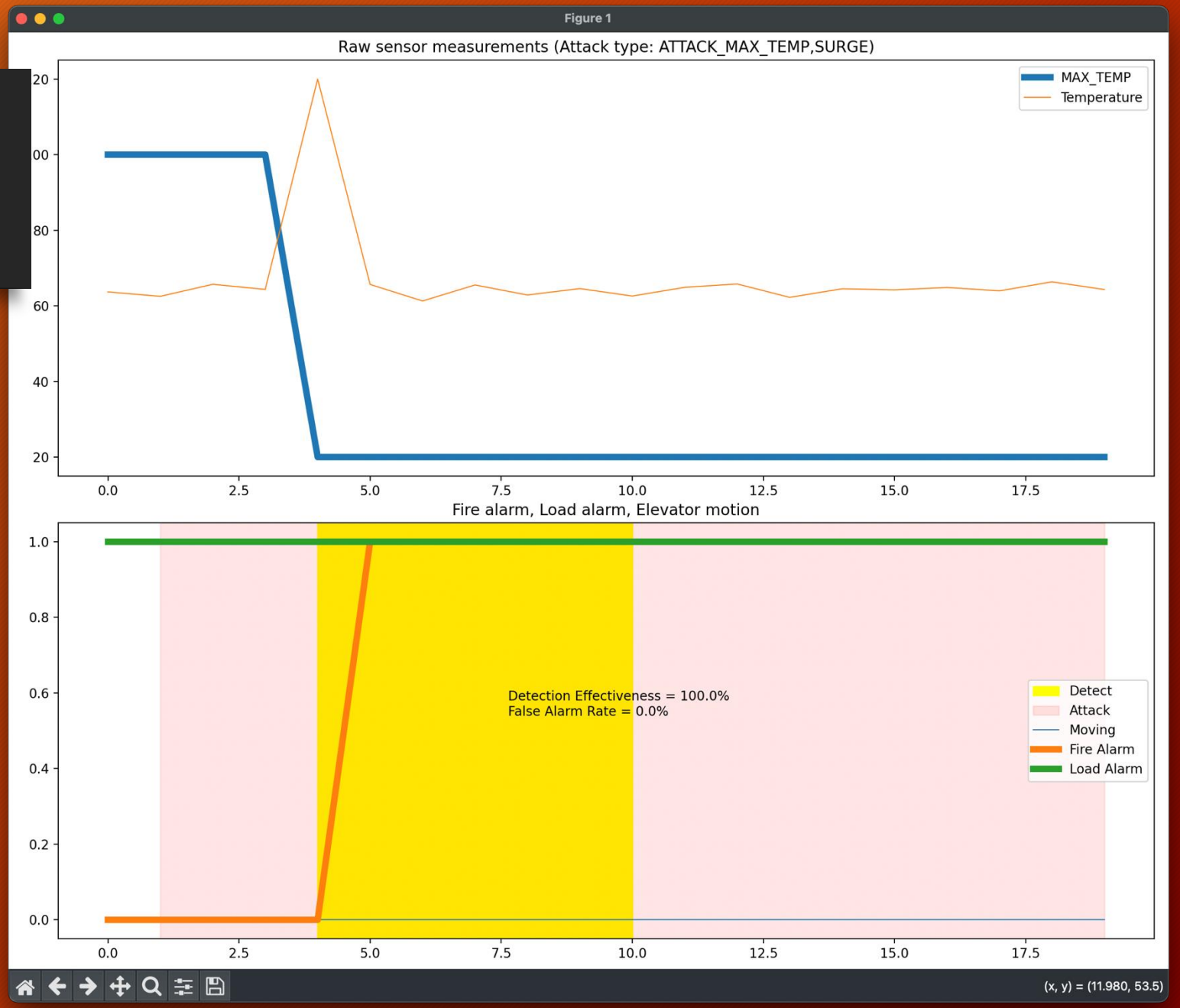
Temperature threshold attacks

- Monitor sensors & components.
- Understand attack types
  - BIAS
  - SURGE
  - RANDOM
  - BUTTON ATTACKS
  - ATTACK MAX WEIGHT
  - **ATTACK MAX TEMPERATURE**
- Prepare a Threat model



