Formal Analysis of Timing Effects on Closed-loop Properties of Cyber Physical Systems

Arne Hamann, Corporate Research, Robert Bosch GmbH

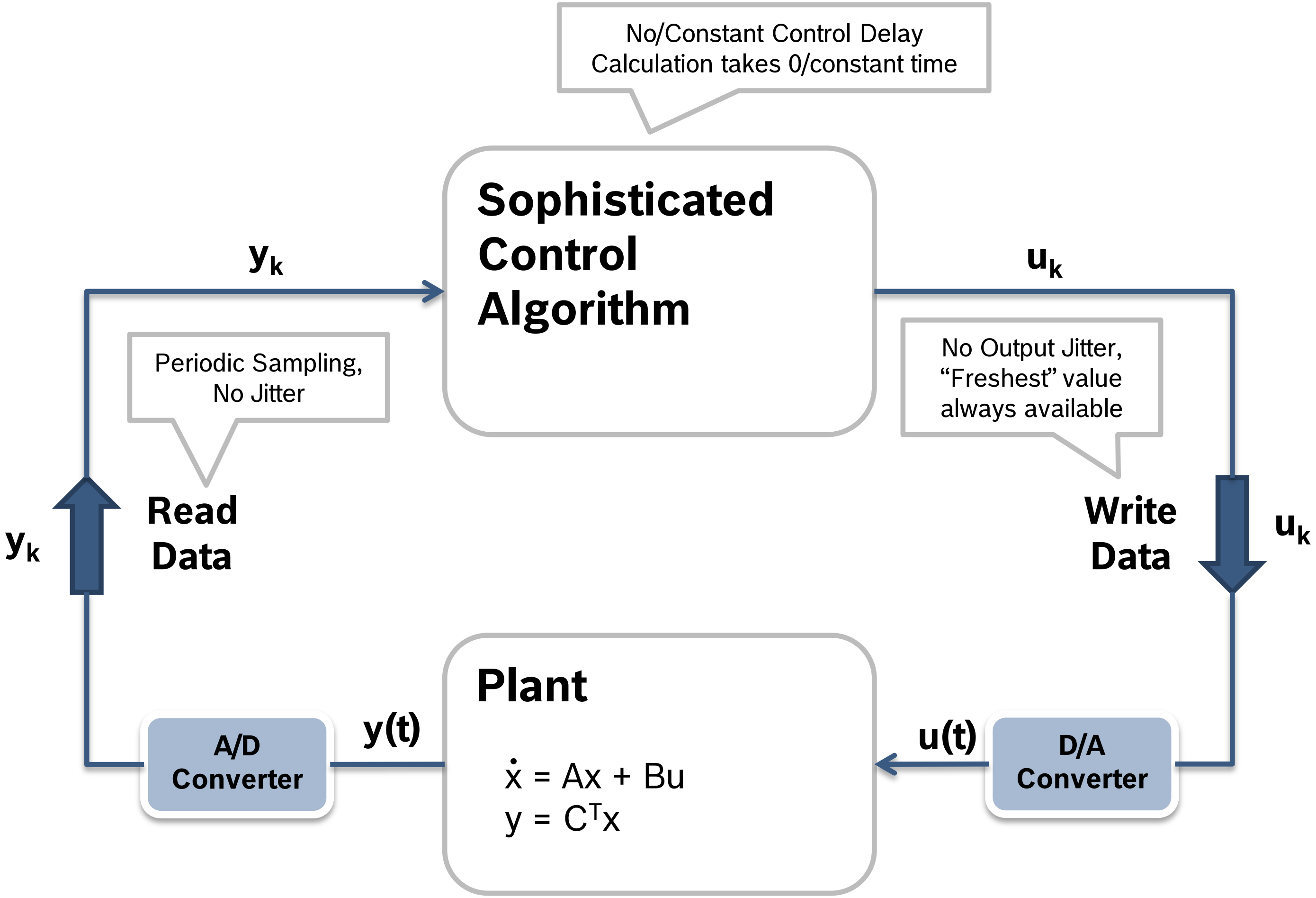
Joint work with: Matthias Wöhrle (Bosch), Goran Frehse (Université Joseph Fourier Grenoble),
Sophie Quinton (INRIA Grenoble)

BOSCH

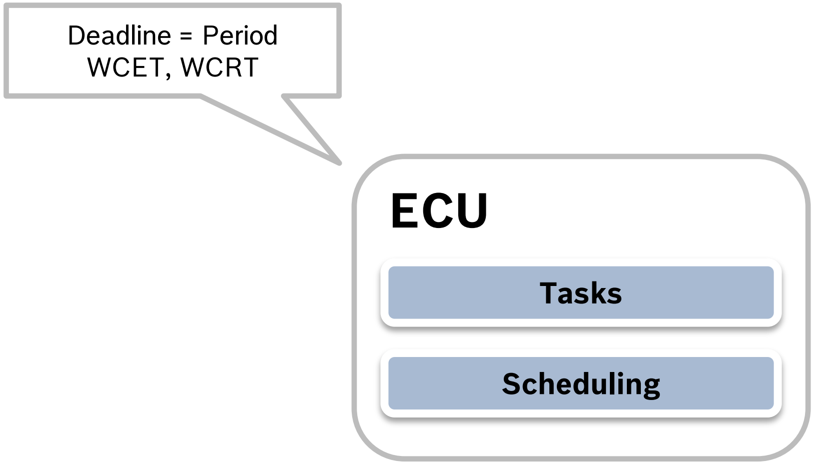
Outline

- Problem statement & goals
- Interaction model for co-engineering between control and real-time engineering
- Electro Mechanic Braking System (EMB)
- Formal analysis of EMB system using hybrid automatons and reachability analysis
- Conclusion

System as seen by the control engineer



System as seen by the real-time engineer



$$\sum_{i=1}^{n} \frac{C_i}{T_i} \leq n \cdot \left(\sqrt[n]{2} - 1\right)$$

$$\ln 2 \approx 69{,}3\%$$

$$R_i = C_i + \sum_{j \in \mathrm{hp}(i)} C_j \left\lceil \frac{R_i}{T_j} \right\rceil \leq D_i = T_i$$

Problem Statement - Shortcomings

Control engineering

- Theory:
  - Equidistant sampling
  - Zero input-output latencies
- Reality:
  - Varying execution and response times due to preemption, blocking, data-dependencies, …
  - Sampling interval jitter
  - Non negligible response times

Real-time system engineering

- Theory:
  - Timing models and requirements that are motivated by the runtime system rather than functionality (e.g. deadline = period)
- Reality:
  - Timing requirements do not exist per se and must be derived from functional requirements

Result:

- Functional integration effects due to timing are unpredictable
- Severe migration problems in case of platform modifications

