An End-to-End Infrastructure for Cyber-Physical Intrusion Detection

REINHARD GENTZ, MAHDI JAMEI, ANNA SCAGLIONE

ARIZONA STATE UNIVERSITY, USA

the sine lab

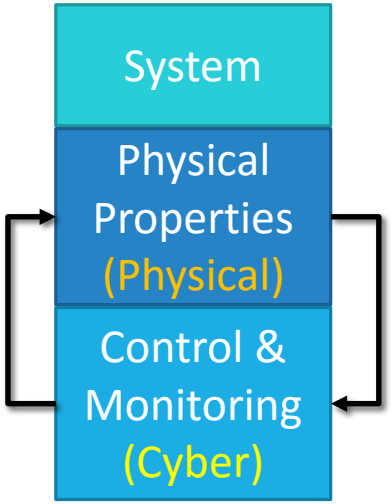
What is Cyber Physical Intrusion Detection

CPS – Cyber Physical System

In a system Cyber & Physical environment is connected

-> Attacks affect both environments

-> We should sense both environments for best attack detection

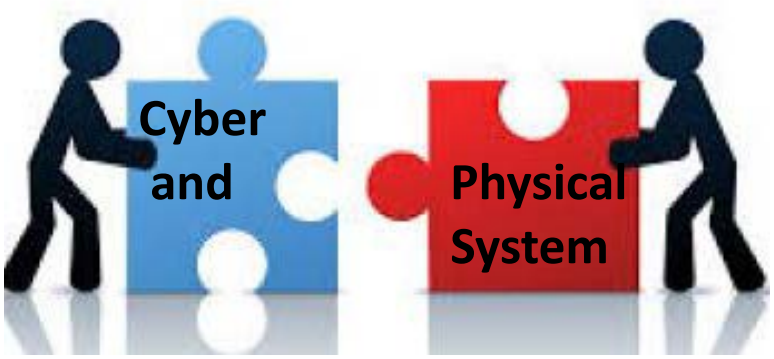


CPS-IDS goes beyond the traditional monitoring solutions adopted in EDS-operations.

It requires new elements :

- High resolution physical-sensing (PMUs)
- Combined network traffic collection & filtering

