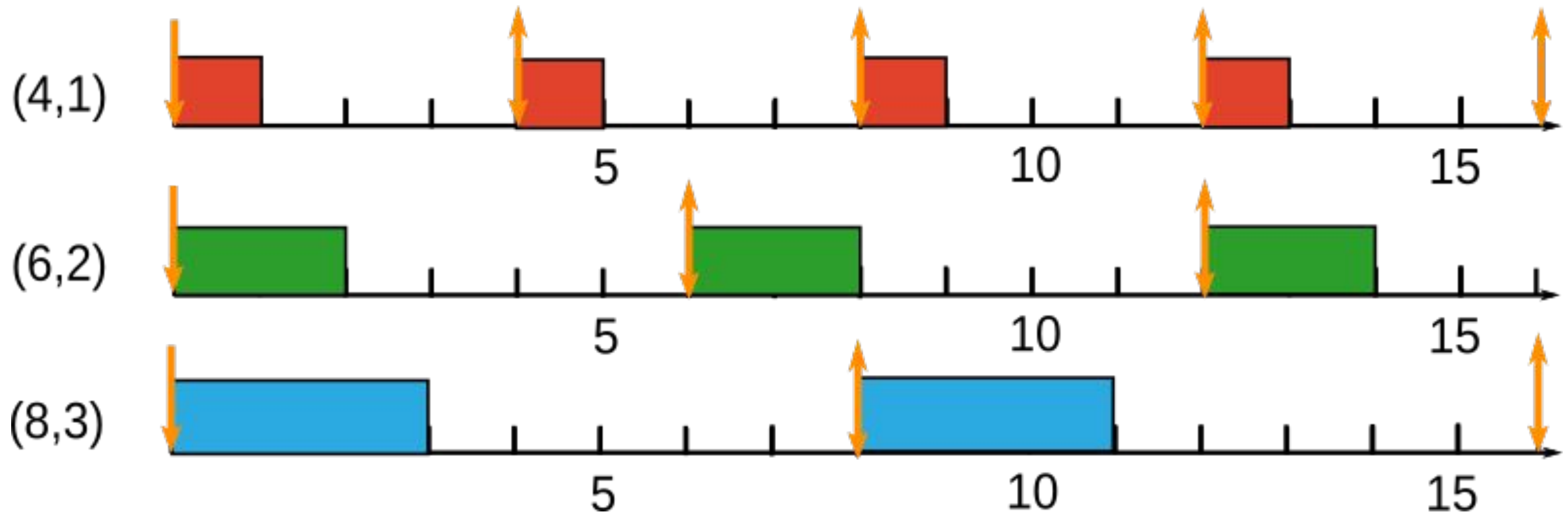
Timed Data: Are deadlines enough?