BOSCH

Goals

- **Co-engineering** between real-time and control engineering
- Assessment of functional behavior under the influence of resource sharing **during design time on PC**
- Systematically **derive timing requirements** that are necessary to fulfill functional requirements
- Use these timing requirements for **system synthesis** using adequate platform mechanisms

BOSCH

Current Interaction Model

Plant, Control Problem, Functional requirements

Control Engineering (per control problem)

- -Analysis of plant dynamics (e.g. time constants)
- -Specification of problem class
- -Choice/derivation of control algorithm
- -Discretization of control laws

MATLAB SIMULINK

-Equations / Code
-Desired sampling rate (range)

Problems:

- **OK only means sampling rate met**
- **NOT that the functionality works**

→ Oversampling to compensate unknown integration effects

Hardware Architecture, Tool Chain

Real-time Engineering

- -Integration of n control functions
- -Mapping to cores
- -Selection of scheduling strategy
- -Assignment of scheduling parameters (offsets, priorities, ...)
- -Assignment of execution orders and sequences

SYMTA VISION

OK
NOK
Really??

BOSCH

Co-engineering Interaction Model

Plant, Control Problem, Functional requirements

Control Engineering (per control problem)

- -Analysis of plant dynamics (e.g. time constants)
- -Specification of problem class
- -Choice/derivation of control algorithm
- -Discretization of control laws

-Derive timing requirements

-Equations / Code
-Desired sampling rate (range)

-Timing requirements (jitter, latency)

Timing structure of controller

-Derive timing Structure

Hardware Architecture, Tool Chain

Real-time Engineering

- -Integration of n control functions
- -Mapping to cores
- -Selection of scheduling strategy
- -Assignment of scheduling parameters (offsets, priorities, ...)
- -Assignment of execution orders and sequences

OK

NOK

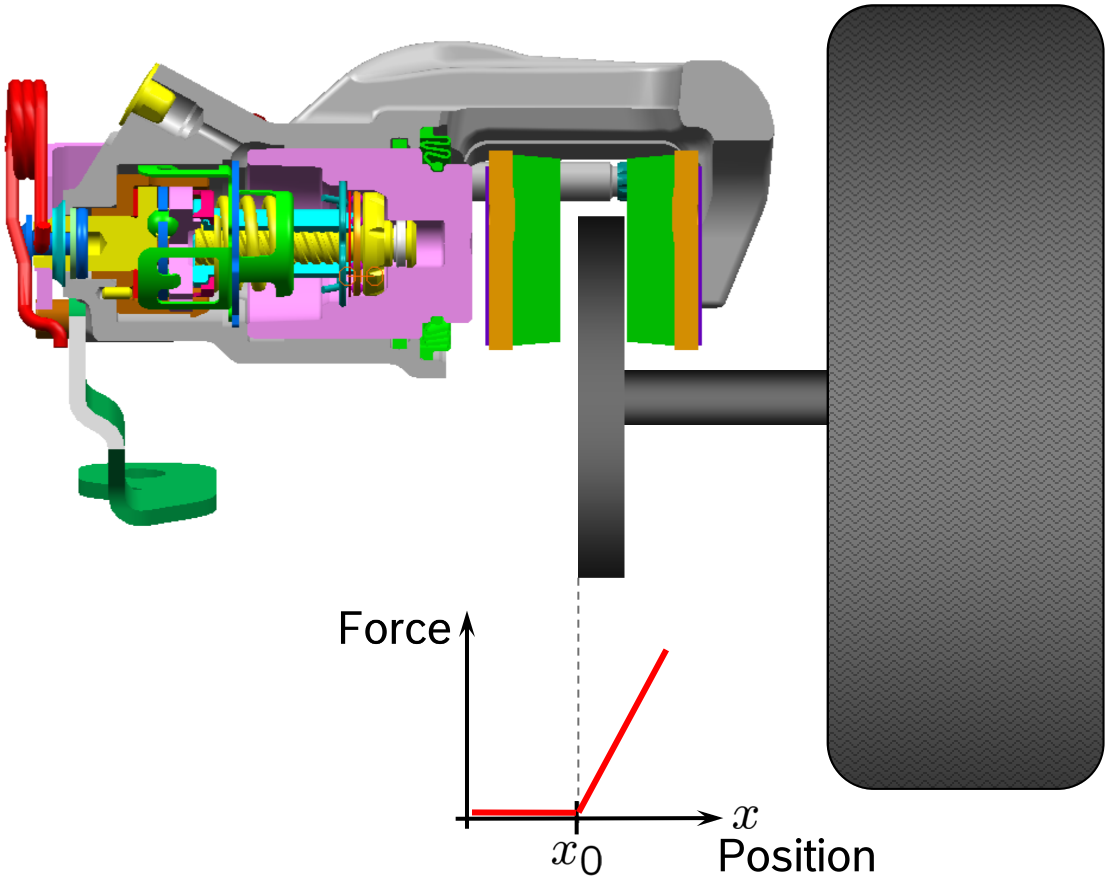
Really!!

