PHYSICAL OPTICS CORPORATION

Avionics Compositional System of Systems Simulation and Modeling Tool Chain ASSIST

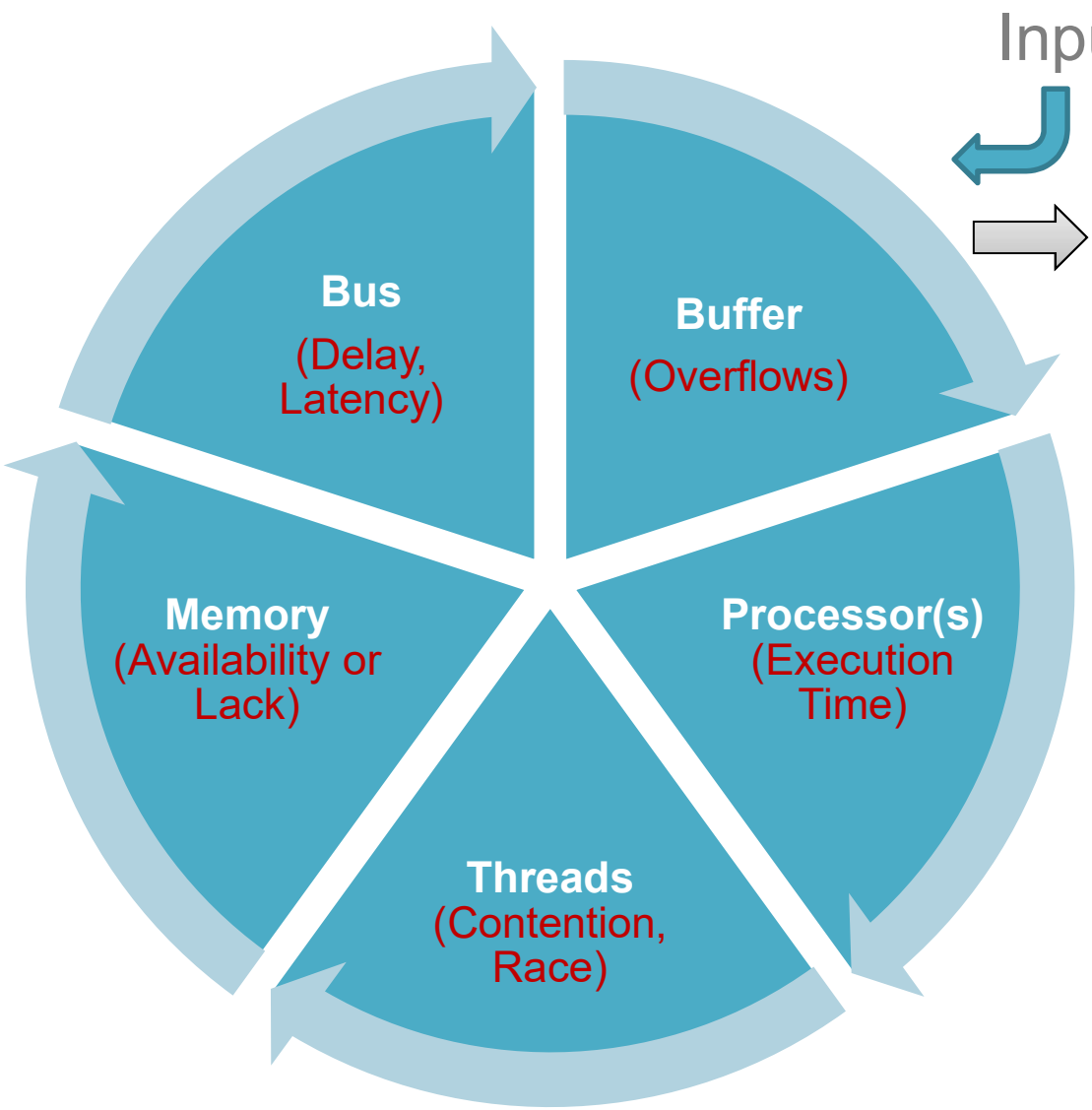
Contract # .: W911W6-18-C-0047

February 14, 2019
Tool Expo for Model Based Embedded Systems Development

Contact Information:
Prachee Sharma, Juan Gutierrez
Phone: 310-320-3088
Email: {psharma, jgutierrez}@poc.com

Physical Optics Corporation
1845 W. 205th Street, Torrance, CA 90501
http://www.poc.com

