Simulink, simulation, code generation and tasks

Marco Di Natale
Associate Professor, Scuola S. Anna - Italy, UTRC Visiting Fellow
Simulink model

Many things…

- A network of blocks
- Workspace variables
- Type declarations (bus objects)
- Matlab code (.m)
- Possibly external code
- Simulator configuration
- Code generation configuration
Simulink semantics and flow preservation

• The system is a network of functional blocks $b_j$
  Blocks can be:
  – regular (Dataflow) blocks or
  – Stateflow (state machine) blocks.

• Dataflow blocks can be of type continuous, discrete or triggered
• Discrete blocks are activated at periodic time instants and process input signals, sampled at periodic time instants producing a set of periodic output signals and the state updates.
Simulation flow

- Model is compiled before simulation
  - Rates are computed, values/types are propagated …
- Initialization stage at the beginning of the simulation
  - Init of simulation structure (entrate, uscite, stati ecc.)
  - Init matrices and variables
- Compute next simulation time for variable rate
- Compute outputs at next major time step
- Update discrete states at next major time step
- Integration of systems with continuous state
- Terminate and cleanup
Functional representation: SR Simulink modeling

- Simulink system = networks of blocks

\[ S = \{b_1, b_2, \ldots, b_n\} \]

- Blocks can be Regular or Stateflow blocks
- Regular blocks can be Continuous or Discrete type.
- All types operate on (right)continuous type signals.
- Blocks may have a state \( S_j \) or may be stateless.

\[ \begin{align*}
  &\overline{i}_j \\
  &i_{j,p}
\end{align*} \quad \begin{align*}
  &b_j \\
  &o_{j,p}
\end{align*} \quad \begin{align*}
  &\overline{o}_j
\end{align*} \]
Functional representation: SR Simulink modeling

- Continuous-type blocks are defined by a set of differential equations
- Discrete-type blocks are activated at events $e_j$ belonging to a periodic sequence with 0 offset and period $T_j$
- When a model generates code, continuous blocks must be implemented by a fixed-step solver, with period $T_b$
- $T_b$ (base period) must be a divisor of any other $T_j$ in the system
Functional representation: SR Simulink modeling

- At each $e_j$ the block computes its out update and state update functions, updating the values on its output signals $S_j^{\text{new}}, \overline{o}_j = f(S_j, \overline{i}_j)$.
Stateflow (or state machine) blocks react to a set of events $e_{j,v}$, derived from signals (generated at each rising or falling edge).

As such, events belong to a set of discrete time bases $kT_{jv}$.
If two blocks $b_i$ and $b_j$ are in an input-output relationship (one of the outputs of $b_i$ is the input of $b_j$), and $b_j$ is of type feedthrough), then

$$b_i \rightarrow b_j$$

In case $b_j$ is not of type feedthrough, then the link has a delay,

$$b_i \rightarrow^{1} b_j$$
Semantics options

- Signals are persistent (Simulink)

- Signals are not persistent

- Algebraic loops (causal loops without delays) result in a fixed point and lack of compositionality
Semantics and Compositionality

- Semantics problem: systems compositions do not behave according to the semantics of the components
  - The problem is typical of SR semantics when there are causal cycles: existence of a fixed point solution cannot be guaranteed (i.e. the system may be ill-defined)
  - When multirate blocks are in a causal loop the composition is always not feasible

![Diagram showing algebraic and absence of causality loops](image_url)
Simulink models (execution order - feedthrough)

May be a problem in a code implementation with (scheduling) delays
Simulink models (execution order - feedthrough)

Let $b_i(k)$ represent the $k$-th occurrence of $bi$ (belonging to the set $\bigcup_v kT_{i,v}$ if a state machine block, or $kT_i$ if a standard block), a sequence of activation times $a_i(k)$ is associated to $b_i$.

$n_i(t)$ is the number of times $b_i$ is activated before or at $t$.

