מחלקים לשלם - ראיה מערכתית בפיתוח מערכות IoT

Dr. Hanan Kohen

TECHNION
Israel Institute of Technology

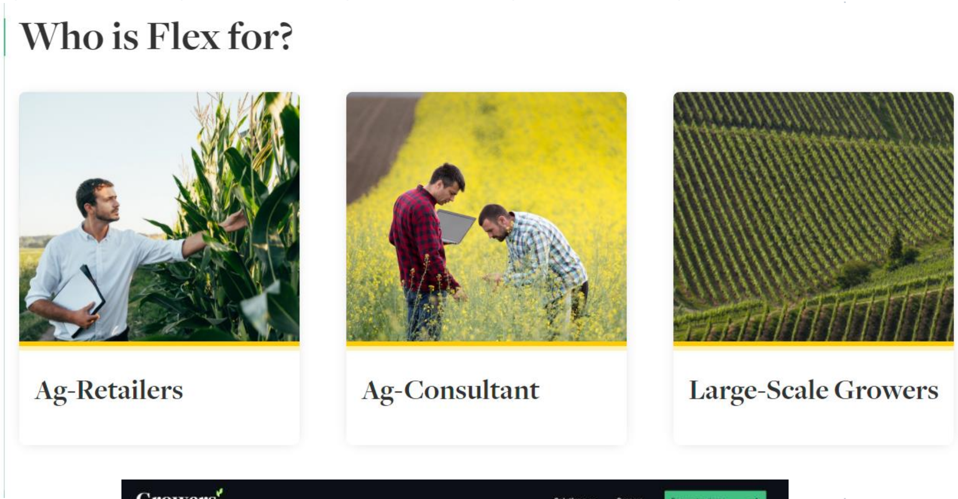
March 2022

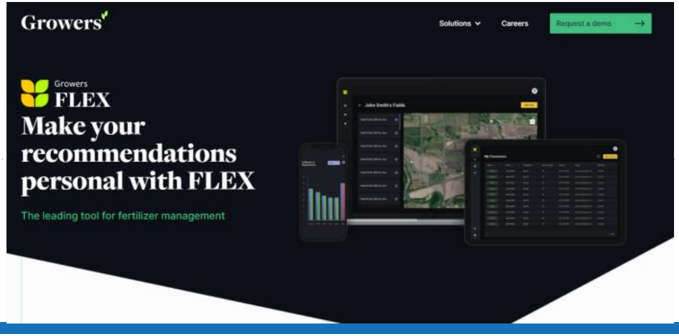
Internet of Things

Internet of Things (IoT)

- Internet of Things (IoT) refers to the interconnection of everyday things, often accompanied by intelligence.
- A platform that interacts electronically, sharing specific information and data with the world around it.
- IoT applications are already being leveraged in diverse domains, such as
  - medical services, smart retail,
  - customer service, smart homes,
  - environmental monitoring, industrial internet.

IoT Example - Growers





- https://www.growerstech.com/
- FLEX is a cross platform that helps Ag-professionals easily and accurately create fertilizer plans that improve field ROI and reduce waste based on comprehensive fertility algorithms and field-proven verified data.

IoT “Parts”

- **Hardware**
  - Sensors
  - Microcontrollers
  - Network components
- **Software**
  - Microcontroller programing
  - Sensors programing
  - Data analytics (including Big data)
- **Network**
  - Internet
  - Device to device
  - Cloud
  - Connection protocols

- **Cross aspects: Security, costs, time, connections…**

So, what we will see today?

- Understand the complexity of IoT development
- See some of the different IoT development aspects
- Understand the need for system thinking
- See what we can focus on for students – give examples from real life

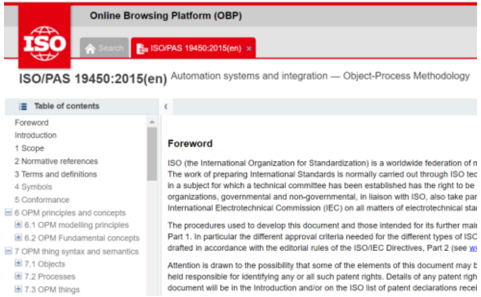
In this Presentation

- OPM – a methodology for system engineering
- OPM model for IoT development
- Sensors
- Sensors data
- Security
- IoT system example

Object-Process Methodology (OPM)

OPM – Object Process Methodology

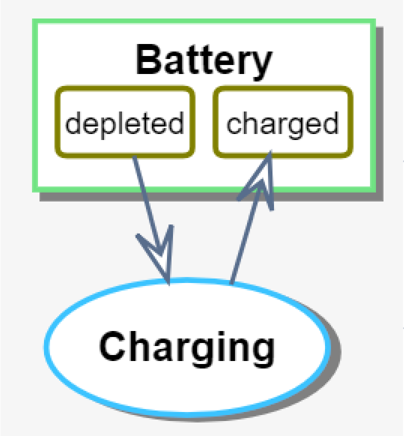
- A visual and textual language for modeling systems and phenomena of all kinds:
  - Natural
  - Human–made
  - Any combination of the above
- Recognized as ISO 19450
- Developed By Prof. Dori



Only two OPM Things:
Objects and Processes

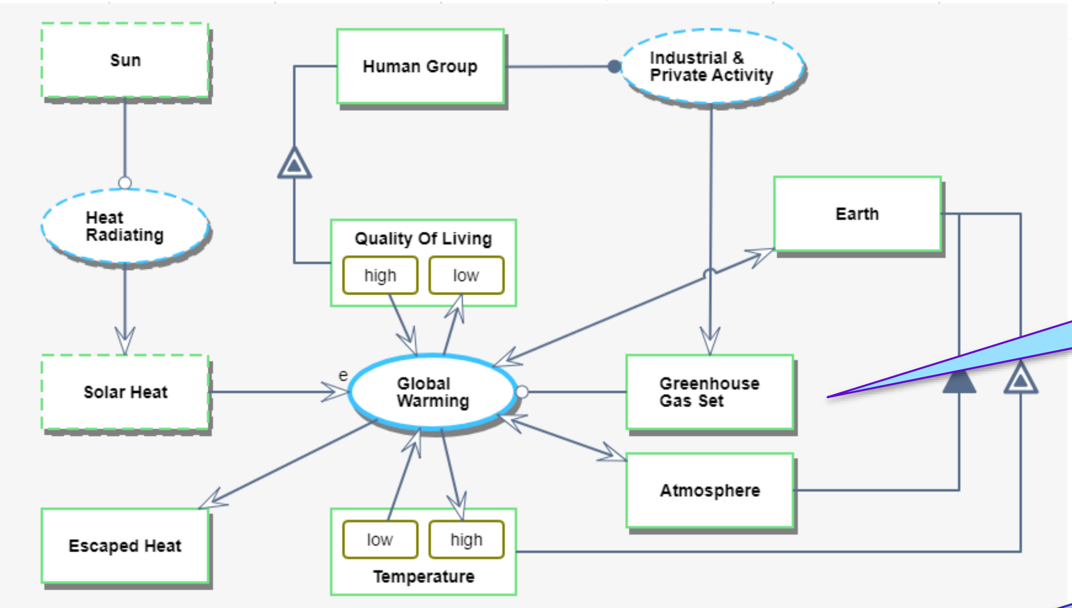
Object: A thing that exists or might exist physically or informatically.

Process: A thing that transforms or might transform one or more objects.



Charging changes Battery from depleted to charged.

OPM = OPD + OPL



OPL

Global Warming is physical and systemic.

Global Warming changes Quality Of Living of Human Group from high to low.

Global Warming changes Temperature of Earth from low to high.

Global Warming requires Greenhouse Gas Set.

Global Warming affects Atmosphere and Earth.

Solar Heat initiates Global Warming, which consumes Solar Heat.

Global Warming yields Escaped Heat.

Industrial & Private Activity is physical and environmental.

Human Group handles Industrial & Private Activity.

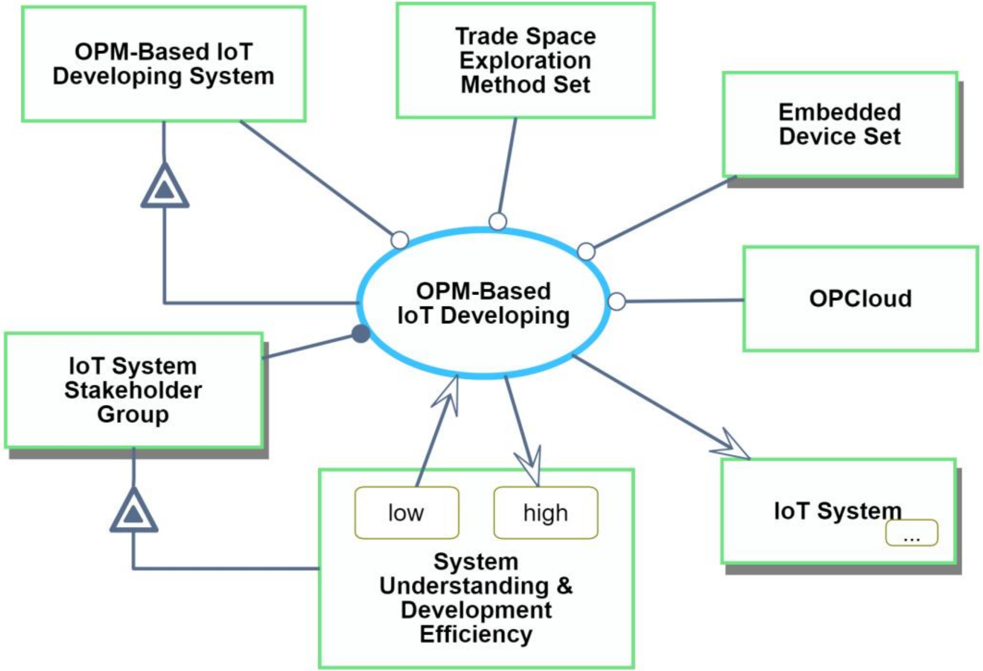
Industrial & Private Activity yields Greenhouse Gas Set.