Pesaresi Seminars
University of Pisa

José Luis Conradi Hoffmann

Supervisors:
Prof. Antônio Augusto Fröhlich, PhD.
UFSC
Prof. Paolo Milazzo
UniPi

The complexity of S-o-t-A Real-Time Systems



The complexity of S-o-t-A Real-Time Systems

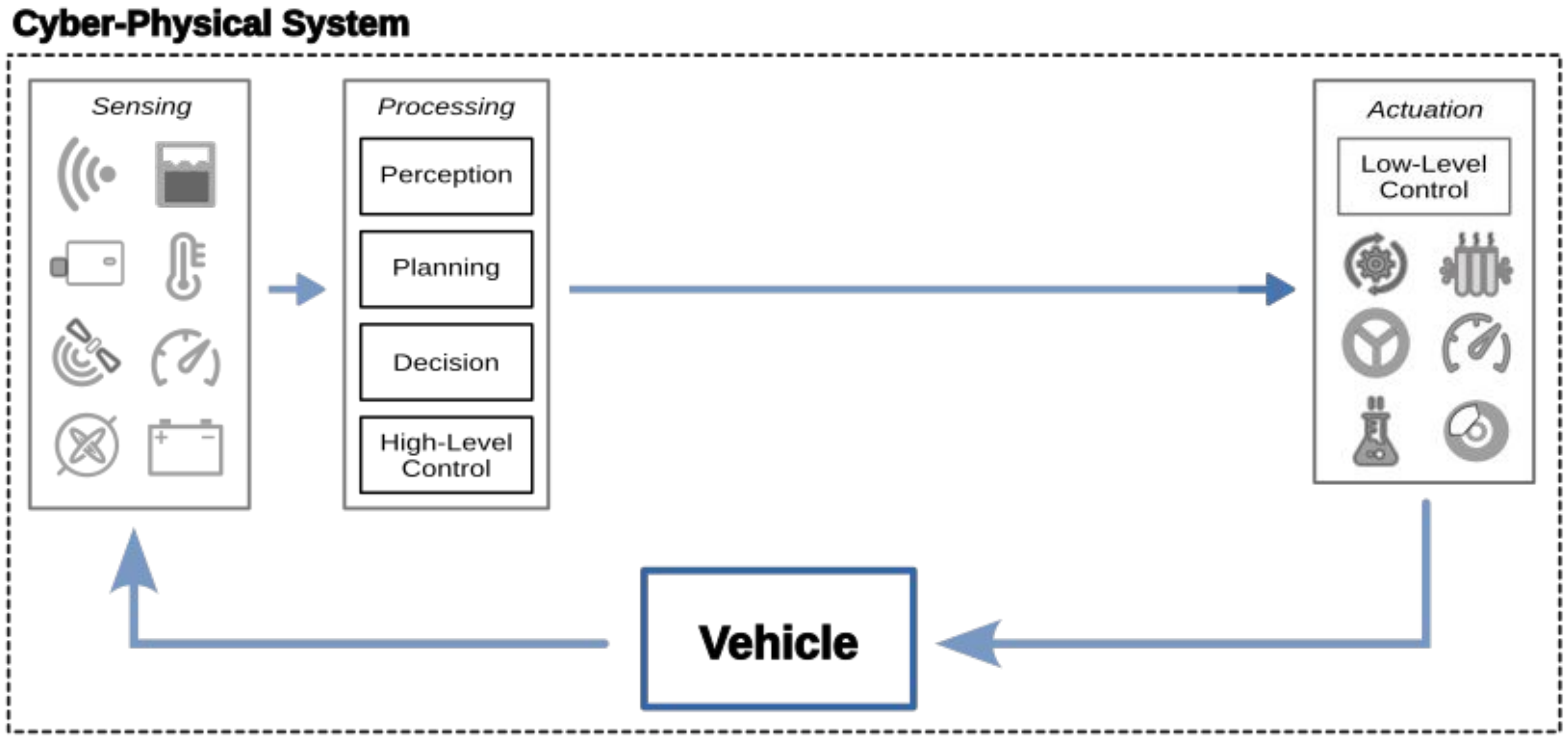


Figure Source: Antônio Augusto Fröhlich

The complexity of S-o-t-A Real-Time Systems

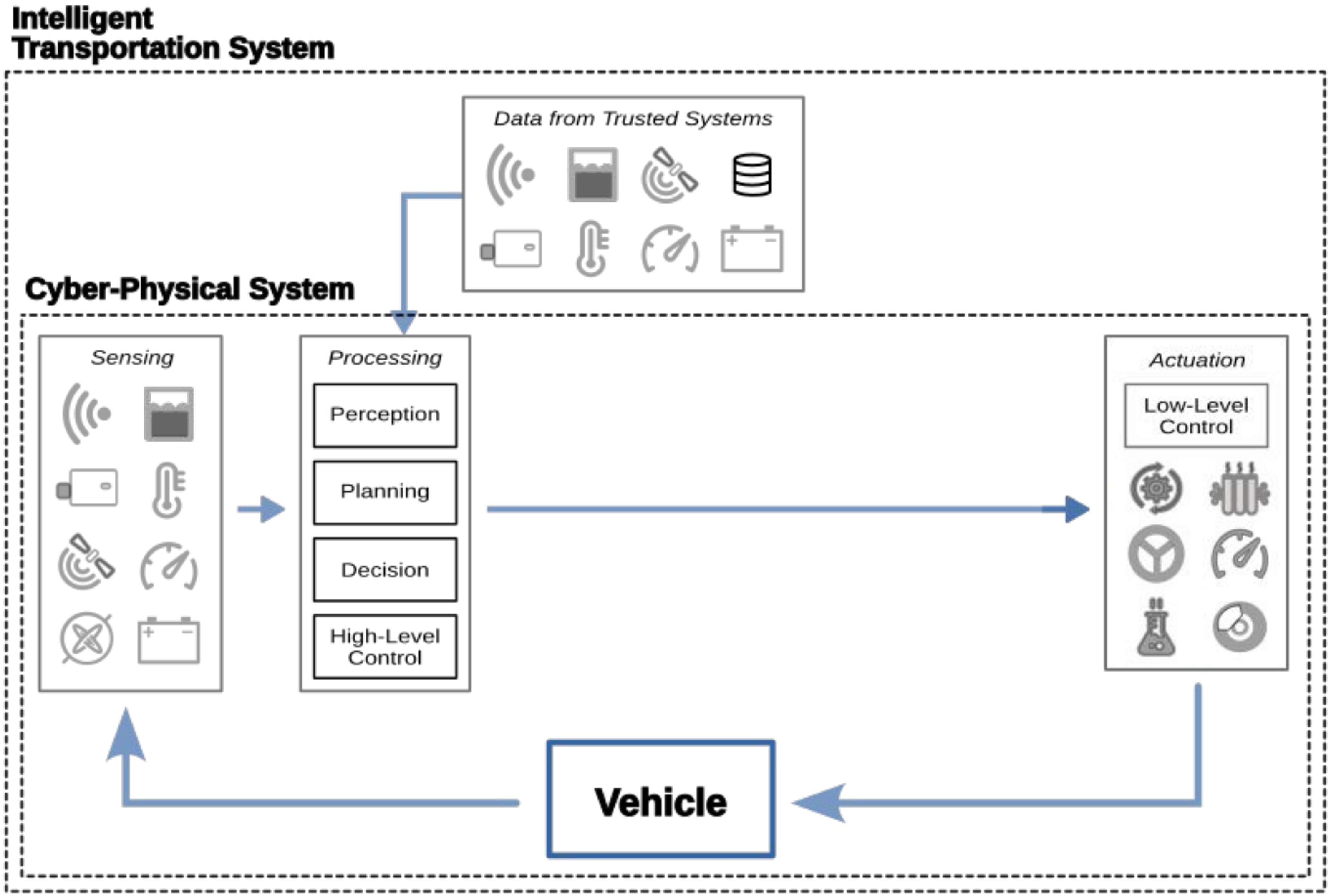


Figure Source: Antônio Augusto Fröhlich

The complexity of S-o-t-A Real-Time Systems

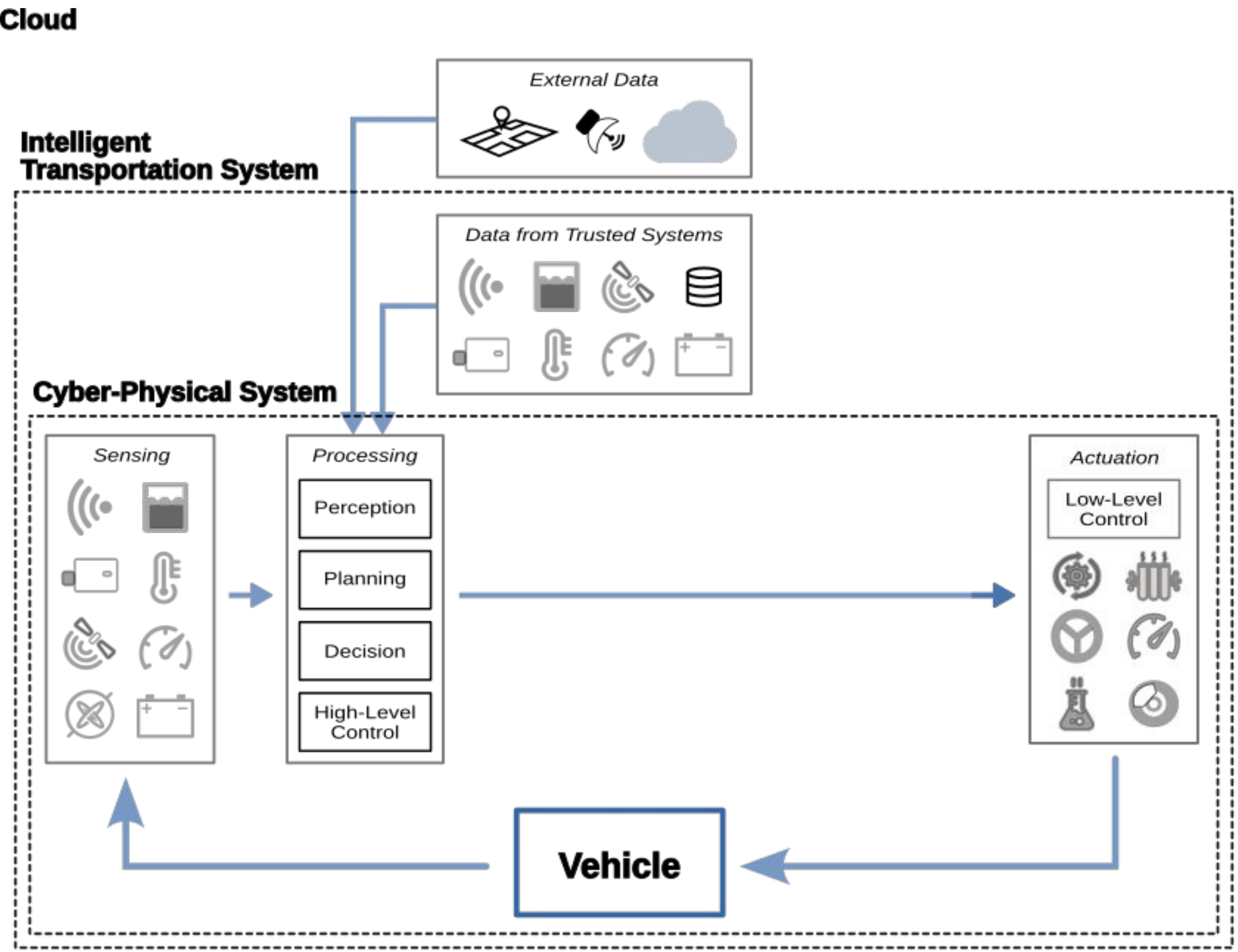


Figure Source: Antônio Augusto Fröhlich

The complexity of S-o-t-A Real-Time Systems

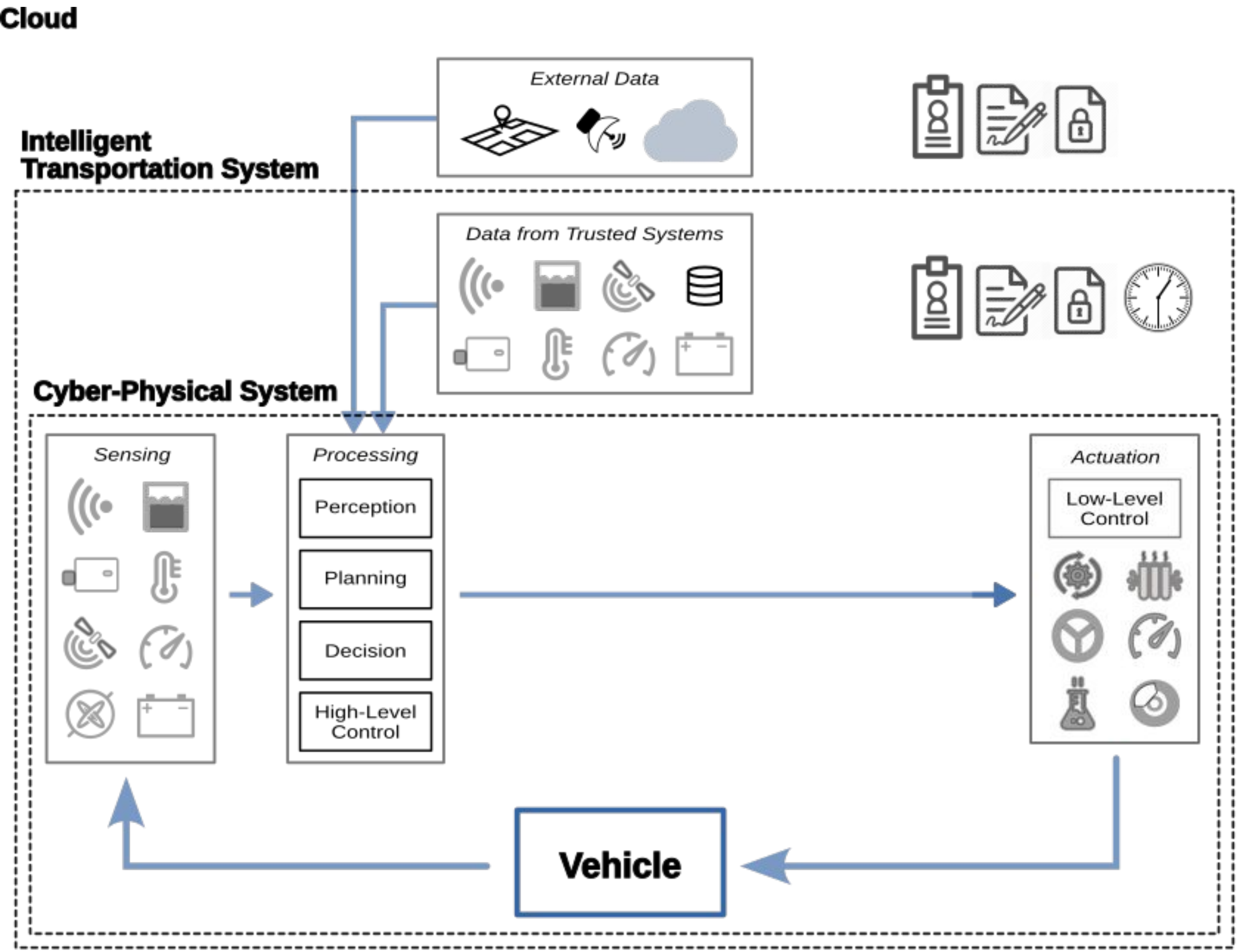
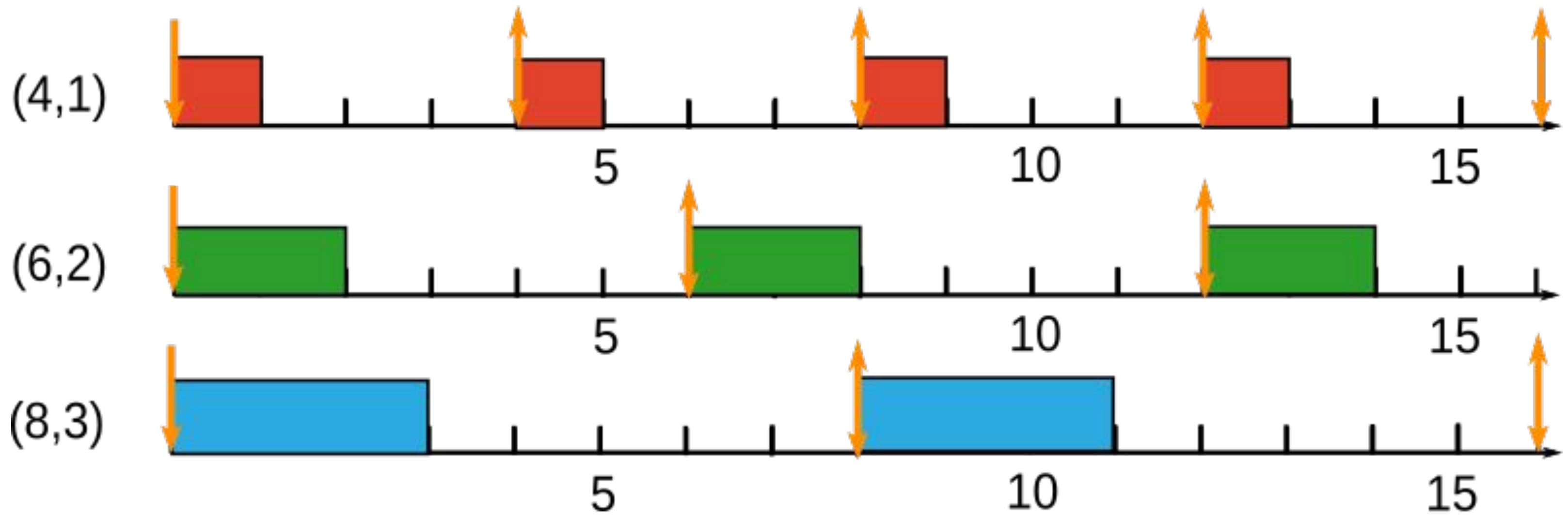


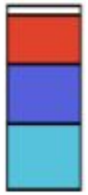
Figure Source: Antônio Augusto Fröhlich

What is lacking from classical RT Theory?

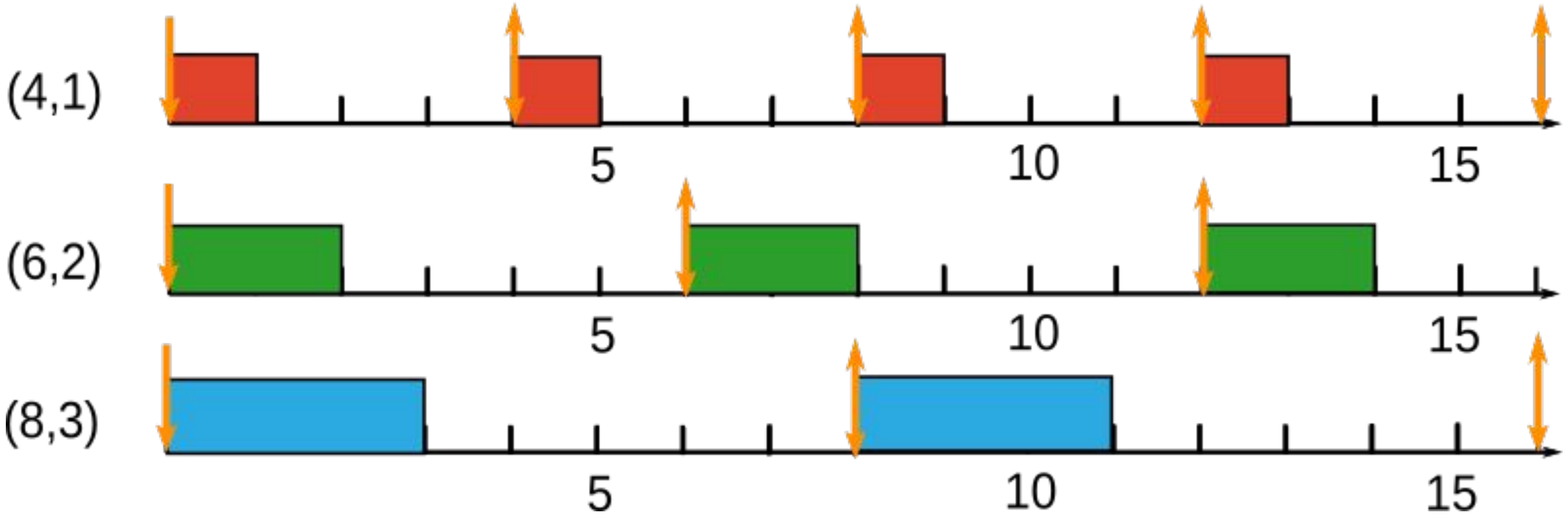


What is lacking from classical RT Theory?

Contention?

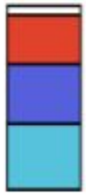


- Multicores
- OS Strategies
  - µ-kernels
  - Isolation
  - Page Coloring
  - Monitoring + ML-Scheduling
- Safety-Critical: WCET estimation
  - Over- or Sub-estimated?



What is lacking from classical RT Theory?

Contention?



Data?

Timed

- What? When? Where?
  - Semantics
  - Fault-Tolerance
    - Fault tracing?
    - Replication?
- Safety-Critical:
  - **Data quality?**
  - **Data Expiration?**

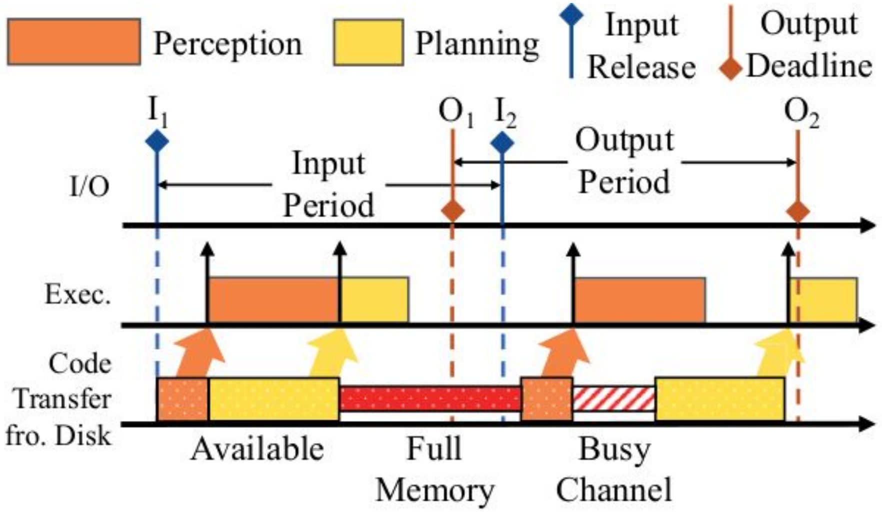


Fig. 1: Autoware with periodic input.

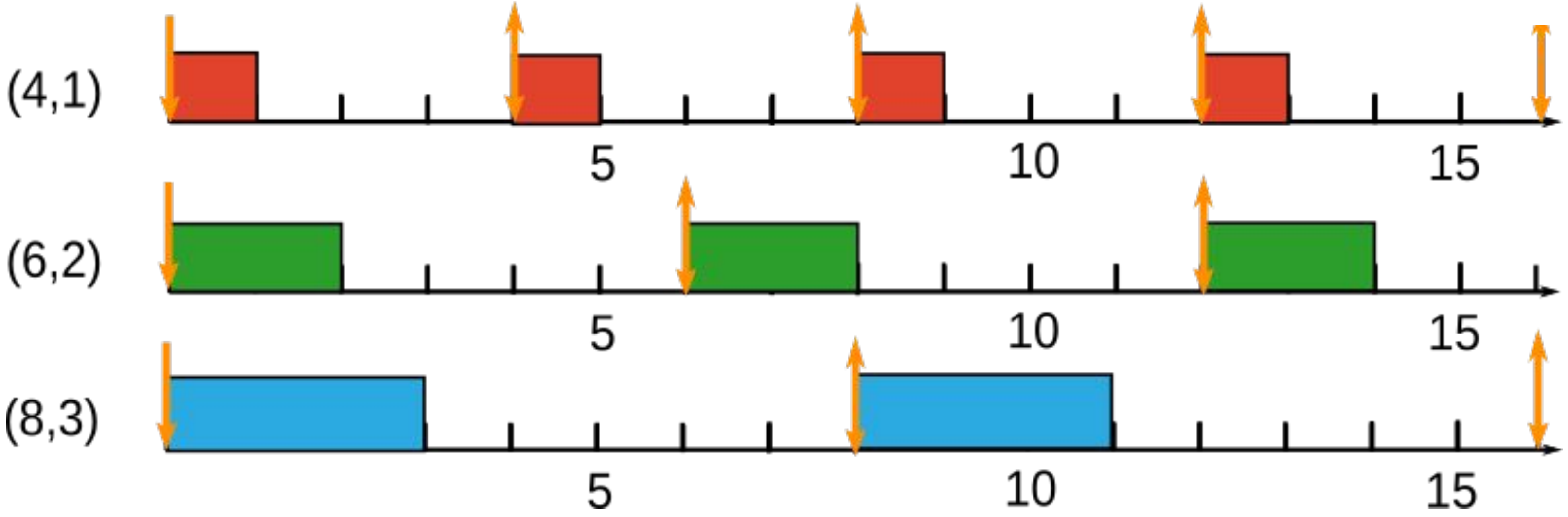
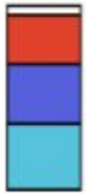


Fig1 Source: Predictable Data-Driven Resource Management (Bateni et al., 2019)

What is lacking from classical RT Theory?

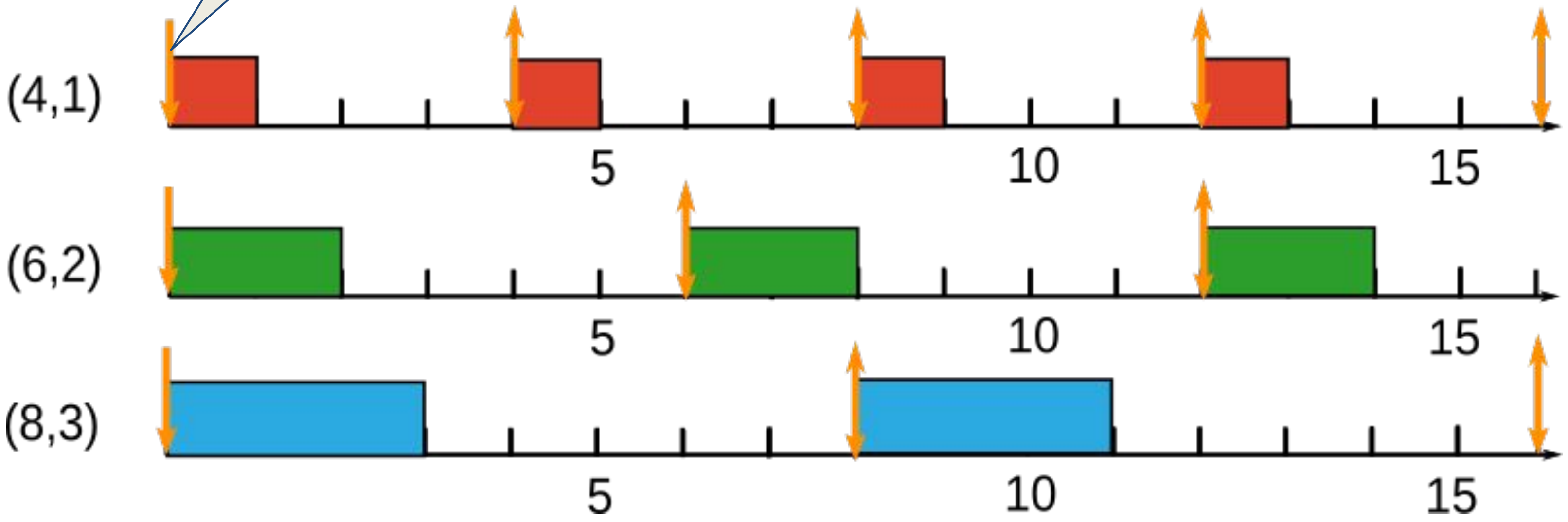
Contention?