MATLAB SIMULINK

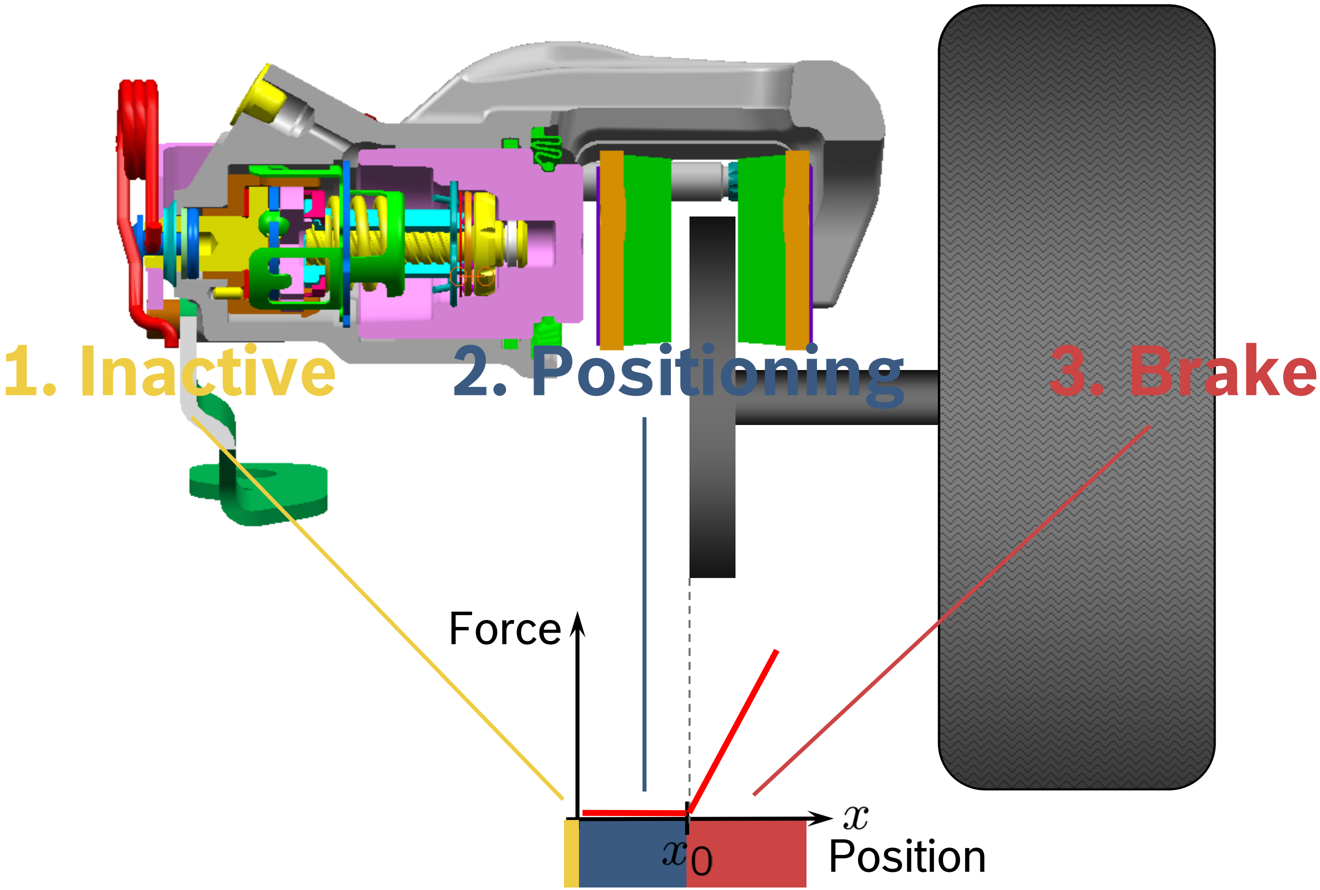
SYMTA VISION

BOSCH

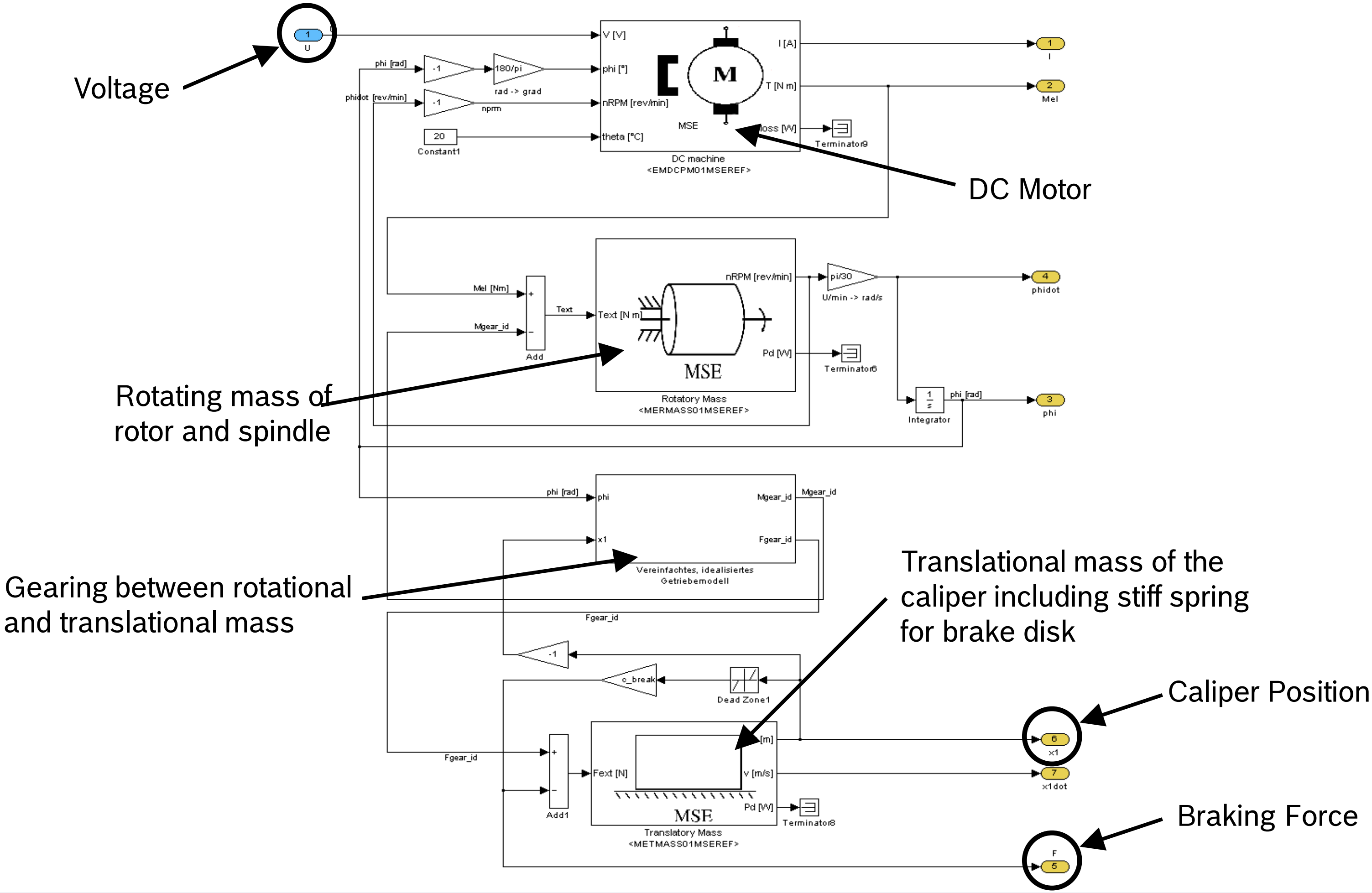
Electro Mechanic Braking System



Electro Mechanic Braking System

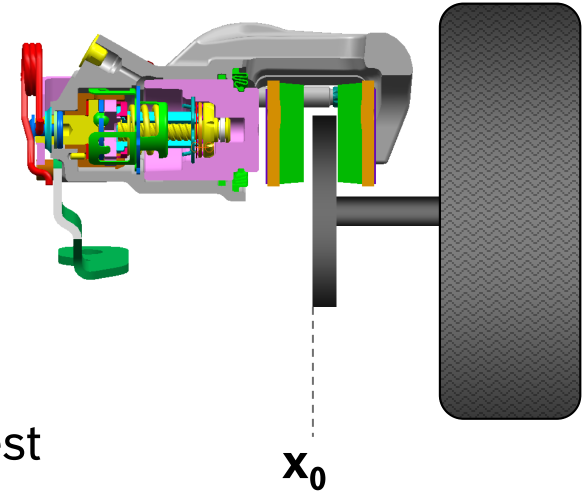


Simulink Plant Model



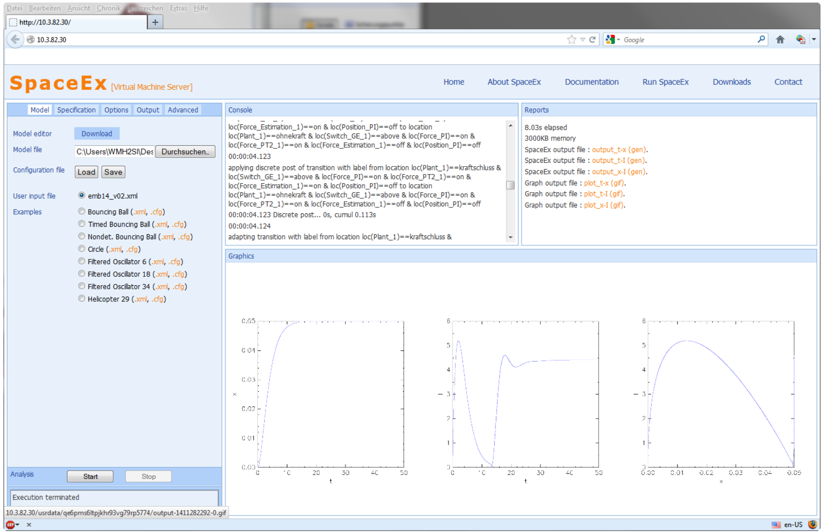
BOSCH

Functional Requirements



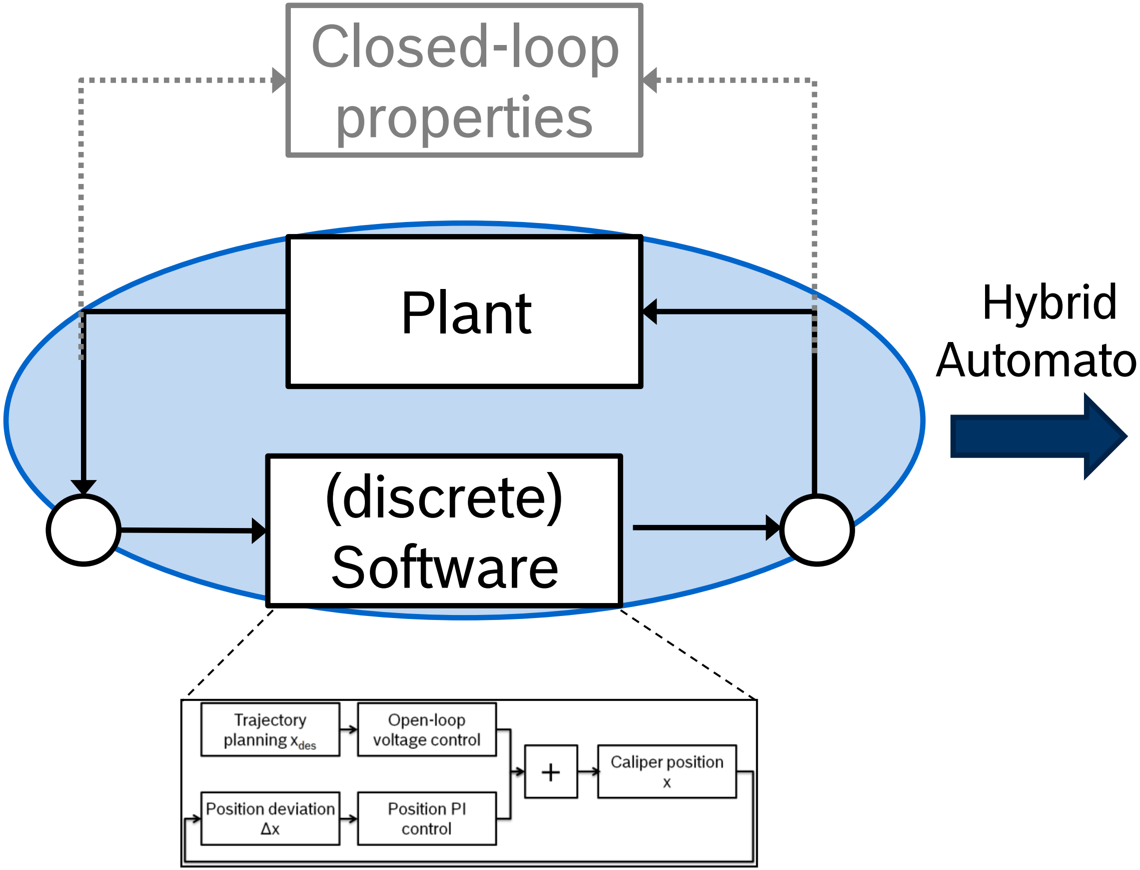
- "Ready-to-brake" position x_0 = 5 mm
  - Preparation of braking system for applying brake force, no force closure
- **Req. 1: Short response time**
  - Reactiveness of the system
  - Caliper must be at x_0 after the braking request is issued within 20ms with a precision of 4%
- **Req. 2: Small impulse before braking**
  - Driver feels an abrupt deceleration
  - The caliper speed at contact must be below 2mm/s
  - Might be acceptable for braking, but not in other scenarios , e.g. disk wiping

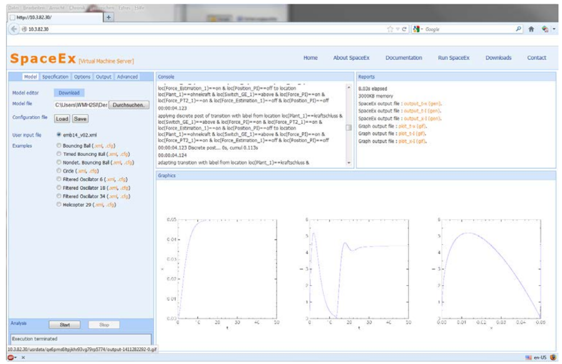
Formal analysis using hybrid automatons and reachability analysis

