ECRTS 2018
3-6 July
Barcelona, Spain

AdaptMC

A Control-Theoretic Approach for Achieving Resilience in Mixed-Criticality Systems

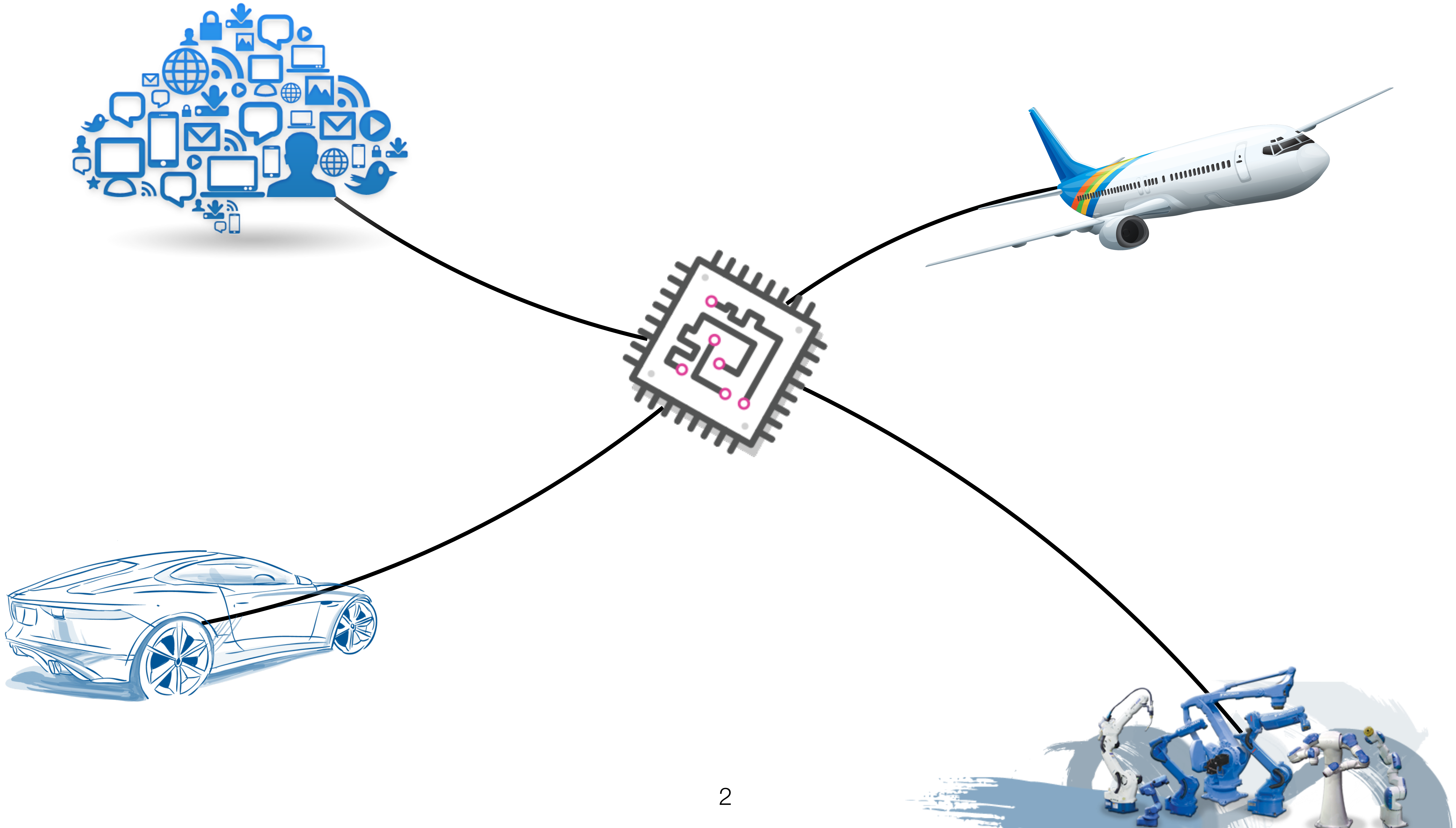
Alessandro V. Papadopoulos, Enrico Bini, Sanjoy Baruah, Alan Burns