Data?

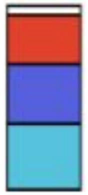
Timed

Data Sampled at T = -1?

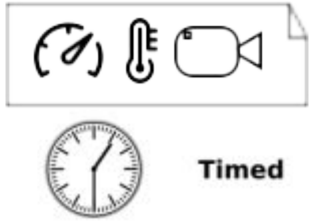


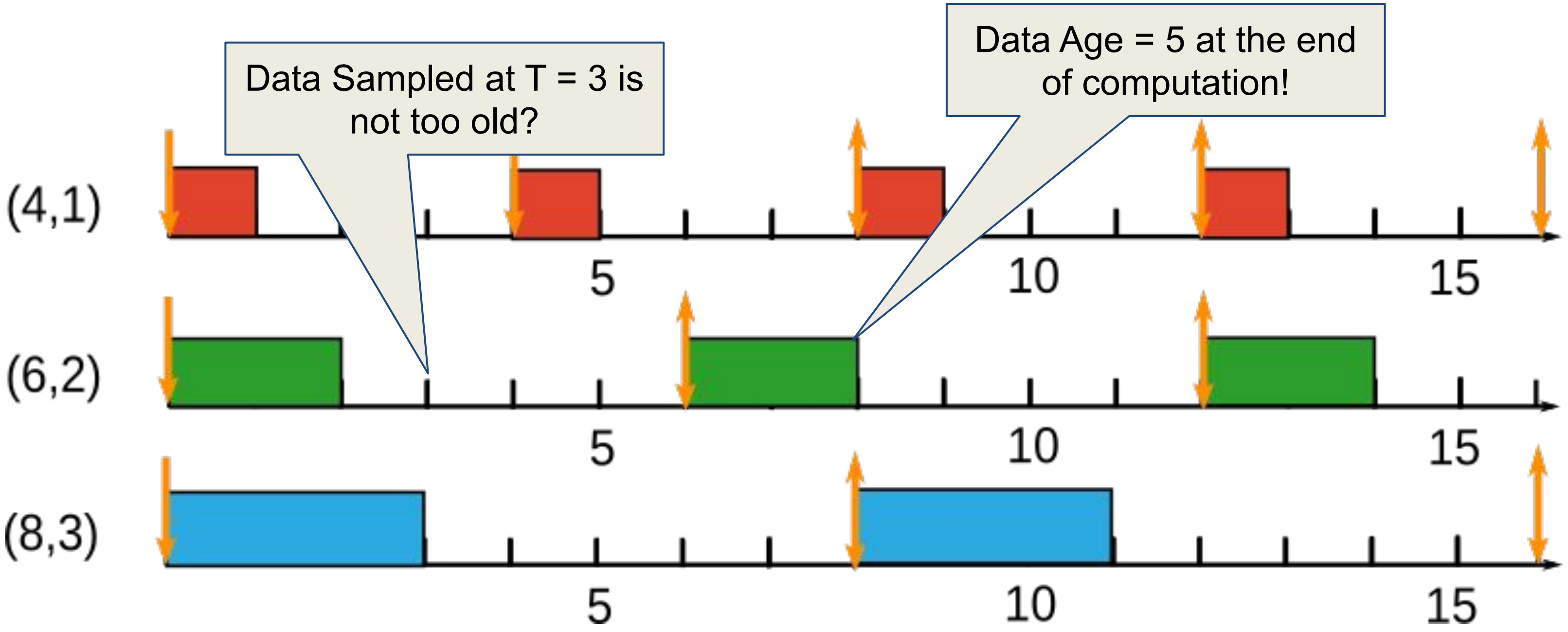
What is lacking from classical RT Theory?

Contention?



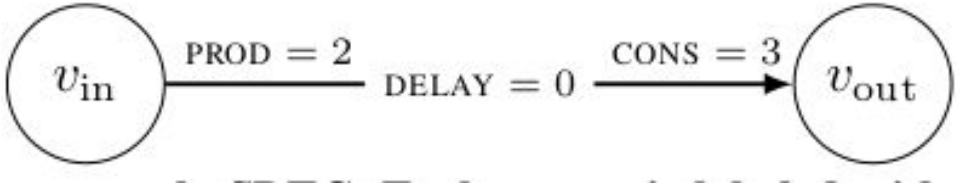
Data?

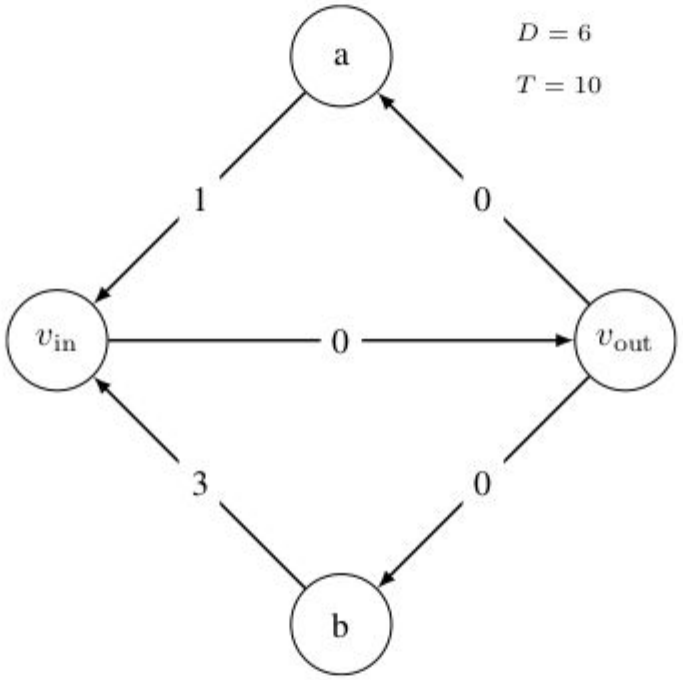




SDFG (Lee et al., 1987)

- Period, Deadlines, and WCET + Data dependency



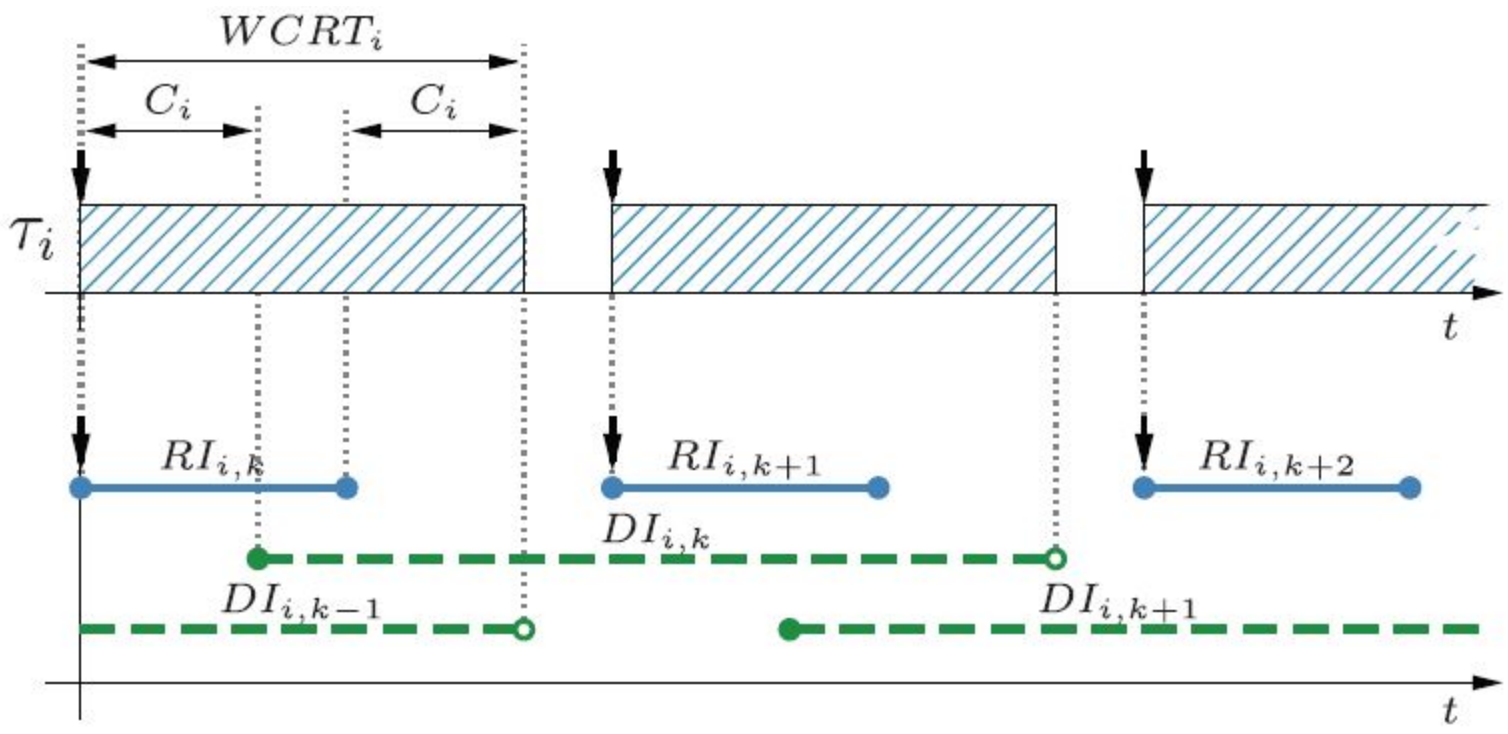


actor	v_{in}	v_{out}	a	b
WCET	1	1	1	2

- Throughput and energy constraints (Damavandpeyma et al., 2013), (Stuijk et al., 2007)
- Dynamic scheduling (Singh et al., 2017)
- Buffer estimation with unrolling techniques over task execution (Shin et al., 2010)
- Inspired Methodologies
    - e.g., Data communication

End-to-end timing analysis (Becker et al. 2017)

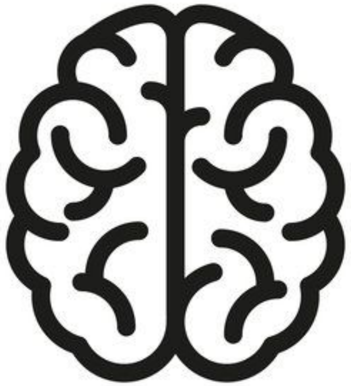
- Task dependency, Cause-effect chains, End-to-End timing, and Data Age Constraint
  - Data propagates through a chain of tasks within certain time bounds.
    - Time from reading the data until the actuation is subject to delay constraints in addition to the task's individual timing constraints
- **Dynamic schedules** → WCRT (earliest and latest moment a task can run)
  - Ci : WCET
  - Ri : Read Interval
  - Di : Data Interval

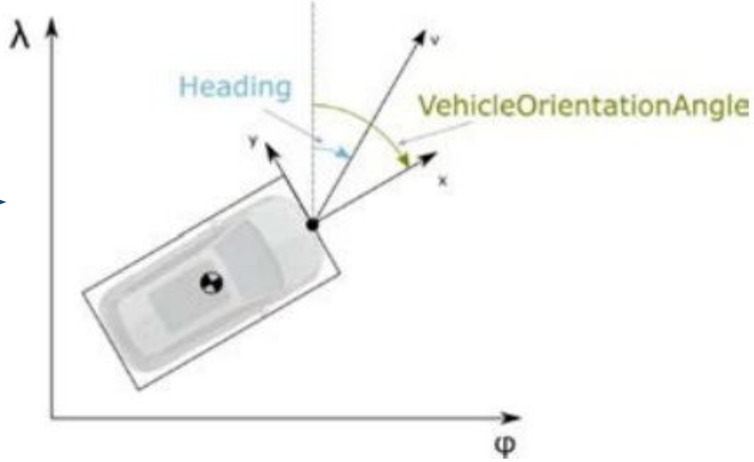


- **What is lacking?**
  - Maximum Age:
    - What about data sampling rate?
  - Everything is at shared memory!
  - Semantics of data?

What is lacking from classical RT Theory?

When?

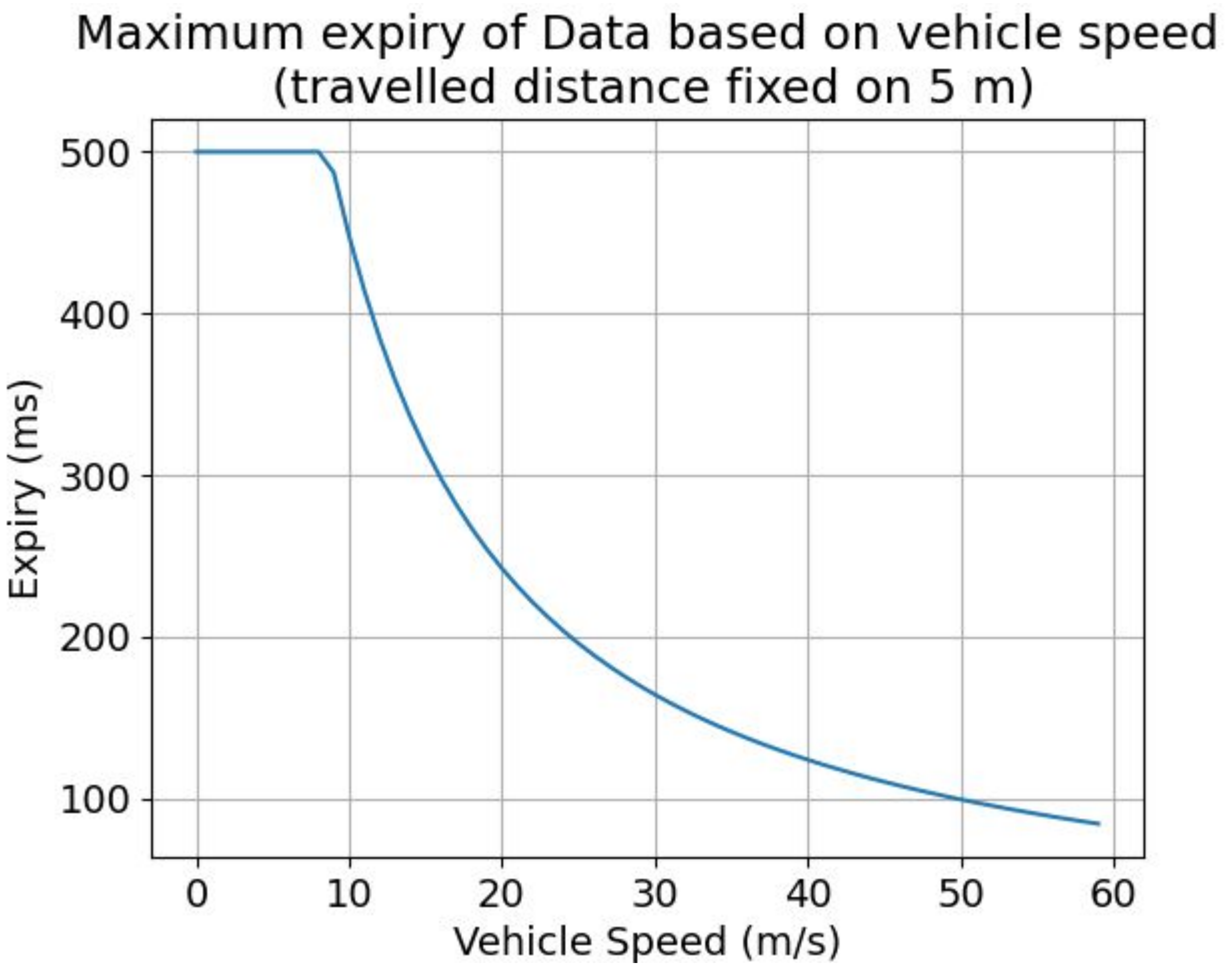




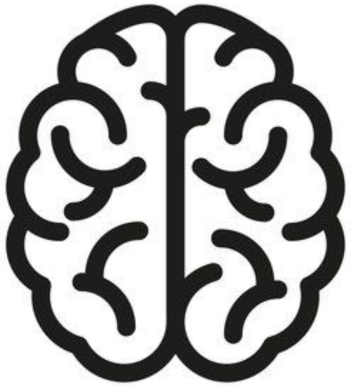
For those using this in next steps:
is it valid until?