Focus: Embedded Systems with MultiCore CPUs



Input

Output

Mutual Dependencies make verification difficult

Verify if soft/hard real-time deadlines are met

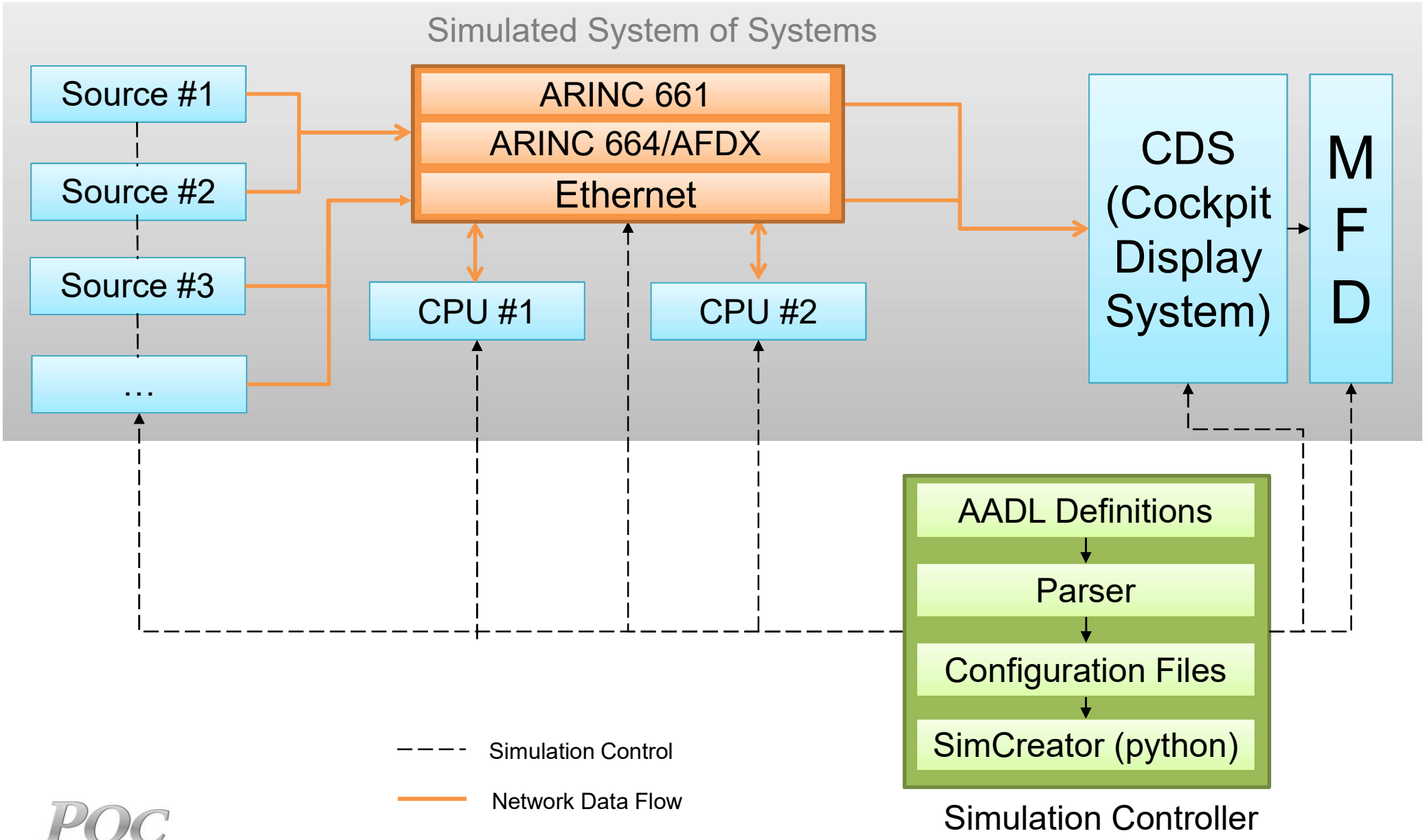
EXISTING TOOLS: WCET ANALYSIS IS INSUFFICIENT

- ***Using multi-core processors in avionics systems***
  - *Sharing of resources results in unpredictable performance*
- ***Inability to verify predictability of runtime behavior in multi-core environment***
  - *Nondeterminism of runtime behavior*
    - *Caused by dependency between shared resource availability and run-time behavior of other processes sharing the same resource.*
    - *Run-time behavior of programs is data dependent and cannot be predicted offline*
  - *Worst case execution time (WCET) analysis depends on understanding all conditions that lead to timing delays and bounds for worst-case conditions*
  - *Multiple shared resources on a single device complicate WCET analysis due to increase in number of delay conditions in multicore environment.*
    - *Interference between cache-fetching activities and I/O peripheral transactions and tasks can create computation time variances of up to 46% in a typical embedded system (https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/media/AR_11_2.pdf)*