In case $bi \rightarrow bj$, if $i_j(k)$ is the input of the $k$-th occurrence of $b_j$, then this input is equal to the output of the last occurrence of $b_i$ that is no later than the $k$-th occurrence of $b_j$:

$$i_j(k) = o_i(m); \text{ where } m = n_i(a_j(k))$$

If the link has a delay, then the previous output value is read, $i_j(k) = o_i(m - 1)$:
From model to code

• The code generation framework follows the general rule set of the simulation engine and must produce an implementation with the same behavior (preserving the semantics).
• Goal 1: preservation of the synchronous assumption:
  • The reaction (the outputs and the next state) of the system must be computed before the next event in the system.
• Goal 2: (looser property, equivalent to untimed simulation), called flow preservation.
• The execution of the system must guarantee
  • $i_j(k) = o_i(m)$; where $m = n_j(a_j(k))$  (1)
Most blocks are of type feedthrough (output does depend on input)

This implies a precedence constraint in the computation of the block output functions
Simulink models (SR)
Simulink models (not feedthrough)

Integrator (output does not depend on input but only on state)
Example of generated code

```c
/* Model step function */
void Subsystem_step(void)
{
    /* Output: '<Root>/Out1' incorporates:
    *  DiscreteIntegrator: '<S1>/Discrete-Time integrator'
    */
    Subsystem_Y.Out1 = Subsystem_DWork.DiscreteTimeIntegrator_DSTATE;

    /* Update for DiscreteIntegrator: '<S1>/Discrete-Time integrator' */
    Subsystem_DWork.DiscreteTimeIntegrator_DSTATE =
        Subsystem_P.DiscreteTimeIntegrator_gain * Subsystem_U.In1 +
        Subsystem_DWork.DiscreteTimeIntegrator_DSTATE;
}
```
Simulink models (feedthrough)

Most blocks are of type feedthrough (output does depend on input)

This implies a precedence constraint in the computation of the block output functions

Some blocks have no state

Dependencies among outputs
Simulation of models

- Simulation of Multirate models
  - order all blocks based upon their topological dependencies
  - The RTW tool (meant for a single processor implementation) generates a total order based on the partial order imposed by the feedthrough semantics
  - *In reality, there are many such total orders that satisfy the dependencies!*
    - *Other choices are possible*
    - *In multiprocessor implementations this can be leveraged to optimize the implementation*
  - Then, for simulation, virtual time is initialized at zero
  - The simulator scans the precedence list in order and execute all the blocks for which the value of the virtual time is an integer multiple of the period of their inputs
  - Simulated execution means computing the block output and then computing the new state
From Models to implementation

- Simulink case

**Purpose**
List simulation methods in the order in which they are executed during a simulation.

**Syntax**
- `elist m:mid [tid:TID]`
- `elist <gcs | s:sid> [mth] [tid:TID]`
- `elist <gcb | sid:bid> [mth] [tid:TID]`

**Description**
elist `m:mid` lists the methods invoked by the system or nonvirtual subsystem method corresponding to the method id `mid` (see the `where` command for information on method IDs), e.g.,

```
sldebug @19): elist n:19
```

```
RootSystem.Outputs 'vdp' [tid=0] :
 0:0 Integrator.Outputs 'x1' [tid=0]
 0:1 Outport.Outputs 'Out1' [tid=0]
 0:2 Integrator.Outputs 'x2' [tid=0]
...
```

- Block id
- Method
- Block
- Task id
From Simulink models to update functions
The result is a network of functions (output/state update) with a set of partial orders.

Each blockset is characterized by an execution rate.
Task implementations (of multirate systems)

- In multitask implementations, the run-time execution of the model is performed by running the code in the context of a set of threads under the control of a priority-based real-time operating system (RTOS).
- The function-to-task mapping consists of a relation between a block update function (or a set of them in the case of an Stateflow block) and a task, and a static scheduling (execution order) of the function code inside the task.
- The $i$-th task is denoted as $\tau_i$.
- $M(f_j, k, i)$ indicates that the step (update) function $f_j$ of block $b_j$ is executed as the $k$-th segment of code in the context of $i$.
- Legal task mappings must guarantee the block execution constraints
Flow preservation

• The implementation of a SR model should preserve its semantics so to retain the validation and verification results.