Challenge: Big Data Problem

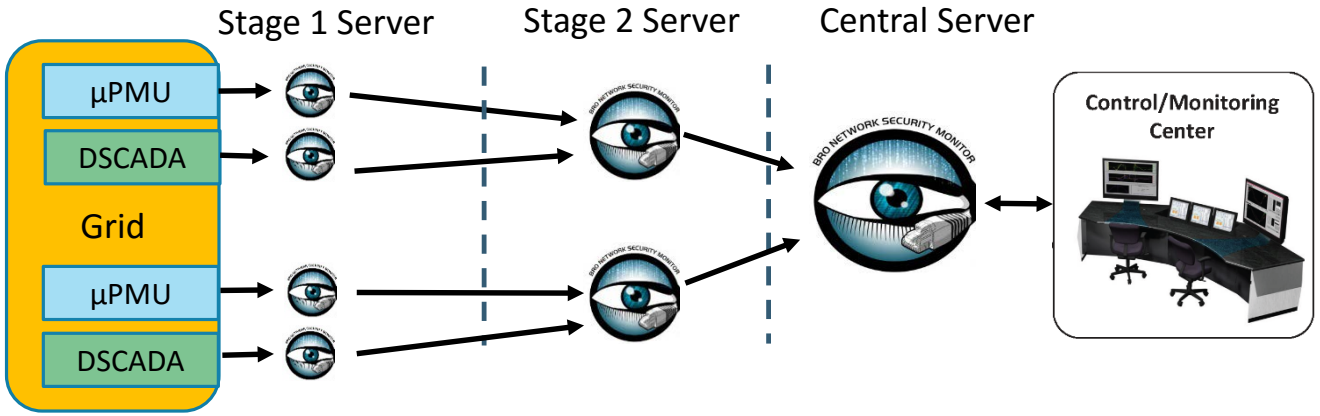


Hierarchical Architecture

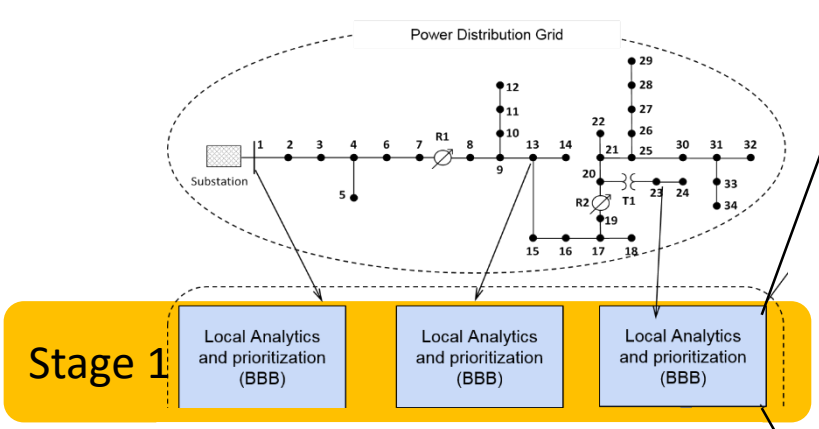
We propose hierarchical architecture:

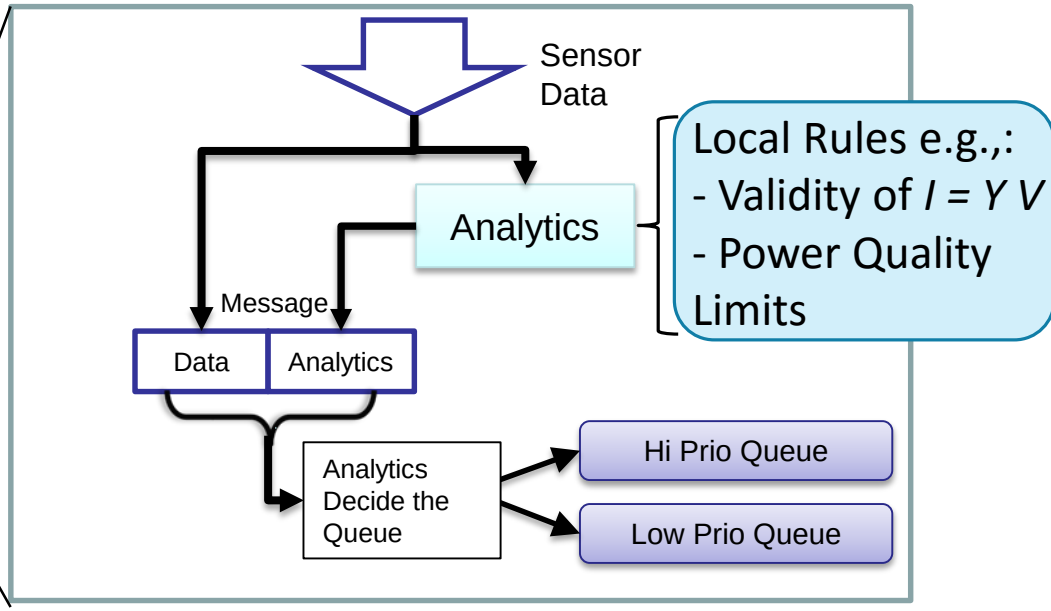
Do as much of the processing locally and only ship what is necessary

- Reduced CPS-IDS network load
- More resilient to network failure – Outages; Attacks
- Distribute computational load – Scalability
- Prioritize important messages (Attacks!) over status messages

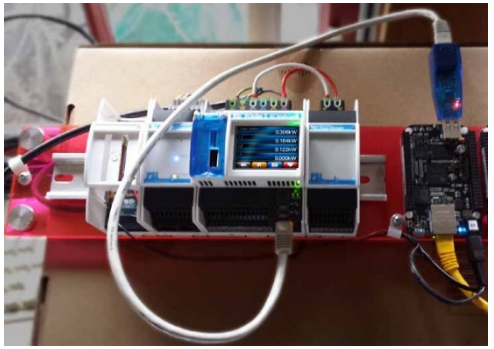


Stage I (Local Processor)



