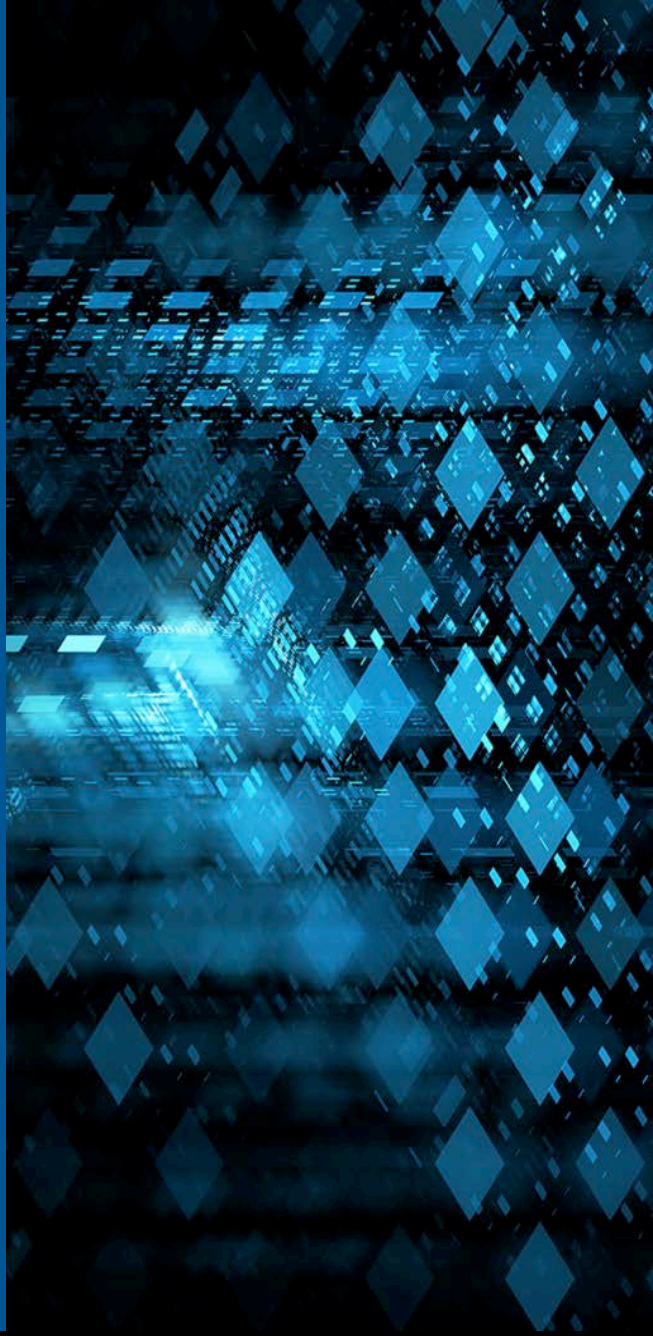
AADL for Secure & Safe Systems Design & Analysis

Part 3 - Latency

Julien Delange

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003990

Tutorial Agenda

Introduction: required background, role of MBE, tutorial overview

AADL Concepts: learn enough to use AADL and OSATE

Flow Latency: how to capture flow characteristics? How can I generate a flow analysis from my architecture model?

Safety Analysis: how to capture safety in an AADL model? What types of reports can I generate? How can I generate them?

Security Analysis: representation of security aspects. How to detect security issues? What type of reports can we generate?

