Automotive Cyber–Physical Systems: A Tutorial Introduction

- IEEE Design & Test, vol. 33, no. 4, May 2016
- SCI 3区
- 慕尼黑工业大学
- 加州大学欧文分校

龚红仿

2017.4.28

一、研究内容

- 这一辅导资料为CPS初学者提供了辅导简介，特别是突出了汽车应用方面的控制理论基础。本文进一步描述了控制模型及其实现上的“语义间隙”，指出需要一种新的面向CPS的设计方法。
- 资源感知的汽车控制软件设计；计算感知的控制系统设计；存储感知的控制系统设计。

二、研究背景

- Most of the innovation in the automotive domain is in electronics and software. All new features in modern cars—like advanced driver assistance systems—are based on electronics and software rather than on mechanical engineering Innovations.
- A modern high-end car has over 100 million lines of code and it is widely believed that this number will continue to grow in the near future.

二、研究背景

- Such code implements different control applications spanning across various functionalities—from safety-critical functions, to driver-assistance and comfort-related ones.
- These applications run on a distributed electronics and electrical (E/E) architecture, consisting of often hundreds of programmable ECUs that communicate via different types of communication buses like CAN, FlexRay, LIN, and more recently also automotive Ethernet.

二、研究背景

- 1.控制算法是基于许多理想的假设，如控制输入能瞬时计算；为了计算控制输入，传感器及其数据的使用没有时延；将控制模型编译为代码时没有系统化处理等等。
- 2.因为在控制理论文献中缺乏稳固的技术，导致这些问题很难找到合适的方法处理。因为汽车E/E体系结构较高的分布式和异构特性，使得这些问题对汽车的影响非常明显。

二、研究背景

- 3.因此，在实现所设计的控制器时，在控制模型与其实现之间存在较大的性能间隙，极端情况下可能导致系统不稳定。这不仅使验证困难，而且导致资源超尺度而增加系统成本。
- 4.在汽车CPS中，除了功能安全关键之外，还存在较高的成本敏感性。因而，汽车控制软件的资源有效实现是一个重要问题。控制算法的有效实现是计算机科学的基石之一。

三、设计方法学

- 1.面向CPS 的设计。 CPS设计范型的基础是控制算法及其运行这些算法的计算平台的集成设计（协同设计）。
- 汽车E/E体系结构的分布式和异构特性使得面向CPS的设计成为完美的选项，但是仅仅最近在这一研究方向上有一些进展。

三、设计方法学

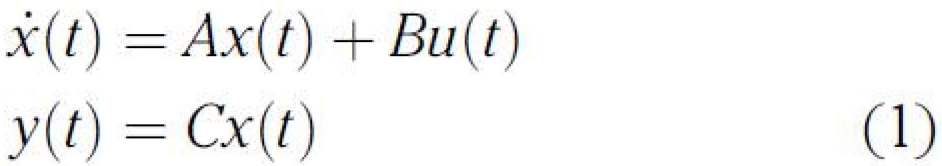
- 例如，传统的HVAC (heating, ventilation, and air conditioning) 仅仅关注乘客的舒适性和能耗，而忽略了电池寿命和ECU的极端高温及电磁干扰的工作环境。通过适当设计控制算法可以解决这些问题。
- 另外，汽车领域的安全性（ security）也是一个具有挑战性的问题，因为资源约束和成本敏感性。寻求安全性和控制性能之间的折中机制，现在开始出现了。

三、设计方法学

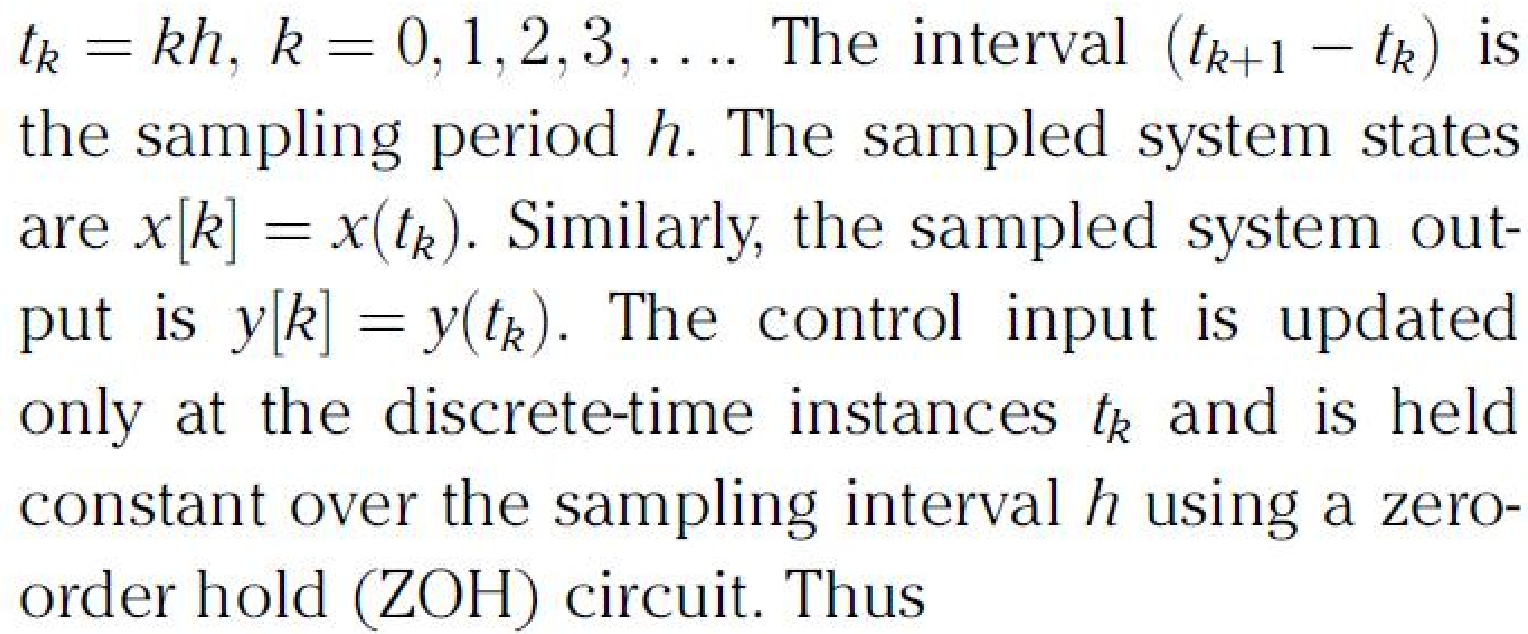
- 2.本文结构。这一辅导资料给出了上述问题的概述，处理这些问题的最新进展以及今后研究的挑战。但是，诸如视频处理、AI和控制理论之间的交互等高级驾驶员辅助系统和自动驾驶方面的重要问题，本文不予讨论，而是集中讨论汽车领域中的嵌入式系统、软件设计和控制理论之间的交互作用。
- 我们也不讨论详细的数学细节，而是关注主要的直觉感知。