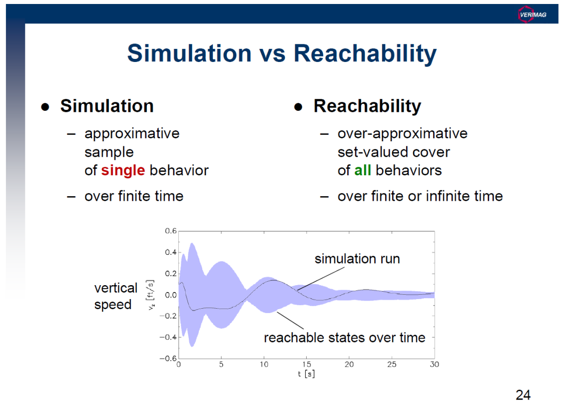


BOSCH

Functional Verification with ZET* Assumption

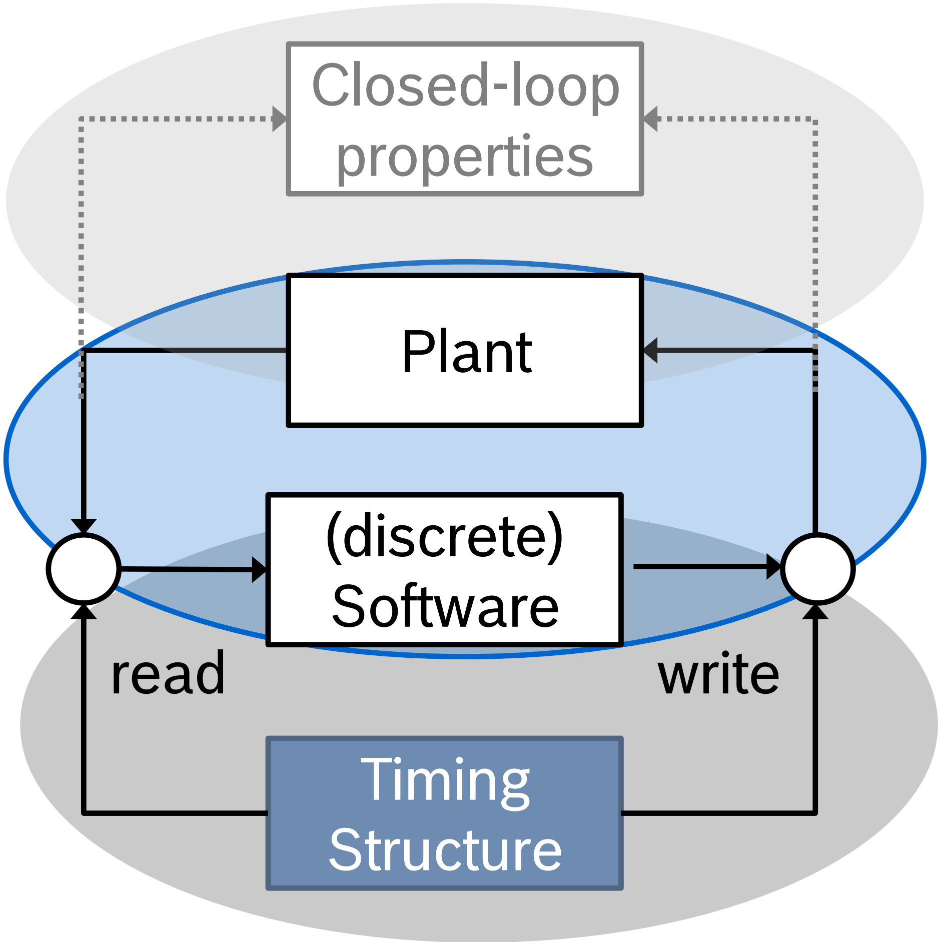






*ZET = Zero Execution Time

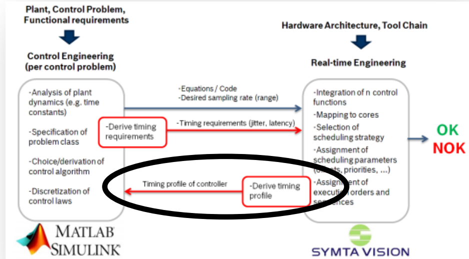
Functional Verification considering Timing

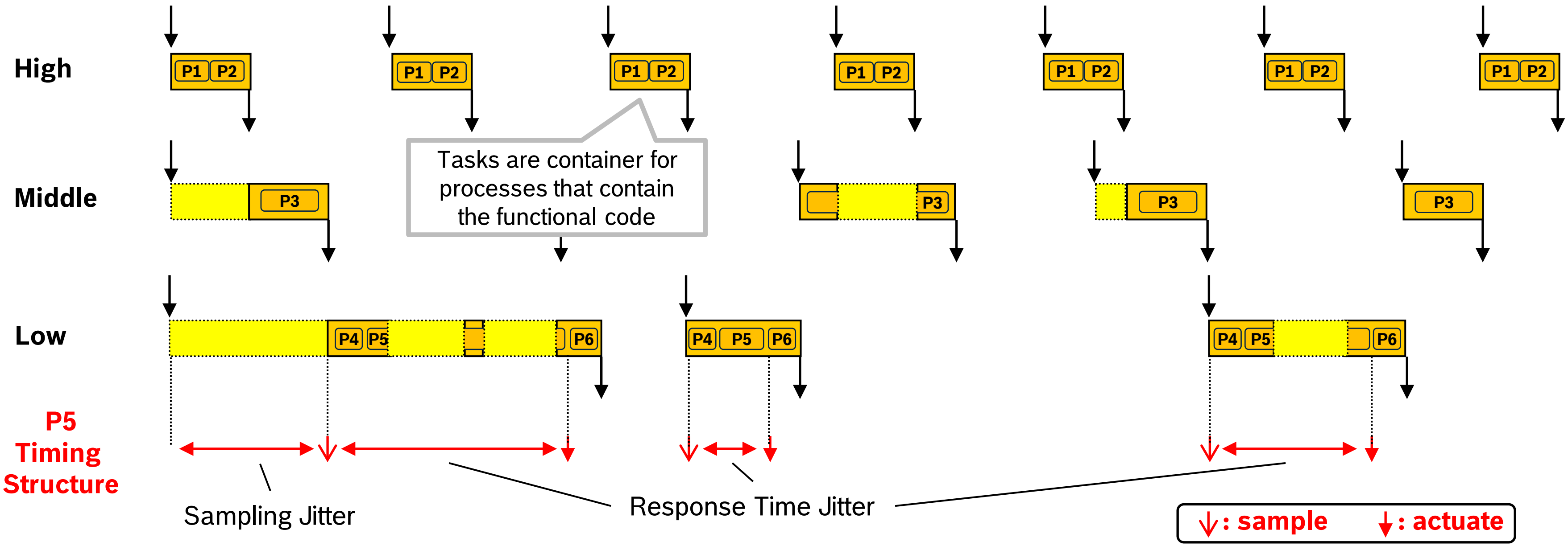


- ➔ Model Timing in Hybrid Automaton
  - When is data written / read
  - Non-deterministic model
- ➔ Possible models
  - Logical Execution Times
  - Arrival Curves
  - Typical Worst-Case Models
  - ...
- ➔ Drivers for choosing a model
  - Generality / analysis trade-off
  - Decision to simplify design for verifiability
  - Functional requirements

Timing Structure – OSEK Systems

- Description of points in time where the plant is sampled, and where the actuation takes place
- Assumption: functionality implemented by a single process
- Example: Bosch Engine Management
  - Copy-in of required data at task release
  - Copy-out of produced data at process completion



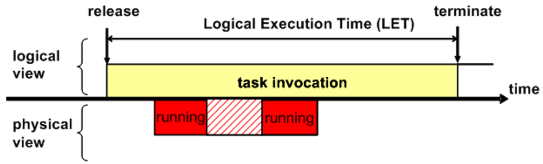


BOSCH

Which Timing Model to choose?