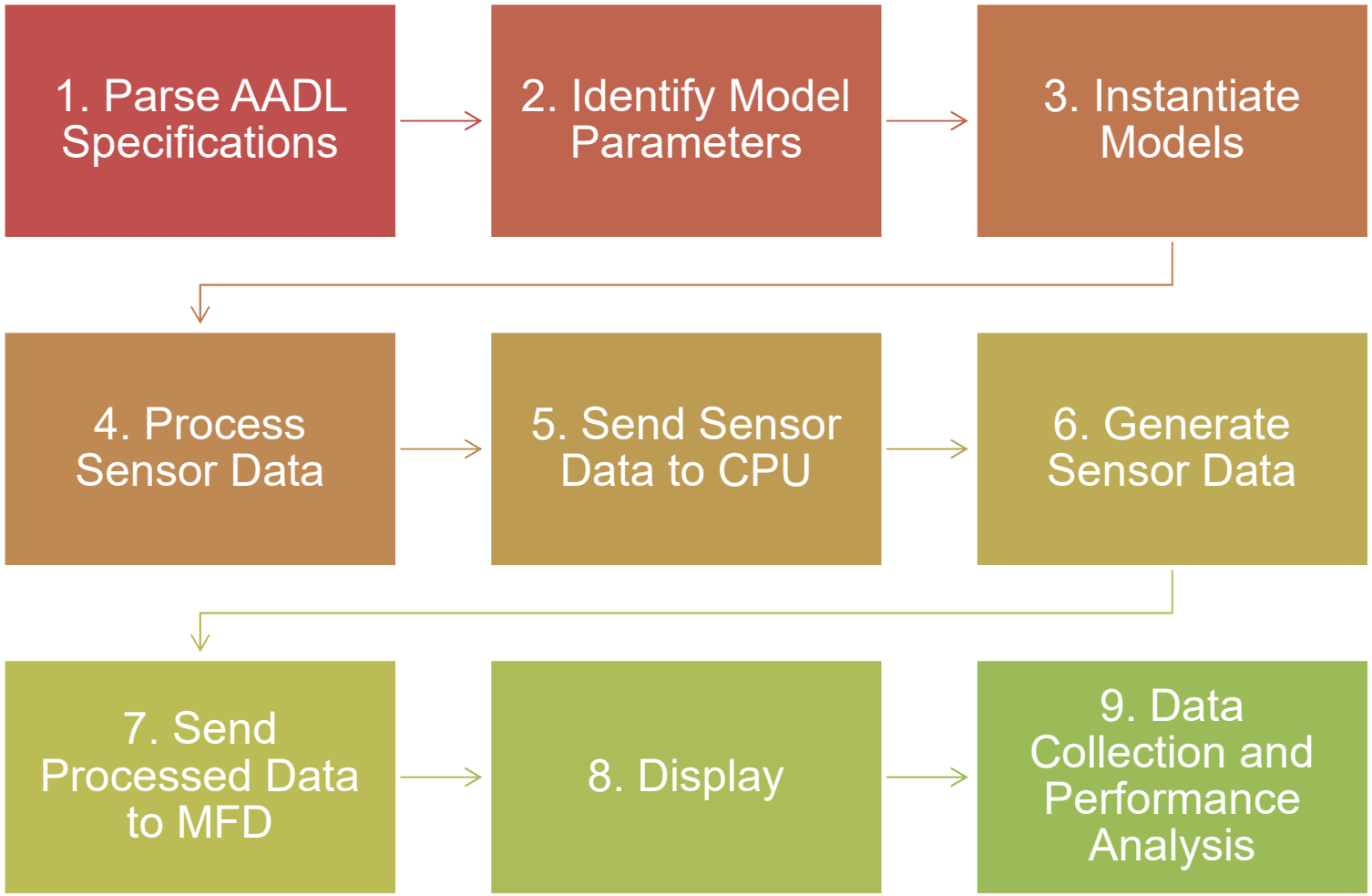
SOLUTION

- ***Avionics Compositional System of Systems Simulation and Modeling Tool Chain (ASSIST)***
- ***Analysis of hard real-time and soft real-time requirements***
  - *Aviation system of systems simulation using representative use case*
  - *Generating configuration for simulation*
  - *Verification of system against architecture model defined in AADL*
- ***Approach***
  - *Simulation of an SoS with multi-core processors*
  - *Input data: AADL specifications*
  - *Output*
    - *SoS model characterized by parameters from AADL specifications*
    - *Data analysis results*
      - *Positive matches between specifications and designed system features*
      - *Specification violations/contradictions in designed system and deficiencies*