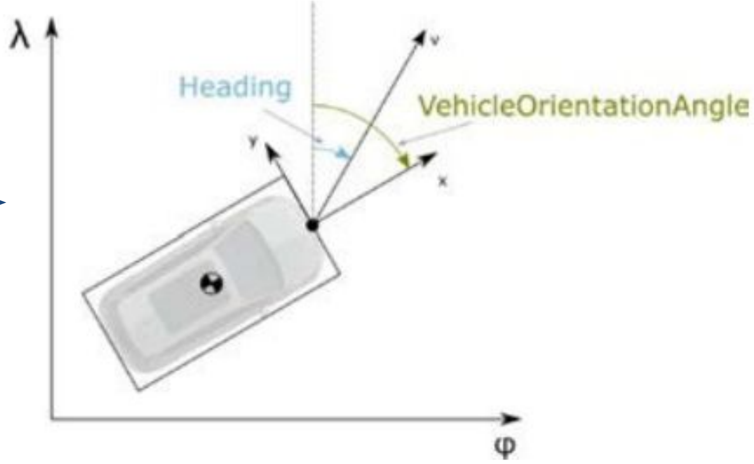
Determined by the state of the system!

Update rate based on how much I have travelled



What is lacking from classical RT Theory?





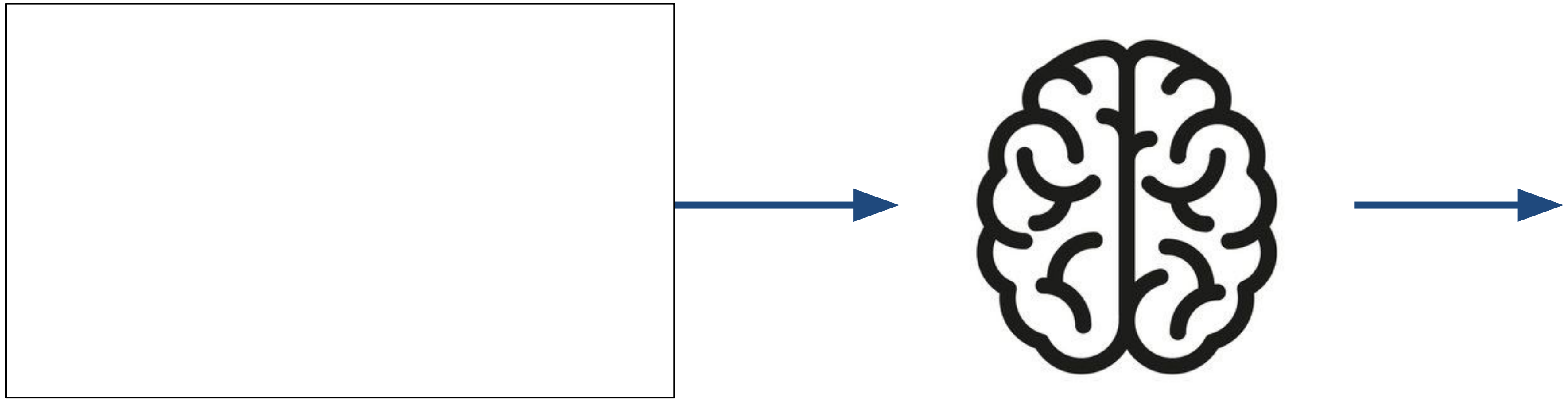
When?

For those using this in next steps:
is it valid until?

Dynamicity in time requirements?!

What is lacking from classical RT Theory?

- Errors on sensor!

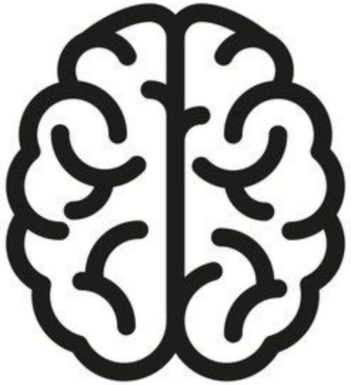


No vehicles ahead…
No need to brake!

Plausible?

What is lacking from classical RT Theory?

- Errors on AI!



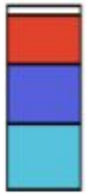
Plausible?

No vehicles ahead…
No need to brake!

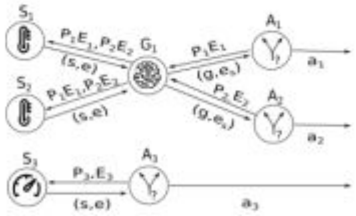
What is lacking from classical RT Theory?

- Not everything is local!
  - shared memory assumption
- Random Delays!
  - Modeling Medium
- Wireless communication
  - Collision, hidden nodes…
- Safety-Critical: **Jitter and Latency!**

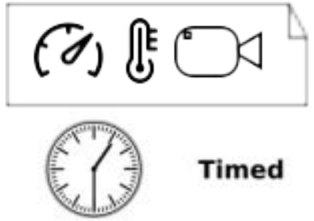
Contention?

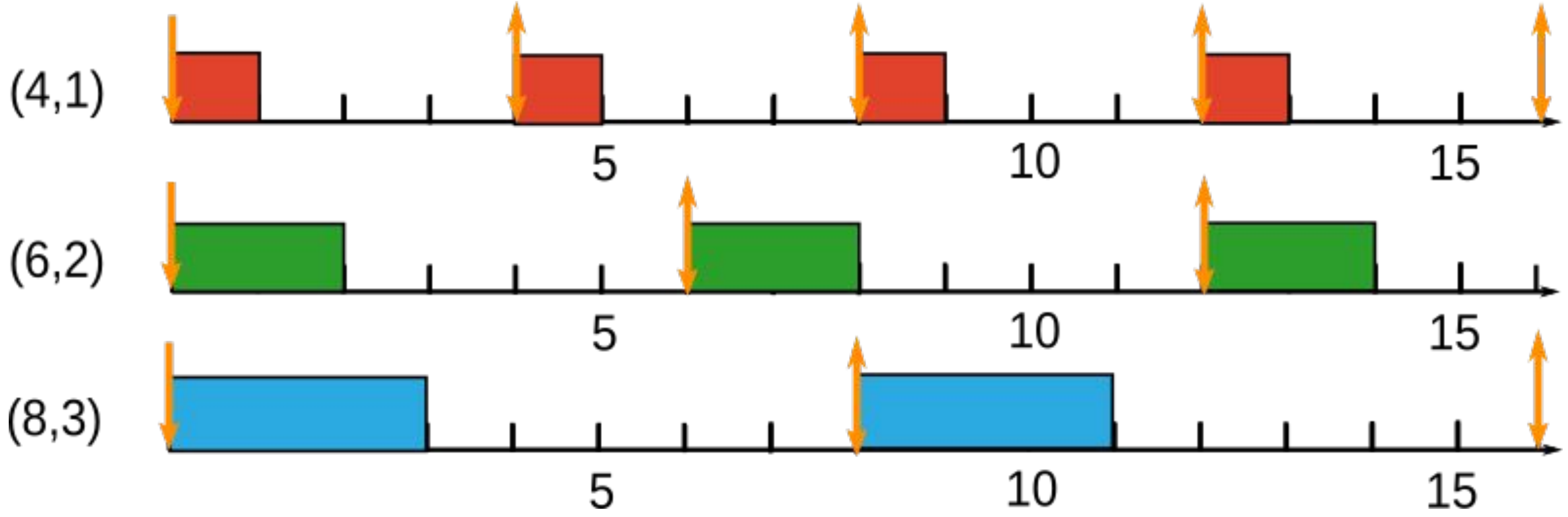


Network?



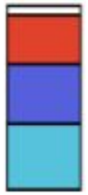
Data?



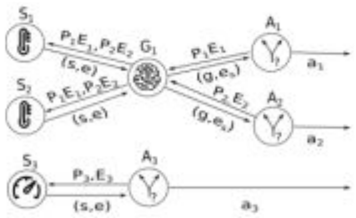


What is lacking from classical RT Theory?

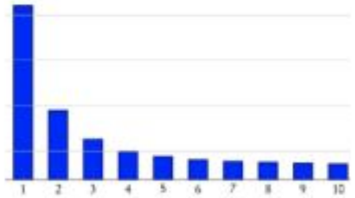
Contention?



Network?

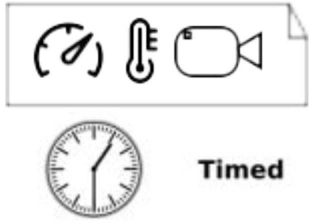


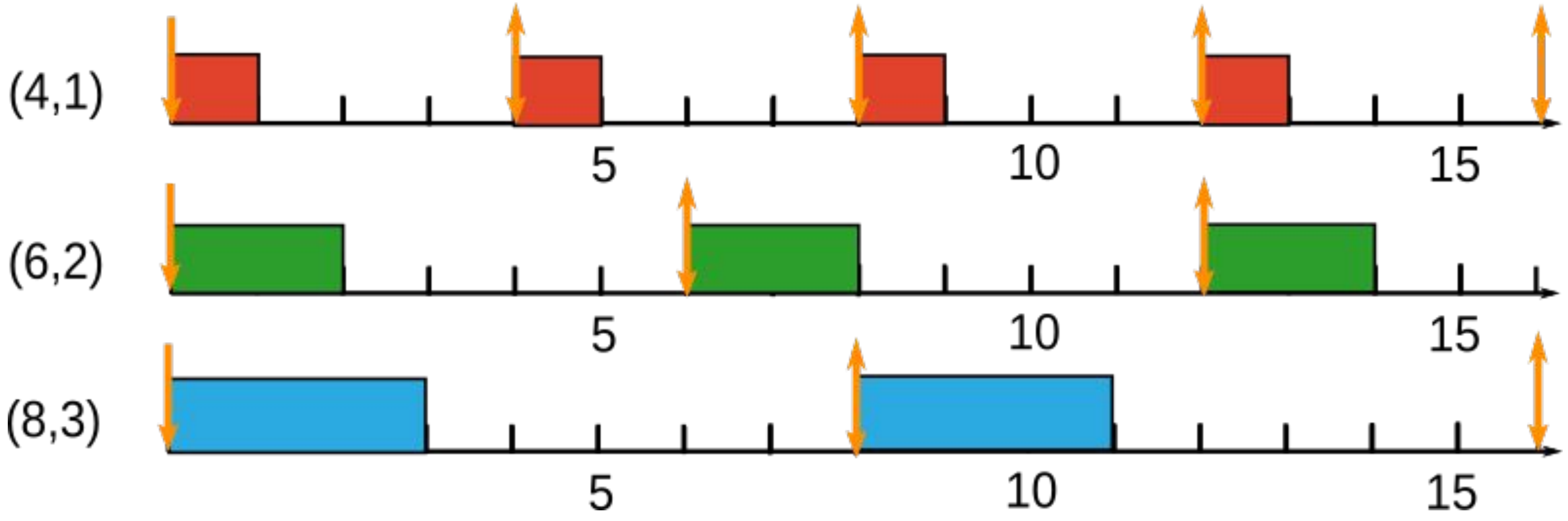
Bandwidth?



- Data flow… GB/s to TB/s
- **Safety-Critical:**
  - Fits in memory?
  - Fits in network?
  - Will it be there when needed?

Data?





