RUHR-UNIVERSITÄT BOCHUM
Institute of Automation and Computer Control
Prof. Dr.-Ing. Jan Lunze

Universitätsstr. 150 Phone +49-(0)234 32-28071
D-44805 Bochum Fax +49-(0)234 32-14101

Fault tolerance in networked control systems by flexible task assignment

Kai Schenk
schenk@atp.rub.de

1 Fault-tolerant systems

The fault-tolerant control of technical systems is an important means for avoiding safety-critical situations and for reducing machine and plant malfunctions due to faults. Active fault tolerance is created by extending the execution layer consisting of the plant P and the controller C^* by a monitoring layer, in which a diagnostic unit D is responsible for detecting and identifying faults and a reconfiguration unit R adapts the nominal controller to the fault situation [1].

One feature of a fault-tolerant system should be its capability to perform its nominal task even if components have failed partially or completely. In systems that are composed of coupled subsystems, the complexity of the fault scenarios increase with the number of components, but simultaneously the freedom in selecting counteractive measures is enhanced by the communication network.

2 Flexible task assignment

This project is motivated by the observation that in many applications networked control systems have to exhibit a certain kind of cooperative behavior [2]. Power plants jointly cover the energy requirements of a city, trucks drive together in a convoy and tugboats manoeuvre together large oil transporters in ports. Usually, the common behavior of the overall system cannot be evaluated by a single subsystem, making direct control of this variable challenging. Instead, the idea of this project is to decompose the cooperative task into suitable subtasks that are then assigned to each subsystem.

In the context of fault-tolerant control, cooperative tasks allow to achieve fault tolerance by redistributing subtasks after the occurrence of a fault. The monitoring layer does not restore the functionality of the faulty subsystem, but ensures the accomplishment of the cooperative behavior by assigning new subtasks to the subsystems [2], [3]. This new method for achieving fault tolerance in networked systems significantly distinguishes from the conventional approach in the literature. This more holistic approach is motivated by several reasons:

- The utilization of the methods for fault-tolerant control proposed in literature requires that any faulty subsystem has redundant components to compensate local faults. However, many applications shows that redundancy is more likely to occur within the other healthy subsystems.

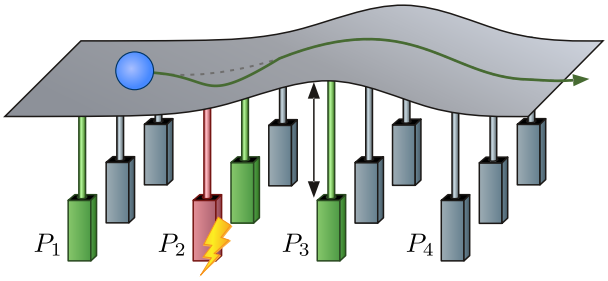

Figure 1: Example for cooperatively acting systems.

- It seems unreasonable to use the faulty but reconfigured subsystem as long as the reason that caused the fault is present, even if the nominal performance is initially restored by a suitable redesign of the control system.
- A redistribution of tasks is more intuitive compared to an adjustment of the controller, because the task has a direct relation to the application and, hence the redistribution process is understandable for the operators.

3 Transportation system

Figure 1 shows a part of a transportation system that is used to illustrate cooperatively acting systems. The linear actuators have the cooperative task to steer the ball along some prescribed trajectory. The control problem requires to find the specific motion for each of the linear actuators that pushes the ball from the left to the right. Thereby it must be considered that the actuators can perform the required behavior. Particularly in the fault case, the actuators have very limited capabilities.

4 Contribution of this project

The aim of this project is to develop a method for the cooperative control of networked systems in which fault tolerance is achieved by redistributing subtasks from faulty to non-faulty subsystems. The cooperative task refers to a performance output

$$\boldsymbol{y}_\mathrm{p}(t) = \boldsymbol{Q}(\sigma(t)) \cdot \begin{bmatrix} y_1(t) & y_2(t) & \cdots & y_N(t) \end{bmatrix}^\mathrm{T} \qquad (1)$$

in which the matrix $\boldsymbol{Q}(\sigma)$ depends on a switching state $\sigma(t)$. The cooperative task of all subsystems is to steer $\boldsymbol{y}_\mathrm{p}(t)$ along a prescribed reference $\boldsymbol{y}_\mathrm{p}^*(t)$: $\boldsymbol{y}_\mathrm{p}(t) = \boldsymbol{y}_\mathrm{p}^*(t)$.