OPD - **O**bject **P**rocess **D**iagram

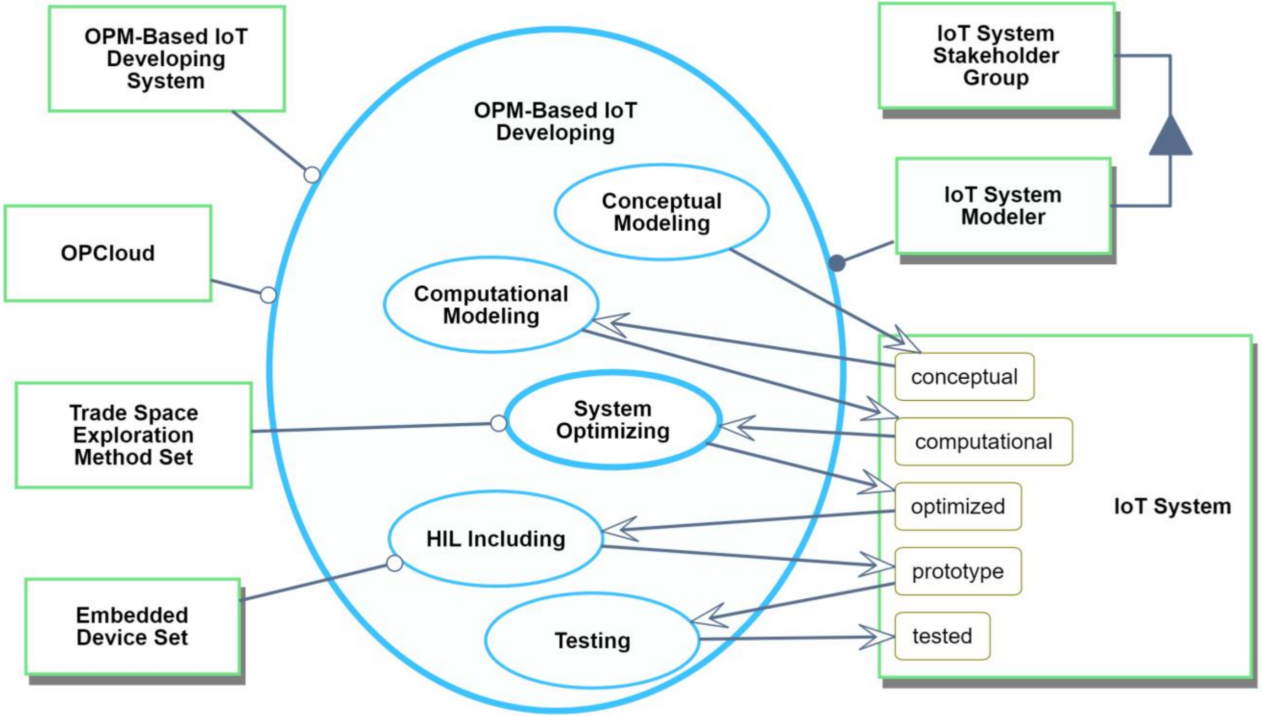
OPL - **O**bject **P**rocess **L**anguage

OPM IoT Development System

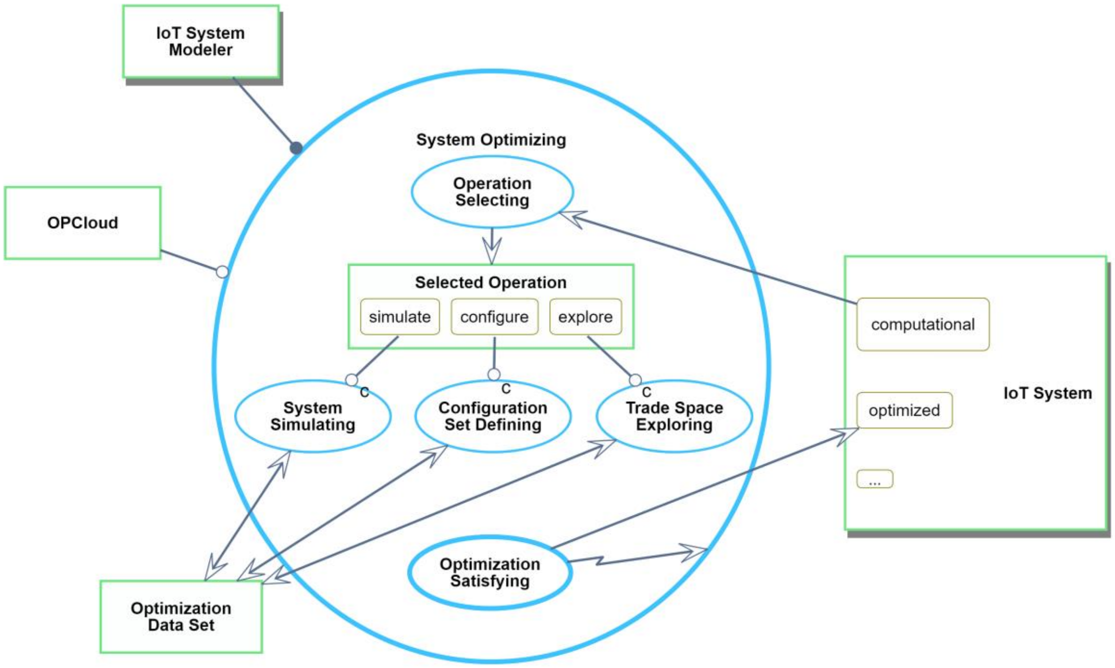
OPM IoT Development Methodology

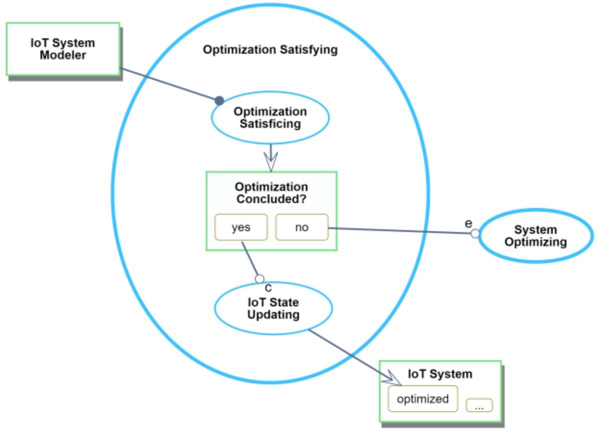


OPM IoT Development Methodology

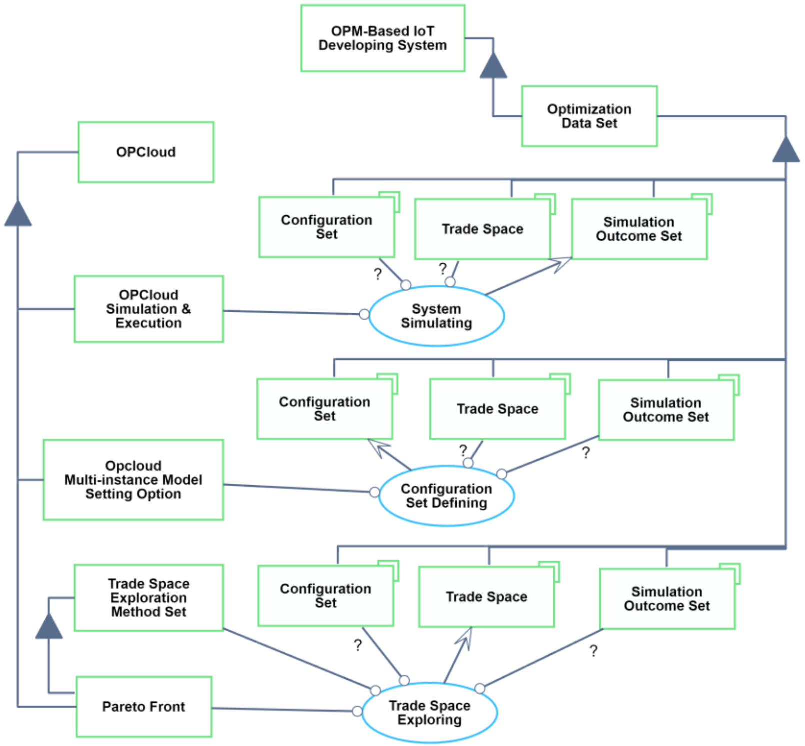


OPM IoT Development Methodology





OPM IoT Development Methodology



SD1.1.1 is a view OPD, derived from SD1.1.
OPCloud consists of **OPCloud Simulation & Execution**, **OPCloud Multi-instance Model Setting Option**, and **Pareto Front**.
Trade Space Exploration Method Set consists of **Pareto Front**.
Optimization Data Set consists of **Configuration Set**, **Simulation Outcome Set**, and **Trade Space**.
OPM-Based IoT Developing System consists of **Optimization Data Set**.
System Simulating requires an optional **Configuration Set**, **OPCloud Simulation & Execution**, and an optional **Trade Space**.
System Simulating yields **Simulation Outcome Set**.
Configuration Set Defining requires **OPCloud Multi-instance Model Setting Option**, an optional **Simulation Outcome Set**, and an optional **Trade Space**.
Configuration Set Defining yields **Configuration Set**.
Trade Space Exploring requires an optional **Configuration Set**, **Pareto Front**, an optional **Simulation Outcome Set**, and **Trade Space Exploration Method Set**.
Trade Space Exploring yields **Trade Space**.

Sensors

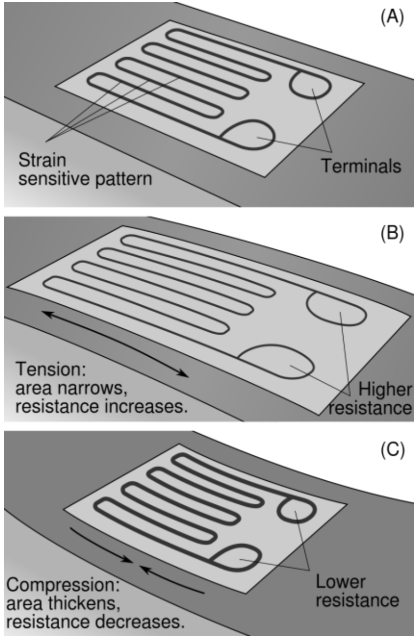
Sensors

- What do we want do measure?
- What exactly the sensor measure?
- What precision we need?
- What is the sensor limitations?
- How is the sensor data received?
- How much does it costs us?

Transducer (מתמר)

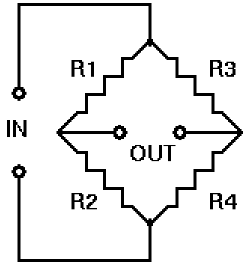
- A device that converts variations in a physical quantity, such as pressure or brightness, into an electrical signal, or vice versa.

Strain Gauge - מד עיבור

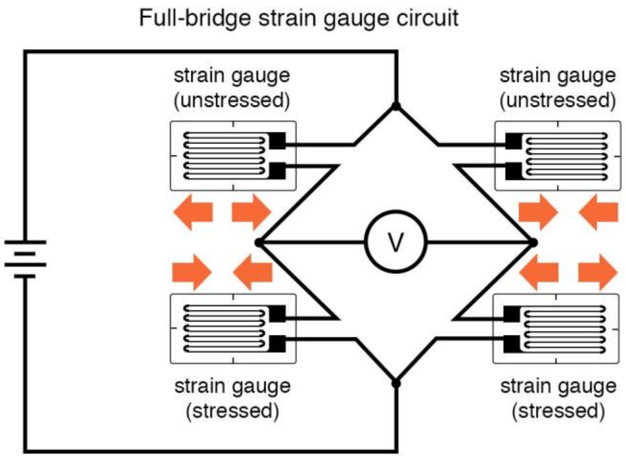


Measuring strain gauges

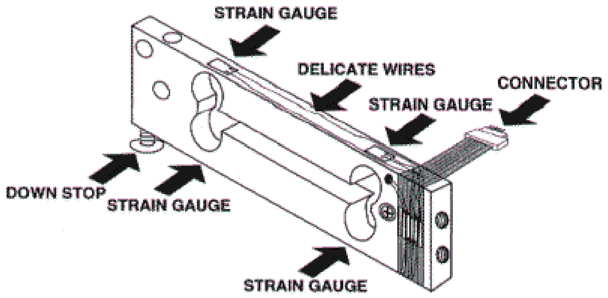
- The resistive changes are very small (~0.1%)