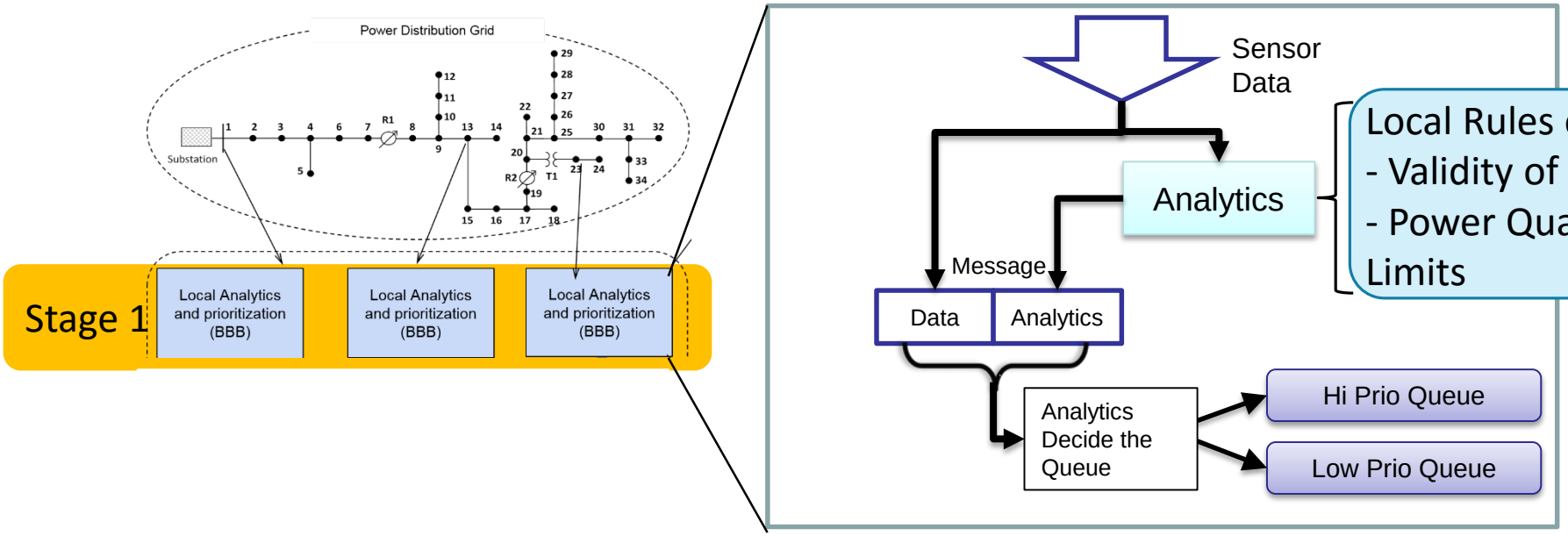


- Gather Local Data:
- Analyze it & based on the result
  - PMUs produce large quantities of precise data
  - Prioritize the message
  - Reduce the message size



a uPMU with a BBB attached

Stage I (Local Processor)



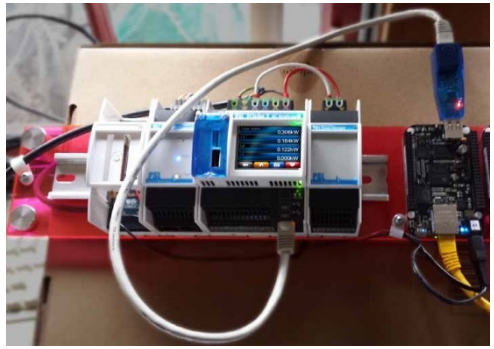
The BBB computer shields the sensor from the outside world