三、设计方法学

- 3.反馈控制系统。



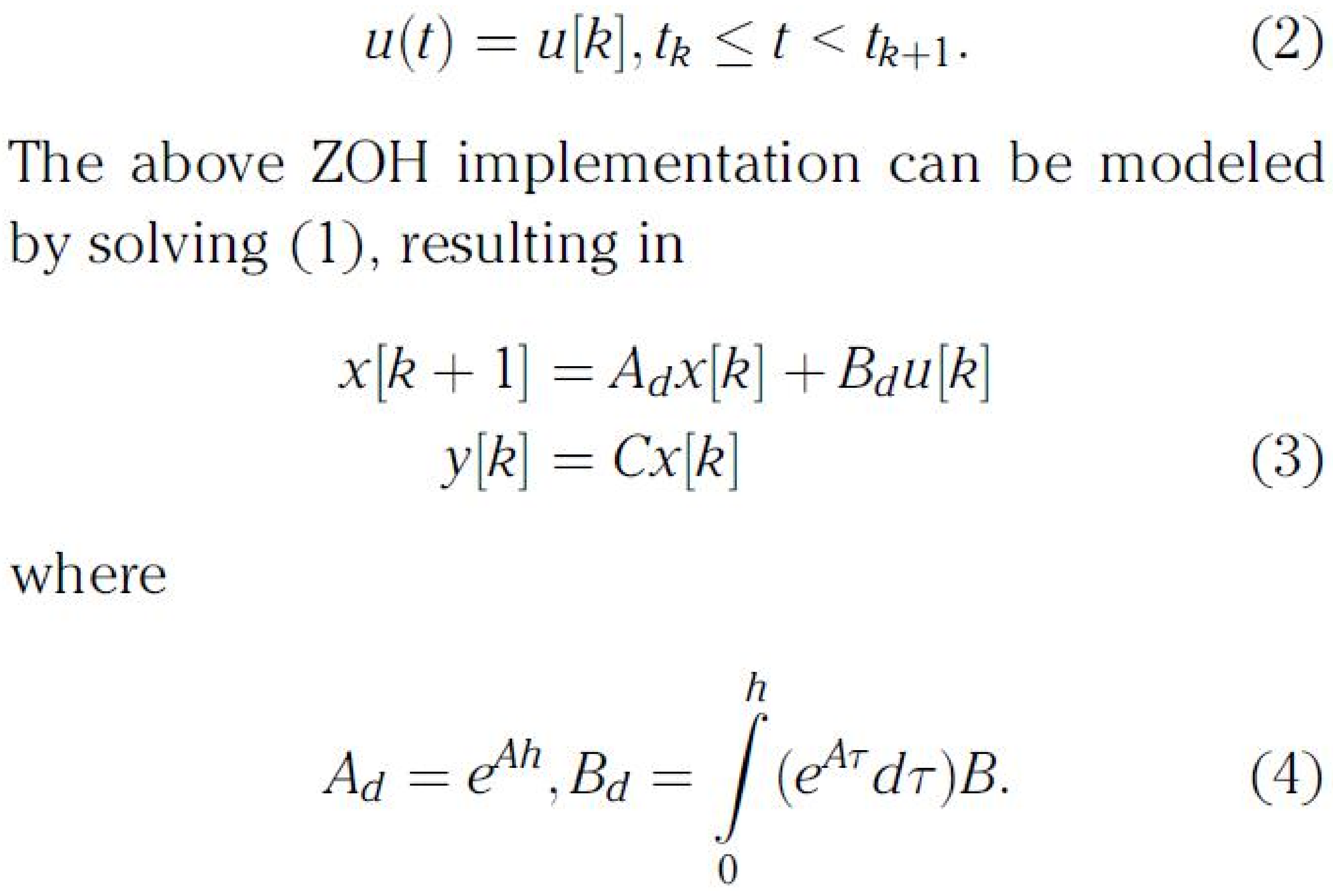
$$\dot{x}(t) = Ax(t) + Bu(t)$$
$$y(t) = Cx(t) \qquad (1)$$



$t_k = kh$, $k = 0, 1, 2, 3, \ldots$. The interval $(t_{k+1} - t_k)$ is the sampling period h. The sampled system states are $x[k] = x(t_k)$. Similarly, the sampled system output is $y[k] = y(t_k)$. The control input is updated only at the discrete-time instances t_k and is held constant over the sampling interval h using a zero-order hold (ZOH) circuit. Thus

三、设计方法学

- 3.反馈控制系统。



$$u(t) = u[k], t_k \leq t < t_{k+1}. \tag{2}$$

The above ZOH implementation can be modeled by solving (1), resulting in

$$\begin{aligned} x[k+1] &= A_d x[k] + B_d u[k] \\ y[k] &= Cx[k] \end{aligned} \tag{3}$$

where

$$A_d = e^{Ah}, B_d = \int_0^h (e^{A\tau} d\tau) B. \tag{4}$$

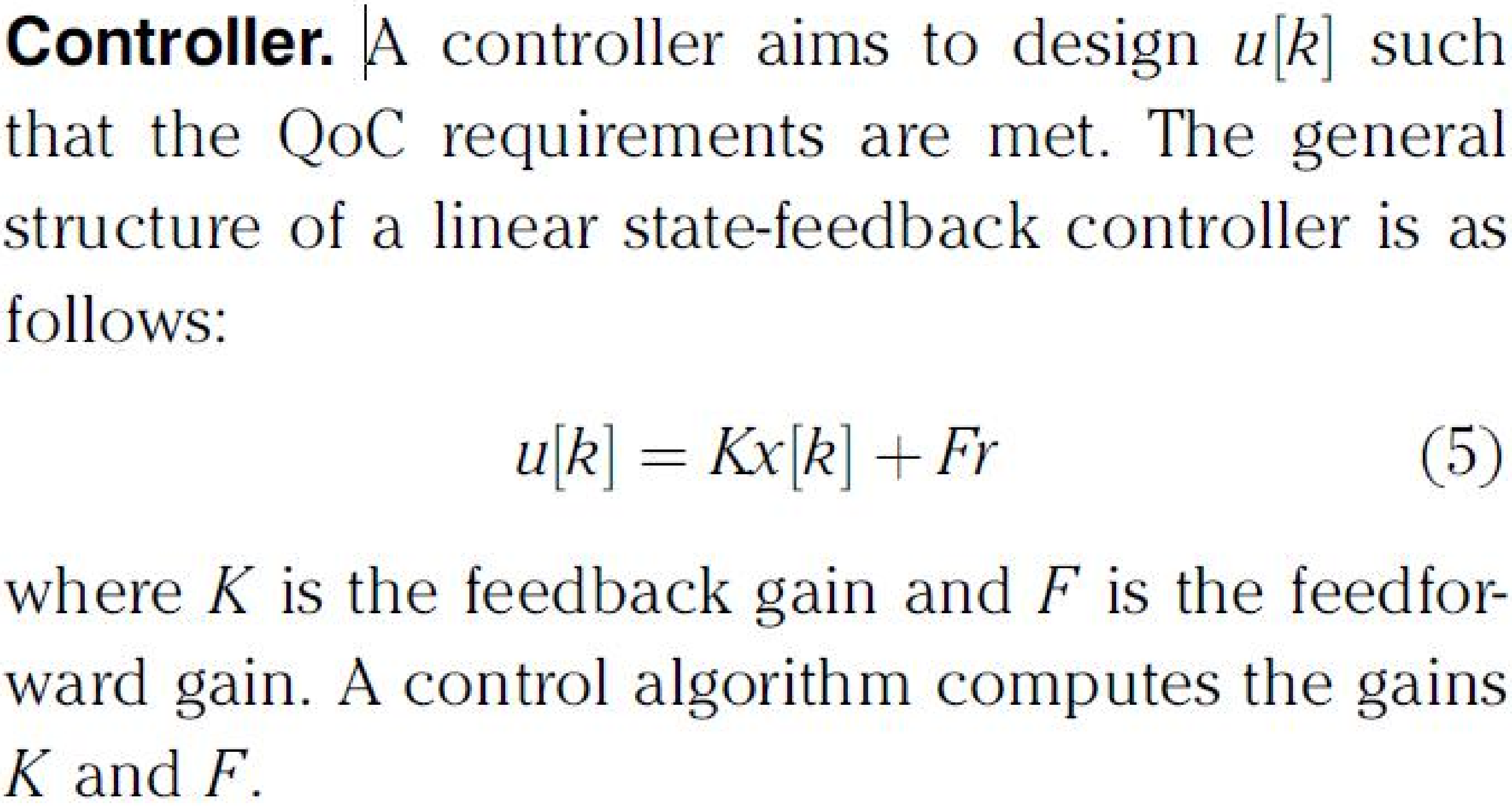
三、设计方法学

- 3.1. Quality of control (QoC).