Simulation: zero logical execution time and zero logical communication time
From Models to implementation

- Simulink case (single task implementation)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Single-Rate</th>
<th>Multi-Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>SingleTasking</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>MultiTasking</td>
<td>Disallowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Auto</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td></td>
<td>(defaults to</td>
<td>(defaults to</td>
</tr>
<tr>
<td></td>
<td>SingleTasking)</td>
<td>MultiTasking)</td>
</tr>
</tbody>
</table>
From Models to implementation

- Simulink case (single task implementation)
• Implementation runs in real-time (code implementing the blocks behavior has finite execution time)
• Generation of code: Singletask implementation
From Models to implementation

- Simulink case (single task implementation)

```c
rt_OneStep()
{
  Check for interrupt overflow or other error
  Enable "rt_OneStep" (timer) interrupt
  ModelStep-- Time step combines output, logging, update
}
```

Single-rate `rt_OneStep` is designed to execute `model_step` within a single clock period. To enforce this timing constraint, `rt_OneStep` maintains and checks a timer overrun flag.
The implementation can use:
- Single task executing at the base rate of the system
- A set of concurrent tasks, with typically one task for each execution rate, and possibly more.

**System base cycle** = 
*Time to execute the longest system reaction*
From Models to implementation

- Multitask implementation

```c
rt_OneStep()
{
    Check for base-rate interrupt overflow
    Enable "rt_OneStep" interrupt
    Determine which rates need to run this time step
    ModelStep(tid=0) --base-rate time step
    For i=1:NumTasks -- iterate over sub-rate tasks
        Check for sub-rate interrupt overflow
        If (sub-rate task i is scheduled)
            ModelStep(tid=i) --sub-rate time step
        EndIf
    EndFor
}
```
Generation of code: multitask mode

- The RTW code generator assigns each block a task identifier (tid) based on its sample rate.
- The blocks with the fastest sample rates are executed by the task with the highest priority, the next slowest blocks are executed by a task with the next lower priority, and so on (Rate Monotonic)
Nondeterminism in time and value

- However, this can lead to the violation of the zero-execution time semantics of the model (without delays) and even to inconsistent state of the communication buffer in the case of
  - low rate (priority) blocks driving high rate (priority) blocks.
  - high rate (priority) blocks driving low rate (priority) blocks.
Model implementation: multi-task

Real-time execution: finite execution time and possible preemption

Inconsistent data

\[ f(4,1)? \]
Model implementation: multi-task

Real-time execution: lack of time determinism (because of preemption)

Behavior different from simulation
Adding determinism: RT blocks

• Solution: Rate Transition blocks
  – added buffer space and added latency/delay
  – relax the scheduling problem by allowing to drop the feedthrough precedence constraint

• The mechanism can only be implemented if the rates of the blocks are harmonic (one multiple of the other)
  – Otherwise, it is possible to make a transition to the gcd of the blocks’ periods, at the price of additional space and delay

• RT Blocks are only for intracore communication
RT blocks: High rate/priority to low rate/priority

**COST**

- space: (possibly) 1 additional set of variables for each link
- time: overhead of RT implement.
- performance: none

Diagram:

- **High rate/priority**
  - pri=1
  - T=1
- **Protected RT**
- **Low rate/priority**
  - pri=2
  - T=2

Consistency here is guaranteed by proving there is no preemption.

Output update only
RT blocks: Low rate/priority to high rate/priority

COST
space: 2 additional set of variables for each link
time: overhead of RT implement.
performance: 1-unit delay (low rate period)

Output update

State update

Consistency here is guaranteed by proving there is no preemption
Limitations in the use of RT blocks (1)
Tradeoffs and design cycles

- RT blocks are **not** a functional entity
  - *but an implementation device*
- RT Blocks are only required
  - because of the selection of the RM scheduling policy
    *in slow to fast transitions*
  - because of the possibility of preemption
    *in both cases*
- In both cases, time determinism (of communication) is obtained at the price of additional memory
- In the case of slow to fast transitions, the RT block also adds a delay equal to the period of the slowest block
  - This is only because of the Rate monotonic scheduling
  - Added delays decrease the performance of controls
RT blocks: Low rate/priority to high rate/priority

- Low rate/low priority
- High rate/high priority

Or... letting the sender have a priority higher than the receiver

Against RM and more difficult to schedule
• **Consistency issues in the 1-1 communication between blocks with different rates may happen:**
  – When blocks are executed in concurrent tasks (activated at different rates or by asynchronous events)
  – When a reader may preempt a writer while updating the communication variables (reader with higher priority than writer)
  – When the writer can preempt the reader while it is reading the communication variables (writer with higher priority).
  – *Necessary condition for data inconsistency is the possibility of preemption reader → writer or writer → reader*
• Also, we may want to enforce time determinism (flow preservation)
Consistency issues