The analytics systems are plug-in modules

– Easy to update and replace

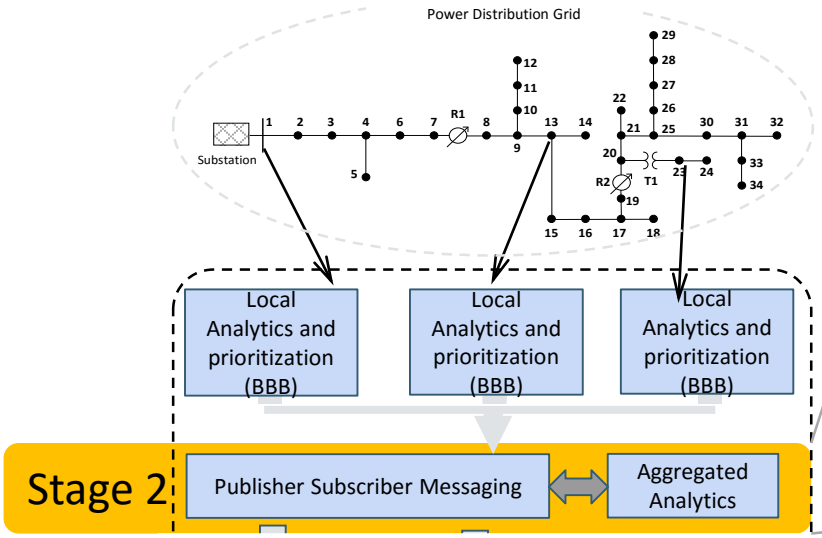
– Not-on-premises can be done by different programmer (Only API knowledge needed)

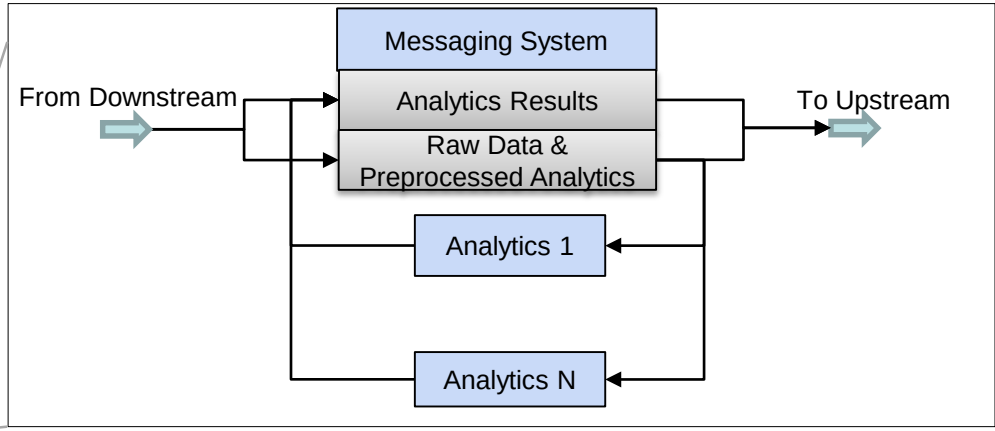
Independence from sensor vendor security updates