Contention in IoT Applications (Alexander and Stefano, 2023)

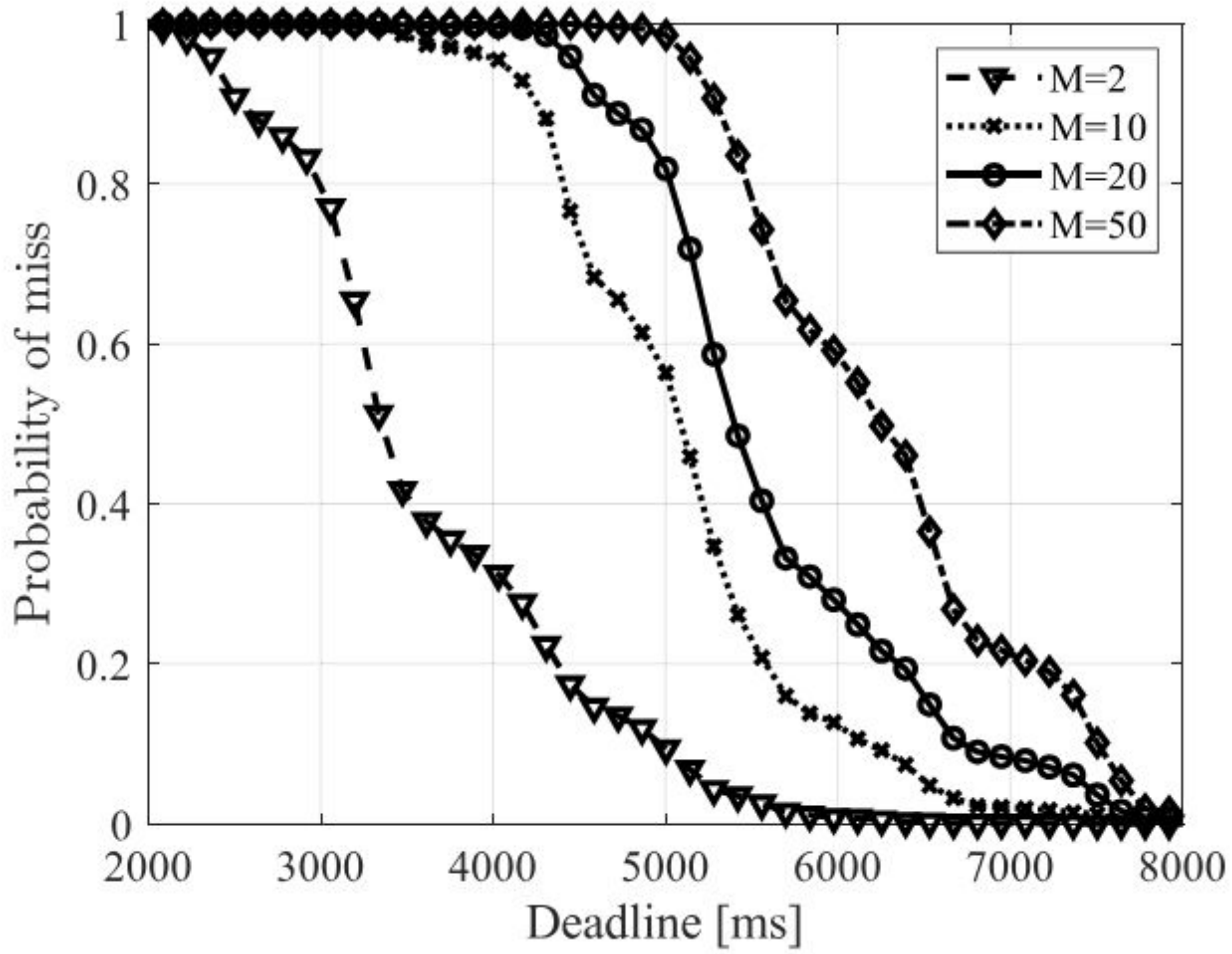
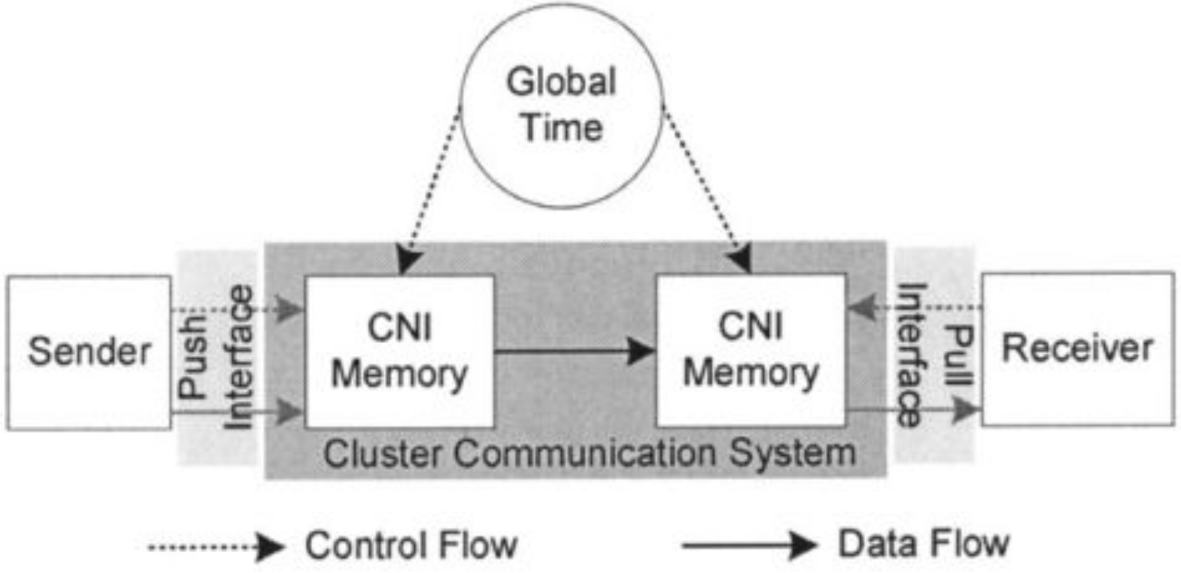


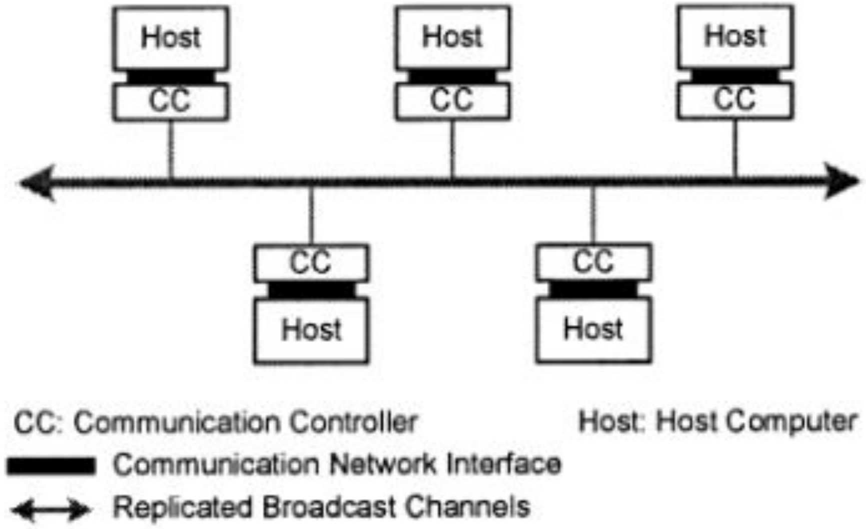
Fig. 7. Miss of deadline for a scenario of M smart sound sensors connected to one server. The GRS algorithm with $I = 1000$ iterations.

Time-Triggered Architecture (TTA) (Kopetz et al., 2003)

- Tasks, Interfaces, Nodes
  - Real-Time
    - Periods, Deadlines, WCET
- **Static** Scheduling (TDMA)
  - A priory send and receive times
- **Guardians**
  - Communication controllers

- TTW – (Jacob et al.,2020)
  - Protocol for Online Switch Mode
    - Pre-Computed Schedules (modes)



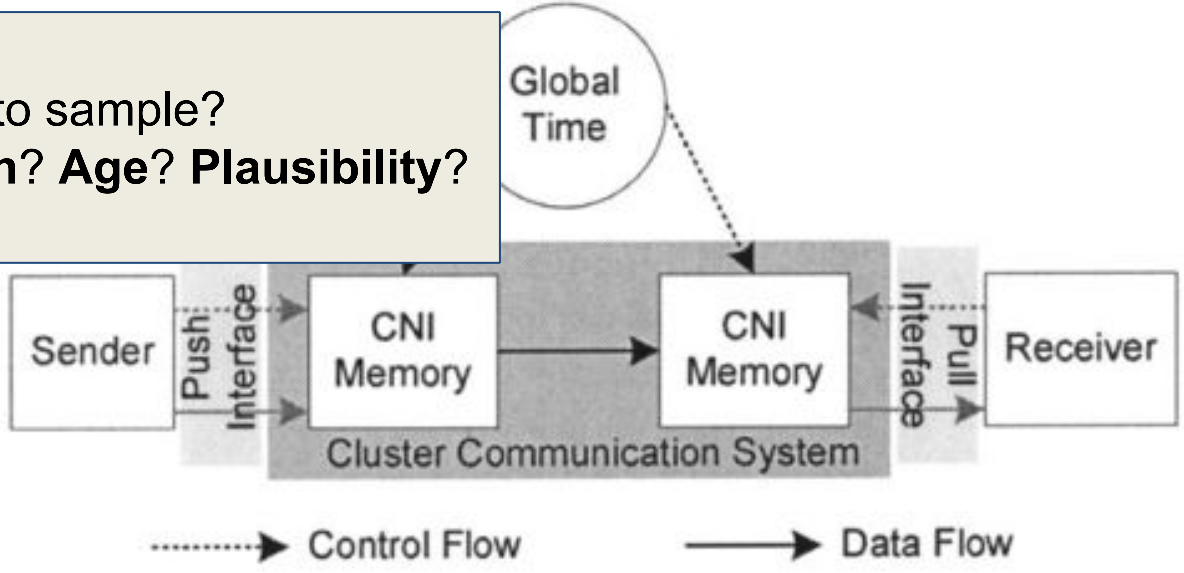


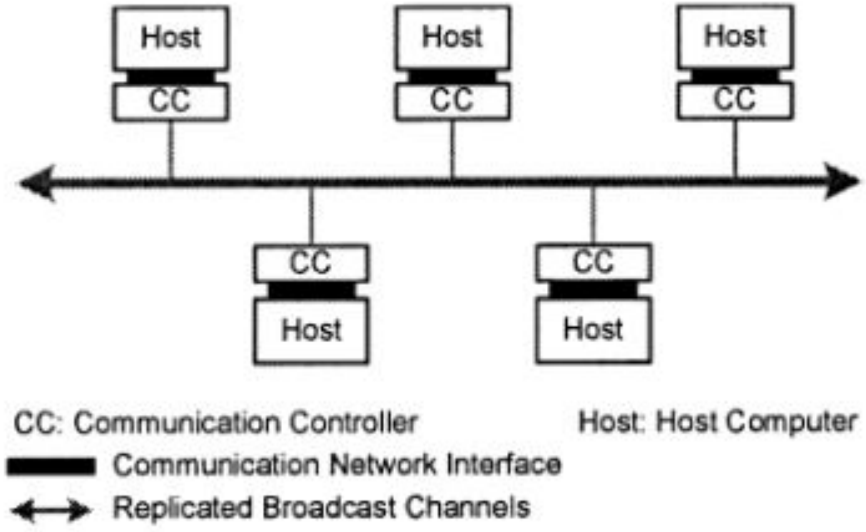
Time-Triggered Architecture (TTA) (Kopetz et al., 2003)

- Tasks, Interfaces, Nodes
  - Real-Time
    - Periods, Deadli
- **Static** Scheduling (TDMA)
  - A priory send and receive times
- **Guardians**
  - Communication controllers

How early do we need to sample?
Freshness? **Expiration**? **Age**? **Plausibility**?

- TTW – (Jacob et al.,2020)
  - Protocol for Online Switch Mode
    - Pre-Computed Schedules (modes)

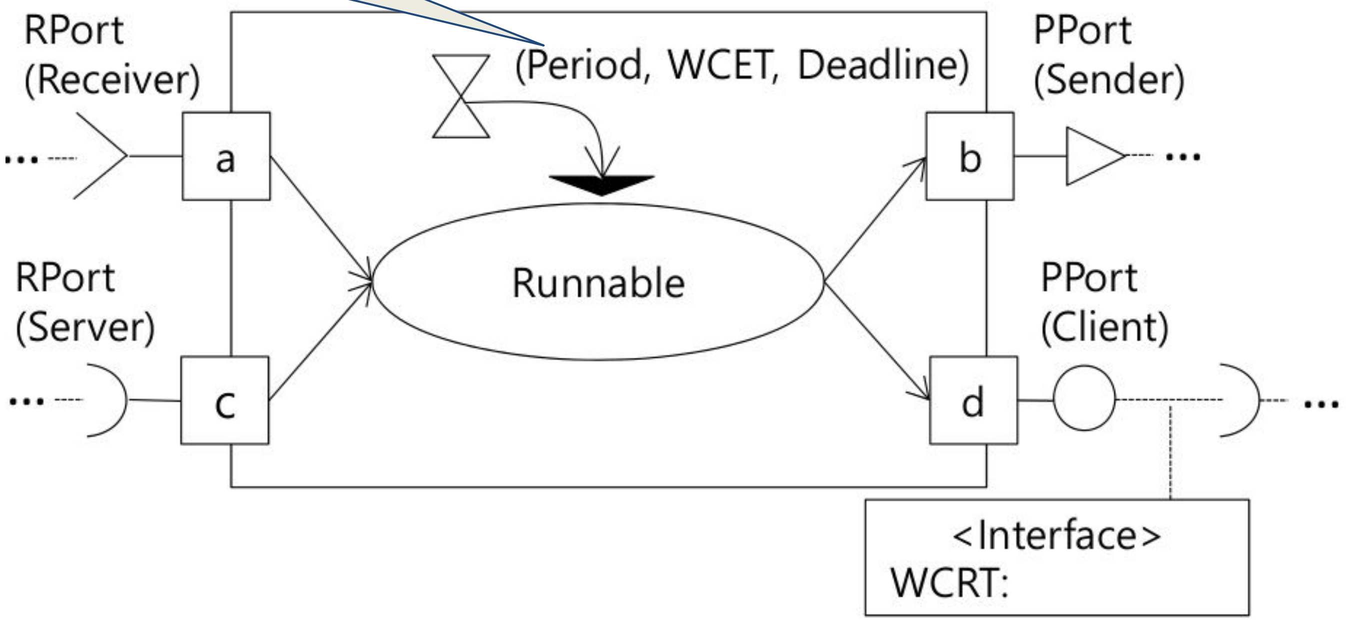


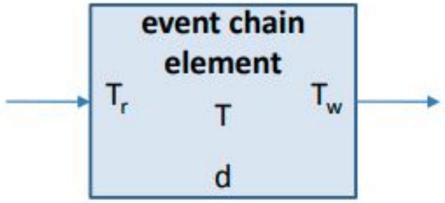


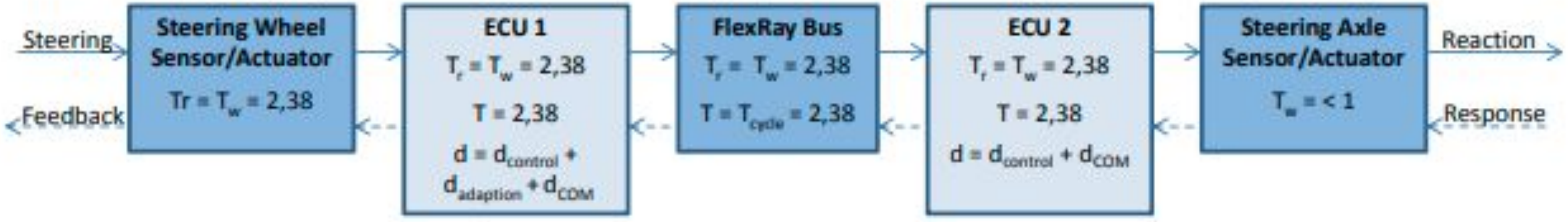
AUTOSAR Design Overview

What if data arrives late?

- Open standard for automotive Electrics/Electronics
  - Layered architecture description
    - **Components, Ports, and Interfaces**
    - **Decoupling** of the **functionality** from the supporting hardware and software services
  - Runnables
    - **Timing**: computation + communications
      - Period, Deadline, WCET, WCRT…
    - **Client-Server:** Operations that can be invoked by components
    - **Sender-Receiver:** interface supports the data communication



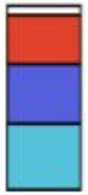




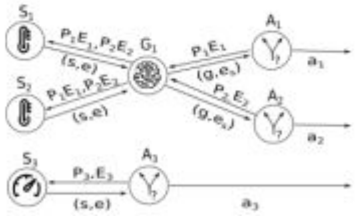
(Klobedanz et al., 2010) and (Kim et al., 2016)

What is lacking from classical RT Theory?