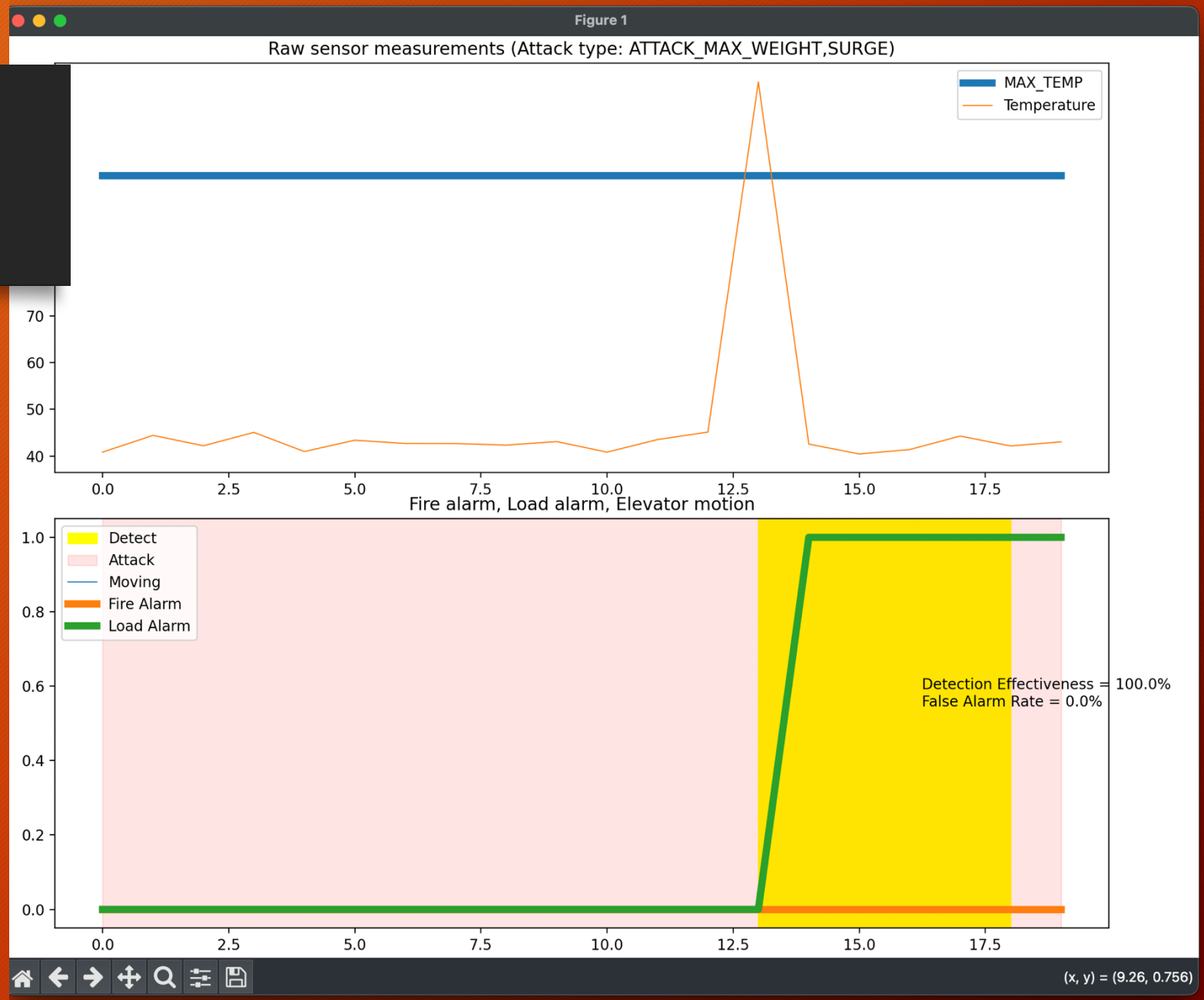
MULTI-point attacks

- Monitor sensors & components.
- Understand MULTI-point attack types. For eg,
  1. **ATTACK_MAX_TEMP + SURGE**
  2. ATTACK_MAX_WEIGHT + SURGE
  3. ATTACK_MAX_TEMP + ATTACK_MAX_WEIGHT
  4. . . .
  5. . . .