- Also, a relaxed form of time determinism may be required
  - Input coherency: when inputs are coming from multiple blocks, we want to read inputs produced by instances activated by the same event.
Guaranteeing data consistency

- Demonstrate impossibility of preemption between readers and writers
  - Appropriate scheduling of blocks into tasks, priority assignment, activation offsets and using worst-case response time analysis
- Avoid preemption between readers and writers
  - Disabling preemption among tasks (blocks) (RES_SCHEDULER in OSEK)
- Allow preemption and protect communication variables
  - Protect all the critical sections by
    - Disabling interrupts
    - Using (immediate) priority ceiling (semaphores/OSEK resources)
  - Problem: need to protect each use of a communication variable. Advantage (does not require extra buffer memory, but only the additional memory of the protection mechanism)
  - Lock-free/Wait-free communication: multiple buffers with protected copy instructions:
    - Typically w. interrupt disabling or kernel-level code
    - Problem: requires additional buffer memory (How much?). Advantage: it is possible to cluster the write/read operations at the end/beginning of a task, with limited change to existing code.
- The best policy may be a mix of all the previous, depending on the timing constraints of the application and on the communication configuration.
Demonstrating impossibility of preemption

• Assign priorities and offsets and use timing analysis to guarantee absence of preemption

• Input data:
  – Mapping of functional blocks into tasks
  – Order of functional blocks inside tasks
  – Worst-case execution time of blocks (tasks)
  – Priorities assigned to tasks
  – Task periods
  – (relative) Offset in the activation of periodic tasks \( o_{wr} \) = minimum offset between writer and reader activations, \( O_{wr} \) = maximum offset between the activations

• Computed data
  – Worst case response time of tasks/blocks (considering interferences and preemptions) \( R_r \) for the writer \( R_w \) for the reader

• Two cases:
  – Priority writer > priority reader
  – Priority reader > priority writer
Absence of preemption/High to low priority

- Condition for avoiding preemption writer→reader (no assumptions about relative rates of reader/writer)

\[
R_r \leq T_w - O_{wr}
\]
Absence of preemption/Low to high priority

- Condition guaranteeing absence of preemption or reader to writer (reader → writer)

Both conditions are unlikely in practice
Absence of preemption/Low to high priority

- These conditions are ultimately used by the Rate Transition block mechanisms!!
Avoiding preemption

- Disabling preemption

The response time of the high priority block/task is affected, need to check real-time properties
Preserving streams

- What buffering mechanisms are needed for the general case?
  - Event-driven activation
  - One-to-many communication
Preserving streams

• What buffering mechanisms are needed for the general case?
  – Stream preservation (requirement)
  – Event-driven activation
  – One to many communication

The value produced by this instance is read by this instance and needs to be buffered in between.

0-delay behavior
Preserving streams

This block instance is assigned a buffer entry at the time of its activation.

The entry is written at running time.

This reader instance is assigned the buffer entry at the time of its activation.

The entry is used by the reader at running time.
Preserving streams

- The time the buffer index is assigned (activation of the block) may differ significantly from the time when the index is actually used (at running time) because of scheduling delays
  - Support from the OS is needed for assigning indexes at block activation times
Preserving streams

- Many issues
  - Defining efficient mechanisms for assigning indexes to the writers and the readers (if they are executed at kernel level)
  - Sizing the communication buffers (given the system characteristics, how many buffers are needed?)

*It is not necessary to store all these (6) values, there are at most 3 readers at each time!*

This reader instance is assigned the buffer entry at the time of its activation.

The entry is used by the reader at running time.

What buffer index is available at the time of the writer activation?
Model implementation: multi-task

- Efficient but issues with data integrity and time determinism

\[ b_i \rightarrow b_j \]

\[ o_i(m) \quad i_j(k) \quad o_i(m+1) \]

Q1: How many buffers do you need?
Q2: How do you define the index to be used (at activation time) and you pass to the runtime instance?

Defined at activation time

Defined at activation time

Written at run time

Read at run time

Defined at activation time

Defined at activation time

Q1: How many buffers do you need?
Q2: How do you define the index to be used (at activation time) and you pass to the runtime instance?
Buffer sizing methods

Two main methods

• preventing concurrent accesses by computing an upper bound for the maximum number of buffers that can be used at any given time by reader tasks. This number depends on the maximum number of reader instances that can be active at any time.