ASSIST ARCHITECTURE



ASSIST SIMULATION STEPS



ASSIST MODELS

- ***Data Source Model***
  - *#s and types of sensors*
  - *Sensor data-rate or sampling rate*
  - *Buffers and queuing*
- ***Processor Model***
  - *# of processors*
    - *Threads, priorities, scheduling and pre-emption,*
  - *Shared resources – memory, bus, buffers, queues*
- ***Network model***
  - *Topology, buffers, queues, delays*
- ***Data Sink***
  - *Multi-function display*
  - *Subsystems*

RUNNING SIMULATION

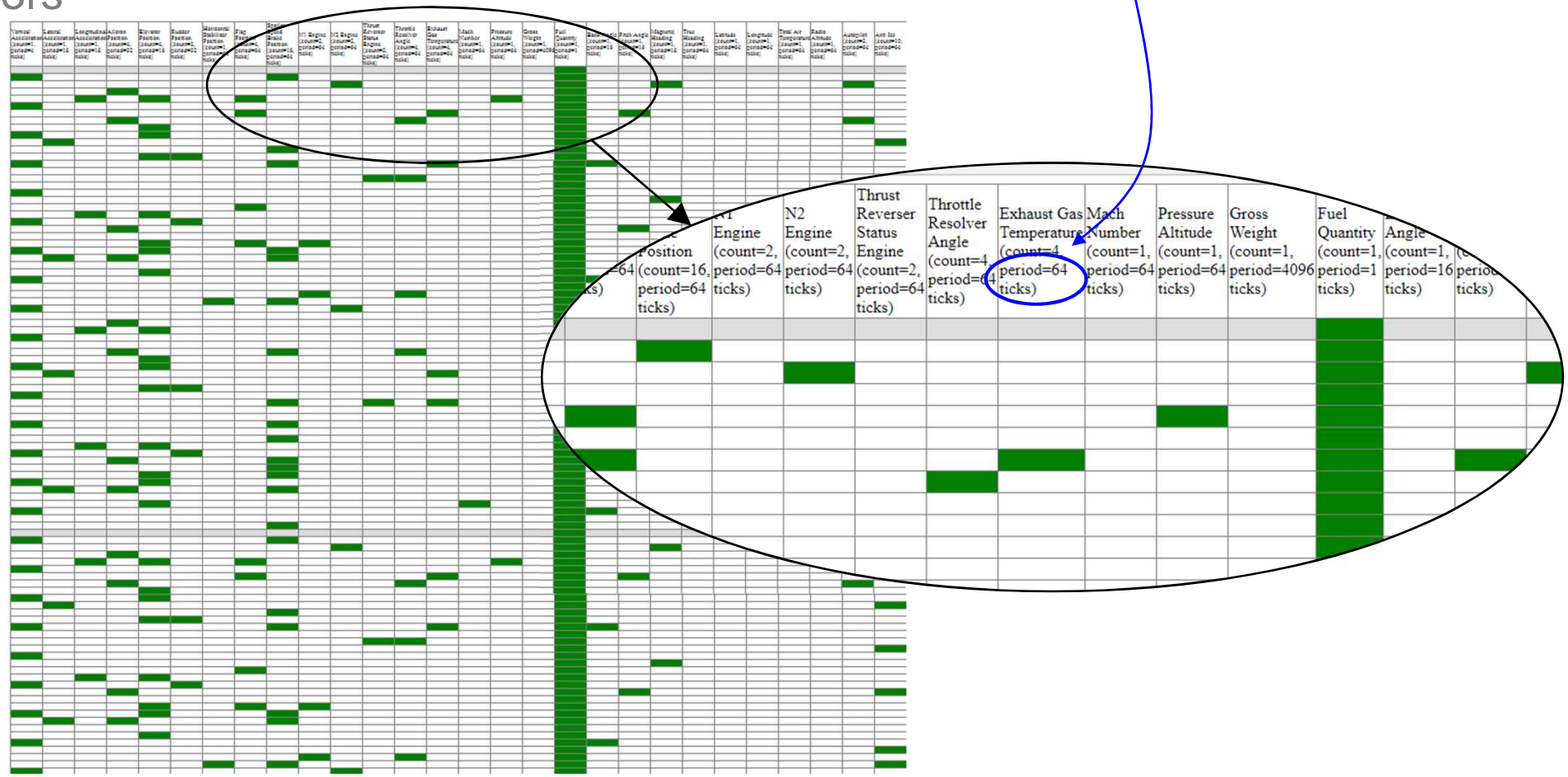
- ***Use AADL specifications***
  - *Obtain target specifications, components parameters to initialize simulation*
- ***Identify SoS components contributing to latency***
  - *Type/# of sensors/devices in the system are modeled*
  - *72 data sources included in the example system*
  - *Other components: Processors, bus, processor connection, message-size, ports*
- ***Flow specification***
  - *Source and sink of data for each device/sensor through network and CPU*
  - *Implementation of end-to-end flow*
    - *Periodic flow starting from source to sink*
    - *Processing: Periodic/data-driven, RMS and prioritization queues*
    - *Runtime latency: Randomization using modeled specifications*
- ***CPU model***
  - *Queues, Scheduling approach, priorities*
- ***Simulate Delays (random values) and Collect data***
  - *Sensor, network, CPU delays*
- ***Results: When latencies comply and violate specifications***