Quality/performance of a control application is often quantified with respect to user requirements, for example, speed of response and comfort. *Settling time* is a widely used metric to quantify QoC. Shorter settling time implies better QoC. In many safety-critical automotive control loops, there is a maximum settling time that must be satisfied for functional correctness.

三、设计方法学

- 3.2. Controller.



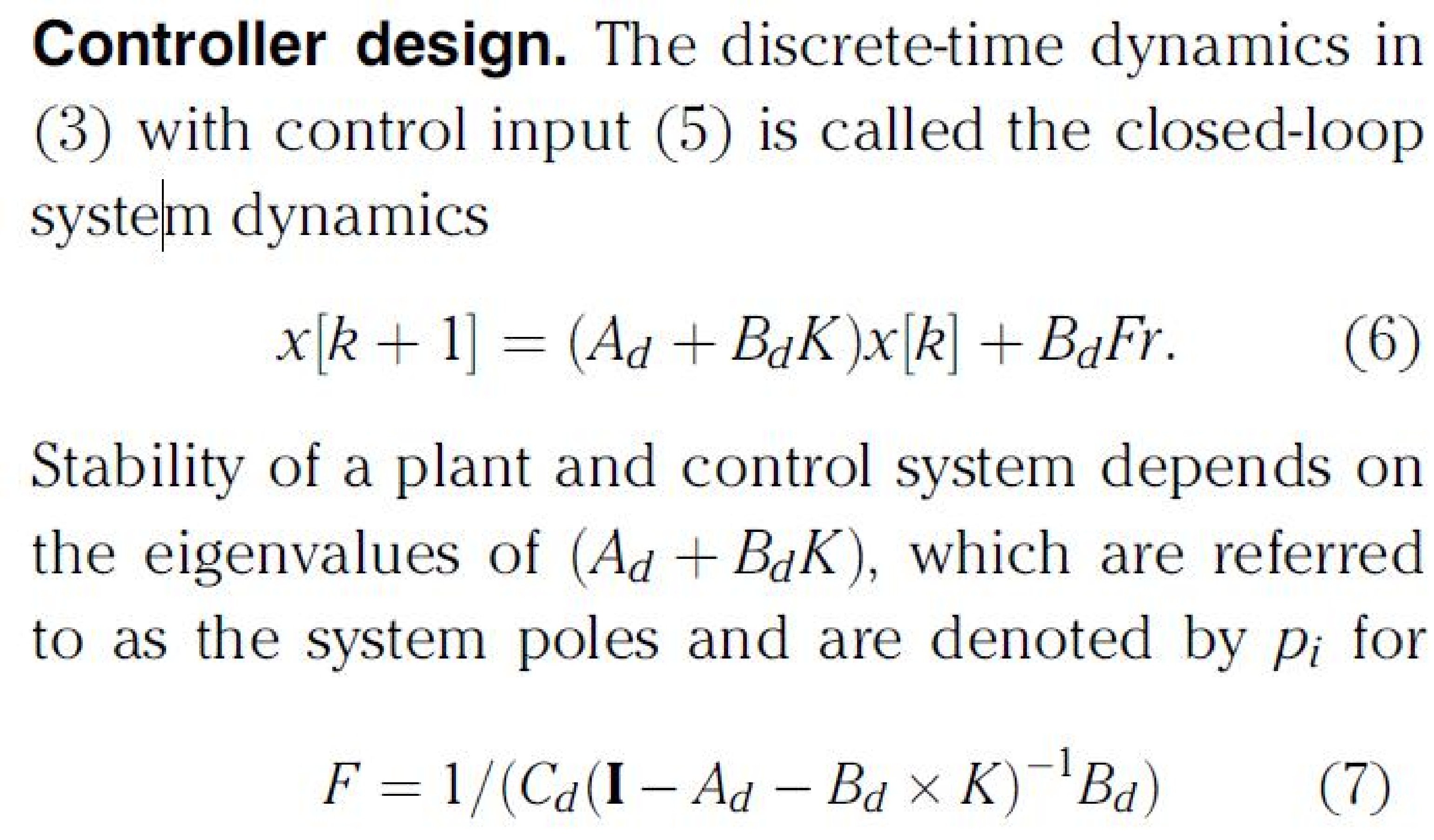
Controller. A controller aims to design $u[k]$ such that the QoC requirements are met. The general structure of a linear state-feedback controller is as follows:

$$u[k] = Kx[k] + Fr \qquad (5)$$

where K is the feedback gain and F is the feedforward gain. A control algorithm computes the gains K and F.

三、设计方法学

- 3.3. Controller design.



Controller design. The discrete-time dynamics in (3) with control input (5) is called the closed-loop system dynamics

$$x[k+1] = (A_d + B_d K)x[k] + B_d F r. \qquad (6)$$

Stability of a plant and control system depends on the eigenvalues of $(A_d + B_d K)$, which are referred to as the system poles and are denoted by p_i for

$$F = 1/(C_d(\mathbf{I} - A_d - B_d \times K)^{-1} B_d) \qquad (7)$$

三、设计方法学

- 4. Resource-aware automotive control software design. In this section, through examples, we outline how computation-, memory-, and communication-aware control applications may be designed.

三、设计方法学

- 4.1. Computation-aware control systems design

OSEK/VDX-compliant operating systems (OSs), with preemptive fixed-priority scheduling, are widely used in the automotive domain. With such an OS once each application gets released, it is allowed to access the processor periodically.