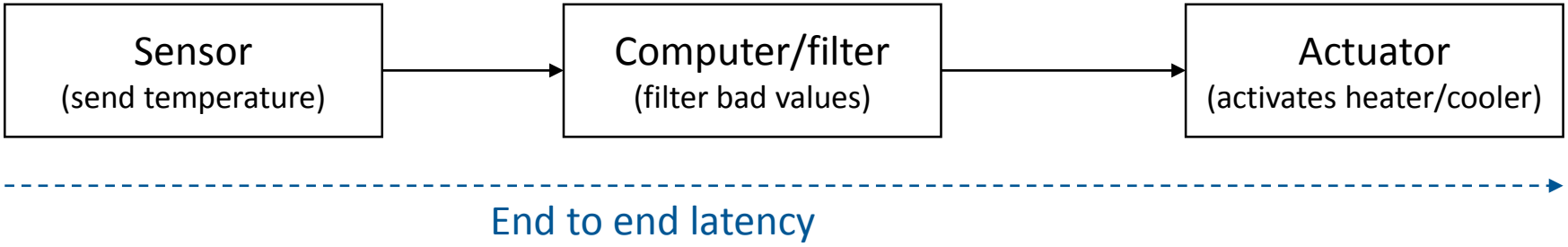
What is latency? Why it matters?

Total time from **data production** to **data consumption**

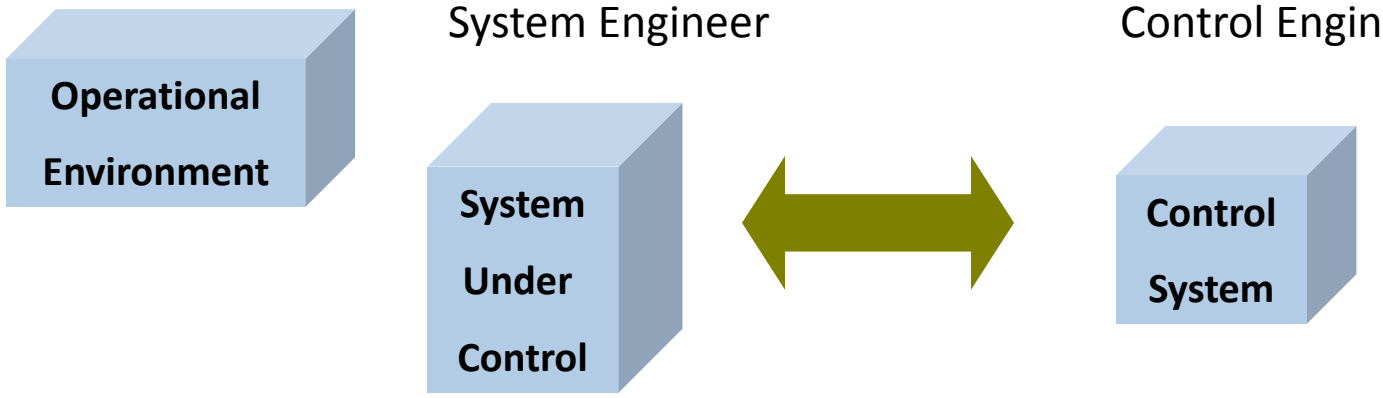
- Production on one end (e.g. sensor) …
- … "something in between" (e.g. processing/computing functions)
- … consumption on another end (e.g. actuator)

Depends on **many factors and dimensions**

- Execution time, processor speed
- Scheduling policy and parameters
- Communication protocols and physical constraints
- Shared resources, software or hardware

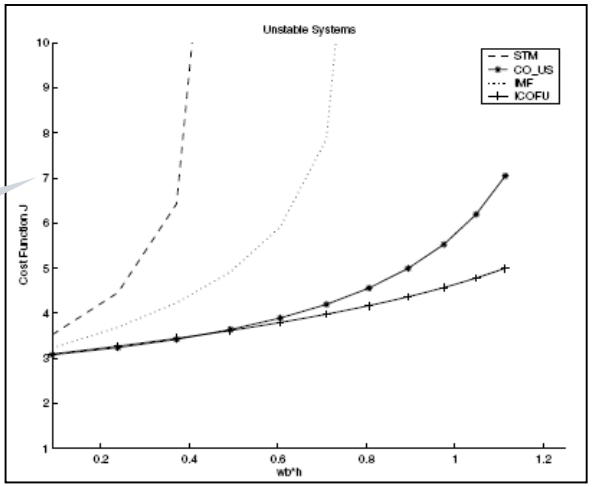


Latency Sensitivity in Control Systems



Common latency data from system engineering

- Processing latency
- Sampling latency
- Physical signal latency



Impact of Scheduler Choice on Controller Stability
A. Cervin, Lund U., CCACSD 2006