SOURCE MESSAGE GENERATION

Simulation Time in "Msg Ticks"
one tick = 1/64th second (i.e. 15.625 ms)

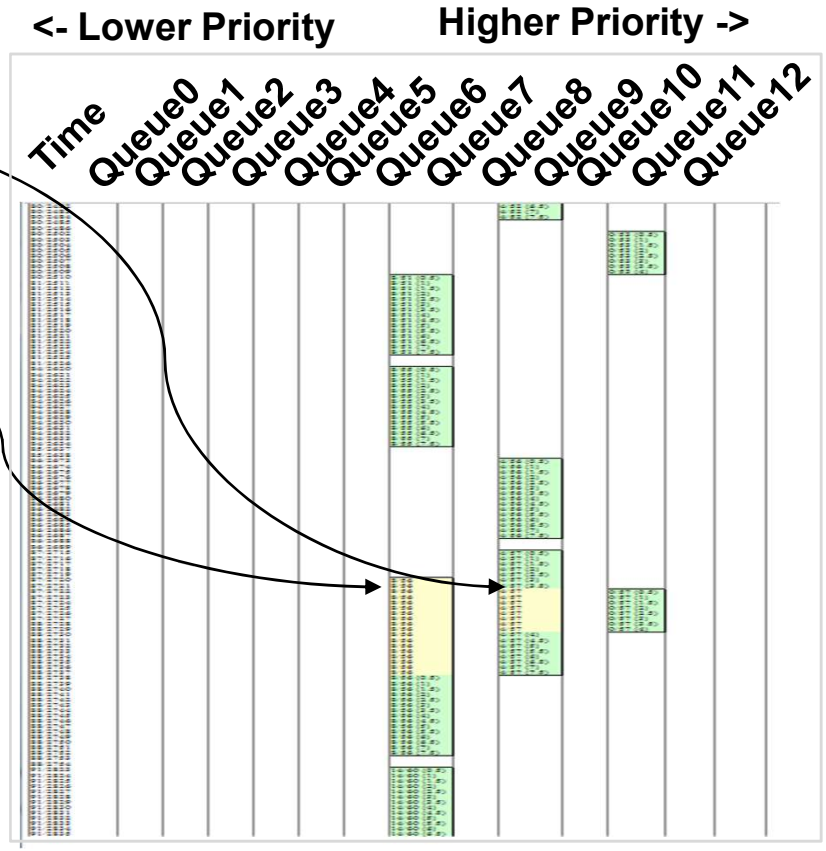
Sensors →

Time ↓



PROCESSOR RATE-MONOTONIC SCHEDULING DELAYS

- ***Scheduling delays***
  - *Interruption due to higher priority queue preemption*
  - *Delayed execution due to higher priority queue in-process*