三、设计方法学

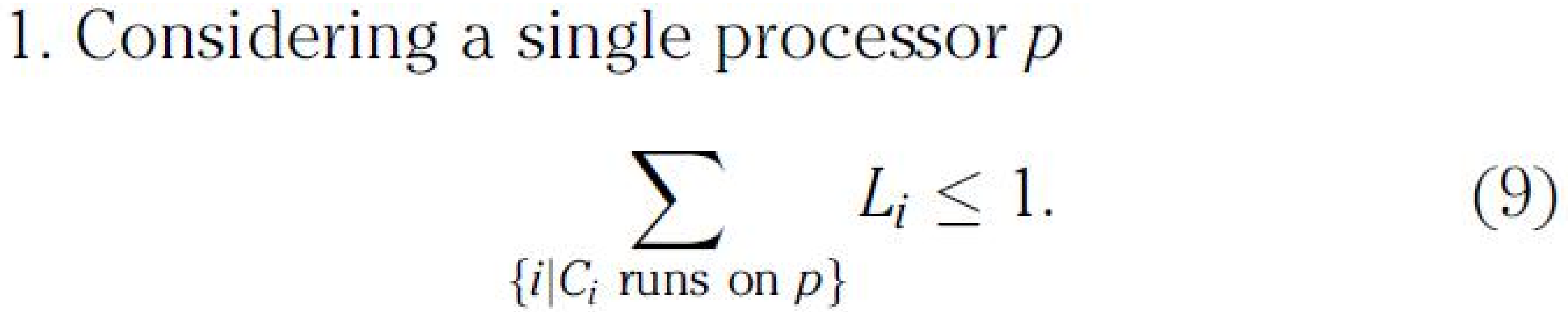
- 4.1. Computation-aware control systems design

Here, a time table containing all the periodic release times within the alleged hyperperiod of the applications needs to be configured.

Generally for a feedback control application, a shorter sampling period allows the controller to respond to its plant more frequently, and is thus potentially able to achieve better QoC. The obvious downside is a higher processor load.

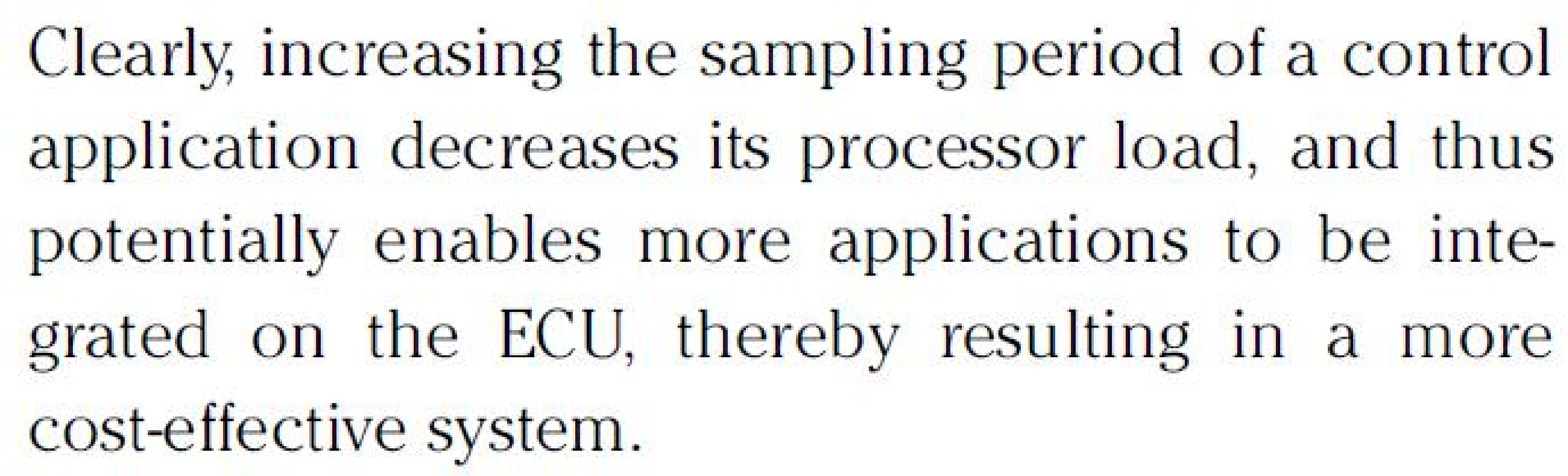
三、设计方法学

- 4.1. Computation-aware control systems design



1. Considering a single processor p

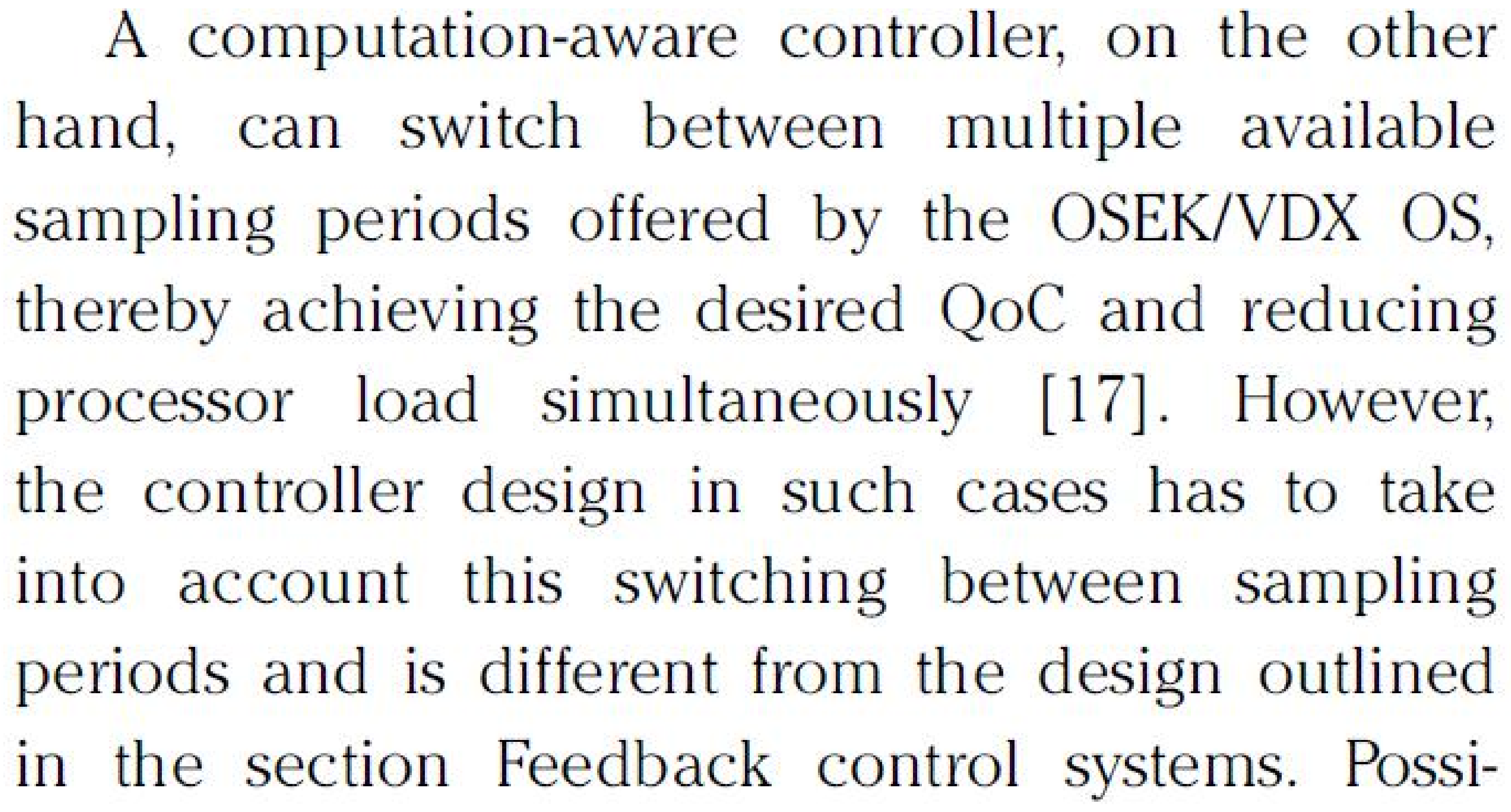
$$\sum_{\{i|C_i \text{ runs on } p\}} L_i \leq 1. \tag{9}$$



Clearly, increasing the sampling period of a control application decreases its processor load, and thus potentially enables more applications to be integrated on the ECU, thereby resulting in a more cost-effective system.