MÄLARDALEN UNIVERSITY SWEDEN

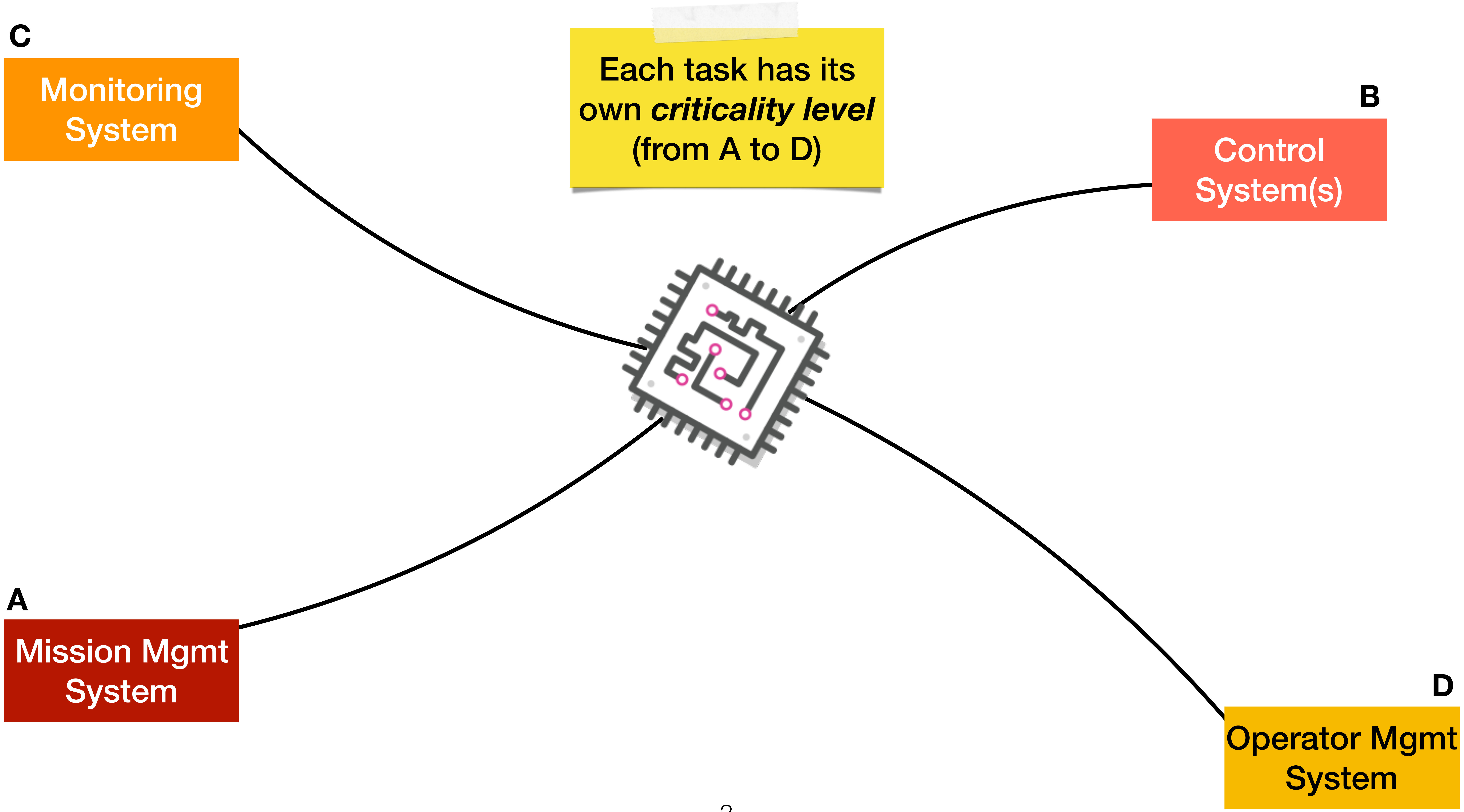
Washington University in St. Louis

UNIVERSITY of York

Embedded system



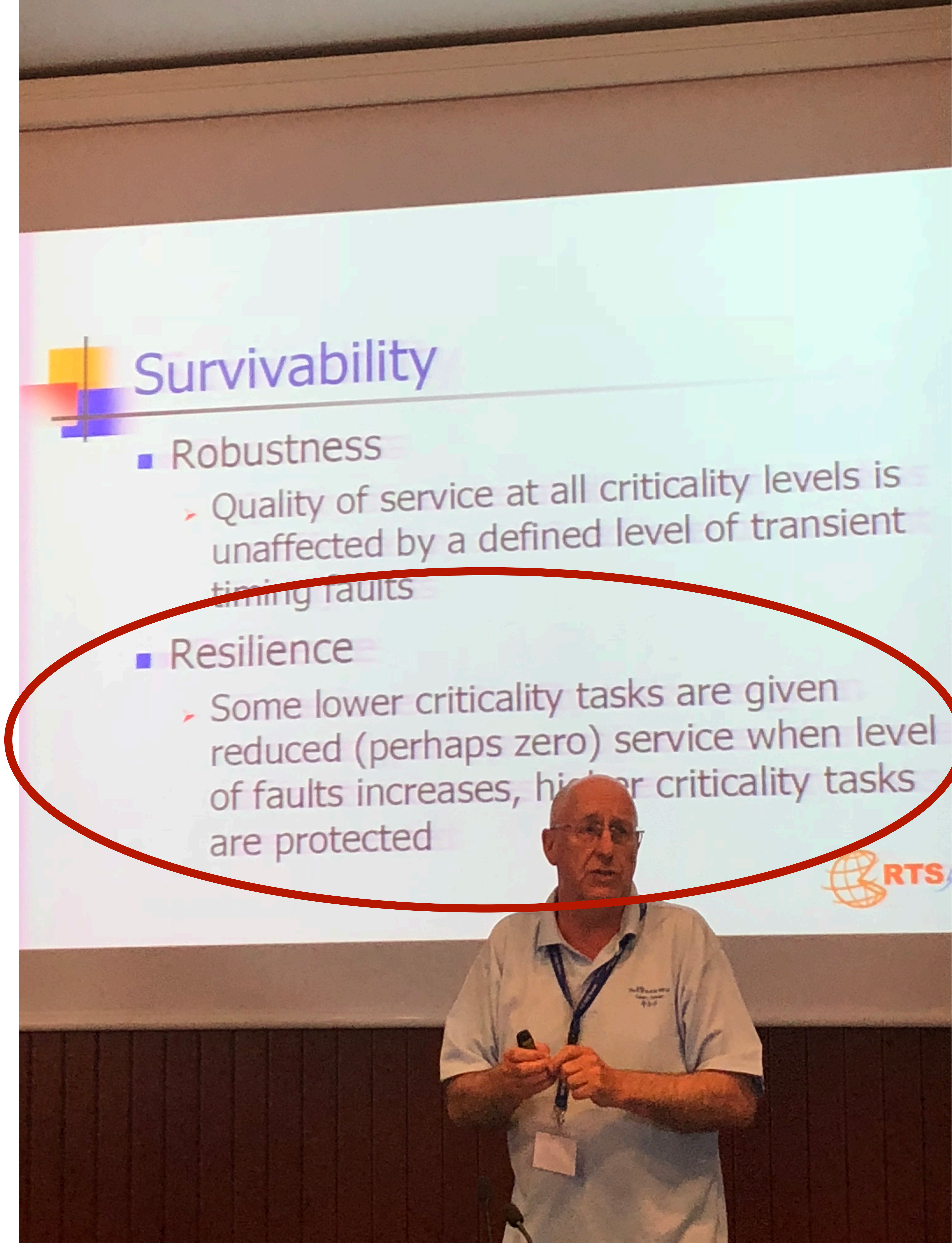
Mixed-criticality system



Vestal model

- Fixed number of distinct criticality levels are defined throughout the system
  - **LO and HI criticality**
- Each piece of code in the system is characterised by
  - The **criticality level** (LO/HI)
  - Two **WCET parameter *estimates***
- *Prior to run-time* the timing behaviour of all functionalities is validated ***according to the WCET parameter estimates***

What does happen at run-time if the WCET estimates are “wrong”?



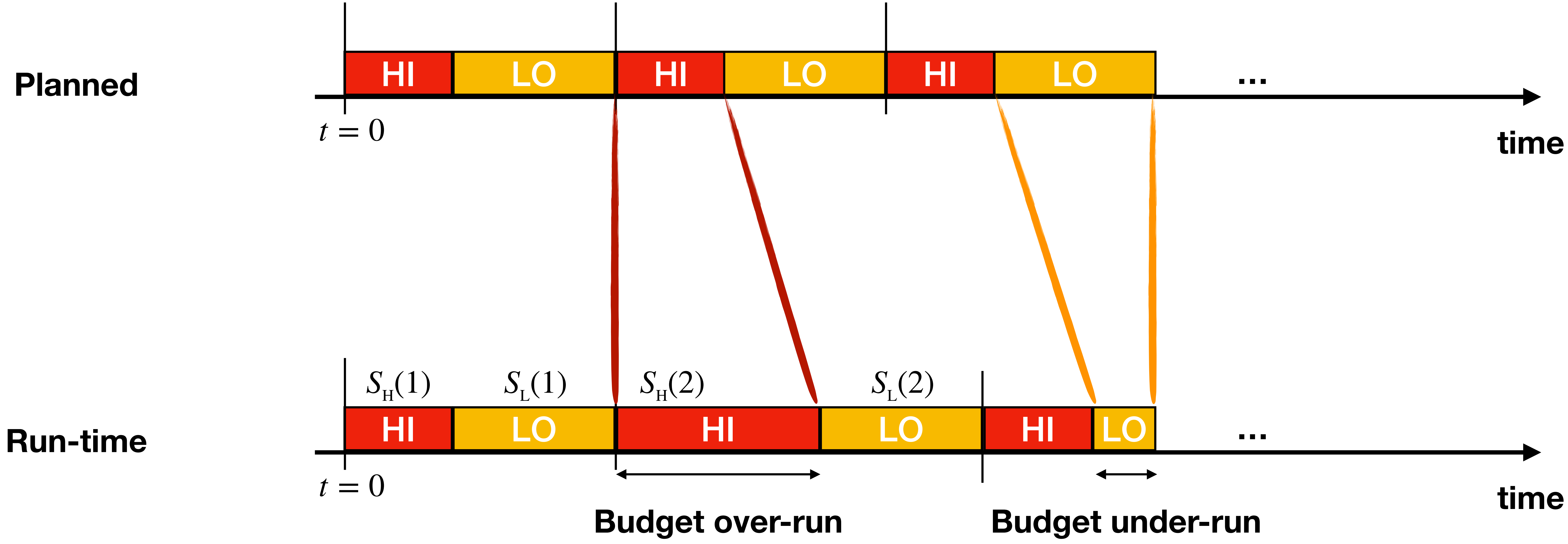
Goals of this paper

- Shift the perspective **from verification to resiliency**
  - What happens when a budget over-run occurs?
- Analyse a control-based approach for **ensuring run-time resiliency**
  - How to adapt the behaviour at run-time?
- Provide **hard real-time guarantees** even with budget over- or under-runs
  - Is it possible to provide such guarantees?

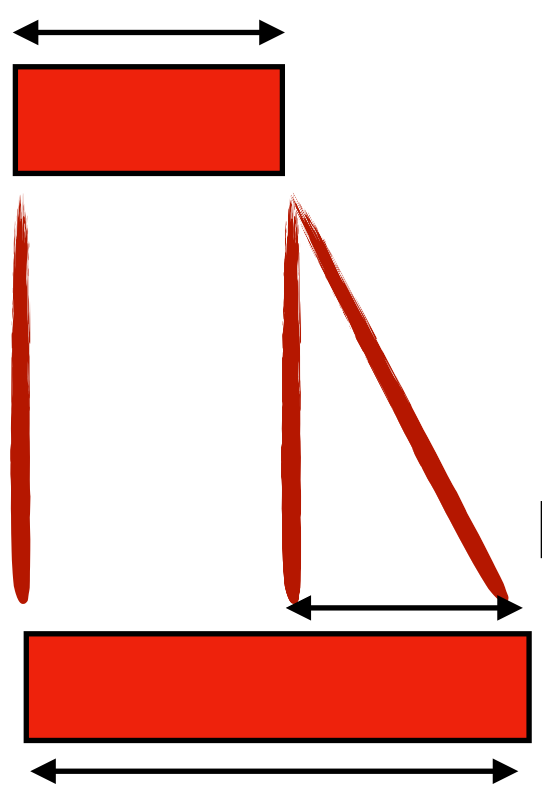
Outline

- **AdaptMC**: Control-based approach for run-time adaptation
- Evaluation
- Conclusion

Definitions



Definitions and assumptions

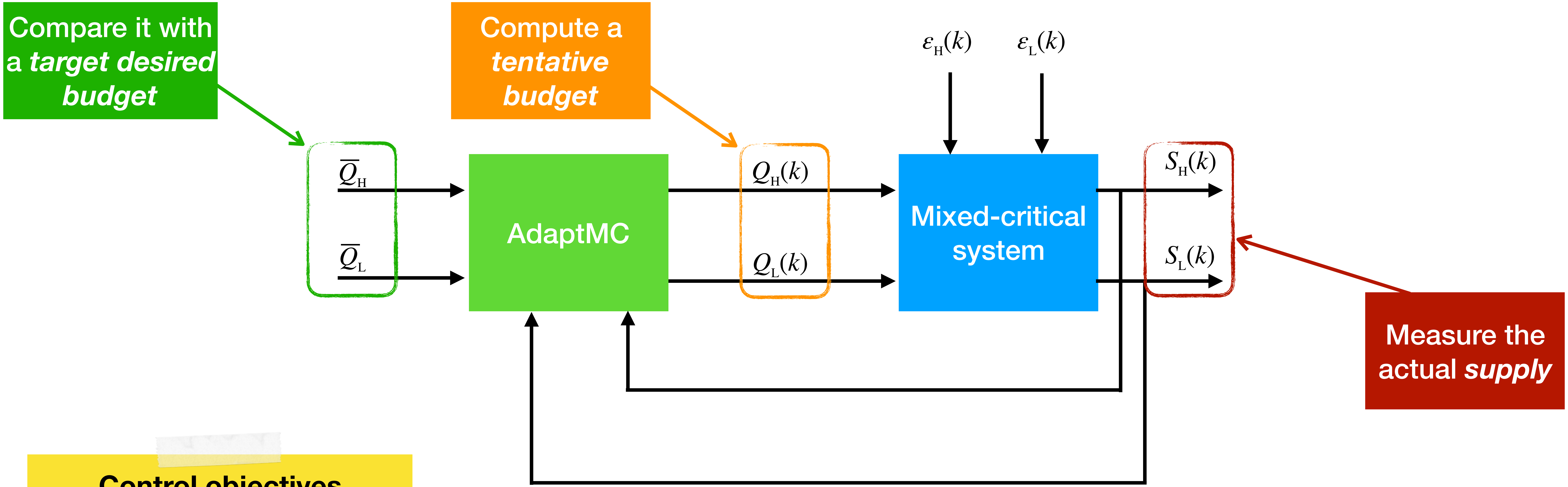


$$S_H(k+1) = Q_H(k) + \varepsilon_H(k)$$
$$S_L(k+1) = Q_L(k) + \varepsilon_L(k)$$