a uPMU with a BBB attached

Stage II

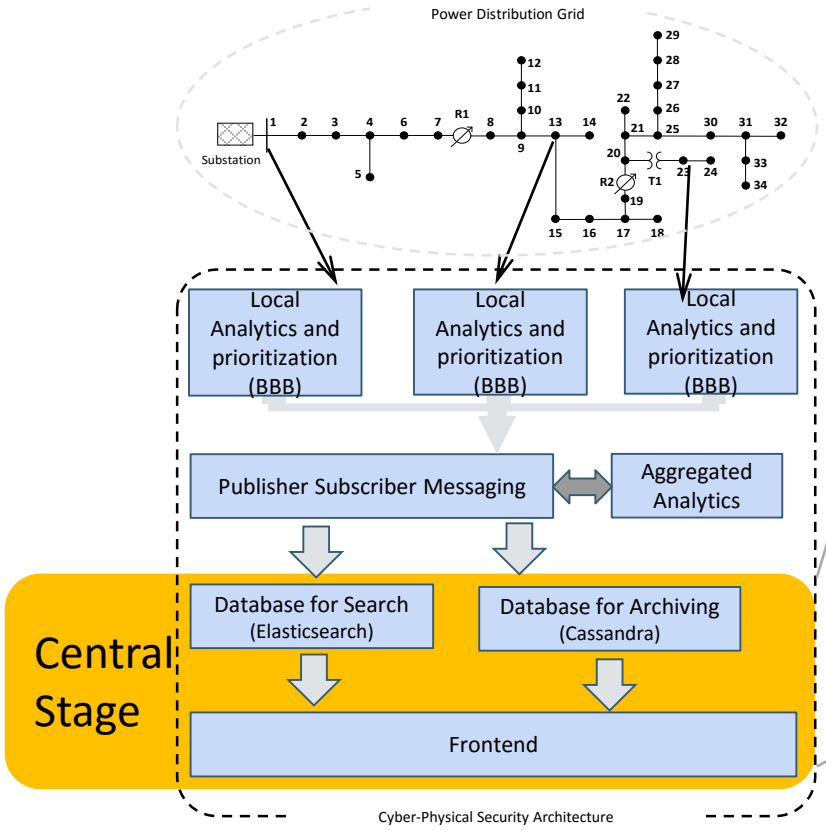




- Aggregate Data from multiple sensors
- & Fuse it with static information, (e.g. reference model for subnetwork)
- Decrease false positive and false negatives
  generate actionable alarms with low latency
- Targeted request of input data with a publisher subscriber model

- Stage can be repeated for scaling, wide area deployment

Central Stage/Human Machine Interface



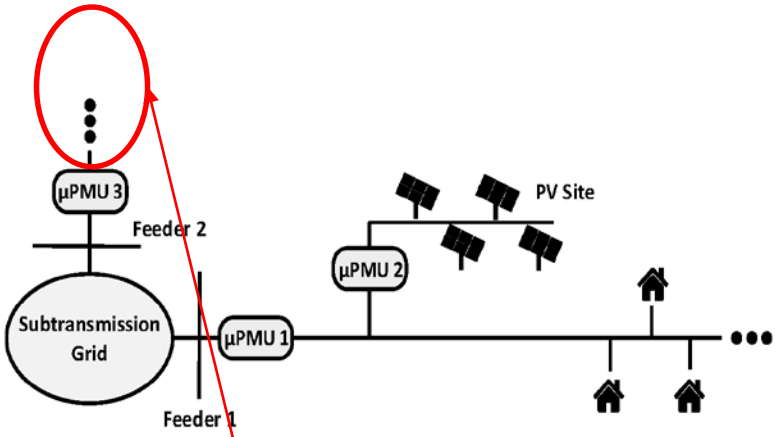
Different databases have different strengths
- Especially for big data