三、设计方法学

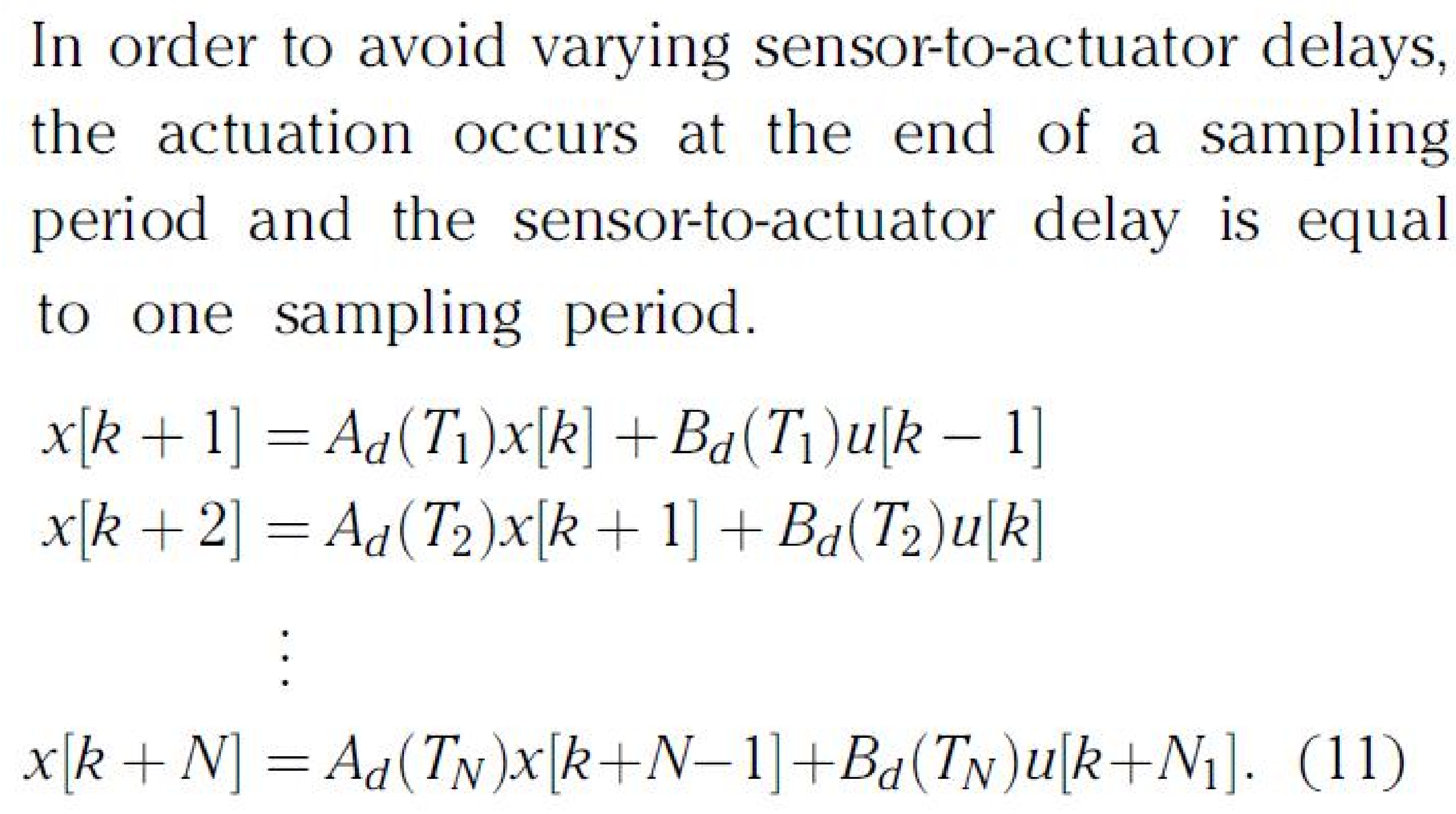
- 4.1. Computation-aware control systems design



A computation-aware controller, on the other hand, can switch between multiple available sampling periods offered by the OSEK/VDX OS, thereby achieving the desired QoC and reducing processor load simultaneously [17]. However, the controller design in such cases has to take into account this switching between sampling periods and is different from the design outlined in the section Feedback control systems. Possi-

三、设计方法学

- 4.1. Computation-aware control systems design

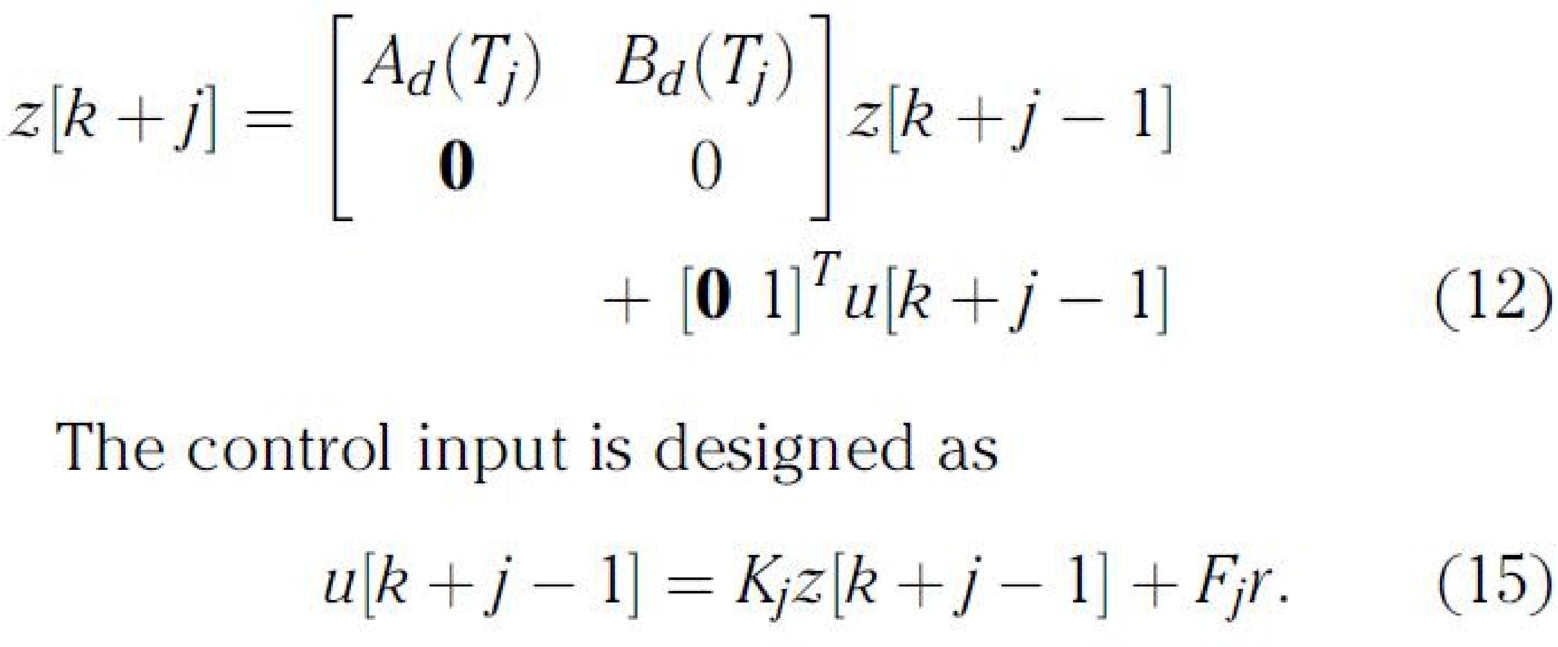


In order to avoid varying sensor-to-actuator delays, the actuation occurs at the end of a sampling period and the sensor-to-actuator delay is equal to one sampling period.