- Assumptions
  1. Executions **rarely** exceed the WCET values
  2. When they do, it is by a "**small amount**"
  3. The "small amount" can be **bounded**

$$-\bar{\varepsilon}_H \leq \varepsilon_H \leq \bar{\varepsilon}_H$$
$$-\bar{\varepsilon}_L \leq \varepsilon_L \leq 0$$

AdaptMC: Control-based approach



Control objectives

- Meet the target desired budgets
- Preserve the bandwidth of the HI and LO critical systems

Deeper in AdaptMC

- The controller adjusts the tentative budgets

$$Q_H(k+1) = Q_H(k) + u_H(k)$$
$$Q_L(k+1) = Q_L(k) + u_L(k)$$

- Based on the **actual supply** and the **target budget**

$$u_H(k) = K_{HH}(\overline{Q}_H - S_H(k)) + \frac{K_{HL}}{\gamma}(\overline{Q}_L - S_L(k))$$
$$u_L(k) = \gamma K_{LH}(\overline{Q}_H - S_H(k+1)) + K_{LL}(\overline{Q}_L - S_L(k))$$

- with $\gamma = \frac{\overline{Q}_L}{\overline{Q}_H}$

Design parameters

Required properties

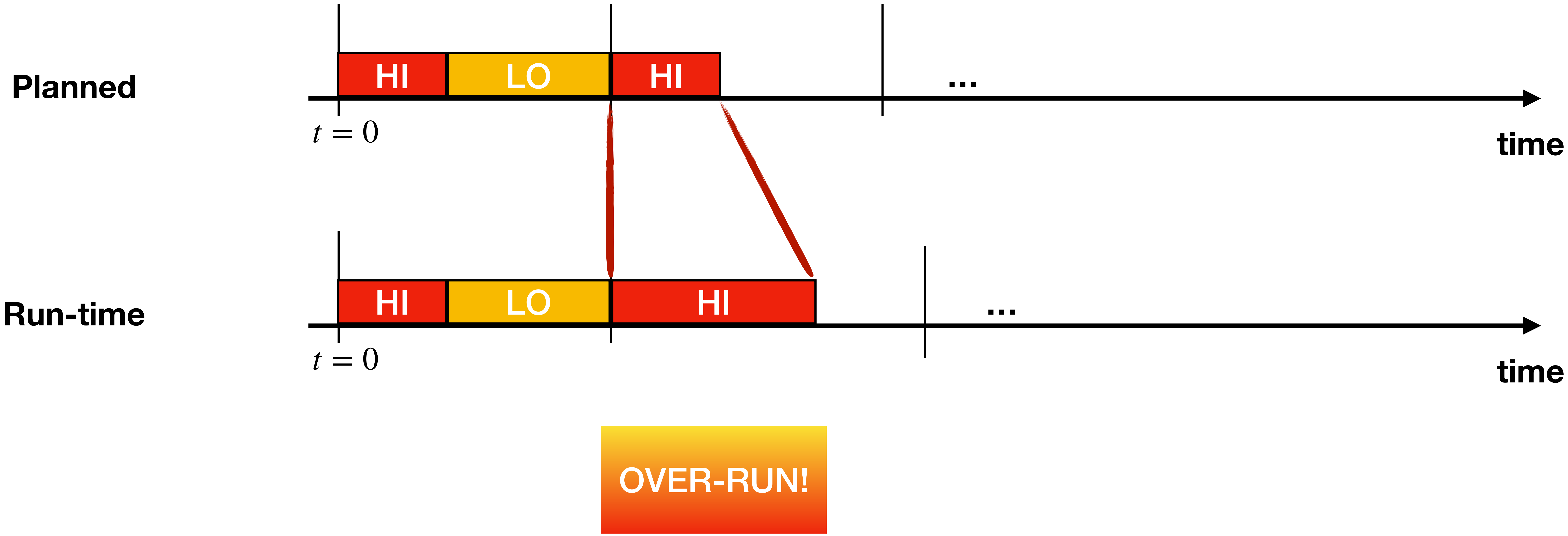
1. **Compensation property**

2. **Stability of the closed-loop system**

3. **Bounding the resource supply**

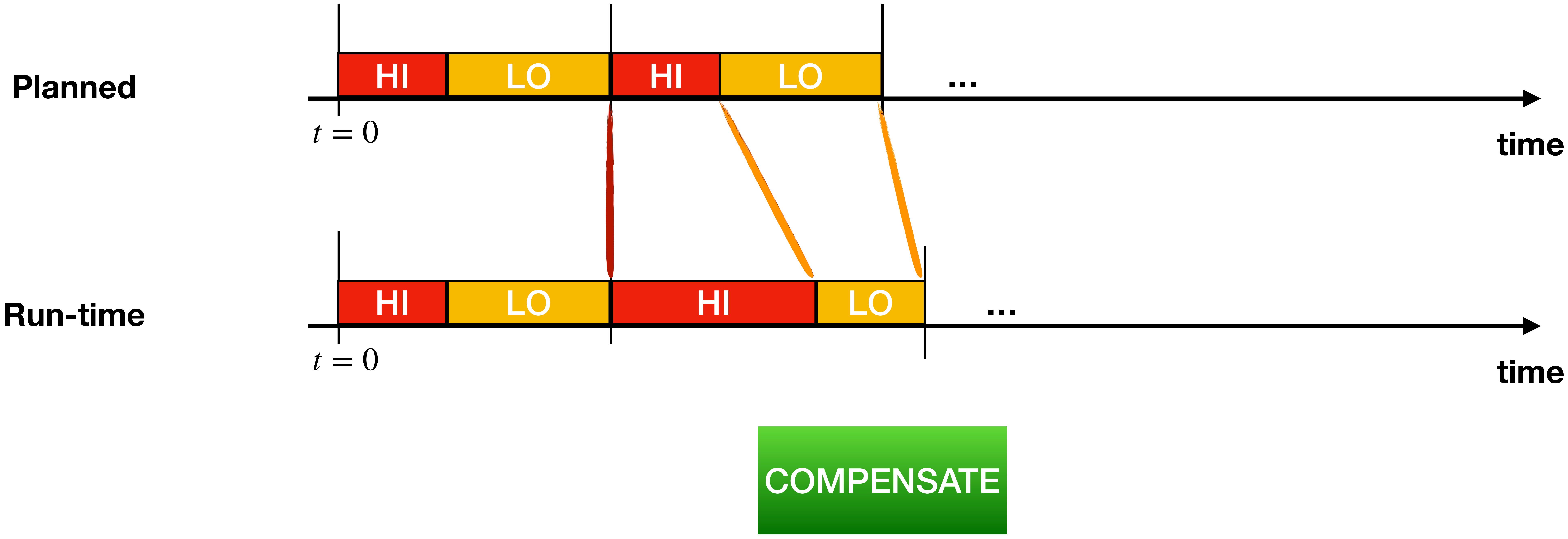
Compensation property

- A disturbance on the HI/LO-criticality server results in an opposite or null effect on the value of the supply of the LO/HI-criticality server