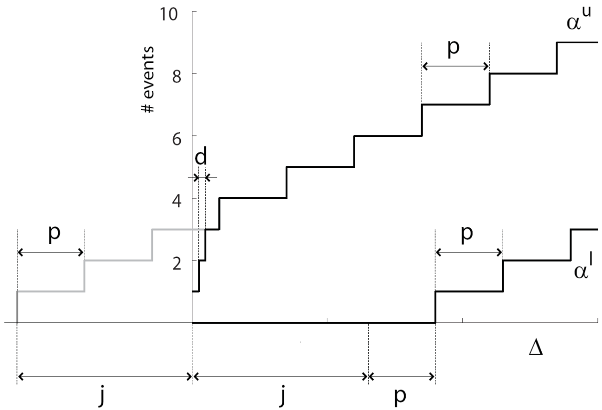
→ LET ?

- Trade Jitter against Latency → Determinism
- Great simplification of verification task
- Ok for “robust” control tasks based on exact models and little external disturbances



→ Arrival Curves?

- Precise model of possible system timing behavior
- Large space of possible timings
- Closed-loop verification very difficult



→ Typical Worst-Case Model !

- Allows for trade-off between both models

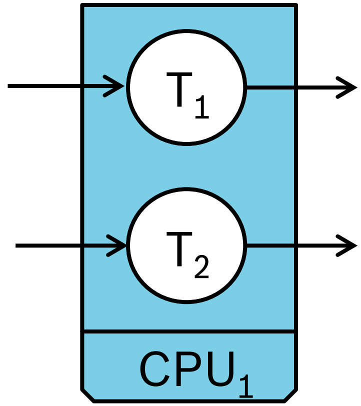
Typical Worst-Case Analysis

- Principle
  - Identify typical bounds for the behavior of a system and how often the system may leave these bounds

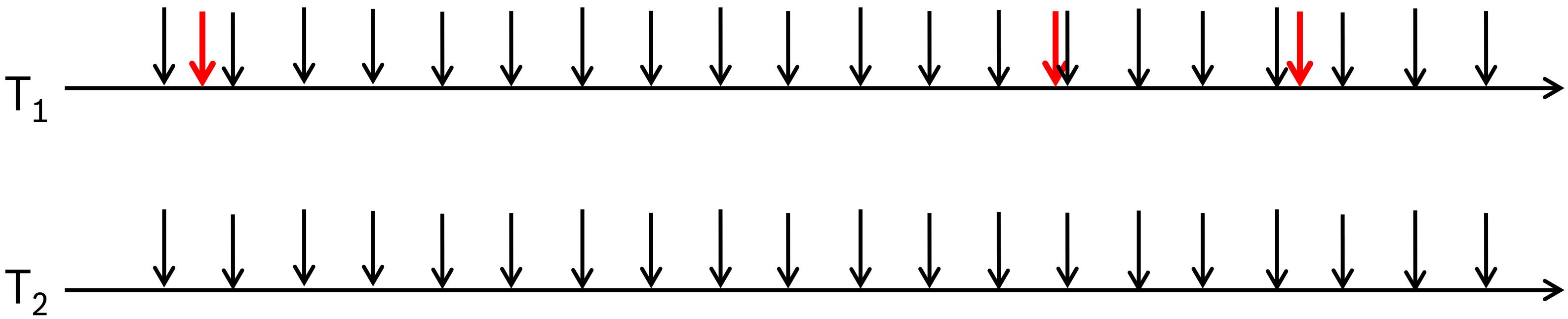
- Output for each task
  - a “safe” bound on its response times: SWCRT
  - a typical bound: TWCRT
  - a function err such that out of every **k** consecutive executions, at most **err(k)** response times may be larger than TWCRT

- Advantages
  - Approach is computationally very efficient
  - **m-out-of-k** constraints are easy to understand
  - No assumptions w.r.t. dependencies