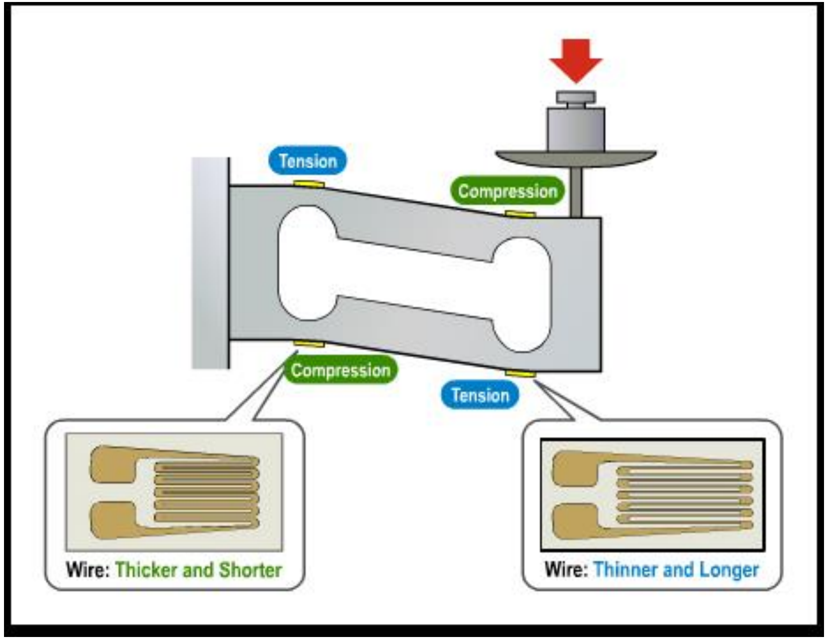


$$Vout = [(R3/(R3 + R4) - R2/(R1 + R2))] * Vin$$

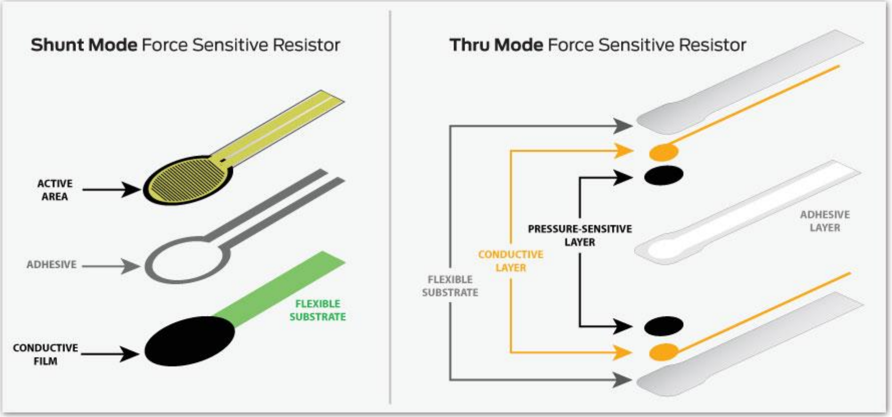


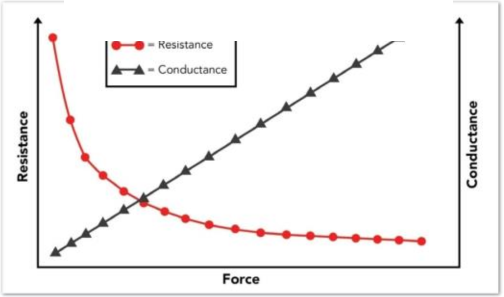
Load Cells


STRAIN GAUGE
DELICATE WIRES
CONNECTOR
STRAIN GAUGE
DOWN STOP
STRAIN GAUGE
STRAIN GAUGE


Tension
Compression
Compression
Tension
Wire: Thicker and Shorter
Wire: Thinner and Longer

Force sensitive resistor (FSR)

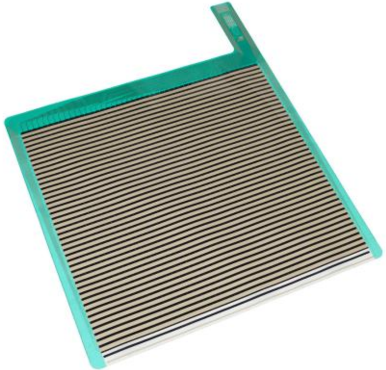


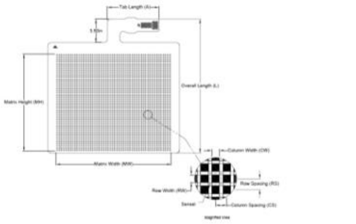


Capacitive Force Sensing

- Similar concept to FSR.
- Measure capacitive properties
- More accurate
- More expensive

Pressure sensing maps



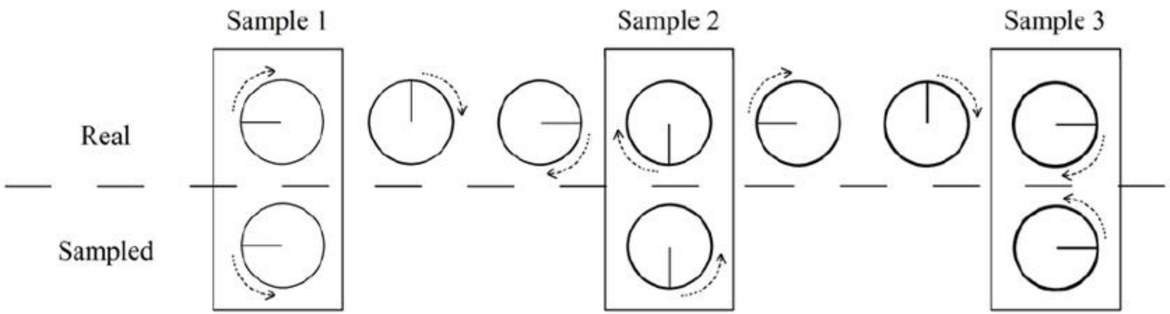


PPS (https://pressureprofile.com/)

https://www.tekscan.com/

Sensors Data

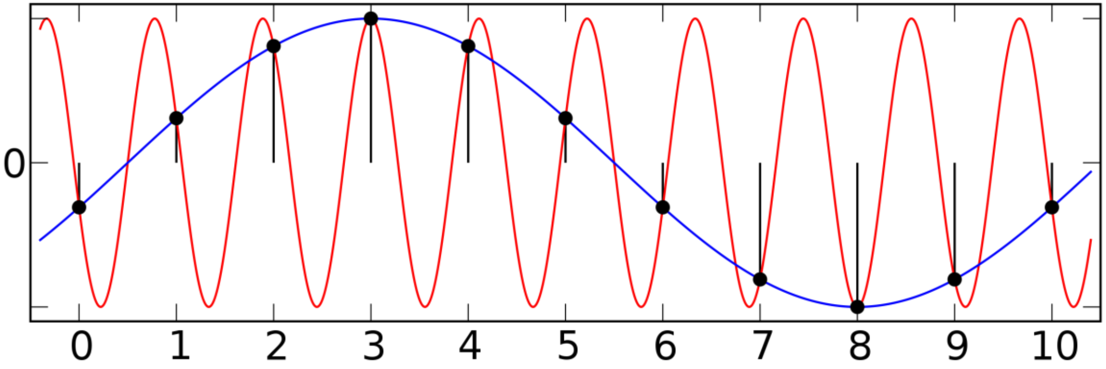
The Wagon Wheel Effect



משפט הדגימה של נייקוויסט-שאנון
Nyquist–Shannon sampling theorem

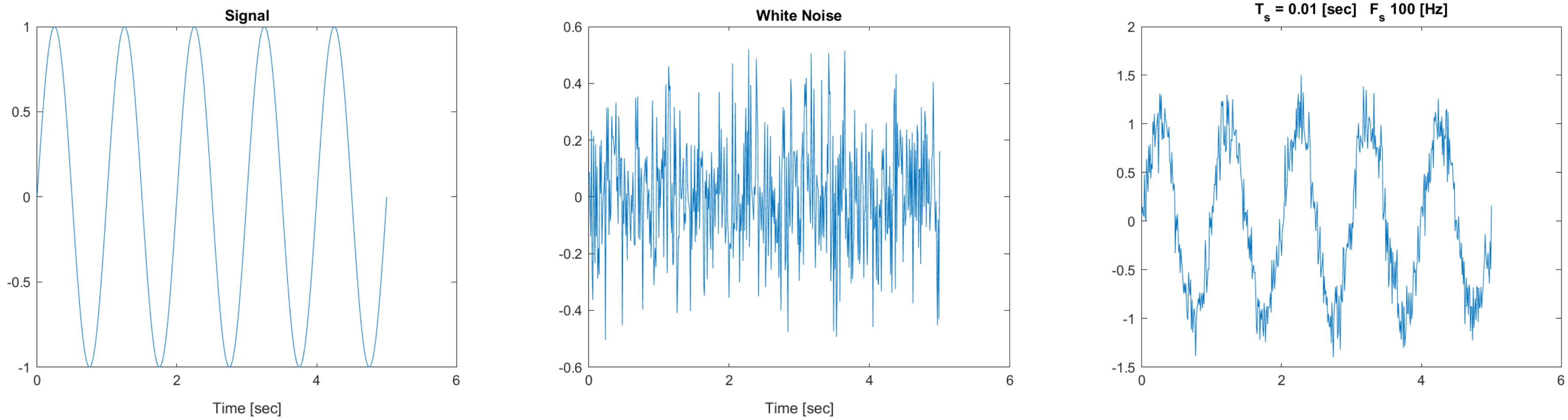
- כאשר דוגמים אות בתדר f, התדר המקסימלי שאותו ניתן לשחזר הוא f/2
- כיוון ששחזור מדויק דורש מסנן אידיאלי, אשר איננו ניתן למימוש מעשי, מקובל לדגום בקצב גבוה מהנדרש.
- לדוגמא התדר המקסימלי שבני אדם מסוגלים לשמוע בוא באזור 20,000 Hz ולכן תדר הדגימה בתקליטורים הוא 44,100 Hz.

Aliasing - התחזות



לכן נעזר לרוב במסנן תדרים – LPF לפני תהליך הדגימה

סינון רעשים



Signal
1
0.5
0
-0.5
-1
0
2
4
6
Time [sec]
White Noise
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
0
2
4
6
Time [sec]
T_s = 0.01 [sec] F_s 100 [Hz]
2
1.5
1
0.5
0
-0.5
-1
-1.5
0
2
4
6