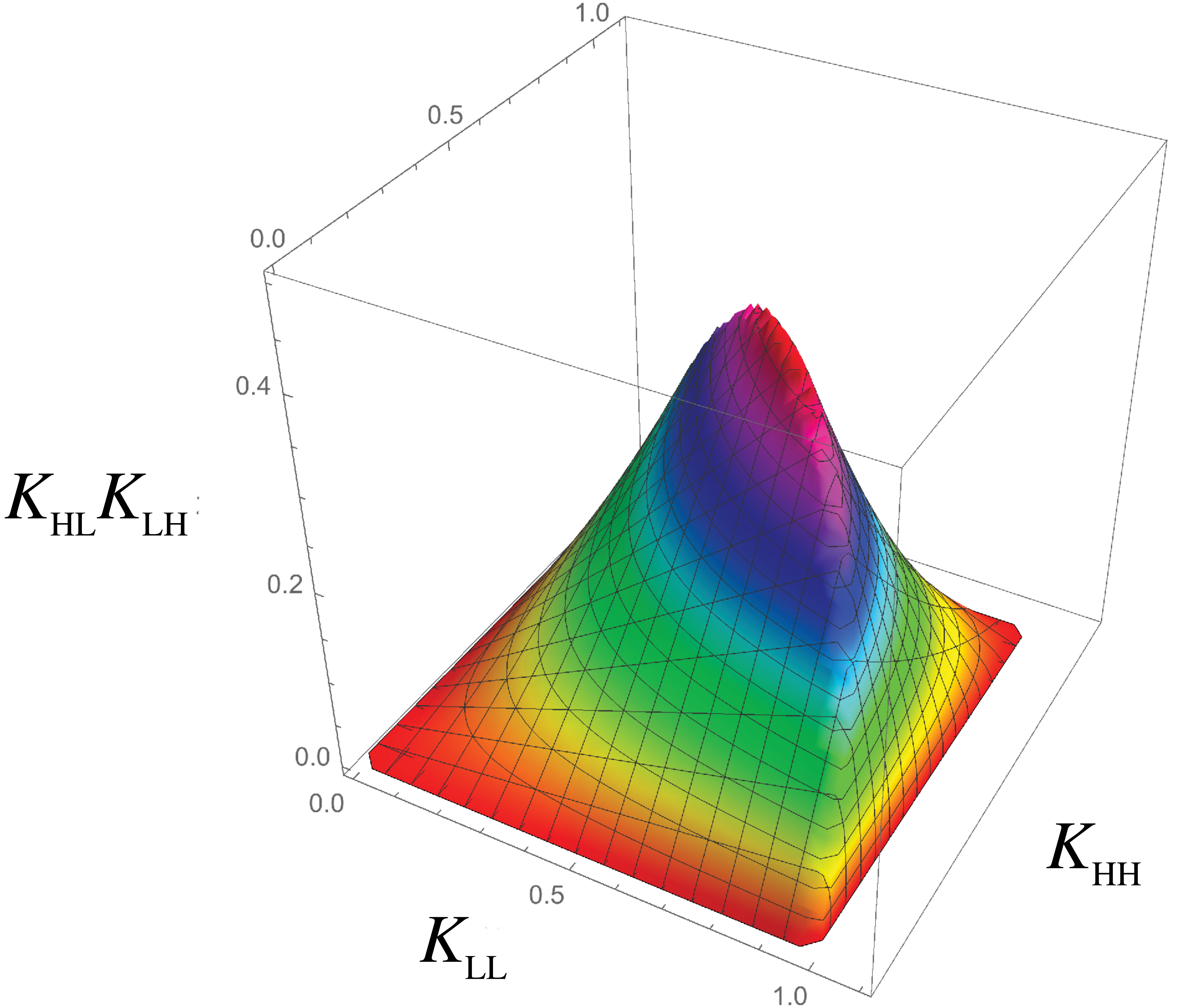


Compensation property

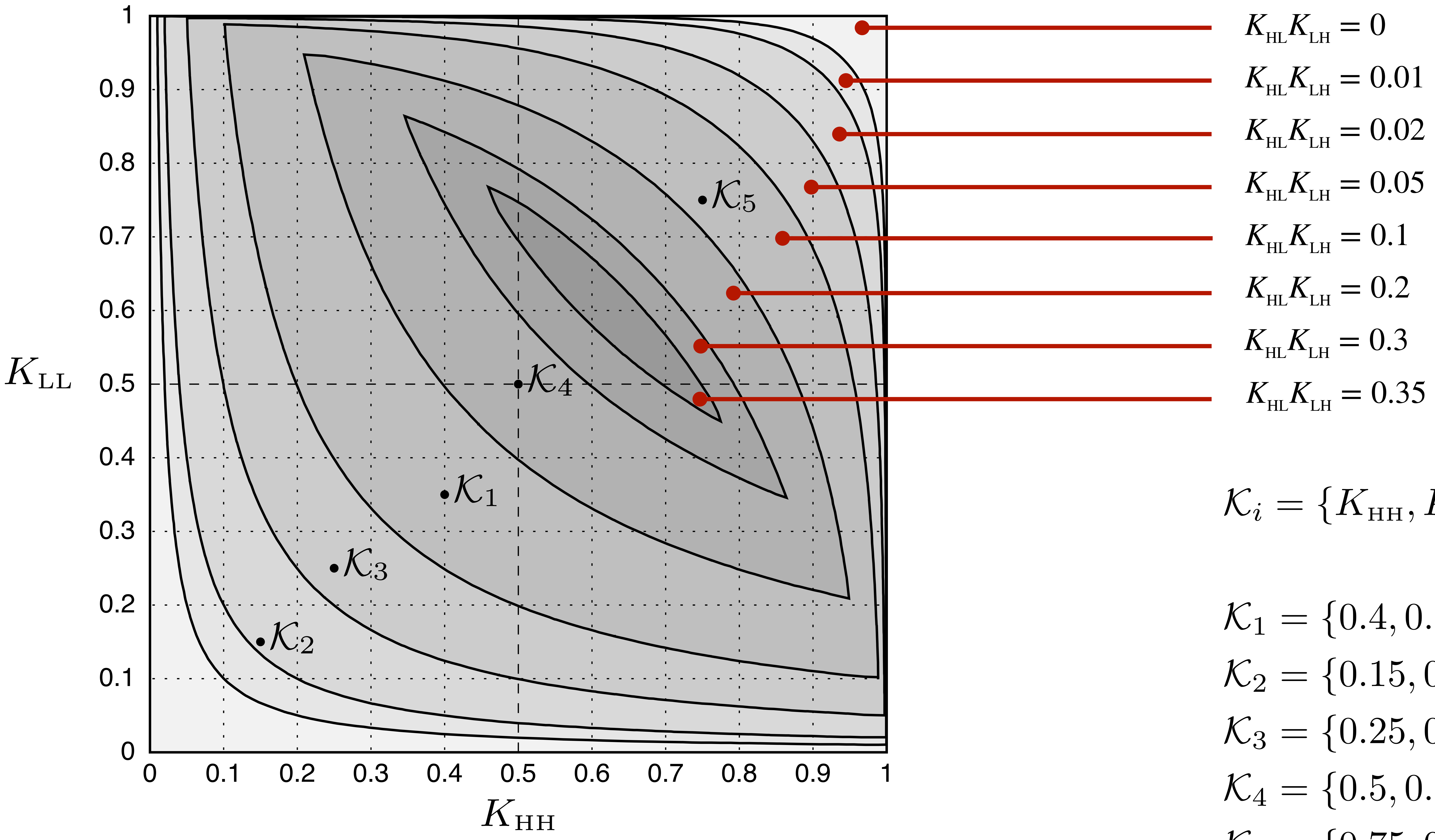
- A disturbance on the HI/LO-criticality server results in an opposite or null effect on the value of the supply of the LO/HI-criticality server