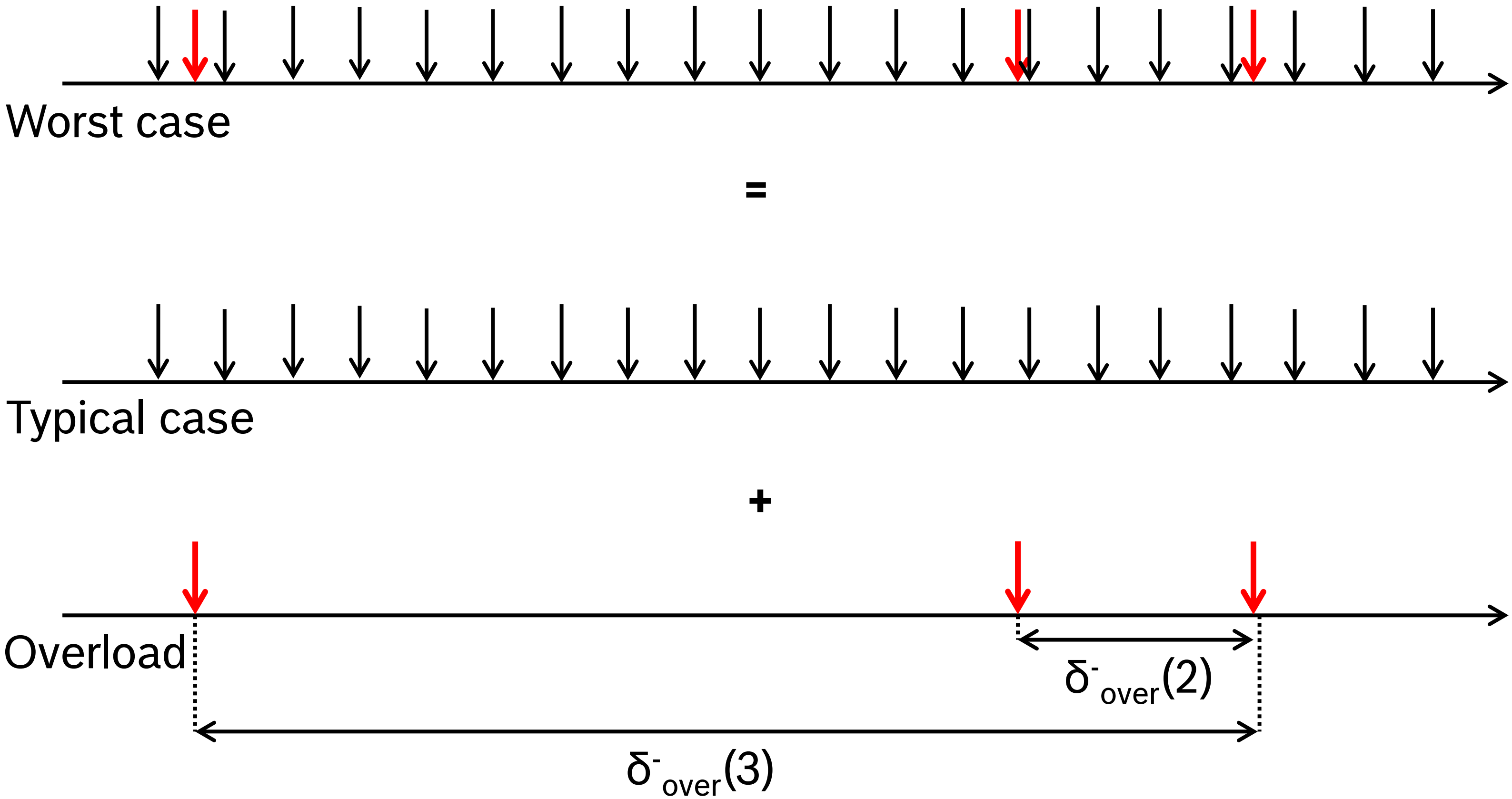
Formal Analysis of Sporadic Overload



Scheduling policy: SPP
(Static Priority Preemptive)
$T_1 > T_2$



Modeling Sporadic Overload



Formal Analysis of Sporadic Overload

- Input:
  1. a worst-case model of the system
  2. a typical model ignoring the overload
  3. a model of the overload

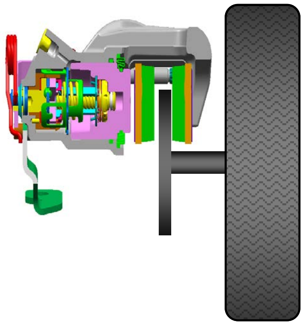
- Analysis (for each task):
  1. a busy window analysis of the worst-case model
     → **Safe Worst-Case Response Time (SWCRT)**
  2. a busy window analysis of the typical-case model
     → **Typical-Case Response Time (TWCRT)**
  3. a computation of the error model based on the result of 1. and the overload model
     → **function err** such that out of every k consecutive executions, at most err(k) response times may be larger than TWCRT

BOSCH

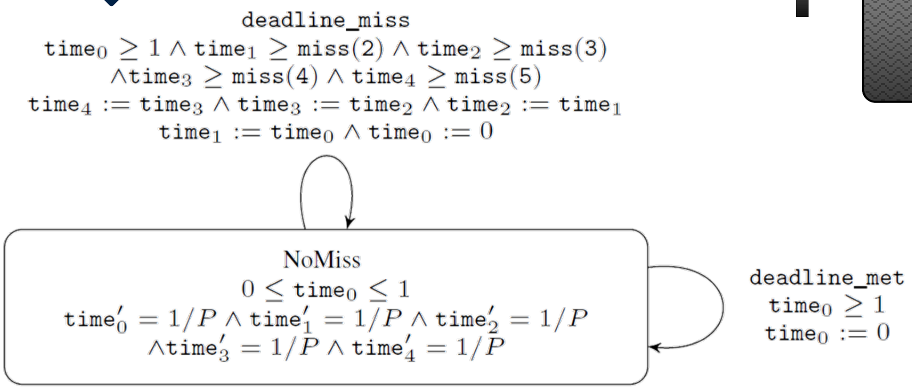
Using TWCRT Model for Closed-loop Functional Verification

- Idea: Data is written to plant deterministically at TWCRT << WCRT (using LET)
  - Trade-off between determinism & functional requirements
- TWCRT misses are bounded by error function
  - Scalable “discrete” timing model

Data for EMB example
Period = 1 ms
WCRT = 0.8 ms
TWCRT = 0.4 ms



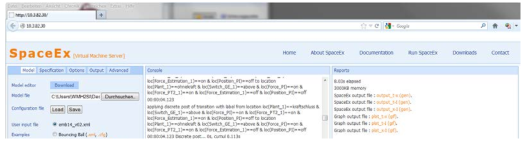
# deadline misses	consecutive executions
2	2
3	18
4	20
5	56