Moving Average

לא סיבתי

$$\tilde{x}[n] = \sum_{-(M-1)/2}^{(M-1)/2} \frac{1}{M} x[n-i]$$

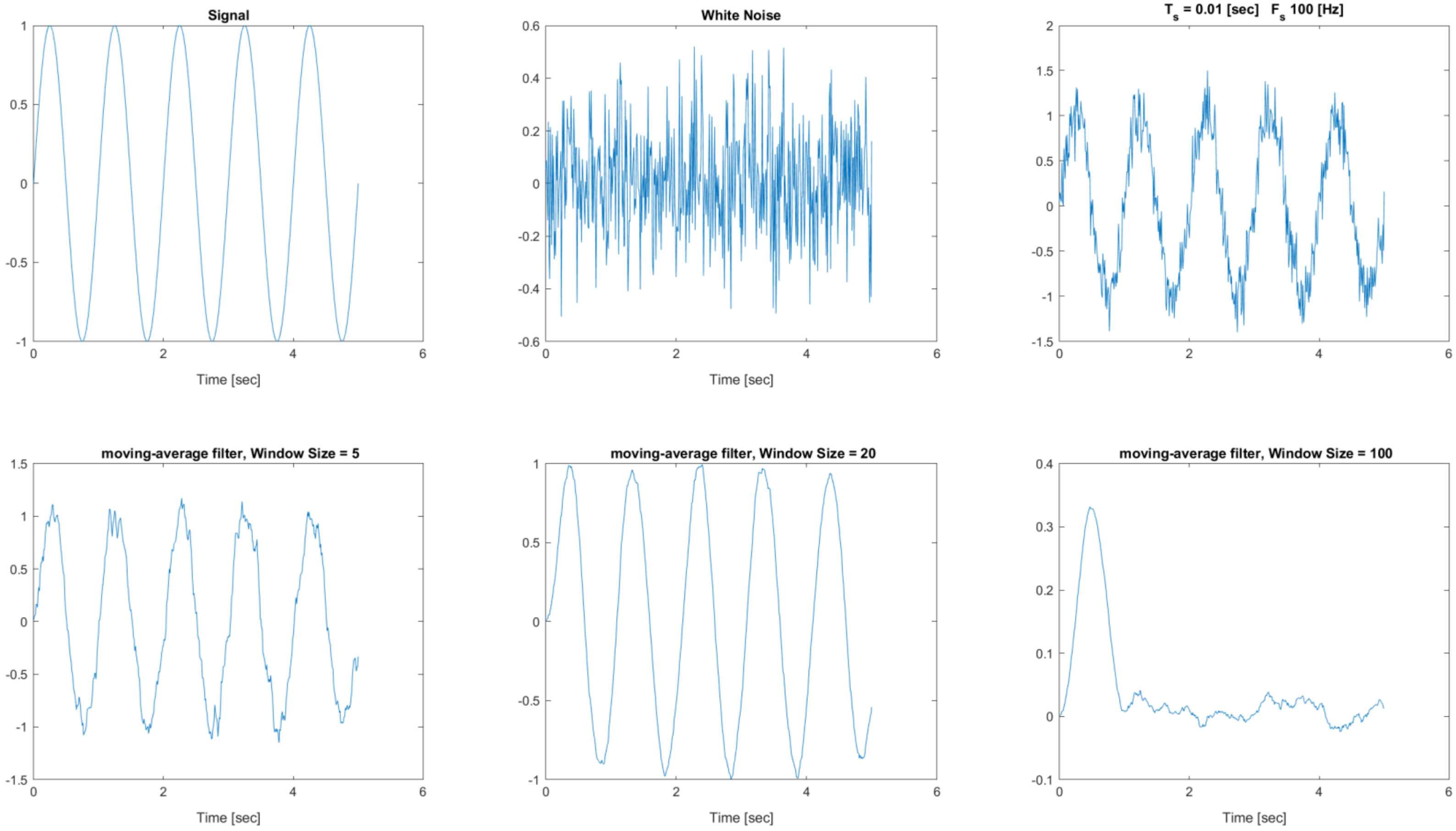
לצורך פשטות נניח m אי זוגי בנוסחה

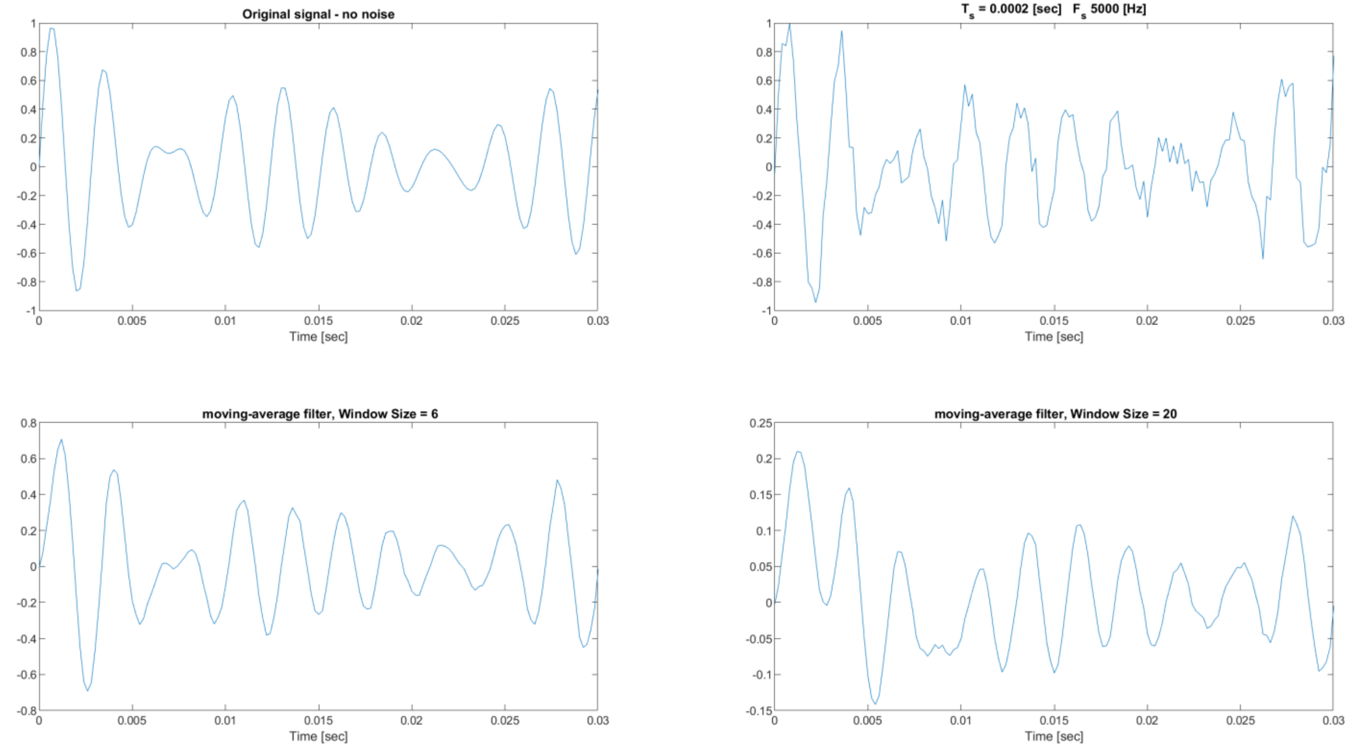
סיבתי

$$\tilde{x}[n] = \sum_{i=1}^{m} \frac{1}{M} x[n-i]$$

ממוצע משוקלל עם מקדמים b(i)

$$\tilde{x}[n] = \sum_{i=1}^{m} b(i) \cdot x[n-i]$$


Signal
White Noise
T_s = 0.01 [sec] F_s 100 [Hz]
moving-average filter, Window Size = 5
moving-average filter, Window Size = 20
moving-average filter, Window Size = 100
Time [sec]


Original signal - no noise
Time [sec]
T_s = 0.0002 [sec] F_s 5000 [Hz]
Time [sec]
moving-average filter, Window Size = 6
Time [sec]
moving-average filter, Window Size = 20
Time [sec]

FIR & IIR filters

- Finite impulse response
- $y[n] = b_0 x[n] + b_1 x[n-1] + \cdots + b_N [n-N] = \sum_{i=0}^{N} b_i \cdot x[n-i]$

- Infinite impulse response
- $y[n] = \frac{1}{a_0} \cdot (b_0 x[n] + b_1 x[n-1] + \cdots + b_N [n-N] +$
- $-a_1 y[n-1] - a_2 y[n-2] - \cdots - a_M [n-M])$
- $y[n] = \frac{1}{a_0} \left(\sum_{i=0}^{N} b_i x[n-i] - \sum_{j=0}^{M} a_j y[n-j] \right)$

FIR vs IIR

- FIR
  - Always stable
  - Better phase behavior
  - Requires more coefficients

IIR

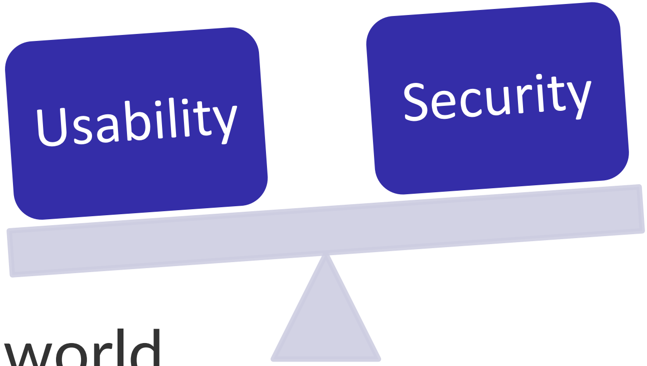
- Harder to design
- Not always stable
- Recursive
- Shorter

FIR and IIR are similar to: Auto-Regressive Moving Average (ARMA)
Different disciples with different terminology

Security

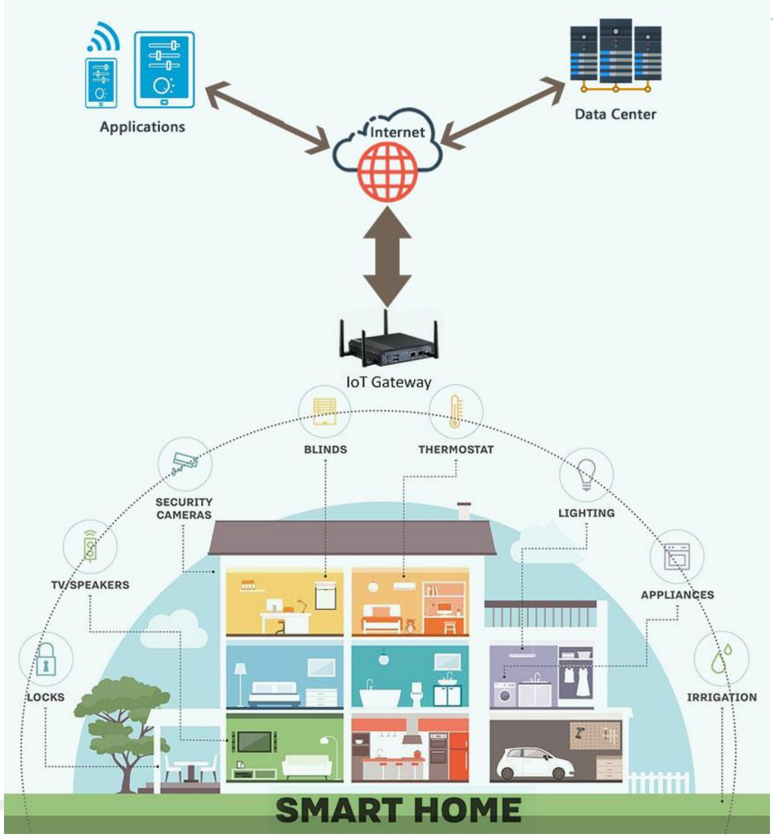
Security related characteristics of IoT

- Always connected
- Minimal UI
- Perceived as appliance
- Cheap
- Interacts with the physical world