• Temporal concurrency control. The size of the buffer can be computed by upper bounding the number of times the writer can produce new values, while a given data item is considered valid by at least one reader.
Bounding the **maximum number of reader instances**

- the size is equal to the maximum number $N$ of reader task instances that can be active at any time (the number of reader tasks if $d \leq T$), plus two more buffers: one for the latest written data and one for use by the writer [Chen97] (no additional information is available, and no delays on the links).

A linked list implementation may trade space for time ($O(1)$ access)
Temporal concurrency control

- Based on the concept of datum lifetime. The writer must not overwrite a buffer until the datum stored in it is still valid for some reader.

\[ \text{lifetime} \quad \text{wr} = O_{\text{wr}} + \max(R_{\text{ri}}) \]

The writer simply writes at the next (modulo N) index.

Item I can be reused when no reader can access it.
Combination

- A combination of the temporal concurrency control and the bounded number of readers approaches can be used to obtain a tighter sizing of the buffer.
- Reader tasks are partitioned into two groups: fast and slow readers. The buffer bound for the fast readers leverages the lifetime-based bound of temporal concurrency control, and the size bound for the slow ones leverages information on the maximum number of reader instances that can be active at any time. Overall, the space requirements are reduced.
Combination

- Readers of $\tau_{wi}$ are sorted by increasing lifetime ($l_i \leq l_{i+1}$). The bound

$$NB_{w_i,j} = \left\lfloor \frac{l_j}{T_w} \right\rfloor$$

- Applies to readers with lifetime $\leq l_j$ (fast readers).
- Once $j$ is chosen, the bound is

$$j \in 0..NR_{w_i}$$

$$\min \left\{ \left\lfloor \frac{l_j}{T_w} \right\rfloor + \sum_{i=j+1}^{NR_{w_i}} \min \left\{ \left\lfloor \frac{R_{r_i}}{T_{r_i}} \right\rfloor \right\} + \max_{i=j+1}^{NR_{w_i}} \text{delay}[i] \right\}$$

Buffer shared among fast readers

based on the number of reader instances inside the lifetime
Wait free solution with flow preservation (slight modification to Chen&Burns protocol)

Data: BUFFER [1,...,NB]; NB: Num of buffers
Data: READINGLP [1,...,nLP]; nLP: Num of lower priority readers
Data: READINGHP [1,...,nHP]; nHP: Num of higher priority readers
Data: PREVIOUS, LATEST

1. GetBuf();
2. begin
3.   bool InUse [1,...,NB];
4.   for i=1 to NB do InUse [i]=false;
5.   LUse[LATEST]=true;
6.   for i=1 to nLP do
7.     j = READINGLP [i];
8.     if j !=0 then InUse [j]=true;
9.   end
10. for i=1 to nHP do
11.   j = READINGHP [i];
12.   if j !=0 then InUse [j]=true;
13. end
14. i=1;
15. while InUse [i] do ++i;
16. return i;
17. end

18. Writer_activation();
19. begin
20.   integer widx, i;
21.   widx = GetBuf();
22.   PREVIOUS = LATEST;
23.   LATEST = widx;
24.   for i=1 to nHP do CAS(READINGHP [i], 0, PREVIOUS);
25.   for i=1 to nLP do CAS(READINGLP [i], 0, LATEST);
26. end
27. Writer_runtime();
28. begin
29.   Write data into BUFFER [widx];
30. end

1. ReaderLP_activation();
2. begin
3.   constant id; — Each lower priority reader has its unique id;
4.   integer ridx;
5.   READINGLP [id]=0;
6.   ridx = LATEST;
7.   CAS(READINGLP [id],0,ridx);
8.   ridx = READINGLP [id];
9. end

10. ReaderHP_activation();
11. begin
12.   constant id; — Each higher priority reader has its unique id;
13.   integer ridx;
14.   READINGHP [id]=0;
15.   ridx = PREVIOUS;
16.   CAS(READINGHP [id],0,ridx);
17.   ridx = READINGHP [id];
18. end

19. Reader_runtime();
20. begin
21.   Read data from BUFFER [ridx];
22. end

---

Runtime part (in the task code)

Activation-time part (supported by the OS or hooks)
Multicore adaption of RT block

High rate to low rate communication: with explicit intercore activation signal and with synchronized activation with offsets