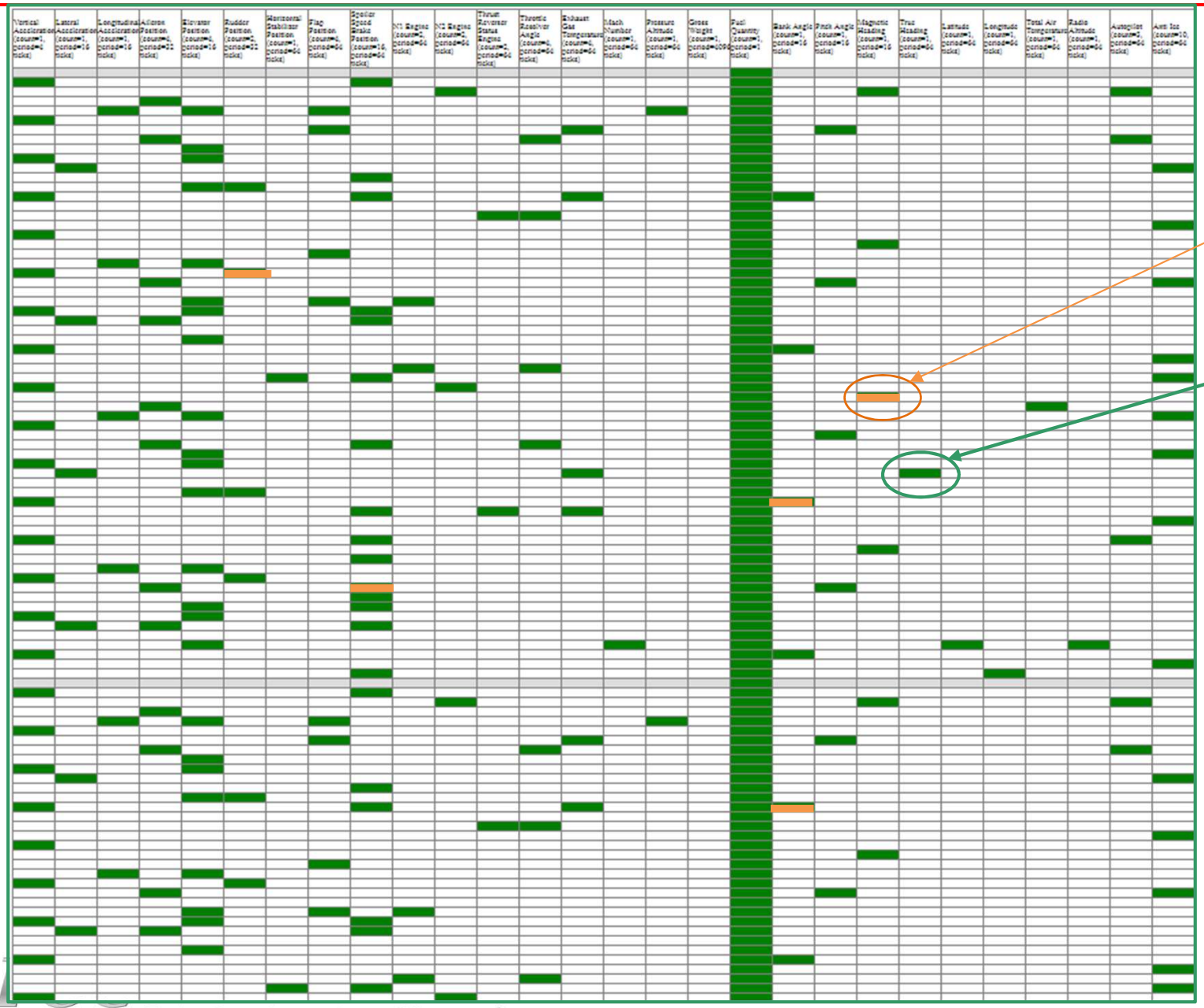
Sensor ID

Sensor Reading Creation Time (Msg Ticks)

CPU Time (ms)

Queue 8	Queue 9	Queue 10
4/25 (0.5)		
4/25 (1)		
4/25 (1.5)		
4/25 (2)		
4/25 (2.5)		
4/25		0/25 (0.5)
4/25		0/25 (1)
4/25		0/25 (1.5)
4/25		0/25 (2)
4/25		0/25 (2.5)
4/25		0/25 (3)
4/25		0/25 (3.5)
4/25		0/25 (4)
4/25 (3)		
4/25 (3.5)		

TOTAL LATENCY MEETING/EXCEEDING THRESHOLD



Latency Threshold is Violated

Latency Threshold is Met

ASSIST DEVELOPMENT PLAN

- ***Preliminary version available by the end of 2019 for evaluation***
- ***Extensions***
  - *Hardware in the loop*
  - *Software in the loop*
  - *Ability analyze various aircraft conditions*