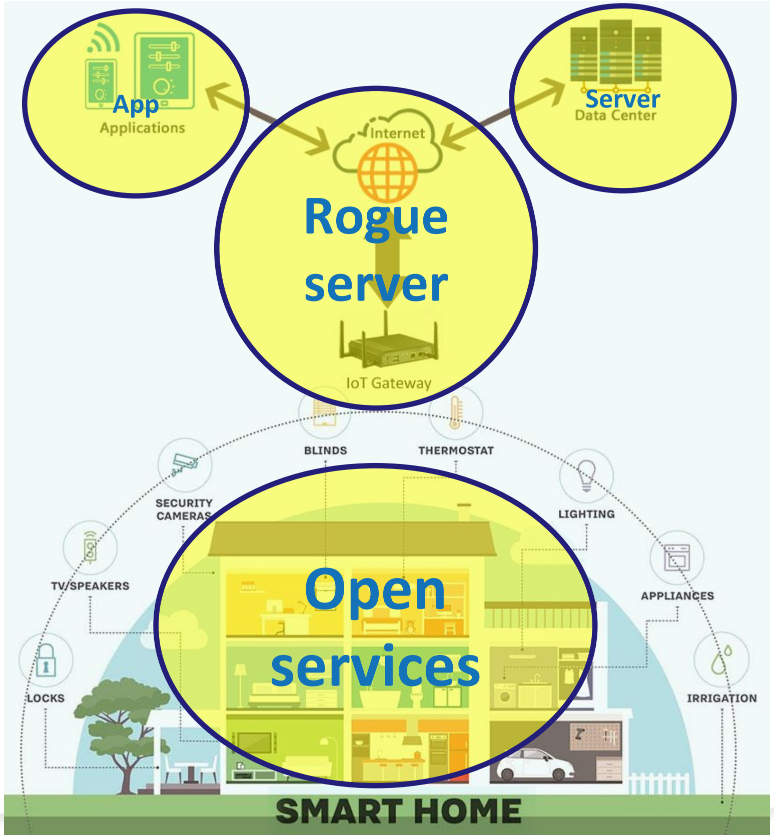
Network topology

- Client
- Server
- Peer-2-Peer / Mesh



Attack types

- Open services
- Rogue server
- Server
- Application
- Physical access



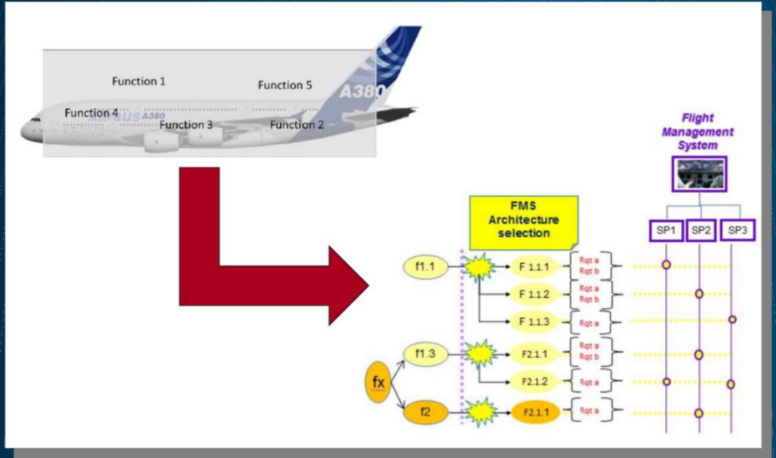
Cross System Aspects - Security

Impact analysis

Asset identification
- Functions
- Data
- Resources

Threat condition
Consequences if an asset looses
- Confidentiality
- Integrity
- Availability

Impact
- Very strong
- Strong
- Medium
- Low
- No impact



Functional breakdown
- Aircraft
- Multi-system
- System

Cross System Aspects

Security measure

Everything which reduces either the likelihood of a successful attack or the severity of an impact is a security measure

Examples of security measures

- Dedicated technical security function
- Technical function already part of the system baseline
- Technical function identified by another processes, e.g. safety
- An operational procedure suggested by the manufacturer or already performed in service
- Prerequisites of an attack
  - Availability of technical information and possibly bespoke equipment
  - Accessibility of system interfaces
  - Necessary skills

Effectiveness

- Based on a scale from 1 to 30
- Normally between 1 and 10 for real security measures
- Higher numbers mean more effective security measures
- Even the minimum effect 1 may reduce the likelihood

If there is no effect it is not a security measure

Least effective ← → Most effective

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

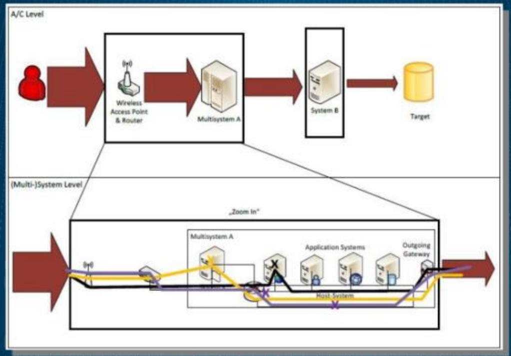
Threat paths

A threat path starts at the **threat vector** and ends at the **target**

Threat vector may be a

- Physical interface
- Logical connection
- Equipment

A threat vector is also called a **threat entry point**

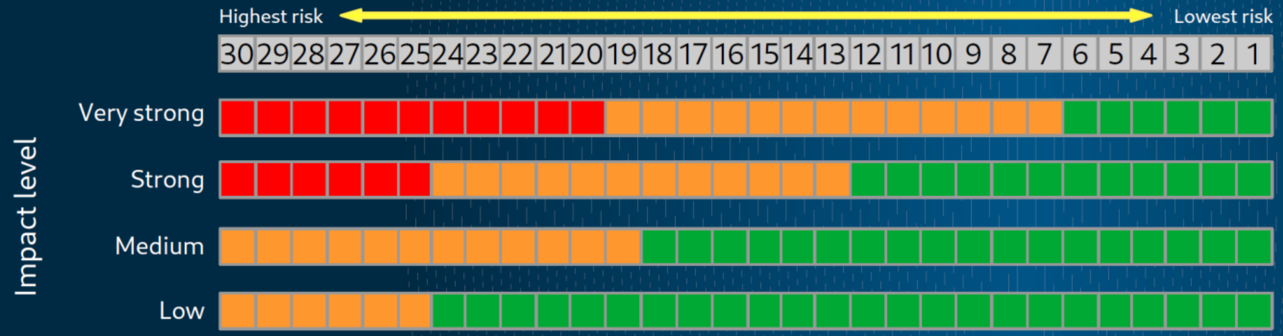


Threat path example with refinement

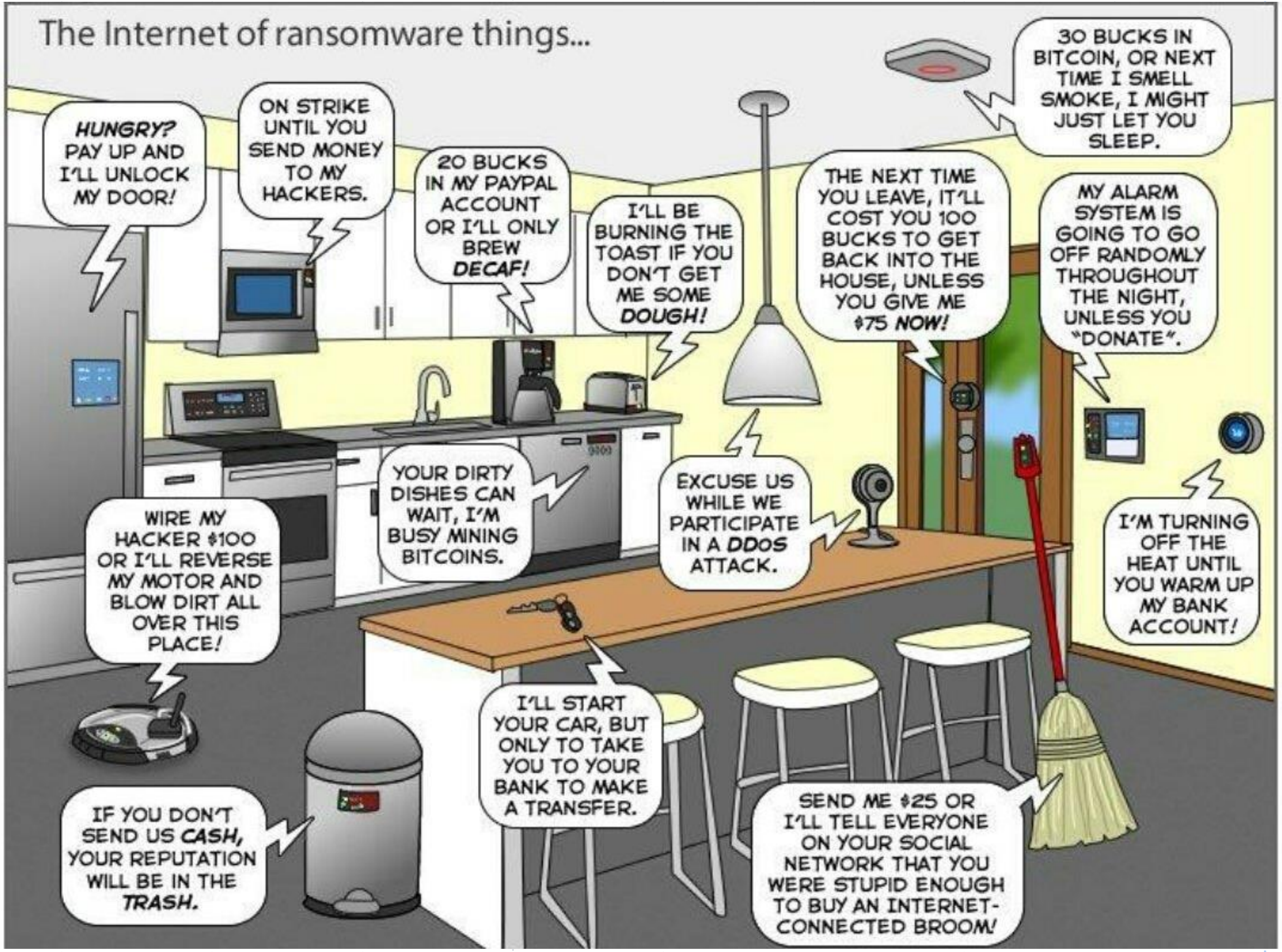
Cross System Aspects

Risk grid

Very likely	Low	Medium	Medium	High	High
Likely	Low	Low	Medium	Medium	High
Unlikely	Low	Low		Medium	Medium
Very unlikely	Low	Low	Low	Low	Medium
Extremely unlikely	Low	Low	Low	Low	Low
	No impact	Low	Medium	Strong	Very strong



The risk scale is colored according to the impact level



The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

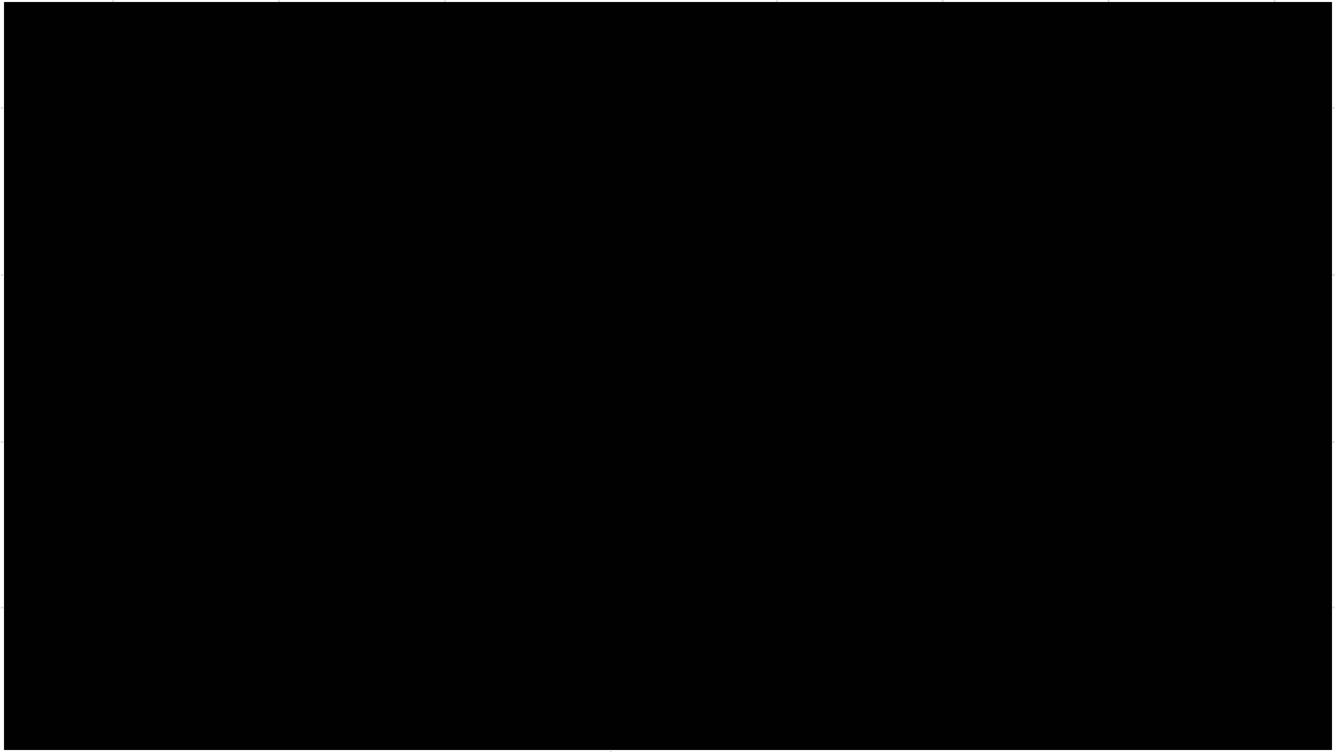
Reverse Sensing System Example

IoT System Example

An example of a system including:

