553g Fault-Tolerant Process Control: Nonlinear Fdi and Reconfiguration

Charles McFall, Adiwinata Gani, Prashant Mhaskar, Panagiotis D. Christofides, and James F. Davis

Chemical plants are large-scale systems that involve a complex, distributed arrangement of a number of processing units (reactors, distillation columns, absorbers, pumps, heat exchangers, etc.) connected in series or in parallel, with recycle of material and energy integration among various parts of the plant. The interconnections among the different units imply that faults will have consequences for the stability and performance of, not only the particular units where the faults may have originated, but other units as well. The interconnection of the units, however, complicates the problem of locating and isolating the fault especially when faults in one unit may cause faults in other units. In some severe cases, if not diagnosed and treated quickly and adequately, the effects of a fault originating in one unit may manifest itself, propagate , and develop into a total failure that forces shutdown of all the units.

In [1] a hybrid systems approach was employed where upon occurrence of a fault, stability region-based rules are used to decide which of the available backup control configuration should be implemented (reconfiguration) to achieve fault-tolerant control. The reconfiguration in [1], however, focused on a single unit and assumed the availability of fault-detection mechanisms that provided information about the occurrence of faults. More recently, in [2] we considered single actuator systems and proposed an integrated framework for designing fault-detection filters based on available process measurements and implementing fault-tolerant control. The operation of chemical processes, however, involves the use of multiple actuators; in this case the filter not only needs to detect the occurrence of a fault, but also needs to isolate the fault, i.e., identify which particular actuator has failed, or in the case of multiple actuators failing at the same time, to isolate the set of actuators that have failed.

Motivated by the considerations above, we consider the problem of fault-detection and isolation and reconfiguration in nonlinear processes when there can be multiple control system/actuator failures. For the processes under consideration, a family of candidate control configurations, characterized by different manipulated inputs, is first identified. We then draw upon observer-based nonlinear fault-detection and isolation technologies to design a filter to detect and isolate the fault. The filter uses available measurements and geometric techniques that exploit the system structure to construct residuals dedicated to each actuator, such that the failure of a given actuator uniquely triggers its residual value to become non-zero. Once the fault is isolated, reconfiguration is carried out on the basis of stability region information for the backup control configurations. To this end, for each control configuration, a Lyapunov-based controller, that enforces asymptotic closed-loop stability in the presence of constraints, is designed, and the constrained stability region, associated with it, is explicitly characterized. A switching policy is then derived to orchestrate the activation/deactivation of the constituent control configurations in a way that guarantees closed-loop stability . Simulation studies are presented to demonstrate the implementation and evaluate the effectiveness of the proposed fault-detection and isolation and reconfiguration scheme.

References:

[1] El-Farra, N., A. Gani and P. D. Christofides, Fault-Tolerant Control of Process Systems Using Communication Networks, AIChE J., 51, 1665-1682, 2005.

[2] Mhaskar, P., A. Gani, N. H. El-Farra, P. D. Christofides and J. F. Davis, Integrated Fault Detection and Fault-Tolerant Control of Process Systems, Proceedings of 16th International Federation of Automatic Control World Congress, to appear, Prague, Czech Republic, 2005.