Software-Based Latency Contributors

Execution time variation: algorithm, use of cache

Processor speed

Resource contention

Preemption

Legacy & shared variable communication

Rate group optimization

Protocol specific communication delay

Partitioned architecture

Migration of functionality

Fault tolerance strategy

Latency modeling with AADL

Data flow: specify the end to end flow in components

- Flow source: where the data originates
- Flow path: where the data pass through components
- Flow sink: where the data is consumed

Flow contributors: aadl elements and properties

- Processor and bus bindings
- Communication/queueing policy
- Configuration and deployment properties

Detailed Latency Analysis Reports

Contributor	Min Specifiec	Min Value	Min Method	Max Speci	Max Value	Max Method	Comments
Partition cpu.part1		0.0ms	partition offset		0.0ms	partition offset	Initial 200.0ms partition latency not added
thread s1.ts		0.0ms	first sampling		0.0ms	first sampling	Initial 20.0ms sampling latency not added
thread s1.ts		1.0ms	processing time		2.0ms	processing time	
Partition cpu.part1		199.0ms	partition output (MF)		198.0ms	partition output (MF)	Output at 200.0ms major frame
Connection		0.0ms	no latency		0.0ms	no latency	
Partition cpu.part3		100.0ms	partition offset		100.0ms	partition offset	Synchronous communication on same platform
thread p.tf		0.0ms	sampling		0.0ms	sampling	**Task period smaller than partition period**
thread p.tf		2.0ms	processing time		3.0ms	processing time	
Partition cpu.part3		98.0ms	partition output (MF)		97.0ms	partition output (MF)	Output at 200.0ms major frame
Connection		0.0ms	no latency		0.0ms	no latency	
Partition cpu.part4		150.0ms	partition offset		150.0ms	partition offset	Synchronous communication on same platform
thread a.tc		0.0ms	sampling		0.0ms	sampling	**Task period smaller than partition period**
thread a.tc		1.0ms	processing time		3.0ms	processing time	
Immediate Connection		0.0ms	no latency		0.0ms	no latency	
thread a.td		0.0ms	no latency		0.0ms	no latency	
thread a.td		1.0ms	processing time		2.0ms	processing time	
Latency Total	0.0ms	552.0ms		0.0ms	555.0ms		
End to End Latency		20.0ms			30.0ms		
End to end Latency Summary							
ERROR	Minimum actual latency total 552.0 ms exceeds expected maximum end to end latency 30.0ms						
ERROR	Maximum actual latency 555.0ms exceeds expected end to end latency 30.0ms						

Introducing AADL flows

Specify data flow in the architecture

- Use on (`event`)? `data ports` features
- Hardware flows coming in AADLv3 (data/bus accesses)

Component type: specification on external interfaces

- Flow source (`out` feature), sink (`in` feature) or path (from `in` to `out`)
- One feature can be source/path or sink/path at the same time

Component implementation: refinement with component internals

- Flow realization with sub-components flow and connections

End to end flows in `system implementation`

- Realize the complete flow within the architecture from source to sink

```
flow source->connection->(flow path -> connection->)*flow sink
```

AADL flow example

```
device sensor
features
  valout : out data port temperature;
flows
  flowout: flow source valout;
end sensor;
```

```
device actuator
features
  valin: in data port temperature;
flows
  flowin: flow sink valin;
end actuator;
```

```
thread filter_thr
features
  valin  : in data port temperature;
  valout : out data port temperature;
flows
  flowpath: flow path valin -> valout;
end filter_thr;
```