- Conceptual modeling
- Quantitative modeling
- Simulation
- Connecting to real hardware (sensors, microcontroller)

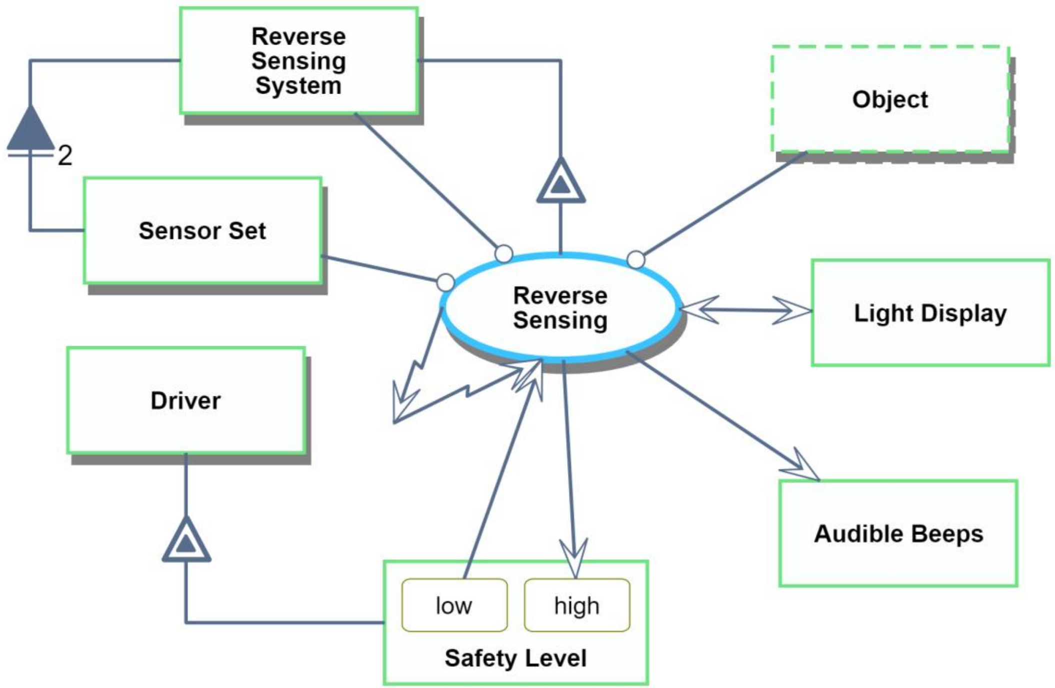
Reverse Sensing System - Ford



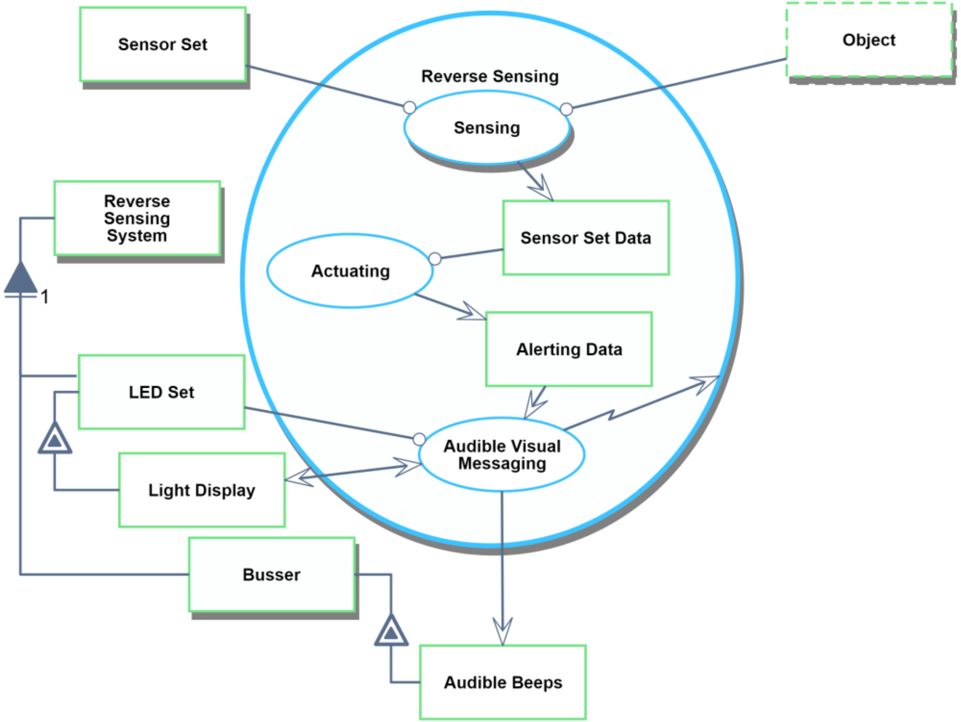
Reverse Sensing System Textual Overview

- This system incorporates four different sensors in the rear bumper.
- The reverse sensors work by emitting audible beeps when it detects that something is behind you. These beeps will increase from a slow beep to a faster beep as you get closer to the object.
- The system also reflect it as visual light display.
- If the vehicle continues to move toward the object, the system will emit one long, connected tone.
- This system is designed to help the driver become more cautious and safe while backing up.

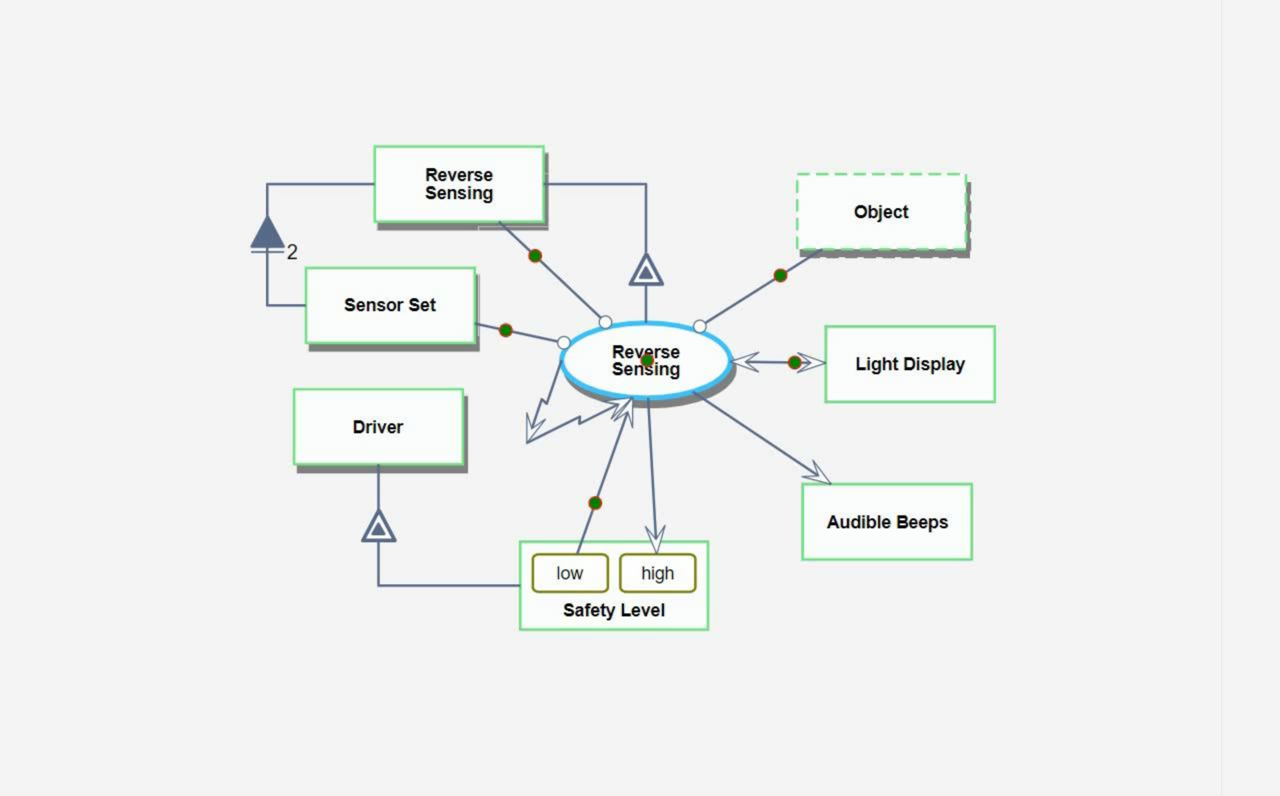
Reverse Sensing System - SD



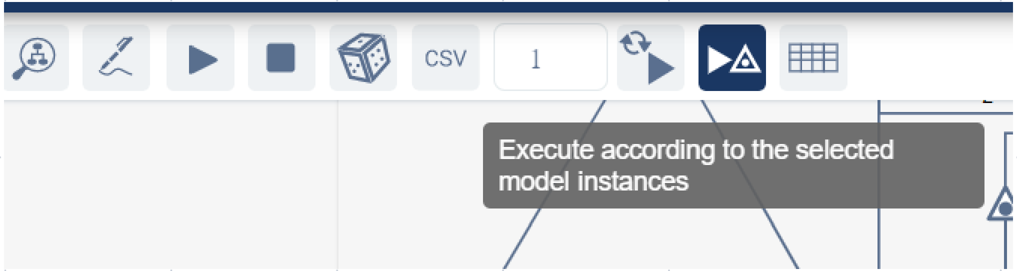
Reverse Sensing System – SD1



Simulating


Reverse Sensing
2
Sensor Set
Object
Reverse Sensing
Light Display
Driver
Audible Beeps
low
high
Safety Level

Simulating Multiple System Configurations

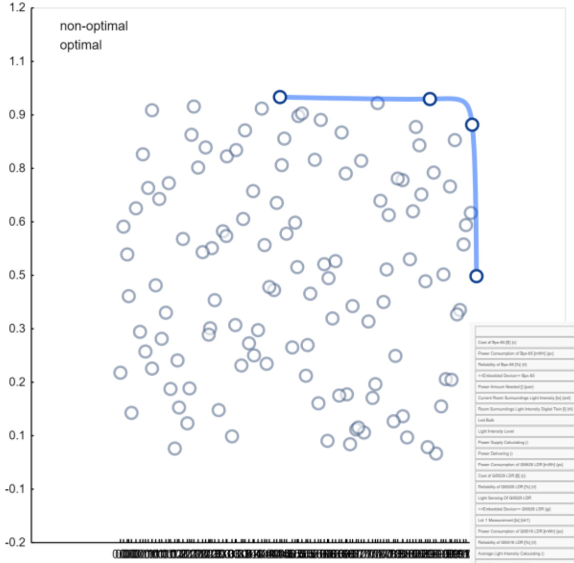


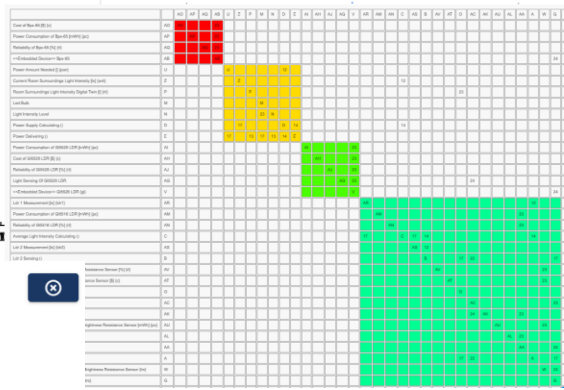
C	B	A	
System Power Consumption	System Costs	Instance Ref#	1
45	15.5	1	2
40	11.4	2	3
50	15.69	3	4
45	11.59	4	5
30	7.69	5	6
25	3.59	6	7
60	18	7	8
55	13.9	8	9
45	10.19	9	10
40	6.09	10	11
40	10	11	12
35	5.9	12	13
50	15.75	13	14
45	11.65	14	15
35	7.94	15	16
30	3.84	16	17
45	10.25	17	18
40	6.15	18	19
30	7.75	19	20
25	3.65	20	21