Stability



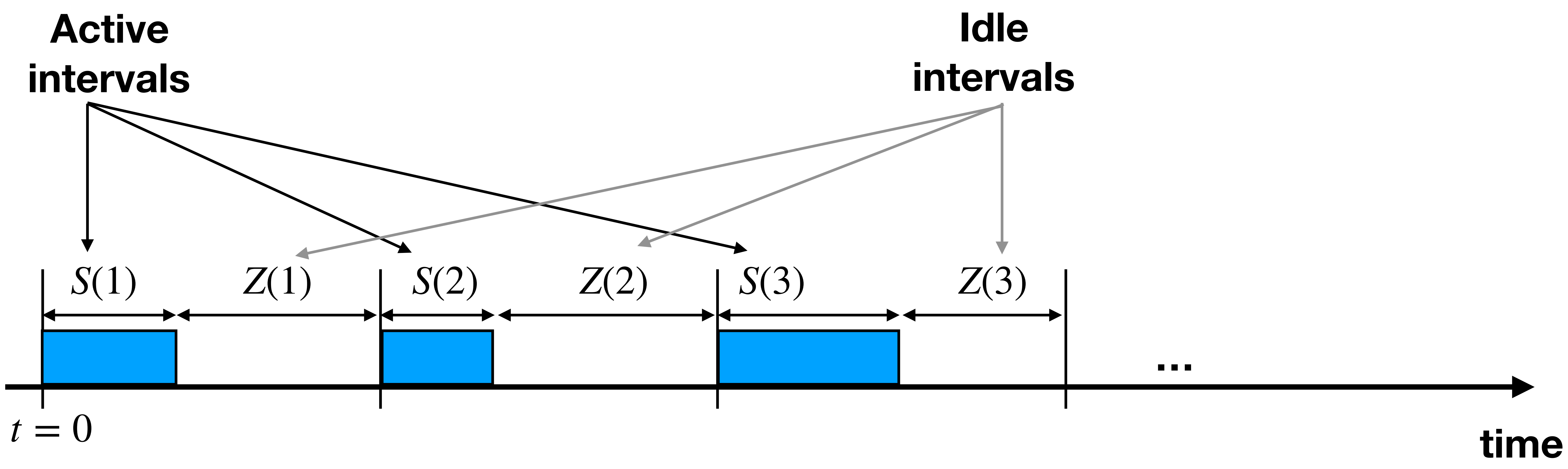
Stability



$$\mathcal{K}_i = \{K_{HH}, K_{HL}, K_{LH}, K_{LL}\}$$

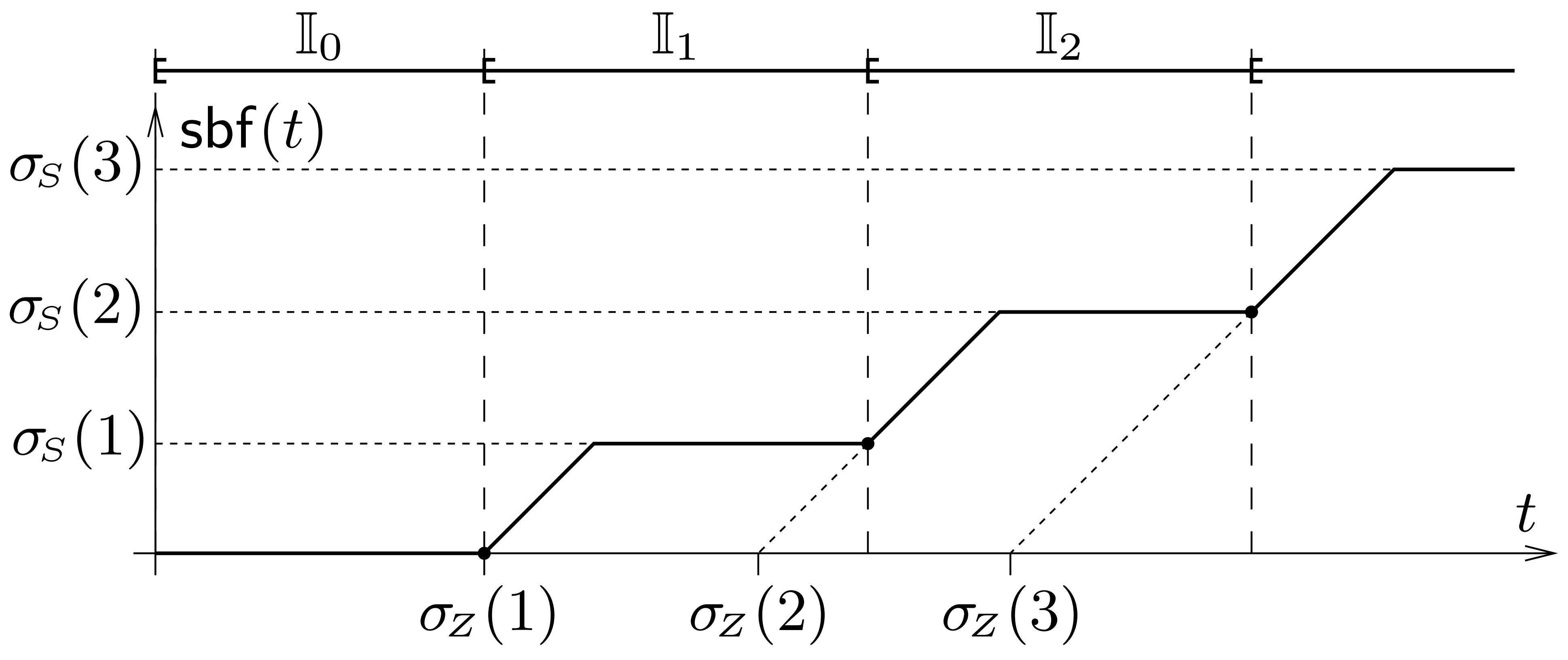
$$\mathcal{K}_1 = \{0.4, 0.1, 0.1, 0.35\}$$
$$\mathcal{K}_2 = \{0.15, 0.1, 0.1, 0.15\}$$
$$\mathcal{K}_3 = \{0.25, 0.1, 0.1, 0.25\}$$
$$\mathcal{K}_4 = \{0.5, 0.1, 0.1, 0.5\}$$
$$\mathcal{K}_5 = \{0.75, 0.1, 0.1, 0.75\}$$

Bounding the resource supply



$$\sigma_S(n) = \inf_{n_0} \sum_{k=n_0}^{n_0+n-1} S(k)$$

$$\sigma_Z(n) = \sup_{n_0} \sum_{k=n_0}^{n_0+n-1} Z(k)$$



Bounding the resource supply

$$\sigma_S(n) = \inf_{n_0} \sum_{k=n_0}^{n_0+n-1} S(k)$$

$$\sigma_Z(n) = \sup_{n_0} \sum_{k=n_0}^{n_0+n-1} Z(k)$$

HI-Criticality

$$\sigma_S(n) = n\overline{Q}_{\mathrm{H}} - \bar{\varepsilon}_{\mathrm{H}}\mathcal{N}_{\mathrm{HH}}(n) - \frac{\bar{\varepsilon}_{\mathrm{L}}}{2}\left(\mathcal{I}_{\mathrm{HL}}(n) + \mathcal{N}_{\mathrm{HL}}\right)$$

$$\sigma_Z(n) = n\overline{Q}_{\mathrm{L}} + \bar{\varepsilon}_{\mathrm{H}}\mathcal{N}_{\mathrm{LH}}(n) + \frac{\bar{\varepsilon}_{\mathrm{L}}}{2}\left(\mathcal{J}_{\mathrm{LL}}(n) + \mathcal{N}_{\mathrm{LL}}\right)$$

LO-Criticality

$$\sigma_S(n) = n\overline{Q}_{\mathrm{L}} - \bar{\varepsilon}_{\mathrm{H}}\mathcal{N}_{\mathrm{LH}}(n) - \frac{\bar{\varepsilon}_{\mathrm{L}}}{2}\left(\mathcal{I}_{\mathrm{LL}}(n) + \mathcal{N}_{\mathrm{LL}}\right)$$

$$\sigma_Z(n) = n\overline{Q}_{\mathrm{H}} + \bar{\varepsilon}_{\mathrm{H}}\mathcal{N}_{\mathrm{HH}}(n) + \frac{\bar{\varepsilon}_{\mathrm{L}}}{2}\left(\mathcal{J}_{\mathrm{HL}}(n) + \mathcal{N}_{\mathrm{HL}}\right)$$

with

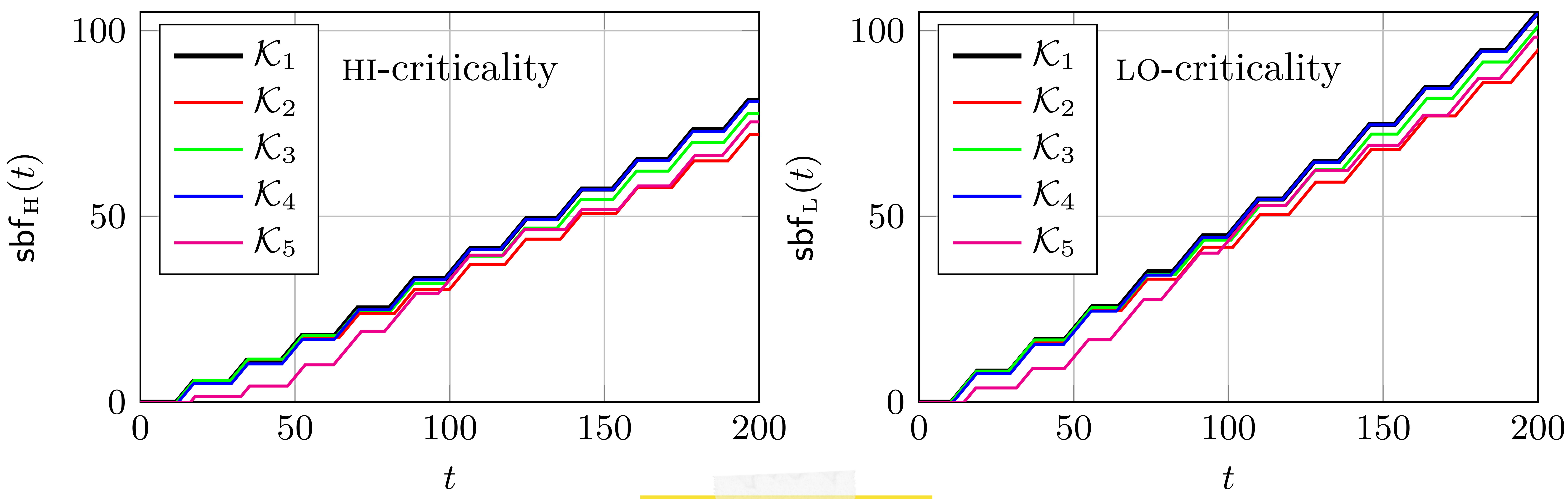
$$\mathcal{N}_{ij}(n) = \sum_{k=0}^{\infty} |g_{ij}(k) - g_{ij}(k-n)|$$

$$\mathcal{I}_{i\mathrm{L}}(n) = \sup_k \left\{r_{i\mathrm{L}}(k) - r_{i\mathrm{L}}(k-n)\right\}$$

$$\mathcal{J}_{i\mathrm{L}}(n) = \sup_k \left\{r_{i\mathrm{L}}(k-n) - r_{i\mathrm{L}}(k)\right\}$$