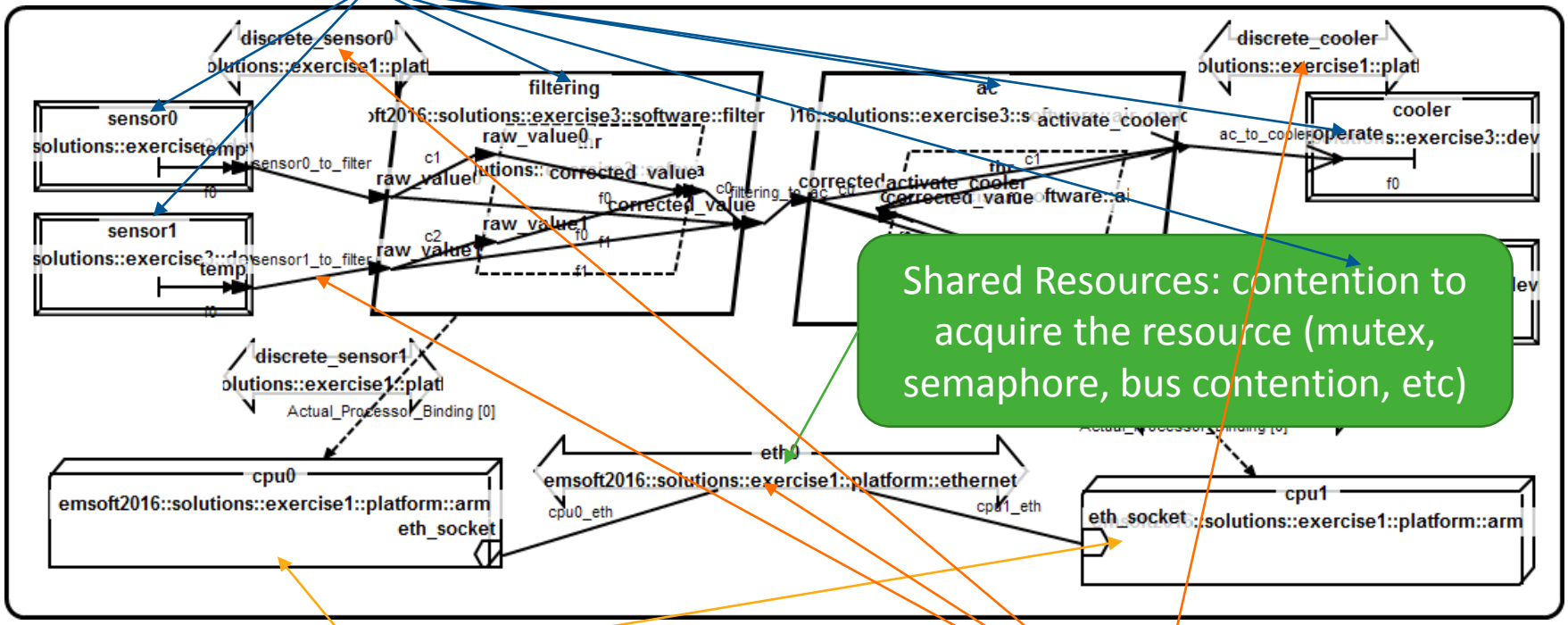
```
process filter_pr
features
  valin  : in data port temperature;
  valout : out data port temperature;
flows
  flowpath: flow path valin -> valout;
end filter_pr;
```

```
process implementation filter_pr.i
subcomponent
  thr : thread filter_thr;
connections
  c0 : port valin -> thr.valin;
  c1 : port thr.valout -> valout;
flows
  flowpath: flow path valin -> c0 ->
            thr.flowpath -> c1 -> valout;
end filter_pr.i;
```

```
system implementation root.i
subcomponents
 s : device sensor;
 p : process filter_pr.i;
 a : device actuator;
connections
 c0 : port s.valout -> p.valin;
 c1 : port p.valout -> a.valin;
flows
 etef1 : end to end flow s.flowout -> c0 -> p.flowpath -> c1 -> a.flowin;
end root.i;
```