$$
\begin{aligned}
x[k+1] &= A_d(T_1)x[k] + B_d(T_1)u[k-1] \\
x[k+2] &= A_d(T_2)x[k+1] + B_d(T_2)u[k] \\
&\vdots \\
x[k+N] &= A_d(T_N)x[k+N-1] + B_d(T_N)u[k+N_1]. \quad (11)
\end{aligned}
$$

三、设计方法学

- 4.1. Computation-aware control systems design



$$z[k+j] = \begin{bmatrix} A_d(T_j) & B_d(T_j) \\ \mathbf{0} & 0 \end{bmatrix} z[k+j-1] + [\mathbf{0}\ 1]^T u[k+j-1] \qquad (12)$$

The control input is designed as

$$u[k+j-1] = K_j z[k+j-1] + F_j r. \qquad (15)$$

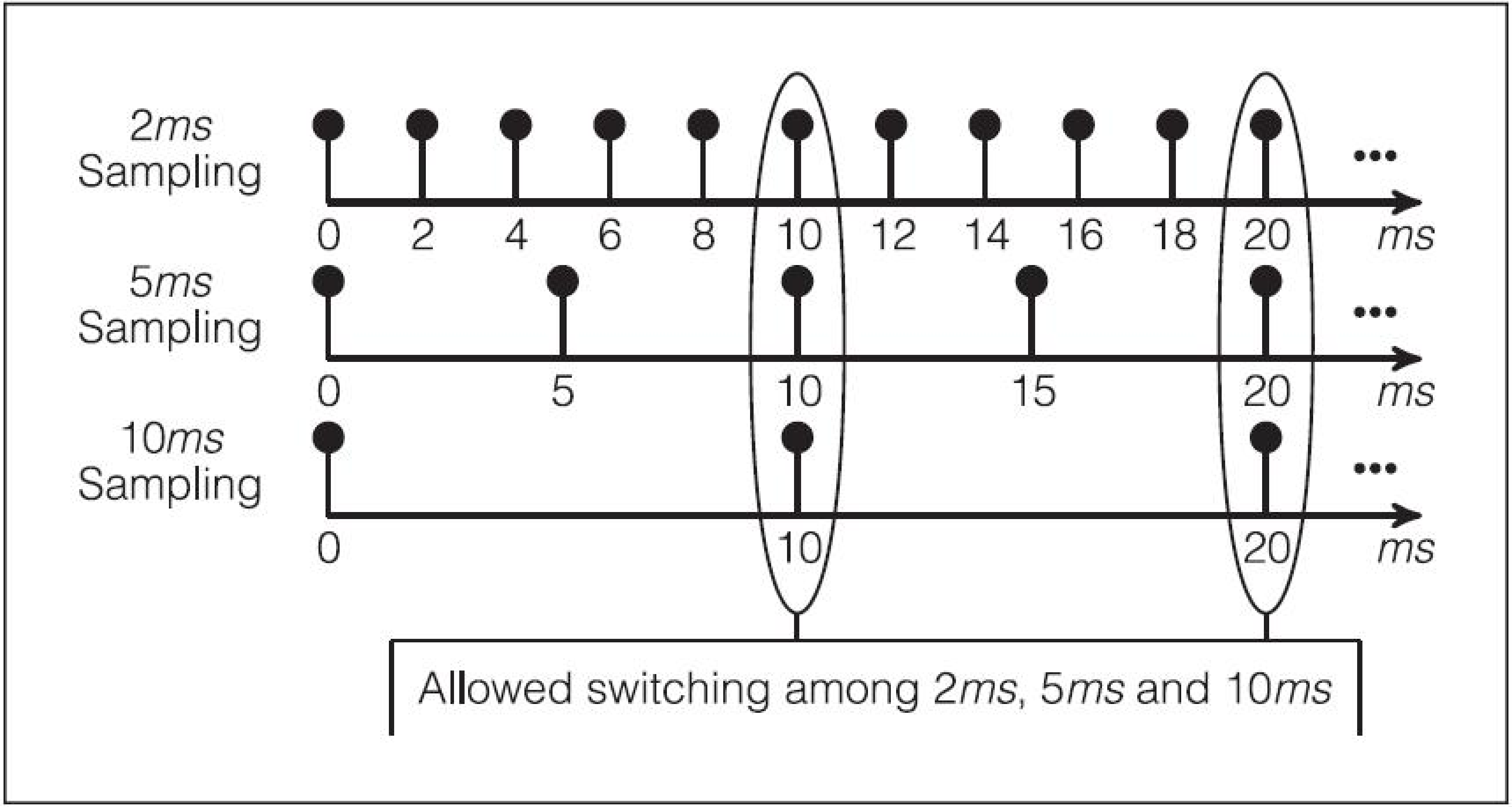


Figure 1. Allowed switching instants among multiple sampling periods.

三、设计方法学

- 4.2. Memory-aware control systems design

  Memory and especially on-chip memory on ECUs substantially increases the ECU cost. In many automotive setups, the code for different control applications is stored in a bigger inexpensive flash memory. Before a particular application is executed, its code is fetched from the flash to the on-chip memory located on the processor. The smaller the on-chip memory is, the more cost effective is the ECU.

三、设计方法学

- 4.2. Memory-aware control systems design

The question is, following a CPS approach, can the control algorithms be designed to mitigate such delays and exploit this memory hierarchy?