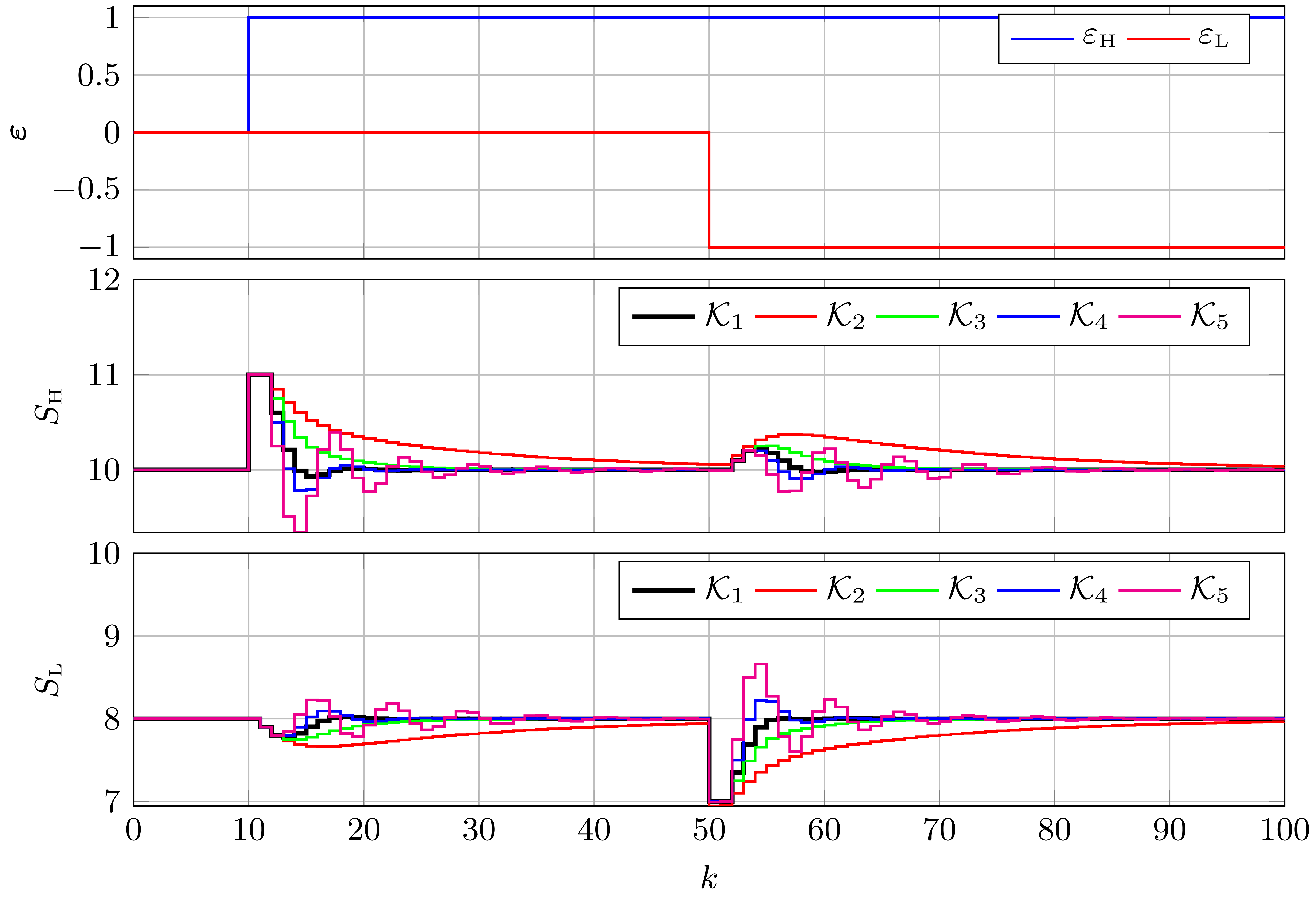
Proof and details in the paper

Evaluation — sbf



K_1 maximises both the sbf

Evaluation — Transient behaviour



K_1 minimises the effect of the transient behaviour

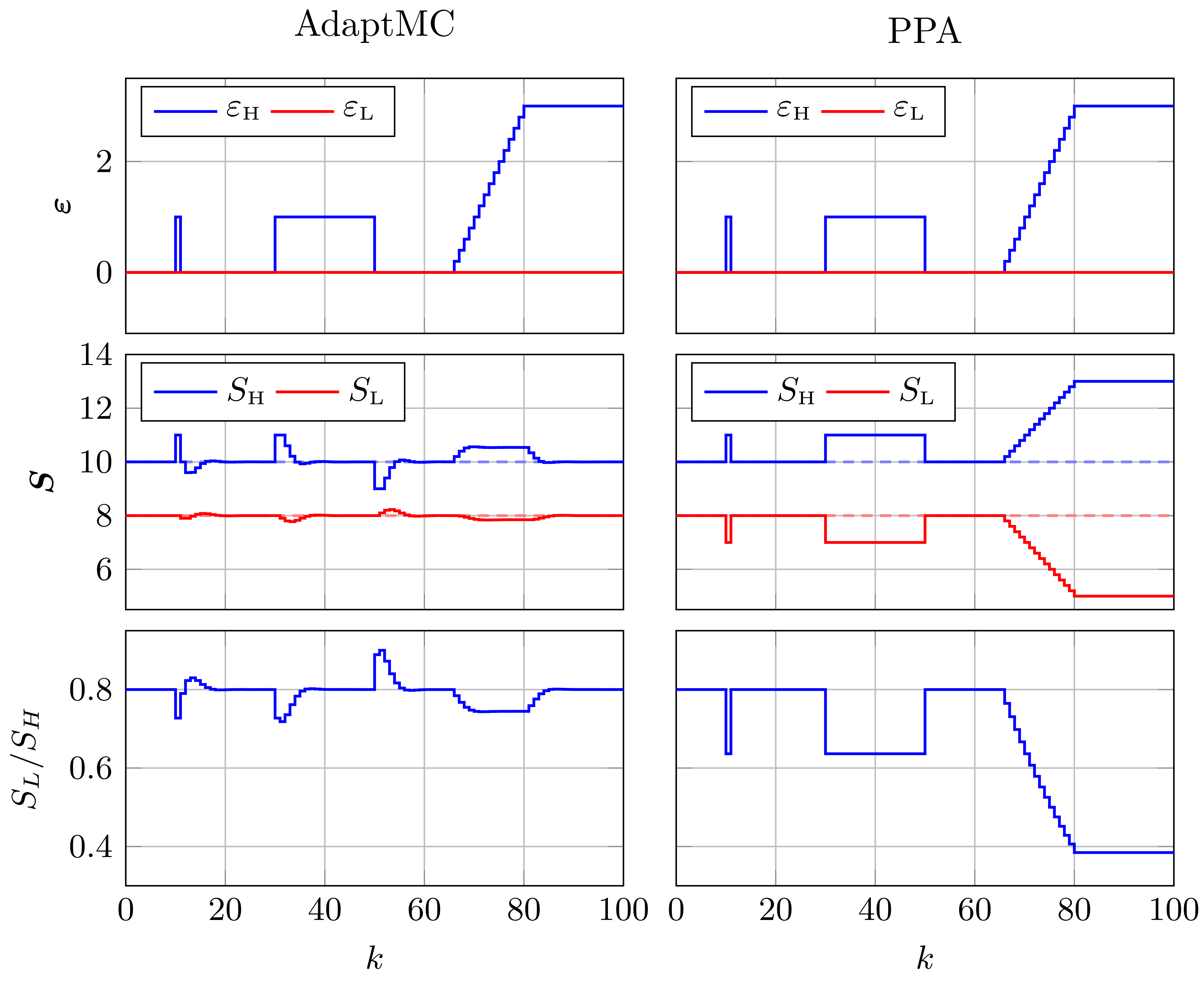
Baseline for comparison — PPA

- Period-Preserving Approach (PPA)
  - Simple approach
  - When HI-criticality over-run, the LO-criticality server compensate by preserving the period

$$S_H(k+1) = \overline{Q}_H + \varepsilon_H(k)$$
$$S_L(k+1) = \max(P - S_H(k+1), 0) + \varepsilon_L(k)$$