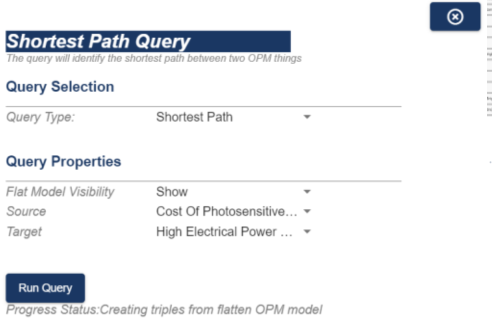
- The simulation runs in a loop according to the selected instances
- If we define 20 configurations (instance combinations) to be simulated, and we run the simulation 100 times, each configuration will be simulated 5 times.

Optimization

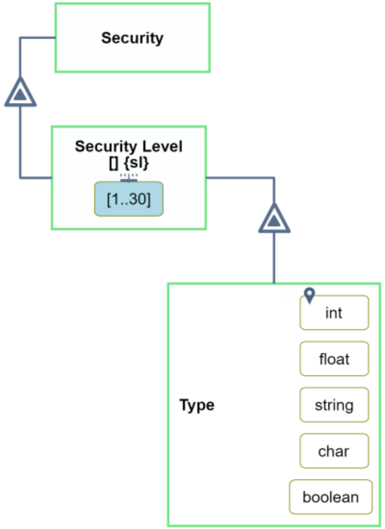
- Searching for the best system configuration on multi-objective problems
- Using Design-Structure Matrix (DSM) based methods
- Applying graph database querying using Neo4J integrated into OPCloud

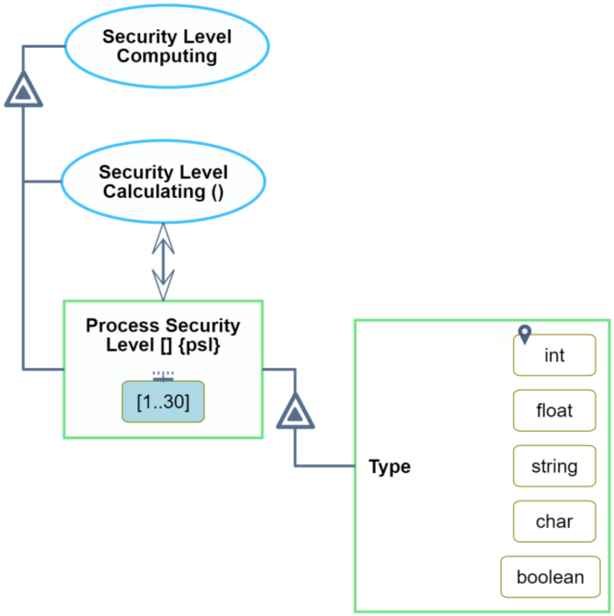




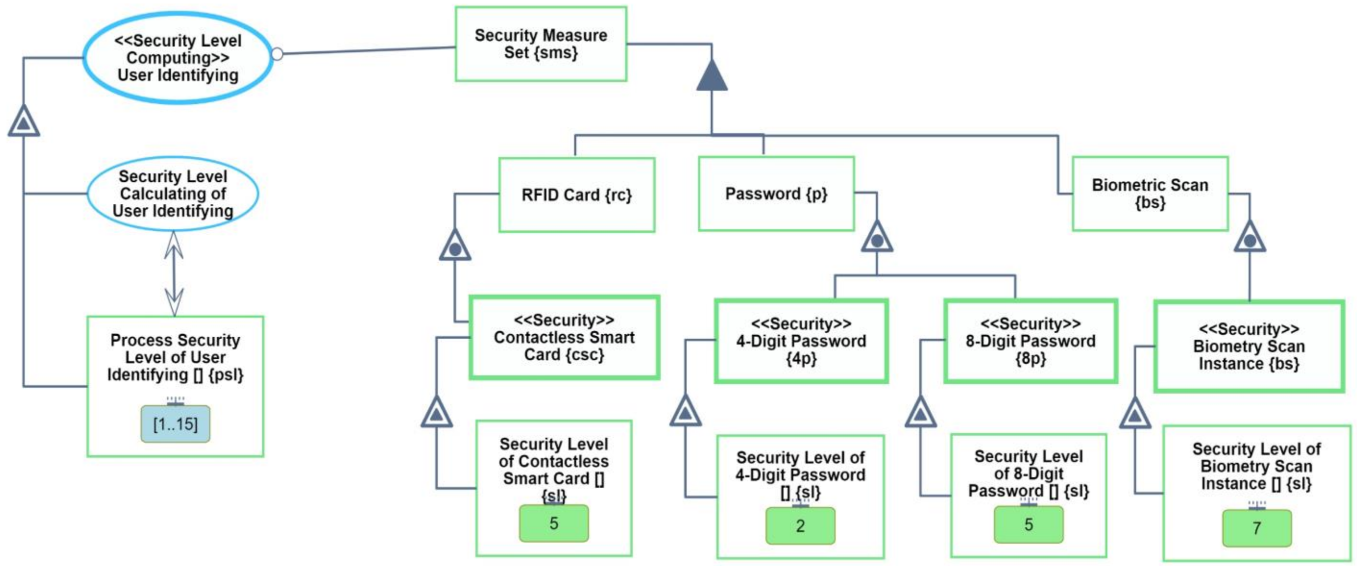


OPM Stereotypes for attributes: Security as an example (mass, price…)





OPM Stereotypes for attributes: Security as an example (mass, price...)

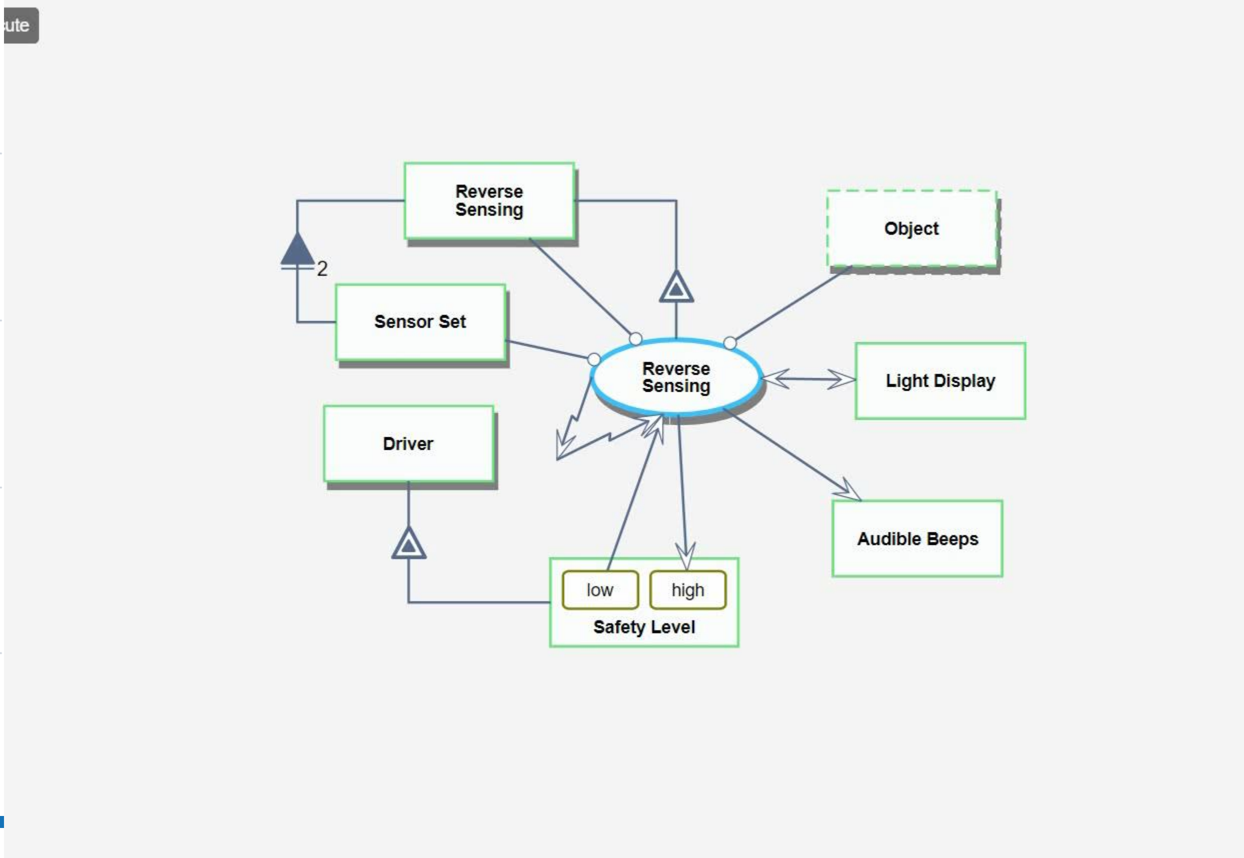


Hardware-in-the-Loop (HIL)

Hardware-in-the-Loop (HIL) simulation

- ❑ Hardware-in-the-Loop (HIL) simulation is a method for developing and testing embedded systems.
- ❑ Entails embedding parts of the real hardware during the system development.
- ❑ Allows to thoroughly test the complex control device in a virtual environment.
- ❑ Provides advantages of:
  - Earlier testing in the development process
  - Reduction of testing costs
  - Increase of test coverage
  - Better test repeatability.