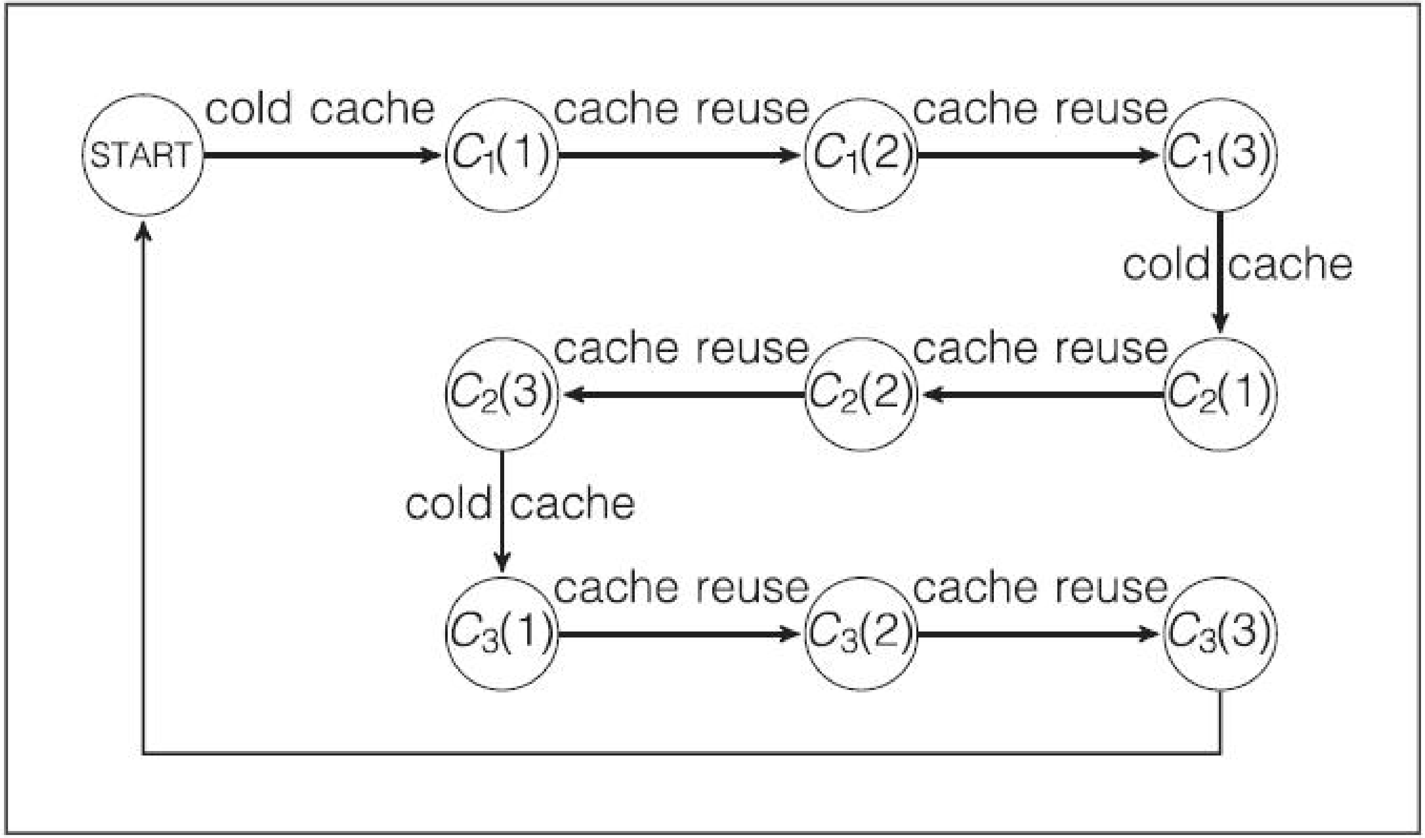


Figure 3. Each application is consecutively executed three times. After the first execution $C_i(1)$, some instructions in the cache can be reused and thus the WCETs of the following two executions are shortened, resulting in improved QoC.

三、设计方法学

- 4.3. Communication-aware control systems design

FlexRay supports both time-triggered (TT) and event-triggered (ET) or priority-based communication schemes. When the characteristics of the communication bus are not considered during the controller design phase, the controller is designed with assumptions on timing parameters like sampling periods and sensor-to-actuator delays.

三、设计方法学

- 4.3. Communication-aware control systems design

In FlexRay, the TT communication has deterministic timing behavior and results in a *constant message delay*, whereas the delay suffered by messages mapped onto the ET segment *varies*. There is a tradeoff between the number of TT slots used and the QoC.

三、设计方法学

- 4.3. Communication-aware control systems design

Hence, configuring the FlexRay parameters appropriately—to ensure certain message delay constraints—and mapping all control messages to the TT segment is a straightforward solution.

三、设计方法学

- 4.3. Communication-aware control systems design

However, TT slots are considered to be more expensive and the question is: Given a set of control applications and their corresponding control signals, can good QoC be achieved by using fewer TT slots compared to when all messages are mapped to TT slots?

三、设计方法学

- 4.3. Communication-aware control systems design

In what follows, we describe a scheme that realizes this. Here, control messages are switched between TT and ET slots. This protocol is illustrated in Figure 4.

三、设计方法学

- 4.3. Communication-aware control systems design

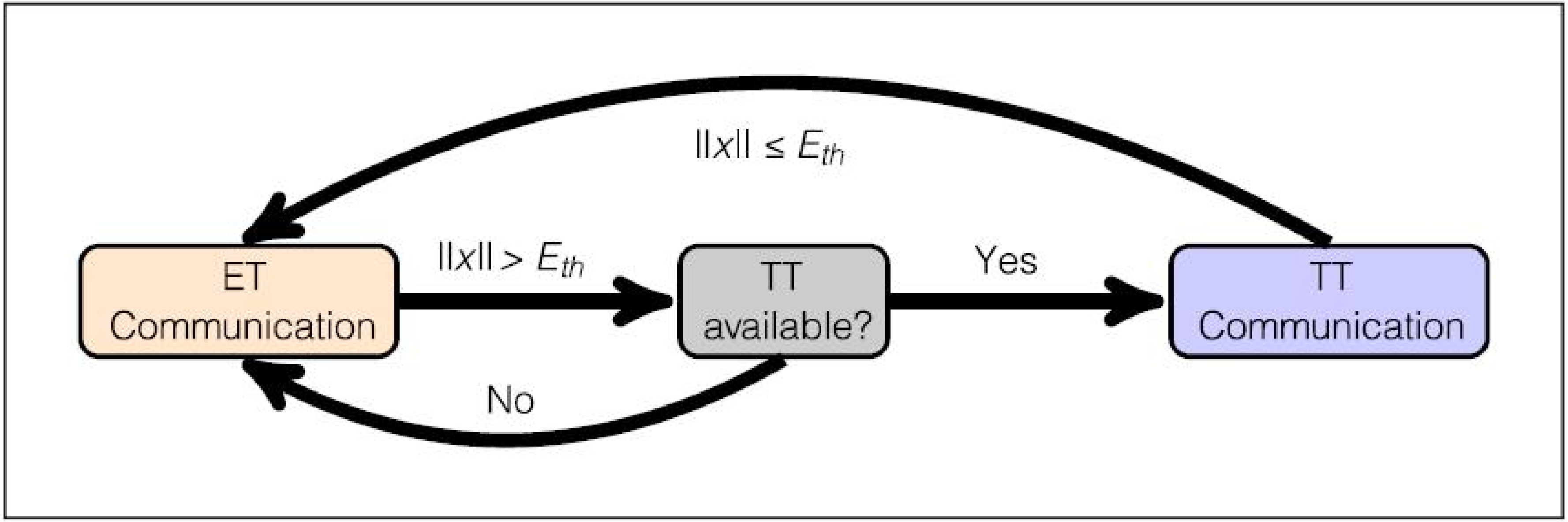


Figure 4. The hybrid communication protocol.

三、设计方法学

- 4.3. Communication-aware control systems design

In addition, the interaction between communication and control theory has attracted a lot of attention in general, and also in the context of invehicle communication protocols. One of the issues here is to quantify the tolerable message loss/delay in the case of distributed controller implementations, while still maintaining control quality.

三、设计方法学

5. Battery- and reliability-aware controllers

5.1. Co-optimizing QoC and battery usage

5.2. Semiconductor aging effects

5.3. Illustrative results: Electric motor control

6. Automotive climate control

三、设计方法学

7. Cyber–physical automotive security

With increasing vehicle intelligence and connectivity, security and privacy have become pressing concerns for automotive systems. In this section, we will discuss automotive security challenges and the importance of using cyber–physical approaches to address them.