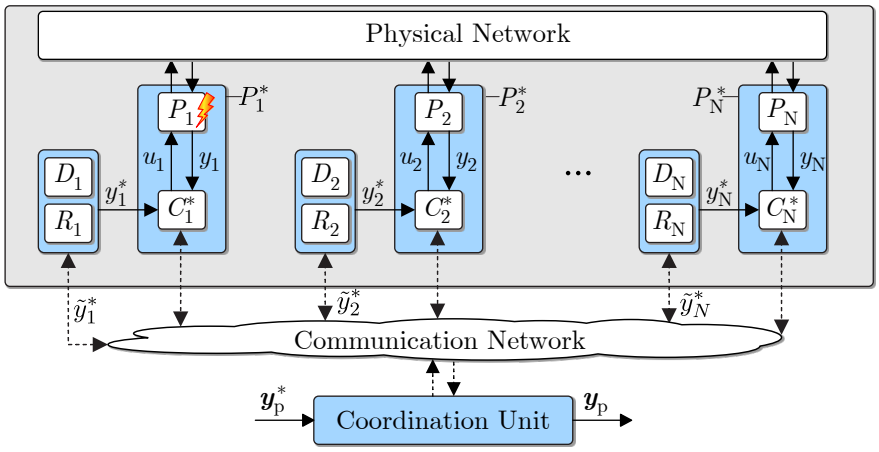

Figure 2: Task assignment in networked systems: The coordination unit decomposes the cooperative task into partial subtasks $\tilde{y}_i^*$, which are used by the reconfiguration units R_i to provide the local controller with a reference $y_i^*(t)$.

The control problem is to find control signals $u_1(t)$, $u_2(t)$, ..., $u_N(t)$ that steer the output of the subsystems $y_1(t)$, $y_2(t)$, ..., $y_N(t)$ in a way such that the performance output (1) follows the reference $\boldsymbol{y}_\mathrm{p}^*(t)$. This project proposes a two-stage process to solve that control problem:

1. **Task assignment:** The reference $\boldsymbol{y}_\mathrm{p}^*(t)$ is decomposed into suitable local references $y_1^*(t)$, $y_2^*(t)$, ..., $y_N^*(t)$ considering the switching character of the overall system.
2. **Trajectory tracking:** Based on the local references $y_1^*(t)$, $y_2^*(t)$, ..., $y_N^*(t)$, networked controllers C_1^*, C_2^*, ..., C_N^* are designed [4] that generate control signals $u_1^*(t)$, $u_2^*(t)$, ..., $u_N^*(t)$ that steer each output along the corresponding reference.

Fault-tolerant control problem: Given the reference performance output $\boldsymbol{y}_\mathrm{p}^*(t)$, find suitable reference trajectories $y_i^*(t)$ for all $i = 1, 2, \ldots, N$ that ensure the fulfillment of the cooperative task $\boldsymbol{y}_\mathrm{p}(t) = \boldsymbol{y}_\mathrm{p}^*(t)$, even in the case of faults.

The specific structure used in this chapter to solve the fault-tolerant control problem is shown in Fig. 2, which is basically a combination of the general fault-tolerant control loop and networked control systems. A coordination unit divides the common task into suitable subtasks. Thereby it is considered that the subsystems are subject to certain restrictions and, hence, cannot fulfil arbitrary subtasks. In particular, faulty subsystems can fulfil tasks only to a limited extent. Each subtask defines the reference trajectory $\tilde{y}_i^*(t)$ of the associated subsystem for a specific time interval, which takes the fact into account that the subsystems do not have a permanent influence on the performance output due to the switching character of the system. Each reconfiguration unit R_i, $(i \in \{1, 2, \ldots, N\})$, contains a unit for trajectory generation that complements the partially defined reference in order to provide the local controllers with a reference defined on the complete time interval. The developed method for fault tolerance is able to satisfy the following three properties:

1. The coordination unit is able to decompose the cooperative task into suitable subtasks.
2. Each subsystem is able to satisfy its subtask.
3. The cooperative task is jointly performed by all subsystems, even if subsystems are defective or temporarily have no influence on the overall objective.

Classification of task assignment in active fault-tolerant control. Faults have a serious impact on the subsystems in which they occur as well as on the entire system as they can cause performance degradation, loss of tracking ability or even instability and the shut-down of a process. The monitoring layers (D_i, R_i), shown in Fig. 2, are designed to compensate for the fault and its consequences in the following three stages:

1. The fault in subsystem P_f is detected, isolated and identified by the diagnostic unit D_f.
2. The reconfiguration units R_i, $(i \in \{1, 2, \ldots, N\})$, adapt the nominal controllers to guarantee stability of the entire system. This step will generally not recover the nominal performance in terms of the ability to follow a certain reference trajectory.
3. The coordination unit has to redistribute the subtasks to guarantee the fulfillment of the cooperative task.

References

[1] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer, 2016.

[2] K. Schenk and J. Lunze. Fault tolerance in networked control systems through flexible task assignment. In *Proc. of 2019 4th Conf. on Control and Fault Tolerant Systems*, pages 257–263, Morocco, 2019.

[3] K. Schenk, B. Gülbitti, and J. Lunze. Cooperative fault-tolerant control of networked control systems. In *Proc. of 10th Symposium on Fault Detection, Supervision and Safety for Technical Processes*, pages 570–577, Poland, 2018.

[4] K. Schenk and J. Lunze. Tracking control of networked and interconnected systems. In *Proc. of 7th IFAC Workshop on Distributed Estimation and Control in Networked Systems*, pages 40–45, Netherland, 2018.