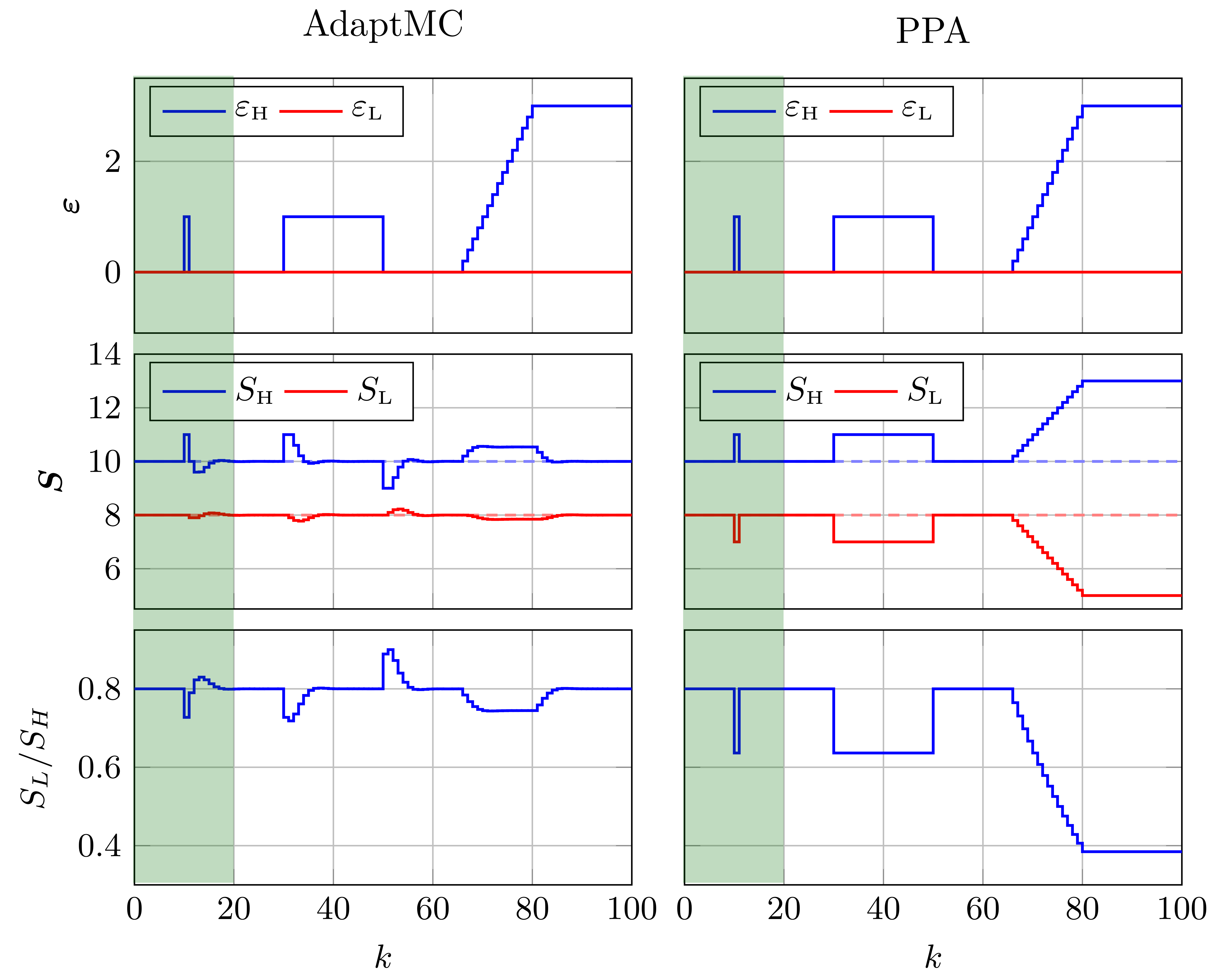
- where *P* is the target period that needs to be maintained