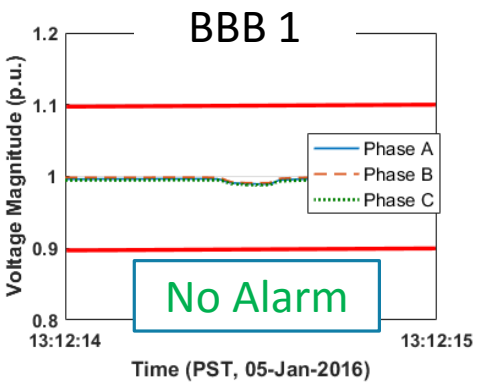
Search for properties? Elasticsearch

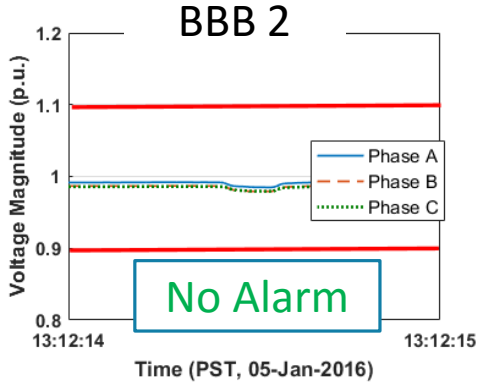
Retrieve lots of raw data? Cassandra

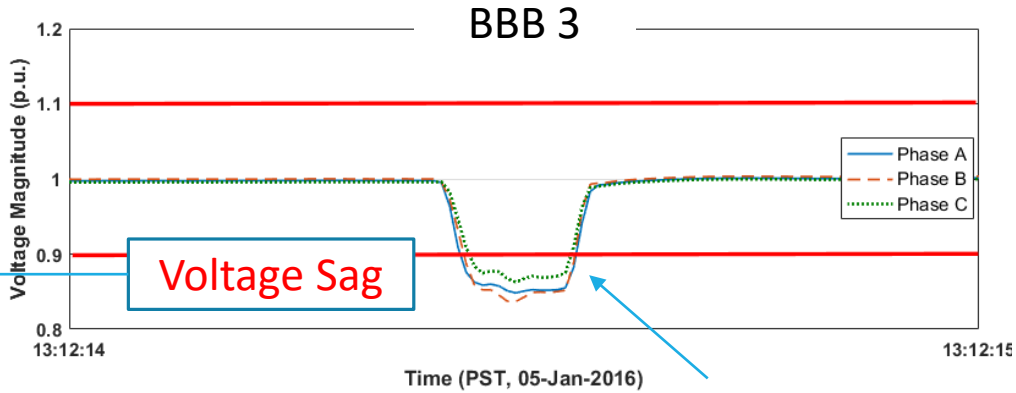
- Archive the data & analytics results
- Frontend to the user

Example Analytics - Localizing Fault









Stage 2's View

No Alarm

No Alarm

Voltage Sag

=>

Fault localized downstream of uPMU 3

Threshold crossed

Results found from data analysis.
Priority for transmission

Thank you

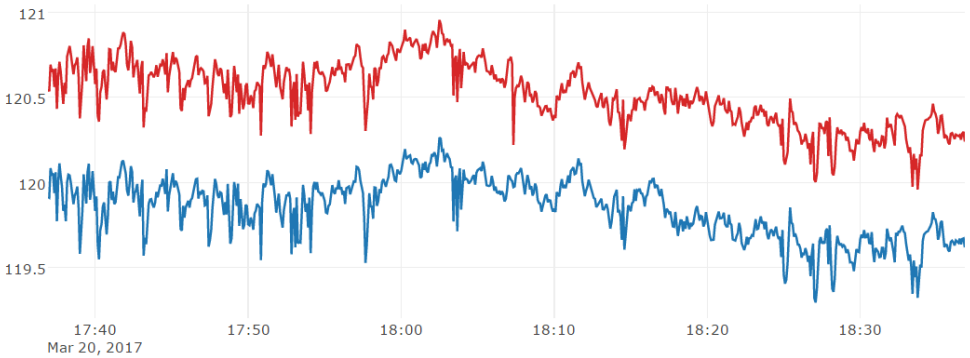
Questions?

Stage II Validation

- We see how the measurements are correlated

Sensor 1
2nd floor

Sensor 2
Basement ServerRack



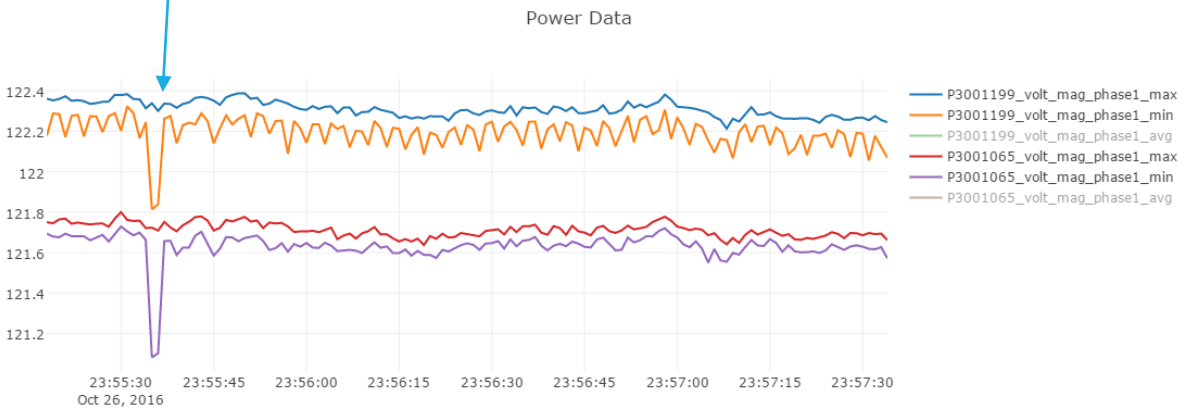
Stage II Validation

Voltage Dip in the whole building

- We see how the measurements are correlated

Min/Max Sensor 1
2nd floor

Min/Max Sensor 2
Basement ServerRack



Question: Is this pattern possible with the specific electrical grid in place? => Further validation