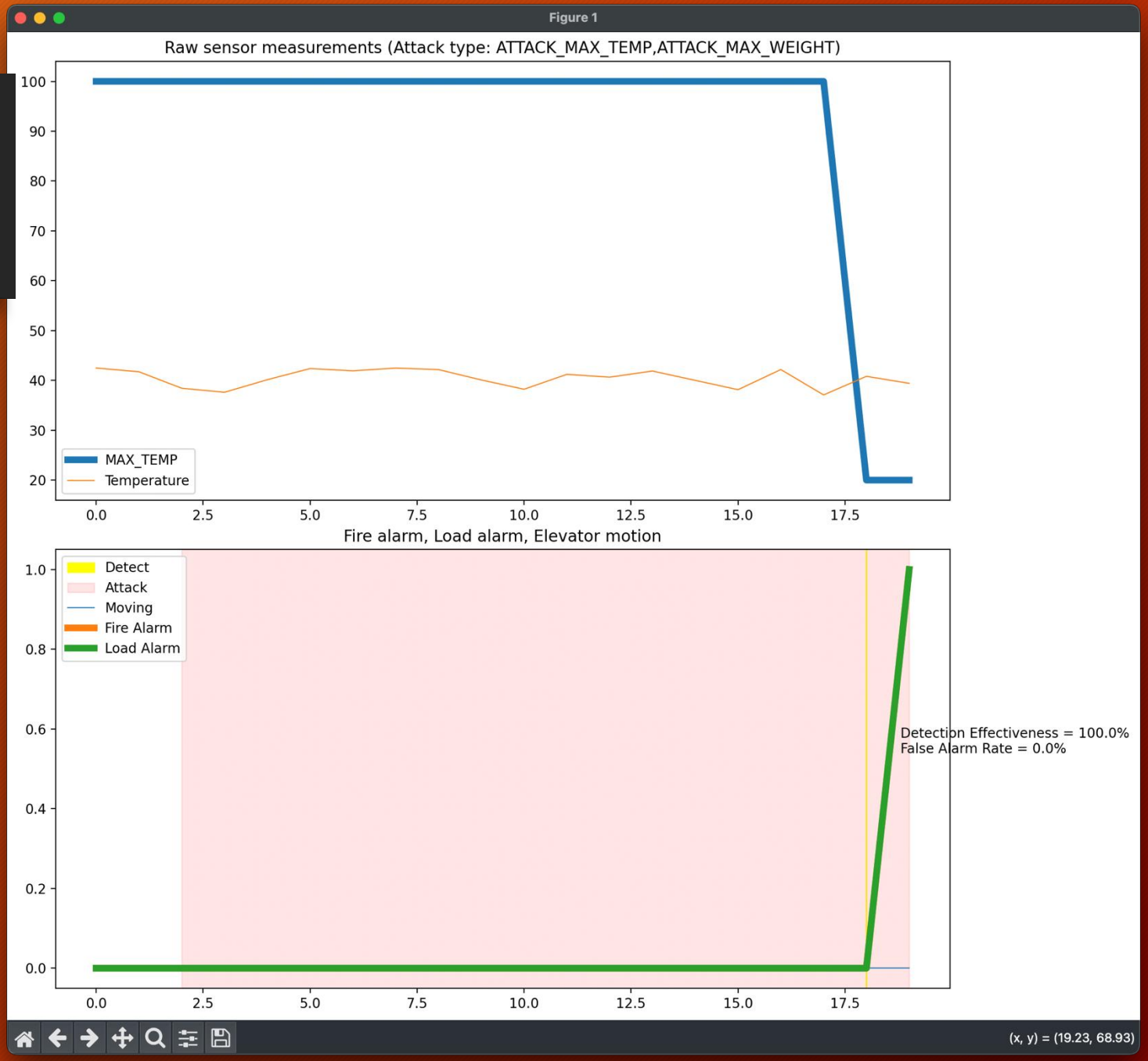
MULTI-point attacks

- Monitor sensors & components.
- Understand MULTI-point attack types. For eg,
  1. ATTACK_MAX_TEMP + SURGE
  2. **ATTACK_MAX_WEIGHT + SURGE**
  3. ATTACK_MAX_TEMP + ATTACK_MAX_WEIGHT
  4. . . .
  5. . . .



MULTI-point attacks

- Monitor sensors & components.
- Understand MULTI-point attack types. For eg,
  1. ATTACK_MAX_TEMP + SURGE
  2. ATTACK_MAX_WEIGHT + SURGE
  3. **ATTACK_MAX_TEMP + ATTACK_MAX_WEIGHT**
  4. . . .
  5. . . .



Thank you!