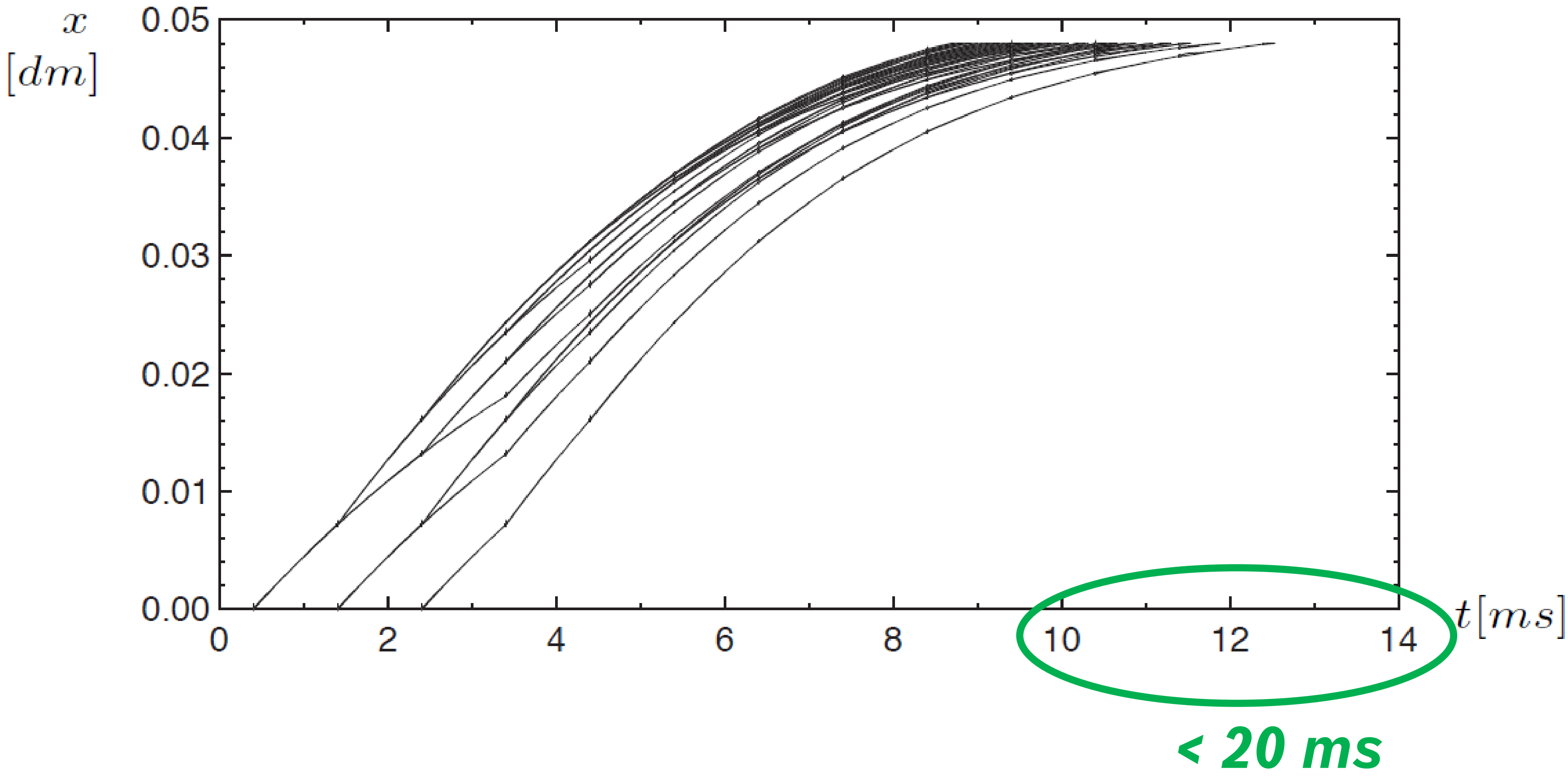


(to be published RTSS 2014)

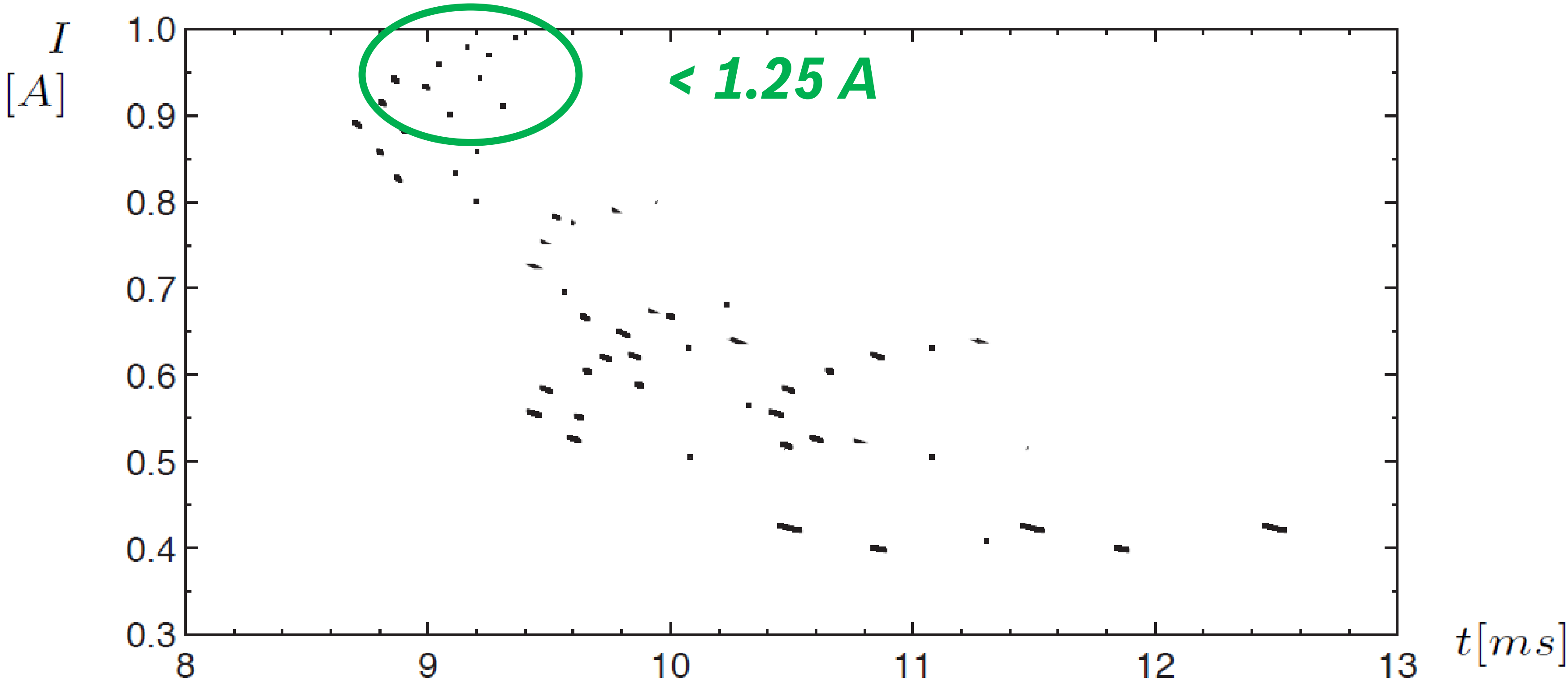
BOSCH

Requirement 1: Response time





Requirement 2: Small impulse



- *Current I* proportional to the caliper velocity
- Intersection reachable states with the plane of contact
- Bounds [0.38, 0.99] satisfies the requirement 2.

BOSCH

Conclusion

- Both control and real-time engineers have idealized system models for physical systems

- Functional integration effects are not considered by both disciplines
  - Integration effects are anticipated with overdesign
  - ...but even then, functional correctness cannot be guaranteed

- Reachability analysis for hybrid automatons is an adequate tool to verify closed loop properties under timing influences
  - Recent advances allow analysis of industrial strength applications

- One promising approach to close the gap between control and real-time system engineering
  - Verify correctness and performance of control software
  - Derive timing requirements for system synthesis

BOSCH

Questions ???

Formal Analysis of Timing Effects on Closed-loop Properties of Cyber Physical Systems

Arne Hamann, Corporate Research, Robert Bosch GmbH

Joint work with: Matthias Wöhrle (Bosch), Goran Frehse (Université Joseph Fourier Grenoble),
Sophie Quinton (INRIA Grenoble)

BOSCH