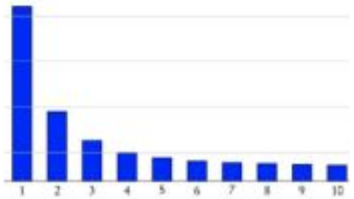
Contention?



Network?



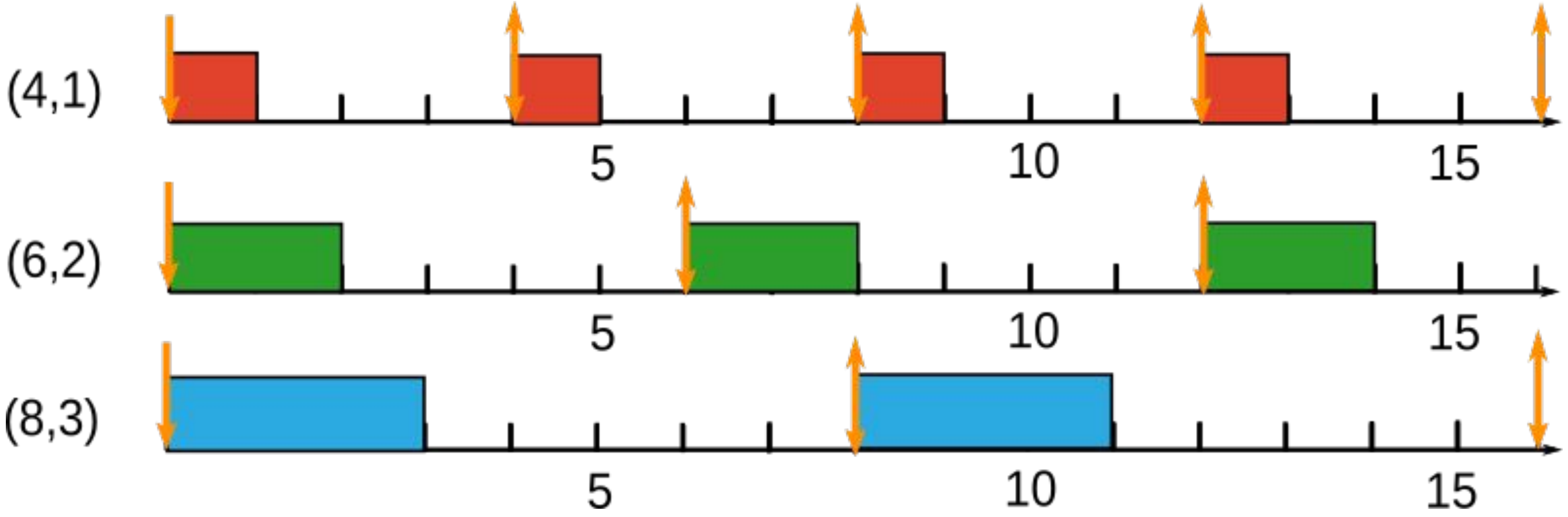
Bandwidth?



Data?

Timed

Security?



- Not everything is isolated…
- **Safety-Critical:**
  - What is safe?
  - Which algorithm?
  - How long does it take to decrypt?
  - Communication Protocol Steps
    - Key update?
    - Interruptions
    - etc.

Open Problems

- How to combine RT-Theory with novel requirements of data, security, dependency, etc…
  - Data-Centric Design

Period and Expiry

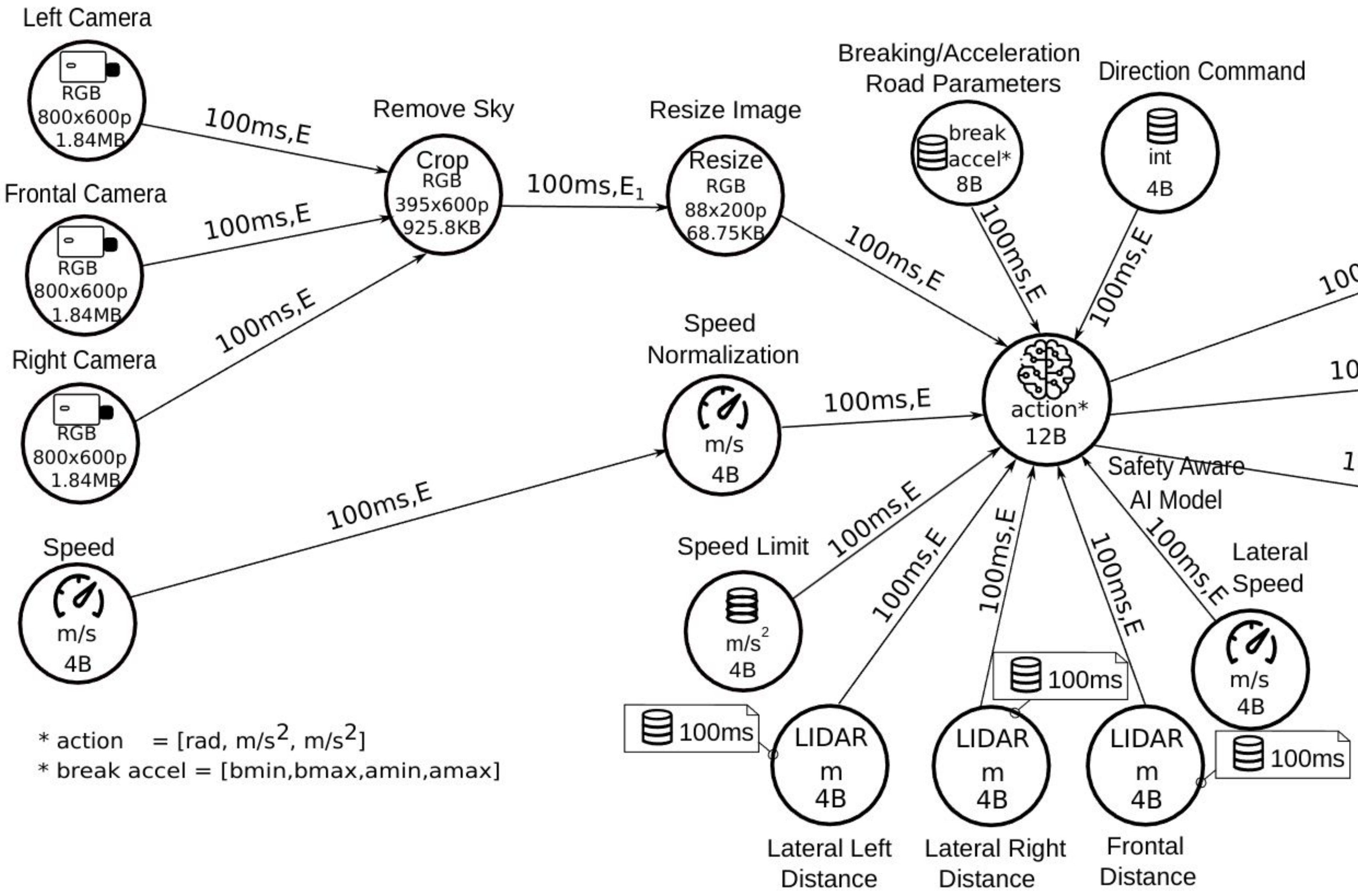
- **Period** = The period to which data must be sampled!
- **Expiry** = The last moment in time a data can be considered valid!

- A valid data shall always be available in the system:
  - Sampling = min(P,E)

- In Network
  - **Priority**: sending data closer to being expired
  - **Optimization**: Discard data that will not reach destination in time

- In computation element
  - S1 uses S2 and S3 to produce a new sample s1
  - P = The period a new data must be produced (s1)
  - E = The last moment in time an input can be considered valid
  - → E = min(s2.E, s3.E)
  - e.g., P = 100 and E = 100
    - Data can be computed any time during period
    - Expiry = Data produced at t = 10 → computation must be finished until 100 (Period)
    - New data produced at t = 90 → Next computation must be finished until 190 (Expiry)
  - Why 10 and 90? → communication delays, re-sampling due to error or low confidence data, etc.

Interest Relationship



Schedulability

- Estimated Costs
  - Data **bandwidth**: **Data Type** and How data is expected to be produced (period, expiry, how many samples per period, etc.)

  - **Account** for **security** in **latency**

  - **Schedulability:** Network model (1 sink vs. N sinks)**, Protocol,** bandwidth**,** topology**,** expiry**,** latency **and jitters, fault tolerance**
    - Huegel et al., 2020

procedure Analyze $(\mathcal{I}, \mathcal{N}, MOS, M_{rate}, t_{mac})$

$\mathcal{I}' \leftarrow \mathcal{I}$ ordered by $min(i.period, i.expiry)$ ascendant, where $i \in \mathcal{I}$

$\mathcal{N}' \leftarrow \mathcal{N}$ ordered by $hops(n, sink)$ descendent, where $n \in \mathcal{N}$

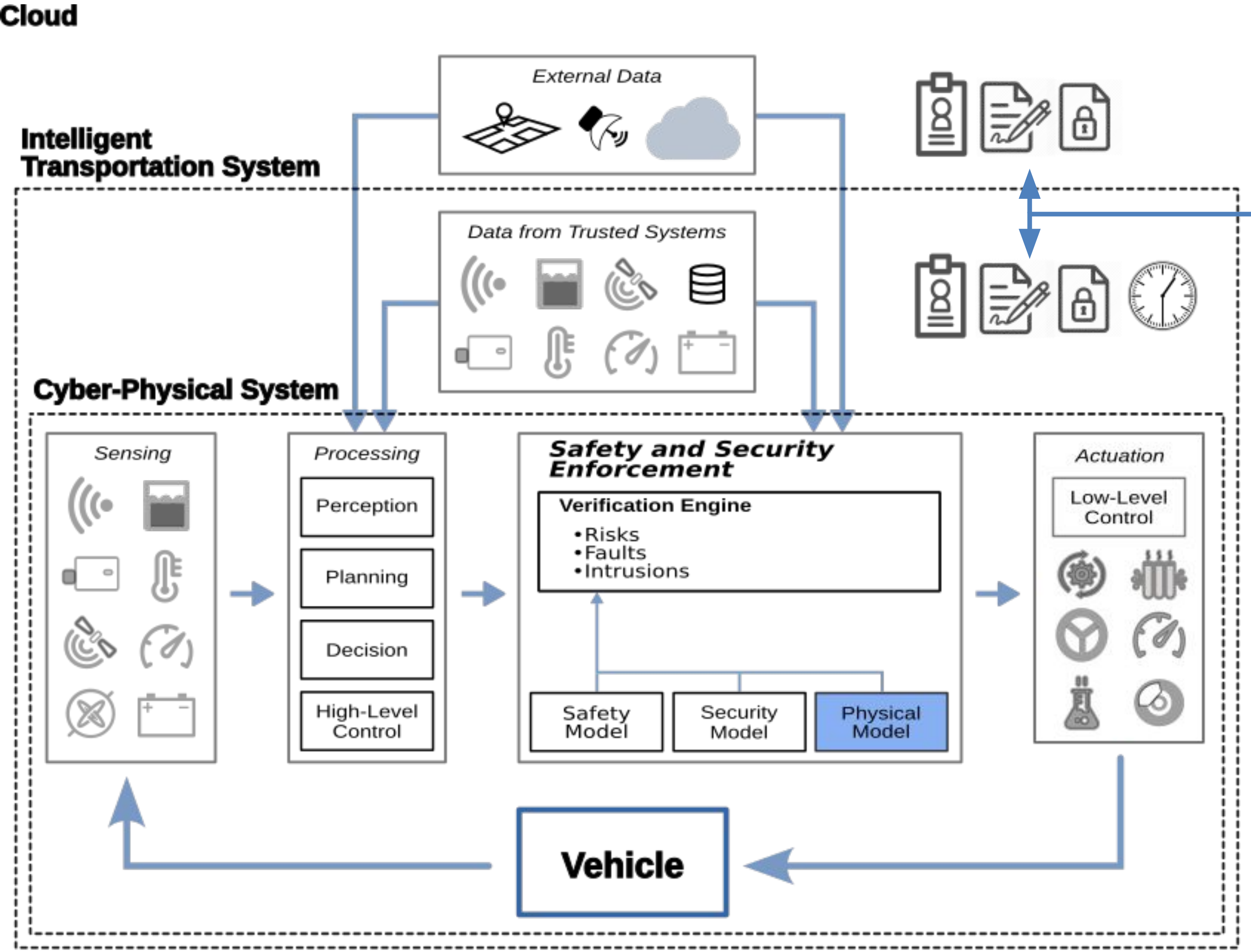
  - **Local Scheduling: Capacity of multiple resources, Expiry,** and **WCET** of updates
    - Local **Bandwidth and Memory** reservation: **Expiry**, **Period**, **latency**, **bandwidth**

  -

Open Problems

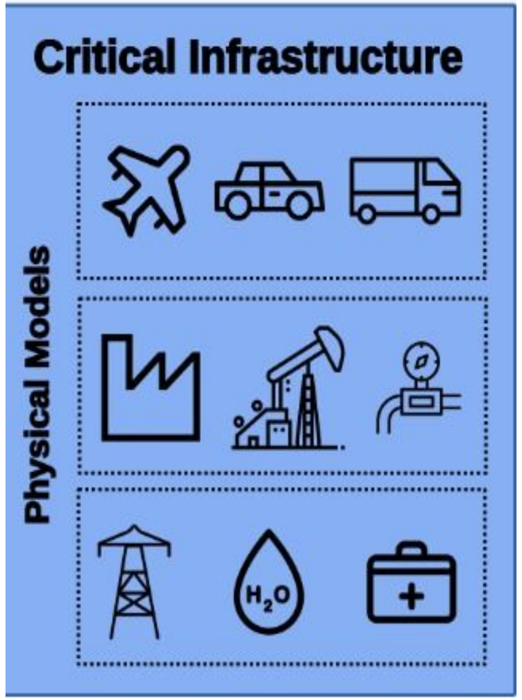
- How to combine RT Theory with novel requirements of data, safety, dependency, and timing
  - Data-Centric Design
- What about safety properties?
  - Formal methods automatically derived from the design

Data-Driven Cyber-Physical System Safety



Security Models

- Security Protocols
  - Confidentiality
  - Authentication
  - Integrity
  - Space/Time