三、设计方法学

7. Cyber–physical automotive security

Researchers have shown that modern vehicles can be attacked from a variety of interfaces including physical access such as OBD-II and USB, short-range wireless such as Bluetooth, remote keyless entry, tire (轮胎) pressure sensors and RFID (无线射频识别) car keys, and long-range wireless channels such as broadcast channels and addressable channels.

三、设计方法学

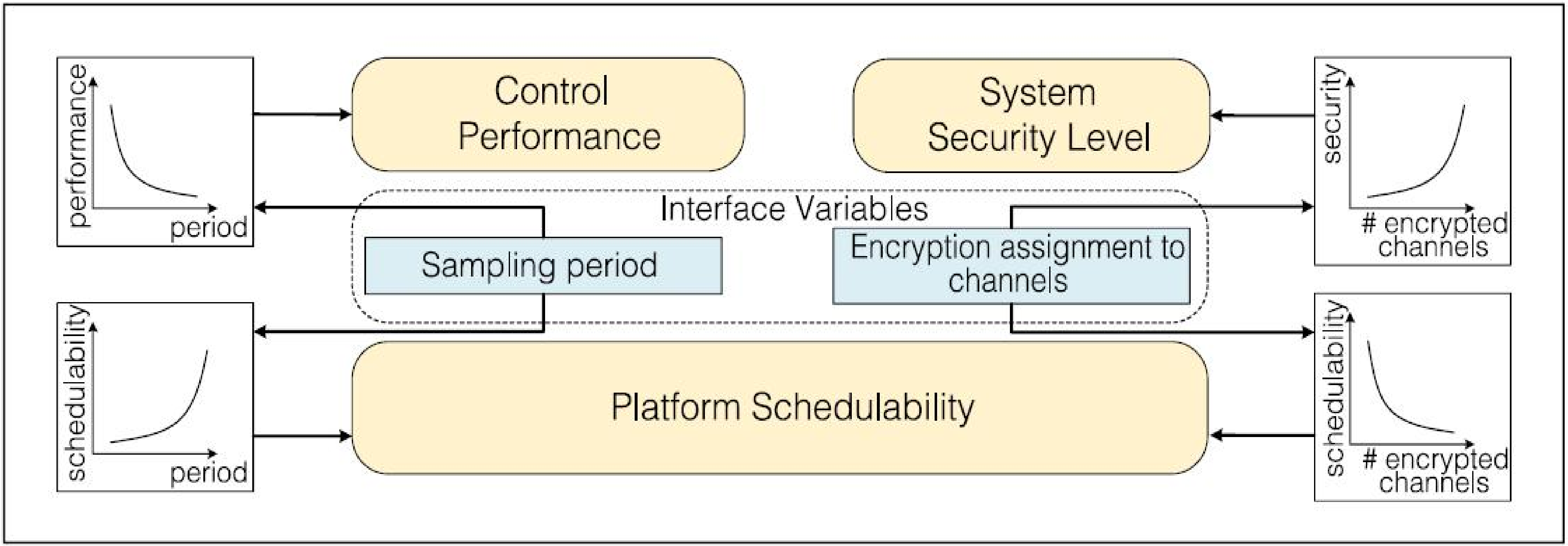
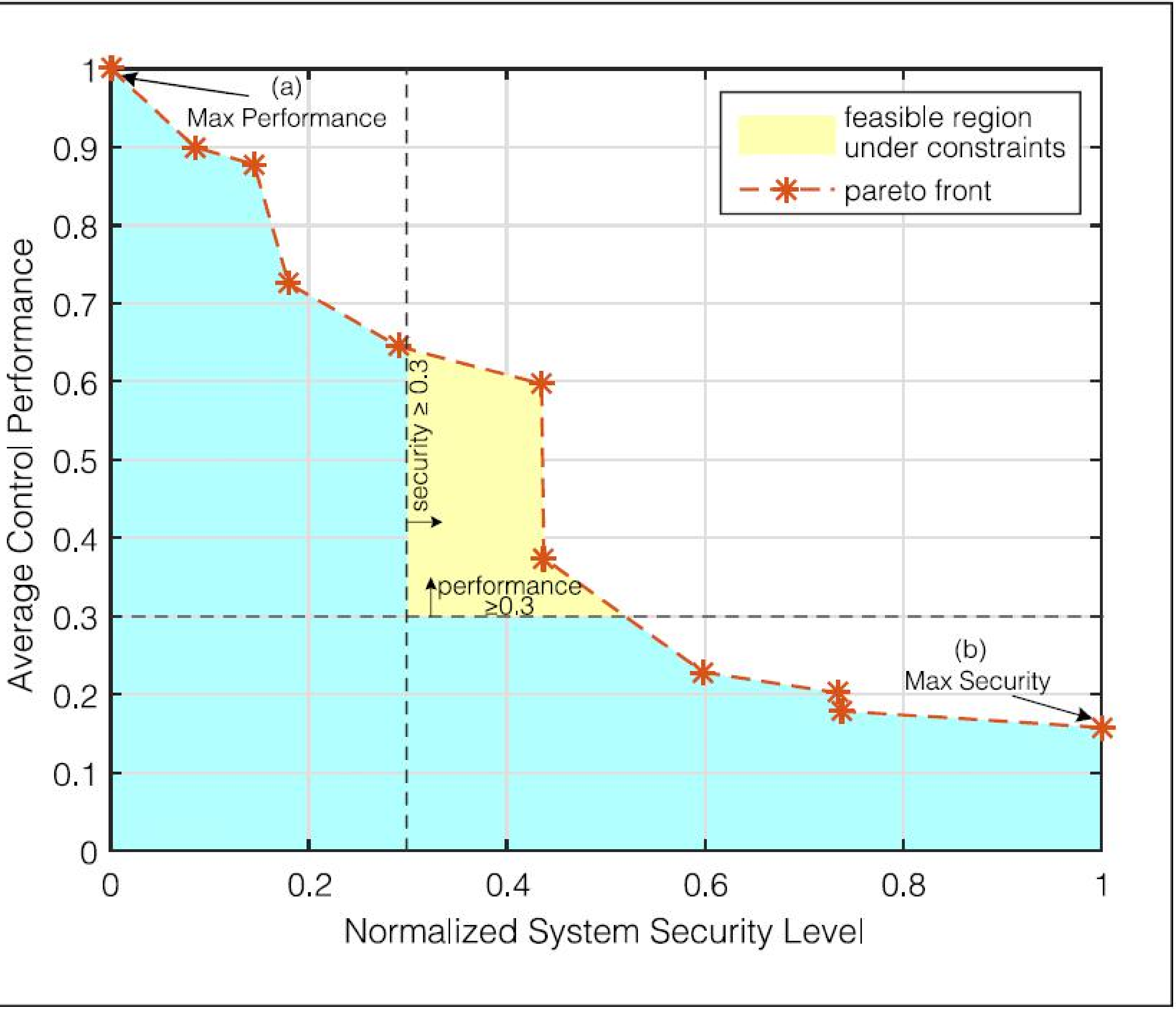


Figure 10. Control and platform codesign for secure cyber-physical systems.


Average Control Performance
Normalized System Security Level
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
0.2
0.4
0.6
0.8
1
(a)
Max Performance
(b)
Max Security
security ≥ 0.3
performance
≥0.3
feasible region
under constraints
pareto front

The end!