Activation with jitter, receiver deadline = period

Need for time synchronization
Activation without jitter
receiver deadline < period
Multicore adaption of RT block

High rate to low rate communication: with explicit intercore activation signal and with synchronized activation with offsets
Model-based design: a functional view

- Advantages of model-based design
  - Possibility of advance verification of correctness of (control) algorithms

- Possible approaches
  1. The model is developed considering the implementation and the platform limitations
     - include from the start considerations about the implementation (tasking model and HW)
       - PROS (apparent)
         - use knowledge about the platform to steer the design towards a feasible solution
           (in reality, this is often a trial-and-error manual process)
       - CONS (true)
         - the model depends on the platform (updates/changes on the platform create opportunities or more often issues that need to be solved by changing the model)
         - Analysis is more difficult, absence of layers makes isolating errors and causes of errors more difficult
         - the process is rarely guided by sound theory (how good is the platform selection and mapping solution?)
         - Added elements (Rate-transition blocks) introduce delays
  2. The model is developed as a “pure functional” model according to a formally defined semantics, irrespective of the possible implementation
     - The model is then refined and matched to a possible implementation platform. Analysis tools check feasibility of an implementation that refines the functional semantics and suggest options when no implementation is feasible (more ...)
Model-based design: a functional view

- Advantages of model-based design starting from a purely functional model
  - Possibility of advance verification of correctness of (control) algorithms
  - Irrespective of implementation
  - This allows an easier retargeting of the function to a different platform if and when needed
    - The functional design does not depend on the platform
  - The verification of the functional design can be performed by domain experts (control engineers) without knowledge of SW or HW implementation issues

- Necessary assets to leverage these advantages …
  - Capability of defining rules for the correct refinement of a functional model into an implementation model on a given platform
  - Capability of supporting design iterations to understand the tradeoffs and the changes that are required when a given functional model cannot be refined (mapped) on a given platform
Model-based development flow

- Platform-based design

![Diagram showing the model-based development flow]

**Functional model**
Independent of Platform

**System platform model**
(possibly the level of the SW implementation in tasks and messages)
Independent from both and suitable for evaluation of mapping solutions

**Execution architecture model**
Independent of Functionality
Platform-dependent modeling: an example

This model demonstrates how to simulate and generate code using the example SetAlarm and ActivateTask blocks for the OSEK real-time operating system. This model contains three function-call subsystems, "Red", "Green", and "Blue" that are generated with RTW-EC as separate OSEK Tasks and thus execute based on assigned priority using the OSEK scheduler. A generic OSEK main program and OIL file are generated by the ERT File customization template: osilk_file_process.tlc. You can modify this template to provide detailed information for your specific OSEK implementation.

Generate Code Using Real-Time Workshop Embedded Coder (double-click)
Inspect Block TLC Code (double-click)
View Template Configuration (double-click)

Copyright 2009 The MathWorks, Inc.
PBD and RTOS/platform

Refinement into a set of concurrent tasks exchanging messages

Platform API (OSEK/AUTOSAR)

Single-processor w. priority-based RTOS

Dist. system w. asynchronous network (CAN)

Dist. system w. time-triggered network (FlexRay)
Design/Scheduling trade-offs

However...

- if the communication is fast-to-slow and the slow block completes before the next instance of the fast writer, the RT block is not required.
- if the communication is from slow to fast, it is possible to selectively preserve the precedence order (giving higher priority to the slow block) at the expense of schedulability.
  - Two tasks at the same rate, one high priority, the other low priority.
An approach

**Required steps**

- Definition of the network of functional blocks with feedthrough dependencies
- Definition of the synchronous sets
- Priority assignment and mapping into tasks
- Definition of the block order inside tasks

![Diagram with functional blocks and task mapping]

- **Type1 RT**
- **Type2 RT**
Conclusions

• Schedulability theory and worst-case timing analysis …
  – From the run-time domain to the design domain (already happening)
  – From the analysis domain to the optimization (synthesis) domain
  – Complemented by sensitivity analysis and uncertainty evaluation

• However …
  – Typical deadline analysis is not enough!
  – Tasks and messages are not the starting point (semantics preservation issues from functional models to tasking models)
  – Worst case analysis needs to be complemented
  – Mixed domains (time-triggered / event-triggered)
Q&A

Thank you!