Comparative results



Comparative results

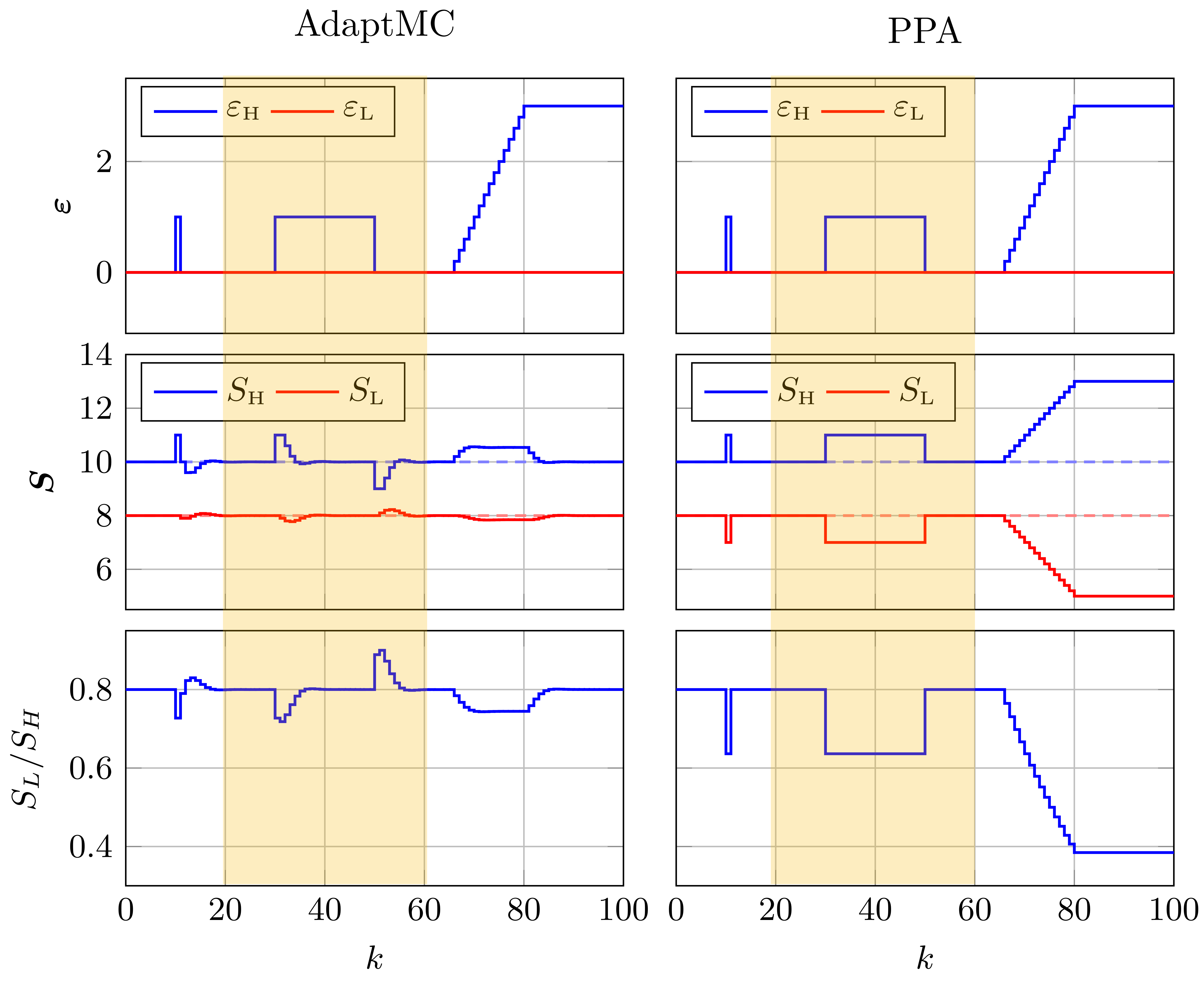
Impulsive disturbance



Comparative results

Impulsive disturbance

Constant disturbance

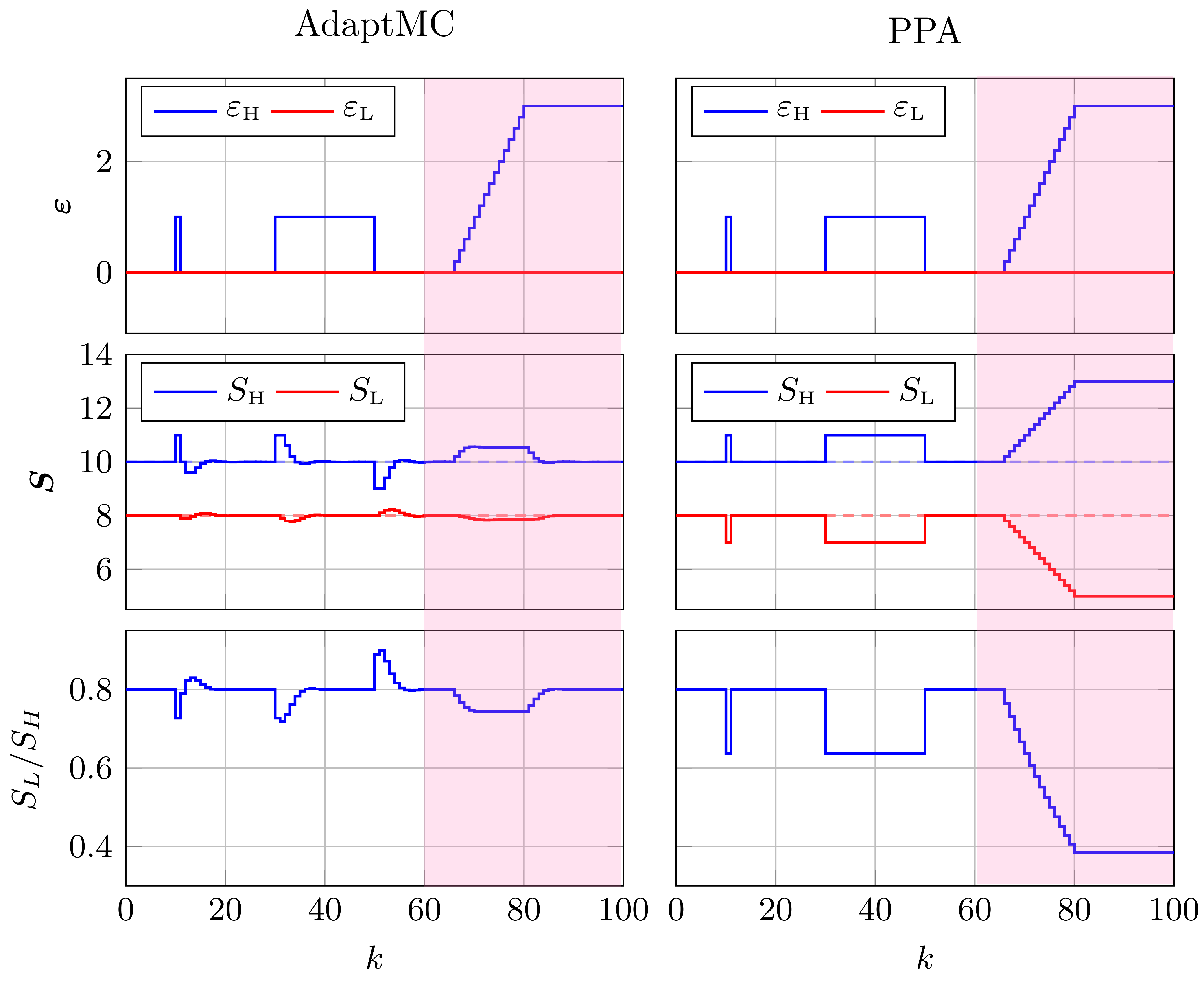


Comparative results

Impulsive disturbance

Constant disturbance

Increasing disturbance

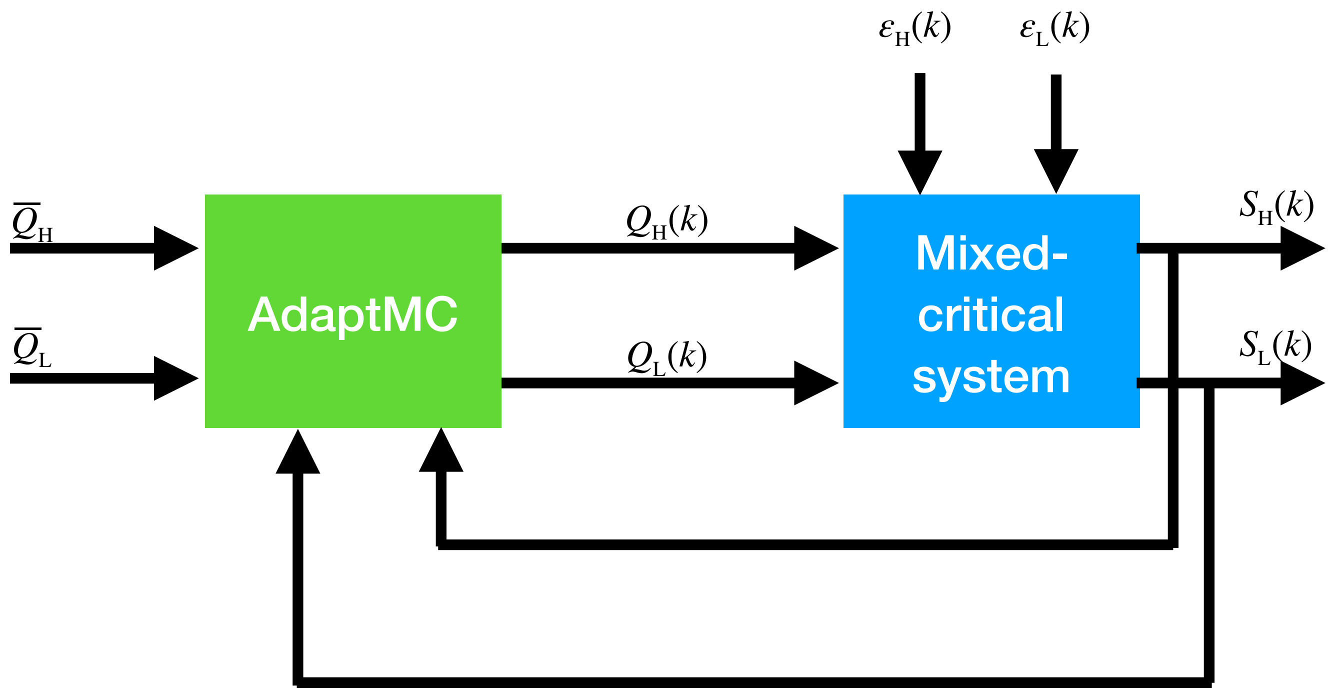


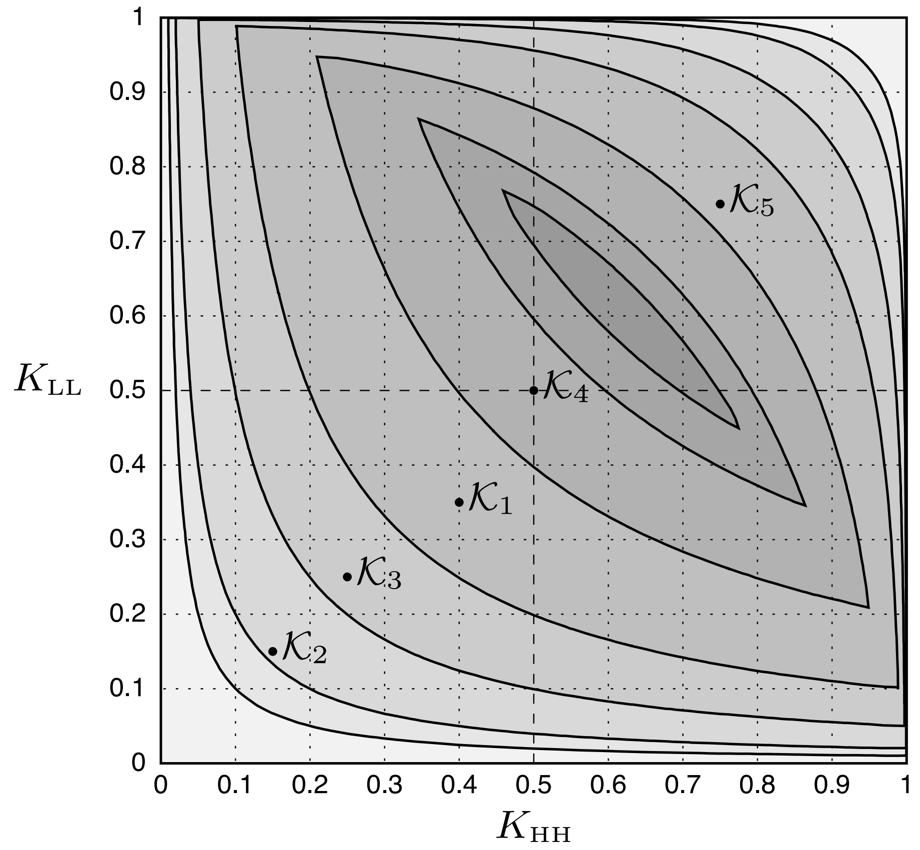
Conclusion and future work

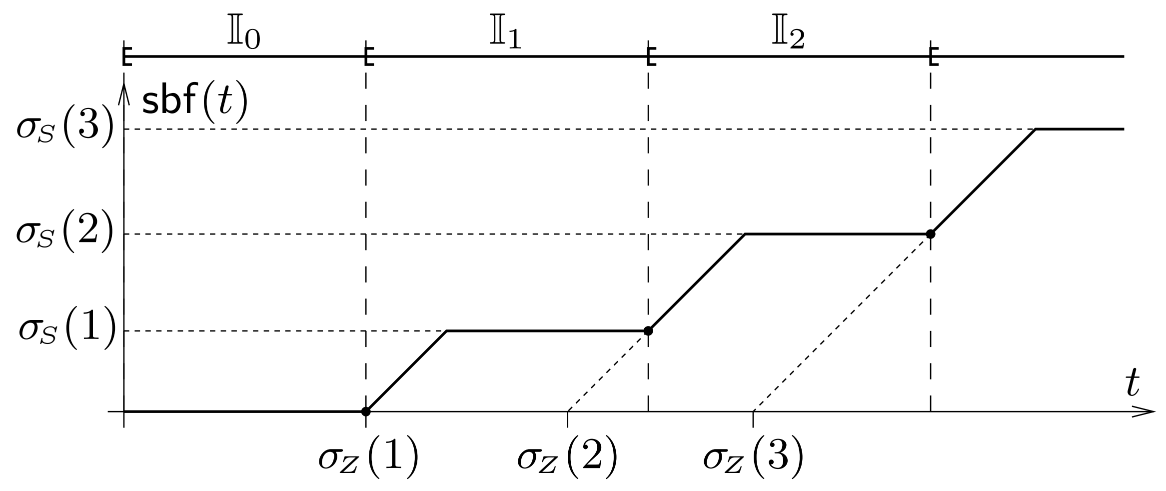
- **Control-theoretic approach for run-time adaptation in mixed-critical systems**
  - Compensation property
  - Stability conditions
  - Supply bound functions

- **Future work**
  - Optimal gain calculation
  - More criticality levels

Questions, comments, remarks?







Alessandro Papadopoulos
alessandro.papadopoulos@mdh.se

Code available: https://github.com/apapadopoulos/AdaptMC
Artifact: http://drops.dagstuhl.de/opus/volltexte/2018/8969/