Latency contributors

Execution rate, deadline, dispatch policy



Shared Resources: contention to acquire the resource (mutex, semaphore, bus contention, etc)

Scheduling policy (RMS, EDF, etc), use of time partitioning

Communication Protocol: TCP/IP, UDP, use of queueing/sampling

Latency contributors in AADL

Scheduling

- `Dispatch_Protocol` in thread and device
- `Period` and `Deadline` on thread and devices
- `Compute_Execution_Time`
- `Actual_Processor_Binding`
- Use of time partitioning

Communication Patterns

- Use of sampling (`data port`) vs. queuing port (`event port`)

Bus and Transport

- `Transmission_Time`
- `Data_Size` of data used on the logical connection

Latency plug-in internals

For each segment of a flow, gather **estimate** and **actual latency**

Best case vs. worst case

Estimate = latency property on each latency element

Actual = use AADL elements and contributors to compute the actual latency

End to end latency

Sums estimates and actual for each segment

Compare with estimate from end to end latency

Generate spreadsheet report with graphical warnings

Detailed Latency Analysis Reports

Contributor	Min Specifiec	Min Value	Min Method	Max Speci	Max Value	Max Method	Comments
Partition cpu.part1		0.0ms	partition offset		0.0ms	partition offset	Initial 200.0ms partition latency not added
thread s1.ts		0.0ms	first sampling		0.0ms	first sampling	Initial 20.0ms sampling latency not added
thread s1.ts		1.0ms	processing time		2.0ms	processing time	
Partition cpu.part1		199.0ms	partition output (MF)		198.0ms	partition output (MF)	Output at 200.0ms major frame
Connection		0.0ms	no latency		0.0ms	no latency	
Partition cpu.part3		100.0ms	partition offset		100.0ms	partition offset	Synchronous communication on same platform
thread p.tf		0.0ms	sampling		0.0ms	sampling	**Task period smaller than partition period**
thread p.tf		2.0ms	processing time		3.0ms	processing time	
Partition cpu.part3		98.0ms	partition output (MF)		97.0ms	partition output (MF)	Output at 200.0ms major frame
Connection		0.0ms	no latency		0.0ms	no latency	
Partition cpu.part4		150.0ms	partition offset		150.0ms	partition offset	Synchronous communication on same platform
thread a.tc		0.0ms	sampling		0.0ms	sampling	**Task period smaller than partition period**
thread a.tc		1.0ms	processing time		3.0ms	processing time	
Immediate Connection		0.0ms	no latency		0.0ms	no latency	
thread a.td		0.0ms	no latency		0.0ms	no latency	
thread a.td		1.0ms	processing time		2.0ms	processing time	
Latency Total	0.0ms	552.0ms		0.0ms	555.0ms		
End to End Latency		20.0ms			30.0ms		
End to end Latency Summary							
ERROR	Minimum actual latency total 552.0 ms exceeds expected maximum end to end latency 30.0ms						
ERROR	Maximum actual latency 555.0ms exceeds expected end to end latency 30.0ms						

Exercise 3 - Objectives

Declare flow in components

- open `device.aadl` and complete devices declaration
- open `software.aadl` and complete `thread` and `process` declarations

Declare end to end flow in the system implementation

- open `integration.aadl`
- declare **end to end flow** in the **functional implementation** that originates from devices (**sensors**) and terminates in actuators (**heater** or **cooler**)

Observe the impact of deployment on latency

- Generate latency report for `integration.local` and `integration.distributed`
- Compare the reports and the impact without changing the local and distributed declaration

Exercise 3 – Generating Latency Report

1. Right Click on the outline view on the system implementation and select “Instantiate System”

2. Right click on the generated system instance and select *AADL Analyses -> Check Flow Latency*

3. Open the Flow Latency report in your favorite productivity tool