454g Failure Analysis in Networked Process Control Systems with Control and Communication Constraints

Nael H. El-Farra

Chemical plants are large-scale systems that involve a complex, distributed arrangement of processing units connected in series or in parallel, with recycle of material and energy among various parts of the plant. The ability of a plant to function safely and efficiently depends to a large extent on effective communication and information sharing between the interconnected units. With the significant growth in computing and networking abilities in recent times, as well as the rapid advances in actuator/sensor technologies, there has been an increased reliance on distributed computing and process operations across computer networks. The process industry is moving towards sensor and control systems that are accessed over networks rather than hardwired. Recently, network standards such as Hartbus®, Fieldbus®, and Industrial Ethernet have become commonplace in the process industry for reliable plant-wide measurement and distributed control. Compared with the point-to-point cables, the introduction of serial communication networks has many advantages, such as high system testability and resource utilization, as well as low weight, space, power and wiring requirements. In addition, the flexibility and ease of diagnosis of a system using a network to transfer information is an appealing goal. Systems designed in this manner allow for easy modification of the control strategy by rerouting signals, having redundant systems that can be activated automatically when component failure occurs, and in general they allow having a high--level supervisor control over the entire plant.

Recently modeling, analysis and control of networked control systems (NCSs) has emerged as a topic of significant interest to the control community (e.g., see [4]-[7]). The defining feature of any NCS is that information (reference input, plant output, control input) is exchanged using a digital bandlimited serial communication channel among control system components (sensors, controller, actuators). The communication channel is typically shared by other feedback control loops. The insertion of a communication network in the feedback control loop makes the analysis and design of an NCS more challenging. Conventional control theory with many ideal assumptions, such as synchronized control and non-delayed sensing and actuation, must be reevaluated to allow the integration of the limitations on communication capabilities within the control design framework. Issues such as network-induced delays, data losses and signal quantization represent some of the more common problems that have to be dealt in this context, and that have motivated significant research work in this area. In the context of chemical process applications, these issues may vary in their levels of significance depending on the process time-scale and the typical rates used for data transmission. For example, communication delays are not a significant concern for most chemical processes due to slow process dynamics. However, for fast-acting control loops, such as local regulatory control involving flows or gas pressure, these delays can degrade closed-loop performance and even lead to instability. Also, depending on the number of bits implemented by industrial networks to represent data, quantization effects may be important. A critical issue, however, that must always be considered in the design of any networked process control system is its robustness with respect to failure situations. By network failure, we mean a total breakdown in the communication between the control system components as a result of, for example, some physical malfunction in the networking devices or severe overloading of the network resources that causes a network shut down.

The immediate result of complete network failure is the loss of all the associated sensor and actuator signals, which in effect switches the plant from a closed-loop to an open-loop mode of operation. For stable plants this may lead to performance degradation only, while for unstable plants it may lead to instabilities. Note that packet losses, which are inevitable in any well-functioning network, lead also to data losses. However, such losses typically occur intermittently and do not cause a breakdown in communication. The losses resulting from network failure, on the other hand, are more prolonged and

sustained over time. Also, unlike the problems of sensor or controller failure in the classical (hardwired) control architecture, where the failure effects maybe confined to a specific control loop, the effects of network failure are typically more severe in the sense that they cause a breakdown in the sensor-controller-actuator communication for multiple loops simultaneously. Depending on the extent to which network architecture is centralized, thousands of sensors and actuators could be connected through the same network and thus suffer the consequences of plant-wide communication failure.

While the designer could try to minimize failure prospects by adopting a decentralized network architecture (e.g., [4]) or selecting efficient communication protocols, there is a need for a systematic, quantitative assessment of the fundamental limitations imposed by network failure on the ability to maintain the desired control objectives in the NCS. An assessment of the robustness of a given NCS, in terms of the duration and frequency of the failure events it can tolerate, is important for a number of reasons. One is the fact that this analysis allows designers to identify the fault-tolerance limits of a given NCS and thus helps determine a priori whether the desired control objectives can be met with a certain kind of network. Another important motivation to analyze network failure is the fact that this analysis can be helpful in situations where the introduction of failure events is desirable in some sense. For example, considerations such as minimizing communication costs and/or maximizing the service life of the network may motivate the designers and operators to suspend the communication purposefully from time to time. Knowledge of how prolonged and how frequent these suspensions, or "failures", can be without losing the desired control objectives is critical in this case. A fundamental tradeoff always exists between bandwidth limitations, which favor reduced communication of measurements, and optimum control performance, which favors increased communication of measurements (e.g., [1]). The analysis of network failure helps elucidate how to balance this tradeoff.

In this work, we present a methodology for the analysis and design of networked process control systems with network failures. The proposed methodology brings together tools from hybrid systems theory and Lyapunov-based analysis and controller design techniques (for recent examples of hybrid systems applications in process control, see [3], [4]). Within a hybrid system framework, the NCS is modeled as a switched system that transits between two modes, a failed mode and a healthy mode. To characterize the fault-tolerance limit of a given network, we initially consider the case when no control constraints are present. By using a piecewise Lyapunov function, we show that if the unavailability rate of the network is smaller than a specified constant and the average time interval between network failures is large enough, then global asymptotic closed-loop stability can be preserved. The significance of this result is the fact that it indicates that, in the absence of control constraints, preserving stability imposes a limit only on the average time interval between network failures. Therefore, long failure intervals can be tolerated as long as they are not too frequent and are followed by a sufficient number of no-failure intervals. A fundamentally different result emerges when hard constraints on the control actuators are considered in the design problem. Stability analysis in this case reveals that restrictions on the average time interval between failure events alone are no longer sufficient to guarantee closed-loop stability, and that restrictions must be placed on the length of each individual failure interval. The reason is the need to prevent the possible escape of the closed-loop trajectory from the stability region imposed by the control constraints (e.g., [2]) during any such interval. To estimate the maximum time interval that the constrained NCS can tolerate, Lyapunov techniques are used to construct appropriate invariant sets to estimate the constrained stability region, and compute the time needed to escape the stability region. Even though derived for the case of general network failure, the results are applicable to the analysis of classical controller and sensor failure problems that can also be modeled as "communication failures." Finally, the theoretical results are applied to the problem of stabilization of an unstable plant that consists of multiple interconnected processing units, with actuators and sensors connected through a communication network.

References:

[1] Brockett, R. "Minimum attention control," In: Proceedings of 36th IEEE Conference on Decision and Control, pp. 2628-–2632, San Diego, CA, 1997.

[2] El-Farra, N. H. and P. D. Christofides. "Bounded robust control of constrained multivariable nonlinear processes," Chem. Eng. Sci., 58:3025-–3047, 2003.

[3] El-Farra, N. H. and P. D. Christofides. "Coordinating feedback and switching for control of hybrid nonlinear processes," AIChE J., 49:2079–-2098, 2003.

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

[5] Tipsuwan, Y. and M. Y. Chow. "Control methodologies in networked control systems," Contr. Eng. Prac., 11:1099-–1111, 2003.

[6] Ydstie, E. B. "New vistas for process control: integrating physics and communication networks," AIChE J., 48:422-–426, 2002.

[7] Zhang, W., M. S. Branicky, and S. M. Phillips, "Stability of networked control systems," IEEE Control Systems Magazine, 21: 84--99, 2001.