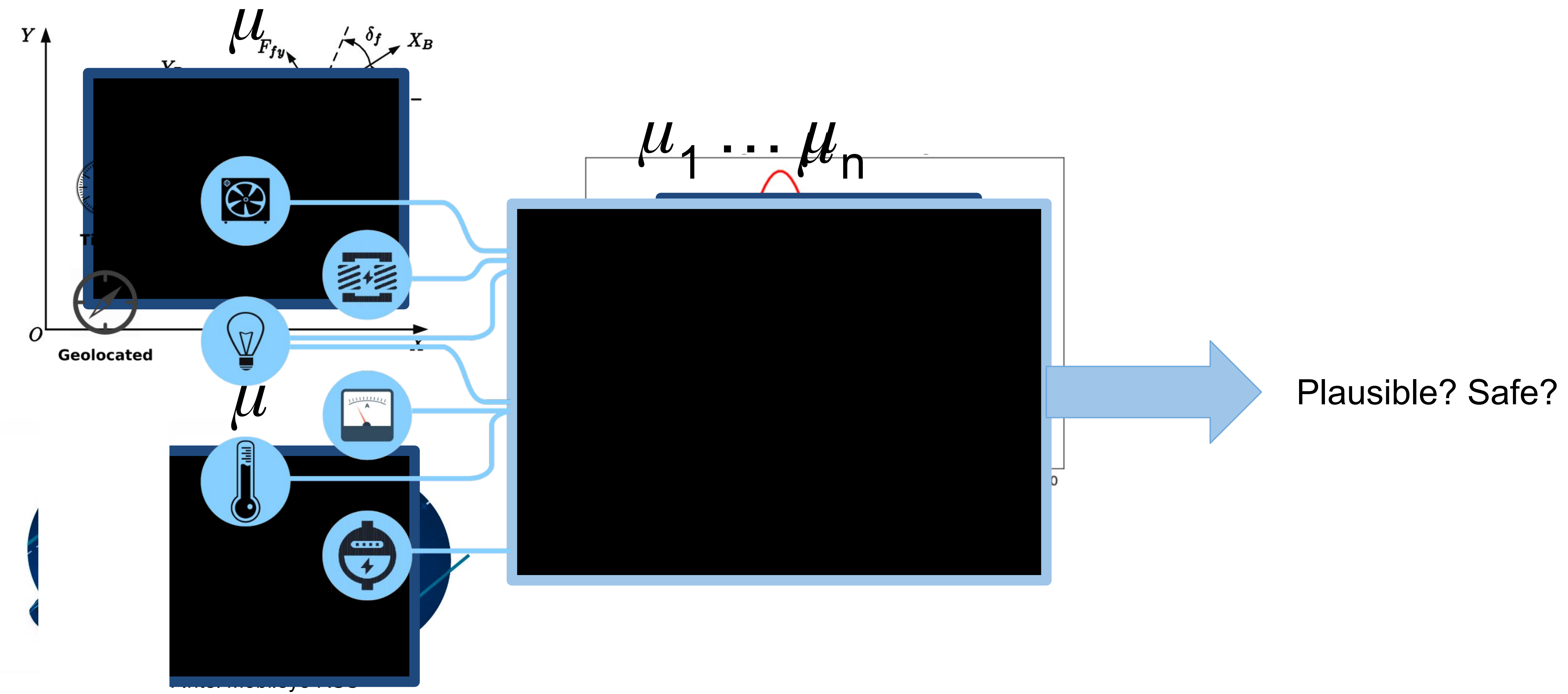


Safety Models

- Data Plausibility
  - Consensus
  - Filters
  - Continuity
- Safe Limits of Actuation
  - Physical Models + Safety
  - e.g., RSS/RSA
- Component Isolation, Replication, and Replacement
- Safe Mode
  - Protection Mechanisms
  - Actuation Override

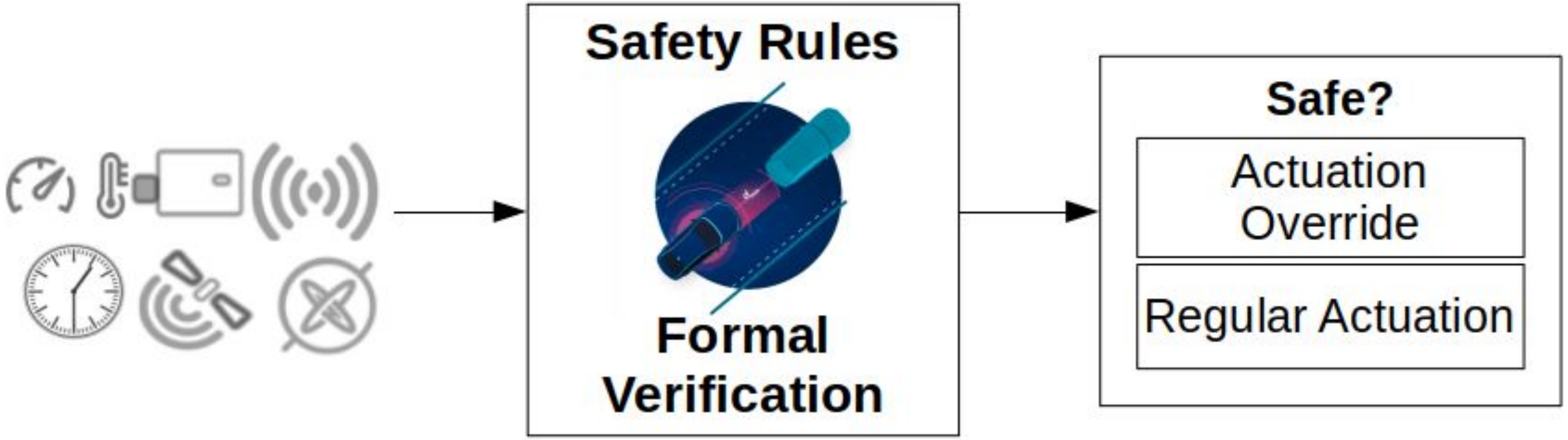
Figure based on original design by: Antônio Augusto Fröhlich

Plausibility Verification → Keep it Simple!



Run-Time Verification

- Formal Logic: Signal Temporal Logic



$$\varphi_{S_k} \models \bigwedge_{j=0}^{|S_k.I|} \left(\varphi_{S_j} U_{[0, i_{S_k, S_j}.e]} \mu(s_k)\right)$$

$$SEU.I = i(SEU, S_k)\ \forall S_k \in S.O \cup S.I \cup S.T.$$

$$\varphi_{SEU_j} \models \Diamond_{[0,P_j]} \varphi_{S_j}$$

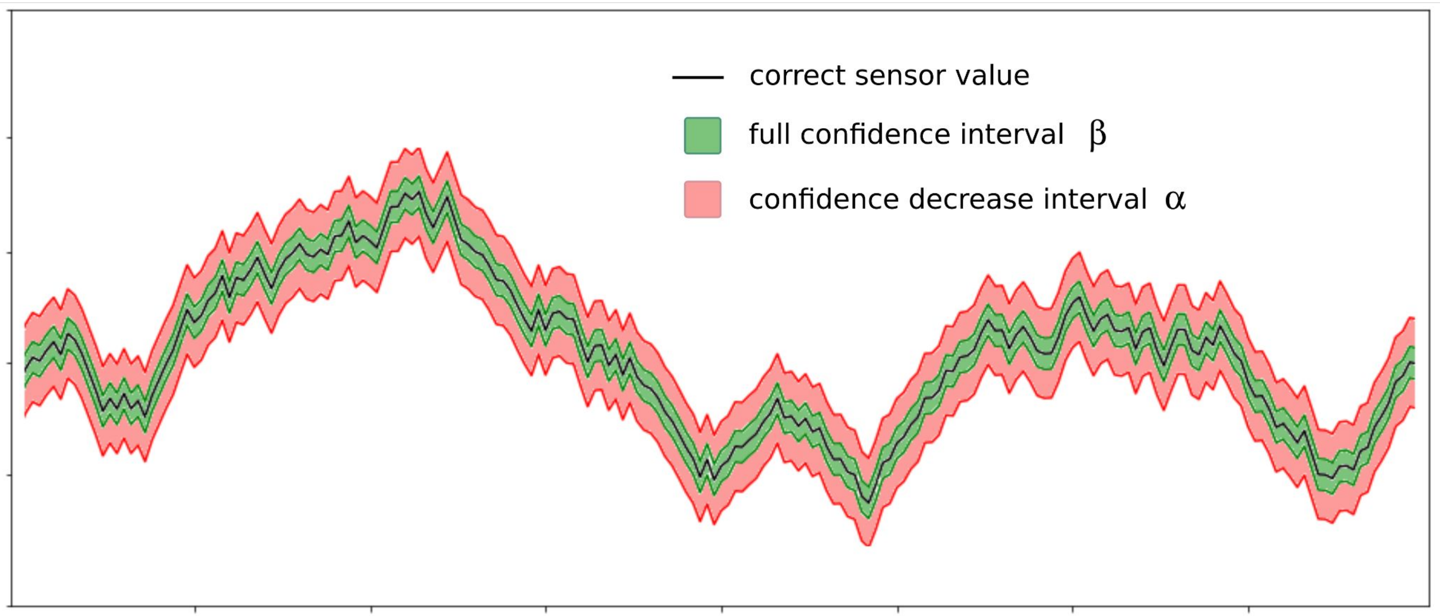
- Automatic code generation!
  - U for each interest and (eventually for each data and phase of security protocol)

Open Problems

- How to combine RT Theory with novel requirements of data, safety, dependency, and timing
- What about safety properties?
- Sensor Plausibility

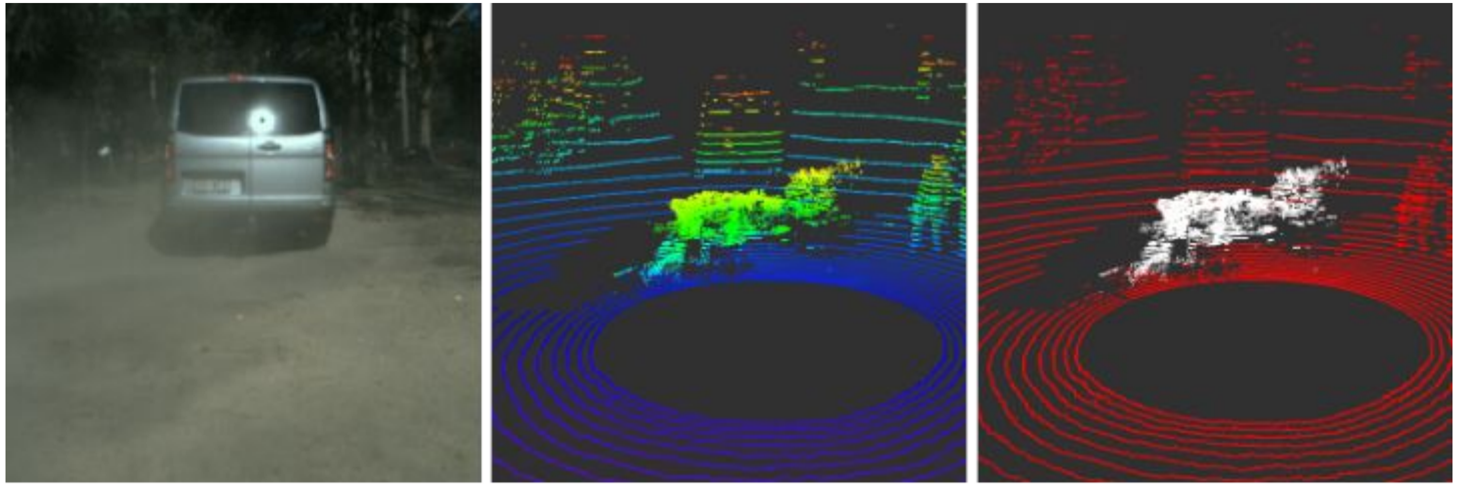
Open Problems

- How to combine RT Theory with novel requirements of data, security, dependency, etc…
- What about safety properties?
- Sensor Plausibility
  - Confidence (Scheffel et al., 2018)
    - Predict data: AI + Data Correlation OR based on a physical model (e.g., CTRV)
    - Compare to real reading and check difference according to threshold (data-driven value)



Open Problems

- How to combine RT Theory with novel requirements of data, security, dependency, etc…
- What about safety properties?
- Sensor Plausibility
  - Confidence (Scheffel et al., 2018)
    - Predict data: AI + Data Correlation OR based on a physical model (e.g., CTRV)
    - Compare to real reading and check difference according to threshold (data-driven value)
  - Specific Sensor approaches
    - Data Filtering, Kalman filters, Time-series (how much changed?)

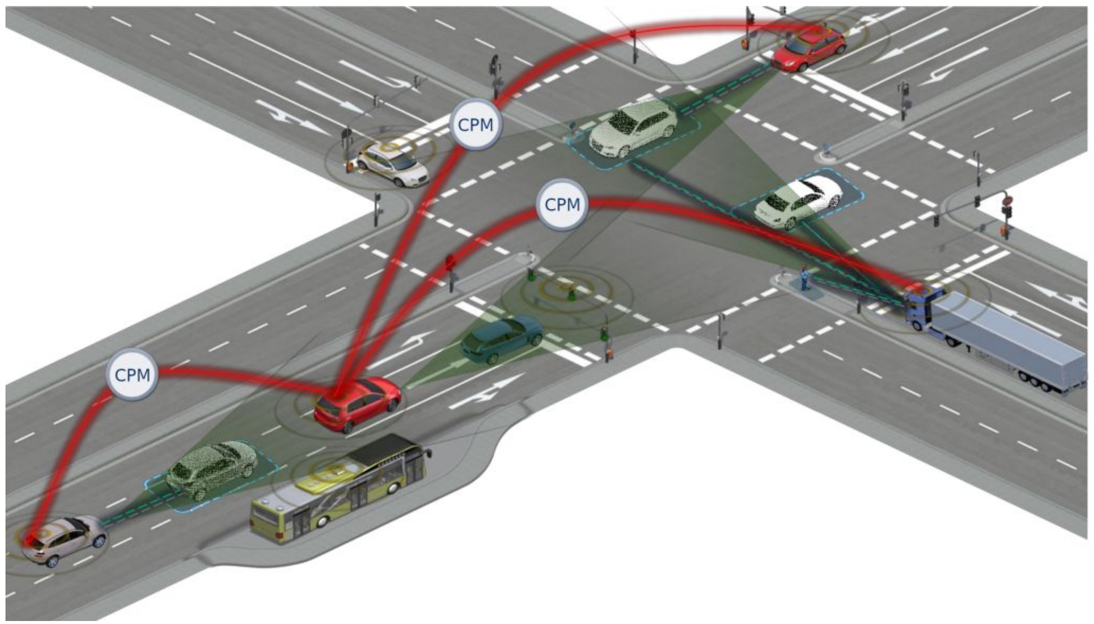


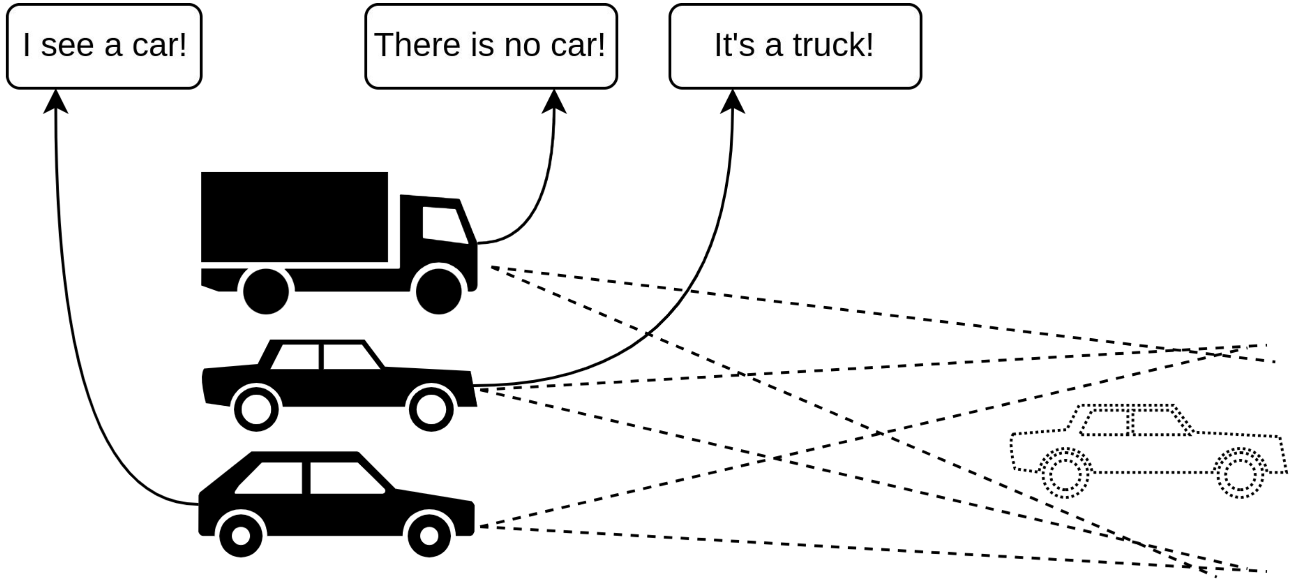
Source: Stanislas et al,. 2021

  - Trigger re-sampling
    - Do we still have time?