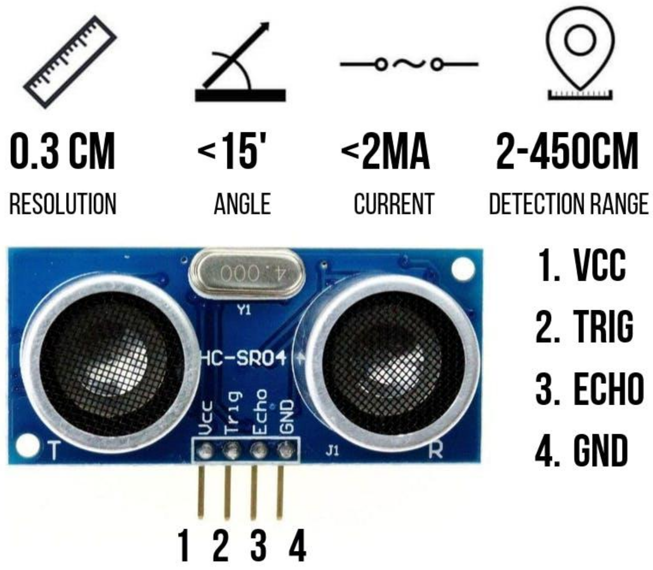
Simulating



ute
Reverse Sensing
2
Sensor Set
Object
Reverse Sensing
Light Display
Driver
Audible Beeps
low
high
Safety Level

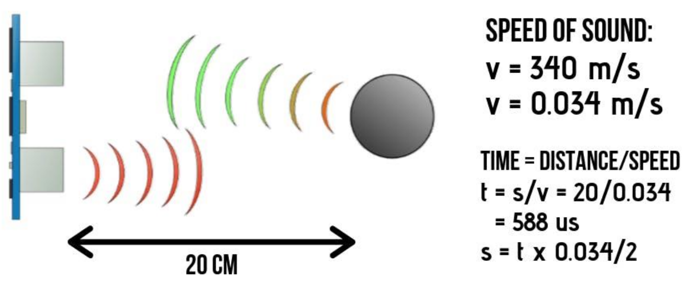
Updated model to include the calculations

- Ultrasonic Sensor HC-SR04 is a sensor that can measure distance. It emits an ultrasound at 40 000 Hz (40kHz)
- In order to generate the ultrasound we need to set the Trigger Pin on a High State for 10 µs. That will send out an 8 cycle sonic burst which will travel at the speed sound and it will be received in the Echo Pin.

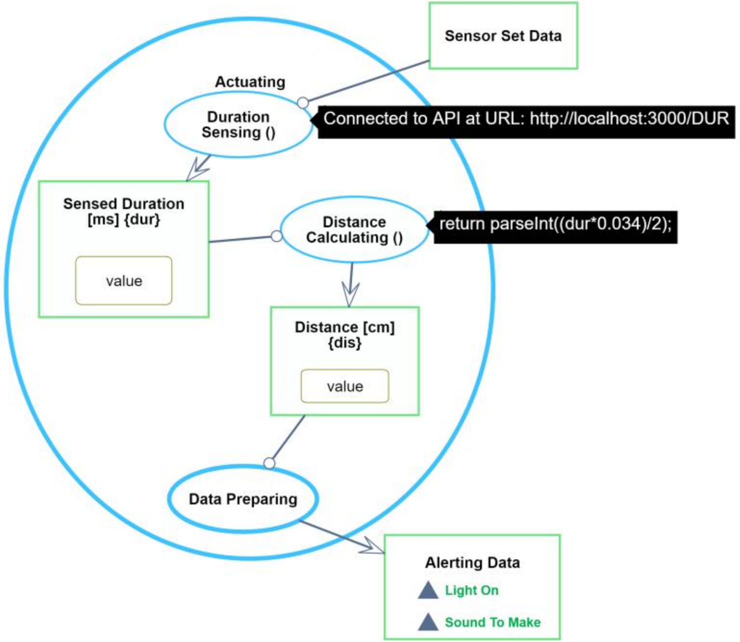


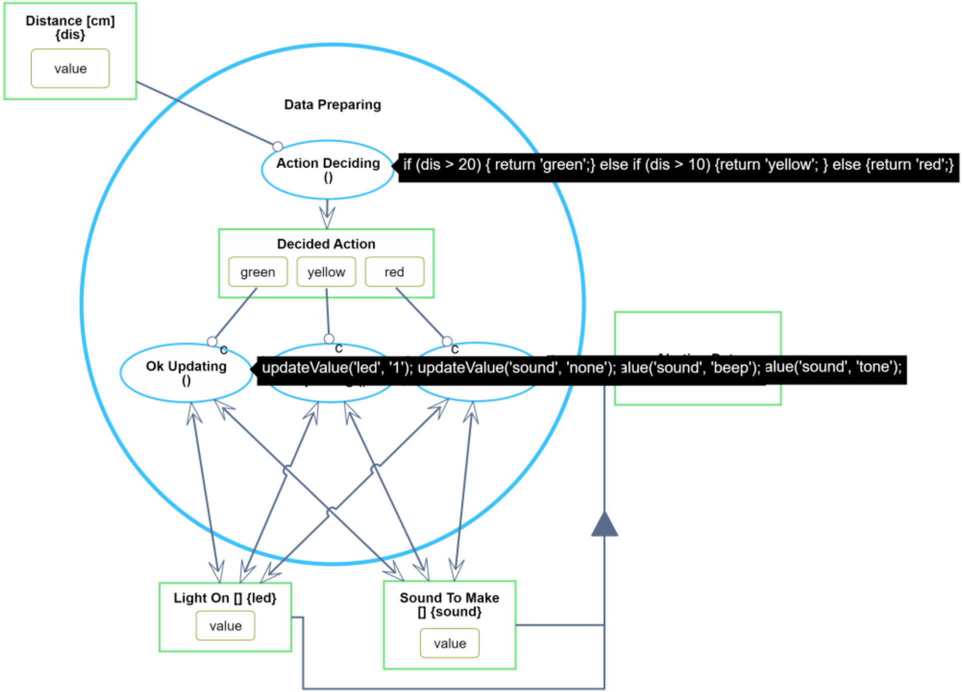
Updated model to include the calculations

- the speed of the sound is 340 m/s or 0.034 cm/µs
- For getting the distance we will multiply the duration by 0.034 and divide it by 2

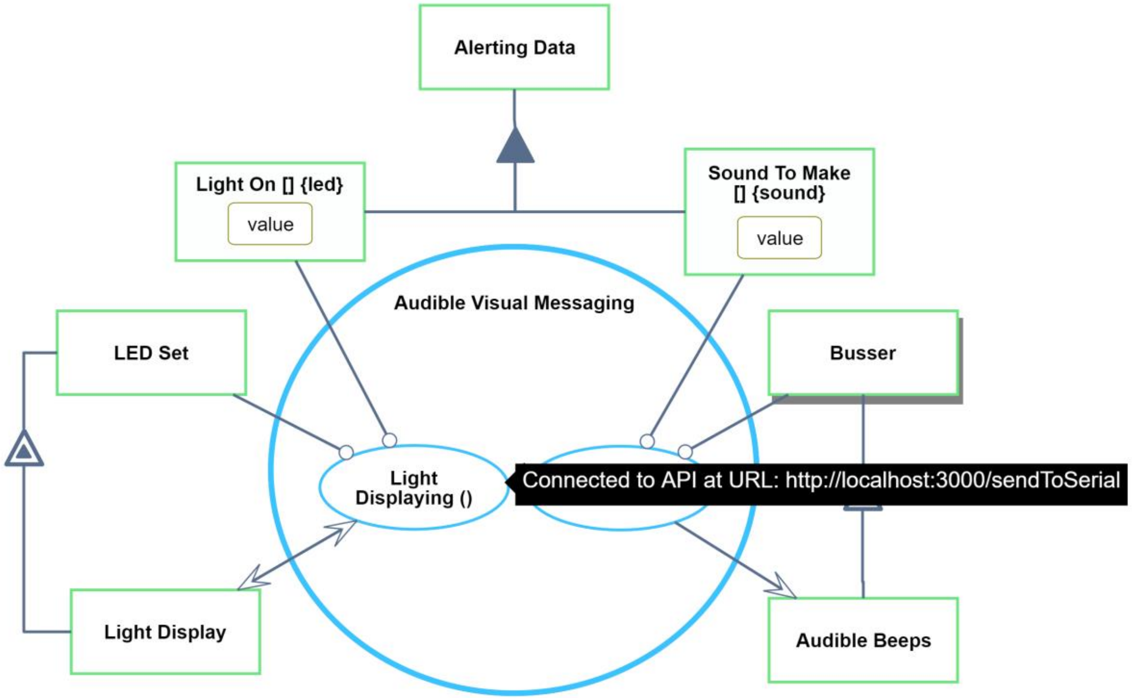


Updated model including calculations

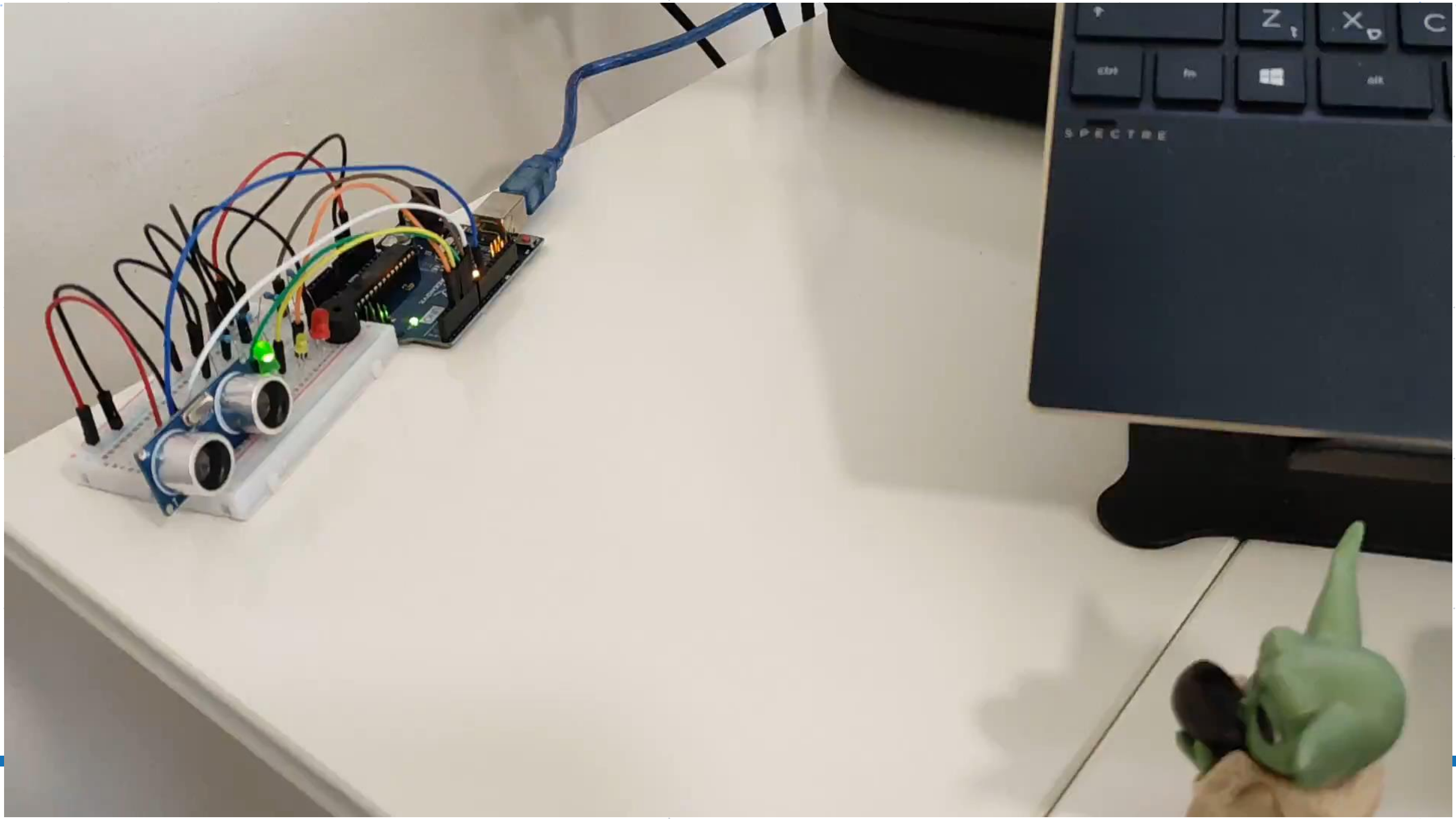




Updated model including calculations



Model Execution with HIL



Thanks for listening!

Experience OPCloud, Cloud-based OPM modeling:
https://www.opcloud.tech/