Open Problems

- How to combine RT Theory with novel requirements of data, security, dependency, etc…
- What about safety properties?
- Sensor Plausibility
  - Confidence (Scheffel et al., 2018)
  - Specific Sensor approaches
  - Cooperative perception (V2X)
    - ETSI standard





Open Problems

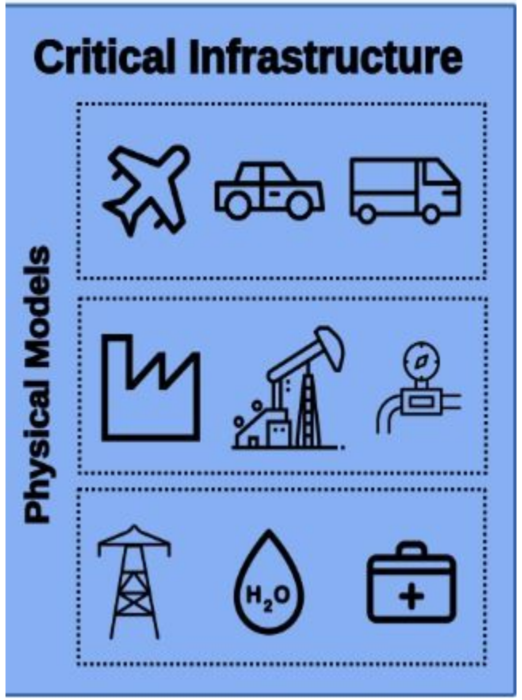
- How to combine RT Theory with novel requirements of data, security, dependency, etc…
- What about safety properties?
- Sensor Plausibility

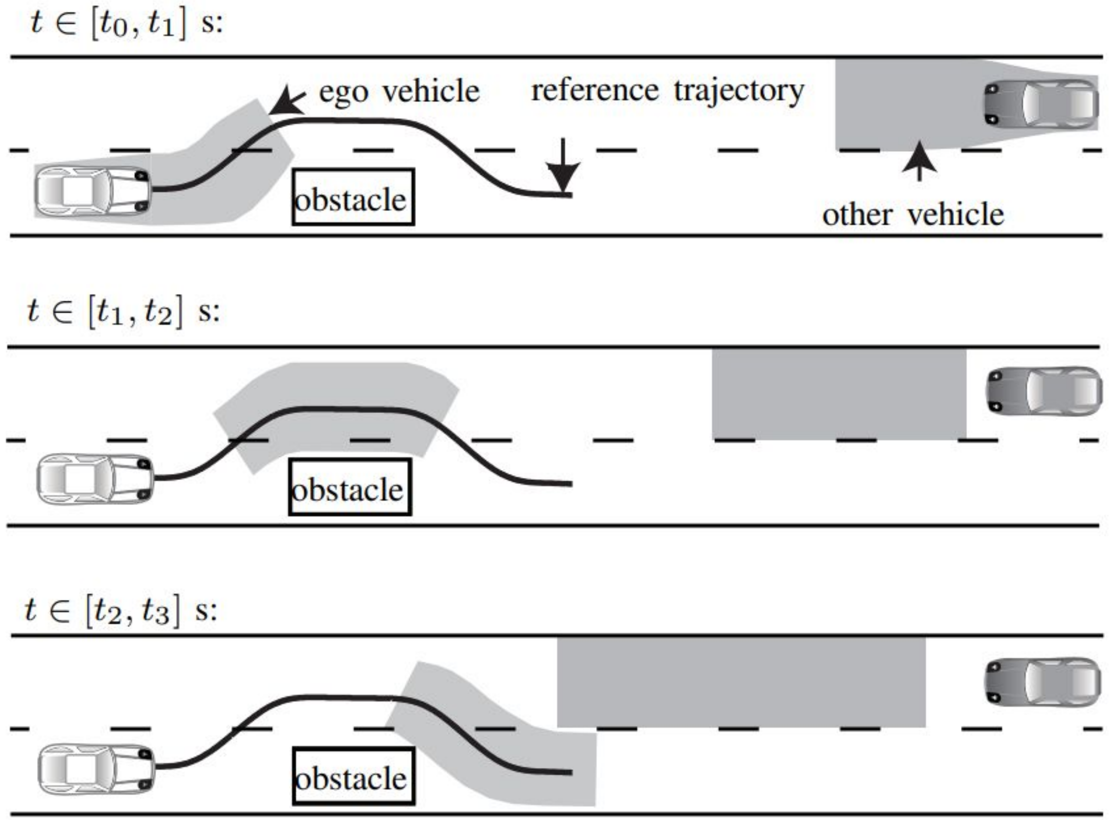
Open Problems

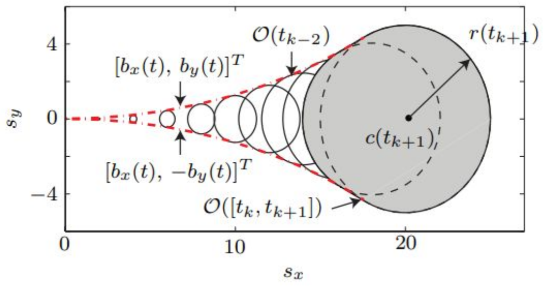
- How to combine RT Theory with novel requirements of data, security, dependency, etc…
- What about safety properties?
- Sensor Plausibility
- AI Plausibility

Open Problems

- How to combine RT Theory with novel requirements of data, security, dependency, etc…
- What about safety properties?
- Sensor Plausibility
- AI Plausibility
  - Cooperative perception (V2X)
  - Confidence?
    - AI to check AI?
  - Physical and Safety Models







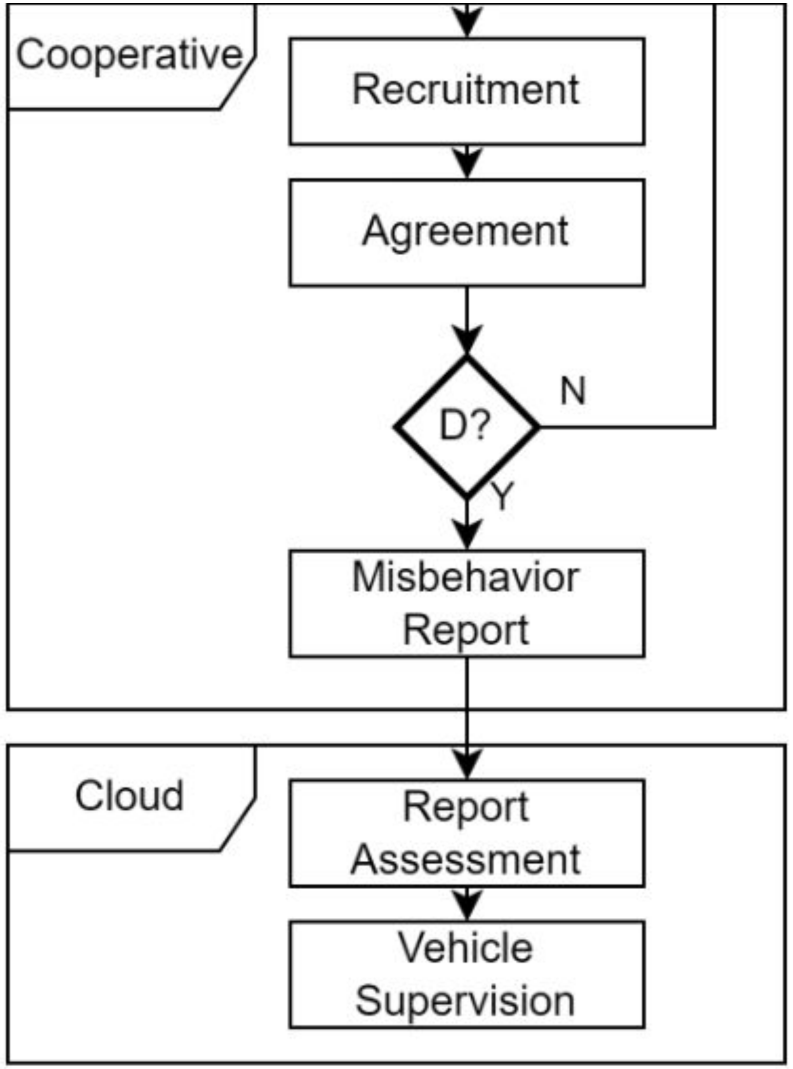
RSA by (Althoff et al. 2016)

Open Problems

- How to combine RT Theory with novel requirements of data, security, dependency, etc…
- What about safety properties?
- Sensor Plausibility
- AI Plausibility
- Security

Open Problems

- How to combine RT Theory with novel requirements of data, security, dependency, etc…
- What about safety properties?
- Sensor Plausibility
- AI Plausibility
- Security
  - Security Protocols
    - State Machine for Protocol
    - Based on Speed define:
      - Time to reach end of current group key → Re-negotiation of keys
  - Data consensus
    - Misbehavior detection
      - Spreading of false data in V2X
      - (Lucena and Fröhlich, 2022)



Timed Data: Are deadlines enough?

Pesaresi Seminars - 2023
University of Pisa

José Luis Conradi Hoffmann

Supervisors:
Prof. Antônio Augusto Fröhlich, PhD.
UFSC
Prof. Paolo Milazzo
UniPi

End-to-end timing analysis (Becker et al. 2017)

- Task dependency, Cause-effect chains, End-to-End timing, and Data Age Constraint
  - Data propagates through a chain of tasks within certain time bounds.
    - Time from reading the data until the actuation is subject to delay constraints in addition to the task's individual timing constraints

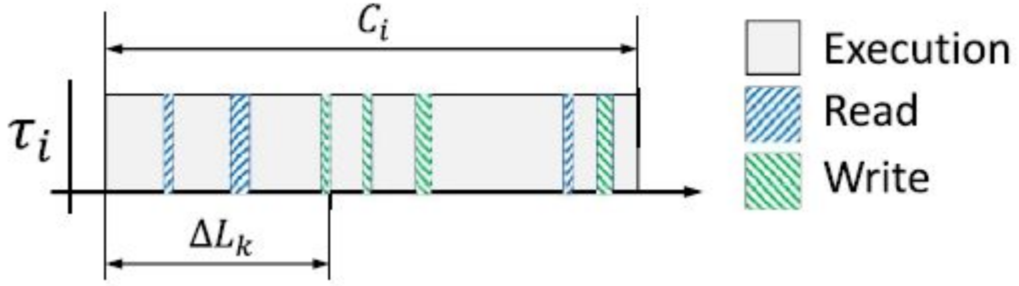
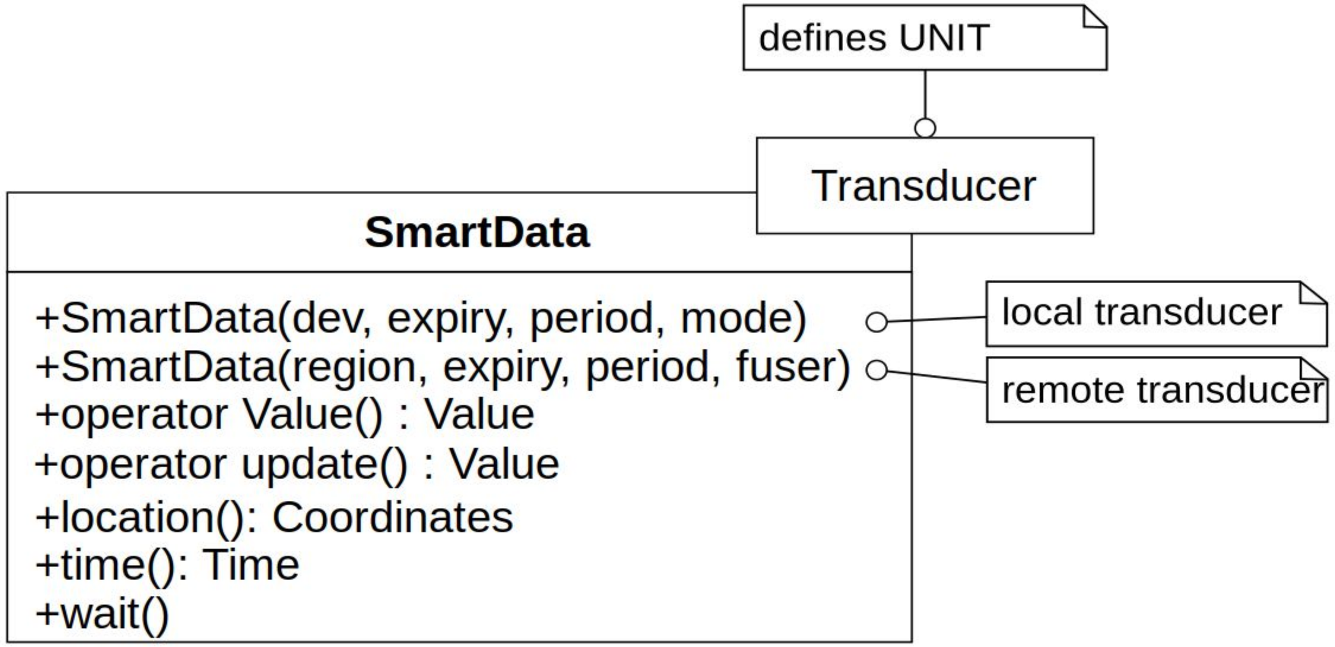


Fig. 8. Read and write operations in the explicit communication model.

Data-Driven Design with SmartData

- "SmartData is a piece of data enriched with enough metadata to make it self-contained regarding semantics, spatial location, timing, and trustfulness"
        - Antônio Augusto Fröhlich, *SmartData: an IoT-Ready API for Sensor Networks*, In: International Journal of Sensor Networks, 28(3):202-210, 2018, 10.1504/IJSNET.2018.096264.
    - Space-Time
        - Timing
        - Location
        - Mobile
    - Semantics
        - Local
        - Remote
        - SI Physical Quantity and Carefully tailored Digital Units



SmartData Interfaces